Barrier-free document
Barrierefreies Dokument

**In the following, "GDPR" shall automatically include the "UK-GDPR" and corresponding legal provisions of the Swiss Federal Data Protection Act (FDPA) and any laws and regulations enacted by Member States and/or other jurisdictions, if required or necessary to comply with these laws.**

**This document also includes the California-Specific Description of Consumers' Privacy Rights of the Business (CCPA/CPRA), and transparency information regarding PDPL (United Arab Emirates), PIPL (People's Republic of China), DPDPA (India) and other laws identified below.**

**The information contained in this Transparancy Document shall also inform all data subjects, including business partners, suppliers and customers and their employees, our employees and job applicants, from all other jurisdictions that are not named or mentioned specifically. If you miss information regarding your jurisdiction, please contact Heiko Jonny Maniero (info@dg-datenschutz.de). He will provide you with additional country or state specific information regarding your specific jurisdiction.**

## A. Identity and the contact details of the Controller (Art. 13 I lit. a, 14 I lit. a GDPR/UK-GDPR, FDPA) and the Business under CCPA/CPRA, PDPL, PIPL, DPDPA and under other laws identified below or applicable to the data subject.

For all customer[1], supplier, employee and applicants' data in possession of the following company and related processing activities the Controller/Business is:

Hforce AG

Chollerstrasse 35

6300 Zug

or the company or business you received an email or other communication from, identified with is details in such email or other communication.

## B. Contact details of the Data Protection Officer (Art. 13 I lit. b, 14 I lit. b GDPR/UK-GDPR) and the Business under CCPA/CPRA, PDPL, PIPL, DPDPA and under aother laws identified below or applicable to the data subject.

Prof. Dr. h.c. Heiko Jonny Maniero, LL.B., LL.M. mult., M.L.E.*
Franz-Joseph-Str. 11
80801 München (Germany)
Phone: (+49) 0800-6264376
Email: info@dg-datenschutz.de
Website: https://dg-datenschutz.de/

*Obligatory information, please see our website.

[1] For reasons of better readability, the simultaneous use of the language forms male, female, diverse and other gender identities (m/f/d/other) are not used on our websites, in publications and communication. All language used shall equaly apply to all genders.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

**C. Identity and contact details of all non-EU controller's EU representative (Article 27 GDPR)**

Heiko Maniero E-Mail: info@dg-datenschutz.de
Franz-Joseph-Str. 11, 80801 München, Bayern, Germany.

**D. Identity and contact details of controller's UK representative (Article 27 UK-GDPR)**

Heiko Maniero E-Mail: info@dg-datenschutz.de
120 High Road, East Finchley, N2 9ED, London, England, United Kingdom.

**E. Identity and contact details of controller's representative in Switzerland (Art. 14 FDPA)**

Heiko Maniero E-Mail: info@dg-datenschutz.de
c/o Cancellarius AG, Attn. Heiko Maniero, Pflanzschulstrasse 3, 8400 Winterthur, Switzerland.

**F. Identity and contact details of the data protection advisor Switzerland (Art. 10 FDPA)**

Antoine Parella E-Mail: office@cancellarius.ch
c/o Cancellarius AG, Attn. Antoine Parella, Pflanzschulstrasse 3, 8400 Winterthur, Switzerland.

**G. Contact person, who is authorized to respond to inquiries or complaints regarding the personal information processing (Art. 6 (1) of the Standard Contract for Outbound Cross-border Transfer of Personal Information for China)**

Heiko Maniero E-Mail: info@dg-datenschutz.de
Franz-Joseph-Str. 11, 80801 München, Bayern, Germany.

**H. Identity and contact details of the controller's contact person for CCPA/CPRA inquiries.**

Heiko Maniero E-Mail: info@dg-datenschutz.de
Franz-Joseph-Str. 11, 80801 München, Bayern, Germany.

USA/Canada Toll Free: +1 (800) 295-8960

(DIRECT LINE TO THE PRIVACY OFFICER - FOR CCPA/CPRA INQUIERIES ONLY)

**I. Data Protection Supervisory Authorities**

The following data protection supervisory authorities are responsible for the Controller/Business.

**EU Lead Data Protection Supervisory Authority (Responsible for EU Data Subjects)**

Bayerisches Landesamt für Datenschutzaufsicht, Promenade 18, 91522 Ansbach

**Data Protection Authority of Switzerland (Responsible for Data Subjects from Switzerland)**

Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter, Feldeggweg 1, 3003 Bern, Switzerland.

**UK Data Protection Supervisory Authority (Responsible for Data Subjects from the UK)**

Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF, United Kingdom.

**California Privacy Protection Agency (CPPA) (Responsible for Data Subjects from California)**

California Privacy Protection Agency (CPPA), 2101 Arena Blvd, Sacramento, CA 95834, USA.

**Data Protection Authority of the United Arab Emirates (Responsible for Data Subjects from UAE)**

UAE Data Office at Telecommunications and Digital Government Regulatory Authority (https://tdra.gov.ae/en/).


© All rights reserved by Heiko Maniero.

## Data Protection Authority of China (Responsible for Data Subjects from China)

Cyberspace Administration of China (CAC) (http://www.cac.gov.cn/) with its local branches.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

# Table of Contents


GERMAN: Information über die Verarbeitung personenbezogener Daten (Artikel 13, 14 DS-GVO) ..... 6
GERMAN: Mitarbeiter- und Bewerberinformation über die Verarbeitung personenbezogener Daten (Artikel 13, 14 DS-GVO) ..... 24

ENGLISH: Information about the Processing of Personal Data (Article 13, 14 GDPR) ..... 41
ENGLISH: Information about the Processing of Personal Data for Employees and Applicants (Article 13, 14 GDPR) ..... 57

SPANISH: Información sobre el tratamiento de datos personales (Artículos 13, 14 RGPD) ..... 71
SPANISH: Información sobre el tratamiento de datos personales de los empleados y solicitantes (artículo 13, 14 del RGPD) ..... 89

FRENCH: Information sur le traitement des données à caractère personnel (Articles 13 et 14 RGPD) ..... 105
FRENCH: Information sur le traitement des données à caractère personnel des employés et des candidates (Articles 13 et 14 RGPD) ..... 122

ITALIAN: Informazioni sul trattamento dei dati personali (articolo 13, 14 GDPR) ..... 138
ITALIAN: Informazioni sul trattamento dei dati personali per dipendenti e richiedenti (articolo 13, 14 GDPR) ..... 155

DUTCH: Informatie over de verwerking van persoonsgegevens (Artikel 13, 14 AVG) ..... 170
DUTCH: Informatie over de verwerking van persoonsgegevens voor werknemers en sollicitanten (artikel 13, 14 AVG) ..... 187

GREEK: Πληροφορίες σχετικά με την επεξεργασία δεδομένων προσωπικού χαρακτήρα (Άρθρα 13, 14 ΓΚΠΔ) ..... 203
GREEK: Πληροφορίες σχετικά με την επεξεργασία δεδομένων προσωπικού χαρακτήρα Εργαζομένων και Υποψηφίων (Άρθρα 13, 14 ΓΚΠΔ) ..... 221

POLISH: Informacja o przetwarzaniu danych osobowych (Artykuł 13 i 14 RODO) ..... 238
POLISH: Informacja o przetwarzaniu danych osobowych pracowników i kandydatów (art. 13 i 14 RODO) ..... 255

HUNGARIAN: Információk személyes adatok kezeléséről (GDPR 13., 14. cikk) ..... 271
HUNGARIAN: A munkavállalók és pályázók személyes adatainak feldolgozásáról szóló információk (GDPR, 13. és 14. cikk) ..... 288

ROMANIAN: Informații despre prelucrarea datelor cu caracter personal (Articolul 13, 14 GDPR) ..... 304
ROMANIAN: Informații privind prelucrarea datelor cu caracter personal pentru angajați și solicitanți (articolul 13, 14 GDPR) ..... 321

CROATIAN: Informacije o obradi osobnih podataka (članak 13, 14 GDPR) ..... 337
CROATIAN: Informacije o obradi osobnih podataka za zaposlenike i podnositelje zahtjeva (članak 13, 14 GDPR) ..... 352

SERBIAN: Информације о обради личних података (члан 13, 14 ГДПР) ..... 367
SERBIAN: Информације о обради личних података за запослене и подносиоце захтева (члан 13, 14 ГДПР) ..... 383

RUSSIAN: Информация об обработке персональных данных (статья 13, 14 Общий Регламент по Защите Данных, ОРЗД (GDPR)) ..... 398
RUSSIAN: Информация об обработке персональных данных для сотрудников и заявителей (статья 13, 14 Общий Регламент по Защите Данных, ОРЗД (GDPR)) ..... 413

INDONESIAN: Informasi tentang Pemrosesan Data Pribadi (Pasal 13, 14 GDPR) ..... 427
INDONESIAN: Informasi tentang Pemrosesan Data Pribadi untuk Karyawan dan Pelamar (Pasal 13, 14 GDPR) ..... 443

JAPANESE: 個人情報の取り扱いに関するご案内 (GDPR第13条、第14条) ..... 458
JAPANESE: 従業員および応募者の個人データ処理に関する情報（GDPR第13条、第14条） ..... 474

TURKISH: Kişisel Verilerin İşlenmesi Hakkında Bilgilendirme (GDPR Madde 13, 14) ..... 490
TURKISH: Çalışanlar ve Başvuru Sahipleri için Kişisel Verilerin İşlenmesi Hakkında Bilgilendirme (GDPR Madde 13, 14) ..... 505

UKRAINIAN: Інформація про обробку персональних даних (стаття 13, 14 GDPR) ..... 519
UKRAINIAN: Інформація про обробку персональних даних для працівників та заявників (стаття 13, 14 GDPR) ..... 536

CHINESE：有**关个人数据**处理的信息（GDPR第13、14条）。 ..... 551
CHINESE：雇员和申请人的个人数据处理信息（GDPR第13、14条）。 ..... 566

CZECH: Informace o zpracování osobních údajů (článek 13, 14 GDPR) ..... 581
CZECH: Informace o zpracování osobních údajů zaměstnanců a uchazečů (článek 13, 14 GDPR) ..... 597

BULGARIAN: Информация за обработката на лични данни (член 13, 14 от ОРЗД) ..... 612
BULGARIAN: Информация за обработката на лични данни за служители и кандидати (член 13, 14 от ОРЗД) ..... 630

ESTONIAN: Teave isikuandmete töötlemise kohta (GDPR artiklid 13, 14) ..... 647
ESTONIAN: Teave töötajate ja taotlejate isikuandmete töötlemise kohta (GDPR artiklid 13, 14) ..... 663




Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

SWEDISH: Information om behandling av personuppgifter (artikel 13, 14 GDPR) ..... 679
SWEDISH: Information om behandling av personuppgifter för anställda och sökande (artikel 13, 14 GDPR) ..... 695

SLOVENIAN: Informacije o obdelavi osebnih podatkov (13., 14. člen SUVP) ..... 710
SLOVENIAN: Informacije o obdelavi osebnih podatkov za zaposlene in kandidate (13., 14. člen SUVP) ..... 726

SLOVAK: Informácie o spracovaní osobných údajov (článok 13, 14 GDPR) ..... 742
SLOVAK: Informácie o spracúvaní osobných údajov zamestnancov a uchádzačov (článok 13, 14 GDPR) ..... 758

PORTUGUESE: Informação sobre o Processamento de Dados Pessoais (Artigo 13, 14 GDPR) ..... 773
PORTUGUESE: Informação sobre o Processamento de Dados Pessoais para Empregados e Candidatos (Artigo 13, 14 GDPR) ..... 790

MALTESE: Informazzjoni dwar l-Ipproċessar tad-Data Personali (Artikolu 13, 14 GDPR) ..... 806
MALTESE: Informazzjoni dwar l-Ipproċessar tad-Data Personali għall-Impjegati u l-Applikanti (Artikolu 13, 14 GDPR) ..... 822

LATVIAN: Informācija par personas datu apstrādi (VDAR 13., 14. pants) ..... 837
LATVIAN: Informācija par darbinieku un pretendentu personas datu apstrādi (VDAR 13., 14. pants) ..... 853

LITHUANIAN: INFORMACIJA APIE ASMENS DUOMENŲ Tvarkymą (BDAR 13, 14 straipsniai) ..... 868
LITHUANIAN: Informacija apie darbuotojų ir kandidatų asmens duomenų tvarkymą (BDAR 13, 14 straipsniai) ..... 885

IRISH: Faisnéis faoi Phróiseáil Sonraí Pearsanta (Airteagal 13, 14 GDPR) ..... 901
IRISH: Eolas faoi Phróiseáil Sonraí Pearsanta le haghaidh Fostaithe agus Iarratasóirí (Airteagal 13, 14 GDPR) ..... 918

FINNISH: Tietoa henkilötietojen käsittelystä (tietosuoja-asetuksen 13 ja 14 artikla) ..... 934
FINNISH: Tietoa työntekijöiden ja hakijoiden henkilötietojen käsittelystä (tietosuoja-asetuksen 13 ja 14 artikla) ..... 951

DANISH: Oplysninger om behandling af personoplysninger (Artikel 13, 14 GDPR) ..... 967
DANISH: Information om behandling af personoplysninger for medarbejdere og ansøgere (Artikel 13, 14 GDPR) ..... 983

NORWEGIAN: Informasjon om behandling av personopplysninger (artikkel 13 og 14 i GDPR) ..... 999
NORWEGIAN: Informasjon om behandling av personopplysninger for ansatte og søkere (artikkel 13 og 14 i GDPR) ..... 1015

ICELANDIC: Upplýsingar um vinnslu persónuupplýsinga (13. gr., 14 GDPR) ..... 1030
ICELANDIC: Upplýsingar um vinnslu persónuupplýsinga fyrir starfsmenn og umsækjendur (13. gr., 14 GDPR) ..... 1045

ENGLISH: California-Specific Description of Consumers' Privacy Rights (CCPA/CPRA) ..... 1060

ENGLISH: Information about the Processing of Personal Data (Decree Law No. 45 of 2021 (PDPL) - United Arab Emirates) ..... 1077
ARABIC: Information about the Processing of Personal Data (Decree Law No. 45 of 2021 (PDPL) - United Arab Emirates) ..... 1086

ENGLISH: Information about the Handling of Personal Data, including Personal Information Handling Rules (Personal Information Protection Law of the People's Republic of China - PIPL) ..... 1096
中译文：个人数据处理（包括个人信息处理规则）告知书（中华人民共和国个人信息保护法-PIPL） ..... 1104

ENGLISH: Information about the Processing of Personal Data (Digital Personal Data Protection Act, 2022 of India - DPDPA) ..... 1111

GERMAN: Information über die Bearbeitung von Personendaten nach dem Datenschutzgesetz (DSG) und der Datenschutzverordnung (DSV) der Schweiz ..... 1117
ITALIAN: Informazioni sul trattamento dei dati personali ai sensi della Legge sulla protezione dei dati (DSG) e dell'Ordinanza sulla protezione dei dati (DSV ) della Svizzera. ..... 1127
FRENCH: Information sur le traitement des données personnelles conformément à la loi sur la protection des données (LPD) et à l'ordonnance sur la protection des données (OPD) de la Suisse ..... 1137


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

# GERMAN: Information über die Verarbeitung personenbezogener Daten (Artikel 13, 14 DS-GVO)

Sehr geehrte Damen und Herren,

die personenbezogenen Daten jedes Einzelnen, der in einer vertraglichen, vorvertraglichen oder anderweitigen Beziehung zu unserem Unternehmen steht, verdienen besonderen Schutz. Wir haben das Ziel, unser Datenschutzniveau auf einem hohen Standard zu halten. Deswegen setzen wir auf eine routinemäßige Weiterentwicklung unserer Datenschutz- und Datensicherheitskonzepte.

Selbstverständlich halten wir die gesetzlichen Vorschriften zum Datenschutz ein. Nach Art. 13, 14 DS-GVO treffen Verantwortliche besondere Informationspflichten, wenn sie personenbezogene Daten erheben. Durch dieses Dokument erfüllen wir diese Verpflichtungen.

Die Terminologie gesetzlicher Vorschriften ist kompliziert. Bei der Ausarbeitung dieses Dokuments konnte leider nicht auf die Verwendung von juristischen Begriffen verzichtet werden. Daher möchten wir darauf hinweisen, dass Sie sich bei allen Fragen zu diesem Dokument, zu den verwendeten Fachbegriffen oder Formulierungen gerne an uns wenden dürfen.

## I. Erfüllung der Informationspflichten im Falle der Erhebung von personenbezogenen Daten bei der betroffenen Person (Art. 13 DS-GVO)

### A. Name und Kontaktdaten des Verantwortlichen (Art. 13 I lit. a DS-GVO)

Siehe oben

### B. Kontaktdaten des Datenschutzbeauftragten (Art. 13 I lit. b DS-GVO)

Siehe oben

### C. Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen, sowie die Rechtsgrundlage für die Verarbeitung (Art. 13 I lit. c DS-GVO)

Zweck der Verarbeitung personenbezogener Daten ist die Abwicklung sämtlicher Vorgänge, die den Verantwortlichen, Kunden, Interessenten, Geschäftspartner oder sonstige vertragliche oder


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

vorvertragliche Beziehungen zwischen den genannten Gruppen (im weitesten Sinne) oder gesetzliche Pflichten des Verantwortlichen betreffen.

Art. 6 I lit. a DS-GVO dient unserem Unternehmen als Rechtsgrundlage für Verarbeitungsvorgänge, bei denen wir eine Einwilligung für einen bestimmten Verarbeitungszweck einholen. Ist die Verarbeitung personenbezogener Daten zur Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, erforderlich, wie dies beispielsweise bei Verarbeitungsvorgängen der Fall ist, die für eine Lieferung von Waren oder die Erbringung einer sonstigen Leistung oder Gegenleistung notwendig sind, so beruht die Verarbeitung auf Art. 6 I lit. b DS-GVO. Gleiches gilt für solche Verarbeitungsvorgänge die zur Durchführung vorvertraglicher Maßnahmen erforderlich sind, etwa in Fällen von Anfragen zu unseren Produkten oder Leistungen. Unterliegt unser Unternehmen einer rechtlichen Verpflichtung durch welche eine Verarbeitung von personenbezogenen Daten erforderlich wird, wie beispielsweise zur Erfüllung steuerlicher Pflichten, so basiert die Verarbeitung auf Art. 6 I lit. c DS-GVO.

In seltenen Fällen könnte die Verarbeitung von personenbezogenen Daten erforderlich werden, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen. Dies wäre beispielsweise der Fall, wenn ein Besucher in unserem Betrieb verletzt werden würde und daraufhin sein Name, sein Alter, seine Krankenkassendaten oder sonstige lebenswichtige Informationen an einen Arzt, ein Krankenhaus oder sonstige Dritte weitergegeben werden müssten. Dann würde die Verarbeitung auf Art. 6 I lit. d DS-GVO beruhen.

Wenn die Verarbeitung für die Wahrnehmung einer Aufgabe erforderlich ist, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde, ist die Rechtsgrundlage Art. 6 I lit. e DS-GVO.

Letztlich könnten Verarbeitungsvorgänge auf Art. 6 I lit. f DS-GVO beruhen. Auf dieser Rechtsgrundlage basieren Verarbeitungsvorgänge, die von keiner der vorgenannten Rechtsgrundlagen erfasst werden, wenn die Verarbeitung zur Wahrung eines berechtigten Interesses unseres Unternehmens oder eines Dritten erforderlich ist, sofern die Interessen, Grundrechte und Grundfreiheiten des Betroffenen nicht überwiegen. Solche Verarbeitungsvorgänge sind uns insbesondere deshalb gestattet, weil sie durch den Europäischen Gesetzgeber besonders erwähnt wurden. Er vertrat insoweit die Auffassung, dass ein berechtigtes Interesse anzunehmen sein könnte, wenn die betroffene Person ein Kunde des Verantwortlichen ist (Erwägungsgrund 47 Satz 2 DS-GVO).

## D. Wenn die Verarbeitung auf Artikel 6 I lit. f DS-GVO beruht, die berechtigten Interessen, die von dem Verantwortlichen oder einem Dritten verfolgt werden (Art. 13 I lit. d DS-GVO)

Basiert die Verarbeitung personenbezogener Daten auf Artikel 6 I lit. f DS-GVO ist unser berechtigtes Interesse die Durchführung unserer Geschäftstätigkeit zugunsten des Wohlergehens all unserer Mitarbeiter und unserer Anteilseigner.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## E. Kategorien von Empfängern der personenbezogenen Daten (Art. 13 I lit. e DS-GVO)

Öffentliche Stellen

Externe Stellen

Weitere externe Stellen

Interne Verarbeitung

Konzerninterne Verarbeitung

Sonstige Stellen

Eine Liste unserer Auftragsverarbeiter und der Datenempfänger in Drittländern sowie ggf. der internationalen Organisationen ist entweder auf unserer Webseite veröffentlicht oder kann kostenfrei bei uns angefordert werden. Bitte wenden Sie sich zur Anforderung dieser Liste an unseren Datenschutzbeauftragten.

## F. Empfänger in einem Drittland und geeignete oder angemessene Garantien und die Möglichkeit, wie eine Kopie von ihnen zu erhalten ist, oder wo sie verfügbar sind (Art. 13 I lit. f, 46 I, II lit. c DS-GVO)

Alle Unternehmen und Niederlassungen, die unserem Konzern angehören (nachfolgend Konzerngesellschaften genannt) und ihren oder einen Geschäftssitz in einem Drittland haben, können zu den Empfängern von personenbezogenen Daten gehören. Eine Liste aller Konzerngesellschaften oder Empfänger kann bei uns angefordert werden.

Gemäß Art. 46 I DS-GVO darf der Verantwortliche oder ein Auftragsverarbeiter nur dann personenbezogene Daten an ein Drittland übermitteln, wenn der Verantwortliche oder der Auftragsverarbeiter geeignete Garantien vorgesehen hat und sofern den betroffenen Personen durchsetzbare Rechte und wirksame Rechtsbehelfe zur Verfügung stehen. Geeignete Garantien können, ohne dass es hierzu einer besonderen Genehmigung einer Aufsichtsbehörde bedarf, durch Standarddatenschutzklauseln abgebildet werden, Art. 46 II lit. c DS-GVO.

Mit allen Empfängern aus Drittländern werden vor der ersten Übermittlung personenbezogener Daten die EU-Standarddatenschutzklauseln oder andere geeignete Garantien vereinbart. Folglich ist sichergestellt, dass für sämtliche Verarbeitungen von personenbezogenen Daten geeignete Garantien, durchsetzbare Rechte und wirksame Rechtsbehelfe gewährleistet sind. Jeder Betroffene kann eine Kopie


© All rights reserved by Heiko Maniero.

der Standarddatenschutzklauseln von uns erhalten. Zudem sind die Standarddatenschutzklauseln auch im Amtsblatt der Europäischen Union verfügbar.

Artikel 45 Absatz 3 der Datenschutz-Grundverordnung (DSGVO) ermächtigt die Europäische Kommission, im Wege eines Durchführungsrechtsakts zu beschließen, dass ein Nicht-EU-Land ein angemessenes Schutzniveau gewährleistet. Dies bedeutet ein Schutzniveau für personenbezogene Daten, das im Wesentlichen dem Schutzniveau innerhalb der EU entspricht. Die Angemessenheitsbeschlüsse haben zur Folge, dass personenbezogene Daten ohne weitere Hindernisse aus der EU (sowie aus Norwegen, Liechtenstein und Island) in ein Drittland fließen können. Ähnliche Vorschriften gelten für das Vereinigte Königreich, die Schweiz und einige andere Länder.

In den Fällen, in denen die Europäische Kommission oder die Regierung eines anderen Landes entschieden hat, dass ein Drittland ein angemessenes Schutzniveau gewährleistet und ein gültiges Rahmenwerk besteht (z.B. EU-U.S. Data Privacy Framework, Swiss-U.S. Data Privacy Framework, UK Extension to the EU-U.S. Data Privacy Framework), basieren alle Übermittlungen von uns an die Mitglieder solcher Rahmenwerke (z.B. selbst zertifizierte Einrichtungen) ausschließlich auf der Mitgliedschaft dieser Einrichtung in dem jeweiligen Rahmenwerk. Wenn wir oder eines unserer Konzernunternehmen Mitglied eines solchen Rahmenwerks sind, basieren alle Übermittlungen an uns oder unser Konzernunternehmen ausschließlich auf der Mitgliedschaft des jeweiligen Unternehmens in diesem Rahmenwerk.

Jeder Betroffene kann eine Kopie der Rahmenwerke von uns erhalten. Zudem sind die Rahmenwerke auch im Amtsblatt der Europäischen Union oder in den publizierten Gesetzesmaterialien oder auf den Webseiten von Aufsichtsbehörden oder anderen zuständigen Behörden oder Institutionen verfügbar.

## G. Dauer, für die die personenbezogenen Daten gespeichert werden oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer (Art. 13 II lit. a DS-GVO)

Das Kriterium für die Dauer der Speicherung von personenbezogenen Daten ist die jeweilige gesetzliche Aufbewahrungsfrist. Nach Ablauf der Frist werden die entsprechenden Daten routinemäßig gelöscht, sofern sie nicht mehr zur Vertragserfüllung oder Vertragsanbahnung erforderlich sind.

Sofern keine gesetzliche Aufbewahrungsfrist besteht, ist das Kriterium die vertragliche oder interne Aufbewahrungsfrist.

## H. Bestehen der Rechte auf Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung und des Widerspruchsrechts gegen die Verarbeitung sowie des Rechts auf Datenübertragbarkeit (Art. 13 II lit. b DS-GVO)

Alle Betroffenen haben die folgenden Rechte:


© All rights reserved by Heiko Maniero.

***Auskunftsrecht***

Jeder Betroffene hat ein Auskunftsrecht über die ihn betreffenden personenbezogenen Daten. Das Auskunftsrecht erstreckt sich auf alle von uns verarbeiteten Daten. Das Recht kann problemlos und in angemessenen Abständen wahrgenommen werden, damit sich alle Betroffenen der Verarbeitung ihrer personenbezogenen Daten stets bewusst sind und deren Rechtmäßigkeit überprüfen können (Erwägungsgrund 63 DS-GVO). Dieses Recht ergibt sich aus Art. 15 DS-GVO. Zur Ausübung des Auskunftsrechts kann sich der Betroffene an uns wenden.

***Recht auf Berichtigung***

Nach Art. 16 Satz 1 DS-GVO haben alle Betroffenen das Recht, von unserem Unternehmen unverzüglich die Berichtigung sie betreffender unrichtiger personenbezogener Daten zu verlangen. Zudem wird durch Art. 16 Satz 2 DS-GVO normiert, dass dem Betroffenen unter Berücksichtigung der Verarbeitungszwecke das Recht zusteht, die Vervollständigung unvollständiger personenbezogener Daten - auch mittels einer ergänzenden Erklärung - zu verlangen. Zur Ausübung des Berichtigungsrechts kann sich jeder Betroffene an uns wenden.

***Recht auf Löschung (Recht auf Vergessenwerden)***

Im Übrigen steht Betroffenen ein Recht auf Löschung und Vergessenwerden nach Art. 17 DS-GVO zu. Auch dieses Recht kann über eine Kontaktaufnahme zu uns geltend gemacht werden. An dieser Stelle erlauben wir uns jedoch den Hinweis, dass dieses Recht nicht gilt, soweit die Verarbeitung zur Erfüllung einer rechtlichen Verpflichtung, dem unser Unternehmen unterliegt, erforderlich ist, Art. 17 III lit. b DS-GVO. Dies bedeutet, dass wir einen Löschantrag erst nach Ablauf der gesetzlichen Aufbewahrungsfrist genehmigen können.

***Einschränkung der Verarbeitung***

Gemäß Art. 18 DS-GVO steht jedem Betroffenen ein Recht auf Einschränkung der Verarbeitung zu. Eine Einschränkung der Verarbeitung kann verlangt werden, wenn eine der Voraussetzungen aus Art. 18 I lit. a-d DS-GVO zutrifft. Das Recht auf Einschränkung der Verarbeitung kann über uns geltend gemacht werden.

***Recht auf Widerspruch***

Des Weiteren garantiert Art. 21 DS-GVO das Recht auf Widerspruch. Das Recht auf Wiederspruch kann über uns geltend gemacht werden.

***Recht auf Datenübertragbarkeit***

Art. 20 DS-GVO gewährt dem Betroffenen ein Recht auf Datenübertragbarkeit. Nach dieser Vorschrift hat die betroffene Person unter den Voraussetzungen des Art. 20 I lit. a und b DS-GVO das Recht, die sie betreffenden personenbezogenen Daten, die sie dem Verantwortlichen bereitgestellt hat, in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten, und diese Daten einem anderen Verantwortlichen ohne Behinderung durch den Verantwortlichen, zu übermitteln. Der Betroffene kann das Recht auf Datenübertragbarkeit über uns ausüben.


© All rights reserved by Heiko Maniero.

## I. Bestehen des Rechts, die Einwilligung jederzeit zu widerrufen, ohne dass die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung berührt wird, sofern die Verarbeitung auf Art. 6 I lit. a DS-GVO oder Art. 9 II lit. a DS-GVO beruht (Art. 13 II lit. c DS-GVO)

Beruht eine Verarbeitung personenbezogener Daten auf Art. 6 I lit. a DS-GVO, was der Fall ist, wenn die betroffene Person eine Einwilligung in eine Verarbeitung sie betreffender personenbezogener Daten für einen oder mehrere bestimmte Zwecke erteilt hat oder beruht die Verarbeitung auf Art. 9 II lit. a DS-GVO, der die ausdrückliche Einwilligung in die Verarbeitung besonderer Kategorien personenbezogener Daten regelt, so hat die betroffene Person nach Art. 7 III Satz 1 DS-GVO das Recht, ihre Einwilligung jederzeit zu widerrufen.

Durch den Widerruf der Einwilligung wird die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung nicht berührt, Art. 7 III Satz 2 DS-GVO. Der Widerruf der Einwilligung muss so einfach wie die Erteilung der Einwilligung sein, Art. 7 III Satz 4 DS-GVO. Daher kann der Widerruf der Einwilligung stets auf demselben Weg erfolgen, wie die Einwilligung erfolgte oder auf jede andere Art, die von der betroffenen Person als einfacher betrachtet wird. In der heutigen Informationsgesellschaft dürfte der wohl einfachste Weg für den Widerruf einer Einwilligung eine simple E-Mail sein. Sofern der Betroffene eine gegenüber uns erteilte Einwilligung widerrufen möchte, so ist eine einfache E-Mail an uns hierfür ausreichend. Alternativ kann die betroffene Person einen beliebigen anderen Weg wählen, um uns den Widerruf der Einwilligung mitzuteilen.

## J. Beschwerderecht bei einer Aufsichtsbehörde (Art. 13 II lit. d, 77 I DS-GVO)

Als Verantwortlicher sind wir verpflichtet, dem Betroffenen das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde mitzuteilen, Art. 13 II lit. d DS-GVO. Das Beschwerderecht wird in Art. 77 I DS-GVO geregelt. Nach dieser Vorschrift hat jede betroffene Person unbeschadet eines anderweitigen verwaltungsrechtlichen oder gerichtlichen Rechtsbehelfs das Recht auf Beschwerde bei einer Aufsichtsbehörde, insbesondere in dem Mitgliedstaat ihres Aufenthaltsorts, ihres Arbeitsplatzes oder des Orts des mutmaßlichen Verstoßes, wenn die betroffene Person der Ansicht ist, dass die Verarbeitung der sie betreffenden personenbezogenen Daten gegen die Datenschutz-Grundverordnung verstößt. Das Beschwerderecht wurde durch den unionalen Gesetzgeber ausschließlich dahingehend beschränkt, dass es nur gegenüber einer einzigen Aufsichtsbehörde ausgeübt werden kann (Erwägungsgrund 141 Satz 1 DS-GVO). Diese Regelung soll Doppelbeschwerden in gleicher Sache durch die gleiche betroffene Person vermeiden. Sofern sich eine betroffene Person über uns beschweren möchte, wird deshalb darum gebeten, nur eine einzige Aufsichtsbehörde zu kontaktieren.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## K. Gesetzliche oder vertragliche Vorschriften zur Bereitstellung der personenbezogenen Daten; Erforderlichkeit für den Vertragsabschluss; Verpflichtung der betroffenen Person, die personenbezogenen Daten bereitzustellen; mögliche Folgen der Nichtbereitstellung (Art. 13 II lit. e DS-GVO)

Wir klären Sie darüber auf, dass die Bereitstellung personenbezogener Daten zum Teil gesetzlich vorgeschrieben ist (z.B. Steuervorschriften) oder sich auch aus vertraglichen Regelungen (z.B. Angaben zum Vertragspartner) ergeben kann.

Mitunter kann es zu einem Vertragsschluss erforderlich sein, dass eine betroffene Person uns personenbezogene Daten zur Verfügung stellt, die in der Folge durch uns verarbeitet werden müssen. Die betroffene Person ist beispielsweise verpflichtet uns personenbezogene Daten bereitzustellen, wenn unser Unternehmen mit ihr einen Vertrag abschließt. Eine Nichtbereitstellung der personenbezogenen Daten hätte zur Folge, dass der Vertrag mit dem Betroffenen nicht geschlossen werden könnte.

Vor einer Bereitstellung personenbezogener Daten durch den Betroffenen muss sich der Betroffene an uns wenden. Wir klären den Betroffenen einzelfallbezogen darüber auf, ob die Bereitstellung der personenbezogenen Daten gesetzlich oder vertraglich vorgeschrieben oder für den Vertragsabschluss erforderlich ist, ob eine Verpflichtung besteht, die personenbezogenen Daten bereitzustellen, und welche Folgen die Nichtbereitstellung der personenbezogenen Daten hätte.

## L. Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling gem. Art. 22 I, IV DS-GVO und - zumindest in diesen Fällen - aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person (Art. 13 II lit. f DS-GVO)

Als verantwortungsbewusstes Unternehmen verzichten wir normalerweise auf eine automatische Entscheidungsfindung oder ein Profiling. Falls wir in Ausnahmefällen eine automatische Entscheidungsfindung oder ein Profiling durchführen, informieren wir die betroffene Person entweder gesondert oder über einen Unterpunkt in unserer Datenschutzerklärung (auf unserer Webseite). In diesem Fall gilt folgendes:

Zu einer automatisierten Entscheidungsfindung – einschließlich Profiling - kann es kommen, wenn dies (1) für den Abschluss oder die Erfüllung eines Vertrags zwischen der betroffenen Person und uns erforderlich ist, oder (2) dies aufgrund von Rechtsvorschriften der Union oder der Mitgliedstaaten, denen wir unterliegen, zulässig ist und diese Rechtsvorschriften angemessene Maßnahmen zur Wahrung der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person enthalten, oder (3) dies mit ausdrücklicher Einwilligung der betroffenen Person erfolgt.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

In den in Artikel 22 Absatz 2 Buchstaben a und c DS-GVO genannten Fällen treffen wir angemessene Maßnahmen, um die Rechte und Freiheiten sowie die berechtigten Interessen der betroffenen Person zu wahren. Im diesen Fällen haben Sie das Recht auf Erwirkung des Eingreifens einer Person seitens des Verantwortlichen, auf Darlegung des eigenen Standpunkts und auf Anfechtung der Entscheidung.

Aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person werden in unserer Datenschutzerklärung aufgeführt.

## II. Erfüllung der Informationspflichten für die Fälle, bei denen die personenbezogenen Daten nicht bei der betroffenen Person erhoben wurden (Art. 14 DS-GVO)

### A. Name und Kontaktdaten des Verantwortlichen (Art. 14 I lit. a DS-GVO)

Siehe oben

### B. Kontaktdaten des Datenschutzbeauftragten (Art. 14 I lit. b DS-GVO)

Siehe oben

### C. Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen, sowie die Rechtsgrundlage für die Verarbeitung (Art. 14 I lit. c DS-GVO)

Zweck der Verarbeitung personenbezogener Daten ist die Abwicklung sämtlicher Vorgänge, die das Unternehmen, Kunden, Interessenten, Geschäftspartner oder sonstige vertragliche oder vorvertragliche Beziehungen zwischen den genannten Beteiligtengruppen (im weitesten Sinne) oder gesetzliche Pflichten des Verantwortlichen betreffen.

Ist die Verarbeitung personenbezogener Daten zur Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, erforderlich, wie dies beispielsweise bei Verarbeitungsvorgängen der Fall ist, die für eine Lieferung von Waren oder die Erbringung einer sonstigen Leistung oder Gegenleistung notwendig sind, so beruht die Verarbeitung auf Art. 6 I lit. b DS-GVO. Gleiches gilt für solche Verarbeitungsvorgänge die zur Durchführung vorvertraglicher Maßnahmen erforderlich sind, etwa in Fällen von Anfragen zu unseren Produkten oder Leistungen. Unterliegt unser Unternehmen einer rechtlichen Verpflichtung durch welche eine Verarbeitung von personenbezogenen Daten erforderlich wird, wie beispielsweise zur Erfüllung steuerlicher Pflichten, so basiert die Verarbeitung auf Art. 6 I lit. c DS-GVO.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

In seltenen Fällen könnte die Verarbeitung von personenbezogenen Daten erforderlich werden, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen. Dies wäre beispielsweise der Fall, wenn ein Besucher in unserem Betrieb verletzt werden würde und daraufhin sein Name, sein Alter, seine Krankenkassendaten oder sonstige lebenswichtige Informationen an einen Arzt, ein Krankenhaus oder sonstige Dritte weitergegeben werden müssten. Dann würde die Verarbeitung auf Art. 6 I lit. d DS-GVO basieren.

Wenn die Verarbeitung für die Wahrnehmung einer Aufgabe erforderlich ist, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde, ist die Rechtsgrundlage Art. 6 I lit. e DS-GVO.

Letztlich könnten Verarbeitungsvorgänge auf Art. 6 I lit. f DS-GVO beruhen. Auf dieser Rechtsgrundlage basieren Verarbeitungsvorgänge, die von keiner der vorgenannten Rechtsgrundlagen erfasst werden, wenn die Verarbeitung zur Wahrung eines berechtigten Interesses unseres Unternehmens oder eines Dritten erforderlich ist, sofern die Interessen, Grundrechte und Grundfreiheiten des Betroffenen nicht überwiegen. Solche Verarbeitungsvorgänge sind uns insbesondere deshalb gestattet, weil sie durch den Europäischen Gesetzgeber besonders erwähnt wurden. Er vertrat insoweit die Auffassung, dass ein berechtigtes Interesse anzunehmen sein könnte, wenn die betroffene Person ein Kunde des Verantwortlichen ist (Erwägungsgrund 47 Satz 2 DS-GVO).

## D. Kategorien personenbezogener Daten, die verarbeitet werden (Art. 14 I lit. d DS-GVO)

Kundendaten

Interessentendaten

Beschäftigtendaten

Lieferantendaten

## E. Kategorien von Empfängern der personenbezogenen Daten (Art. 14 I lit. e DS-GVO)

Öffentliche Stellen

Externe Stellen

Weitere externe Stellen


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

Interne Verarbeitung

Konzerninterne Verarbeitung

Sonstige Stellen

Eine Liste unserer Auftragsverarbeiter und der Datenempfänger in Drittländern sowie ggf. der internationalen Organisationen ist entweder auf unserer Webseite veröffentlicht oder kann kostenfrei bei uns angefordert werden. Bitte wenden Sie sich zur Anforderung dieser Liste an unseren Datenschutzbeauftragten.

## F. Empfänger in einem Drittland und geeignete oder angemessene Garantien und die Möglichkeit, eine Kopie von ihnen zu erhalten, oder wo sie verfügbar sind (Art. 14 I lit. f, 46 I, II lit. c DS-GVO)

Alle Unternehmen und Niederlassungen, die unserem Konzern angehören (nachfolgend "Konzerngesellschaften" genannt) und ihren oder einen Geschäftssitz in einem Drittland haben, können zu den Empfängern von personenbezogenen Daten gehören. Eine Liste aller Konzerngesellschaften oder Empfänger kann bei uns angefordert werden.

Gemäß Art. 46 I DS-GVO darf der Verantwortliche oder ein Auftragsverarbeiter nur dann personenbezogene Daten an ein Drittland übermitteln, wenn der Verantwortliche oder der Auftragsverarbeiter geeignete Garantien vorgesehen hat und sofern den betroffenen Personen durchsetzbare Rechte und wirksame Rechtsbehelfe zur Verfügung stehen. Geeignete Garantien können, ohne dass es hierzu einer besonderen Genehmigung einer Aufsichtsbehörde bedarf, durch Standarddatenschutzklauseln abgebildet werden, Art. 46 II lit. c DS-GVO.

Mit allen Empfängern aus Drittländern werden vor der ersten Übermittlung personenbezogener Daten die EU-Standarddatenschutzklauseln oder andere geeignete Garantien vereinbart. Folglich ist sichergestellt, dass für sämtliche Verarbeitungen von personenbezogenen Daten geeignete Garantien, durchsetzbare Rechte und wirksame Rechtsbehelfe gewährleistet sind. Jeder Betroffene kann eine Kopie der Standarddatenschutzklauseln von uns erhalten. Zudem sind die Standarddatenschutzklauseln auch im Amtsblatt der Europäischen Union verfügbar.

Artikel 45 Absatz 3 der Datenschutz-Grundverordnung (DSGVO) ermächtigt die Europäische Kommission, im Wege eines Durchführungsrechtsakts zu beschließen, dass ein Nicht-EU-Land ein angemessenes Schutzniveau gewährleistet. Dies bedeutet ein Schutzniveau für personenbezogene Daten, das im Wesentlichen dem Schutzniveau innerhalb der EU entspricht. Die Angemessenheitsbeschlüsse haben zur Folge, dass personenbezogene Daten ohne weitere Hindernisse aus der EU (sowie aus Norwegen, Liechtenstein und Island) in ein Drittland fließen können. Ähnliche Vorschriften gelten für das Vereinigte Königreich, die Schweiz und einige andere Länder.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

In den Fällen, in denen die Europäische Kommission oder die Regierung eines anderen Landes entschieden hat, dass ein Drittland ein angemessenes Schutzniveau gewährleistet und ein gültiges Rahmenwerk besteht (z. B. EU-U.S. Data Privacy Framework, Swiss-U.S. Data Privacy Framework, UK Extension to the EU-U.S. Data Privacy Framework), basieren alle Übermittlungen von uns an die Mitglieder solcher Rahmenwerke (z. B. selbst zertifizierte Einrichtungen) ausschließlich auf der Mitgliedschaft dieser Einrichtung in dem jeweiligen Rahmenwerk. Wenn wir oder eines unserer Konzernunternehmen Mitglied eines solchen Rahmenwerks sind, basieren alle Übermittlungen an uns oder unser Konzernunternehmen ausschließlich auf der Mitgliedschaft des jeweiligen Unternehmens in diesem Rahmenwerk.

Jeder Betroffene kann eine Kopie der Rahmenwerke von uns erhalten. Zudem sind die Rahmenwerke auch im Amtsblatt der Europäischen Union oder in den publizierten Gesetzesmaterialien oder auf den Webseiten von Aufsichtsbehörden oder anderen zuständigen Behörden oder Institutionen verfügbar.

## G. Dauer, für die die personenbezogenen Daten gespeichert werden oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer (Art. 14 II lit. a DS-GVO)

Das Kriterium für die Dauer der Speicherung von personenbezogenen Daten ist die jeweilige gesetzliche Aufbewahrungsfrist. Nach Ablauf der Frist werden die entsprechenden Daten routinemäßig gelöscht, sofern sie nicht mehr zur Vertragserfüllung oder Vertragsanbahnung erforderlich sind.

Sofern keine gesetzliche Aufbewahrungsfrist besteht, ist das Kriterium die vertragliche oder interne Aufbewahrungsfrist.

## H. Mitteilung der berechtigten Interessen, die vom Verantwortlichen oder einem Dritten verfolgt werden, wenn die Verarbeitung auf Art. 6 I lit. f DS-GVO beruht (Art. 14 II lit. b DS-GVO)

Gemäß Art. 6 I lit. f DS-GVO ist eine Verarbeitung nur rechtmäßig, wenn sie zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen. Nach Erwägungsgrund 47 Satz 2 DS-GVO kann ein berechtigtes Interesse vorliegen, wenn eine maßgebliche und angemessene Beziehung zwischen der betroffenen Person und dem Verantwortlichen besteht, z. B. wenn die betroffene Person ein Kunde des Verantwortlichen ist. In allen Fällen in denen unser Unternehmen die Verarbeitung von personenbezogenen Daten auf Art. 6 I lit. f DS-GVO stützt, liegt unser berechtigtes Interesse in der Durchführung unserer Geschäftstätigkeit zugunsten des Wohlergehens all unserer Mitarbeiter und unserer Anteilseigner.


© All rights reserved by Heiko Maniero.

## I. Bestehen des Rechts auf Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung und des Widerspruchsrechts gegen die Verarbeitung sowie des Rechts auf Datenübertragbarkeit (Art. 14 II lit. c DS-GVO)

Alle Betroffenen haben die folgenden Rechte:

***Auskunftsrecht***

Jeder Betroffene hat ein Auskunftsrecht über die ihn betreffenden personenbezogenen Daten. Das Auskunftsrecht erstreckt sich auf alle von uns verarbeiteten Daten. Das Recht kann problemlos und in angemessenen Abständen wahrgenommen werden, damit sich alle Betroffenen der Verarbeitung ihrer personenbezogenen Daten stets bewusst sind und deren Rechtmäßigkeit überprüfen können (Erwägungsgrund 63 DS-GVO). Dieses Recht ergibt sich aus Art. 15 DS-GVO. Zur Ausübung des Auskunftsrechts kann sich der Betroffene an uns wenden.

***Recht auf Berichtigung***

Nach Art. 16 Satz 1 DS-GVO haben alle Betroffenen das Recht, von unserem Unternehmen unverzüglich die Berichtigung sie betreffender unrichtiger personenbezogener Daten zu verlangen. Zudem wird durch Art. 16 Satz 2 DS-GVO normiert, dass dem Betroffenen unter Berücksichtigung der Verarbeitungszwecke das Recht zusteht, die Vervollständigung unvollständiger personenbezogener Daten - auch mittels einer ergänzenden Erklärung - zu verlangen. Zur Ausübung des Berichtigungsrechts kann sich jeder Betroffene an uns wenden.

***Recht auf Löschung (Recht auf Vergessenwerden)***

Im Übrigen steht Betroffenen ein Recht auf Löschung und Vergessenwerden nach Art. 17 DS-GVO zu. Auch dieses Recht kann über eine Kontaktaufnahme zu uns geltend gemacht werden. An dieser Stelle erlauben wir uns jedoch den Hinweis, dass dieses Recht nicht gilt, soweit die Verarbeitung zur Erfüllung einer rechtlichen Verpflichtung, dem unser Unternehmen unterliegt, erforderlich ist, Art. 17 III lit. b DS-GVO. Dies bedeutet, dass wir einen Löschantrag erst nach Ablauf der gesetzlichen Aufbewahrungsfrist genehmigen können.

***Einschränkung der Verarbeitung***

Gemäß Art. 18 DS-GVO steht jedem Betroffenen ein Recht auf Einschränkung der Verarbeitung zu. Eine Einschränkung der Verarbeitung kann verlangt werden, wenn eine der Voraussetzungen aus Art. 18 I lit. a-d DS-GVO zutrifft. Das Recht auf Einschränkung der Verarbeitung kann über uns geltend gemacht werden.

***Recht auf Widerspruch***

Des Weiteren garantiert Art. 21 DS-GVO das Recht auf Widerspruch. Das Recht auf Wiederspruch kann über uns geltend gemacht werden.

***Recht auf Datenübertragbarkeit***

Art. 20 DS-GVO gewährt dem Betroffenen ein Recht auf Datenübertragbarkeit. Nach dieser Vorschrift hat die betroffene Person unter den Voraussetzungen des Art. 20 I lit. a und b DS-GVO das Recht, die


© All rights reserved by Heiko Maniero.

sie betreffenden personenbezogenen Daten, die sie dem Verantwortlichen bereitgestellt hat, in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten, und diese Daten einem anderen Verantwortlichen ohne Behinderung durch den Verantwortlichen, zu übermitteln. Der Betroffene kann das Recht auf Datenübertragbarkeit über uns ausüben.

## J. Bestehen des Rechts, die Einwilligung jederzeit zu widerrufen, ohne dass die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung berührt wird, sofern die Verarbeitung auf Art. 6 I lit. a oder Art. 9 II lit. a DS-GVO beruht (Art. 14 II lit. d DS-GVO)

Beruht eine Verarbeitung personenbezogener Daten auf Art. 6 I lit. a DS-GVO, was der Fall ist, wenn die betroffene Person eine Einwilligung in eine Verarbeitung sie betreffender personenbezogener Daten für einen oder mehrere bestimmte Zwecke erteilt hat oder beruht die Verarbeitung auf Art. 9 II lit. a DS-GVO, der die ausdrückliche Einwilligung in die Verarbeitung besonderer Kategorien personenbezogener Daten regelt, so hat die betroffene Person nach Art. 7 III Satz 1 DS-GVO das Recht, ihre Einwilligung jederzeit zu widerrufen.

Durch den Widerruf der Einwilligung wird die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung nicht berührt, Art. 7 III Satz 2 DS-GVO. Der Widerruf der Einwilligung muss so einfach wie die Erteilung der Einwilligung sein, Art. 7 III Satz 4 DS-GVO. Daher kann der Widerruf der Einwilligung stets auf demselben Weg erfolgen, wie die Einwilligung erfolgte oder auf jeder anderen Art, die von der betroffenen Person als einfacher betrachtet wird. In der heutigen Informationsgesellschaft dürfte der wohl einfachste Weg für den Widerruf einer Einwilligung eine simple E-Mail sein. Sofern der Betroffene eine gegenüber uns erteilte Einwilligung widerrufen möchte, so ist eine einfache E-Mail an uns hierfür ausreichend. Alternativ kann die betroffene Person einen beliebigen anderen Weg wählen, um uns den Widerruf der Einwilligung mitzuteilen.

## K. Beschwerderecht bei einer Aufsichtsbehörde (Art. 14 II lit. e, 77 I DS-GVO)

Als Verantwortlicher sind wir verpflichtet, dem Betroffenen das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde mitzuteilen, Art. 14 II lit. e DS-GVO. Das Beschwerderecht wird in Art. 77 I DS-GVO geregelt. Nach dieser Vorschrift hat jede betroffene Person unbeschadet eines anderweitigen verwaltungsrechtlichen oder gerichtlichen Rechtsbehelfs das Recht auf Beschwerde bei einer Aufsichtsbehörde, insbesondere in dem Mitgliedstaat ihres Aufenthaltsorts, ihres Arbeitsplatzes oder des Orts des mutmaßlichen Verstoßes, wenn die betroffene Person der Ansicht ist, dass die Verarbeitung der sie betreffenden personenbezogenen Daten gegen die Datenschutz-Grundverordnung verstößt. Das Beschwerderecht wurde durch den unionalen Gesetzgeber ausschließlich dahingehend beschränkt, dass es nur gegenüber einer einzigen Aufsichtsbehörde ausgeübt werden kann (Erwägungsgrund 141 Satz 1 DS-GVO). Diese Regelung soll Doppelbeschwerden in gleicher Sache durch die gleiche


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

betroffene Person vermeiden. Sofern sich eine betroffene Person über uns beschweren möchte, wird deshalb darum gebeten, nur eine einzige Aufsichtsbehörde zu kontaktieren.

## L. Quelle aus der die personenbezogenen Daten stammen und gegebenenfalls, ob sie aus öffentlich zugänglichen Quellen stammen (Art. 14 II lit. f DS-GVO)

Grundsätzlich werden personenbezogene Daten direkt beim Betroffenen oder im Zusammenwirken mit einer Behörde erhoben (z.B. Auslesen von Daten eines behördlichen Registers). Andere Daten über Betroffene stammen aus Übermittlungen von Konzerngesellschaften. Im Rahmen dieser allgemein zu haltenden Information ist eine Mitteilung der exakten Quellen aus denen die personenbezogenen Daten stammen entweder unmöglich oder verursacht unverhältnismäßigen Aufwand im Sinne von Art. 14 V lit. b DS-GVO. Wir erheben grundsätzlich keine personenbezogenen Daten aus öffentlich zugänglichen Quellen.

Jeder Betroffene kann sich jederzeit an uns wenden, um genauere Informationen über exakte Quellen der sie betreffenden personenbezogenen Daten zu erhalten. Kann der betroffenen Person nicht exakt mitgeteilt werden, woher die personenbezogenen Daten stammen, weil verschiedene Quellen benutzt wurden, so wird die individuelle Unterrichtung allgemein gehalten (Erwägungsgrund 61 Satz 4 DS-GVO).

## M. Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling gem. Art. 22 I, IV DS-GVO und - zumindest in diesen Fällen - aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person (Art. 14 II lit. g DS-GVO)

Als verantwortungsbewusstes Unternehmen verzichten wir normalerweise auf eine automatische Entscheidungsfindung oder ein Profiling. Falls wir in Ausnahmefällen eine automatische Entscheidungsfindung oder ein Profiling durchführen, informieren wir die betroffene Person entweder gesondert oder über einen Unterpunkt in unserer Datenschutzerklärung (auf unserer Webseite). In diesem Fall gilt folgendes:

Zu einer automatisierten Entscheidungsfindung – einschließlich Profiling - kann es kommen, wenn dies (1) für den Abschluss oder die Erfüllung eines Vertrags zwischen der betroffenen Person und uns erforderlich ist, oder (2) dies aufgrund von Rechtsvorschriften der Union oder der Mitgliedstaaten, denen wir unterliegen, zulässig ist und diese Rechtsvorschriften angemessene Maßnahmen zur Wahrung der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person enthalten, oder (3) dies mit ausdrücklicher Einwilligung der betroffenen Person erfolgt.

In den in Artikel 22 Absatz 2 Buchstaben a und c DS-GVO genannten Fällen treffen wir angemessene Maßnahmen, um die Rechte und Freiheiten sowie die berechtigten Interessen der betroffenen Person zu


© All rights reserved by Heiko Maniero.

wahren. Im diesen Fällen haben Sie das Recht auf Erwirkung des Eingreifens einer Person seitens des Verantwortlichen, auf Darlegung des eigenen Standpunkts und auf Anfechtung der Entscheidung.

Aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person werden in unserer Datenschutzerklärung aufgeführt.

## III. EU-U.S. Data Privacy Framework (EU-U.S. DPF), UK Extension to the EU-U.S. DPF, Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF)

Wenn unsere Organisation ein zertifiziertes Mitglied des EU-U.S. Data Privacy Framework (EU-U.S. DPF) und/oder der UK Extension to the EU-U.S. DPF und/oder des Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF) ist, gilt das Folgende:

Wir halten uns an das EU-U.S. Data Privacy Framework (EU-U.S. DPF) und die UK Extension to the EU-U.S. DPF sowie an das Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF), wie es vom U.S. Department of Commerce festgelegt wurde. Unser Unternehmen hat gegenüber dem US-Handelsministerium bestätigt, dass es die EU-U.S. Data Privacy Framework Principles (EU-U.S. DPF Principles) in Bezug auf die Verarbeitung personenbezogener Daten einhält, die es aus der Europäischen Union und dem Vereinigten Königreich unter Berufung auf das EU-U.S. DPF und die UK Extension to the EU-U.S. DPF erhält. Unser Unternehmen hat gegenüber dem US-Handelsministerium bestätigt, dass es die Swiss-U.S. Data Privacy Framework Principles (Swiss-U.S. DPF Principles) in Bezug auf die Verarbeitung personenbezogener Daten, die es aus der Schweiz unter Berufung auf die Swiss-U.S. DPF erhält, einhält. Im Falle eines Widerspruchs zwischen den Bestimmungen unserer Datenschutzerklärung und den EU-U.S. DPF Principles und/oder den Swiss-U.S. DPF Principles sind die Principles maßgebend.

Um mehr über das Data Privacy Framework (DPF) Programm zu erfahren und um unsere Zertifizierung einzusehen, besuchen Sie bitte https://www.dataprivacyframework.gov/.

Die anderen US-Einheiten oder US-Tochtergesellschaften unseres Unternehmens, die sich ebenfalls an die EU-U.S. DPF Principals halten, einschließlich der UK Extension to the EU-U.S. DPF und der Swiss-U.S. DPF Principals, sofern vorhanden, werden in unserer Datenschutzerklärung genannt.

In Übereinstimmung mit dem EU-U.S. DPF und der UK Extension to the EU-U.S. DPF sowie des Swiss-U.S. DPF verpflichtet sich unser Unternehmen, mit dem von den EU-Datenschutzbehörden und dem britischen Information Commissioner's Office (ICO) sowie dem Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) eingerichteten Gremium zusammenzuarbeiten und dessen Ratschläge in Bezug auf ungelöste Beschwerden über unseren Umgang mit personenbezogenen Daten


© All rights reserved by Heiko Maniero.

zu befolgen, die wir unter Berufung auf die EU-U.S. DPF und die UK Extension to the EU-U.S. DPF und die Swiss-U.S. DPF erhalten haben.

Wir informieren die betroffenen Personen über die zuständigen europäischen Datenschutzbehörden, die für die Bearbeitung von Beschwerden über den Umgang unserer Organisation mit personenbezogenen Daten zuständig sind, im oberen Teil dieses Transparenzdokuments und darüber, dass wir den betroffenen Personen einen angemessenen und kostenlosen Rechtsbehelf anbieten.

Wir informieren alle betroffenen Personen darüber, dass unser Unternehmen den Ermittlungs- und Durchsetzungsbefugnissen der Federal Trade Commission (FTC) unterliegt.

Betroffene Personen haben unter bestimmten Voraussetzungen die Möglichkeit, ein verbindliches Schiedsverfahren in Anspruch zu nehmen. Unsere Organisation ist verpflichtet, Ansprüche zu schlichten und die Bedingungen gemäß Anhang I der DPF-Principals einzuhalten, sofern die betroffene Person ein verbindliches Schiedsverfahren beantragt hat, indem sie unsere Organisation benachrichtigt hat und die Verfahren und Bedingungen gemäß Anhang I der Principals eingehalten hat.

Wir informieren hiermit alle betroffenen Personen über die Haftung unserer Organisation im Falle der Weitergabe von personenbezogenen Daten an Dritte.

Für Fragen der betroffenen Personen oder der Datenschutzaufsichtsbehörden haben wir die oben in diesem Transparenzdokument genannten lokalen Vertreter benannt.

Wir bieten Ihnen die Möglichkeit zu wählen (Opt-out), ob Ihre personenbezogenen Daten (i) an Dritte weitergegeben oder (ii) für einen Zweck verwendet werden sollen, der sich wesentlich von dem/den Zweck(en) unterscheidet, für den/die sie ursprünglich erhoben oder später von Ihnen genehmigt wurden. Der eindeutige, gut sichtbare und leicht zugängliche Mechanismus zur Ausübung Ihres Wahlrechts besteht darin, unseren Datenschutzbeauftragten (DSB) per E-Mail zu kontaktieren. Sie haben keine Wahlmöglichkeit und wir sind auch nicht dazu verpflichtet, wenn die Daten an einen Dritten weitergegeben werden, der als Beauftragter oder Auftragsverarbeiter in unserem Namen und auf unsere Anweisung hin Aufgaben wahrnimmt. Wir schließen jedoch immer einen Vertrag mit einem solchen Beauftragten oder Auftragsverarbeiter ab.

Für sensible Daten (d. h. personenbezogene Daten, die Angaben über den Gesundheitszustand, die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, die Mitgliedschaft in einer Gewerkschaft oder Angaben zum Sexualleben der betreffenden Person enthalten) holen wir Ihre ausdrückliche Zustimmung (Opt-in) ein, wenn diese Daten (i) an Dritte weitergegeben oder (ii) für einen anderen Zweck als denjenigen verwendet werden sollen, für den sie ursprünglich erhoben wurden oder für den Sie nachträglich Ihre Zustimmung erteilt haben, indem Sie Ihre Opt-in-Wahl getroffen haben. Darüber hinaus behandeln wir alle personenbezogenen Daten, die wir von Dritten erhalten, als sensibel, wenn der Dritte sie als sensibel identifiziert und behandelt.


© All rights reserved by Heiko Maniero.

Wir informieren Sie hiermit über das Erfordernis, personenbezogene Daten in Reaktion auf rechtmäßige Anfragen von Behörden offenzulegen, einschließlich der Erfüllung von Anforderungen der nationalen Sicherheit oder der Strafverfolgung.

Bei der Übermittlung personenbezogener Daten an einen Dritten, der als Verantwortlicher handelt, halten wir uns an die Principals der Benachrichtigung und der Wahlmöglichkeit. Außerdem schließen wir mit dem Dritten, der für die Verarbeitung verantwortlich ist, einen Vertrag ab, der vorsieht, dass diese Daten nur für begrenzte und festgelegte Zwecke in Übereinstimmung mit der von Ihnen erteilten Einwilligung verarbeitet werden dürfen und dass der Empfänger das gleiche Schutzniveau wie die Principals des DPF bietet und uns benachrichtigt, wenn er feststellt, dass er diese Verpflichtung nicht mehr erfüllen kann. Der Vertrag sieht vor, dass der Dritte, der Verantwortlicher ist, die Verarbeitung einstellt oder andere angemessene und geeignete Maßnahmen ergreift, um Abhilfe zu schaffen, wenn eine solche Feststellung getroffen wird.

Bei der Übermittlung personenbezogener Daten an einen Dritten, der als Beauftragter oder Auftragsverarbeiter handelt, (i) übermitteln wir diese Daten nur für begrenzte und festgelegte Zwecke; (ii) vergewissern wir uns, dass der Beauftragte oder Auftragsverarbeiter verpflichtet ist, mindestens das gleiche Maß an Datenschutz zu gewährleisten, wie es die DPF-Principals verlangen; (iii) ergreifen wir angemessene und geeignete Maßnahmen, um sicherzustellen, dass der Beauftragte oder Auftragsverarbeiter die übermittelten personenbezogenen Daten tatsächlich in einer Weise verarbeitet, die mit unseren Verpflichtungen gemäß den DPF-Principals übereinstimmt; (iv) von dem Beauftragten oder Auftragsverarbeiter zu verlangen, dass er unsere Organisation benachrichtigt, wenn er feststellt, dass er seiner Verpflichtung nicht mehr nachkommen kann, das gleiche Schutzniveau zu bieten, wie es die DPF-Principals vorsehen; (v) nach einer Benachrichtigung, auch unter (iv), angemessene und geeignete Schritte zu unternehmen, um die unbefugte Verarbeitung zu stoppen und Abhilfe zu schaffen; und (vi) dem DPF Department auf Anfrage eine Zusammenfassung oder ein repräsentatives Exemplar der einschlägigen Datenschutzbestimmungen seines Vertrags mit diesem Beauftragten zur Verfügung zu stellen.

In Übereinstimmung mit dem EU-U.S. DPF und/oder der UK Extension to the EU-U.S. DPF und/oder der Swiss-U.S. DPF verpflichtet sich unsere Organisation, mit dem von den EU-Datenschutzbehörden und dem britischen Information Commissioner's Office (ICO) bzw. dem Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) eingerichteten Gremium zusammenzuarbeiten und dessen Ratschläge in Bezug auf ungelöste Beschwerden über unseren Umgang mit Personaldaten, die wir unter Berufung auf die EU-U.S. DPF und der UK-Erweiterung der EU-U.S. DPF und der Swiss-U.S. DPF im Zusammenhang mit dem Arbeitsverhältnis erhalten, zu befolgen.

Allen betroffenen Personen, die sich vorübergehend in der Europäischen Union (EU), im Europäischen Wirtschaftsraum (EWR) oder im Vereinigten Königreich aufhalten oder dort ihren Wohnsitz oder gewöhnlichen Aufenthaltsort haben, stehen die in unserem Transparenzdokument publizierten Rechte und Betroffenenrechte zu, die sich auch aus Artikeln 15 bis 22 DS-GVO ergeben, inklusive dem Recht


© All rights reserved by Heiko Maniero.

auf Auskunft. Diese Informationen haben wir in allen Sprachen der EU und des EWR zur Verfügung gestellt. Die englische Sprachfassung gilt für das Vereinigte Königreich.

Allen betroffenen Personen, die sich vorübergehend in der Schweiz aufhalten oder dort ihren Wohnsitz oder gewöhnlichen Aufenthaltsort haben, stehen die in unserem Transparenzdokument publizierten Rechte und Betroffenenrechte aus dem Schweizer Datenschutzgesetz (DSG) und der Schweizer Datenschutzverordnung (DSV) zu, inklusive dem Recht auf Auskunft. Diese Informationen haben wir in den drei offiziellen Sprachen der Schweiz (Deutsch, Italienisch und Französisch) zur Verfügung gestellt.


© All rights reserved by Heiko Maniero.

# GERMAN: Mitarbeiter- und Bewerberinformation über die Verarbeitung personenbezogener Daten (Artikel 13, 14 DS-GVO)

Sehr geehrte Damen und Herren,

personenbezogene Daten von Mitarbeitern und Bewerbern verdienen besonderen Schutz. Wir haben uns zum Ziel gesetzt, unser Datenschutzniveau auf einem hohen Standard zu halten. Deswegen setzen wir auf eine routinemäßige Weiterentwicklung unserer Datenschutz- und Datensicherheitskonzepte.

Selbstverständlich halten wir die gesetzlichen Vorschriften zum Datenschutz ein. Nach Art. 13, 14 DS-GVO treffen Verantwortliche besondere Informationspflichten, wenn sie personenbezogene Daten verarbeiten. Durch dieses Dokument erfüllen wir diese Verpflichtungen.

Die Terminologie gesetzlicher Vorschriften ist kompliziert. Bei der Ausarbeitung dieses Dokuments konnte leider nicht auf die Verwendung von juristischen Begriffen verzichtet werden. Daher möchten wir darauf hinweisen, dass Sie sich bei allen Fragen zu diesem Dokument, zu den verwendeten Fachbegriffen oder Formulierungen gerne an uns wenden dürfen.

## I. Erfüllung der Informationspflichten im Falle der Erhebung von personenbezogenen Daten bei der betroffenen Person (Art. 13 DS-GVO)

### A. Name und Kontaktdaten des Verantwortlichen (Art. 13 I lit. a DS-GVO)

Siehe oben

### B. Kontaktdaten des Datenschutzbeauftragten (Art. 13 I lit. b DS-GVO)

Siehe oben

### C. Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen, sowie die Rechtsgrundlage für die Verarbeitung (Art. 13 I lit. c DS-GVO)

Für Bewerberdaten ist der Zweck der Datenverarbeitung, eine Prüfung der Bewerbung im Bewerbungsverfahren durchzuführen. Für diesen Zweck verarbeiten wir alle von Ihnen zur Verfügung gestellten Daten. Auf Basis der im Rahmen der Bewerbung übermittelten Daten prüfen wir, ob Sie zu einem Vorstellungsgespräch (Teil des Auswahlverfahrens) eingeladen werden. Sodann verarbeiten wir


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

im Falle von grundsätzlich geeigneten Bewerberinnen und Bewerbern, insbesondere im Rahmen des Bewerbungsgesprächs, bestimmte weitere von Ihnen zur Verfügung gestellte personenbezogene Daten, die für unsere Auswahlentscheidung wesentlich sind. Werden Sie von uns eingestellt, wandeln sich Bewerberdaten automatisch in Mitarbeiterdaten. Im Rahmen des Einstellungsverfahrens werden wir sodann weitere personenbezogene Daten von Ihnen verarbeiten, die wir von Ihnen abfragen und die zur Vertragsanbahnung oder Vertragserfüllung erforderlich sind (z.B. Personenidentifikationsnummern oder Steuernummern). Für Mitarbeiterdaten ist der Zweck der Datenverarbeitung, die Erfüllung des Arbeitsvertrages, sonstiger gesetzlicher Vorschriften, die auf das Arbeitsverhältnis anwendbar sind (z.B. aus dem Steuerrecht), sowie der Einsatz Ihrer Person zur Durchführung des mit Ihnen abgeschlossenen Arbeitsvertrages (z.B. Veröffentlichung Ihres Namens und der Kontaktdaten innerhalb des Unternehmens oder gegenüber Kunden). Mitarbeiterdaten werden nach Beendigung des Arbeitsverhältnisses zur Erfüllung gesetzlicher Aufbewahrungsfristen gespeichert.

Rechtsgrundlagen für die Datenverarbeitung sind Art. 6 Abs. 1 Buchst. b DS-GVO, Art. 9 Abs. 2 Buchst. b und h DS-GVO, Art. 88 Abs. 1 DS-GVO sowie nationale Rechtsvorschriften, wie etwa für Deutschland § 26 BDSG.

## D. Kategorien von Empfängern der personenbezogenen Daten (Art. 13 I lit. e DS-GVO)

Öffentliche Stellen

Externe Stellen

Weitere externe Stellen

Interne Verarbeitung

Konzerninterne Verarbeitung

Sonstige Stellen

Eine Liste unserer Auftragsverarbeiter und der Datenempfänger in Drittländern sowie ggf. der internationalen Organisationen ist entweder auf unserer Webseite veröffentlicht oder kann kostenfrei bei uns angefordert werden. Bitte wenden Sie sich zur Anforderung dieser Liste an unseren Datenschutzbeauftragten.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## E. Empfänger in einem Drittland und geeignete oder angemessene Garantien und die Möglichkeit, wie eine Kopie von ihnen zu erhalten ist, oder wo sie verfügbar sind (Art. 13 I lit. f, 46 I, II lit. c DS-GVO)

Alle Unternehmen und Niederlassungen, die unserer Unternehmensgruppe angehören (nachfolgend Konzerngesellschaften genannt) und ihren oder einen Geschäftssitz in einem Drittland haben, können zu den Empfängern von personenbezogenen Daten gehören. Eine Liste aller Konzerngesellschaften oder Empfänger kann bei uns angefordert werden.

Gemäß Art. 46 I DS-GVO darf der Verantwortliche oder ein Auftragsverarbeiter nur dann personenbezogene Daten an ein Drittland übermitteln, wenn der Verantwortliche oder der Auftragsverarbeiter geeignete Garantien vorgesehen hat und sofern den betroffenen Personen durchsetzbare Rechte und wirksame Rechtsbehelfe zur Verfügung stehen. Geeignete Garantien können, ohne dass es hierzu einer besonderen Genehmigung einer Aufsichtsbehörde bedarf, durch Standarddatenschutzklauseln abgebildet werden, Art. 46 II lit. c DS-GVO.

Mit allen Empfängern aus Drittländern werden vor der ersten Übermittlung personenbezogener Daten die EU-Standarddatenschutzklauseln oder andere geeignete Garantien vereinbart. Folglich ist sichergestellt, dass für sämtliche Verarbeitungen von personenbezogenen Daten geeignete Garantien, durchsetzbare Rechte und wirksame Rechtsbehelfe gewährleistet sind. Jeder Betroffene kann eine Kopie der Standarddatenschutzklauseln von uns erhalten. Zudem sind die Standarddatenschutzklauseln auch im Amtsblatt der Europäischen Union verfügbar.

Artikel 45 Absatz 3 der Datenschutz-Grundverordnung (DSGVO) ermächtigt die Europäische Kommission, im Wege eines Durchführungsrechtsakts zu beschließen, dass ein Nicht-EU-Land ein angemessenes Schutzniveau gewährleistet. Dies bedeutet ein Schutzniveau für personenbezogene Daten, das im Wesentlichen dem Schutzniveau innerhalb der EU entspricht. Die Angemessenheitsbeschlüsse haben zur Folge, dass personenbezogene Daten ohne weitere Hindernisse aus der EU (sowie aus Norwegen, Liechtenstein und Island) in ein Drittland fließen können. Ähnliche Vorschriften gelten für das Vereinigte Königreich, die Schweiz und einige andere Länder.

In den Fällen, in denen die Europäische Kommission oder die Regierung eines anderen Landes entschieden hat, dass ein Drittland ein angemessenes Schutzniveau gewährleistet und ein gültiges Rahmenwerk besteht (z. B. EU-U.S. Data Privacy Framework, Swiss-U.S. Data Privacy Framework, UK Extension to the EU-U.S. Data Privacy Framework), basieren alle Übermittlungen von uns an die Mitglieder solcher Rahmenwerke (z. B. selbst zertifizierte Einrichtungen) ausschließlich auf der Mitgliedschaft dieser Einrichtung in dem jeweiligen Rahmenwerk. Wenn wir oder eines unserer Konzernunternehmen Mitglied eines solchen Rahmenwerks sind, basieren alle Übermittlungen an uns oder unser Konzernunternehmen ausschließlich auf der Mitgliedschaft des jeweiligen Unternehmens in diesem Rahmenwerk.


© All rights reserved by Heiko Maniero.

Jeder Betroffene kann eine Kopie der Rahmenwerke von uns erhalten. Zudem sind die Rahmenwerke auch im Amtsblatt der Europäischen Union oder in den publizierten Gesetzesmaterialien oder auf den Webseiten von Aufsichtsbehörden oder anderen zuständigen Behörden oder Institutionen verfügbar.

## F. Dauer, für die die personenbezogenen Daten gespeichert werden oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer (Art. 13 II lit. a DS-GVO)

Die Dauer der Speicherung personenbezogener Daten von Bewerbern beträgt 6 Monate. Für Mitarbeiterdaten gilt die gesetzliche Aufbewahrungspflicht. Nach Ablauf der Frist werden die entsprechenden Daten routinemäßig gelöscht, sofern sie nicht mehr zur Vertragserfüllung oder Vertragsanbahnung erforderlich sind.

## G. Bestehen der Rechte auf Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung und des Widerspruchsrechts gegen die Verarbeitung sowie des Rechts auf Datenübertragbarkeit (Art. 13 II lit. b DS-GVO)

Alle Betroffenen haben die folgenden Rechte:

***Auskunftsrecht***

Jeder Betroffene hat ein Auskunftsrecht über die ihn betreffenden personenbezogenen Daten. Das Auskunftsrecht erstreckt sich auf alle von uns verarbeiteten Daten. Das Recht kann problemlos und in angemessenen Abständen wahrgenommen werden, damit sich alle Betroffenen der Verarbeitung ihrer personenbezogenen Daten stets bewusst sind und deren Rechtmäßigkeit überprüfen können (Erwägungsgrund 63 DS-GVO). Dieses Recht ergibt sich aus Art. 15 DS-GVO. Zur Ausübung des Auskunftsrechts kann sich der Betroffene an uns wenden.

***Recht auf Berichtigung***

Nach Art. 16 Satz 1 DS-GVO haben alle Betroffenen das Recht, vom Verantwortlichen unverzüglich die Berichtigung sie betreffender unrichtiger personenbezogener Daten zu verlangen. Zudem wird durch Art. 16 Satz 2 DS-GVO normiert, dass dem Betroffenen unter Berücksichtigung der Verarbeitungszwecke das Recht zusteht, die Vervollständigung unvollständiger personenbezogener Daten - auch mittels einer ergänzenden Erklärung - zu verlangen. Zur Ausübung des Berichtigungsrechts kann sich jeder Betroffene an uns wenden.

***Recht auf Löschung (Recht auf Vergessenwerden)***

Im Übrigen steht Betroffenen ein Recht auf Löschung und Vergessenwerden nach Art. 17 DS-GVO zu. Auch dieses Recht kann über eine Kontaktaufnahme zu uns geltend gemacht werden. An dieser Stelle erlauben wir uns jedoch den Hinweis, dass dieses Recht nicht gilt, soweit die Verarbeitung zur Erfüllung einer rechtlichen Verpflichtung, dem unser Unternehmen unterliegt, erforderlich ist, Art. 17 III lit. b DS-


© All rights reserved by Heiko Maniero.

GVO. Dies bedeutet, dass wir einen Löschantrag erst nach Ablauf der gesetzlichen Aufbewahrungsfrist genehmigen können.

***Einschränkung der Verarbeitung***

Gemäß Art. 18 DS-GVO steht jedem Betroffenen ein Recht auf Einschränkung der Verarbeitung zu. Eine Einschränkung der Verarbeitung kann verlangt werden, wenn eine der Voraussetzungen aus Art. 18 I lit. a-d DS-GVO zutrifft. Das Recht auf Einschränkung der Verarbeitung kann über uns geltend gemacht werden.

***Recht auf Widerspruch***

Des Weiteren garantiert Art. 21 DS-GVO das Recht auf Widerspruch. Das Recht auf Wiederspruch kann über uns geltend gemacht werden.

***Recht auf Datenübertragbarkeit***

Art. 20 DS-GVO gewährt dem Betroffenen ein Recht auf Datenübertragbarkeit. Nach dieser Vorschrift hat die betroffene Person unter den Voraussetzungen des Art. 20 I lit. a und b DS-GVO das Recht, die sie betreffenden personenbezogenen Daten, die sie dem Verantwortlichen bereitgestellt hat, in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten, und diese Daten einem anderen Verantwortlichen ohne Behinderung durch den Verantwortlichen, zu übermitteln. Der Betroffene kann das Recht auf Datenübertragbarkeit über uns ausüben.

## H. Bestehen des Rechts, die Einwilligung jederzeit zu widerrufen, ohne dass die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung berührt wird, sofern die Verarbeitung auf Art. 6 I lit. a DS-GVO oder Art. 9 II lit. a DS-GVO beruht (Art. 13 II lit. c DS-GVO)

Beruht eine Verarbeitung personenbezogener Daten auf Art. 6 I lit. a DS-GVO, was der Fall ist, wenn die betroffene Person eine Einwilligung in eine Verarbeitung sie betreffender personenbezogener Daten für einen oder mehrere bestimmte Zwecke erteilt hat oder beruht die Verarbeitung auf Art. 9 II lit. a DS-GVO, der die ausdrückliche Einwilligung in die Verarbeitung besonderer Kategorien personenbezogener Daten regelt, so hat die betroffene Person nach Art. 7 III Satz 1 DS-GVO das Recht, ihre Einwilligung jederzeit zu widerrufen.

Durch den Widerruf der Einwilligung wird die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung nicht berührt, Art. 7 III Satz 2 DS-GVO. Der Widerruf der Einwilligung muss so einfach wie die Erteilung der Einwilligung sein, Art. 7 III Satz 4 DS-GVO. Daher kann der Widerruf der Einwilligung stets auf demselben Weg erfolgen, wie die Einwilligung erfolgte oder auf jede andere Art, die von der betroffenen Person als einfacher betrachtet wird. In der heutigen Informationsgesellschaft dürfte der wohl einfachste Weg für den Widerruf einer Einwilligung eine simple E-Mail sein. Sofern der Betroffene eine gegenüber uns erteilte Einwilligung widerrufen möchte, so ist eine


© All rights reserved by Heiko Maniero.

einfache E-Mail an uns hierfür ausreichend. Alternativ kann die betroffene Person einen beliebigen anderen Weg wählen, um uns den Widerruf der Einwilligung mitzuteilen.

## I. Beschwerderecht bei einer Aufsichtsbehörde (Art. 13 II lit. d, 77 I DS-GVO)

Als Verantwortlicher sind wir verpflichtet, dem Betroffenen das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde mitzuteilen, Art. 13 II lit. d DS-GVO. Das Beschwerderecht wird in Art. 77 I DS-GVO geregelt. Nach dieser Vorschrift hat jede betroffene Person unbeschadet eines anderweitigen verwaltungsrechtlichen oder gerichtlichen Rechtsbehelfs das Recht auf Beschwerde bei einer Aufsichtsbehörde, insbesondere in dem Mitgliedstaat ihres Aufenthaltsorts, ihres Arbeitsplatzes oder des Orts des mutmaßlichen Verstoßes, wenn die betroffene Person der Ansicht ist, dass die Verarbeitung der sie betreffenden personenbezogenen Daten gegen die Datenschutz-Grundverordnung verstößt. Das Beschwerderecht wurde durch den unionalen Gesetzgeber ausschließlich dahingehend beschränkt, dass es nur gegenüber einer einzigen Aufsichtsbehörde ausgeübt werden kann (Erwägungsgrund 141 Satz 1 DS-GVO). Diese Regelung soll Doppelbeschwerden in gleicher Sache durch die gleiche betroffene Person vermeiden. Sofern sich eine betroffene Person über uns beschweren möchte, wird deshalb darum gebeten, nur eine einzige Aufsichtsbehörde zu kontaktieren.

## J. Gesetzliche oder vertragliche Vorschriften zur Bereitstellung der personenbezogenen Daten; Erforderlichkeit für den Vertragsabschluss; Verpflichtung der betroffenen Person, die personenbezogenen Daten bereitzustellen; mögliche Folgen der Nichtbereitstellung (Art. 13 II lit. e DS-GVO)

Wir klären Sie darüber auf, dass die Bereitstellung personenbezogener Daten zum Teil gesetzlich vorgeschrieben ist (z.B. Steuervorschriften) oder sich auch aus vertraglichen Regelungen (z.B. Angaben zum Vertragspartner) ergeben kann.

Mitunter kann es zu einem Vertragsschluss erforderlich sein, dass eine betroffene Person uns personenbezogene Daten zur Verfügung stellt, die in der Folge durch uns verarbeitet werden müssen. Die betroffene Person ist beispielsweise verpflichtet uns personenbezogene Daten bereitzustellen, wenn unser Unternehmen mit ihr einen Vertrag abschließt. Eine Nichtbereitstellung der personenbezogenen Daten hätte zur Folge, dass der Vertrag mit dem Betroffenen nicht geschlossen werden könnte.

Vor einer Bereitstellung personenbezogener Daten durch den Betroffenen muss sich der Betroffene an uns wenden. Wir klären den Betroffenen einzelfallbezogen darüber auf, ob die Bereitstellung der personenbezogenen Daten gesetzlich oder vertraglich vorgeschrieben oder für den Vertragsabschluss erforderlich ist, ob eine Verpflichtung besteht, die personenbezogenen Daten bereitzustellen, und welche Folgen die Nichtbereitstellung der personenbezogenen Daten hätte.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

### K. Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling gem. Art. 22 I, IV DS-GVO und - zumindest in diesen Fällen - aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person (Art. 13 II lit. f DS-GVO)

Als verantwortungsbewusstes Unternehmen verzichten wir normalerweise auf eine automatische Entscheidungsfindung oder ein Profiling. Falls wir in Ausnahmefällen eine automatische Entscheidungsfindung oder ein Profiling durchführen, informieren wir die betroffene Person entweder gesondert oder über einen Unterpunkt in unserer Datenschutzerklärung (auf unserer Webseite). In diesem Fall gilt folgendes:

Zu einer automatisierten Entscheidungsfindung – einschließlich Profiling - kann es kommen, wenn dies (1) für den Abschluss oder die Erfüllung eines Vertrags zwischen der betroffenen Person und uns erforderlich ist, oder (2) dies aufgrund von Rechtsvorschriften der Union oder der Mitgliedstaaten, denen wir unterliegen, zulässig ist und diese Rechtsvorschriften angemessene Maßnahmen zur Wahrung der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person enthalten, oder (3) dies mit ausdrücklicher Einwilligung der betroffenen Person erfolgt.

In den in Artikel 22 Absatz 2 Buchstaben a und c DS-GVO genannten Fällen treffen wir angemessene Maßnahmen, um die Rechte und Freiheiten sowie die berechtigten Interessen der betroffenen Person zu wahren. Im diesen Fällen haben Sie das Recht auf Erwirkung des Eingreifens einer Person seitens des Verantwortlichen, auf Darlegung des eigenen Standpunkts und auf Anfechtung der Entscheidung.

Aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person werden in unserer Datenschutzerklärung aufgeführt.

## II. Erfüllung der Informationspflichten für die Fälle, bei denen die personenbezogenen Daten nicht bei der betroffenen Person erhoben wurden (Art. 14 DS-GVO)

### A. Name und Kontaktdaten des Verantwortlichen (Art. 14 I lit. a DS-GVO)

Siehe oben

### B. Kontaktdaten des Datenschutzbeauftragten (Art. 14 I lit. b DS-GVO)

Siehe oben


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## C. Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen, sowie die Rechtsgrundlage für die Verarbeitung (Art. 14 I lit. c DS-GVO)

Für Bewerberdaten die nicht bei der betroffenen Person erhoben wurden, ist der Zweck der Datenverarbeitung, eine Prüfung der Bewerbung im Bewerbungsverfahren durchzuführen. Für diesen Zweck verarbeiten wir alle von uns nicht bei Ihnen erhobenen Daten. Auf Basis der im Rahmen der Bewerbung verarbeiteten Daten prüfen wir, ob Sie zu einem Vorstellungsgespräch (Teil des Auswahlverfahrens) eingeladen werden. Werden Sie von uns eingestellt, wandeln sich nicht bei Ihnen erhobene Bewerberdaten automatisch in Mitarbeiterdaten. Für solche Mitarbeiterdaten ist der Zweck der Datenverarbeitung, die Erfüllung des Arbeitsvertrages und sonstiger gesetzlicher Vorschriften die auf das Arbeitsverhältnis anwendbar sind. Mitarbeiterdaten werden nach Beendigung des Arbeitsverhältnisses zur Erfüllung gesetzlicher Aufbewahrungsfristen gespeichert.

Rechtsgrundlagen für die Datenverarbeitung sind Art. 6 Abs. 1 Buchst. b und f DS-GVO, Art. 9 Abs. 2 Buchst. b und h DS-GVO, Art. 88 Abs. 1 DS-GVO sowie nationale Rechtsvorschriften, wie etwa für Deutschland § 26 BDSG.

## D. Kategorien personenbezogener Daten, die verarbeitet werden (Art. 14 I lit. d DS-GVO)

Bewerberdaten

Mitarbeiterdaten

## E. Kategorien von Empfängern der personenbezogenen Daten (Art. 14 I lit. e DS-GVO)

Öffentliche Stellen

Externe Stellen

Weitere externe Stellen

Interne Verarbeitung

Konzerninterne Verarbeitung

Sonstige Stellen


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

Eine Liste unserer Auftragsverarbeiter und der Datenempfänger in Drittländern sowie ggf. der internationalen Organisationen ist entweder auf unserer Webseite veröffentlicht oder kann kostenfrei bei uns angefordert werden. Bitte wenden Sie sich zur Anforderung dieser Liste an unseren Datenschutzbeauftragten.

## F. Empfänger in einem Drittland und geeignete oder angemessene Garantien und die Möglichkeit, eine Kopie von ihnen zu erhalten, oder wo sie verfügbar sind (Art. 14 I lit. f, 46 I, II lit. c DS-GVO)

Alle Unternehmen und Niederlassungen, die unserem Konzern angehören (nachfolgend "Konzerngesellschaften" genannt) und ihren oder einen Geschäftssitz in einem Drittland haben, können zu den Empfängern von personenbezogenen Daten gehören. Eine Liste aller Konzerngesellschaften oder Empfänger kann bei uns angefordert werden.

Gemäß Art. 46 I DS-GVO darf der Verantwortliche oder ein Auftragsverarbeiter nur dann personenbezogene Daten an ein Drittland übermitteln, wenn der Verantwortliche oder der Auftragsverarbeiter geeignete Garantien vorgesehen hat und sofern den betroffenen Personen durchsetzbare Rechte und wirksame Rechtsbehelfe zur Verfügung stehen. Geeignete Garantien können, ohne dass es hierzu einer besonderen Genehmigung einer Aufsichtsbehörde bedarf, durch Standarddatenschutzklauseln abgebildet werden, Art. 46 II lit. c DS-GVO.

Mit allen Empfängern aus Drittländern werden vor der ersten Übermittlung personenbezogener Daten die EU-Standarddatenschutzklauseln oder andere geeignete Garantien vereinbart. Folglich ist sichergestellt, dass für sämtliche Verarbeitungen von personenbezogenen Daten geeignete Garantien, durchsetzbare Rechte und wirksame Rechtsbehelfe gewährleistet sind. Jeder Betroffene kann eine Kopie der Standarddatenschutzklauseln von uns erhalten. Zudem sind die Standarddatenschutzklauseln auch im Amtsblatt der Europäischen Union verfügbar.

Artikel 45 Absatz 3 der Datenschutz-Grundverordnung (DSGVO) ermächtigt die Europäische Kommission, im Wege eines Durchführungsrechtsakts zu beschließen, dass ein Nicht-EU-Land ein angemessenes Schutzniveau gewährleistet. Dies bedeutet ein Schutzniveau für personenbezogene Daten, das im Wesentlichen dem Schutzniveau innerhalb der EU entspricht. Die Angemessenheitsbeschlüsse haben zur Folge, dass personenbezogene Daten ohne weitere Hindernisse aus der EU (sowie aus Norwegen, Liechtenstein und Island) in ein Drittland fließen können. Ähnliche Vorschriften gelten für das Vereinigte Königreich, die Schweiz und einige andere Länder.

In den Fällen, in denen die Europäische Kommission oder die Regierung eines anderen Landes entschieden hat, dass ein Drittland ein angemessenes Schutzniveau gewährleistet und ein gültiges Rahmenwerk besteht (z. B. EU-U.S. Data Privacy Framework, Swiss-U.S. Data Privacy Framework, UK Extension to the EU-U.S. Data Privacy Framework), basieren alle Übermittlungen von uns an die Mitglieder solcher Rahmenwerke (z. B. selbst zertifizierte Einrichtungen) ausschließlich auf der


© All rights reserved by Heiko Maniero.

Mitgliedschaft dieser Einrichtung in dem jeweiligen Rahmenwerk. Wenn wir oder eines unserer Konzernunternehmen Mitglied eines solchen Rahmenwerks sind, basieren alle Übermittlungen an uns oder unser Konzernunternehmen ausschließlich auf der Mitgliedschaft des jeweiligen Unternehmens in diesem Rahmenwerk.

Jeder Betroffene kann eine Kopie der Rahmenwerke von uns erhalten. Zudem sind die Rahmenwerke auch im Amtsblatt der Europäischen Union oder in den publizierten Gesetzesmaterialien oder auf den Webseiten von Aufsichtsbehörden oder anderen zuständigen Behörden oder Institutionen verfügbar.

## G. Dauer, für die die personenbezogenen Daten gespeichert werden oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer (Art. 14 II lit. a DS-GVO)

Die Dauer der Speicherung personenbezogener Daten von Bewerbern beträgt 6 Monate. Für Mitarbeiterdaten gilt die gesetzliche Aufbewahrungsfrist. Nach Ablauf der Frist werden die entsprechenden Daten routinemäßig gelöscht, sofern sie nicht mehr zur Vertragserfüllung oder Vertragsanbahnung erforderlich sind.

## H. Mitteilung der berechtigten Interessen, die vom Verantwortlichen oder einem Dritten verfolgt werden, wenn die Verarbeitung auf Art. 6 I lit. f DS-GVO beruht (Art. 14 II lit. b DS-GVO)

Gemäß Art. 6 I lit. f DS-GVO ist eine Verarbeitung nur rechtmäßig, wenn sie zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen. Nach Erwägungsgrund 47 Satz 2 DS-GVO kann ein berechtigtes Interesse vorliegen, wenn eine maßgebliche und angemessene Beziehung zwischen der betroffenen Person und dem Verantwortlichen besteht, z. B. wenn die betroffene Person ein Kunde des Verantwortlichen ist. In allen Fällen in denen unser Unternehmen die Verarbeitung von personenbezogenen Bewerberdaten und Mitarbeiterdaten auf Art. 6 I lit. f DS-GVO stützt, liegt unser berechtigtes Interesse in der Beschäftigung von geeignetem Personal und Fachkräften.

## I. Bestehen des Rechts auf Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung und des Widerspruchsrechts gegen die Verarbeitung sowie des Rechts auf Datenübertragbarkeit (Art. 14 II lit. c DS-GVO)

Alle Betroffenen haben die folgenden Rechte:


© All rights reserved by Heiko Maniero.

***Auskunftsrecht***

Jeder Betroffene hat ein Auskunftsrecht über die ihn betreffenden personenbezogenen Daten. Das Auskunftsrecht erstreckt sich auf alle von uns verarbeiteten Daten. Das Recht kann problemlos und in angemessenen Abständen wahrgenommen werden, damit sich alle Betroffenen der Verarbeitung ihrer personenbezogenen Daten stets bewusst sind und deren Rechtmäßigkeit überprüfen können (Erwägungsgrund 63 DS-GVO). Dieses Recht ergibt sich aus Art. 15 DS-GVO. Zur Ausübung des Auskunftsrechts kann sich der Betroffene an uns wenden.

***Recht auf Berichtigung***

Nach Art. 16 Satz 1 DS-GVO haben alle Betroffenen das Recht, vom Verantwortlichen unverzüglich die Berichtigung sie betreffender unrichtiger personenbezogener Daten zu verlangen. Zudem wird durch Art. 16 Satz 2 DS-GVO normiert, dass dem Betroffenen unter Berücksichtigung der Verarbeitungszwecke das Recht zusteht, die Vervollständigung unvollständiger personenbezogener Daten - auch mittels einer ergänzenden Erklärung - zu verlangen. Zur Ausübung des Berichtigungsrechts kann sich jeder Betroffene an uns wenden.

***Recht auf Löschung (Recht auf Vergessenwerden)***

Im Übrigen steht Betroffenen ein Recht auf Löschung und Vergessenwerden nach Art. 17 DS-GVO zu. Auch dieses Recht kann über eine Kontaktaufnahme zu uns geltend gemacht werden. An dieser Stelle erlauben wir uns jedoch den Hinweis, dass dieses Recht nicht gilt, soweit die Verarbeitung zur Erfüllung einer rechtlichen Verpflichtung, dem unser Unternehmen unterliegt, erforderlich ist, Art. 17 III lit. b DS-GVO. Dies bedeutet, dass wir einen Löschantrag erst nach Ablauf der gesetzlichen Aufbewahrungsfrist genehmigen können.

***Einschränkung der Verarbeitung***

Gemäß Art. 18 DS-GVO steht jedem Betroffenen ein Recht auf Einschränkung der Verarbeitung zu. Eine Einschränkung der Verarbeitung kann verlangt werden, wenn eine der Voraussetzungen aus Art. 18 I lit. a-d DS-GVO zutrifft. Das Recht auf Einschränkung der Verarbeitung kann uns geltend gemacht werden.

***Recht auf Widerspruch***

Des Weiteren garantiert Art. 21 DS-GVO das Recht auf Widerspruch. Das Recht auf Wiederspruch kann über uns geltend gemacht werden.

***Recht auf Datenübertragbarkeit***

Art. 20 DS-GVO gewährt dem Betroffenen ein Recht auf Datenübertragbarkeit. Nach dieser Vorschrift hat die betroffene Person unter den Voraussetzungen des Art. 20 I lit. a und b DS-GVO das Recht, die sie betreffenden personenbezogenen Daten, die sie dem Verantwortlichen bereitgestellt hat, in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten, und diese Daten einem anderen Verantwortlichen ohne Behinderung durch den Verantwortlichen, zu übermitteln. Der Betroffene kann das Recht auf Datenübertragbarkeit über uns ausüben.


© All rights reserved by Heiko Maniero.

## J. Bestehen des Rechts, die Einwilligung jederzeit zu widerrufen, ohne dass die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung berührt wird, sofern die Verarbeitung auf Art. 6 I lit. a oder Art. 9 II lit. a DS-GVO beruht (Art. 14 II lit. d DS-GVO)

Beruht eine Verarbeitung personenbezogener Daten auf Art. 6 I lit. a DS-GVO, was der Fall ist, wenn die betroffene Person eine Einwilligung in eine Verarbeitung sie betreffender personenbezogener Daten für einen oder mehrere bestimmte Zwecke erteilt hat oder beruht die Verarbeitung auf Art. 9 II lit. a DS-GVO, der die ausdrückliche Einwilligung in die Verarbeitung besonderer Kategorien personenbezogener Daten regelt, so hat die betroffene Person nach Art. 7 III Satz 1 DS-GVO das Recht, ihre Einwilligung jederzeit zu widerrufen.

Durch den Widerruf der Einwilligung wird die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung nicht berührt, Art. 7 III Satz 2 DS-GVO. Der Widerruf der Einwilligung muss so einfach wie die Erteilung der Einwilligung sein, Art. 7 III Satz 4 DS-GVO. Daher kann der Widerruf der Einwilligung stets auf demselben Weg erfolgen, wie die Einwilligung erfolgte oder auf jeder anderen Art, die von der betroffenen Person als einfacher betrachtet wird. In der heutigen Informationsgesellschaft dürfte der wohl einfachste Weg für den Widerruf einer Einwilligung eine simple E-Mail sein. Sofern der Betroffene eine gegenüber uns erteilte Einwilligung widerrufen möchte, so ist eine einfache E-Mail an uns hierfür ausreichend. Alternativ kann die betroffene Person einen beliebigen anderen Weg wählen, um uns den Widerruf der Einwilligung mitzuteilen.

## K. Beschwerderecht bei einer Aufsichtsbehörde (Art. 14 II lit. e, 77 I DS-GVO)

Als Verantwortlicher sind wir verpflichtet, dem Betroffenen das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde mitzuteilen, Art. 14 II lit. e DS-GVO. Das Beschwerderecht wird in Art. 77 I DS-GVO geregelt. Nach dieser Vorschrift hat jede betroffene Person unbeschadet eines anderweitigen verwaltungsrechtlichen oder gerichtlichen Rechtsbehelfs das Recht auf Beschwerde bei einer Aufsichtsbehörde, insbesondere in dem Mitgliedstaat ihres Aufenthaltsorts, ihres Arbeitsplatzes oder des Orts des mutmaßlichen Verstoßes, wenn die betroffene Person der Ansicht ist, dass die Verarbeitung der sie betreffenden personenbezogenen Daten gegen die Datenschutz-Grundverordnung verstößt. Das Beschwerderecht wurde durch den unionalen Gesetzgeber ausschließlich dahingehend beschränkt, dass es nur gegenüber einer einzigen Aufsichtsbehörde ausgeübt werden kann (Erwägungsgrund 141 Satz 1 DS-GVO). Diese Regelung soll Doppelbeschwerden in gleicher Sache durch die gleiche betroffene Person vermeiden. Sofern sich eine betroffene Person über uns beschweren möchte, wird deshalb darum gebeten, nur eine einzige Aufsichtsbehörde zu kontaktieren.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## L. Quelle aus der die personenbezogenen Daten stammen und gegebenenfalls ob sie aus öffentlich zugänglichen Quellen stammen (Art. 14 II lit. f DS-GVO)

Grundsätzlich werden personenbezogene Daten direkt beim Betroffenen oder im Zusammenwirken mit einer Behörde erhoben (z.B. Auslesen von Daten eines behördlichen Registers). Andere Daten über Betroffene stammen aus Übermittlungen von Konzerngesellschaften. Im Rahmen dieser allgemein zu haltenden Information ist eine Mitteilung der exakten Quellen aus denen die personenbezogenen Daten stammen entweder unmöglich oder verursacht unverhältnismäßigen Aufwand im Sinne von Art. 14 V lit. b DS-GVO. Wir erheben grundsätzlich keine personenbezogenen Daten aus öffentlich zugänglichen Quellen.

Jeder Betroffene kann sich jederzeit an uns wenden, um genauere Informationen über exakte Quellen der sie betreffenden personenbezogenen Daten zu erhalten. Kann der betroffenen Person nicht exakt mitgeteilt werden, woher die personenbezogenen Daten stammen, weil verschiedene Quellen benutzt wurden, so wird die individuelle Unterrichtung allgemein gehalten (Erwägungsgrund 61 Satz 4 DS-GVO).

## M. Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling gem. Art. 22 I, IV DS-GVO und - zumindest in diesen Fällen - aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person (Art. 14 II lit. g DS-GVO)

Als verantwortungsbewusstes Unternehmen verzichten wir normalerweise auf eine automatische Entscheidungsfindung oder ein Profiling. Falls wir in Ausnahmefällen eine automatische Entscheidungsfindung oder ein Profiling durchführen, informieren wir die betroffene Person entweder gesondert oder über einen Unterpunkt in unserer Datenschutzerklärung (auf unserer Webseite). In diesem Fall gilt folgendes:

Zu einer automatisierten Entscheidungsfindung – einschließlich Profiling - kann es kommen, wenn dies (1) für den Abschluss oder die Erfüllung eines Vertrags zwischen der betroffenen Person und uns erforderlich ist, oder (2) dies aufgrund von Rechtsvorschriften der Union oder der Mitgliedstaaten, denen wir unterliegen, zulässig ist und diese Rechtsvorschriften angemessene Maßnahmen zur Wahrung der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person enthalten, oder (3) dies mit ausdrücklicher Einwilligung der betroffenen Person erfolgt.

In den in Artikel 22 Absatz 2 Buchstaben a und c DS-GVO genannten Fällen treffen wir angemessene Maßnahmen, um die Rechte und Freiheiten sowie die berechtigten Interessen der betroffenen Person zu wahren. Im diesen Fällen haben Sie das Recht auf Erwirkung des Eingreifens einer Person seitens des Verantwortlichen, auf Darlegung des eigenen Standpunkts und auf Anfechtung der Entscheidung.


© All rights reserved by Heiko Maniero.

Aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person werden in unserer Datenschutzerklärung aufgeführt.

## III. EU-U.S. Data Privacy Framework (EU-U.S. DPF), UK Extension to the EU-U.S. DPF, Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF)

Wenn unsere Organisation ein zertifiziertes Mitglied des EU-U.S. Data Privacy Framework (EU-U.S. DPF) und/oder der UK Extension to the EU-U.S. DPF und/oder des Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF) ist, gilt das Folgende:

Wir halten uns an das EU-U.S. Data Privacy Framework (EU-U.S. DPF) und die UK Extension to the EU-U.S. DPF sowie an das Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF), wie es vom U.S. Department of Commerce festgelegt wurde. Unser Unternehmen hat gegenüber dem US-Handelsministerium bestätigt, dass es die EU-U.S. Data Privacy Framework Principles (EU-U.S. DPF Principles) in Bezug auf die Verarbeitung personenbezogener Daten einhält, die es aus der Europäischen Union und dem Vereinigten Königreich unter Berufung auf das EU-U.S. DPF und die UK Extension to the EU-U.S. DPF erhält. Unser Unternehmen hat gegenüber dem US-Handelsministerium bestätigt, dass es die Swiss-U.S. Data Privacy Framework Principles (Swiss-U.S. DPF Principles) in Bezug auf die Verarbeitung personenbezogener Daten, die es aus der Schweiz unter Berufung auf die Swiss-U.S. DPF erhält, einhält. Im Falle eines Widerspruchs zwischen den Bestimmungen unserer Datenschutzerklärung und den EU-U.S. DPF Principles und/oder den Swiss-U.S. DPF Principles sind die Principles maßgebend.

Um mehr über das Data Privacy Framework (DPF) Programm zu erfahren und um unsere Zertifizierung einzusehen, besuchen Sie bitte https://www.dataprivacyframework.gov/.

Die anderen US-Einheiten oder US-Tochtergesellschaften unseres Unternehmens, die sich ebenfalls an die EU-U.S. DPF Principals halten, einschließlich der UK Extension to the EU-U.S. DPF und der Swiss-U.S. DPF Principals, sofern vorhanden, werden in unserer Datenschutzerklärung genannt.

In Übereinstimmung mit dem EU-U.S. DPF und der UK Extension to the EU-U.S. DPF sowie des Swiss-U.S. DPF verpflichtet sich unser Unternehmen, mit dem von den EU-Datenschutzbehörden und dem britischen Information Commissioner's Office (ICO) sowie dem Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) eingerichteten Gremium zusammenzuarbeiten und dessen Ratschläge in Bezug auf ungelöste Beschwerden über unseren Umgang mit personenbezogenen Daten zu befolgen, die wir unter Berufung auf die EU-U.S. DPF und die UK Extension to the EU-U.S. DPF und die Swiss-U.S. DPF erhalten haben.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

Wir informieren die betroffenen Personen über die zuständigen europäischen Datenschutzbehörden, die für die Bearbeitung von Beschwerden über den Umgang unserer Organisation mit personenbezogenen Daten zuständig sind, im oberen Teil dieses Transparenzdokuments und darüber, dass wir den betroffenen Personen einen angemessenen und kostenlosen Rechtsbehelf anbieten.

Wir informieren alle betroffenen Personen darüber, dass unser Unternehmen den Ermittlungs- und Durchsetzungsbefugnissen der Federal Trade Commission (FTC) unterliegt.

Betroffene Personen haben unter bestimmten Voraussetzungen die Möglichkeit, ein verbindliches Schiedsverfahren in Anspruch zu nehmen. Unsere Organisation ist verpflichtet, Ansprüche zu schlichten und die Bedingungen gemäß Anhang I der DPF-Principals einzuhalten, sofern die betroffene Person ein verbindliches Schiedsverfahren beantragt hat, indem sie unsere Organisation benachrichtigt hat und die Verfahren und Bedingungen gemäß Anhang I der Principals eingehalten hat.

Wir informieren hiermit alle betroffenen Personen über die Haftung unserer Organisation im Falle der Weitergabe von personenbezogenen Daten an Dritte.

Für Fragen der betroffenen Personen oder der Datenschutzaufsichtsbehörden haben wir die oben in diesem Transparenzdokument genannten lokalen Vertreter benannt.

Wir bieten Ihnen die Möglichkeit zu wählen (Opt-out), ob Ihre personenbezogenen Daten (i) an Dritte weitergegeben oder (ii) für einen Zweck verwendet werden sollen, der sich wesentlich von dem/den Zweck(en) unterscheidet, für den/die sie ursprünglich erhoben oder später von Ihnen genehmigt wurden. Der eindeutige, gut sichtbare und leicht zugängliche Mechanismus zur Ausübung Ihres Wahlrechts besteht darin, unseren Datenschutzbeauftragten (DSB) per E-Mail zu kontaktieren. Sie haben keine Wahlmöglichkeit und wir sind auch nicht dazu verpflichtet, wenn die Daten an einen Dritten weitergegeben werden, der als Beauftragter oder Auftragsverarbeiter in unserem Namen und auf unsere Anweisung hin Aufgaben wahrnimmt. Wir schließen jedoch immer einen Vertrag mit einem solchen Beauftragten oder Auftragsverarbeiter ab.

Für sensible Daten (d. h. personenbezogene Daten, die Angaben über den Gesundheitszustand, die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, die Mitgliedschaft in einer Gewerkschaft oder Angaben zum Sexualleben der betreffenden Person enthalten) holen wir Ihre ausdrückliche Zustimmung (Opt-in) ein, wenn diese Daten (i) an Dritte weitergegeben oder (ii) für einen anderen Zweck als denjenigen verwendet werden sollen, für den sie ursprünglich erhoben wurden oder für den Sie nachträglich Ihre Zustimmung erteilt haben, indem Sie Ihre Opt-in-Wahl getroffen haben. Darüber hinaus behandeln wir alle personenbezogenen Daten, die wir von Dritten erhalten, als sensibel, wenn der Dritte sie als sensibel identifiziert und behandelt.

Wir informieren Sie hiermit über das Erfordernis, personenbezogene Daten in Reaktion auf rechtmäßige Anfragen von Behörden offenzulegen, einschließlich der Erfüllung von Anforderungen der nationalen Sicherheit oder der Strafverfolgung.


© All rights reserved by Heiko Maniero.

Bei der Übermittlung personenbezogener Daten an einen Dritten, der als Verantwortlicher handelt, halten wir uns an die Principals der Benachrichtigung und der Wahlmöglichkeit. Außerdem schließen wir mit dem Dritten, der für die Verarbeitung verantwortlich ist, einen Vertrag ab, der vorsieht, dass diese Daten nur für begrenzte und festgelegte Zwecke in Übereinstimmung mit der von Ihnen erteilten Einwilligung verarbeitet werden dürfen und dass der Empfänger das gleiche Schutzniveau wie die Principals des DPF bietet und uns benachrichtigt, wenn er feststellt, dass er diese Verpflichtung nicht mehr erfüllen kann. Der Vertrag sieht vor, dass der Dritte, der Verantwortlicher ist, die Verarbeitung einstellt oder andere angemessene und geeignete Maßnahmen ergreift, um Abhilfe zu schaffen, wenn eine solche Feststellung getroffen wird.

Bei der Übermittlung personenbezogener Daten an einen Dritten, der als Beauftragter oder Auftragsverarbeiter handelt, (i) übermitteln wir diese Daten nur für begrenzte und festgelegte Zwecke; (ii) vergewissern wir uns, dass der Beauftragte oder Auftragsverarbeiter verpflichtet ist, mindestens das gleiche Maß an Datenschutz zu gewährleisten, wie es die DPF-Principals verlangen; (iii) ergreifen wir angemessene und geeignete Maßnahmen, um sicherzustellen, dass der Beauftragte oder Auftragsverarbeiter die übermittelten personenbezogenen Daten tatsächlich in einer Weise verarbeitet, die mit unseren Verpflichtungen gemäß den DPF-Principals übereinstimmt; (iv) von dem Beauftragten oder Auftragsverarbeiter zu verlangen, dass er unsere Organisation benachrichtigt, wenn er feststellt, dass er seiner Verpflichtung nicht mehr nachkommen kann, das gleiche Schutzniveau zu bieten, wie es die DPF-Principals vorsehen; (v) nach einer Benachrichtigung, auch unter (iv), angemessene und geeignete Schritte zu unternehmen, um die unbefugte Verarbeitung zu stoppen und Abhilfe zu schaffen; und (vi) dem DPF Department auf Anfrage eine Zusammenfassung oder ein repräsentatives Exemplar der einschlägigen Datenschutzbestimmungen seines Vertrags mit diesem Beauftragten zur Verfügung zu stellen.

In Übereinstimmung mit dem EU-U.S. DPF und/oder der UK Extension to the EU-U.S. DPF und/oder der Swiss-U.S. DPF verpflichtet sich unsere Organisation, mit dem von den EU-Datenschutzbehörden und dem britischen Information Commissioner's Office (ICO) bzw. dem Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) eingerichteten Gremium zusammenzuarbeiten und dessen Ratschläge in Bezug auf ungelöste Beschwerden über unseren Umgang mit Personaldaten, die wir unter Berufung auf die EU-U.S. DPF und der UK-Erweiterung der EU-U.S. DPF und der Swiss-U.S. DPF im Zusammenhang mit dem Arbeitsverhältnis erhalten, zu befolgen.

Allen betroffenen Personen, die sich vorübergehend in der Europäischen Union (EU), im Europäischen Wirtschaftsraum (EWR) oder im Vereinigten Königreich aufhalten oder dort ihren Wohnsitz oder gewöhnlichen Aufenthaltsort haben, stehen die in unserem Transparenzdokument publizierten Rechte und Betroffenenrechte zu, die sich auch aus Artikeln 15 bis 22 DS-GVO ergeben, inklusive dem Recht auf Auskunft. Diese Informationen haben wir in allen Sprachen der EU und des EWR zur Verfügung gestellt. Die englische Sprachfassung gilt für das Vereinigte Königreich.

Allen betroffenen Personen, die sich vorübergehend in der Schweiz aufhalten oder dort ihren Wohnsitz oder gewöhnlichen Aufenthaltsort haben, stehen die in unserem Transparenzdokument publizierten


© All rights reserved by Heiko Maniero.

Rechte und Betroffenenrechte aus dem Schweizer Datenschutzgesetz (DSG) und der Schweizer Datenschutzverordnung (DSV) zu, inklusive dem Recht auf Auskunft. Diese Informationen haben wir in den drei offiziellen Sprachen der Schweiz (Deutsch, Italienisch und Französisch) zur Verfügung gestellt.


© All rights reserved by Heiko Maniero.

# ENGLISH: Information about the Processing of Personal Data (Article 13, 14 GDPR)

Dear Sir or Madam,

The personal data of every individual who is in a contractual, pre-contractual or other relationship with our company deserve special protection. Our goal is to keep our data protection level to a high standard. Therefore, we are routinely developing our data protection and data security concepts.

Of course, we comply with the statutory provisions on data protection. According to Article 13, 14 GDPR, controllers meet specific information requirements when collecting personal data. This document fulfills these obligations.

The terminology of legal regulations is complicated. Unfortunately, the use of legal terms could not be dispensed with in the preparation of this document. Therefore, we would like to point out that you are always welcome to contact us for all questions concerning this document, the used terms or formulations.

## I. Compliance with the information requirements when personal data is collected from the data subject (Article 13 GDPR)

### A. Identity and the contact details of the controller (Article 13(1) lit. a GDPR)

See above

### B. Contact details of the Data Protection Officer (Article 13(1) lit. b GDPR)

See above

### C. Purposes of the processing for which the personal data are intended as well as the legal basis for the processing (Article 13(1) lit. c GDPR)

The purpose of the processing of personal data is the handling of all operations which concern the controller, customers, prospective customers, business partners or other contractual or pre-contractual relations between the named groups (in the broadest sense) or legal obligations of the controller.

Art. 6(1) lit. a GDPR serves as the legal basis for processing operations for which we obtain consent for a specific processing purpose. If the processing of personal data is necessary for the performance of a contract to which the data subject is party, as is the case, for example, when processing operations are


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

necessary for the supply of goods or to provide any other service, the processing is based on Article 6(1) lit. b GDPR. The same applies to such processing operations which are necessary for carrying out pre-contractual measures, for example in the case of inquiries concerning our products or services. Is our company subject to a legal obligation by which processing of personal data is required, such as for the fulfillment of tax obligations, the processing is based on Art. 6(1) lit. c GDPR.

In rare cases, the processing of personal data may be necessary to protect the vital interests of the data subject or of another natural person. This would be the case, for example, if a visitor were injured in our company and his name, age, health insurance data or other vital information would have to be passed on to a doctor, hospital or other third party. Then the processing would be based on Art. 6(1) lit. d GDPR.

Where the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, the legal basis is Art. 6(1) lit. e GDPR.

Finally, processing operations could be based on Article 6(1) lit. f GDPR. This legal basis is used for processing operations which are not covered by any of the abovementioned legal grounds, if processing is necessary for the purposes of the legitimate interests pursued by our company or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data. Such processing operations are particularly permissible because they have been specifically mentioned by the European legislator. He considered that a legitimate interest could be assumed if the data subject is a client of the controller (Recital 47 Sentence 2 GDPR).

## D. Where the processing is based on Article 6(1) lit. f GDPR the legitimate interests pursued by the controller or by a third party (Article 13(1) lit. d GDPR)

Where the processing of personal data is based on Article 6(1) lit. f GDPR our legitimate interest is to carry out our business in favor of the well-being of all our employees and the shareholders.

## E. Categories of recipients of the personal data (Article 13(1) lit. e GDPR)

Public authorities

External bodies

Further external bodies

Internal processing

Intragroup processing


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

Other bodies

A list of our processors and data recipients in third countries and, if applicable, international organizations is either published on our website or can be requested from us free of charge. Please contact our data protection officer to request this list.

## F. Recipients in a third country and appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available (Article 13(1) lit. f, 46(1), 46 (2) lit. c GDPR)

All companies and branches that are part of our group (hereinafter referred to as "group companies") that have their place of business or an office in a third country may belong to the recipients of personal data. A list of all group companies or recipients can be requested from us.

According to Article 46(1) GDPR a controller or processor may transfer personal data only to a third country if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available. Appropriate safeguards may be provided without requiring any specific authorisation from a supervisory authority by means of standard contractual clauses, Article 46(2) lit. c GDPR.

The standard contractual clauses of the European Union or other appropriate safeguards are agreed on with all recipients from third countries before the first transmission of personal data. Consequently, it is ensured that appropriate safeguards, enforceable data subject rights and effective legal remedies for data subjects are guaranteed. Every data subject can obtain a copy of the standard contractual clauses from us. The standard contractual clauses are also available in the Official Journal of the European Union.

Article 45(3) of the General Data Protection Regulation (GDPR) grants the European Commission the power to decide, by means of an implementing act, that a non-EU country ensures an adequate level of protection. This means a level of protection for personal data that is essentially equivalent to the level of protection within the EU. The effect of adequacy decisions is that personal data can flow freely from the EU (and Norway, Liechtenstein and Iceland) to a third country without further obstacles. Similar rules exist for the United Kingdom, Switzerland and some other Countries.

Where the European Commission or the goverment of another country decided that a third country ensures an adequate level of protection, and a valid Framework is in place (e.g, EU-U.S. Data Privacy Framework, Swiss-U.S. Data Privacy Framework, UK Extension to the EU-U.S. Data Privacy Framework), all transfers by us to the members of such frameworks (e.g. self certified entities) are exclusively based on that entities membership in the respective framework. Where we or one of our group entitities is a member of such framework, all transfers to us or our group entity are exclusively based on the entities membership in such framework.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

Any data subject can obtain a copy of the frameworks from us. In addition, the frameworks are also available in the Official Journal of the European Union or in the published legal materials or on the websites of supervisory authorities or other competent authorities or institutions.

## G. Period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period (Article 13(2) lit. a GDPR)

The criteria used to determine the period of storage of personal data is the respective statutory retention period. After expiration of that period, the corresponding data is routinely deleted, as long as it is no longer necessary for the fulfillment of the contract or the initiation of a contract.

If there is no statutory retention period, the criterion is the contractual or internal retention period.

## H. Existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability (Article 13(2) lit. b GDPR)

All data subjects have the following rights:

***Right to access***

Each data subject has a right to access the personal data concerning him or her. The right to access extends to all data processed by us. The right can be exercised easily and at reasonable intervals, in order to be aware of, and verify, the lawfulness of the processing (Recital 63 GDPR). This right results from Art. 15 GDPR. The data subject may contact us to exercise the right to access.

***Right to rectification***

According to Article 16 Sentence 1 GDPR the data subject has the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. Moreover, Article 16 Sentence 2 GDPR provides that the data subject is entitled, taking into account the purposes of the processing, to have incomplete personal data completed, including by means of providing a supplementary statement. The data subject may contact us to exercise the right of rectification.

***Right to erasure (right to be forgotten)***

In addition, data subjects are entitled to a right to erasure and to be forgotten under Art. 17 GDPR. This right can also be exercised by contacting us. At this point, however, we would like to point out that this right does not apply insofar as the processing is necessary to fulfill a legal obligation to which our company is subject to, Article 17(3) lit. b GDPR. This means that we can approve an application to erase only after the expiration of the statutory retention period.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

***Right to restriction of processing***

According to Article 18 GDPR any data subject is entitled to a restriction of processing. The restriction of processing may be demanded if one of the conditions set out in Article 18(1) lit. a-d GDPR is fulfilled. The data subject may contact us to exercise the right to restriction of processing.

***Right to object***

Furthermore, Art. 21 GDPR guarantees the right to object. The data subject may contact us to exercise the right to object.

***Right to data portability***

Art. 20 GDPR grants the data subject the right to data portability. Under this provision, the data subject has under the conditions laid down in Article 20(1) lit. a and b GDPR the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided. The data subject may contact us to exercise the right to data portability.

## I. The existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal, where the processing is based on Article 6(1) lit. a GDPR or Article 9(2) lit. a GDPR (Article 13(2) lit. c GDPR)

If processing of personal data is based on Art. 6(1) lit. a GDPR, which is the case, if the data subject has given consent to the processing of personal data for one or more specific purposes or is it based on Article 9(2) lit. a GDPR, which regulates the explicit consent to the processing of special categories of personal data, the data subject has according to Article 7(3) Sentence 1 GDPR the right to withdraw his or her consent at any time.

Withdraw of consent shall not affect the lawfulness of processing based on consent before its withdrawal, Article 7(3) Sentence 2 GDPR. It shall be as easy to withdraw as to give consent, Art. 7(3) Sentence 4 GDPR. Therefore, the withdrawal of consent can always take place in the same way as consent has been given or in any other way, that is considered by the data subject to be simpler. In todays information society, probably the simplest way to withdraw consent is a simple email. If the data subject wishes to withdraw his or her consent granted to us, a simple email to us is sufficient. Alternatively, the data subject may choose any other way to communicate his or her withdraw of consent to us.

## J. Right to lodge a complaint with a supervisory authority (Article 13(2) lit. d, 77(1) GDPR)

As the controller, we are obliged to notify the data subject of the right to lodge a complaint with a supervisory authority, Article 13(2) lit. d GDPR. The right to lodge a complaint with a supervisory authority


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

is regulated by Article 77(1) GDPR. According to this provision, without prejudice to any other administrative or judicial remedy, every data subject shall have the right to lodge a complaint with a supervisory authority, in particular in the Member State of his or her habitual residence, place of work or place of the alleged infringement if the data subject considers that the processing of personal data relating to him or her infringes the General Data Protection Regulation. The right to lodge a complaint with a supervisory authority was only limited by the law of the Union in such way, that it can only be exercised before a single supervisory authority (Recital 141 Sentence 1 GDPR). This rule is intended to avoid double complaints of the same data subject in the same matter. If a data subject wants to lodge a complaint about us, we therefore asked to contact only a single supervisory authority.

## K. Provision of personal data as statutory or contractual requirement; Requirement necessary to enter into a contract; Obligation of the data subject to provide the personal data; possible consequences of failure to provide such data (Art. 13(2) lit. e GDPR)

We clarify that the provision of personal data is partly required by law (e.g. tax regulations) or can also result from contractual provisions (e.g. information on the contractual partner).

Sometimes it may be necessary to conclude a contract that the data subject provides us with personal data, which must subsequently be processed by us. The data subject is, for example, obliged to provide us with personal data when our company signs a contract with him or her. The non-provision of the personal data would have the consequence that the contract with the data subject could not be concluded.

Before personal data is provided by the data subject, the data subject must contact us. We clarify to the data subject whether the provision of the personal data is required by law or contract or is necessary for the conclusion of the contract, whether there is an obligation to provide the personal data and the consequences of non-provision of the personal data.

## L. Existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) GDPR and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject (Article 13 (2) lit. f GDPR)

As a responsible company, usually we do not use automated decision-making or profiling. If, in exceptional cases, we carry out automated decision-making or profiling, we will inform the data subject either separately or via a sub-section in our privacy policy (on our website). In this case, the following applies:

Automated decision-making - including profiling - may occur if (1) this is necessary for entering into, or performance of, a contract between the data subject and us, or (2) this is authorised by Union or Member


© All rights reserved by Heiko Maniero.

State law to which we are subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or (3) this is based on the data subject's explicit consent.

In the cases referred to in Article 22(2) (a) and (c) GDPR, we shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests. In these cases, you have the right to obtain human intervention on the part of the controller, to express your point of view and to contest the decision.

Meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject is set out in our privacy policy.

## II. Compliance with the information requirements when personal data is not collected from the data subject (Article 14 GDPR)

### A. Identity and the contact details of the controller (Article 14(1) lit. a GDPR)

See above

### B. Contact details of the Data Protection Officer (Article 14(1) lit. b GDPR)

See above

### C. Purposes of the processing for which the personal data are intended as well as the legal basis for the processing (Article 14(1) lit. c GDPR)

The purpose of the processing of personal data is the handling of all operations which concern the controller, customers, prospective customers, business partners or other contractual or pre-contractual relations between the named groups (in the broadest sense) or legal obligations of the controller.

If the processing of personal data is necessary for the performance of a contract to which the data subject is party, as is the case, for example, when processing operations are necessary for the supply of goods or to provide any other service, the processing is based on Article 6(1) lit. b GDPR. The same applies to such processing operations which are necessary for carrying out pre-contractual measures, for example in the case of inquiries concerning our products or services. Is our company subject to a legal obligation by which processing of personal data is required, such as for the fulfillment of tax obligations, the processing is based on Art. 6(1) lit. c GDPR.

In rare cases, the processing of personal data may be necessary to protect the vital interests of the data subject or of another natural person. This would be the case, for example, if a visitor were injured in our


© All rights reserved by Heiko Maniero.

company and his name, age, health insurance data or other vital information would have to be passed on to a doctor, hospital or other third party. Then the processing would be based on Art. 6(1) lit. d GDPR.

Where the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, the legal basis is Art. 6(1) lit. e GDPR.

Finally, processing operations could be based on Article 6(1) lit. f GDPR. This legal basis is used for processing operations which are not covered by any of the abovementioned legal grounds, if processing is necessary for the purposes of the legitimate interests pursued by our company or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data. Such processing operations are particularly permissible because they have been specifically mentioned by the European legislator. He considered that a legitimate interest could be assumed if the data subject is a client of the controller (Recital 47 Sentence 2 GDPR).

## D. Categories of personal data concerned (Article 14(1) lit. d GDPR)

Customer data

Data of potential customers

Data of employees

Data of suppliers

## E. Categories of recipients of the personal data (Article 14(1) lit. e GDPR)

Public authorities

External bodies

Further external bodies

Internal processing

Intragroup processing

Other bodies


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

A list of our processors and data recipients in third countries and, if applicable, international organizations is either published on our website or can be requested from us free of charge. Please contact our data protection officer to request this list.

## F. Recipients in a third country and appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available (Article 14(1) lit. f, 46(1), 46(2) lit. c GDPR)

All companies and branches that are part of our group (hereinafter referred to as "group companies") that have their place of business or an office in a third country may belong to the recipients of personal data. A list of all group companies can be requested from us.

According to Article 46(1) GDPR a controller or processor may transfer personal data only to a third country if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available. Appropriate safeguards may be provided without requiring any specific authorisation from a supervisory authority by means of standard data protection clauses, Article 46(2) lit. c GDPR.

The standard contractual clauses of the European Union or other appropriate safeguards are agreed on with all recipients from third countries before the first transmission of personal data. Consequently, it is ensured that appropriate safeguards, enforceable data subject rights and effective legal remedies for data subjects are guaranteed. Every data subject can obtain a copy of the standard contractual clauses from us. The standard contractual clauses are also available in the Official Journal of the European Union.

Article 45(3) of the General Data Protection Regulation (GDPR) grants the European Commission the power to decide, by means of an implementing act, that a non-EU country ensures an adequate level of protection. This means a level of protection for personal data that is essentially equivalent to the level of protection within the EU. The effect of adequacy decisions is that personal data can flow freely from the EU (and Norway, Liechtenstein and Iceland) to a third country without further obstacles. Similar rules exist for the United Kingdom, Switzerland and some other Countries.

Where the European Commission or the goverment of another country decided that a third country ensures an adequate level of protection, and a valid Framework is in place (e.g, EU-U.S. Data Privacy Framework, Swiss-U.S. Data Privacy Framework, UK Extension to the EU-U.S. Data Privacy Framework), all transfers by us to the members of such frameworks (e.g. self certified entities) are exclusively based on that entities membership in the respective framework. Where we or one of our group entitities is a member of such framework, all transfers to us or our group entity are exclusively based on the entities membership in such framework.

Any data subject can obtain a copy of the frameworks from us. In addition, the frameworks are also available in the Official Journal of the European Union or in the published legal materials or on the websites of supervisory authorities or other competent authorities or institutions.


© All rights reserved by Heiko Maniero.

## G. Period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period (Article 14(2) lit. a GDPR)

The criteria used to determine the period of storage of personal data is the respective statutory retention period. After expiration of that period, the corresponding data is routinely deleted, as long as it is no longer necessary for the fulfillment of the contract or the initiation of a contract.

If there is no statutory retention period, the criterion is the contractual or internal retention period.

## H. Notification of the legitimate interests pursued by the controller or by a third party if the processing is based on Article 6(1) lit. f GDPR (Art. 14(2) lit. b GDPR)

According to Article 6(1) lit. f GDPR, processing shall be lawful only if the processing is necessary for the purposes of legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data. According to Recital 47 Sentence 2 GDPR a legitimate interest could exist where there is a relevant and appropriate relationship between the data subject and the controller, e.g. in situations where the data subject is a client of the controller. In all cases in which our company processes personal data based on Article 6(1) lit. f GDPR, our legitimate interest is in carrying out our business in favor of the well-being of all our employees and the shareholders.

## I. Existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject and to object to processing as well as the right to data portability (Article 14(2) lit. c GDPR)

All data subjects have the following rights:

***Right to access***

Each data subject has a right to access the personal data concerning him or her. The right to access extends to all data processed by us. The right can be exercised easily and at reasonable intervals, in order to be aware of, and verify, the lawfulness of the processing (Recital 63 GDPR). This right results from Art. 15 GDPR. The data subject may contact us to exercise the right to access.

***Right to rectification***

According to Article 16 Sentence 1 GDPR the data subject has the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. Moreover, Article 16 Sentence 2 GDPR provides that the data subject is entitled, taking into account the purposes of the processing, to have incomplete personal data completed, including by means of providing a supplementary statement. The data subject may contact us to exercise the right of rectification.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

***Right to erasure (right to be forgotten)***

In addition, data subjects are entitled to a right to erasure and to be forgotten under Art. 17 GDPR. This right can also be exercised by contacting us. At this point, however, we would like to point out that this right does not apply insofar as the processing is necessary to fulfill a legal obligation to which our company is subject to, Article 17(3) lit. b GDPR. This means that we can approve an application to erase only after the expiration of the statutory retention period.

***Right to restriction of processing***

According to Article 18 GDPR any data subject is entitled to restriction of processing. The restriction of processing may be demanded if one of the conditions set out in Article 18(1) lit. a-d GDPR is fulfilled. The data subject may contact us to exercise the right to restriction of processing.

***Right to object***

Furthermore, Art. 21 GDPR guarantees the right to object. The data subject may contact us to exercise the right to object.

***Right to data portability***

Art. 20 GDPR grants the data subject the right to data portability. According to this provision the data subject has under the conditions laid down in Article 20(1) lit. a and b GDPR the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided. The data subject may contact us to exercise the right to data portability.

## J. The existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal, where the processing is based on Article 6(1) lit. a or Article 9(2) lit. a GDPR (Art. 14(2) lit. d GDPR)

If processing of personal data is based on Art. 6(1) lit. a GDPR, which is the case, if the data subject has given consent to the processing of personal data for one or more specific purposes or is it based on Article 9(2) lit. a GDPR, which regulates the explicit consent to the processing of special categories of personal data, the data subject has according to Article 7(3) Sentence 1 GDPR the right to withdraw his or her consent at any time.

Withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal, Article 7(3) Sentence 2 GDPR. It shall be as easy to withdraw as to give consent, Art. 7(3) Sentence 4 GDPR. Therefore, the withdrawal of consent can always take place in the same way as consent has been given or in any other way, that is considered by the data subject to be simpler. In todays information society, probably the simplest way to withdraw consent is a simple email. If the data subject wishes to withdraw his or her consent granted to us, a simple email to us is sufficient. Alternatively, the data subject may choose any other way to communicate his or her withdraw of consent to us.


© All rights reserved by Heiko Maniero.

## K. Right to lodge a complaint with a supervisory authority (Article 14(2) lit. e, 77(1) GDPR)

As the controller, we are obliged to notify the data subject of the right to lodge a complaint with a supervisory authority, Article 14(2) lit. e GDPR. The right to lodge a complaint with a supervisory authority is regulated by Article 77(1) GDPR. According to this provision, without prejudice to any other administrative or judicial remedy, every data subject shall have the right to lodge a complaint with a supervisory authority, in particular in the Member State of his or her habitual residence, place of work or place of the alleged infringement if the data subject considers that the processing of personal data relating to him or her infringes the General Data Protection Regulation. The right to lodge a complaint with a supervisory authority was only limited by the law of the Union in such way, that it can only be exercised before a single supervisory authority (Recital 141 Sentence 1 GDPR). This rule is intended to avoid double complaints of the same data subject in the same matter. If a data subject wants to lodge a complaint about us, we therefore asked to contact only a single supervisory authority.

## L. Source the personal data originate, and if applicable, whether it came from publicly accessible sources (Article 14(2) lit. f GDPR)

In principle, personal data is collected directly from the data subject or in cooperation with an authority (e.g. retrieval of data from an official register). Other data on data subjects are derived from transfers of group companies. In the context of this general information, the naming of the exact sources from which personal data is originated is either impossible or would involve a disproportionate effort within the meaning of Art. 14(5) lit. b GDPR. In principle, we do not collect personal data from publicly accessible sources.

Any data subject can contact us at any time to obtain more detailed information about the exact sources of the personal data concerning him or her. Where the origin of the personal data cannot be provided to the data subject because various sources have been used, general information should be provided (Recital 61 Sentence 4 GDPR).

## M. Existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) GDPR and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject (Article 14(2) lit. g GDPR)

As a responsible company, usually we do not use automated decision-making or profiling. If, in exceptional cases, we carry out automated decision-making or profiling, we will inform the data subject


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

either separately or via a sub-section in our privacy policy (on our website). In this case, the following applies:

Automated decision-making - including profiling - may occur if (1) this is necessary for entering into, or performance of, a contract between the data subject and us, or (2) this is authorised by Union or Member State law to which we are subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or (3) this is based on the data subject's explicit consent.

In the cases referred to in Article 22(2) (a) and (c) GDPR, we shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests. In these cases, you have the right to obtain human intervention on the part of the controller, to express your point of view and to contest the decision.

Meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject is set out in our privacy policy.

## III. EU-U.S. Data Privacy Framework (EU-U.S. DPF), UK Extension to the EU-U.S. DPF, Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF)

If our organisation is a certified member of the EU-U.S. Data Privacy Framework (EU-U.S. DPF) and/or the UK Extension to the EU-U.S. DPF and/or the Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF), the following applies:

We comply with the EU-U.S. Data Privacy Framework (EU-U.S. DPF) and the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF) as set forth by the U.S. Department of Commerce. Our organization has certified to the U.S. Department of Commerce that it adheres to the EU-U.S. Data Privacy Framework Principles (EU-U.S. DPF Principles) with regard to the processing of personal data received from the European Union and the United Kingdom in reliance on the EU-U.S. DPF and the UK Extension to the EU-U.S. DPF. Our organization has certified to the U.S. Department of Commerce that it adheres to the Swiss-U.S. Data Privacy Framework Principles (Swiss-U.S. DPF Principles) with regard to the processing of personal data received from Switzerland in reliance on the Swiss-U.S. DPF. If there is any conflict between the terms in our privacy policy and the EU-U.S. DPF Principles and/or the Swiss-U.S. DPF Principles, the Principles shall govern.

To learn more about the Data Privacy Framework (DPF) program, and to view our certification, please visit https://www.dataprivacyframework.gov/.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

The other U.S. entities or U.S. subsidiaries of our organization that are also adhering to the EU-U.S. DPF Principles, including as applicable under the UK Extension to the EU-U.S. DPF, and Swiss-U.S. DPF Principles and that are covered, if any, are named in our privacy policy.

In compliance with the EU-U.S. DPF and the UK Extension to the EU-U.S. DPF and the Swiss-U.S. DPF, our organization commits to cooperate and comply respectively with the advice of the panel established by the EU data protection authorities (DPAs) and the UK Information Commissioner's Office (ICO) and the Swiss Federal Data Protection and Information Commissioner (FDPIC) with regard to unresolved complaints concerning our handling of personal data received in reliance on the EU-U.S. DPF and the UK Extension to the EU-U.S. DPF and the Swiss-U.S. DPF.

We inform data subjects about the relevant European Data Protection Authorities designated to address complaints concerning our organization's handling of personal data in the top of this Transparency Document and that we provide appropriate recourse free of charge to the affected individual.

We inform all data subjects that our organization is subject to the investigatory and enforcement powers of the Federal Trade Commission (FTC).

Data subjects have the possibility, under certain conditions, to invoke binding arbitration. Our organisation is obligated to arbitrate claims and follow the terms as set forth in Annex I of the DPF Principles, provided that the data subject has invoked binding arbitration by delivering notice to our organization and following the procedures and subject to conditions set forth in Annex I of Principles.

We hereby inform all data subjects about our organization's liability in cases of onward transfers to third parties.

For any questions by data subjects or Data Protection Supervisory Authorities we designated the local representatives mentioned in the top of this Transparency Document.

We offer you the opportunity to choose (opt out) whether your personal information is (i) to be disclosed to a third party or (ii) to be used for a purpose that is materially different from the purpose(s) for which it was originally collected or subsequently authorized by you. The clear, conspicuous, and readily available mechanism to exercise your choice is to contact our Data Protection Officer (DPO) by email. We do not provide choice or are obliged to when disclosure is made to a third party that is acting as an agent or processor to perform tasks on behalf of us and under the instructions of us. However, we always enter into a contract with such agent or processor.

For sensitive information (i.e., personal information specifying medical or health conditions, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership or information specifying the sex life of the individual), we obtain your affirmative express consent (opt in) if such information is to be (i) disclosed to a third party or (ii) used for a purpose other than those for which it was originally collected or subsequently authorized by you through your exercise of opt-in choice. In addition, we treat as sensitive any personal information received from a third party where the third party identifies and treats it as sensitive.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

We hereby inform you about the requirement to disclose personal information in response to lawful requests by public authorities, including to meet national security or law enforcement requirements.

To transfer personal information to a third party acting as a controller, we comply with the Notice and Choice Principles. We also enter into a contract with the third-party controller that provides that such data may only be processed for limited and specified purposes consistent with the consent provided by you and that the recipient will provide the same level of protection as the DPF Principles and will notify us if it makes a determination that it can no longer meet this obligation. The contract provides that when such a determination is made the third party controller ceases processing or takes other reasonable and appropriate steps to remediate.

To transfer personal data to a third party acting as an agent or processor, we (i) transfer such data only for limited and specified purposes; (ii) ascertain that the agent or processor is obligated to provide at least the same level of privacy protection as is required by the DPF Principles; (iii) take reasonable and appropriate steps to ensure that the agent or processor effectively processes the personal information transferred in a manner consistent with our obligations under the DPF Principles; (iv) require the agent or processor to notify the organization if it makes a determination that it can no longer meet its obligation to provide the same level of protection as is required by the DPF Principles; (v) upon notice, including under (iv), take reasonable and appropriate steps to stop and remediate unauthorized processing; and (vi) provide a summary or a representative copy of the relevant privacy provisions of its contract with that agent to the DPF Department upon request.

In compliance with the EU-U.S. DPF and/or the UK Extension to the EU-U.S. DPF and/or the Swiss-U.S. DPF, our organisation commits to cooperate and comply respectively with the advice of the panel established by the EU data protection authorities (DPAs) and the UK Information Commissioner's Office (ICO) and the Swiss Federal Data Protection and Information Commissioner (FDPIC) with regard to unresolved complaints concerning our handling of human resources data received in reliance on the EU-U.S. DPF and the UK Extension to the EU-U.S. DPF and the Swiss-U.S. DPF in the context of the employment relationship.

All data subjects who are temporarily in the European Union (EU), the European Economic Area (EEA) or the United Kingdom, or who have their domicile or habitual residence there, are entitled to the rights and data subject rights which are published in our Transparency Document, which also arise from Articles 15 to 22 GDPR, including the right to access personal data. We have made this information available in all EU and EEA languages. The English language version applies to the United Kingdom.

All data subjects who are temporarily resident in Switzerland or have their domicile or habitual residence there are entitled to the rights and data subject rights under the Swiss Data Protection Act (DPA) and the Swiss Data Protection Regulation (DPR) which are published in our Transparency Document, including the right to access personal data. We have provided this information in the three official languages of Switzerland (German, Italian and French).


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

© All rights reserved by Heiko Maniero.

# ENGLISH: Information about the Processing of Personal Data for Employees and Applicants (Article 13, 14 GDPR)

Dear Sir or Madam,

Personal data of employees and applicants deserves special protection. Our goal is to keep our data protection level to a high standard. Therefore, we are routinely developing our data protection and data security concepts.

Of course, we comply with the statutory provisions on data protection. According to Article 13, 14 GDPR, controllers meet specific information requirements when processing personal data. This document fulfills these obligations.

The terminology of legal regulation is complicated. Unfortunately, the use of legal terms could not be dispensed with in the preparation of this document. Therefore, we would like to point out that you are always welcome to contact us for all questions concerning this document, the terms used or formulations.

## I. Compliance with the information requirements when personal data is collected from the data subject (Article 13 GDPR)

### A. Identity and the contact details of the controller (Article 13(1) lit. a GDPR)

See above

### B. Contact details of the Data Protection Officer (Article 13(1) lit. b GDPR)

See above

### C. Purposes of the processing for which the personal data are intended as well as the legal basis for the processing (Article 13(1) lit. c GDPR)

For applicant's data, the purpose of data processing is to conduct an examination of the application during the recruitment process. For this purpose, we process all data provided by you. Based on the data submitted during the recruitment process, we will check whether you are invited to a job interview (part of the selection process). In case of generally suitable candidates, in particular in the context of the job interview, we process certain other personal data provided by you, which is essential for our selection decision. If you are hired by us, applicant's data will automatically change into employee data. As part of the recruitment process, we will process other personal data about you that we request from you and that


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

is required to initiate or fulfill your contract (such as personal identification numbers or tax numbers). For employee data, the purpose of data processing is the performance of the employment contract or compliance with other legal provisions applicable to the employment relationship (e.g. tax law) as well as the use of your personal data to carry out the employment contract concluded with you (e.g. publication of your name and the contact information within the company or to customers). Employee data is stored after termination of the employment relationship to fulfill legal retention periods.

The legal basis for data processing is Article 6(1) lit. b GDPR, Article 9(2) lit. b and h GDPR, Article 88 (1) GDPR and national legislation, such as for Germany Section 26 BDSG (Federal Data Protection Act).

## D. Categories of recipients of the personal data (Article 13(1) lit. e GDPR)

Public authorities

External bodies

Further external bodies

Internal processing

Intragroup processing

Other bodies

A list of our processors and data recipients in third countries and, if applicable, international organizations is either published on our website or can be requested from us free of charge. Please contact our data protection officer to request this list.

## E. Recipients in a third country and appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available (Article 13(1) lit. f, 46(1), 46 (2) lit. c GDPR)

All companies and branches that are part of our group (hereinafter referred to as "group companies") that have their place of business or an office in a third country may belong to the recipients of personal data. A list of all group companies or recipients can be requested from us.

According to Article 46(1) GDPR a controller or processor may transfer personal data only to a third country if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available. Appropriate safeguards may be provided without requiring any specific authorisation from a supervisory authority by means of standard contractual clauses, Article 46(2) lit. c GDPR.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

The standard contractual clauses of the European Union or other appropriate safeguards are agreed on with all recipients from third countries before the first transmission of personal data. Consequently, it is ensured that appropriate safeguards, enforceable data subject rights and effective legal remedies for data subjects are guaranteed. Every data subject can obtain a copy of the standard contractual clauses from us. The standard contractual clauses are also available in the Official Journal of the European Union.

Article 45(3) of the General Data Protection Regulation (GDPR) grants the European Commission the power to decide, by means of an implementing act, that a non-EU country ensures an adequate level of protection. This means a level of protection for personal data that is essentially equivalent to the level of protection within the EU. The effect of adequacy decisions is that personal data can flow freely from the EU (and Norway, Liechtenstein and Iceland) to a third country without further obstacles. Similar rules exist for the United Kingdom, Switzerland and some other Countries.

Where the European Commission or the goverment of another country decided that a third country ensures an adequate level of protection, and a valid Framework is in place (e.g, EU-U.S. Data Privacy Framework, Swiss-U.S. Data Privacy Framework, UK Extension to the EU-U.S. Data Privacy Framework), all transfers by us to the members of such frameworks (e.g. self certified entities) are exclusively based on that entities membership in the respective framework. Where we or one of our group entitities is a member of such framework, all transfers to us or our group entity are exclusively based on the entities membership in such framework.

Any data subject can obtain a copy of the frameworks from us. In addition, the frameworks are also available in the Official Journal of the European Union or in the published legal materials or on the websites of supervisory authorities or other competent authorities or institutions.

## F. Period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period (Article 13(2) lit. a GDPR)

The duration of storage of personal data of applicants is 6 months. For employee data the respective statutory retention period applies. After expiration of that period, the corresponding data is routinely deleted, as long as it is no longer necessary for the fulfillment of the contract or the initiation of a contract.

## G. Existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability (Article 13(2) lit. b GDPR)

All data subjects have the following rights:

***Right to access***

Each data subject has a right to access the personal data concerning him or her. The right to access extends to all data processed by us. The right can be exercised easily and at reasonable intervals, in


© All rights reserved by Heiko Maniero.

order to be aware of, and verify, the lawfulness of the processing (Recital 63 GDPR). This right results from Art. 15 GDPR. The data subject may contact us to exercise the right to access.

***Right to rectification***

According to Article 16 Sentence 1 GDPR the data subject has the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. Moreover, Article 16 Sentence 2 GDPR provides that the data subject is entitled, taking into account the purposes of the processing, to have incomplete personal data completed, including by means of providing a supplementary statement. The data subject may contact us to exercise the right of rectification.

***Right to erasure (right to be forgotten)***

In addition, data subjects are entitled to a right to erasure and to be forgotten under Art. 17 GDPR. This right can also be exercised by contacting us. At this point, however, we would like to point out that this right does not apply insofar as the processing is necessary to fulfill a legal obligation to which our company is subject to, Article 17(3) lit. b GDPR. This means that we can approve an application to erase only after the expiration of the statutory retention period.

***Right to restriction of processing***

According to Article 18 GDPR any data subject is entitled to a restriction of processing. The restriction of processing may be demanded if one of the conditions set out in Article 18(1) lit. a-d GDPR is fulfilled. The data subject may contact us to exercise the right to restriction of processing.

***Right to object***

Furthermore, Art. 21 GDPR guarantees the right to object. The data subject may contact us to exercise the right to object.

***Right to data portability***

Art. 20 GDPR grants the data subject the right to data portability. Under this provision, the data subject has under the conditions laid down in Article 20(1) lit. a and b GDPR the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided. The data subject may contact us to exercise the right to data portability.

## H. The existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal, where the processing is based on Article 6(1) lit. a GDPR or Article 9(2) lit. a GDPR (Article 13(2) lit. c GDPR)

If processing of personal data is based on Art. 6(1) lit. a GDPR, which is the case, if the data subject has given consent to the processing of personal data for one or more specific purposes or is it based on Article 9(2) lit. a GDPR, which regulates the explicit consent to the processing of special categories of


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

personal data, the data subject has according to Article 7(3) Sentence 1 GDPR the right to withdraw his or her consent at any time.

Withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal, Article 7(3) Sentence 2 GDPR. It shall be as easy to withdraw as to give consent, Art. 7(3) Sentence 4 GDPR. Therefore, the withdrawal of consent can always take place in the same way as consent has been given or in any other way, that is considered by the data subject to be simpler. In today's information society, probably the simplest way to withdraw consent is a simple email. If the data subject wishes to withdraw his or her consent granted to us, a simple email to us is sufficient. Alternatively, the data subject may choose any other way to communicate his or her withdraw of consent to us.

## I. Right to lodge a complaint with a supervisory authority (Article 13(2) lit. d, 77(1) GDPR)

As the controller, we are obliged to notify the data subject of the right to lodge a complaint with a supervisory authority, Article 13(2) lit. d GDPR. The right to lodge a complaint with a supervisory authority is regulated by Article 77(1) GDPR. According to this provision, without prejudice to any other administrative or judicial remedy, every data subject shall have the right to lodge a complaint with a supervisory authority, in particular in the Member State of his or her habitual residence, place of work or place of the alleged infringement if the data subject considers that the processing of personal data relating to him or her infringes the General Data Protection Regulation. The right to lodge a complaint with a supervisory authority was only limited by the law of the Union in such way, that it can only be exercised before a single supervisory authority (Recital 141 Sentence 1 GDPR). This rule is intended to avoid double complaints of the same data subject in the same matter. If a data subject wants to lodge a complaint about us, we therefore asked to contact only a single supervisory authority.

## J. Provision of personal data as statutory or contractual requirement; Requirement necessary to enter into a contract; Obligation of the data subject to provide the personal data; possible consequences of failure to provide such data (Art. 13(2) lit. e GDPR)

We clarify that the provision of personal data is partly required by law (e.g. tax regulations) or can also result from contractual provisions (e.g. information on the contractual partner).

Sometimes it may be necessary to conclude a contract that the data subject provides us with personal data, which must subsequently be processed by us. The data subject is, for example, obliged to provide us with personal data when our company signs a contract with him or her. The non-provision of the personal data would have the consequence that the contract with the data subject could not be concluded.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

Before personal data is provided by the data subject, the data subject must contact us. We clarify to the data subject whether the provision of the personal data is required by law or contract or is necessary for the conclusion of the contract, whether there is an obligation to provide the personal data and the consequences of non-provision of the personal data.

### K. Existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) GDPR and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject (Article 13 (2) lit. f GDPR)

As a responsible company, usually we do not use automated decision-making or profiling. If, in exceptional cases, we carry out automated decision-making or profiling, we will inform the data subject either separately or via a sub-section in our privacy policy (on our website). In this case, the following applies:

Automated decision-making - including profiling - may occur if (1) this is necessary for entering into, or performance of, a contract between the data subject and us, or (2) this is authorised by Union or Member State law to which we are subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or (3) this is based on the data subject's explicit consent.

In the cases referred to in Article 22(2) (a) and (c) GDPR, we shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests. In these cases, you have the right to obtain human intervention on the part of the controller, to express your point of view and to contest the decision.

Meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject is set out in our privacy policy.

## II. Compliance with the information requirements when personal data is not collected from the data subject (Article 14 GDPR)

### A. Identity and the contact details of the controller (Article 14(1) lit. a GDPR)

See above

### B. Contact details of the Data Protection Officer (Article 14(1) lit. b GDPR)

See above


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## C. Purposes of the processing for which the personal data are intended as well as the legal basis for the processing (Article 14(1) lit. c GDPR)

For applicant's data not collected from the data subject, the purpose of data processing is to conduct an examination of the application during the recruitment process. For this purpose, we may process data not collected from you. Based on the data processed during the recruitment process, we will check whether you are invited to a job interview (part of the selection process). If you are hired by us, applicant's data will automatically convert into employee data. For employee data, the purpose of data processing is the performance of the employment contract or compliance with other legal provisions applicable to the employment relationship. Employee data is stored after termination of the employment relationship to fulfill legal retention periods.

The legal basis for data processing is Article 6(1) lit. b and f GDPR, Article 9(2) lit. b and h GDPR, Article 88 (1) GDPR and national legislation, such as for Germany Section 26 BDSG (Federal Data Protection Act).

## D. Categories of personal data concerned (Article 14(1) lit. d GDPR)

Applicant's data

Employee data

## E. Categories of recipients of the personal data (Article 14(1) lit. e GDPR)

Public authorities

External bodies

Further external bodies

Internal processing

Intragroup processing

Other bodies

A list of our processors and data recipients in third countries and, if applicable, international organizations is either published on our website or can be requested from us free of charge. Please contact our data protection officer to request this list.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## F. Recipients in a third country and appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available (Article 14(1) lit. f, 46(1), 46(2) lit. c GDPR)

All companies and branches that are part of our group (hereinafter referred to as "group companies") that have their place of business or an office in a third country may belong to the recipients of personal data. A list of all group companies or recipients can be requested from us.

According to Article 46(1) GDPR a controller or processor may transfer personal data only to a third country if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available. Appropriate safeguards may be provided without requiring any specific authorisation from a supervisory authority by means of standard data protection clauses, Article 46(2) lit. c GDPR.

The standard contractual clauses of the European Union or other appropriate safeguards are agreed on with all recipients from third countries before the first transmission of personal data. Consequently, it is ensured that appropriate safeguards, enforceable data subject rights and effective legal remedies for data subjects are guaranteed. Every data subject can obtain a copy of the standard contractual clauses from us. The standard contractual clauses are also available in the Official Journal of the European Union.

Article 45(3) of the General Data Protection Regulation (GDPR) grants the European Commission the power to decide, by means of an implementing act, that a non-EU country ensures an adequate level of protection. This means a level of protection for personal data that is essentially equivalent to the level of protection within the EU. The effect of adequacy decisions is that personal data can flow freely from the EU (and Norway, Liechtenstein and Iceland) to a third country without further obstacles. Similar rules exist for the United Kingdom, Switzerland and some other Countries.

Where the European Commission or the goverment of another country decided that a third country ensures an adequate level of protection, and a valid Framework is in place (e.g, EU-U.S. Data Privacy Framework, Swiss-U.S. Data Privacy Framework, UK Extension to the EU-U.S. Data Privacy Framework), all transfers by us to the members of such frameworks (e.g. self certified entities) are exclusively based on that entities membership in the respective framework. Where we or one of our group entitities is a member of such framework, all transfers to us or our group entity are exclusively based on the entities membership in such framework.

Any data subject can obtain a copy of the frameworks from us. In addition, the frameworks are also available in the Official Journal of the European Union or in the published legal materials or on the websites of supervisory authorities or other competent authorities or institutions.


© All rights reserved by Heiko Maniero.

## G. Period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period (Article 14(2) lit. a GDPR)

The duration of storage of personal data of applicants is 6 months. For employee data the respective statutory retention period applies. After expiration of that period, the corresponding data is routinely deleted, as long as it is no longer necessary for the fulfillment of the contract or the initiation of a contract.

## H. Notification of the legitimate interests pursued by the controller or by a third party if the processing is based on Article 6(1) lit. f GDPR (Art. 14(2) lit. b GDPR)

According to Article 6(1) lit. f GDPR, processing shall be lawful only if the processing is necessary for the purposes of legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data. According to Recital 47 Sentence 2 GDPR a legitimate interest could exist where there is a relevant and appropriate relationship between the data subject and the controller, e.g. in situations where the data subject is a client of the controller. In all cases in which our company processes applicant's data based on Article 6(1) lit. f GDPR, our legitimate interest is the employment of suitable personnel and professionals.

## I. Existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject and to object to processing as well as the right to data portability (Article 14(2) lit. c GDPR)

All data subjects have the following rights:

***Right to access***

Each data subject has a right to access the personal data concerning him or her. The right to access extends to all data processed by us. The right can be exercised easily and at reasonable intervals, in order to be aware of, and verify, the lawfulness of the processing (Recital 63 GDPR). This right results from Art. 15 GDPR. The data subject may contact us to exercise the right to access.

***Right to rectification***

According to Article 16 Sentence 1 GDPR the data subject has the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. Moreover, Article 16 Sentence 2 GDPR provides that the data subject is entitled, taking into account the purposes of the processing, to have incomplete personal data completed, including by means of providing a supplementary statement. The data subject may contact us to exercise the right of rectification.

***Right to erasure (right to be forgotten)***

In addition, data subjects are entitled to a right to erasure and to be forgotten under Art. 17 GDPR. This right can also be exercised by contacting us. At this point, however, we would like to point out that this


© All rights reserved by Heiko Maniero.

right does not apply insofar as the processing is necessary to fulfill a legal obligation to which our company is subject to, Article 17(3) lit. b GDPR. This means that we can approve an application to erase only after the expiration of the statutory retention period.

***Right to restriction of processing***

According to Article 18 GDPR any data subject is entitled to restriction of processing. The restriction of processing may be demanded if one of the conditions set out in Article 18(1) lit. a-d GDPR is fulfilled. The data subject may contact us to exercise the right to restriction of processing.

***Right to object***

Furthermore, Art. 21 GDPR guarantees the right to object. The data subject may contact us to exercise the right to object.

***Right to data portability***

Art. 20 GDPR grants the data subject the right to data portability. According to this provision the data subject has under the conditions laid down in Article 20(1) lit. a and b GDPR the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided. The data subject may contact us to exercise the right to data portability.

## J. The existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal, where the processing is based on Article 6(1) lit. a or Article 9(2) lit. a GDPR (Art. 14(2) lit. d GDPR)

If processing of personal data is based on Art. 6(1) lit. a GDPR, which is the case, if the data subject has given consent to the processing of personal data for one or more specific purposes or is it based on Article 9(2) lit. a GDPR, which regulates the explicit consent to the processing of special categories of personal data, the data subject has according to Article 7(3) Sentence 1 GDPR the right to withdraw his or her consent at any time.

Withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal, Article 7(3) Sentence 2 GDPR. It shall be as easy to withdraw as to give consent, Art. 7(3) Sentence 4 GDPR. Therefore, the withdrawal of consent can always take place in the same way as consent has been given or in any other way, that is considered by the data subject to be simpler. In today's information society, probably the simplest way to withdraw consent is a simple email. If the data subject wishes to withdraw his or her consent granted to us, a simple email to us is sufficient. Alternatively, the data subject may choose any other way to communicate his or her withdraw of consent to us.


© All rights reserved by Heiko Maniero.

## K. Right to lodge a complaint with a supervisory authority (Article 14(2) lit. e, 77(1) GDPR)

As the controller, we are obliged to notify the data subject of the right to lodge a complaint with a supervisory authority, Article 14(2) lit. e GDPR. The right to lodge a complaint with a supervisory authority is regulated by Article 77(1) GDPR. According to this provision, without prejudice to any other administrative or judicial remedy, every data subject shall have the right to lodge a complaint with a supervisory authority, in particular in the Member State of his or her habitual residence, place of work or place of the alleged infringement if the data subject considers that the processing of personal data relating to him or her infringes the General Data Protection Regulation. The right to lodge a complaint with a supervisory authority was only limited by the law of the Union in such way, that it can only be exercised before a single supervisory authority (Recital 141 Sentence 1 GDPR). This rule is intended to avoid double complaints of the same data subject in the same matter. If a data subject wants to lodge a complaint about us, we therefore asked to contact only a single supervisory authority.

## L. Source the personal data originate, and if applicable, whether it came from publicly accessible sources (Article 14(2) lit. f GDPR)

In principle, personal data is collected directly from the data subject or in cooperation with an authority (e.g. retrieval of data from an official register). Other data on data subjects are derived from transfers of group companies. In the context of this general information, the naming of the exact sources from which personal data is originated is either impossible or would involve a disproportionate effort within the meaning of Art. 14(5) lit. b GDPR. In principle, we do not collect personal data from publicly accessible sources.

Any data subject can contact us at any time to obtain more detailed information about the exact sources of the personal data concerning him or her. Where the origin of the personal data cannot be provided to the data subject because various sources have been used, general information should be provided (Recital 61 Sentence 4 GDPR).

## M. Existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) GDPR and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject (Article 14(2) lit. g GDPR)

As a responsible company, usually we do not use automated decision-making or profiling. If, in exceptional cases, we carry out automated decision-making or profiling, we will inform the data subject either separately or via a sub-section in our privacy policy (on our website). In this case, the following applies:


© All rights reserved by Heiko Maniero.

Automated decision-making - including profiling - may occur if (1) this is necessary for entering into, or performance of, a contract between the data subject and us, or (2) this is authorised by Union or Member State law to which we are subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or (3) this is based on the data subject's explicit consent.

In the cases referred to in Article 22(2) (a) and (c) GDPR, we shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests. In these cases, you have the right to obtain human intervention on the part of the controller, to express your point of view and to contest the decision.

Meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject is set out in our privacy policy.

## III. EU-U.S. Data Privacy Framework (EU-U.S. DPF), UK Extension to the EU-U.S. DPF, Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF)

If our organisation is a certified member of the EU-U.S. Data Privacy Framework (EU-U.S. DPF) and/or the UK Extension to the EU-U.S. DPF and/or the Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF), the following applies:

We comply with the EU-U.S. Data Privacy Framework (EU-U.S. DPF) and the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF) as set forth by the U.S. Department of Commerce. Our organization has certified to the U.S. Department of Commerce that it adheres to the EU-U.S. Data Privacy Framework Principles (EU-U.S. DPF Principles) with regard to the processing of personal data received from the European Union and the United Kingdom in reliance on the EU-U.S. DPF and the UK Extension to the EU-U.S. DPF. Our organization has certified to the U.S. Department of Commerce that it adheres to the Swiss-U.S. Data Privacy Framework Principles (Swiss-U.S. DPF Principles) with regard to the processing of personal data received from Switzerland in reliance on the Swiss-U.S. DPF. If there is any conflict between the terms in our privacy policy and the EU-U.S. DPF Principles and/or the Swiss-U.S. DPF Principles, the Principles shall govern.

To learn more about the Data Privacy Framework (DPF) program, and to view our certification, please visit https://www.dataprivacyframework.gov/.

The other U.S. entities or U.S. subsidiaries of our organization that are also adhering to the EU-U.S. DPF Principles, including as applicable under the UK Extension to the EU-U.S. DPF, and Swiss-U.S. DPF Principles and that are covered, if any, are named in our privacy policy.


© All rights reserved by Heiko Maniero.

In compliance with the EU-U.S. DPF and the UK Extension to the EU-U.S. DPF and the Swiss-U.S. DPF, our organization commits to cooperate and comply respectively with the advice of the panel established by the EU data protection authorities (DPAs) and the UK Information Commissioner's Office (ICO) and the Swiss Federal Data Protection and Information Commissioner (FDPIC) with regard to unresolved complaints concerning our handling of personal data received in reliance on the EU-U.S. DPF and the UK Extension to the EU-U.S. DPF and the Swiss-U.S. DPF.

We inform data subjects about the relevant European Data Protection Authorities designated to address complaints concerning our organization's handling of personal data in the top of this Transparency Document and that we provide appropriate recourse free of charge to the affected individual.

We inform all data subjects that our organization is subject to the investigatory and enforcement powers of the Federal Trade Commission (FTC).

Data subjects have the possibility, under certain conditions, to invoke binding arbitration. Our organisation is obligated to arbitrate claims and follow the terms as set forth in Annex I of the DPF Principles, provided that the data subject has invoked binding arbitration by delivering notice to our organization and following the procedures and subject to conditions set forth in Annex I of Principles.

We hereby inform all data subjects about our organization's liability in cases of onward transfers to third parties.

For any questions by data subjects or Data Protection Supervisory Authorities we designated the local representatives mentioned in the top of this Transparency Document.

We offer you the opportunity to choose (opt out) whether your personal information is (i) to be disclosed to a third party or (ii) to be used for a purpose that is materially different from the purpose(s) for which it was originally collected or subsequently authorized by you. The clear, conspicuous, and readily available mechanism to exercise your choice is to contact our Data Protection Officer (DPO) by email. We do not provide choice or are obliged to when disclosure is made to a third party that is acting as an agent or processor to perform tasks on behalf of us and under the instructions of us. However, we always enter into a contract with such agent or processor.

For sensitive information (i.e., personal information specifying medical or health conditions, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership or information specifying the sex life of the individual), we obtain your affirmative express consent (opt in) if such information is to be (i) disclosed to a third party or (ii) used for a purpose other than those for which it was originally collected or subsequently authorized by you through your exercise of opt-in choice. In addition, we treat as sensitive any personal information received from a third party where the third party identifies and treats it as sensitive.

We hereby inform you about the requirement to disclose personal information in response to lawful requests by public authorities, including to meet national security or law enforcement requirements.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

To transfer personal information to a third party acting as a controller, we comply with the Notice and Choice Principles. We also enter into a contract with the third-party controller that provides that such data may only be processed for limited and specified purposes consistent with the consent provided by you and that the recipient will provide the same level of protection as the DPF Principles and will notify us if it makes a determination that it can no longer meet this obligation. The contract provides that when such a determination is made the third party controller ceases processing or takes other reasonable and appropriate steps to remediate.

To transfer personal data to a third party acting as an agent or processor, we (i) transfer such data only for limited and specified purposes; (ii) ascertain that the agent or processor is obligated to provide at least the same level of privacy protection as is required by the DPF Principles; (iii) take reasonable and appropriate steps to ensure that the agent or processor effectively processes the personal information transferred in a manner consistent with our obligations under the DPF Principles; (iv) require the agent or processor to notify the organization if it makes a determination that it can no longer meet its obligation to provide the same level of protection as is required by the DPF Principles; (v) upon notice, including under (iv), take reasonable and appropriate steps to stop and remediate unauthorized processing; and (vi) provide a summary or a representative copy of the relevant privacy provisions of its contract with that agent to the DPF Department upon request.

In compliance with the EU-U.S. DPF and/or the UK Extension to the EU-U.S. DPF and/or the Swiss-U.S. DPF, our organisation commits to cooperate and comply respectively with the advice of the panel established by the EU data protection authorities (DPAs) and the UK Information Commissioner's Office (ICO) and the Swiss Federal Data Protection and Information Commissioner (FDPIC) with regard to unresolved complaints concerning our handling of human resources data received in reliance on the EU-U.S. DPF and the UK Extension to the EU-U.S. DPF and the Swiss-U.S. DPF in the context of the employment relationship.

All data subjects who are temporarily in the European Union (EU), the European Economic Area (EEA) or the United Kingdom, or who have their domicile or habitual residence there, are entitled to the rights and data subject rights which are published in our Transparency Document, which also arise from Articles 15 to 22 GDPR, including the right to access personal data. We have made this information available in all EU and EEA languages. The English language version applies to the United Kingdom.

All data subjects who are temporarily resident in Switzerland or have their domicile or habitual residence there are entitled to the rights and data subject rights under the Swiss Data Protection Act (DPA) and the Swiss Data Protection Regulation (DPR) which are published in our Transparency Document, including the right to access personal data. We have provided this information in the three official languages of Switzerland (German, Italian and French).


© All rights reserved by Heiko Maniero.

# SPANISH: Información sobre el tratamiento de datos personales (Artículos 13, 14 RGPD)

Estimado señor o señora:

Los datos personales de toda persona que se encuentre en una relación contractual, precontractual o de otro tipo con nuestra empresa merecen una protección especial. Nuestro objetivo es mantener nuestro nivel de protección de datos a un alto nivel. Por lo tanto, estamos desarrollando rutinariamente nuestros conceptos de protección y seguridad de datos.

Por supuesto, cumplimos con las disposiciones legales sobre protección de datos. De acuerdo con los artículos 13 y 14 del RGPD, las empresas cumplen requisitos específicos de información al recoger datos personales. Este documento cumple con estas obligaciones.

La terminología de las normas legales es complicada. Desafortunadamente, no se pudo prescindir del uso de términos legales en la preparación de este documento. Por lo tanto, nos gustaría señalar que usted es siempre bienvenido a ponerse en contacto con nuestro delegado de protección de datos para todas las preguntas relativas a este documento, los términos utilizados o formulaciones.

## I. Cumplimiento de los requisitos de información cuando se recogen datos personales del interesado (artículo 13 del RGPD)

### A. Identidad y datos de contacto del responsable (artículo 13.1 lit. a RGPD)

Véase arriba

### B. Datos de contacto del delegado de protección de datos (artículo 13(1) lit. b RGPD)

Véase arriba

### C. Fines del tratamiento a que se destinan los datos personales y la base jurídica del tratamiento (artículo 13(1) lit. c RGPD)

La finalidad del tratamiento de datos personales es el tratamiento de todas las operaciones que afecten al responsable del tratamiento, a los clientes, a los posibles clientes, a los socios comerciales o a otras


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

relaciones contractuales o precontractuales entre los grupos mencionados (en el sentido más amplio) o a las obligaciones legales del responsable del tratamiento.

Art. 6(1) lit. a RGPD sirve como base legal para operaciones de tratamiento para las cuales obtenemos el consentimiento para un propósito específico de tratamiento. Si el tratamiento de datos personales es necesario para la ejecución de un contrato en el que el interesado es parte, como es el caso, por ejemplo, cuando las operaciones de tratamiento son necesarias para el suministro de bienes o para prestar cualquier otro servicio, el tratamiento se basa en el artículo 6(1) lit. b RGPD. Lo mismo se aplica a los tratamientos necesarios para la realización de medidas precontractuales, por ejemplo, en el caso de consultas sobre nuestros productos o servicios. Nuestra empresa está sujeta a una obligación legal por la que se requiere el tratamiento de datos personales, como por ejemplo para el cumplimiento de obligaciones fiscales, el tratamiento se basa en el Art. 6(1) lit. c RGPD.

En raras ocasiones, el tratamiento de datos personales puede ser necesario para proteger los intereses vitales del interesado o de otra persona física. Este sería el caso, por ejemplo, si un visitante sufriera una lesión en nuestra empresa y su nombre, edad, datos del seguro médico u otra información vital tuviera que ser transmitida a un médico, hospital u otro tercero. Entonces el tratamiento se basaría en el Art. 6(1) lit. d RGPD.

Cuando el tratamiento sea necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento, la base jurídica es el art. 6(1) lit. e RGPD.

Por último, las operaciones de tratamiento podrían basarse en el artículo 6(1) lit. f del RGPD. Este fundamento jurídico se utiliza para operaciones de tratamiento que no están cubiertas por ninguno de los fundamentos jurídicos antes mencionados, si el tratamiento es necesario para los fines de los intereses legítimos perseguidos por nuestra empresa o por un tercero, excepto cuando dichos intereses estén superados por los intereses o los derechos y libertades fundamentales del interesado que requieren la protección de los datos personales. Estos tratamientos son especialmente admisibles porque el legislador europeo los ha mencionado expresamente. Consideraba que se podía presumir un interés legítimo si el interesado era cliente del responsable del tratamiento (segunda frase del considerando 47 del RGPD).

## D. Cuando el tratamiento se base en el artículo 6, apartado 1, letra f), los intereses legítimos del responsable o de un tercero (artículo 13, apartado 1, letra d), del RGPD)

Cuando el tratamiento de datos personales se basa en el artículo 6(1) lit. f RGPD, nuestro interés legítimo es llevar a cabo nuestro negocio en favor del bienestar de todos nuestros empleados y accionistas.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## E. Categorías de destinatarios de los datos personales (artículo 13, apartado 1, lit. e RGPD)

Autoridades públicas

Organismos externos

Otros organismos externos

Tratamiento interno

Tratamiento dentro del grupo

Otros organismos

En nuestro sitio web se publica una lista de nuestros encargados del tratamiento y destinatarios de datos en terceros países y, en su caso, organizaciones internacionales, o bien puede solicitárnosla gratuitamente. Póngase en contacto con nuestro responsable de protección de datos para solicitar esta lista.

## F. Destinatarios en un tercer país y las garantías adecuadas o apropiadas y los medios para obtener una copia de estas o al hecho de que se hayan prestado (artículo 13, apartado 1, letra f), artículo 46, apartados 1 y 2, letra c), del RGPD)

Todas las empresas y sucursales que forman parte de nuestro grupo (en lo sucesivo denominadas "empresas del grupo") que tienen su sede o una oficina en un tercer país pueden pertenecer a los destinatarios de los datos personales.

De conformidad con el artículo 46, apartado 1, del Reglamento de protección de datos (RGPD), un responsable del tratamiento o un encargado del tratamiento sólo puede transferir datos personales a un tercer país si el responsable del tratamiento o el encargado del tratamiento ha ofrecido las garantías adecuadas, y a condición de que se disponga de derechos exigibles a los interesados de vías de recurso efectivas para los interesados. Se pueden proporcionar garantías apropiadas sin requerir ninguna autorización específica de una autoridad de control por medio de cláusulas contractuales estándar, artículo 46(2) lit. c RGPD.

Las cláusulas contractuales de la Unión Europea se acuerdan con todos los destinatarios de terceros países antes de la primera transmisión de datos personales. En consecuencia, se aseguran las garantías adecuadas, los derechos exigibles de los interesados los recursos legales efectivos para los interesados que se derivan de las cláusulas contractuales estándares de la UE. Todos los interesados pueden obtener una copia de las cláusulas contractuales tipo a través de nuestro delegado de protección de


© All rights reserved by Heiko Maniero.

datos. Las cláusulas contractuales tipo también están disponibles en el Diario Oficial de la Unión Europea.

El artículo 45, apartado 3, del Reglamento General de Protección de Datos (RGPD) otorga a la Comisión Europea la facultad de decidir, mediante un acto de ejecución, que un país no perteneciente a la UE garantiza un nivel de protección adecuado. Esto significa un nivel de protección de los datos personales esencialmente equivalente al nivel de protección dentro de la UE. El efecto de las decisiones de adecuación es que los datos personales pueden circular libremente desde la UE (y Noruega, Liechtenstein e Islandia) a un tercer país sin más obstáculos. Existen normas similares para el Reino Unido, Suiza y algunos otros países.

Cuando la Comisión Europea o el gobierno de otro país decida que un tercer país garantiza un nivel adecuado de protección y exista un marco válido (por ejemplo, EU-U.S. Data Privacy Framework, Swiss-U.S. Data Privacy Framework, UK Extension to the EU-U.S. Data Privacy Framework), todas las transferencias que realicemos a los miembros de dichos marcos (por ejemplo, entidades autocertificadas) se basarán exclusivamente en la pertenencia de dichas entidades al marco respectivo. Cuando nosotros o una de las entidades de nuestro grupo sea miembro de dicho marco, todas las transferencias a nosotros o a la entidad de nuestro grupo se basarán exclusivamente en la pertenencia de la entidad a dicho marco.

Cualquier interesado puede solicitarnos una copia de los marcos. Además, los marcos también están disponibles en el Diario Oficial de la Unión Europea o en los materiales jurídicos publicados o en los sitios web de las autoridades de control o de otras autoridades o instituciones competentes.

## G. Plazo durante el cual se conservarán los datos personales o, cuando no sea posible, los criterios utilizados para determinar este plazo (artículo 13(2) lit. a RGPD)

El criterio utilizado para determinar el plazo de portabilidad de los datos personales es el plazo de conservación legal respectivo. Una vez transcurrido dicho plazo, los datos correspondientes se borran de forma rutinaria, siempre que ya no sean necesarios para el cumplimiento del contrato o la iniciación de un contrato.

Si no existe un periodo de conservación legal, el criterio es el periodo de conservación contractual o interno.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## H. La existencia del derecho a solicitar al responsable del tratamiento el acceso a los datos personales relativos al interesado, y su rectificación o supresión, o la limitación de su tratamiento, o a oponerse al tratamiento, así como el derecho a la portabilidad de los datos (artículo 13, apartado 2, letra b), del RGPD)

Todos los interesados tienen los siguientes derechos:

***Derecho de acceso***

Cada interesado tiene derecho a acceder a los datos personales que le conciernen. El derecho de acceso se extiende a todos los datos procesados por nosotros. El derecho puede ejercerse fácilmente y a intervalos razonables para conocer y verificar la legalidad del tratamiento (considerando 63 del RGPD). Este derecho resulta del Art. 15 RGPD. El interesado puede ponerse en contacto con nuestro delegado de protección de datos para ejercer el derecho de acceso.

***Derecho a rectificación***

De conformidad con la primera frase del artículo 16 del RGPD, el interesado tiene derecho a obtener del responsable del tratamiento, sin demora injustificada, la rectificación de los datos personales inexactos que le conciernan. Además, la segunda frase del artículo 16 del RGPD establece que el interesado tiene derecho, teniendo en cuenta los fines del tratamiento, a que se completen los datos personales incompletos, incluso mediante una declaración complementaria. El interesado puede ponerse en contacto con nuestro delegado de protección de datos para ejercer el derecho de rectificación.

***Derecho a la supresión (derecho al olvido)***

Además, los interesados tienen derecho a ser borrados y olvidados en virtud del Art. 17 RGPD. Este derecho también puede ejercerse poniéndose en contacto con nuestro delegado de protección de datos. En este punto, sin embargo, nos gustaría señalar que este derecho no se aplica en la medida en que el tratamiento es necesario para cumplir con una obligación legal a la que nuestra empresa está sujeta, el artículo 17, apartado 3, letra b). RGPD. Esto significa que podemos aprobar una solicitud para borrar sólo después de la expiración del plazo de retención legal.

***Derecho a la limitación de tratamiento***

De conformidad con el artículo 18 del RGPD, todo interesado tiene derecho a una limitación de tratamiento. La limitación de tratamiento podrá exigirse si se cumple una de las condiciones establecidas en el artículo 18, apartado 1, letra a-d, del RGPD. El interesado puede ponerse en contacto con nuestro delegado de protección de datos para ejercer el derecho a la limitación de tratamiento.

***Derecho de oposición***

Además, el Art. 21 del RGPD garantiza el derecho a objetar. El interesado puede ponerse en contacto con nuestro delegado de protección de datos para ejercer el derecho de oposición.

***Derecho a la portabilidad de datos***

El Art. 20 del RGPD concede al interesado el derecho a la portabilidad de datos. En virtud de esta disposición, el interesado, en las condiciones establecidas en el artículo 20, apartado 1, letras a) y b),


© All rights reserved by Heiko Maniero.

del RGPD, tiene derecho a recibir los datos personales que le conciernan a él o ella, que él o ella haya facilitado a un responsable del tratamiento, en un formato estructurado, comúnmente utilizado y legible por máquinas, y tiene derecho a transmitirlos a otro responsable del tratamiento sin obstáculos por parte del responsable del tratamiento al que se hayan facilitado los datos personales. El interesado puede ponerse en contacto con nuestro delegado de protección de datos para ejercer el derecho a la portabilidad de datos.

## I. La existencia del derecho a retirar el consentimiento en cualquier momento, sin que ello afecte a la licitud del tratamiento basado en el consentimiento previo a su retirada, cuando el tratamiento esté basado en el artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a) (artículo 13, apartado 2, letra c), del RGPD)

Si el tratamiento de datos personales se basa en el Art. 6(1) lit. del RGPD, que es el caso, si el interesado ha dado su consentimiento al tratamiento de datos personales para uno o más fines específicos o si se basa en el artículo 9(2) lit. del RGPD, que regula el consentimiento explícito al tratamiento de categorías especiales de datos personales, el interesado tiene, de acuerdo con el artículo 7(3) frase 1 del RGPD, el derecho de retirar su consentimiento en cualquier momento.

La revocación del consentimiento no afectará a la legalidad del tratamiento basado en el consentimiento antes de su revocación, artículo 7(3) frase 2 RGPD. Se reserva el derecho de retirar su consentimiento, Art. 7(3) Sentencia 4 RGPD. Por lo tanto, la revocación del consentimiento siempre puede tener lugar de la misma forma en que se ha dado el consentimiento o de cualquier otra forma que el interesado considere más sencilla. En la sociedad de la información actual, probablemente la forma más sencilla de retirar el consentimiento es un simple correo electrónico. Si el interesado desea revocar el consentimiento que nos ha dado, basta con enviarle un simple correo electrónico a nuestro delegado de protección de datos. De forma alternativa, el interesado puede elegir cualquier otra forma de comunicarnos la revocación de su consentimiento.

## J. Derecho a presentar una reclamación ante una autoridad de control (letra d) del apartado 2 del artículo 13 y apartado 1 del artículo 77 del RGPD)

Como responsable del tratamiento, estamos obligados a notificar al interesado su derecho a presentar una reclamación ante una autoridad de control, artículo 13(2) lit. d RGPD El derecho a presentar una reclamación ante una autoridad de control está regulado por el artículo 77, apartado 1, del RGPD. Con arreglo a esta disposición, sin perjuicio de cualquier otro recurso administrativo o judicial, todo interesado tendrá derecho a presentar una reclamación ante una autoridad de control, en particular en el Estado miembro de su residencia habitual, lugar de trabajo o lugar de la supuesta infracción, si el interesado considera que el tratamiento de los datos personales que le conciernen infringe el Reglamento General de Protección de Datos. El derecho a presentar una reclamación ante una autoridad de control sólo


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

estaba limitado por la legislación de la Unión de tal manera que sólo puede ejercerse ante una única autoridad de control (primera frase del considerando 141 del RGPD). Esta norma tiene por objeto evitar la doble reclamación del mismo interesado en la misma materia. Si un interesado desea presentar una reclamación sobre nosotros, le pedimos que se ponga en contacto con una única autoridad de control.

## K. La comunicación de datos personales es un requisito legal o contractual, o un requisito necesario para suscribir un contrato, y si el interesado está obligado a facilitar los datos personales y está informado de las posibles consecuencias de que no facilitar tales datos (Art. 13(2) lit. e RGPD)

Aclaramos que el suministro de datos personales es requerido en parte por la ley (p.ej. regulaciones fiscales) o también puede resultar de disposiciones contractuales (p.ej. información sobre la parte contratante).

A veces puede ser necesario celebrar un contrato en el que el interesado nos proporciona datos personales, que deben ser procesados posteriormente por nosotros. Por ejemplo, el interesado está obligado a facilitarnos datos personales cuando nuestra empresa firma un contrato con él. La no comunicación de los datos personales tendría como consecuencia que no se pudiera celebrar el contrato con el interesado.

Antes de que el interesado facilite datos personales, el interesado deberá ponerse en contacto con nuestro delegado de protección de datos. Nuestro delegado de protección de datos aclara al interesado si el suministro de los datos personales es requerido por la ley o el contrato o si es necesario para la conclusión del contrato, si existe una obligación de proporcionar los datos personales y las consecuencias de la no entrega de los datos personales.

## L. La existencia de decisiones automatizadas, incluida la elaboración de perfiles, a que se refiere el artículo 22, apartados 1 y 4, y, al menos en tales casos, información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado (artículo 13, apartado 2, letra f), del RGPD)

Como empresa responsable, normalmente no utilizamos la toma de decisiones automatizada ni la elaboración de perfiles. Si, en casos excepcionales, llevamos a cabo la toma de decisiones automatizada o la elaboración de perfiles, informaremos al interesado por separado o a través de una subsección de nuestra política de privacidad (en nuestro sitio web). En este caso, se aplicará lo siguiente

La toma de decisiones automatizada -incluida la elaboración de perfiles- puede producirse si (1) es necesaria para celebrar o ejecutar un contrato entre el interesado y nosotros, o (2) está autorizada por


© All rights reserved by Heiko Maniero.

la legislación de la Unión o de los Estados miembros a la que estamos sujetos y que también establece medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado; o (3) se basa en el consentimiento explícito del interesado.

En los casos contemplados en el artículo 22, apartado 2, letras a) y c) del RGPD, aplicaremos las medidas adecuadas para salvaguardar los derechos y libertades e intereses legítimos del interesado. En estos casos, tiene derecho a obtener intervención humana por parte del responsable del tratamiento, a expresar su punto de vista y a impugnar la decisión.

En nuestra política de privacidad se ofrece información significativa sobre la lógica implicada, así como sobre la importancia y las consecuencias previstas de dicho tratamiento para el interesado.

## II. Cumplimiento de los requisitos de información cuando no se reciben datos personales del interesado (artículo 14 del RGPD)

### A. La identidad y los datos de contacto del responsable y, en su caso, de su representante (artículo 14.1 lit. a RGPD)

Véase arriba

### B. Datos de contacto del delegado de protección de datos, en su caso (artículo 14(1) lit. b RGPD)

Véase arriba

### C. Los fines del tratamiento a que se destinan los datos personales, así como la base jurídica del tratamiento (artículo 14(1) lit. c RGPD)

La finalidad del tratamiento de datos personales es el tratamiento de todas las operaciones que afecten al responsable del tratamiento, a los clientes, a los posibles clientes, a los socios comerciales o a otras relaciones contractuales o precontractuales entre los grupos mencionados (en el sentido más amplio) o a las obligaciones legales del responsable del tratamiento.

Si el tratamiento de datos personales es necesario para la ejecución de un contrato en el que el interesado es parte, como es el caso, por ejemplo, cuando las operaciones de tratamiento son necesarias para el suministro de bienes o para prestar cualquier otro servicio, el tratamiento se basa en el artículo 6(1) lit. b RGPD. Lo mismo se aplica a los tratamientos necesarios para la realización de medidas precontractuales, por ejemplo, en el caso de consultas sobre nuestros productos o servicios. Nuestra empresa está sujeta a una obligación legal por la que se requiere el tratamiento de datos


© All rights reserved by Heiko Maniero.

personales, como por ejemplo para el cumplimiento de obligaciones fiscales, el tratamiento se basa en el Art. 6(1) lit. c RGPD.

En raras ocasiones, el tratamiento de datos personales puede ser necesario para proteger los intereses vitales del interesado o de otra persona física. Este sería el caso, por ejemplo, si un visitante sufriera una lesión en nuestra empresa y su nombre, edad, datos del seguro médico u otra información vital tuviera que ser transmitida a un médico, hospital u otro tercero. Entonces el tratamiento se basaría en el Art. 6(1) lit. d RGPD.

Cuando el tratamiento sea necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento, la base jurídica es el art. 6(1) lit. e RGPD.

Por último, las operaciones de tratamiento podrían basarse en el artículo 6(1) lit. f del RGPD. Este fundamento jurídico se utiliza para operaciones de tratamiento que no están cubiertas por ninguno de los fundamentos jurídicos antes mencionados, si el tratamiento es necesario para los fines de los intereses legítimos perseguidos por nuestra empresa o por un tercero, excepto cuando dichos intereses estén superados por los intereses o los derechos y libertades fundamentales del interesado que requieren la protección de los datos personales. Estos tratamientos son especialmente admisibles porque el legislador europeo los ha mencionado expresamente. Consideraba que se podía presumir un interés legítimo si el interesado era cliente del responsable del tratamiento (segunda frase del considerando 47 del RGPD).

## D. Categorías de datos personales de que se trate (artículo 14, apartado 1, letra d), del RGPD)

Datos del cliente

Datos de clientes potenciales

Datos de los empleados

Datos de los proveedores

## E. Destinatarios o las categorías de destinatarios de los datos personales, en su caso (artículo 14.1 lit. e RGPD)

Autoridades públicas


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

Organismos externos

Otros organismos externos

Tratamiento interno

Tratamiento dentro del grupo

Otros organismos

En nuestro sitio web se publica una lista de nuestros encargados del tratamiento y destinatarios de datos en terceros países y, en su caso, organizaciones internacionales, o bien puede solicitárnosla gratuitamente. Póngase en contacto con nuestro responsable de protección de datos para solicitar esta lista.

## F. Destinatarios en un tercer país u organización internacional y las garantías adecuadas o apropiadas y a los medios para obtener una copia de ellas o al hecho de que se hayan prestado (artículo 14, apartado 1, letra f), artículo 46, apartados 1 y 2, letra c), del RGPD)

Todas las empresas y sucursales que forman parte de nuestro grupo (en lo sucesivo denominadas "empresas del grupo") que tienen su sede o una oficina en un tercer país pueden pertenecer a los destinatarios de los datos personales.

De conformidad con el artículo 46, apartado 1, del Reglamento de protección de datos (RGPD), un responsable del tratamiento o un encargado del tratamiento sólo puede transferir datos personales a un tercer país si el responsable del tratamiento o el encargado del tratamiento ha ofrecido las garantías adecuadas, y a condición de que se disponga de derechos exigibles a los interesados de vías de recurso efectivas para los interesados. Se pueden proporcionar garantías apropiadas sin requerir ninguna autorización específica de una autoridad de control por medio de cláusulas contractuales estándar, artículo 46(2) lit. c RGPD.

Las cláusulas contractuales de la Unión Europea se acuerdan con todos los destinatarios de terceros países antes de la primera transmisión de datos personales. En consecuencia, se aseguran las garantías adecuadas, los derechos exigibles de los interesados los recursos legales efectivos para los interesados que se derivan de las cláusulas contractuales estándares de la UE. Todos los interesados pueden obtener una copia de las cláusulas contractuales tipo a través de nuestro delegado de protección de datos. Las cláusulas contractuales tipo también están disponibles en el Diario Oficial de la Unión Europea.

El artículo 45, apartado 3, del Reglamento General de Protección de Datos (RGPD) otorga a la Comisión Europea la facultad de decidir, mediante un acto de ejecución, que un país no perteneciente a la UE garantiza un nivel de protección adecuado. Esto significa un nivel de protección de los datos personales


© All rights reserved by Heiko Maniero.

esencialmente equivalente al nivel de protección dentro de la UE. El efecto de las decisiones de adecuación es que los datos personales pueden circular libremente desde la UE (y Noruega, Liechtenstein e Islandia) a un tercer país sin más obstáculos. Existen normas similares para el Reino Unido, Suiza y algunos otros países.

Cuando la Comisión Europea o el gobierno de otro país decida que un tercer país garantiza un nivel adecuado de protección y exista un marco válido (por ejemplo, EU-U.S. Data Privacy Framework, Swiss-U.S. Data Privacy Framework, UK Extension to the EU-U.S. Data Privacy Framework), todas las transferencias que realicemos a los miembros de dichos marcos (por ejemplo, entidades autocertificadas) se basarán exclusivamente en la pertenencia de dichas entidades al marco respectivo. Cuando nosotros o una de las entidades de nuestro grupo sea miembro de dicho marco, todas las transferencias a nosotros o a la entidad de nuestro grupo se basarán exclusivamente en la pertenencia de la entidad a dicho marco.

Cualquier interesado puede solicitarnos una copia de los marcos. Además, los marcos también están disponibles en el Diario Oficial de la Unión Europea o en los materiales jurídicos publicados o en los sitios web de las autoridades de control o de otras autoridades o instituciones competentes.

## G. Plazo durante el cual se conservarán los datos personales o, cuando eso no sea posible, los criterios utilizados para determinar este plazo (artículo 14(2) lit. a RGPD)

El criterio utilizado para determinar el plazo de portabilidad de los datos personales es el plazo de conservación legal respectivo. Una vez transcurrido dicho plazo, los datos correspondientes se borran de forma rutinaria, siempre que ya no sean necesarios para el cumplimiento del contrato o la iniciación de un contrato.

Si no existe un periodo de conservación legal, el criterio es el periodo de conservación contractual o interno.

## H. Notificación de los intereses legítimos del responsable del tratamiento o de un tercero si el tratamiento se basa en el artículo 6, apartado 1, letra f), del RGPD (Art. 14(2) lit. b RGPD)

De conformidad con el artículo 6, apartado 1, letra f), del RGPD, el tratamiento sólo será lícito si el tratamiento es necesario para satisfacer intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, salvo cuando los intereses o los derechos y libertades fundamentales del interesado prevalezcan sobre los intereses o libertades fundamentales del interesado que requieran la protección de datos personales. Según la segunda frase del considerando 47 del RGPD, podría existir un interés legítimo cuando exista una relación pertinente y adecuada entre el interesado y el responsable del tratamiento, por ejemplo, en situaciones en las que el interesado sea cliente del responsable del


© All rights reserved by Heiko Maniero.

tratamiento. En todos los casos en los que nuestra empresa trata datos personales basados en el artículo 6(1) lit. f del RGPD, nuestro interés legítimo es llevar a cabo nuestro negocio a favor del bienestar de todos nuestros empleados y accionistas.

## I. La existencia del derecho a solicitar al responsable del tratamiento el acceso a los datos personales relativos al interesado, y su rectificación o supresión, o la limitación de su tratamiento, y a oponerse al tratamiento, así como el derecho a la portabilidad de los datos (artículo 14, apartado 2, letra c), del RGPD)

Todos los interesados tienen los siguientes derechos:

***Derecho de acceso***

Cada interesado tiene derecho a acceder a los datos personales que le conciernen. El derecho de acceso se extiende a todos los datos procesados por nosotros. El derecho puede ejercerse fácilmente y a intervalos razonables para conocer y verificar la legalidad del tratamiento (considerando 63 del RGPD). Este derecho resulta del Art. 15 RGPD. El interesado puede ponerse en contacto con nuestro delegado de protección de datos para ejercer el derecho de acceso.

***Derecho a rectificación***

De conformidad con la primera frase del artículo 16 del RGPD, el interesado tiene derecho a obtener del responsable del tratamiento, sin demora injustificada, la rectificación de los datos personales inexactos que le conciernan. Además, la segunda frase del artículo 16 del RGPD establece que el interesado tiene derecho, teniendo en cuenta los fines del tratamiento, a que se completen los datos personales incompletos, incluso mediante una declaración complementaria. El interesado puede ponerse en contacto con nuestro delegado de protección de datos para ejercer el derecho de rectificación.

***Derecho a la supresión (derecho al olvido)***

Además, los interesados tienen derecho a ser borrados y olvidados en virtud del Art. 17 RGPD. Este derecho también puede ejercerse poniéndose en contacto con nuestro delegado de protección de datos. En este punto, sin embargo, nos gustaría señalar que este derecho no se aplica en la medida en que el tratamiento es necesario para cumplir con una obligación legal a la que nuestra empresa está sujeta, el artículo 17, apartado 3, letra b). RGPD. Esto significa que podemos aprobar una solicitud para borrar sólo después de la expiración del plazo de retención legal.

***Derecho a la limitación de tratamiento***

De conformidad con el artículo 18 del RGPD, todo interesado tiene derecho a una limitación de tratamiento. La limitación de tratamiento podrá exigirse si se cumple una de las condiciones establecidas en el artículo 18, apartado 1, letra a-d, del RGPD. El interesado puede ponerse en contacto con nuestro delegado de protección de datos para ejercer el derecho a la limitación de tratamiento.


© All rights reserved by Heiko Maniero.

***Derecho de oposición***

Además, el Art. 21 del RGPD garantiza el derecho a objetar. El interesado puede ponerse en contacto con nuestro delegado de protección de datos para ejercer el derecho de oposición.

***Derecho a la portabilidad de datos***

El Art. 20 del RGPD concede al interesado el derecho a la portabilidad de datos. En virtud de esta disposición, el interesado, en las condiciones establecidas en el artículo 20, apartado 1, letras a) y b), del RGPD, tiene derecho a recibir los datos personales que le conciernan a el o ella, que el o ella haya facilitado a un responsable del tratamiento, en un formato estructurado, comúnmente utilizado y legible por máquinas, y tiene derecho a transmitirlos a otro responsable del tratamiento sin obstáculos por parte del responsable del tratamiento al que se hayan facilitado los datos personales. El interesado puede ponerse en contacto con nuestro delegado de protección de datos para ejercer el derecho a la portabilidad de datos.

## J. La existencia del derecho a retirar el consentimiento en cualquier momento, sin que ello afecte a la licitud del tratamiento basada en el consentimiento antes de su retirada, cuando el tratamiento esté basado en el artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a) (Art. 14(2) lit. d RGPD)

Si el tratamiento de datos personales se basa en el Art. 6(1) lit. del RGPD, que es el caso, si el interesado ha dado su consentimiento al tratamiento de datos personales para uno o más fines específicos o si se basa en el artículo 9(2) lit. del RGPD, que regula el consentimiento explícito al tratamiento de categorías especiales de datos personales, el interesado tiene, de acuerdo con el artículo 7(3) frase 1 del RGPD, el derecho de retirar su consentimiento en cualquier momento.

La revocación del consentimiento no afectará a la legalidad del tratamiento basado en el consentimiento antes de su revocación, artículo 7(3) frase 2 RGPD. Se reserva el derecho de retirar su consentimiento, Art. 7(3) Sentencia 4 RGPD. Por lo tanto, la revocación del consentimiento siempre puede tener lugar de la misma forma en que se ha dado el consentimiento o de cualquier otra forma que el interesado considere más sencilla. En la sociedad de la información actual, probablemente la forma más sencilla de retirar el consentimiento es un simple correo electrónico. Si el interesado desea revocar el consentimiento que nos ha dado, basta con enviarle un simple correo electrónico a nuestro delegado de protección de datos. De forma alternativa, el interesado puede elegir cualquier otra forma de comunicarnos la revocación de su consentimiento.

## K. Derecho a presentar una reclamación ante una autoridad de control (artículo 14, apartado 2, letra e), y artículo 77, apartado 1, del RGPD)

Como responsable del tratamiento, estamos obligados a notificar al interesado su derecho a presentar una reclamación ante una autoridad de control, artículo 13(2) lit. d RGPD El derecho a presentar una


© All rights reserved by Heiko Maniero.

reclamación ante una autoridad de control está regulado por el artículo 77, apartado 1, del RGPD. Con arreglo a esta disposición, sin perjuicio de cualquier otro recurso administrativo o judicial, todo interesado tendrá derecho a presentar una reclamación ante una autoridad de control, en particular en el Estado miembro de su residencia habitual, lugar de trabajo o lugar de la supuesta infracción, si el interesado considera que el tratamiento de los datos personales que le conciernen infringe el Reglamento General de Protección de Datos. El derecho a presentar una reclamación ante una autoridad de control sólo estaba limitado por la legislación de la Unión de tal manera que sólo puede ejercerse ante una única autoridad de control (primera frase del considerando 141 del RGPD). Esta norma tiene por objeto evitar la doble reclamación del mismo interesado en la misma materia. Si un interesado desea presentar una reclamación sobre nosotros, le pedimos que se ponga en contacto con una única autoridad de control.

## L. Fuente de la que proceden los datos personales y, en su caso, si proceden de fuentes de acceso público (artículo 14(2) lit. f RGPD)

En principio, los datos personales se recogen directamente del interesado o en cooperación con una autoridad (por ejemplo, extracción de datos de un registro oficial). Otros datos sobre los interesados se derivan de las transmisiones de empresas del grupo. En el contexto de esta información general, la indicación de las fuentes exactas de las que proceden los datos personales es imposible o supondría un esfuerzo desproporcionado en el sentido del artículo. 14(5) lit. b RGPD. En principio, no recogemos datos personales de fuentes de acceso público.

Cualquier interesado puede ponerse en contacto con nuestro delegado de protección de datos en cualquier momento para obtener información más detallada sobre las fuentes exactas de los datos personales que le conciernen. En los casos en que no pueda facilitarse al interesado el origen de los datos personales porque se hayan utilizado varias fuentes, deberá facilitarse información general (cuarta frase del considerando 61 del RGPD).

## M. La existencia de decisiones automatizadas, incluida la elaboración de perfiles, a que se refiere el artículo 22, apartados 1 y 4, y, al menos en tales casos, información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado (artículo 14, apartado 2, letra g), del RGPD)

Como empresa responsable, normalmente no utilizamos la toma de decisiones automatizada ni la elaboración de perfiles. Si, en casos excepcionales, llevamos a cabo la toma de decisiones automatizada o la elaboración de perfiles, informaremos al interesado por separado o a través de una subsección de nuestra política de privacidad (en nuestro sitio web). En este caso, se aplicará lo siguiente


© All rights reserved by Heiko Maniero.

La toma de decisiones automatizada -incluida la elaboración de perfiles- puede producirse si (1) es necesaria para celebrar o ejecutar un contrato entre el interesado y nosotros, o (2) está autorizada por la legislación de la Unión o de los Estados miembros a la que estamos sujetos y que también establece medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado; o (3) se basa en el consentimiento explícito del interesado.

En los casos contemplados en el artículo 22, apartado 2, letras a) y c) del RGPD, aplicaremos las medidas adecuadas para salvaguardar los derechos y libertades e intereses legítimos del interesado. En estos casos, tiene derecho a obtener intervención humana por parte del responsable del tratamiento, a expresar su punto de vista y a impugnar la decisión.

En nuestra política de privacidad se ofrece información significativa sobre la lógica implicada, así como sobre la importancia y las consecuencias previstas de dicho tratamiento para el interesado.

## III. EU-U.S. Data Privacy Framework (EU-U.S. DPF), UK Extension to the EU-U.S. DPF, Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF)

Si nuestra organización es un miembro certificado del EU-U.S. Data Privacy Framework (EU-U.S. DPF) y/o de la UK Extension to the EU-U.S. DPF y/o del Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF), se aplicará lo siguiente:

Nos adherimos al EU-U.S. Data Privacy Framework (EU-U.S. DPF) y a la UK Extension to the EU-U.S. DPF, así como al Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF), según lo establecido por el U.S. Department of Commerce. Nuestra empresa ha confirmado al Departamento de Comercio de los EE. UU. que cumple con los EU-U.S. Data Privacy Framework Principles (EU-U.S. DPF Principles) en relación con el procesamiento de datos personales que recibe de la Unión Europea y del Reino Unido en referencia al EU-U.S. DPF y la UK Extension to the EU-U.S. DPF. Nuestra empresa ha confirmado al Departamento de Comercio de los EE. UU. que cumple con los Swiss-U.S. Data Privacy Framework Principles (Swiss-U.S. DPF Principles) en relación con el procesamiento de datos personales que recibe de Suiza bajo el Swiss-U.S. DPF. En caso de conflicto entre las disposiciones de nuestra política de privacidad y los EU-U.S. DPF Principles y/o los Swiss-U.S. DPF Principles, los Principles prevalecerán.

Para aprender más sobre el programa Data Privacy Framework (DPF) y ver nuestra certificación, visite por favor https://www.dataprivacyframework.gov/.

Otras entidades estadounidenses o filiales de nuestra empresa que también se adhieren a los EU-U.S. DPF Principals, incluyendo la UK Extension to the EU-U.S. DPF y los Swiss-U.S. DPF Principals, si los hay, se mencionarán en nuestra política de privacidad.


© All rights reserved by Heiko Maniero.

De acuerdo con el EU-U.S. DPF, la UK Extension to the EU-U.S. DPF, y el Swiss-U.S. DPF, nuestra empresa se compromete a cooperar con el panel establecido por las autoridades de protección de datos de la UE, la Oficina del Comisionado de Información del Reino Unido (ICO) y el Comisionado Federal de Protección de Datos y Transparencia Pública (EDÖB) de Suiza, y seguir sus consejos en relación con quejas no resueltas sobre nuestro manejo de datos personales que recibimos bajo el EU-U.S. DPF, la UK Extension to the EU-U.S. DPF y el Swiss-U.S. DPF.

Informamos a las personas afectadas sobre las autoridades de protección de datos europeas competentes para manejar quejas sobre cómo nuestra organización gestiona datos personales, en la parte superior de este documento de transparencia, y que ofrecemos un remedio legal adecuado y gratuito.

Informamos a todas las personas afectadas de que nuestra empresa está sujeta a las facultades de investigación y ejecución de la Federal Trade Commission (FTC).

Las personas afectadas tienen la opción, bajo ciertas condiciones, de solicitar un arbitraje vinculante. Nuestra organización está obligada a resolver reclamaciones y cumplir con las condiciones según el Anexo I de los DPF-Principals, siempre que la persona afectada haya solicitado un arbitraje vinculante notificando a nuestra organización y se hayan cumplido los procedimientos y condiciones según el Anexo I de los Principals.

Informamos por este medio a todas las personas afectadas sobre la responsabilidad de nuestra organización en caso de transferencia de datos personales a terceros.

Para preguntas de las personas afectadas o de las autoridades de supervisión de protección de datos, hemos nombrado a los representantes locales mencionados en la parte superior de este documento de transparencia.

Ofrecemos la opción de elegir (Opt-out), si sus datos personales (i) serán compartidos con terceros o (ii) serán utilizados para un propósito sustancialmente diferente de aquel para el que fueron originalmente recopilados o posteriormente autorizados por usted. El mecanismo claramente visible y fácilmente accesible para ejercer su derecho de elección es contactar a nuestro Oficial de Protección de Datos (DSB) por correo electrónico. Usted no tiene opción, y no estamos obligados, cuando los datos se comparten con un tercero que actúa como agente o procesador en nuestro nombre y siguiendo nuestras instrucciones. Sin embargo, siempre firmamos un contrato con dicho agente o procesador.

Para datos sensibles (es decir, datos personales que incluyen información sobre el estado de salud, origen racial o étnico, opiniones políticas, creencias religiosas o filosóficas, membresía sindical o información sobre la vida sexual de la persona), obtenemos su consentimiento explícito (Opt-in) si estos datos (i) van a ser compartidos o (ii) van a ser utilizados para un propósito diferente al que fueron originalmente recopilados o para el que usted posteriormente dio su consentimiento al hacer su elección de Opt-in. Además, tratamos todos los datos personales que recibimos de terceros como sensibles si el tercero los ha identificado y tratado como tales.


© All rights reserved by Heiko Maniero.

Le informamos sobre la necesidad de divulgar datos personales en respuesta a solicitudes legales de autoridades, incluyendo el cumplimiento de requisitos de seguridad nacional o aplicación de la ley.

Al transferir datos personales a un tercero que actúa como controlador, cumplimos con los Principals de notificación y elección. Además, firmamos un contrato con el tercero responsable del procesamiento que estipula que esos datos solo pueden ser procesados para fines limitados y específicos de acuerdo con el consentimiento que usted proporcionó y que el receptor proporciona el mismo nivel de protección que los Principals del DPF y nos notifica si determina que ya no puede cumplir con esta obligación. El contrato estipula que el tercero que actúa como controlador debe cesar el procesamiento o tomar otras medidas razonables y adecuadas para remediar la situación si se hace tal determinación.

Al transferir datos personales a un tercero que actúa como agente o procesador, (i) solo transferimos esos datos para fines limitados y específicos; (ii) nos aseguramos de que el agente o procesador esté obligado a proporcionar al menos el mismo nivel de protección de datos requerido por los DPF-Principals; (iii) tomamos medidas razonables y adecuadas para asegurar que el agente o procesador realmente procese los datos personales transferidos de una manera que sea consistente con nuestras obligaciones bajo los DPF-Principals; (iv) exigimos que el agente o procesador nos notifique si determina que ya no puede cumplir con su obligación de proporcionar el mismo nivel de protección requerido por los DPF-Principals; (v) tras una notificación, también bajo (iv), tomamos medidas razonables y adecuadas para detener el procesamiento no autorizado y remediar la situación; y (vi) proporcionamos al DPF Department, a solicitud, un resumen o un ejemplar representativo de las disposiciones relevantes de privacidad de nuestro contrato con ese agente.

En conformidad con el EU-U.S. DPF y/o la UK Extension to the EU-U.S. DPF y/o el Swiss-U.S. DPF, nuestra organización se compromete a cooperar con el panel establecido por las autoridades de protección de datos de la UE y el Information Commissioner's Office (ICO) del Reino Unido y el Comisionado Federal de Protección de Datos y Transparencia Pública (EDÖB) de Suiza, y a seguir sus consejos respecto a quejas no resueltas sobre nuestro manejo de datos personales que recibimos en relación con el empleo bajo el EU-U.S. DPF, la UK Extension to the EU-U.S. DPF y el Swiss-U.S. DPF.

Todos los interesados que se encuentren temporalmente en la Unión Europea (UE), el Espacio Económico Europeo (EEE) o el Reino Unido, o que tengan allí su domicilio o residencia habitual, tienen los derechos y los derechos del interesado que se publican en nuestro Documento de Transparencia, que también se derivan de los artículos 15 a 22 del GDPR, incluido el derecho de acceso a los datos personales. Hemos publicado esta información en todos los idiomas de la UE y del EEE. La versión en inglés se aplica al Reino Unido.

Todos los interesados que residan temporalmente en Suiza o tengan allí su domicilio o residencia habitual gozan de los derechos y garantías previstos en la Ley suiza de protección de datos (LPD) y en el Reglamento suizo de protección de datos (RGPD) que se publican en nuestro Documento de Transparencia, incluido el derecho de acceso a los datos personales. Hemos facilitado esta información en las tres lenguas oficiales de Suiza (alemán, italiano y francés).


© All rights reserved by Heiko Maniero.

© All rights reserved by Heiko Maniero.

# SPANISH: Información sobre el tratamiento de datos personales de los empleados y solicitantes (artículo 13, 14 del RGPD)

Estimado señor o señora:

Los datos personales de empleados y solicitantes merecen una protección especial. Nuestro objetivo es mantener nuestro nivel de protección de datos en los más altos estándares. Por lo tanto, estamos desarrollando rutinariamente nuestros conceptos de protección y seguridad de datos.

Por supuesto, cumplimos con las disposiciones legales sobre protección de datos. De acuerdo con los artículos 13 y 14 del RGPD, los responsables del tratamiento cumplen requisitos específicos de información al tratar datos personales. Este documento cumple con estas obligaciones.

La terminología de las normas legales es complicada. Desafortunadamente, no se pudo prescindir del uso de términos legales en la preparación de este documento. Por lo tanto, nos gustaría señalar que usted es siempre bienvenido a ponerse en contacto con nosotros para todas las preguntas relativas a este documento, los términos utilizados o formulaciones.

## I. Cumplimiento de los requisitos de información cuando se recogen datos personales de el interesado (artículo 13 del RGPD)

### A. Identidad y datos de contacto del responsable (artículo 13.1 lit. a RGPD)

Véase arriba

### B. Datos de contacto del delegado de protección de datos (artículo 13(1) lit. b RGPD)

Véase arriba

### C. Finalidades del tratamiento al que se destinan los datos personales, así como el fundamento jurídico del tratamiento (artículo 13, apartado 1, letra c), del RGPD)

Para los datos de solicitantes, el fin del tratamiento de datos es realizar un examen de la solicitud durante el proceso de selección. Por este motivo, tratamos todos los datos que nos proporcione. Basándonos en los datos suministrados durante el proceso de selección, comprobaremos si se le invita a una entrevista


© All rights reserved by Heiko Maniero.

de trabajo (parte del proceso de selección). En caso de candidatos generalmente aptos, en particular en el contexto de la entrevista de trabajo, trataremos otro tipo determinado de datos personales que usted nos proporcione, algo esencial para tomar una decisión en el proceso de selección. Si nosotros le contratamos, los datos de solicitante cambiarán automáticamente a datos de empleado. Como parte del proceso de selección, trataremos otros datos personales de usted que le solicitemos y que son necesarios para iniciar o cumplir con su contrato (como números de identidad personal o números fiscales). En relación a los datos de empleados, el fin del tratamiento de datos es la ejecución del contrato de trabajo o el cumplimiento de otras obligaciones legales aplicables a la relación laboral (p. ej., legislación tributaria) así como el uso de sus datos personales para llevar a cabo el contrato de trabajo celebrado con usted (p. ej., la publicación de su nombre e información de contacto en la empresa o a disposición de los usuarios). Los datos de empleados se almacenan una vez concluida la relación laboral para cumplir con los periodos legales de conservación.

La base jurídica para el tratamiento de datos es el artículo 6, apartado 1, letra b), del RGPD, artículo 9, apartado 2, letras b) y h), del RGPD, artículo 88, apartado 1 del RGPD y la legislación nacional, tal como el artículo 26 de la BDSG (Ley Federal sobre Protección de Datos alemana).

## D. Categorías de destinatarios de los datos personales (artículo 13, apartado 1, lit. e RGPD)

Autoridades públicas

Organismos externos

Otros organismos externos

Tratamiento interno

Tratamiento dentro del grupo

Otros organismos

En nuestro sitio web se publica una lista de nuestros encargados del tratamiento y destinatarios de datos en terceros países y, en su caso, organizaciones internacionales, o bien puede solicitárnosla gratuitamente. Póngase en contacto con nuestro responsable de protección de datos para solicitar esta lista.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## E. Destinatarios en un tercer país y las garantías adecuadas o apropiadas y los medios para obtener una copia de estas o al hecho de que se hayan prestado (artículo 13, apartado 1, letra f), artículo 46, apartados 1 y 2, letra c), del RGPD)

Todas las empresas y sucursales que forman parte de nuestro grupo (en lo sucesivo denominadas "empresas del grupo") que tienen su sede o una oficina en un tercer país pueden pertenecer a los destinatarios de los datos personales.

De conformidad con el artículo 46, apartado 1, del Reglamento de protección de datos (RGPD), un responsable del tratamiento o un encargado del tratamiento sólo puede transferir datos personales a un tercer país si el responsable del tratamiento o el encargado del tratamiento ha ofrecido las garantías adecuadas, y a condición de que se disponga de derechos exigibles a los interesados de vías de recurso efectivas para los interesados. Se pueden proporcionar garantías apropiadas sin requerir ninguna autorización específica de una autoridad de control por medio de cláusulas contractuales estándar, artículo 46(2) lit. c RGPD.

Las cláusulas contractuales de la Unión Europea se acuerdan con todos los destinatarios de terceros países antes de la primera transmisión de datos personales. En consecuencia, se aseguran las garantías adecuadas, los derechos exigibles de los interesados los recursos legales efectivos para los interesados que se derivan de las cláusulas contractuales estándares de la UE. Todos los interesados pueden obtener una copia de las cláusulas contractuales tipo a través de nuestro delegado de protección de datos. Las cláusulas contractuales tipo también están disponibles en el Diario Oficial de la Unión Europea.

El artículo 45, apartado 3, del Reglamento General de Protección de Datos (RGPD) otorga a la Comisión Europea la facultad de decidir, mediante un acto de ejecución, que un país no perteneciente a la UE garantiza un nivel de protección adecuado. Esto significa un nivel de protección de los datos personales esencialmente equivalente al nivel de protección dentro de la UE. El efecto de las decisiones de adecuación es que los datos personales pueden circular libremente desde la UE (y Noruega, Liechtenstein e Islandia) a un tercer país sin más obstáculos. Existen normas similares para el Reino Unido, Suiza y algunos otros países.

Cuando la Comisión Europea o el gobierno de otro país decida que un tercer país garantiza un nivel adecuado de protección y exista un marco válido (por ejemplo, EU-U.S. Data Privacy Framework, Swiss-U.S. Data Privacy Framework, UK Extension to the EU-U.S. Data Privacy Framework), todas las transferencias que realicemos a los miembros de dichos marcos (por ejemplo, entidades autocertificadas) se basarán exclusivamente en la pertenencia de dichas entidades al marco respectivo. Cuando nosotros o una de las entidades de nuestro grupo sea miembro de dicho marco, todas las transferencias a nosotros o a la entidad de nuestro grupo se basarán exclusivamente en la pertenencia de la entidad a dicho marco.


© All rights reserved by Heiko Maniero.

Cualquier interesado puede solicitarnos una copia de los marcos. Además, los marcos también están disponibles en el Diario Oficial de la Unión Europea o en los materiales jurídicos publicados o en los sitios web de las autoridades de control o de otras autoridades o instituciones competentes.

## F. Plazo durante el cual se conservarán los datos personales o, cuando no sea posible, los criterios utilizados para determinar este plazo (artículo 13, apartado 2, letra a), del RGPD).

La duración del almacenamiento de datos personales de los solicitantes es de 6 meses. Se aplica el correspondiente periodo legal de conservación para los datos de empleados. Una vez transcurrido dicho plazo, los datos correspondientes se borran de forma rutinaria, siempre que ya no sean necesarios para el cumplimiento del contrato o la iniciación de un contrato.

## G. La existencia del derecho a solicitar al responsable del tratamiento el acceso a los datos personales relativos al interesado, y su rectificación o supresión, o la limitación de su tratamiento, o a oponerse al tratamiento, así como el derecho a la portabilidad de los datos (artículo 13, apartado 2, letra b), del RGPD)

Todos los interesados tienen los siguientes derechos:

***Derecho de acceso***

Cada interesado tiene derecho a acceder a los datos personales que le conciernen. El derecho de acceso se extiende a todos los datos procesados por nosotros. El derecho puede ejercerse fácilmente y a intervalos razonables para conocer y verificar la legalidad del tratamiento (considerando 63 del RGPD). Este derecho resulta del Art. 15 RGPD. El interesado puede ponerse en contacto con nuestro delegado de protección de datos para ejercer el derecho de acceso.

***Derecho a rectificación***

De conformidad con la primera frase del artículo 16 del RGPD, el interesado tiene derecho a obtener del responsable del tratamiento, sin demora injustificada, la rectificación de los datos personales inexactos que le conciernan. Además, la segunda frase del artículo 16 del RGPD establece que el interesado tiene derecho, teniendo en cuenta los fines del tratamiento, a que se completen los datos personales incompletos, incluso mediante una declaración complementaria. El interesado puede ponerse en contacto con nuestro delegado de protección de datos para ejercer el derecho de rectificación.

***Derecho a la supresión (derecho al olvido)***

Además, los interesados tienen derecho a ser borrados y olvidados en virtud del Art. 17 RGPD. Este derecho también puede ejercerse poniéndose en contacto con nuestro delegado de protección de datos. En este punto, sin embargo, nos gustaría señalar que este derecho no se aplica en la medida en que el tratamiento es necesario para cumplir con una obligación legal a la que nuestra empresa está sujeta, el


© All rights reserved by Heiko Maniero.

artículo 17, apartado 3, letra b). RGPD. Esto significa que podemos aprobar una solicitud para borrar sólo después de la expiración del plazo de retención legal.

***Derecho a la limitación de tratamiento***

De conformidad con el artículo 18 del RGPD, todo interesado tiene derecho a una limitación de tratamiento. La limitación de tratamiento podrá exigirse si se cumple una de las condiciones establecidas en el artículo 18, apartado 1, letra a-d, del RGPD. El interesado puede ponerse en contacto con nuestro delegado de protección de datos para ejercer el derecho a la limitación de tratamiento.

***Derecho de oposición***

Además, el Art. 21 del RGPD garantiza el derecho a objetar. El interesado puede ponerse en contacto con nuestro delegado de protección de datos para ejercer el derecho de oposición.

***Derecho a la portabilidad de datos***

El Art. 20 del RGPD concede al interesado el derecho a la portabilidad de datos. En virtud de esta disposición, el interesado, en las condiciones establecidas en el artículo 20, apartado 1, letras a) y b), del RGPD, tiene derecho a recibir los datos personales que le conciernan a el o ella, que el o ella haya facilitado a un responsable del tratamiento, en un formato estructurado, comúnmente utilizado y legible por máquinas, y tiene derecho a transmitirlos a otro responsable del tratamiento sin obstáculos por parte del responsable del tratamiento al que se hayan facilitado los datos personales. El interesado puede ponerse en contacto con nuestro delegado de protección de datos para ejercer el derecho a la portabilidad de datos.

## H. La existencia del derecho a retirar el consentimiento en cualquier momento, sin que ello afecte a la licitud del tratamiento basado en el consentimiento previo a su retirada, cuando el tratamiento esté basado en el artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a) (artículo 13, apartado 2, letra c), del RGPD)

Si el tratamiento de datos personales se basa en el Art. 6(1) lit. del RGPD, que es el caso, si el interesado ha dado su consentimiento al tratamiento de datos personales para uno o más fines específicos o si se basa en el artículo 9(2) lit. del RGPD, que regula el consentimiento explícito al tratamiento de categorías especiales de datos personales, el interesado tiene, de acuerdo con el artículo 7(3) frase 1 del RGPD, el derecho de retirar su consentimiento en cualquier momento.

La revocación del consentimiento no afectará a la legalidad del tratamiento basado en el consentimiento antes de su revocación, artículo 7(3) frase 2 RGPD. Se reserva el derecho de retirar su consentimiento, Art. 7(3) Sentencia 4 RGPD. Por lo tanto, la revocación del consentimiento siempre puede tener lugar de la misma forma en que se ha dado el consentimiento o de cualquier otra forma que el interesado considere más sencilla. En la sociedad de la información actual, probablemente la forma más sencilla


© All rights reserved by Heiko Maniero.

de retirar el consentimiento es un simple correo electrónico. Si el interesado desea revocar el consentimiento que nos ha dado, basta con enviarle un simple correo electrónico a nuestro delegado de protección de datos. De forma alternativa, el interesado puede elegir cualquier otra forma de comunicarnos la revocación de su consentimiento.

## I. Derecho a presentar una reclamación ante una autoridad de control (letra d) del apartado 2 del artículo 13 y apartado 1 del artículo 77 del RGPD)

Como responsable del tratamiento, estamos obligados a notificar al interesado su derecho a presentar una reclamación ante una autoridad de control, artículo 13(2) lit. d RGPD El derecho a presentar una reclamación ante una autoridad de control está regulado por el artículo 77, apartado 1, del RGPD. Con arreglo a esta disposición, sin perjuicio de cualquier otro recurso administrativo o judicial, todo interesado tendrá derecho a presentar una reclamación ante una autoridad de control, en particular en el Estado miembro de su residencia habitual, lugar de trabajo o lugar de la supuesta infracción, si el interesado considera que el tratamiento de los datos personales que le conciernen infringe el Reglamento General de Protección de Datos. El derecho a presentar una reclamación ante una autoridad de control sólo estaba limitado por la legislación de la Unión de tal manera que sólo puede ejercerse ante una única autoridad de control (primera frase del considerando 141 del RGPD). Esta norma tiene por objeto evitar la doble reclamación del mismo interesado en la misma materia. Si un interesado desea presentar una reclamación sobre nosotros, le pedimos que se ponga en contacto con una única autoridad de control.

## J. La comunicación de datos personales es un requisito legal o contractual, o un requisito necesario para suscribir un contrato, y si el interesado está obligado a facilitar los datos personales y está informado de las posibles consecuencias de que no facilitar tales datos (Art. 13(2) lit. e RGPD)

Aclaramos que el suministro de datos personales es requerido en parte por la ley (p.ej. regulaciones fiscales) o también puede resultar de disposiciones contractuales (p.ej. información sobre la parte contratante).

A veces puede ser necesario celebrar un contrato en el que el interesado nos proporciona datos personales, que deben ser procesados posteriormente por nosotros. Por ejemplo, el interesado está obligado a facilitarnos datos personales cuando nuestra empresa firma un contrato con él. La no comunicación de los datos personales tendría como consecuencia que no se pudiera celebrar el contrato con el interesado.

Antes de que el interesado facilite datos personales, el interesado deberá ponerse en contacto con nuestro delegado de protección de datos. Nuestro delegado de protección de datos aclara al interesado si el suministro de los datos personales es requerido por la ley o el contrato o si es necesario para la


© All rights reserved by Heiko Maniero.

conclusión del contrato, si existe una obligación de proporcionar los datos personales y las consecuencias de la no entrega de los datos personales.

### K. La existencia de decisiones automatizadas, incluida la elaboración de perfiles, a que se refiere el artículo 22, apartados 1 y 4, y, al menos en tales casos, información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado (artículo 13, apartado 2, letra f), del RGPD)

Como empresa responsable, normalmente no utilizamos la toma de decisiones automatizada ni la elaboración de perfiles. Si, en casos excepcionales, llevamos a cabo la toma de decisiones automatizada o la elaboración de perfiles, informaremos al interesado por separado o a través de una subsección de nuestra política de privacidad (en nuestro sitio web). En este caso, se aplicará lo siguiente

La toma de decisiones automatizada -incluida la elaboración de perfiles- puede producirse si (1) es necesaria para celebrar o ejecutar un contrato entre el interesado y nosotros, o (2) está autorizada por la legislación de la Unión o de los Estados miembros a la que estamos sujetos y que también establece medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado; o (3) se basa en el consentimiento explícito del interesado.

En los casos contemplados en el artículo 22, apartado 2, letras a) y c) del RGPD, aplicaremos las medidas adecuadas para salvaguardar los derechos y libertades e intereses legítimos del interesado. En estos casos, tiene derecho a obtener intervención humana por parte del responsable del tratamiento, a expresar su punto de vista y a impugnar la decisión.

En nuestra política de privacidad se ofrece información significativa sobre la lógica implicada, así como sobre la importancia y las consecuencias previstas de dicho tratamiento para el interesado.

## II. Cumplimiento de los requisitos de información cuando no se reciben datos personales del interesado (artículo 14 del RGPD)

### A. La identidad y los datos de contacto del responsable y, en su caso, de su representante (artículo 14.1 lit. a RGPD)

Véase arriba


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## B. Datos de contacto del delegado de protección de datos, en su caso (artículo 14(1) lit. b RGPD)

Véase arriba

## C. Finalidades del tratamiento al que se destinan los datos personales, así como el fundamento jurídico del tratamiento (artículo 14, apartado 1, letra c), del RGPD)

Si los datos de los solicitantes no se obtienen de los interesados, el fin del tratamiento de datos es realizar un examen de la solicitud durante el proceso de selección. Para tal fin, podremos tratar datos no obtenidos de usted. Basándonos en los datos tratados durante el proceso de selección, comprobaremos si se le invita a una entrevista de trabajo (parte del proceso de selección). Si nosotros le contratamos, los datos de solicitante se convertirán automáticamente en datos de empleado. Para los datos de empleados, el fin del tratamiento de los datos es la ejecución del contrato de empleo o el cumplimiento de otras obligaciones legales aplicables a la relación laboral. Los datos de empleados se almacenan una vez concluida la relación laboral para cumplir con los periodos legales de conservación.

La base jurídica para el tratamiento de datos es el artículo 6, apartado 1, letra b) y f), del RGPD, artículo 9, apartado 2, letras b) y h), del RGPD, artículo 88, apartado 1 del RGPD y la legislación nacional, tal como el artículo 26 de la BDSG (Ley Federal sobre Protección de Datos alemana).

## D. Categorías de datos personales de que se trate (artículo 14, apartado 1, letra d), del RGPD)

Datos de solicitantes

Datos de empleados

## E. Categorías de destinatarios de los datos personales (artículo 14, apartado 1, lit. e RGPD)

Autoridades públicas

Organismos externos

Otros organismos externos

Tratamiento interno

Tratamiento dentro del grupo

Otros organismos


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

En nuestro sitio web se publica una lista de nuestros encargados del tratamiento y destinatarios de datos en terceros países y, en su caso, organizaciones internacionales, o bien puede solicitárnosla gratuitamente. Póngase en contacto con nuestro responsable de protección de datos para solicitar esta lista.

## F. Destinatarios en un tercer país u organización internacional y las garantías adecuadas o apropiadas y a los medios para obtener una copia de ellas o al hecho de que se hayan prestado (artículo 14, apartado 1, letra f), artículo 46, apartados 1 y 2, letra c), del RGPD)

Todas las empresas y sucursales que forman parte de nuestro grupo (en lo sucesivo denominadas "empresas del grupo") que tienen su sede o una oficina en un tercer país pueden pertenecer a los destinatarios de los datos personales.

De conformidad con el artículo 46, apartado 1, del Reglamento de protección de datos (RGPD), un responsable del tratamiento o un encargado del tratamiento sólo puede transferir datos personales a un tercer país si el responsable del tratamiento o el encargado del tratamiento ha ofrecido las garantías adecuadas, y a condición de que se disponga de derechos exigibles a los interesados de vías de recurso efectivas para los interesados. Se pueden proporcionar garantías apropiadas sin requerir ninguna autorización específica de una autoridad de control por medio de cláusulas contractuales estándar, artículo 46(2) lit. c RGPD.

Las cláusulas contractuales de la Unión Europea se acuerdan con todos los destinatarios de terceros países antes de la primera transmisión de datos personales. En consecuencia, se aseguran las garantías adecuadas, los derechos exigibles de los interesados los recursos legales efectivos para los interesados que se derivan de las cláusulas contractuales estándares de la UE. Todos los interesados pueden obtener una copia de las cláusulas contractuales tipo a través de nuestro delegado de protección de datos. Las cláusulas contractuales tipo también están disponibles en el Diario Oficial de la Unión Europea.

El artículo 45, apartado 3, del Reglamento General de Protección de Datos (RGPD) otorga a la Comisión Europea la facultad de decidir, mediante un acto de ejecución, que un país no perteneciente a la UE garantiza un nivel de protección adecuado. Esto significa un nivel de protección de los datos personales esencialmente equivalente al nivel de protección dentro de la UE. El efecto de las decisiones de adecuación es que los datos personales pueden circular libremente desde la UE (y Noruega, Liechtenstein e Islandia) a un tercer país sin más obstáculos. Existen normas similares para el Reino Unido, Suiza y algunos otros países.


© All rights reserved by Heiko Maniero.

Cuando la Comisión Europea o el gobierno de otro país decida que un tercer país garantiza un nivel adecuado de protección y exista un marco válido (por ejemplo, EU-U.S. Data Privacy Framework, Swiss-U.S. Data Privacy Framework, UK Extension to the EU-U.S. Data Privacy Framework), todas las transferencias que realicemos a los miembros de dichos marcos (por ejemplo, entidades autocertificadas) se basarán exclusivamente en la pertenencia de dichas entidades al marco respectivo. Cuando nosotros o una de las entidades de nuestro grupo sea miembro de dicho marco, todas las transferencias a nosotros o a la entidad de nuestro grupo se basarán exclusivamente en la pertenencia de la entidad a dicho marco.

Cualquier interesado puede solicitarnos una copia de los marcos. Además, los marcos también están disponibles en el Diario Oficial de la Unión Europea o en los materiales jurídicos publicados o en los sitios web de las autoridades de control o de otras autoridades o instituciones competentes.

## G. Plazo durante el cual se conservarán los datos personales o, cuando eso no sea posible, los criterios utilizados para determinar este plazo (artículo 14, apartado 2, letra a), del RGPD)

La duración del almacenamiento de datos personales de los solicitantes es de 6 meses. Se aplica el correspondiente periodo legal de conservación para los datos de empleados. Una vez transcurrido dicho plazo, los datos correspondientes se borran de forma rutinaria, siempre que ya no sean necesarios para el cumplimiento del contrato o la iniciación de un contrato.

## H. Notificación de los intereses legítimos perseguidos por el responsable del tratamiento o por un tercero si el tratamiento se basa en el artículo 6, apartado 1, letra f), del RGPD (artículo 14, apartado 2, letra b), del RGPD)

De conformidad con el artículo 6, apartado 1, letra f), del RGPD, el tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un niño. Según la segunda frase del considerando 47 del RGPD, podría existir un interés legítimo cuando exista una relación pertinente y adecuada entre el interesado y el responsable del tratamiento, por ejemplo, en situaciones en las que el interesado sea cliente del responsable del tratamiento. En todos los casos en los que nuestra empresa trate datos de solicitantes en base al artículo 6, apartado 1, letra f), del RGPD, nuestro interés legítimo es el empleo de profesionales y personal aptos.


© All rights reserved by Heiko Maniero.

## I. La existencia del derecho a solicitar al responsable del tratamiento el acceso a los datos personales relativos al interesado, y su rectificación o supresión, o la limitación de su tratamiento, y a oponerse al tratamiento, así como el derecho a la portabilidad de los datos (artículo 14, apartado 2, letra c), del RGPD)

Todos los interesados tienen los siguientes derechos:

***Derecho de acceso***

Cada interesado tiene derecho a acceder a los datos personales que le conciernen. El derecho de acceso se extiende a todos los datos procesados por nosotros. El derecho puede ejercerse fácilmente y a intervalos razonables para conocer y verificar la legalidad del tratamiento (considerando 63 del RGPD). Este derecho resulta del Art. 15 RGPD. El interesado puede ponerse en contacto con nuestro delegado de protección de datos para ejercer el derecho de acceso.

***Derecho a rectificación***

De conformidad con la primera frase del artículo 16 del RGPD, el interesado tiene derecho a obtener del responsable del tratamiento, sin demora injustificada, la rectificación de los datos personales inexactos que le conciernan. Además, la segunda frase del artículo 16 del RGPD establece que el interesado tiene derecho, teniendo en cuenta los fines del tratamiento, a que se completen los datos personales incompletos, incluso mediante una declaración complementaria. El interesado puede ponerse en contacto con nuestro delegado de protección de datos para ejercer el derecho de rectificación.

***Derecho a la supresión (derecho al olvido)***

Además, los interesados tienen derecho a ser borrados y olvidados en virtud del Art. 17 RGPD. Este derecho también puede ejercerse poniéndose en contacto con nuestro delegado de protección de datos. En este punto, sin embargo, nos gustaría señalar que este derecho no se aplica en la medida en que el tratamiento es necesario para cumplir con una obligación legal a la que nuestra empresa está sujeta, el artículo 17, apartado 3, letra b). RGPD. Esto significa que podemos aprobar una solicitud para borrar sólo después de la expiración del plazo de retención legal.

***Derecho a la limitación de tratamiento***

De conformidad con el artículo 18 del RGPD, todo interesado tiene derecho a una limitación de tratamiento. La limitación de tratamiento podrá exigirse si se cumple una de las condiciones establecidas en el artículo 18, apartado 1, letra a-d, del RGPD. El interesado puede ponerse en contacto con nuestro delegado de protección de datos para ejercer el derecho a la limitación de tratamiento.

***Derecho de oposición***

Además, el Art. 21 del RGPD garantiza el derecho a objetar. El interesado puede ponerse en contacto con nuestro delegado de protección de datos para ejercer el derecho de oposición.

***Derecho a la portabilidad de datos***

El Art. 20 del RGPD concede al interesado el derecho a la portabilidad de datos. En virtud de esta disposición, el interesado, en las condiciones establecidas en el artículo 20, apartado 1, letras a) y b),


© All rights reserved by Heiko Maniero.

del RGPD, tiene derecho a recibir los datos personales que le conciernan a el o ella, que el o ella haya facilitado a un responsable del tratamiento, en un formato estructurado, comúnmente utilizado y legible por máquinas, y tiene derecho a transmitirlos a otro responsable del tratamiento sin obstáculos por parte del responsable del tratamiento al que se hayan facilitado los datos personales. El interesado puede ponerse en contacto con nuestro delegado de protección de datos para ejercer el derecho a la portabilidad de datos.

## J. La existencia del derecho a retirar el consentimiento en cualquier momento, sin que ello afecte a la licitud del tratamiento basada en el consentimiento antes de su retirada, cuando el tratamiento esté basado en el artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a) (Art. 14(2) lit. d RGPD)

Si el tratamiento de datos personales se basa en el Art. 6(1) lit. del RGPD, que es el caso, si el interesado ha dado su consentimiento al tratamiento de datos personales para uno o más fines específicos o si se basa en el artículo 9(2) lit. del RGPD, que regula el consentimiento explícito al tratamiento de categorías especiales de datos personales, el interesado tiene, de acuerdo con el artículo 7(3) frase 1 del RGPD, el derecho de retirar su consentimiento en cualquier momento.

La revocación del consentimiento no afectará a la legalidad del tratamiento basado en el consentimiento antes de su revocación, artículo 7(3) frase 2 RGPD. Se reserva el derecho de retirar su consentimiento, Art. 7(3) Sentencia 4 RGPD. Por lo tanto, la revocación del consentimiento siempre puede tener lugar de la misma forma en que se ha dado el consentimiento o de cualquier otra forma que el interesado considere más sencilla. En la sociedad de la información actual, probablemente la forma más sencilla de retirar el consentimiento es un simple correo electrónico. Si el interesado desea revocar el consentimiento que nos ha dado, basta con enviarle un simple correo electrónico a nuestro delegado de protección de datos. De forma alternativa, el interesado puede elegir cualquier otra forma de comunicarnos la revocación de su consentimiento.

## K. Derecho a presentar una reclamación ante una autoridad de control (artículo 14, apartado 2, letra e), y artículo 77, apartado 1, del RGPD)

Como responsable del tratamiento, estamos obligados a notificar al interesado su derecho a presentar una reclamación ante una autoridad de control, artículo 13(2) lit. d RGPD El derecho a presentar una reclamación ante una autoridad de control está regulado por el artículo 77, apartado 1, del RGPD. Con arreglo a esta disposición, sin perjuicio de cualquier otro recurso administrativo o judicial, todo interesado tendrá derecho a presentar una reclamación ante una autoridad de control, en particular en el Estado miembro de su residencia habitual, lugar de trabajo o lugar de la supuesta infracción, si el interesado considera que el tratamiento de los datos personales que le conciernen infringe el Reglamento General de Protección de Datos. El derecho a presentar una reclamación ante una autoridad de control sólo


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

estaba limitado por la legislación de la Unión de tal manera que sólo puede ejercerse ante una única autoridad de control (primera frase del considerando 141 del RGPD). Esta norma tiene por objeto evitar la doble reclamación del mismo interesado en la misma materia. Si un interesado desea presentar una reclamación sobre nosotros, le pedimos que se ponga en contacto con una única autoridad de control.

## L. Fuente de la que proceden los datos personales y, en su caso, si proceden de fuentes de acceso público (artículo 14(2) lit. f RGPD)

En principio, los datos personales se recogen directamente del interesado o en cooperación con una autoridad (por ejemplo, extracción de datos de un registro oficial). Otros datos sobre los interesados se derivan de las transmisiones de empresas del grupo. En el contexto de esta información general, la indicación de las fuentes exactas de las que proceden los datos personales es imposible o supondría un esfuerzo desproporcionado en el sentido del artículo. 14(5) lit. b RGPD. En principio, no recogemos datos personales de fuentes de acceso público.

Cualquier interesado puede ponerse en contacto con nuestro delegado de protección de datos en cualquier momento para obtener información más detallada sobre las fuentes exactas de los datos personales que le conciernen. En los casos en que no pueda facilitarse al interesado el origen de los datos personales porque se hayan utilizado varias fuentes, deberá facilitarse información general (cuarta frase del considerando 61 del RGPD).

## M. La existencia de decisiones automatizadas, incluida la elaboración de perfiles, a que se refiere el artículo 22, apartados 1 y 4, y, al menos en tales casos, información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado (artículo 14, apartado 2, letra g), del RGPD)

Como empresa responsable, normalmente no utilizamos la toma de decisiones automatizada ni la elaboración de perfiles. Si, en casos excepcionales, llevamos a cabo la toma de decisiones automatizada o la elaboración de perfiles, informaremos al interesado por separado o a través de una subsección de nuestra política de privacidad (en nuestro sitio web). En este caso, se aplicará lo siguiente

La toma de decisiones automatizada -incluida la elaboración de perfiles- puede producirse si (1) es necesaria para celebrar o ejecutar un contrato entre el interesado y nosotros, o (2) está autorizada por la legislación de la Unión o de los Estados miembros a la que estamos sujetos y que también establece medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado; o (3) se basa en el consentimiento explícito del interesado.

En los casos contemplados en el artículo 22, apartado 2, letras a) y c) del RGPD, aplicaremos las medidas adecuadas para salvaguardar los derechos y libertades e intereses legítimos del interesado.


© All rights reserved by Heiko Maniero.

En estos casos, tiene derecho a obtener intervención humana por parte del responsable del tratamiento, a expresar su punto de vista y a impugnar la decisión.

En nuestra política de privacidad se ofrece información significativa sobre la lógica implicada, así como sobre la importancia y las consecuencias previstas de dicho tratamiento para el interesado.

## III. EU-U.S. Data Privacy Framework (EU-U.S. DPF), UK Extension to the EU-U.S. DPF, Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF)

Si nuestra organización es un miembro certificado del EU-U.S. Data Privacy Framework (EU-U.S. DPF) y/o de la UK Extension to the EU-U.S. DPF y/o del Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF), se aplicará lo siguiente:

Nos adherimos al EU-U.S. Data Privacy Framework (EU-U.S. DPF) y a la UK Extension to the EU-U.S. DPF, así como al Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF), según lo establecido por el U.S. Department of Commerce. Nuestra empresa ha confirmado al Departamento de Comercio de los EE. UU. que cumple con los EU-U.S. Data Privacy Framework Principles (EU-U.S. DPF Principles) en relación con el procesamiento de datos personales que recibe de la Unión Europea y del Reino Unido en referencia al EU-U.S. DPF y la UK Extension to the EU-U.S. DPF. Nuestra empresa ha confirmado al Departamento de Comercio de los EE. UU. que cumple con los Swiss-U.S. Data Privacy Framework Principles (Swiss-U.S. DPF Principles) en relación con el procesamiento de datos personales que recibe de Suiza bajo el Swiss-U.S. DPF. En caso de conflicto entre las disposiciones de nuestra política de privacidad y los EU-U.S. DPF Principles y/o los Swiss-U.S. DPF Principles, los Principles prevalecerán.

Para aprender más sobre el programa Data Privacy Framework (DPF) y ver nuestra certificación, visite por favor https://www.dataprivacyframework.gov/.

Otras entidades estadounidenses o filiales de nuestra empresa que también se adhieren a los EU-U.S. DPF Principals, incluyendo la UK Extension to the EU-U.S. DPF y los Swiss-U.S. DPF Principals, si los hay, se mencionarán en nuestra política de privacidad.

De acuerdo con el EU-U.S. DPF, la UK Extension to the EU-U.S. DPF, y el Swiss-U.S. DPF, nuestra empresa se compromete a cooperar con el panel establecido por las autoridades de protección de datos de la UE, la Oficina del Comisionado de Información del Reino Unido (ICO) y el Comisionado Federal de Protección de Datos y Transparencia Pública (EDÖB) de Suiza, y seguir sus consejos en relación con quejas no resueltas sobre nuestro manejo de datos personales que recibimos bajo el EU-U.S. DPF, la UK Extension to the EU-U.S. DPF y el Swiss-U.S. DPF.

Informamos a las personas afectadas sobre las autoridades de protección de datos europeas competentes para manejar quejas sobre cómo nuestra organización gestiona datos personales, en la


© All rights reserved by Heiko Maniero.

parte superior de este documento de transparencia, y que ofrecemos un remedio legal adecuado y gratuito.

Informamos a todas las personas afectadas de que nuestra empresa está sujeta a las facultades de investigación y ejecución de la Federal Trade Commission (FTC).

Las personas afectadas tienen la opción, bajo ciertas condiciones, de solicitar un arbitraje vinculante. Nuestra organización está obligada a resolver reclamaciones y cumplir con las condiciones según el Anexo I de los DPF-Principals, siempre que la persona afectada haya solicitado un arbitraje vinculante notificando a nuestra organización y se hayan cumplido los procedimientos y condiciones según el Anexo I de los Principals.

Informamos por este medio a todas las personas afectadas sobre la responsabilidad de nuestra organización en caso de transferencia de datos personales a terceros.

Para preguntas de las personas afectadas o de las autoridades de supervisión de protección de datos, hemos nombrado a los representantes locales mencionados en la parte superior de este documento de transparencia.

Ofrecemos la opción de elegir (Opt-out), si sus datos personales (i) serán compartidos con terceros o (ii) serán utilizados para un propósito sustancialmente diferente de aquel para el que fueron originalmente recopilados o posteriormente autorizados por usted. El mecanismo claramente visible y fácilmente accesible para ejercer su derecho de elección es contactar a nuestro Oficial de Protección de Datos (DSB) por correo electrónico. Usted no tiene opción, y no estamos obligados, cuando los datos se comparten con un tercero que actúa como agente o procesador en nuestro nombre y siguiendo nuestras instrucciones. Sin embargo, siempre firmamos un contrato con dicho agente o procesador.

Para datos sensibles (es decir, datos personales que incluyen información sobre el estado de salud, origen racial o étnico, opiniones políticas, creencias religiosas o filosóficas, membresía sindical o información sobre la vida sexual de la persona), obtenemos su consentimiento explícito (Opt-in) si estos datos (i) van a ser compartidos o (ii) van a ser utilizados para un propósito diferente al que fueron originalmente recopilados o para el que usted posteriormente dio su consentimiento al hacer su elección de Opt-in. Además, tratamos todos los datos personales que recibimos de terceros como sensibles si el tercero los ha identificado y tratado como tales.

Le informamos sobre la necesidad de divulgar datos personales en respuesta a solicitudes legales de autoridades, incluyendo el cumplimiento de requisitos de seguridad nacional o aplicación de la ley.

Al transferir datos personales a un tercero que actúa como controlador, cumplimos con los Principals de notificación y elección. Además, firmamos un contrato con el tercero responsable del procesamiento que estipula que esos datos solo pueden ser procesados para fines limitados y específicos de acuerdo con el consentimiento que usted proporcionó y que el receptor proporciona el mismo nivel de protección que los Principals del DPF y nos notifica si determina que ya no puede cumplir con esta obligación. El contrato


© All rights reserved by Heiko Maniero.

estipula que el tercero que actúa como controlador debe cesar el procesamiento o tomar otras medidas razonables y adecuadas para remediar la situación si se hace tal determinación.

Al transferir datos personales a un tercero que actúa como agente o procesador, (i) solo transferimos esos datos para fines limitados y específicos; (ii) nos aseguramos de que el agente o procesador esté obligado a proporcionar al menos el mismo nivel de protección de datos requerido por los DPF-Principals; (iii) tomamos medidas razonables y adecuadas para asegurar que el agente o procesador realmente procese los datos personales transferidos de una manera que sea consistente con nuestras obligaciones bajo los DPF-Principals; (iv) exigimos que el agente o procesador nos notifique si determina que ya no puede cumplir con su obligación de proporcionar el mismo nivel de protección requerido por los DPF-Principals; (v) tras una notificación, también bajo (iv), tomamos medidas razonables y adecuadas para detener el procesamiento no autorizado y remediar la situación; y (vi) proporcionamos al DPF Department, a solicitud, un resumen o un ejemplar representativo de las disposiciones relevantes de privacidad de nuestro contrato con ese agente.

En conformidad con el EU-U.S. DPF y/o la UK Extension to the EU-U.S. DPF y/o el Swiss-U.S. DPF, nuestra organización se compromete a cooperar con el panel establecido por las autoridades de protección de datos de la UE y el Information Commissioner's Office (ICO) del Reino Unido y el Comisionado Federal de Protección de Datos y Transparencia Pública (EDÖB) de Suiza, y a seguir sus consejos respecto a quejas no resueltas sobre nuestro manejo de datos personales que recibimos en relación con el empleo bajo el EU-U.S. DPF, la UK Extension to the EU-U.S. DPF y el Swiss-U.S. DPF.

Todos los interesados que se encuentren temporalmente en la Unión Europea (UE), el Espacio Económico Europeo (EEE) o el Reino Unido, o que tengan allí su domicilio o residencia habitual, tienen los derechos y los derechos del interesado que se publican en nuestro Documento de Transparencia, que también se derivan de los artículos 15 a 22 del GDPR, incluido el derecho de acceso a los datos personales. Hemos publicado esta información en todos los idiomas de la UE y del EEE. La versión en inglés se aplica al Reino Unido.

Todos los interesados que residan temporalmente en Suiza o tengan allí su domicilio o residencia habitual gozan de los derechos y garantías previstos en la Ley suiza de protección de datos (LPD) y en el Reglamento suizo de protección de datos (RGPD) que se publican en nuestro Documento de Transparencia, incluido el derecho de acceso a los datos personales. Hemos facilitado esta información en las tres lenguas oficiales de Suiza (alemán, italiano y francés).


© All rights reserved by Heiko Maniero.

# FRENCH: Information sur le traitement des données à caractère personnel (Articles 13 et 14 RGPD)

Madame ou Monsieur,

Les données à caractère personnel de chaque personne qui est à une relation contractuelle, précontractuelle ou une autre relation avec note entreprise méritent une protection particulière. Notre but est de maintenir la protection des données à un niveau élevé. Nous développons régulièrement nos concepts de protection et de sécurité des données.

Bien entendu, nous respectons les dispositions statutaires sur la protection des données. Selon les articles 13 et 14 RGPD, les responsables du traitement respectent des exigences des informations spécifiques quand ils traitement des données à caractère personnel. Ce document remplit ces conditions.

La terminologie des réglementslégales est compliquée. Malheureusement, l'utilisation de termes juridiques ne pouvait pas être évitée dans la préparation de ce document. Par conséquent, nous voulons souligner que vous êtes toujours bienvenues pour nous contacter de toutes questions concernant ce document, les termes utilisés ou les formulations.

## I. Informations à fournir lorsque des données à caractère personnel sont collectées auprès de la personne concernée (Article 13 RGPD)

### A. Identité et coordonnées du responsable du traitement (art. 13(1) lit. a RGPD)

Voir au-dessus

### B. Coordonnées du délégué à la protection des données (art. 13(1) lit. b RGPD)

Voir au-dessus

### C. Finalités du traitement auquel sont destinées les données à caractère personnel ainsi que la base juridique du traitement (art. 13(1) lit. c RGPD)

La finalité du traitement des données à caractère personnelles le traitement de toutes opérations concernant le responsable du traitement, les clients, les clientes potentiels, les partenaires commerciaux ou d'autres relations contractuelles ou précontractuelles entre les équipes désignés (au sens le plus large) ou des obligations légales du responsable du traitement.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

L'article 6(1) lit. a RGPD sert comme la base légale des opérations du traitement pour lesquels nous obtenons le consentement à une finalité spécifique du traitement. Si le traitement des données a caractère personnel est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie, le cas échéant, pour exemple, quand le traitement est nécessaire à la fourniture de biens ou à la fourniture de tout autre service, la base du traitement est l'article 6(1) lit. B RGPD.

Dans de rares cas, le traitement de données à caractère personnel peut être nécessaire pour protéger les intérêts vitaux de la personne concernée ou d'une autre personne physique. Ce serait le cas, par exemple, si un visiteur était blessé dans notre entreprise et que son nom, son âge, ses données d'assurance maladie ou d'autres informations vitales devraient être transmises à un médecin, à un hôpital ou à une autre tierce partie. Le traitement serait fondé sur l'art. 6 (1) lit. d RGPD.

Lorsque le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement, la base juridique est l'art. 6(1) lit. e RGPD.

Finalement, les opérations de traitement peuvent être fondes sur l'article 6(1) lit. f RGPD. Cette base légale est utilisée pour les opérations de traitement qui ne sont pas couvertes par l'une des bases légales susmentionnés, si le traitement est nécessaire aux fins des intérêts légitimes poursuivis par notre entreprise ou par un tiers, sauf si ces intérêts sont outrepassés par des libertés et droits fondamentaux de la personne concernée qui nécessitent la protection de données à caractère personnel. De tels opérations du traitement sont particulièrement autorisées car ils ont été spécifiquement mentionnés par le législateur européen. Un tel intérêt légitime pourrait, par exemple, exister lorsqu'il existe une relation pertinente et appropriée entre la personne concernée et le responsable du traitement dans des situations telles que celles où la personne concernée est un client du responsable du traitement ou est à son service.

## D. Lorsque le traitement est fondé sur l'article 6(1) lit. f, les intérêts légitimes poursuivis par le responsable du traitement ou par un tiers (article 13(1) lit. d RGPD)

Lorsque le traitement des données à caractère personnel est fondé sur l'article 6(1) point f RGPD notre intérêt légitime est de mener nos activités en faveur du bien-être de tous nos employés et de nos actionnaires.

## E. Catégories des destinataires des données à caractère personnel (art. 13(1) lit. e RGPD)

Autorités publiques


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

Organisations externes

Autres organisations externes

Traitement interne

Traitement intragroupe

Autres organisations

Une liste de nos sous-traitants et de nos destinataires de données dans les pays tiers et, le cas échéant, des organisations internationales est publiée sur notre site web ou peut être demandée gratuitement. Pour obtenir cette liste, veuillez contacter notre délégué à la protection des données.

## F. Destinataires dans un pays tiers et garanties appropriées ou appropriées et moyens permettant d'en obtenir une copie ou lorsqu'ils ont été mis à disposition (Article 13(1) lit. f, 46(2) lit. c RGPD)

Toutes les entreprises et filiales faisant partie de notre groupe (ci-après dénommées "entreprises du groupe") ayant leur siège ou un bureau dans un pays tiers peuvent appartenir aux destinataires des données à caractère personnel. Une liste des toutes les entreprises du groupe ou de tous destinataires peut nous être demandée.

Selon l'article 46(1) RGPD, un responsable du traitement or sous-traitant peut transférer des données caractère personnel vers un pays tiers si le responsable du traitement ou le sous-traitant a mis en place les garanties appropriées, et à condition que des droits applicables des personnes concernées et des recours légaux efficaces soient disponibles. Des garanties appropriées peuvent être fournies sans autorisation spécifique d'une autorité de surveillance au moyen de clauses contractuelles types (art. 46(2) lit. c RGPD).

Les clauses contractuelles types de l'Union Européenne ou d'autres garanties appropriées sont convenues avec tous les destinataires de pays tiers avant la première transmission de données à caractère personnel. Par conséquence, il est garanti que des garanties appropriées, des droits applicables des personnes concernées et des recours légaux efficaces pour les personnes concernées sont garantis. Chaque personne concernée peut obtenir une copie des clauses contractuelles types par nous. Les clauses contractuelles types sont aussi disponibles dans le Journal Official de l'Union Européenne.

L'article 45, paragraphe 3, du règlement général sur la protection des données (RGPD) confère à la Commission européenne le pouvoir de décider, au moyen d'un acte d'exécution, qu'un pays tiers assure un niveau de protection adéquat. Cela signifie que le niveau de protection des données à caractère personnel est essentiellement équivalent au niveau de protection au sein de l'UE. Les décisions d'adéquation ont pour effet que les données à caractère personnel peuvent circuler librement de l'UE (et


© All rights reserved by Heiko Maniero.

de la Norvège, du Liechtenstein et de l'Islande) vers un pays tiers sans autres obstacles. Des règles similaires existent pour le Royaume-Uni, la Suisse et certains autres pays.

Lorsque la Commission européenne ou le gouvernement d'un autre pays a décidé qu'un pays tiers assure un niveau de protection adéquat et qu'un cadre valide est en place (par exemple, EU-U.S. Data Privacy Framework, Swiss-U.S. Data Privacy Framework, UK Extension to the EU-U.S. Data Privacy Framework), tous les transferts que nous effectuons vers les membres de ces cadres (par exemple, les entités autocertifiées) sont exclusivement fondés sur l'appartenance de ces entités au cadre respectif. Lorsque nous ou l'une des entités de notre groupe sommes membres d'un tel cadre, tous les transferts à nous ou à l'entité de notre groupe sont exclusivement basés sur l'appartenance de l'entité à ce cadre.

Toute personne concernée peut obtenir une copie des cadres auprès de nous. En outre, les cadres sont également disponibles au Journal officiel de l'Union européenne, dans les documents juridiques publiés ou sur les sites web des autorités de contrôle ou d'autres autorités ou institutions compétentes.

## G. Durée de conservation des données à caractère personnel ou, lorsque ce n'est pas possible, critères pour déterminer cette durée (Article 13(2) lit. a RGPD)

Le critère utilisé pour déterminer la durée de conservation des données à caractère personnel est la durée de conservation statutaire respective. Apres l'expiration de cette durée, les données correspondantes sont systématiquement supprimées, dans la mesure où elles ne sont plus nécessaires à l'exécution du contrat ou à la conclusion d'un contrat.

S'il n'existe pas de délai de conservation légal, le critère est le délai de conservation contractuel ou interne.

## H. Existence du droit de demander au responsable du traitement l'accès aux données à caractère personnel, la rectification ou l'effacement de celles-ci, ou une limitation du traitement relatif à la personne concernée, ou du droit de s'opposer au traitement et du droit à la portabilité des données (Article 13(2) lit. b RGPD)

Toutes les personnes concernées ont les droits suivants:

***Droit d'accès***

La personne concernée a le droit d'obtenir du responsable du traitement l'accès aux données à caractère personnel. Il est possible d'accéder aux données traitées par nous. Le droit peut être exercé facilement à des intervalles raisonnables, sans connaissance préalable et sans justification, de la légalité du traitement (Récital 63 RGPD). Ce droit résulte de l'article 15 RGPD. La personne concernée peut nous contacter afin d'exercer le droit d'accès.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

***Droit de rectification***

Selon l'article 16 phrase 1 RGPD, la personne concernée a le droit d'obtenir du responsable du traitement, dans les meilleurs délais, la rectification des données à caractère personnel la concernant qui sont inexactes. En outre, selon l'article 16 phase 2 RGPD la personne concernée a le droit d'obtenir que les données à caractère personnel incomplètes soient complétées, y compris en fournissant une déclaration complémentaire. La personne concernée peut nous contacter afin d'exercer le droit de rectification.

***Droit à l'effacement («droit à l'oubli»)***

En outre, les personnes concernées ont le droit à l'effacement et à l'oubli en vertu de l'art. 17 GDPR. Ce droit peut également être exercé en nous contactant. À ce stade, cependant, nous tenons à souligner que ce droit ne s'applique pas dans la mesure où le traitement est nécessaire pour respecter une obligation légale à laquelle notre entreprise est soumise (article 17(3) lit. b RGPD).

***Droit à la limitation du traitement***

Selon l'article 18 RGPD, la personne concernée a le droit d'obtenir du responsable du traitement la limitation du traitement. La limitation du traitement peut être demande si l'un des éléments de l'article 18(1) lit. a-d s'applique. La personne concernée peut nous contacter afin d'exercer le droit à la limitation du traitement.

***Droit d'opposition***

En outre, l'art. 21 GDPR garantit le droit d'opposition. La personne concernée peut nous contacter pour exercer le droit d'opposition.

***Droit à la portabilité des données***

L'article 20 RGPD garantit le droit a la portabilité des données de la personne concernée. En vertu de cette disposition, la personne concernée a dans les conditions de l'article 20(1) lit. a et b RGPD le droit de recevoir les données à caractère personnel le concernant, qu'elles ont fournies à un responsable du traitement, dans un format structuré, couramment utilisé et lisible par machine, et ont le droit de transmettre ces données à un autre responsable du traitement sans que le responsable du traitement auquel les données à caractère personnel ont été communiquées y fasse obstacle. La personne concernée peut nous contacter afin d'exercer le droit à la portabilité de données.

## I. Existence du droit de retirer son consentement à tout moment, sans porter atteinte à la licéité du traitement fondé sur le consentement effectué avant le retrait de celui-ci, lorsque le traitement est fondé sur l'article 6(1)(a), ou sur l'article 9(2)(a)(Article 13(3) lit. c RGPD)

Si le traitement des données à caractère personnel est fondé sur l'article 6(1) lit. a RGPD, quel soit le cas, si la personne concernée a donné son consentement pour le traitement des données à caractère personnel pour une ou plusieurs finalités spécifiques ou si il est fonde sur l'article 9(2) lit. a RGPD, qui


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

régit le consentement explicite au traitement de catégories particulières de données à caractère personnel, la personne concernée a selon l'article 7(3) phrase 1 RGPD le droit de retirer son consentement à tout moment.

Le retrait du consentement ne compromet pas la licéité du traitement fondé sur le consentement effectué avant ce retrait (art. 7(3) phrase 2 RGPD). Il est aussi simple de retirer que de donner son consentement) art. 7(3) phrase 4 RGPD). Par conséquent, le retrait du consentement peut toujours se dérouler de la même manière que le consentement ou de toute autre manière, considérée par la personne concernée comme plus simple. Dans la société de l'information d'aujourd'hui, le moyen le plus simple de retirer son consentement consiste à utiliser un simple courrier électronique. Si la personne concernée souhaite retirer son consentement, un simple courrier électronique nous suffit. Par ailleurs, la personne concernée peut choisir par tout autre moyen de communiquer son retrait de consentement.

## J. Droit d'introduire une réclamation auprès d'une autorité de contrôle (Article 13(2) lit. d, 77(1) RGPD)

Comme le responsable du traitement, nous sommes obligés d'informer la personne concernée du droit d'introduire une réclamation auprès d'une autorité de contrôle (art. 13(2) lit. d RGPD). Le droit d'introduire une réclamation auprès une autorité de contrôle est régi par l'article 77(1) RGPD. Selon cette disposition, sans préjudice de tout autre recours administratif ou extrajudiciaire, toute personne concernée a le droit d'introduire une réclamation auprès d'une autorité de contrôle, en particulier dans l'État membre dans lequel se trouve sa résidence habituelle, son lieu de travail ou le lieu où la violation aurait été commise, si elle considère que le traitement de données à caractère personnel la concernant constitue une violation du présent règlement. Le droit d'introduire une réclamation auprès une autorité de contrôle n'était limite que seulement par le droit de l'Union Européenne de manière à ce qu'il ne puisse être exercé que devant une seule autorité de contrôle (Récital 141 phrase 1 RGPD). Cette règle vise à éviter les doubles plaintes de la même personne concernée dans la même affaire. Si une personne concernée souhaite introduire une réclamation nous concernant, nous demandons que vous contactiez une seule autorité de contrôle.

## K. Fourniture de données à caractère personnel contractuel; Obligation pour la conclusion d'un contrat; Obligation de la personne concernée de fournir les données à caractère personnel; Conséquences éventuelles de la non-fourniture des données (article 13(2) lit. e RGPD)

Nous clarifions que la que la fourniture de données à caractère personnel est en partie requise par la loi (par exemple, la réglementation fiscale) ou peut également résulter de dispositions contractuelles (par exemple, des informations sur le partenaire contractuel).

Quelques fois, il peut être nécessaire de conclure un contrat prévoyant que la personne concernée nous fournisse des données à caractère personnel, qui doivent ensuite être traitées par nous. La personne


© All rights reserved by Heiko Maniero.

concernée est par exemple obligée de nous fournir des données à caractère personnel lorsque notre société signe un contrat avec elle. La non-communication des données à caractère personnel aurait pour conséquence que le contrat avec la personne concernée ne pourrait pas être conclu.

### L. Existence d'une prise de décision automatisée, y compris profilage, visée à l'article 22 (1) et (4) RGPD, et, au moins en pareils cas, informations utiles concernant la logique sous-jacente, ainsi que l'importance et les conséquences prévues de ce traitement pour la personne concernée (art. 13(2) lit. f RGPD)

En tant qu'entreprise responsable, nous ne recourons généralement pas à la prise de décision automatisée ou au profilage. Si, dans des cas exceptionnels, nous procédons à une prise de décision automatisée ou à un profilage, nous en informons la personne concernée, soit séparément, soit par le biais d'une sous-section de notre politique de confidentialité (sur notre site web). Dans ce cas, les dispositions suivantes s'appliquent :

La prise de décision automatisée - y compris le profilage - peut avoir lieu si (1) elle est nécessaire à la conclusion ou à l'exécution d'un contrat entre la personne concernée et nous, ou (2) elle est autorisée par le droit de l'Union ou de l'État membre auquel nous sommes soumis et qui prévoit également des mesures appropriées pour la sauvegarde des droits et libertés et des intérêts légitimes de la personne concernée, ou (3) elle est fondée sur le consentement explicite de la personne concernée.

Dans les cas visés à l'article 22, paragraphe 2, points a) et c), du RGPD, nous mettons en œuvre des mesures appropriées pour la sauvegarde des droits et libertés et des intérêts légitimes de la personne concernée. Dans ces cas, vous avez le droit d'obtenir une intervention humaine de la part du responsable du traitement, d'exprimer votre point de vue et de contester la décision.

Des informations utiles sur la logique mise en œuvre, ainsi que sur l'importance et les conséquences envisagées de ce traitement pour la personne concernée, sont fournies dans notre politique de confidentialité.

## II. Informations à fournir lorsque les données à caractère personnel n'ont pas été collectées auprès de la personne concernée (Article 14 RGPD)

### A. Identité et coordonnées du responsable du traitement (art. 13(1) lit. a RGPD)

Voir au-dessus

### B. Coordonnées du délégué à la protection des données (art. 13(1) lit. b RGPD)

Voir au-dessus


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## C. Les finalités du traitement auquel sont destinées les données à caractère personnel ainsi que la base juridique du traitement (article 14(1) lit. c RGPD)

La finalité du traitement des données à caractère personnelles le traitement de toutes opérations concernant le responsable du traitement, les clients, les clientes potentiels, les partenaires commerciaux ou d'autres relations contractuelles ou précontractuelles entre les équipes désignés (au sens le plus large) ou des obligations légales du responsable du traitement.

Si le traitement est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie comme par exemple lorsque des opérations de traitement sont nécessaires à la fourniture de biens ou à la fourniture de tout autre service, le traitement est fondé sur l'article 6(1) lit. b RGPD. La même s'applique lorsque le traitement est nécessaire à l'exécution de mesures précontractuelles prises comme par exemple en cas des demandes concernant nos produits ou services. Si notre société est soumise à une obligation légale imposant le traitement de données à caractère personnel, notamment pour le respect des obligations fiscales, le traitement est fondé sur l'article 6(1) lit. c RGPD.

Dans de rares cas, le traitement de données à caractère personnel peut être nécessaire pour protéger les intérêts vitaux de la personne concernée ou d'une autre personne physique. Ce serait le cas, par exemple, si un visiteur était blessé dans notre entreprise et que son nom, son âge, ses données d'assurance maladie ou d'autres informations vitales devraient être transmises à un médecin, à un hôpital ou à une autre tierce partie. Le traitement serait fondé sur l'art. 6 (1) lit. d GDPR.

Lorsque le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement, la base juridique est l'art. 6(1) lit. e RGPD.

Finalement, les opérations de traitement peuvent être fondes sur l'article 6(1) lit. f RGPD. Cette base légale est utilisée pour les opérations de traitement qui ne sont pas couvertes par l'une des bases légales susmentionnés, si le traitement est nécessaire aux fins des intérêts légitimes poursuivis par notre entreprise ou par un tiers, sauf si ces intérêts sont outrepassés par des libertés et droits fondamentaux de la personne concernée qui nécessitent la protection de données à caractère personnel. De tels opérations du traitement sont particulièrement autorisés car ils ont été spécifiquement mentionnés par le législateur européen. Il a considéré qu'un tel intérêt légitime pourrait exister lorsqu'il existe où la personne concernée est un client du responsable du traitement (Récital 47 phrase 2 RGPD).

## D. Les catégories de données à caractère personnel concernées (art. 14(1) lit. d RGPD)

Données des clientes


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

Données des clientes potentielles

Données des employés

Données des fournisseurs

## E. Catégories des destinataires des données à caractère personnel (art. 14(1) lit. e RGPD)

Autorités publiques

Organisations externes

Autres organisations externes

Traitement interne

Traitement intragroupe

Autres organisations

Une liste de nos sous-traitants et de nos destinataires de données dans les pays tiers et, le cas échéant, des organisations internationales est publiée sur notre site web ou peut être demandée gratuitement. Pour obtenir cette liste, veuillez contacter notre délégué à la protection des données.

## F. Destinataires dans pays tiers ou une organisation internationale, et garanties appropriées ou adaptées et les moyens d'en obtenir une copie ou l'endroit où elles ont été mises à disposition (art. 14(1) lit. f RGPD, 46(1), 46(2) lit. c RGPD)

Toutes les entreprises et filiales faisant partie de notre groupe (ci-après dénommées "entreprises du groupe") ayant leur siège ou un bureau dans un pays tiers peuvent appartenir aux destinataires des données à caractère personnel. Une liste des toutes les entreprises du groupe ou de tous destinataires peut nous être demandée.

Selon l'article 46(1) RGPD, un responsable du traitement or sous-traitant peut transférer des données à caractère personnel vers un pays tiers si le responsable du traitement ou le sous-traitant a mis en place les garanties appropriées, et à condition que des droits applicables des personnes concernées et des recours légaux efficaces soient disponibles. Des garanties appropriées peuvent être fournies sans autorisation spécifique d'une autorité de surveillance au moyen de clauses contractuelles types (art. 46(2) lit. c RGPD).


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

Les clauses contractuelles types de l'Union Européenne ou d'autres garanties appropriées sont convenues avec tous les destinataires de pays tiers avant la première transmission de données à caractère personnel. Par conséquence, il est garanti que des garanties appropriées, des droits applicables des personnes concernées et des recours légaux efficaces pour les personnes concernées sont garantis. Chaque personne concernée peut obtenir une copie des clauses contractuelles types par nous. Les clauses contractuelles types sont aussi disponibles dans le Journal Official de l'Union Européenne.

L'article 45, paragraphe 3, du règlement général sur la protection des données (RGPD) confère à la Commission européenne le pouvoir de décider, au moyen d'un acte d'exécution, qu'un pays tiers assure un niveau de protection adéquat. Cela signifie que le niveau de protection des données à caractère personnel est essentiellement équivalent au niveau de protection au sein de l'UE. Les décisions d'adéquation ont pour effet que les données à caractère personnel peuvent circuler librement de l'UE (et de la Norvège, du Liechtenstein et de l'Islande) vers un pays tiers sans autres obstacles. Des règles similaires existent pour le Royaume-Uni, la Suisse et certains autres pays.

Lorsque la Commission européenne ou le gouvernement d'un autre pays a décidé qu'un pays tiers assure un niveau de protection adéquat et qu'un cadre valide est en place (par exemple, EU-U.S. Data Privacy Framework, Swiss-U.S. Data Privacy Framework, UK Extension to the EU-U.S. Data Privacy Framework), tous les transferts que nous effectuons vers les membres de ces cadres (par exemple, les entités autocertifiées) sont exclusivement fondés sur l'appartenance de ces entités au cadre respectif. Lorsque nous ou l'une des entités de notre groupe sommes membres d'un tel cadre, tous les transferts à nous ou à l'entité de notre groupe sont exclusivement basés sur l'appartenance de l'entité à ce cadre.

Toute personne concernée peut obtenir une copie des cadres auprès de nous. En outre, les cadres sont également disponibles au Journal officiel de l'Union européenne, dans les documents juridiques publiés ou sur les sites web des autorités de contrôle ou d'autres autorités ou institutions compétentes.

## G. Durée pendant laquelle les données à caractère personnel seront conservées ou, lorsque ce n'est pas possible, les critères utilisés pour déterminer cette durée (art. 14(1) lit. a RGPD)

Le critère utilisé pour déterminer la durée de conservation des données à caractère personnel est la durée de conservation statutaire respective. Apres l'expiration de cette durée, les données correspondantes sont systématiquement supprimées, dans la mesure où elles ne sont plus nécessaires à l'exécution du contrat ou à la conclusion d'un contrat.

S'il n'existe pas de délai de conservation légal, le critère est le délai de conservation contractuel ou interne.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## H. Les intérêts légitimes poursuivis par le responsable du traitement ou par un tiers, lorsque le traitement est fondé sur l'article 6(1) lit. f RGPD (art. 14(2) lit. b RGPD)

Selon l'article 6(1) lit. f RGPD, le traitement n'est licite que le traitement est nécessaire aux fins des intérêts légitimes poursuivis par le responsable du traitement ou par un tiers, à moins que ne prévalent les intérêts ou les libertés et droits fondamentaux de la personne concernée qui exigent une protection des données à caractère personnel. Selon le récital 47 phrase 2 RGPD, un tel intérêt légitime pourrait exister lorsqu'il existe une relation pertinente et appropriée entre la personne concernée et le responsable du traitement, par exemple où la personne concernée est un client du responsable du traitement. Dans tous les cas où notre société traite des données à caractère personnel sur la base de l'article 6(1) lit. f RGPD, notre intérêt légitime est de mener nos activités en faveur du bien-être de tous nos employés et de nos actionnaires.

## I. Existence du droit de demander au responsable du traitement l'accès aux données à caractère personnel, la rectification ou l'effacement de celles-ci, ou une limitation du traitement relatif à la personne concernée, ou du droit de s'opposer au traitement et du droit à la portabilité des données (Article 13(2) lit.b RGPD)

Toutes les personnes concernées ont les droits suivants:

***Droit d'accès***

La personne concernée a le droit d'obtenir du responsable du traitement l'accès aux données à caractère personnel. Il est possible d'accéder aux données traitées par nous. Le droit peut être exercé facilement à des intervalles raisonnables, sans connaissance préalable et sans justification, de la légalité du traitement (Récital 63 RGPD). Ce droit résulte de l'article 15 RGPD. La personne concernée peut nous contacter afin d'exercer le droit d'accès.

***Droit de rectification***

Selon l'article 16 phrase 1 RGPD, la personne concernée a le droit d'obtenir du responsable du traitement, dans les meilleurs délais, la rectification des données à caractère personnel la concernant qui sont inexactes. En outre, selon l'article 16 phase 2 RGPD la personne concernée a le droit d'obtenir que les données à caractère personnel incomplètes soient complétées, y compris en fournissant une déclaration complémentaire. La personne concernée peut nous contacter afin d'exercer le droit de rectification.

***Droit à l'effacement («droit à l'oubli»)***

En outre, les personnes concernées ont le droit à l'effacement et à l'oubli en vertu de l'art. 17 GDPR. Ce droit peut également être exercé en nous contactant. À ce stade, cependant, nous tenons à souligner que ce droit ne s'applique pas dans la mesure où le traitement est nécessaire pour respecter une obligation légale à laquelle notre entreprise est soumise (article 17(3) lit. b RGPD).


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

***Droit à la limitation du traitement***

Selon l'article 18 RGPD, la personne concernée a le droit d'obtenir du responsable du traitement la limitation du traitement. La limitation du traitement peut être demande si l'un des éléments de l'article 18(1) lit. a-d s'appliquent. La personne concernée peut nous contacter afin d'exercer le droit à la limitation du traitement.

***Droit d'opposition***

En outre, l'art. 21 GDPR garantit le droit d'opposition. La personne concernée peut nous contacter pour exercer le droit d'opposition.

***Droit à la portabilité des données***

L'article 20 RGPD garantit le droit à la portabilité des données de la personne concernée. En vertu de cette disposition, la personne concernée a dans les conditions de l'article 20(1) lit. a et b RGPD le droit de recevoir les données à caractère personnel le concernant, qu'elles ont fournies à un responsable du traitement, dans un format structuré, couramment utilisé et lisible par machine, et ont le droit de transmettre ces données à un autre responsable du traitement sans que le responsable du traitement auquel les données à caractère personnel ont été communiquées y fasse obstacle. La personne concernée peut nous contacter afin d'exercer le droit à la portabilité de données.

## J. Existence du droit de retirer le consentement à tout moment, sans porter atteinte à la licéité du traitement fondé sur le consentement effectué avant le retrait de celui-ci, lorsque le traitement est fondé sur l'article 6(1) lit. a, ou sur l'article 9(2) lit. a RGPD (art. 14 (2) lit. d RGPD)

Si le traitement des données à caractère personnel est fondé sur l'article 6(1) lit. a RGPD, quel soit le cas, si la personne concernée a donné son consentement pour le traitement des données à caractère personnel pour une ou plusieurs finalités spécifiques ou si il est fonde sur l'article 9(2) lit. a RGPD, qui régit le consentement explicite au traitement de catégories particulières de données à caractère personnel, la personne concernée a selon l'article 7(3) phrase 1 RGPD le droit de retirer son consentement à tout moment.

Le retrait du consentement ne compromet pas la licéité du traitement fondé sur le consentement effectué avant ce retrait (art. 7(3) phrase 2 RGPD).Il est aussi simple de retirer que de donner son consentement) art. 7(3) phrase 4 RGPD). Par conséquent, le retrait du consentement peut toujours se dérouler de la même manière que le consentement ou de toute autre manière, considérée par la personne concernée comme plus simple. Dans la société de l'information d'aujourd'hui, le moyen le plus simple de retirer son consentement consiste à utiliser un simple courrier électronique. Si la personne concernée souhaite retirer son consentement, un simple courrier électronique nous suffit. Par ailleurs, la personne concernée peut choisir par tout autre moyen de communiquer son retrait de consentement.


© All rights reserved by Heiko Maniero.

## K. Droit d'introduire une réclamation auprès d'une autorité de contrôle (Article 13(2) lit. d, 77(1) RGPD)

Comme le responsable du traitement, nous sommes obligés d'informer la personne concernée du droit d'introduire une réclamation auprès d'une autorité de contrôle (art. 14(2) lit. e RGPD). Le droit d'introduire une réclamation auprès une autorité de contrôle est régi par l'article 77(1) RGPD. Selon cette disposition, sans préjudice de tout autre recours administratif ou extrajudiciaire, toute personne concernée a le droit d'introduire une réclamation auprès d'une autorité de contrôle, en particulier dans l'État membre dans lequel se trouve sa résidence habituelle, son lieu de travail ou le lieu où la violation aurait été commise, si elle considère que le traitement de données à caractère personnel la concernant constitue une violation du présent règlement. Le droit d'introduire une réclamation auprès une autorité de contrôle n'était limite que seulement par le droit de l'Union Européenne de manière à ce qu'il ne puisse être exercé que devant une seule autorité de contrôle (Récital 141 phrase 1 RGPD). Cette règle vise à éviter les doubles plaintes de la même personne concernée dans la même affaire. Si une personne concernée souhaite introduire une réclamation nous concernant, nous demandons que vous contactiez une seule autorité de contrôle.

## L. La source d'où proviennent les données à caractère personnel et, le cas échéant, une mention indiquant qu'elles sont issues ou non de sources accessibles au public (art. 14(2) lit. f RGPD)

En principe, les données à caractère personnel sont collectées directement auprès de la personne concernée ou en coopération avec une autorité (par exemple, la récupération de données à partir d'un registre officiel). Les autres données relatives aux personnes concernées proviennent de transferts des entreprises du groupe. Dans le contexte de ces informations générales, la désignation des sources exactes à l'origine des données à caractère personnel est impossible ou impliquerait un effort disproportionné au sens de l'art. 14 (5) lit. b GDPR. En principe, nous ne collectons pas de données à caractère personnel à partir de sources accessibles au public.

Toute personne concernée peut nous contacter à tout moment pour obtenir des informations plus détaillées sur les sources exactes des données à caractère personnel la concernant. Lorsque l'origine des données à caractère personnel n'a pas pu être communiquée à la personne concernée parce que plusieurs sources ont été utilisées, des informations générales devraient être fournies (récital 61 phrase 4 RGPD).


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

### M. Existence d'une prise de décision automatisée, y compris profilage, visée à l'article 22 (1) et (4) RGPD, et, au moins en pareils cas, informations utiles concernant la logique sous-jacente, ainsi que l'importance et les conséquences prévues de ce traitement pour la personne concernée (art. 14(2) lit. g RGPD)

En tant qu'entreprise responsable, nous ne recourons généralement pas à la prise de décision automatisée ou au profilage. Si, dans des cas exceptionnels, nous procédons à une prise de décision automatisée ou à un profilage, nous en informons la personne concernée, soit séparément, soit par le biais d'une sous-section de notre politique de confidentialité (sur notre site web). Dans ce cas, les dispositions suivantes s'appliquent :

La prise de décision automatisée - y compris le profilage - peut avoir lieu si (1) elle est nécessaire à la conclusion ou à l'exécution d'un contrat entre la personne concernée et nous, ou (2) elle est autorisée par le droit de l'Union ou de l'État membre auquel nous sommes soumis et qui prévoit également des mesures appropriées pour la sauvegarde des droits et libertés et des intérêts légitimes de la personne concernée, ou (3) elle est fondée sur le consentement explicite de la personne concernée.

Dans les cas visés à l'article 22, paragraphe 2, points a) et c), du RGPD, nous mettons en œuvre des mesures appropriées pour la sauvegarde des droits et libertés et des intérêts légitimes de la personne concernée. Dans ces cas, vous avez le droit d'obtenir une intervention humaine de la part du responsable du traitement, d'exprimer votre point de vue et de contester la décision.

Des informations utiles sur la logique mise en œuvre, ainsi que sur l'importance et les conséquences envisagées de ce traitement pour la personne concernée, sont fournies dans notre politique de confidentialité.

## III. EU-U.S. Data Privacy Framework (EU-U.S. DPF), UK Extension to the EU-U.S. DPF, Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF)

Si notre organisation est un membre certifié de l'EU-U.S. Data Privacy Framework (EU-U.S. DPF) et/ou de la UK Extension to the EU-U.S. DPF et/ou du Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF), les dispositions suivantes s'appliquent:

Nous adhérons à l'EU-U.S. Data Privacy Framework (EU-U.S. DPF) et à la UK Extension to the EU-U.S. DPF ainsi qu'au Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF), tel qu'établi par le U.S. Department of Commerce. Notre entreprise a confirmé au U.S. Department of Commerce qu'elle respecte les EU-U.S. Data Privacy Framework Principles (EU-U.S. DPF Principles) concernant le traitement des données personnelles qu'elle reçoit de l'Union européenne et du Royaume-Uni en vertu de l'EU-U.S. DPF et de la UK Extension to the EU-U.S. DPF. Notre entreprise a également confirmé qu'elle respecte les Swiss-U.S. Data Privacy Framework Principles (Swiss-U.S. DPF Principles)


© All rights reserved by Heiko Maniero.

concernant le traitement des données personnelles qu'elle reçoit de la Suisse sous le Swiss-U.S. DPF. En cas de contradiction entre les dispositions de notre politique de confidentialité et les EU-U.S. DPF Principles et/ou les Swiss-U.S. DPF Principles, les Principles prévalent.

Pour en savoir plus sur le programme Data Privacy Framework (DPF) et consulter notre certification, veuillez visiter https://www.dataprivacyframework.gov/.

Les autres entités américaines ou filiales de notre entreprise qui adhèrent également aux EU-U.S. DPF Principals, y compris la UK Extension to the EU-U.S. DPF et les Swiss-U.S. DPF Principals, si elles existent, sont mentionnées dans notre politique de confidentialité.

Conformément à l'EU-U.S. DPF, à la UK Extension to the EU-U.S. DPF et au Swiss-U.S. DPF, notre entreprise s'engage à coopérer avec le comité établi par les autorités de protection des données de l'UE, le UK Information Commissioner's Office (ICO) et le Préposé fédéral à la protection des données et à la transparence (EDÖB) de Suisse, et à suivre leurs conseils concernant les plaintes non résolues sur notre gestion des données personnelles que nous recevons sous l'EU-U.S. DPF, la UK Extension to the EU-U.S. DPF et le Swiss-U.S. DPF.

Nous informons les personnes concernées des autorités européennes de protection des données compétentes pour traiter les plaintes concernant la manière dont notre organisation gère les données personnelles, en haut de ce document de transparence, et que nous offrons un recours juridique adéquat et gratuit.

Nous informons toutes les personnes concernées que notre entreprise est soumise aux pouvoirs d'enquête et de contrôle de la Federal Trade Commission (FTC).

Les personnes affectées ont la possibilité, sous certaines conditions, de demander un arbitrage contraignant. Notre organisation est tenue de régler les réclamations et de respecter les conditions énoncées à l'Annexe I des DPF-Principals, à condition que la personne concernée ait demandé un arbitrage contraignant en notifiant notre organisation et que les procédures et conditions de l'Annexe I des Principals aient été respectées.

Nous informons par la présente toutes les personnes concernées de la responsabilité de notre organisation en cas de transfert de données personnelles à des tiers.

Pour les questions des personnes affectées ou des autorités de contrôle de la protection des données, nous avons nommé les représentants locaux mentionnés en haut de ce document de transparence.

Nous vous offrons la possibilité de choisir (Opt-out), si vos données personnelles (i) doivent être partagées avec des tiers ou (ii) doivent être utilisées à des fins substantiellement différentes de celles pour lesquelles elles ont été initialement collectées ou ultérieurement autorisées par vous. Le mécanisme clair, bien visible et facilement accessible pour exercer votre droit de choix consiste à contacter notre responsable de la protection des données (DSB) par courriel. Vous n'avez pas le choix et nous ne sommes pas obligés lorsque les données sont partagées avec un tiers qui agit en tant qu'agent ou


© All rights reserved by Heiko Maniero.

processeur en notre nom et selon nos instructions. Nous concluons cependant toujours un contrat avec un tel agent ou processeur.

Pour les données sensibles (c'est-à-dire les données personnelles incluant des informations sur l'état de santé, l'origine raciale ou ethnique, les opinions politiques, les croyances religieuses ou philosophiques, l'appartenance syndicale ou les informations sur la vie sexuelle de la personne), nous obtenons votre consentement explicite (Opt-in) si ces données (i) doivent être partagées ou (ii) doivent être utilisées à des fins différentes de celles pour lesquelles elles ont été initialement collectées ou pour lesquelles vous avez ensuite donné votre consentement, en faisant votre choix d'Opt-in. De plus, nous traitons toutes les données personnelles que nous recevons de tiers comme sensibles si le tiers les a identifiées et traitées comme telles.

Nous vous informons de la nécessité de divulguer des données personnelles en réponse à des demandes légales des autorités, y compris pour répondre aux exigences de la sécurité nationale ou de l'application de la loi.

Lors du transfert de données personnelles à un tiers qui agit en tant que contrôleur, nous respectons les Principals de notification et de choix. En outre, nous concluons un contrat avec le tiers responsable du traitement qui stipule que ces données ne peuvent être traitées que pour des fins limitées et spécifiées conformément au consentement que vous avez fourni et que le destinataire offre le même niveau de protection que les Principals du DPF et nous informe s'il détermine qu'il ne peut plus remplir cette obligation. Le contrat prévoit que le tiers, qui agit en tant que contrôleur, doit cesser le traitement ou prendre d'autres mesures raisonnables et appropriées pour remédier à la situation si une telle détermination est faite.

Lors du transfert de données personnelles à un tiers qui agit en tant qu'agent ou processeur, (i) nous transférons ces données uniquement à des fins limitées et spécifiées ; (ii) nous nous assurons que l'agent ou le processeur est tenu de fournir au moins le même niveau de protection des données exigé par les DPF-Principals ; (iii) nous prenons des mesures raisonnables et appropriées pour nous assurer que l'agent ou le processeur traite réellement les données personnelles transférées d'une manière conforme à nos obligations en vertu des DPF-Principals ; (iv) nous exigeons que l'agent ou le processeur nous informe s'il détermine qu'il ne peut plus respecter son obligation de fournir le même niveau de protection requis par les DPF-Principals ; (v) après une telle notification, également sous (iv), nous prenons des mesures raisonnables et appropriées pour arrêter le traitement non autorisé et remédier à la situation ; et (vi) nous fournissons au DPF Department, sur demande, un résumé ou un exemplaire représentatif des dispositions pertinentes de confidentialité de notre contrat avec cet agent.

Conformément à l'EU-U.S. DPF et/ou à la UK Extension to the EU-U.S. DPF et/ou au Swiss-U.S. DPF, notre organisation s'engage à coopérer avec le comité établi par les autorités de protection des données de l'UE et le UK Information Commissioner's Office (ICO) ainsi que le Préposé fédéral à la protection des données et à la transparence (EDÖB) de Suisse, et à suivre leurs conseils concernant les plaintes non


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

résolues sur notre gestion des données personnelles que nous recevons en relation avec l'emploi sous l'EU-U.S. DPF, la UK Extension to the EU-U.S. DPF et le Swiss-U.S. DPF.

Toutes les personnes concernées qui se trouvent temporairement dans l'Union européenne (UE), l'Espace économique européen (EEE) ou le Royaume-Uni, ou qui y ont leur domicile ou leur résidence habituelle, bénéficient des droits et des droits des personnes concernées publiés dans notre document de transparence, qui découlent également des articles 15 à 22 du RGPD, y compris le droit d'accès aux données à caractère personnel. Ces informations sont disponibles dans toutes les langues de l'UE et de l'EEE. La version anglaise s'applique au Royaume-Uni.

Toutes les personnes concernées qui résident temporairement en Suisse ou qui y ont leur domicile ou leur résidence habituelle bénéficient des droits et des droits des personnes concernées en vertu de la loi suisse sur la protection des données (LPD) et du règlement suisse sur la protection des données (RGPD) qui sont publiés dans notre document de transparence, y compris le droit d'accès aux données à caractère personnel. Nous avons fourni ces informations dans les trois langues officielles de la Suisse (allemand, italien et français).


© All rights reserved by Heiko Maniero.

# FRENCH: Information sur le traitement des données à caractère personnel des employés et des candidates (Articles 13 et 14 RGPD)

Madame ou Monsieur,

Les données à caractère personnel des employés et des candidats méritent une protection particulière. Notre objectif est de maintenir la protection de nos données à un niveau élevé. Par conséquent, nous développons régulièrement nos concepts de protection et de sécurité des données.

Bien entendu, nous respectons les dispositions légales en matière de protection des données. Selon les articles 13 et 14 RGPD, les responsables du traitement répondent à des exigences d'information spécifiques lors du traitement de données à caractère personnel. Ce document remplit ces obligations.

La terminologie de la réglementation légale est compliquée. Malheureusement, l'utilisation de termes juridiques n'a pas pu être abandonnée lors de la préparation de ce document. Toutefois, nous tenons à souligner que vous êtes toujours le bienvenu pour nous contacter pour toutes questions concernant ce document, les termes utilisés ou les formulations.

## I. Informations à fournir lorsque des données à caractère personnel sont collectées auprès de la personne concernée (Article 13 RGPD)

### A. Identité et coordonnées du responsable du traitement (art. 13(1) lit. a RGPD)

Voir au-dessus

### B. Coordonnées du délégué à la protection des données (art. 13(1) lit. b RGPD)

Voir au-dessus

### C. Finalités du traitement auquel sont destinées les données à caractère personnel ainsi que la base juridique du traitement (art. 13(1) lit. c RGPD)

Pour les données du candidat, le traitement des données a pour objet de procéder à un examen de la candidature au cours du processus de recrutement. À cette fin, nous traitons toutes les données que vous avez fournies. Fonde sur des données soumises lors du processus de recrutement, nous vérifierons si vous êtes invité à un entretien d'embauche (élément du processus de sélection).Dans le cas de candidats généralement qualifiés, en particulier dans le cadre de l'entretien d'embauche, nous traitons


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

certaines autres données à caractère personnel que vous nous avez fournies, ce qui est essentiel pour notre décision de sélection. Si vous êtes embauché par nous, les données du demandeur seront automatiquement converties en données relatives aux employés. Dans le cadre du processus de recrutement, nous traiterons les autres données à caractère personnel vous concernant que nous vous demandons et qui sont nécessaires pour initier ou exécuter votre contrat (telles que du numéro d'identification personnel ou du numéro d'identification fiscale).Pour les données relatives aux employés, le traitement des données a pour objet l'exécution du contrat de travail ou le respect d'autres dispositions légales applicables à la relation de travail (droit fiscal, par exemple), ainsi que l'utilisation de vos données à caractère personnel pour exécuter le contrat de travail conclu avec vous.

La base légale pour le traitement de données est l'article 6 (1) lit. b RGPD, article 9(2) lit. b et h RGPD, l'article 88(1) RGPD et de la législation nationale.

## D. Catégories des destinataires des données à caractère personnel (art. 14(1) lit. e RGPD)

Autorités publiques

Organisations externes

Autres organisations externes

Traitement interne

Traitement intragroupe

Autres organisations

Une liste de nos sous-traitants et de nos destinataires de données dans les pays tiers et, le cas échéant, des organisations internationales est publiée sur notre site web ou peut être demandée gratuitement. Pour obtenir cette liste, veuillez contacter notre délégué à la protection des données.

## E. Destinataires dans un pays tiers et garanties appropriées ou appropriées et moyens permettant d'en obtenir une copie ou lorsqu'ils ont été mis à disposition (Article 13(1) lit. f, 46(2) lit. c RGPD)

Toutes les entreprises et filiales faisant partie de notre groupe (ci-après dénommées "entreprises du groupe") ayant leur siège ou un bureau dans un pays tiers peuvent appartenir aux destinataires des données à caractère personnel. Une liste des toutes les entreprises du groupe ou de tous destinataires peut nous être demandée.


© All rights reserved by Heiko Maniero.

Selon l'article 46(1) RGPD, un responsable du traitement or sous-traitant peut transférer des données à caractère personnel vers un pays tiers si le responsable du traitement ou le sous-traitant a mis en place les garanties appropriées, et à condition que des droits applicables des personnes concernées et des recours légaux efficaces soient disponibles. Des garanties appropriées peuvent être fournies sans autorisation spécifique d'une autorité de surveillance au moyen de clauses contractuelles types (art. 46(2) lit. c RGPD).

Les clauses contractuelles types de l'Union Européenne ou d'autres garanties appropriées sont convenues avec tous les destinataires de pays tiers avant la première transmission de données à caractère personnel. Par conséquence, il est garanti que des garanties appropriées, des droits applicables des personnes concernées et des recours légaux efficaces pour les personnes concernées sont garantis. Chaque personne concernée peut obtenir une copie des clauses contractuelles types par nous. Les clauses contractuelles types sont aussi disponibles dans le Journal Official de l'Union Européenne.

L'article 45, paragraphe 3, du règlement général sur la protection des données (RGPD) confère à la Commission européenne le pouvoir de décider, au moyen d'un acte d'exécution, qu'un pays tiers assure un niveau de protection adéquat. Cela signifie que le niveau de protection des données à caractère personnel est essentiellement équivalent au niveau de protection au sein de l'UE. Les décisions d'adéquation ont pour effet que les données à caractère personnel peuvent circuler librement de l'UE (et de la Norvège, du Liechtenstein et de l'Islande) vers un pays tiers sans autres obstacles. Des règles similaires existent pour le Royaume-Uni, la Suisse et certains autres pays.

Lorsque la Commission européenne ou le gouvernement d'un autre pays a décidé qu'un pays tiers assure un niveau de protection adéquat et qu'un cadre valide est en place (par exemple, EU-U.S. Data Privacy Framework, Swiss-U.S. Data Privacy Framework, UK Extension to the EU-U.S. Data Privacy Framework), tous les transferts que nous effectuons vers les membres de ces cadres (par exemple, les entités autocertifiées) sont exclusivement fondés sur l'appartenance de ces entités au cadre respectif. Lorsque nous ou l'une des entités de notre groupe sommes membres d'un tel cadre, tous les transferts à nous ou à l'entité de notre groupe sont exclusivement basés sur l'appartenance de l'entité à ce cadre.

Toute personne concernée peut obtenir une copie des cadres auprès de nous. En outre, les cadres sont également disponibles au Journal officiel de l'Union européenne, dans les documents juridiques publiés ou sur les sites web des autorités de contrôle ou d'autres autorités ou institutions compétentes.

## F. Durée de conservation des données à caractère personnel ou, lorsque ce n'est pas possible, critères pour déterminer cette durée (Article 13(2) lit. a RGPD)

Le critère utilisé pour déterminer la durée de conservation des données à caractère personnel est la durée de conservation statutaire respective. Apres l'expiration de cette durée, les données


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

correspondantes sont systématiquement supprimées, dans la mesure où elles ne sont plus nécessaires à l'exécution du contrat ou à la conclusion d'un contrat.

## G. Existence du droit de demander au responsable du traitement l'accès aux données à caractère personnel, la rectification ou l'effacement de celles-ci, ou une limitation du traitement relatif à la personne concernée, ou du droit de s'opposer au traitement et du droit à la portabilité des données (Article 13(2) lit. b RGPD)

Toutes les personnes concernées ont les droits suivants:

***Droit d'accès***

La personne concernée a le droit d'obtenir du responsable du traitement l'accès aux données à caractère personnel. Il est possible d'accéder aux données traitées par nous. Le droit peut être exercé facilement à des intervalles raisonnables, sans connaissance préalable et sans justification, de la légalité du traitement (Récital 63 RGPD). Ce droit résulte de l'article 15 RGPD. La personne concernée peut nous contacter afin d'exercer le droit d'accès.

***Droit de rectification***

Selon l'article 16 phrase 1 RGPD, la personne concernée a le droit d'obtenir du responsable du traitement, dans les meilleurs délais, la rectification des données à caractère personnel la concernant qui sont inexactes. En outre, selon l'article 16 phase 2 RGPD la personne concernée a le droit d'obtenir que les données à caractère personnel incomplètes soient complétées, y compris en fournissant une déclaration complémentaire. La personne concernée peut nous contacter afin d'exercer le droit de rectification.

***Droit à l'effacement («droit à l'oubli»)***

En outre, les personnes concernées ont le droit à l'effacement et à l'oubli en vertu de l'art. 17 GDPR. Ce droit peut également être exercé en nous contactant. À ce stade, cependant, nous tenons à souligner que ce droit ne s'applique pas dans la mesure où le traitement est nécessaire pour respecter une obligation légale à laquelle notre entreprise est soumise (article 17(3) lit. b RGPD).

***Droit à la limitation du traitement***

Selon l'article 18 RGPD, la personne concernée a le droit d'obtenir du responsable du traitement la limitation du traitement. La limitation du traitement peut être demande si l'un des éléments de l'article 18(1) lit. a-d s'applique. La personne concernée peut nous contacter afin d'exercer le droit à la limitation du traitement.

***Droit d'opposition***

En outre, l'art. 21 GDPR garantit le droit d'opposition. La personne concernée peut nous contacter pour exercer le droit d'opposition.


© All rights reserved by Heiko Maniero.

***Droit à la portabilité des données***

L'article 20 RGPD garantit le droit à la portabilité des données de la personne concernée. En vertu de cette disposition, la personne concernée a dans les conditions de l'article 20(1) lit. a et b RGPD le droit de recevoir les données à caractère personnel le concernant, qu'elles ont fournies à un responsable du traitement, dans un format structuré, couramment utilisé et lisible par machine, et ont le droit de transmettre ces données à un autre responsable du traitement sans que le responsable du traitement auquel les données à caractère personnel ont été communiquées y fasse obstacle. La personne concernée peut nous contacter afin d'exercer le droit à la portabilité de données.

## H. Droit de retirer son consentement à tout moment, sans porter atteinte à la licéité du traitement fondé sur le consentement effectué avant le retrait de celui-ci, lorsque le traitement est fondé sur l'article 6(1) lit. a, ou sur l'article 9(2) lit a RGPD

Si le traitement des données à caractère personnel est fondé sur l'article 6(1) lit. a RGPD, quel soit le cas, si la personne concernée a donné son consentement pour le traitement des données à caractère personnel pour une ou plusieurs finalités spécifiques ou si il est fonde sur l'article 9(2) lit. a RGPD, qui régit le consentement explicite au traitement de catégories particulières de données à caractère personnel, la personne concernée a selon l'article 7(3) phrase 1 RGPD le droit de retirer son consentement à tout moment.

Le retrait du consentement ne compromet pas la licéité du traitement fondé sur le consentement effectué avant ce retrait (art. 7(3) phrase 2 RGPD). Il est aussi simple de retirer que de donner son consentement (art. 7(3) phrase 4 RGPD). Par conséquent, le retrait du consentement peut toujours se dérouler de la même manière que le consentement ou de toute autre manière, considérée par la personne concernée comme plus simple. Dans la société de l'information d'aujourd'hui, le moyen le plus simple de retirer son consentement consiste à utiliser un courrier électronique. Si la personne concernée souhaite retirer son consentement, un simple courrier électronique nous suffit. Par ailleurs, la personne concernée peut choisir par tout autre moyen de communiquer son retrait de consentement.

## I. Droit d'introduire une réclamation auprès d'une autorité de contrôle (art.13(2) lit. d, 77(1) RGPD)

Comme le responsable du traitement, nous sommes obligés d'informer la personne concernée du droit d'introduire une réclamation auprès d'une autorité de contrôle (art. 13(2) lit. d RGPD). Le droit d'introduire une réclamation auprès une autorité de contrôle est régie par l'article 77(1) RGPD. Selon cette disposition, sans préjudice de tout autre recours administratif ou extrajudiciaire, toute personne concernée a le droit d'introduire une réclamation auprès d'une autorité de contrôle, en particulier dans l'État membre dans lequel se trouve sa résidence habituelle, son lieu de travail ou le lieu où la violation aurait été commise, si elle considère que le traitement de données à caractère personnel la concernant


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

constitue une violation du règlement général sur la protection des données. Le droit d'introduire une réclamation auprès une autorité de contrôle n'était limite que seulement par le droit de l'Union Européenne de manière à ce qu'il ne puisse être exercé que devant une seule autorité de contrôle (Récital 141 phrase 1 RGPD). Cette règle vise à éviter les doubles plaintes de la même personne concernée dans la même affaire. Si une personne concernée souhaite introduire une réclamation nous concernant, nous demandons que vous contactiez une seule autorité de contrôle.

## J. Fourniture de données à caractère personnel contractuel; Obligation pour la conclusion d'un contrat; Obligation de la personne concernée de fournir les données à caractère personnel; Conséquences éventuelles de la non-fourniture des données (article 13(2) lit. e RGPD)

Nous clarifions que la que la fourniture de données à caractère personnel est en partie requise par la loi (par exemple, la réglementation fiscale) ou peut également résulter de dispositions contractuelles (par exemple, des informations sur le partenaire contractuel).

Quelques fois, il peut être nécessaire de conclure un contrat prévoyant que la personne concernée nous fournisse des données à caractère personnel, qui doivent ensuite être traitées par nous. La personne concernée est par exemple obligée de nous fournir des données à caractère personnel lorsque notre société signe un contrat avec elle. La non-communication des données à caractère personnel aurait pour conséquence que le contrat avec la personne concernée ne pourrait pas être conclu.

Avant que les données personnelles soient fournies par la personne concernée, celle-ci doit nous contacter. Nous précisons à la personne concernée si la fourniture des données à caractère personnel est requise par la loi ou par un contrat ou si elle est nécessaire à la conclusion du contrat, s'il existe une obligation de fournir des données à caractère personnel et les conséquences de la non-fourniture des données à caractère personnel.

## K. Existence d'une prise de décision automatisée, y compris profilage, visée à l'article 22 (1) et (4) RGPD, et, au moins en pareils cas, informations utiles concernant la logique sous-jacente, ainsi que l'importance et les conséquences prévues de ce traitement pour la personne concernée (art. 13(2) lit. f RGPD)

En tant qu'entreprise responsable, nous ne recourons généralement pas à la prise de décision automatisée ou au profilage. Si, dans des cas exceptionnels, nous procédons à une prise de décision automatisée ou à un profilage, nous en informons la personne concernée, soit séparément, soit par le biais d'une sous-section de notre politique de confidentialité (sur notre site web). Dans ce cas, les dispositions suivantes s'appliquent :


© All rights reserved by Heiko Maniero.

La prise de décision automatisée - y compris le profilage - peut avoir lieu si (1) elle est nécessaire à la conclusion ou à l'exécution d'un contrat entre la personne concernée et nous, ou (2) elle est autorisée par le droit de l'Union ou de l'État membre auquel nous sommes soumis et qui prévoit également des mesures appropriées pour la sauvegarde des droits et libertés et des intérêts légitimes de la personne concernée, ou (3) elle est fondée sur le consentement explicite de la personne concernée.

Dans les cas visés à l'article 22, paragraphe 2, points a) et c), du RGPD, nous mettons en œuvre des mesures appropriées pour la sauvegarde des droits et libertés et des intérêts légitimes de la personne concernée. Dans ces cas, vous avez le droit d'obtenir une intervention humaine de la part du responsable du traitement, d'exprimer votre point de vue et de contester la décision.

Des informations utiles sur la logique mise en œuvre, ainsi que sur l'importance et les conséquences envisagées de ce traitement pour la personne concernée, sont fournies dans notre politique de confidentialité.

## II. Informations à fournir lorsque les données à caractère personnel n'ont pas été collectées auprès de la personne concernée (Article 14 RGPD)

### A. Identité et coordonnées du responsable du traitement (art. 13(1) lit. a RGPD)

Voir au-dessus

### B. Coordonnées du délégué à la protection des données (art. 13(1) lit. b RGPD)

Voir au-dessus

### C. Finalités du traitement auquel sont destinées les données à caractère personnel ainsi que la base juridique du traitement (art. 14(1) lit. c RGPD)

Pour les données du candidat, le traitement des données a pour objet de procéder à un examen de la candidature au cours du processus de recrutement. À cette fin, nous traitons toutes les données que vous avez fournies. Fonde sur des données soumises lors du processus de recrutement, nous vérifierons si vous êtes invité à un entretien d'embauche (élément du processus de sélection). Si vous êtes embauché par nous, les données du demandeur seront automatiquement converties en données relatives aux employés. Pour les données relatives aux employés, le traitement des données a pour objet l'exécution du contrat de travail ou le respect d'autres dispositions légales applicables à la relation de travail, ainsi que l'utilisation de vos données à caractère personnel pour exécuter le contrat de travail conclu avec vous. Les données relatives aux employés sont conservées après la fin de la relation de travail afin de respecter les délais de conservation légaux.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

La base légale pour le traitement de données est les articles 6 (1) lit. b RGPD, 9(2) lit. b et h RGPD, 88(1) RGPD et de la législation nationale.

## D. Les catégories de données à caractère personnel concernées (art. 14(1) lit. d RGPD)

Données des candidats

Données des employés

## E. Catégories des destinataires des données à caractère personnel (art. 14(1) lit. e RGPD)

Autorités publiques

Organisations externes

Autres organisations externes

Traitement interne

Traitement intragroupe

Autres organisations

Une liste de nos sous-traitants et de nos destinataires de données dans les pays tiers et, le cas échéant, des organisations internationales est publiée sur notre site web ou peut être demandée gratuitement. Pour obtenir cette liste, veuillez contacter notre délégué à la protection des données.

## F. Destinataires dans pays tiers ou une organisation internationale, et garanties appropriées ou adaptées et les moyens d'en obtenir une copie ou l'endroit où elles ont été mises à disposition (art. 14(1) lit. f RGPD, 46(1), 46(2) lit. c RGPD)

Toutes les entreprises et filiales faisant partie de notre groupe (ci-après dénommées "entreprises du groupe") ayant leur siège ou un bureau dans un pays tiers peuvent appartenir aux destinataires des données à caractère personnel. Une liste des toutes les entreprises du groupe ou de tous destinataires peut nous être demandée.


© All rights reserved by Heiko Maniero.

Selon l'article 46(1) RGPD, un responsable du traitement or sous-traitant peut transférer des données à caractère personnel vers un pays tiers si le responsable du traitement ou le sous-traitant a mis en place les garanties appropriées, et à condition que des droits applicables des personnes concernées et des recours légaux efficaces soient disponibles. Des garanties appropriées peuvent être fournies sans autorisation spécifique d'une autorité de surveillance au moyen de clauses contractuelles types (art. 46(2) lit. c RGPD).

Les clauses contractuelles types de l'Union Européenne ou d'autres garanties appropriées sont convenues avec tous les destinataires de pays tiers avant la première transmission de données à caractère personnel. Par conséquence, il est garanti que des garanties appropriées, des droits applicables des personnes concernées et des recours légaux efficaces pour les personnes concernées sont garantis. Chaque personne concernée peut obtenir une copie des clauses contractuelles types par nous. Les clauses contractuelles types sont aussi disponibles dans le Journal Official de l'Union Européenne.

L'article 45, paragraphe 3, du règlement général sur la protection des données (RGPD) confère à la Commission européenne le pouvoir de décider, au moyen d'un acte d'exécution, qu'un pays tiers assure un niveau de protection adéquat. Cela signifie que le niveau de protection des données à caractère personnel est essentiellement équivalent au niveau de protection au sein de l'UE. Les décisions d'adéquation ont pour effet que les données à caractère personnel peuvent circuler librement de l'UE (et de la Norvège, du Liechtenstein et de l'Islande) vers un pays tiers sans autres obstacles. Des règles similaires existent pour le Royaume-Uni, la Suisse et certains autres pays.

Lorsque la Commission européenne ou le gouvernement d'un autre pays a décidé qu'un pays tiers assure un niveau de protection adéquat et qu'un cadre valide est en place (par exemple, EU-U.S. Data Privacy Framework, Swiss-U.S. Data Privacy Framework, UK Extension to the EU-U.S. Data Privacy Framework), tous les transferts que nous effectuons vers les membres de ces cadres (par exemple, les entités autocertifiées) sont exclusivement fondés sur l'appartenance de ces entités au cadre respectif. Lorsque nous ou l'une des entités de notre groupe sommes membres d'un tel cadre, tous les transferts à nous ou à l'entité de notre groupe sont exclusivement basés sur l'appartenance de l'entité à ce cadre.

Toute personne concernée peut obtenir une copie des cadres auprès de nous. En outre, les cadres sont également disponibles au Journal officiel de l'Union européenne, dans les documents juridiques publiés ou sur les sites web des autorités de contrôle ou d'autres autorités ou institutions compétentes.

## G. Durée de conservation des données à caractère personnel ou, lorsque ce n'est pas possible, critères pour déterminer cette durée (Article 14(2) lit. a RGPD)

Le critère utilisé pour déterminer la durée de conservation des données à caractère personnel est la durée de conservation statutaire respective. Apres l'expiration de cette durée, les données


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

correspondantes sont systématiquement supprimées, dans la mesure où elles ne sont plus nécessaires à l'exécution du contrat ou à la conclusion d'un contrat.

## H. Les intérêts légitimes poursuivis par le responsable du traitement ou par un tiers, lorsque le traitement est fondé sur l'article 6(1) lit. f RGPD (art. 14(2) lit. b RGPD)

Selon l'article 6(1) lit. f RGPD, le traitement n'est licite que le traitement est nécessaire aux fins des intérêts légitimes poursuivis par le responsable du traitement ou par un tiers, à moins que ne prévalent les intérêts ou les libertés et droits fondamentaux de la personne concernée qui exigent une protection des données à caractère personnel. Selon le récital 47 phrase 2 RGPD, un tel intérêt légitime pourrait exister lorsqu'il existe une relation pertinente et appropriée entre la personne concernée et le responsable du traitement, par exemple où la personne concernée est un client du responsable du traitement. Dans tous les cas où notre société traite des données à caractère personnel sur la base de l'article 6(1) lit. f RGPD, notre intérêt légitime est de mener nos activités en faveur du bien-être de tous nos employés et de nos actionnaires.

## I. Existence du droit de demander au responsable du traitement l'accès aux données à caractère personnel, la rectification ou l'effacement de celles-ci, ou une limitation du traitement relatif à la personne concernée, ou du droit de s'opposer au traitement et du droit à la portabilité des données (Article 13(2) lit. b RGPD)

Toutes les personnes concernées ont les droits suivants:

***Droit d'accès***

La personne concernée a le droit d'obtenir du responsable du traitement l'accès aux données à caractère personnel. Il est possible d'accéder aux données traitées par nous. Le droit peut être exercé facilement à des intervalles raisonnables, sans connaissance préalable et sans justification, de la légalité du traitement (Récital 63 RGPD). Ce droit résulte de l'article 15 RGPD. La personne concernée peut nous contacter afin d'exercer le droit d'accès.

***Droit de rectification***

Selon l'article 16 phrase 1 RGPD, la personne concernée a le droit d'obtenir du responsable du traitement, dans les meilleurs délais, la rectification des données à caractère personnel la concernant qui sont inexactes. En outre, selon l'article 16 phase 2 RGPD la personne concernée a le droit d'obtenir que les données à caractère personnel incomplètes soient complétées, y compris en fournissant une déclaration complémentaire. La personne concernée peut nous contacter afin d'exercer le droit de rectification.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

***Droit à l'effacement («droit à l'oubli»)***

En outre, les personnes concernées ont le droit à l'effacement et à l'oubli en vertu de l'art. 17 GDPR. Ce droit peut également être exercé en nous contactant. À ce stade, cependant, nous tenons à souligner que ce droit ne s'applique pas dans la mesure où le traitement est nécessaire pour respecter une obligation légale à laquelle notre entreprise est soumise (article 17(3) lit. b RGPD).

***Droit à la limitation du traitement***

Selon l'article 18 RGPD, la personne concernée a le droit d'obtenir du responsable du traitement la limitation du traitement. La limitation du traitement peut être demande si l'un des éléments de l'article 18(1) lit. a-d s'applique. La personne concernée peut nous contacter afin d'exercer le droit à la limitation du traitement.

***Droit d'opposition***

En outre, l'art. 21 GDPR garantit le droit d'opposition. La personne concernée peut nous contacter pour exercer le droit d'opposition.

***Droit à la portabilité des données***

L'article 20 RGPD garantit le droit à la portabilité des données de la personne concernée. En vertu de cette disposition, la personne concernée a dans les conditions de l'article 20(1) lit. a et b RGPD le droit de recevoir les données à caractère personnel le concernant, qu'elles ont fournies à un responsable du traitement, dans un format structuré, couramment utilisé et lisible par machine, et ont le droit de transmettre ces données à un autre responsable du traitement sans que le responsable du traitement auquel les données à caractère personnel ont été communiquées y fasse obstacle. La personne concernée peut nous contacter afin d'exercer le droit à la portabilité de données.

## J. Existence du droit de retirer le consentement à tout moment, sans porter atteinte à la licéité du traitement fondé sur le consentement effectué avant le retrait de celui-ci, lorsque le traitement est fondé sur l'article 6(1) lit. a, ou sur l'article 9(2) lit. a RGPD (art. 14(2) lit. d RGPD)

Si le traitement des données à caractère personnel est fondé sur l'article 6(1) lit. a RGPD, quel soit le cas, si la personne concernée a donné son consentement pour le traitement des données à caractère personnel pour une ou plusieurs finalités spécifiques ou si il est fonde sur l'article 9(2) lit. a RGPD, qui régit le consentement explicite au traitement de catégories particulières de données à caractère personnel, la personne concernée a selon l'article 7(3) phrase 1 RGPD le droit de retirer son consentement à tout moment.

Le retrait du consentement ne compromet pas la licéité du traitement fondé sur le consentement effectué avant ce retrait (art. 7(3) phrase 2 RGPD).Il est aussi simple de retirer que de donner son consentement) art. 7(3) phrase 4 RGPD). Par conséquent, le retrait du consentement peut toujours se dérouler de la même manière que le consentement ou de toute autre manière, considérée par la personne concernée


© All rights reserved by Heiko Maniero.

comme plus simple. Dans la société de l'information d'aujourd'hui, le moyen le plus simple de retirer son consentement consiste à utiliser un simple courrier électronique. Si la personne concernée souhaite retirer son consentement, un simple courrier électronique nous suffit. Par ailleurs, la personne concernée peut choisir par tout autre moyen de communiquer son retrait de consentement.

## K. Droit d'introduire une réclamation auprès d'une autorité de contrôle (Article 14(2) lit. e, 77(1) RGPD)

Comme le responsable du traitement, nous sommes obligés d'informer la personne concernée du droit d'introduire une réclamation auprès d'une autorité de contrôle (art. 14(2) lit. e RGPD). Le droit d'introduire une réclamation auprès une autorité de contrôle est régie par l'article 77(1) RGPD. Selon cette disposition, sans préjudice de tout autre recours administratif ou extrajudiciaire, toute personne concernée a le droit d'introduire une réclamation auprès d'une autorité de contrôle, en particulier dans l'État membre dans lequel se trouve sa résidence habituelle, son lieu de travail ou le lieu où la violation aurait été commise, si elle considère que le traitement de données à caractère personnel la concernant constitue une violation du présent règlement. Le droit d'introduire une réclamation auprès une autorité de contrôle n'était limite que seulement par le droit de l'Union Européenne de manière à ce qu'il ne puisse être exercé que devant une seule autorité de contrôle (Récital 141 phrase 1 RGPD). Cette règle vise à éviter les doubles plaintes de la même personne concernée dans la même affaire. Si une personne concernée souhaite introduire une réclamation nous concernant, nous demandons que vous contactiez une seule autorité de contrôle.

## L. La source d'où proviennent les données à caractère personnel et, le cas échéant, une mention indiquant qu'elles sont issues ou non de sources accessibles au public (art. 14(2) lit. f RGPD)

En principe, les données à caractère personnel sont collectées directement auprès de la personne concernée ou en coopération avec une autorité (par exemple, la récupération de données à partir d'un registre officiel). Les autres données relatives aux personnes concernées proviennent de transferts des entreprises du groupe. Dans le contexte de ces informations générales, la désignation des sources exactes à l'origine des données à caractère personnel est impossible ou impliquerait un effort disproportionné au sens de l'art. 14 (5) lit. b GDPR. En principe, nous ne collectons pas de données à caractère personnel à partir de sources accessibles au public.

Toute personne concernée peut nous contacter à tout moment pour obtenir des informations plus détaillées sur les sources exactes des données à caractère personnel la concernant. Lorsque l'origine des données à caractère personnel n'a pas pu être communiquée à la personne concernée parce que plusieurs sources ont été utilisées, des informations générales devraient être fournies (récital 61 phrase 4 RGPD).


© All rights reserved by Heiko Maniero.

### M. Existence d'une prise de décision automatisée, y compris profilage, visée à l'article 22 (1) et (4) RGPD, et, au moins en pareils cas, informations utiles concernant la logique sous-jacente, ainsi que l'importance et les conséquences prévues de ce traitement pour la personne concernée (art. 14(2) lit. g RGPD)

En tant qu'entreprise responsable, nous ne recourons généralement pas à la prise de décision automatisée ou au profilage. Si, dans des cas exceptionnels, nous procédons à une prise de décision automatisée ou à un profilage, nous en informons la personne concernée, soit séparément, soit par le biais d'une sous-section de notre politique de confidentialité (sur notre site web). Dans ce cas, les dispositions suivantes s'appliquent :

La prise de décision automatisée - y compris le profilage - peut avoir lieu si (1) elle est nécessaire à la conclusion ou à l'exécution d'un contrat entre la personne concernée et nous, ou (2) elle est autorisée par le droit de l'Union ou de l'État membre auquel nous sommes soumis et qui prévoit également des mesures appropriées pour la sauvegarde des droits et libertés et des intérêts légitimes de la personne concernée, ou (3) elle est fondée sur le consentement explicite de la personne concernée.

Dans les cas visés à l'article 22, paragraphe 2, points a) et c), du RGPD, nous mettons en œuvre des mesures appropriées pour la sauvegarde des droits et libertés et des intérêts légitimes de la personne concernée. Dans ces cas, vous avez le droit d'obtenir une intervention humaine de la part du responsable du traitement, d'exprimer votre point de vue et de contester la décision.

Des informations utiles sur la logique mise en œuvre, ainsi que sur l'importance et les conséquences envisagées de ce traitement pour la personne concernée, sont fournies dans notre politique de confidentialité.

## III. EU-U.S. Data Privacy Framework (EU-U.S. DPF), UK Extension to the EU-U.S. DPF, Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF)

Si notre organisation est un membre certifié de l'EU-U.S. Data Privacy Framework (EU-U.S. DPF) et/ou de la UK Extension to the EU-U.S. DPF et/ou du Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF), les dispositions suivantes s'appliquent:

Nous adhérons à l'EU-U.S. Data Privacy Framework (EU-U.S. DPF) et à la UK Extension to the EU-U.S. DPF ainsi qu'au Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF), tel qu'établi par le U.S. Department of Commerce. Notre entreprise a confirmé au U.S. Department of Commerce qu'elle respecte les EU-U.S. Data Privacy Framework Principles (EU-U.S. DPF Principles) concernant le traitement des données personnelles qu'elle reçoit de l'Union européenne et du Royaume-Uni en vertu


© All rights reserved by Heiko Maniero.

de l'EU-U.S. DPF et de la UK Extension to the EU-U.S. DPF. Notre entreprise a également confirmé qu'elle respecte les Swiss-U.S. Data Privacy Framework Principles (Swiss-U.S. DPF Principles) concernant le traitement des données personnelles qu'elle reçoit de la Suisse sous le Swiss-U.S. DPF. En cas de contradiction entre les dispositions de notre politique de confidentialité et les EU-U.S. DPF Principles et/ou les Swiss-U.S. DPF Principles, les Principles prévalent.

Pour en savoir plus sur le programme Data Privacy Framework (DPF) et consulter notre certification, veuillez visiter https://www.dataprivacyframework.gov/.

Les autres entités américaines ou filiales de notre entreprise qui adhèrent également aux EU-U.S. DPF Principals, y compris la UK Extension to the EU-U.S. DPF et les Swiss-U.S. DPF Principals, si elles existent, sont mentionnées dans notre politique de confidentialité.

Conformément à l'EU-U.S. DPF, à la UK Extension to the EU-U.S. DPF et au Swiss-U.S. DPF, notre entreprise s'engage à coopérer avec le comité établi par les autorités de protection des données de l'UE, le UK Information Commissioner's Office (ICO) et le Préposé fédéral à la protection des données et à la transparence (EDÖB) de Suisse, et à suivre leurs conseils concernant les plaintes non résolues sur notre gestion des données personnelles que nous recevons sous l'EU-U.S. DPF, la UK Extension to the EU-U.S. DPF et le Swiss-U.S. DPF.

Nous informons les personnes concernées des autorités européennes de protection des données compétentes pour traiter les plaintes concernant la manière dont notre organisation gère les données personnelles, en haut de ce document de transparence, et que nous offrons un recours juridique adéquat et gratuit.

Nous informons toutes les personnes concernées que notre entreprise est soumise aux pouvoirs d'enquête et de contrôle de la Federal Trade Commission (FTC).

Les personnes affectées ont la possibilité, sous certaines conditions, de demander un arbitrage contraignant. Notre organisation est tenue de régler les réclamations et de respecter les conditions énoncées à l'Annexe I des DPF-Principals, à condition que la personne concernée ait demandé un arbitrage contraignant en notifiant notre organisation et que les procédures et conditions de l'Annexe I des Principals aient été respectées.

Nous informons par la présente toutes les personnes concernées de la responsabilité de notre organisation en cas de transfert de données personnelles à des tiers.

Pour les questions des personnes affectées ou des autorités de contrôle de la protection des données, nous avons nommé les représentants locaux mentionnés en haut de ce document de transparence.

Nous vous offrons la possibilité de choisir (Opt-out), si vos données personnelles (i) doivent être partagées avec des tiers ou (ii) doivent être utilisées à des fins substantiellement différentes de celles pour lesquelles elles ont été initialement collectées ou ultérieurement autorisées par vous. Le mécanisme clair, bien visible et facilement accessible pour exercer votre droit de choix consiste à contacter notre


© All rights reserved by Heiko Maniero.

responsable de la protection des données (DSB) par courriel. Vous n'avez pas le choix et nous ne sommes pas obligés lorsque les données sont partagées avec un tiers qui agit en tant qu'agent ou processeur en notre nom et selon nos instructions. Nous concluons cependant toujours un contrat avec un tel agent ou processeur.

Pour les données sensibles (c'est-à-dire les données personnelles incluant des informations sur l'état de santé, l'origine raciale ou ethnique, les opinions politiques, les croyances religieuses ou philosophiques, l'appartenance syndicale ou les informations sur la vie sexuelle de la personne), nous obtenons votre consentement explicite (Opt-in) si ces données (i) doivent être partagées ou (ii) doivent être utilisées à des fins différentes de celles pour lesquelles elles ont été initialement collectées ou pour lesquelles vous avez ensuite donné votre consentement, en faisant votre choix d'Opt-in. De plus, nous traitons toutes les données personnelles que nous recevons de tiers comme sensibles si le tiers les a identifiées et traitées comme telles.

Nous vous informons de la nécessité de divulguer des données personnelles en réponse à des demandes légales des autorités, y compris pour répondre aux exigences de la sécurité nationale ou de l'application de la loi.

Lors du transfert de données personnelles à un tiers qui agit en tant que contrôleur, nous respectons les Principals de notification et de choix. En outre, nous concluons un contrat avec le tiers responsable du traitement qui stipule que ces données ne peuvent être traitées que pour des fins limitées et spécifiées conformément au consentement que vous avez fourni et que le destinataire offre le même niveau de protection que les Principals du DPF et nous informe s'il détermine qu'il ne peut plus remplir cette obligation. Le contrat prévoit que le tiers, qui agit en tant que contrôleur, doit cesser le traitement ou prendre d'autres mesures raisonnables et appropriées pour remédier à la situation si une telle détermination est faite.

Lors du transfert de données personnelles à un tiers qui agit en tant qu'agent ou processeur, (i) nous transférons ces données uniquement à des fins limitées et spécifiées ; (ii) nous nous assurons que l'agent ou le processeur est tenu de fournir au moins le même niveau de protection des données exigé par les DPF-Principals ; (iii) nous prenons des mesures raisonnables et appropriées pour nous assurer que l'agent ou le processeur traite réellement les données personnelles transférées d'une manière conforme à nos obligations en vertu des DPF-Principals ; (iv) nous exigeons que l'agent ou le processeur nous informe s'il détermine qu'il ne peut plus respecter son obligation de fournir le même niveau de protection requis par les DPF-Principals ; (v) après une telle notification, également sous (iv), nous prenons des mesures raisonnables et appropriées pour arrêter le traitement non autorisé et remédier à la situation ; et (vi) nous fournissons au DPF Department, sur demande, un résumé ou un exemplaire représentatif des dispositions pertinentes de confidentialité de notre contrat avec cet agent.

Conformément à l'EU-U.S. DPF et/ou à la UK Extension to the EU-U.S. DPF et/ou au Swiss-U.S. DPF, notre organisation s'engage à coopérer avec le comité établi par les autorités de protection des données de l'UE et le UK Information Commissioner's Office (ICO) ainsi que le Préposé fédéral à la protection des


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

données et à la transparence (EDÖB) de Suisse, et à suivre leurs conseils concernant les plaintes non résolues sur notre gestion des données personnelles que nous recevons en relation avec l'emploi sous l'EU-U.S. DPF, la UK Extension to the EU-U.S. DPF et le Swiss-U.S. DPF.

Toutes les personnes concernées qui se trouvent temporairement dans l'Union européenne (UE), l'Espace économique européen (EEE) ou le Royaume-Uni, ou qui y ont leur domicile ou leur résidence habituelle, bénéficient des droits et des droits des personnes concernées publiés dans notre document de transparence, qui découlent également des articles 15 à 22 du RGPD, y compris le droit d'accès aux données à caractère personnel. Ces informations sont disponibles dans toutes les langues de l'UE et de l'EEE. La version anglaise s'applique au Royaume-Uni.

Toutes les personnes concernées qui résident temporairement en Suisse ou qui y ont leur domicile ou leur résidence habituelle bénéficient des droits et des droits des personnes concernées en vertu de la loi suisse sur la protection des données (LPD) et du règlement suisse sur la protection des données (RGPD) qui sont publiés dans notre document de transparence, y compris le droit d'accès aux données à caractère personnel. Nous avons fourni ces informations dans les trois langues officielles de la Suisse (allemand, italien et français).


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

# ITALIAN: Informazioni sul trattamento dei dati personali (articolo 13, 14 GDPR)

Gentile signore o signora,

I dati personali di ogni individuo che abbia un rapporto contrattuale, precontrattuale o di altro tipo con la nostra azienda merita una protezione speciale. Il nostro obiettivo è di mantenere il nostro livello di protezione dei dati ad un alto livello. Pertanto, sviluppiamo ordinariamente i nostri concetti di protezione dei dati e sicurezza dei dati.

Ovviamente, rispettiamo le disposizioni legali sulla protezione dei dati. Ai sensi dell'articolo 13, 14 GDPR, i titolari del trattamento soddisfano specifici requisiti di informazione nella raccolta di dati personali. Questo documento soddisfa questi obblighi.

La terminologia delle normative legali è complicata. Sfortunatamente, l'uso di termini legali non può essere evitato nella preparazione di questo documento. Pertanto, vorremmo sottolineare che siete sempre i benvenuti a contattarci per tutte le domande riguardanti questo documento, i termini usati o le formulazioni.

## I. Rispetto dei requisiti in materia di informazione quando i dati personali sono raccolti dall'interessato (articolo 13 del GDPR)

### A. Identità e recapiti del titolare del trattamento (articolo 13, paragrafo 1, lett. a) del GDPR)

Vedi sopra

### B. Dati di contatto del responsabile della protezione dei dati (articolo 13, paragrafo 1, lett. b) del GDPR)

Vedi sopra


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## C. Finalità del trattamento al quale sono destinati i dati personali nonché base legale per il trattamento (articolo 13, paragrafo 1, lett. c) GDPR)

Lo scopo del trattamento dei dati personali è la gestione di tutte le operazioni che riguardano il titolare del trattamento, i clienti, i potenziali clienti, i partner commerciali o altre relazioni contrattuali o precontrattuali tra i gruppi nominati (nel senso più ampio) o gli obblighi legali del titolare del trattamento.

Art. 6 (1) lett. c GDPR funge da base legale per le operazioni di elaborazione per le quali otteniamo il consenso per uno scopo di elaborazione specifico. Se il trattamento di dati personali è necessario per l'esecuzione di un contratto a cui l'interessato è parte, come ad esempio quando le operazioni di trattamento sono necessarie per la fornitura di beni o per fornire qualsiasi altro servizio, il trattamento è basato sull'articolo 6, paragrafo 1, lett. b) GDPR. Lo stesso vale per le operazioni di trattamento necessarie per l'esecuzione di misure precontrattuali, ad esempio nel caso di richieste relative ai nostri prodotti o servizi. La nostra azienda è soggetta all'obbligo legale in base al quale è richiesto il trattamento dei dati personali, ad esempio per l'adempimento di obblighi fiscali, il trattamento è basato sull'art. 6 (1) lett. c) GDPR.

In rari casi, il trattamento di dati personali può essere necessario per proteggere gli interessi vitali dell'interessato o di un'altra persona fisica. Questo sarebbe il caso, ad esempio, se un visitatore fosse ferito nella nostra azienda e il suo nome, età, dati di assicurazione sanitaria o altre informazioni vitali dovrebbero essere trasmessi a un medico, ospedale o altra terza parte. Quindi l'elaborazione si baserebbe sull'art. 6 (1) lett. d) GDPR.

Se il trattamento è necessario per l'esecuzione di un compito svolto nell'interesse pubblico o nell'esercizio di pubblici poteri di cui è investito il responsabile del trattamento, la base giuridica è l'Art. 6(1) lett. e GDPR.

Infine, le operazioni di trattamento potrebbero essere basate sull'articolo 6, paragrafo 1, lett. f) GDPR. Questa base giuridica viene utilizzata per le operazioni di trattamento che non sono coperte da nessuno dei summenzionati motivi legali, se il trattamento è necessario ai fini degli interessi legittimi perseguiti dalla nostra azienda o da una terza parte, eccetto laddove tali interessi siano superati dagli interessi o diritti e libertà fondamentali dell'interessato che richiedono la protezione dei dati personali. Tali operazioni di trattamento sono particolarmente ammissibili in quanto sono state espressamente menzionate dal legislatore europeo. Riteneva che potesse essere assunto un interesse legittimo se l'interessato fosse un cliente del titolare del trattamento (considerando 47, frase 2, GDPR).

## D. Se il trattamento si basa sull'articolo 6, paragrafo 1, lett. f) GDPR gli interessi legittimi perseguiti dal titolare del trattamento o da un terzo (articolo 13, paragrafo 1, lett. d) del GDPR)

Se il trattamento dei dati personali si basa sull'articolo 6, paragrafo 1, lett. f) GDPR il nostro legittimo interesse è di svolgere la nostra attività in favore del benessere di tutti i nostri dipendenti e azionisti.


© All rights reserved by Heiko Maniero.

## E. Categorie di destinatari dei dati personali (articolo 13, paragrafo 1, lettere e) GDPR)

Autorità pubbliche

Entità esterne

Ulteriori entità esterne

Elaborazione interna

Elaborazione intragruppo

Altre entità

L'elenco dei nostri responsabili del trattamento e dei destinatari dei dati nei Paesi terzi e, se del caso, delle organizzazioni internazionali è pubblicato sul nostro sito web o può essere richiesto gratuitamente. Per richiedere tale elenco, si prega di contattare il nostro responsabile della protezione dei dati.

## F. Destinatari in un paese terzo e garanzie appropriate o adeguate e i mezzi con cui ottenerne una copia o quando sono stati resi disponibili (articolo 13, paragrafo 1, lett. f), 46, paragrafo 1, articolo 46, paragrafo 2, lett. c) GDPR)

Tutte le società e le filiali che fanno parte del nostro gruppo (in seguito denominate "società del gruppo") che hanno la loro sede di attività o un ufficio in un paese terzo possono appartenere ai destinatari dei dati personali. Un elenco di tutte le società del gruppo o dei destinatari può essere richiesto a noi.

Ai sensi dell'articolo 46, paragrafo 1 del GDPR, un titolare del trattamento o un responsabile del trattamento può trasferire dati personali solo a un paese terzo se il titolare del trattamento o il responsabile del trattamento ha fornito garanzie appropriate e a condizione che siano disponibili diritti soggetti a diritti esecutivi e rimedi giuridici efficaci per le persone interessate. Possono essere fornite appropriate misure di salvaguardia senza richiedere un'autorizzazione specifica da parte di un'autorità di vigilanza mediante clausole contrattuali standard, articolo 46, paragrafo 2, lett. c) GDPR.

Le clausole contrattuali standard dell'Unione europea o altre garanzie appropriate sono concordate con tutti i beneficiari di paesi terzi prima della prima trasmissione di dati personali. Di conseguenza, è garantito che siano garantite garanzie appropriate, diritti soggetti a diritti esecutivi e rimedi giuridici efficaci per gli interessati. Ogni persona interessata può ottenere da noi una copia delle clausole contrattuali standard. Le clausole contrattuali standard sono inoltre disponibili nella Gazzetta ufficiale dell'Unione europea.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

L'articolo 45, paragrafo 3, del Regolamento generale sulla protezione dei dati (GDPR) conferisce alla Commissione europea il potere di decidere, mediante un atto di esecuzione, che un Paese non appartenente all'UE garantisce un livello di protezione adeguato. Ciò significa un livello di protezione dei dati personali sostanzialmente equivalente al livello di protezione all'interno dell'UE. L'effetto delle decisioni di adeguatezza è che i dati personali possono fluire liberamente dall'UE (e da Norvegia, Liechtenstein e Islanda) verso un Paese terzo senza ulteriori ostacoli. Regole simili esistono anche per il Regno Unito, la Svizzera e alcuni altri Paesi.

Laddove la Commissione Europea o il governo di un altro Paese abbia deciso che un Paese terzo garantisce un livello di protezione adeguato e sia in vigore un quadro normativo valido (ad esempio, EU-U.S. Data Privacy Framework, Swiss-U.S. Data Privacy Framework, UK Extension to the EU-U.S. Data Privacy Framework), tutti i trasferimenti da parte nostra ai membri di tali quadri normativi (ad esempio, entità autocertificate) si basano esclusivamente sull'appartenenza di tali entità al rispettivo quadro normativo. Nel caso in cui noi o una delle entità del nostro gruppo sia membro di tale quadro, tutti i trasferimenti a noi o alla nostra entità del gruppo si basano esclusivamente sull'appartenenza dell'entità a tale quadro.

Ogni interessato può ottenere da noi una copia dei quadri normativi. Inoltre, i quadri sono disponibili anche nella Gazzetta ufficiale dell'Unione europea o nei materiali legali pubblicati o sui siti web delle autorità di controllo o di altre autorità o istituzioni competenti.

## G. Periodo per il quale saranno conservati i dati personali o, se ciò non fosse possibile, i criteri utilizzati per determinare tale periodo (articolo 13, paragrafo 2, lett. a) GDPR)

I criteri utilizzati per determinare il periodo di conservazione dei dati personali sono i rispettivi periodi di conservazione previsti dalla legge. Dopo la scadenza di tale periodo, i dati corrispondenti vengono regolarmente cancellati, a condizione che non siano più necessari per l'adempimento del contratto o l'inizio di un contratto.

Se non esiste un periodo di conservazione legale, il criterio è il periodo di conservazione contrattuale o interno.

## H. Esistenza del diritto di richiedere al titolare del trattamento l'accesso e la rettifica o cancellazione di dati personali o la limitazione del trattamento della persona interessata o di opporsi al trattamento nonché il diritto alla portabilità dei dati (articolo 13, paragrafo 2, lett. b) del GDPR).

Tutte le persone interessate hanno i seguenti diritti:


© All rights reserved by Heiko Maniero.

***Diritto di accesso***

Ogni soggetto interessato ha il diritto di accedere ai dati personali che lo riguardano. Il diritto di accesso si estende a tutti i dati elaborati da noi. Il diritto può essere esercitato facilmente e ad intervalli ragionevoli, al fine di essere a conoscenza e verificare la liceità del trattamento (Considerando 63 GDPR). Questo diritto deriva dall'art. 15 GDPR. L'interessato può contattarci per esercitare il diritto di accesso.

***Diritto di rettifica***

Ai sensi dell'articolo 16, paragrafo 1, del GDPR, l'interessato ha il diritto di ottenere dal titolare del trattamento, senza indebito ritardo, la rettifica di dati personali inesatti che lo riguardano. Inoltre, l'articolo 16, paragrafo 2 del GDPR prevede che l'interessato abbia diritto, in considerazione delle finalità del trattamento, a che i dati personali siano incompleti, anche mediante la presentazione di una dichiarazione integrativa. L'interessato può contattarci per esercitare il diritto di rettifica.

***Diritto alla cancellazione (diritto di essere dimenticato)***

Inoltre, l'interessato ha il diritto alla cancellazione e all'oblio ai sensi dell'art. 17 GDPR. Questo diritto può essere esercitato anche contattandoci. A questo punto, tuttavia, vorremmo sottolineare che questo diritto non si applica nella misura in cui il trattamento è necessario per adempiere a un obbligo legale a cui è soggetta la nostra società, articolo 17, paragrafo 3, lett. b) GDPR. Ciò significa che possiamo approvare un'applicazione da cancellare solo dopo la scadenza del periodo di conservazione previsto dalla legge.

***Diritto alla restrizione dell'elaborazione***

Ai sensi dell'articolo 18 del GDPR, ogni interessato ha diritto a una restrizione del trattamento. La restrizione del trattamento può essere richiesta se una delle condizioni di cui all'articolo 18, paragrafo 1, lettere a) - d) GDPR è soddisfatto. L'interessato può contattarci per esercitare il diritto alla restrizione del trattamento.

***Diritto di obiettare***

Inoltre, l'art. 21 GDPR garantisce il diritto di obiettare. L'interessato può contattarci per esercitare il diritto di obiettare.

***Diritto alla portabilità dei dati***

L'articolo 20 del GDPR conferisce all'interessato il diritto alla portabilità dei dati. Ai sensi di questa disposizione, la persona interessata ha le condizioni di cui all'articolo 20, paragrafo 1, lett. a) e b) GDPR il diritto di ricevere i dati personali che lo riguardano, che lui o lei ha fornito a un titolare del trattamento, in un formato strutturato, comunemente usato e leggibile da una macchina e ha il diritto di trasmettere tali dati a un altro titolare del trattamento senza impedimenti dal controllore a cui sono stati forniti i dati personali. L'interessato può contattarci per esercitare il diritto alla portabilità dei dati.


© All rights reserved by Heiko Maniero.

## I. L'esistenza del diritto di revocare il consenso in qualsiasi momento, senza pregiudizio della liceità del trattamento basato sul consenso prima del suo ritiro, qualora il trattamento si basi sull'articolo 6, paragrafo 1, lett. a) GDPR o l'Articolo 9 (2) lett. a) GDPR (articolo 13, paragrafo 2, lett. c) del GDPR)

Se il trattamento dei dati personali è basato sull'art. 6 (1) lett. a) GDPR, che è il caso, se l'interessato ha acconsentito al trattamento dei dati personali per uno o più scopi specifici o è basato sull'articolo 9, paragrafo 2, lett. a) GDPR, che regola il consenso esplicito al trattamento di categorie speciali di dati personali, l'interessato ha in base all'articolo 7 (3) Frase 1 GDPR il diritto di revocare il proprio consenso in qualsiasi momento.

Il ritiro del consenso non pregiudica la liceità del trattamento basato sul consenso prima del suo ritiro, articolo 7, paragrafo 3, frase 2 GDPR. Deve essere facile ritirare il consenso, art. 7 (3) Frase 4 GDPR. Pertanto, il ritiro del consenso può sempre avvenire nello stesso modo in cui è stato dato il consenso o in qualsiasi altro modo, che è considerato dall'interessato essere più semplice. Nella società dell'informazione di oggi, probabilmente il modo più semplice per ritirare il consenso è una semplice email. Se l'interessato desidera ritirare il suo consenso, ci è sufficiente una semplice email. In alternativa, l'interessato può scegliere qualsiasi altro modo per comunicare il suo ritiro del consenso a noi.

## J. Diritto di presentare un reclamo all'autorità di controllo (articolo 13, paragrafo 2, lett. d), 77, paragrafo 1 del GDPR)

Come titolare del trattamento, siamo obbligati a comunicare all'interessato il diritto di presentare un reclamo all'autorità di controllo, articolo 13, paragrafo 2, lett. d) GDPR. Il diritto di presentare un reclamo presso un'autorità di controllo è regolato dall'articolo 77, paragrafo 1 del GDPR. In base a tale disposizione, fatto salvo ogni altro rimedio amministrativo o giudiziario, ogni interessato ha il diritto di presentare un reclamo all'autorità di controllo, in particolare nello Stato membro della sua residenza abituale, luogo di lavoro o luogo di la presunta violazione se l'interessato ritiene che il trattamento di dati personali che lo riguardano violino il regolamento generale sulla protezione dei dati. Il diritto di presentare una denuncia presso un'autorità di controllo era limitato dal diritto dell'Unione solo in tal modo, che poteva essere esercitato solo dinanzi a un'unica autorità di vigilanza (Considerando 141, frase 1, del GDPR). Questa regola è intesa ad evitare i doppi reclami della stessa persona interessata nella stessa materia. Se una persona interessata desidera presentare un reclamo su di noi, abbiamo quindi chiesto di contattare solo una singola autorità di controllo.


© All rights reserved by Heiko Maniero.

## K. Fornitura di dati personali come requisito legale o contrattuale; Requisito necessario per stipulare un contratto; Obbligo dell'interessato di fornire i dati personali; possibili conseguenze del mancato conferimento di tali dati (articolo 13, paragrafo 2, lett. e) GDPR)

Chiariamo che la fornitura di dati personali è in parte richiesta dalla legge (ad es. Regolamenti fiscali) o può anche derivare da disposizioni contrattuali (ad esempio informazioni sul partner contrattuale).

A volte può essere necessario concludere un contratto che l'interessato fornisca dati personali, che devono successivamente essere elaborati da noi. L'interessato è, per esempio, obbligato a fornire dati personali quando la nostra azienda firma un contratto con lui o lei. La mancata fornitura dei dati personali avrebbe come conseguenza che il contratto con l'interessato non poteva essere concluso.

Prima che i dati personali siano forniti dall'interessato, l'interessato deve contattarci. Chiariamo all'interessato se la fornitura dei dati personali è richiesta dalla legge o dal contratto o è necessaria per la conclusione del contratto, se esiste l'obbligo di fornire i dati personali e le conseguenze della mancata fornitura dei dati personali.

## L. Esistenza di processi decisionali automatizzati, inclusa la profilazione, di cui all'articolo 22, paragrafi 1 e 4, del GDPR e, almeno in tali casi, informazioni significative sulla logica in questione, nonché sulla significatività e le conseguenze previste di tale trattamento per l'interessato (articolo 13, paragrafo 2, lett. f) GDPR)

In quanto azienda responsabile, di solito non utilizziamo il processo decisionale automatizzato o la profilazione. Se, in casi eccezionali, effettuiamo un processo decisionale o di profilazione automatizzato, informeremo l'interessato separatamente o tramite una sottosezione della nostra informativa sulla privacy (sul nostro sito web). In tal caso, si applica quanto segue:

Il processo decisionale automatizzato - compresa la profilazione - può avvenire se (1) è necessario per la stipula o l'esecuzione di un contratto tra l'interessato e noi, oppure (2) è autorizzato dal diritto dell'Unione o degli Stati membri a cui siamo soggetti e che prevede anche misure idonee a salvaguardare i diritti e le libertà dell'interessato e i suoi legittimi interessi, oppure (3) si basa sul consenso esplicito dell'interessato.

Nei casi di cui all'articolo 22, paragrafo 2, lettere a) e c), del GDPR, attueremo misure adeguate per salvaguardare i diritti e le libertà dell'interessato e i suoi legittimi interessi. In questi casi, l'interessato ha il diritto di ottenere l'intervento umano da parte del responsabile del trattamento, di esprimere il proprio punto di vista e di contestare la decisione.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

Informazioni significative sulla logica, l'importanza e le conseguenze previste di tale trattamento per l'interessato sono contenute nella nostra politica sulla privacy.

## II. Rispetto dei requisiti di informazione quando i dati personali non sono raccolti dall'interessato (articolo 14 del GDPR)

### A. Identità e recapiti del titolare del trattamento (articolo 14, paragrafo 1, lett. a), del GDPR)

Vedi sopra

### B. Dati di contatto del responsabile della protezione dei dati (articolo 14, paragrafo 1, lett. b) del GDPR)

Vedi sopra

### C. Finalità del trattamento per il quale sono destinati i dati personali nonché base legale per il trattamento (articolo 14, paragrafo 1, lett. c) GDPR)

Lo scopo del trattamento dei dati personali è la gestione di tutte le operazioni che riguardano il titolare del trattamento, i clienti, i potenziali clienti, i partner commerciali o altre relazioni contrattuali o precontrattuali tra i gruppi nominati (nel senso più ampio) o gli obblighi legali del titolare del trattamento.

Se il trattamento di dati personali è necessario per l'esecuzione di un contratto a cui l'interessato è parte, come ad esempio quando le operazioni di trattamento sono necessarie per la fornitura di beni o per fornire qualsiasi altro servizio, il trattamento è basato sull'articolo 6, paragrafo 1, lett. b) GDPR. Lo stesso vale per le operazioni di trattamento necessarie per l'esecuzione di misure precontrattuali, ad esempio nel caso di richieste relative ai nostri prodotti o servizi. La nostra azienda è soggetta all'obbligo legale in base al quale è richiesto il trattamento dei dati personali, ad esempio per l'adempimento di obblighi fiscali, il trattamento è basato sull'art. 6 (1) lett. c) GDPR.

In rari casi, il trattamento di dati personali può essere necessario per proteggere gli interessi vitali dell'interessato o di un'altra persona fisica. Questo sarebbe il caso, ad esempio, se un visitatore fosse ferito nella nostra azienda e il suo nome, età, dati di assicurazione sanitaria o altre informazioni vitali dovrebbero essere trasmessi a un medico, ospedale o altra terza parte. Quindi l'elaborazione si baserebbe sull'art. 6 (1) lett. d) GDPR.


© All rights reserved by Heiko Maniero.

Se il trattamento è necessario per l'esecuzione di un compito svolto nell'interesse pubblico o nell'esercizio di pubblici poteri di cui è investito il responsabile del trattamento, la base giuridica è l'Art. 6(1) lett. e GDPR.

Infine, le operazioni di trattamento potrebbero essere basate sull'articolo 6, paragrafo 1, lett. f) GDPR. Questa base giuridica viene utilizzata per le operazioni di trattamento che non sono coperte da nessuno dei summenzionati motivi legali, se il trattamento è necessario ai fini degli interessi legittimi perseguiti dalla nostra azienda o da una terza parte, eccetto laddove tali interessi siano superati dagli interessi o diritti e libertà fondamentali dell'interessato che richiedono la protezione dei dati personali. Tali operazioni di trattamento sono particolarmente ammissibili in quanto sono state espressamente menzionate dal legislatore europeo. Riteneva che potesse essere assunto un interesse legittimo se l'interessato fosse un cliente del titolare del trattamento (considerando 47, frase 2, GDPR).

## D. Categorie di dati personali interessati (articolo 14, paragrafo 1, lett. d) GDPR)

Dati dei clienti

Dati di potenziali clienti

Dati dei dipendenti

Dati dei fornitori

## E. Categorie di destinatari dei dati personali (articolo 14, paragrafo 1, lett. e) GDPR)

Autorità pubbliche

Entità esterne

Ulteriori entità esterne

Elaborazione interna

Elaborazione intragruppo

Altre entità

L'elenco dei nostri responsabili del trattamento e dei destinatari dei dati nei Paesi terzi e, se del caso, delle organizzazioni internazionali è pubblicato sul nostro sito web o può essere richiesto gratuitamente. Per richiedere tale elenco, si prega di contattare il nostro responsabile della protezione dei dati.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## F. Destinatari in un paese terzo e garanzie appropriate o adeguate e mezzi per ottenerne una copia o quando sono stati resi disponibili (articolo 14, paragrafo 1, lett. f), 46, paragrafo 1, articolo 46, paragrafo 2, lett. c) GDPR)

Tutte le società e le filiali che fanno parte del nostro gruppo (in seguito denominate "società del gruppo") che hanno la loro sede di attività o un ufficio in un paese terzo possono appartenere ai destinatari dei dati personali. Un elenco di tutte le società del gruppo può essere richiesto a noi.

Ai sensi dell'articolo 46, paragrafo 1, del GDPR, un titolare del trattamento o un responsabile del trattamento può trasferire dati personali solo a un paese terzo se il titolare del trattamento o il responsabile del trattamento ha fornito garanzie appropriate e a condizione che siano disponibili diritti soggetti a diritti esecutivi e rimedi giuridici efficaci per le persone interessate. Possono essere fornite opportune salvaguardie senza richiedere un'autorizzazione specifica da parte di un'autorità di vigilanza mediante clausole standard di protezione dei dati, articolo 46, paragrafo 2, lett. c) GDPR.

Le clausole contrattuali standard dell'Unione europea o altre garanzie appropriate sono concordate con tutti i beneficiari di paesi terzi prima della prima trasmissione di dati personali. Di conseguenza, è garantito che siano garantite garanzie appropriate, diritti soggetti a diritti esecutivi e rimedi giuridici efficaci per gli interessati. Ogni persona interessata può ottenere da noi una copia delle clausole contrattuali standard. Le clausole contrattuali standard sono inoltre disponibili nella Gazzetta ufficiale dell'Unione europea.

L'articolo 45, paragrafo 3, del Regolamento generale sulla protezione dei dati (GDPR) conferisce alla Commissione europea il potere di decidere, mediante un atto di esecuzione, che un Paese non appartenente all'UE garantisce un livello di protezione adeguato. Ciò significa un livello di protezione dei dati personali sostanzialmente equivalente al livello di protezione all'interno dell'UE. L'effetto delle decisioni di adeguatezza è che i dati personali possono fluire liberamente dall'UE (e da Norvegia, Liechtenstein e Islanda) verso un Paese terzo senza ulteriori ostacoli. Regole simili esistono anche per il Regno Unito, la Svizzera e alcuni altri Paesi.

Laddove la Commissione Europea o il governo di un altro Paese abbia deciso che un Paese terzo garantisce un livello di protezione adeguato e sia in vigore un quadro normativo valido (ad esempio, EU-U.S. Data Privacy Framework, Swiss-U.S. Data Privacy Framework, UK Extension to the EU-U.S. Data Privacy Framework), tutti i trasferimenti da parte nostra ai membri di tali quadri normativi (ad esempio, entità autocertificate) si basano esclusivamente sull'appartenenza di tali entità al rispettivo quadro normativo. Nel caso in cui noi o una delle entità del nostro gruppo sia membro di tale quadro, tutti i trasferimenti a noi o alla nostra entità del gruppo si basano esclusivamente sull'appartenenza dell'entità a tale quadro.

Ogni interessato può ottenere da noi una copia dei quadri normativi. Inoltre, i quadri sono disponibili anche nella Gazzetta ufficiale dell'Unione europea o nei materiali legali pubblicati o sui siti web delle autorità di controllo o di altre autorità o istituzioni competenti.


© All rights reserved by Heiko Maniero.

## G. Periodo per il quale saranno conservati i dati personali o, se ciò non fosse possibile, i criteri utilizzati per determinare tale periodo (articolo 14, paragrafo 2, lett. a), GDPR)

I criteri utilizzati per determinare il periodo di conservazione dei dati personali sono i rispettivi periodi di conservazione previsti dalla legge. Dopo la scadenza di tale periodo, i dati corrispondenti vengono regolarmente cancellati, a condizione che non siano più necessari per l'adempimento del contratto o l'inizio di un contratto.

Se non esiste un periodo di conservazione legale, il criterio è il periodo di conservazione contrattuale o interno.

## H. Notifica degli interessi legittimi perseguiti dal titolare del trattamento o da un terzo se il trattamento si basa sull'articolo 6, paragrafo 1, lett. f) GDPR (Art. 14 (2) lett. b) GDPR)

Ai sensi dell'articolo 6, paragrafo 1, lett. f) GDPR, il trattamento è lecito solo se il trattamento è necessario ai fini di interessi legittimi perseguiti dal titolare del trattamento o da un terzo, eccetto laddove tali interessi siano superati dagli interessi o dai diritti e dalle libertà fondamentali dell'interessato che richiedono protezione di dati personali. Secondo il considerando 47, frase 2, GDPR, potrebbe esistere un interesse legittimo qualora esista una relazione pertinente e appropriata tra l'interessato e il titolare del trattamento, ad es. in situazioni in cui l'interessato è un cliente del controllore. In tutti i casi in cui la nostra azienda elabora i dati personali in base all'articolo 6, paragrafo 1, lett. f) GDPR, il nostro interesse legittimo è nello svolgere la nostra attività a favore del benessere di tutti i nostri dipendenti e azionisti.

## I. Esistenza del diritto di richiedere al titolare del trattamento accesso e rettifica o cancellazione di dati personali o restrizione del trattamento in relazione all'interessato e di opporsi al trattamento nonché al diritto alla portabilità dei dati (articolo 14, paragrafo 2, lett. c) del GDPR)

Tutte le persone interessate hanno i seguenti diritti:

***Diritto di accesso***

Ogni soggetto interessato ha il diritto di accedere ai dati personali che lo riguardano. Il diritto di accesso si estende a tutti i dati elaborati da noi. Il diritto può essere esercitato facilmente e ad intervalli ragionevoli, al fine di essere a conoscenza e verificare la liceità del trattamento (Considerando 63 GDPR). Questo diritto deriva dall'art. 15 GDPR. L'interessato può contattarci per esercitare il diritto di accesso.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

***Diritto di rettifica***

Ai sensi dell'articolo 16, paragrafo 1, del GDPR, l'interessato ha il diritto di ottenere dal titolare del trattamento, senza indebito ritardo, la rettifica di dati personali inesatti che lo riguardano. Inoltre, l'articolo 16, paragrafo 2 del GDPR prevede che l'interessato abbia diritto, in considerazione delle finalità del trattamento, a che i dati personali siano incompleti, anche mediante la presentazione di una dichiarazione integrativa. L'interessato può contattarci per esercitare il diritto di rettifica.

***Diritto alla cancellazione (diritto di essere dimenticato)***

Inoltre, l'interessato ha il diritto alla cancellazione e all'oblio ai sensi dell'art. 17 GDPR. Questo diritto può essere esercitato anche contattandoci. A questo punto, tuttavia, vorremmo sottolineare che questo diritto non si applica nella misura in cui il trattamento è necessario per adempiere a un obbligo legale a cui è soggetta la nostra società, articolo 17, paragrafo 3, lett. b) GDPR. Ciò significa che possiamo approvare un'applicazione da cancellare solo dopo la scadenza del periodo di conservazione previsto dalla legge.

***Diritto alla restrizione dell'elaborazione***

Ai sensi dell'articolo 18 del GDPR, ogni interessato ha diritto a una restrizione del trattamento. La restrizione del trattamento può essere richiesta se una delle condizioni di cui all'articolo 18, paragrafo 1, lettere a) - d) GDPR è soddisfatto. L'interessato può contattarci per esercitare il diritto alla restrizione del trattamento.

***Diritto di obiettare***

Inoltre, l'art. 21 GDPR garantisce il diritto di obiettare. L'interessato può contattarci per esercitare il diritto di obiettare.

***Diritto alla portabilità dei dati***

L'articolo 20 del GDPR conferisce all'interessato il diritto alla portabilità dei dati. Ai sensi di questa disposizione, la persona interessata ha le condizioni di cui all'articolo 20, paragrafo 1, lett. a) e b) GDPR il diritto di ricevere i dati personali che lo riguardano, che lui o lei ha fornito a un titolare del trattamento, in un formato strutturato, comunemente usato e leggibile da una macchina e ha il diritto di trasmettere tali dati a un altro titolare del trattamento senza impedimenti dal controllore a cui sono stati forniti i dati personali. L'interessato può contattarci per esercitare il diritto alla portabilità dei dati.

## J. L'esistenza del diritto di revocare il consenso in qualsiasi momento, senza pregiudizio della liceità del trattamento basato sul consenso prima del suo ritiro, qualora il trattamento si basi sull'articolo 6, paragrafo 1, lett. a), l'articolo 9, paragrafo 2, lett. a) GDPR (articolo 14, paragrafo 2, lett. d) GDPR)

Se il trattamento dei dati personali è basato sull'art. 6 (1) lett. a) GDPR, che è il caso, se l'interessato ha acconsentito al trattamento dei dati personali per uno o più scopi specifici o è basato sull'articolo 9, paragrafo 2, lett. a) GDPR, che regola il consenso esplicito al trattamento di categorie speciali di dati


© All rights reserved by Heiko Maniero.

personali, l'interessato ha in base all'articolo 7 (3) Frase 1 GDPR il diritto di revocare il proprio consenso in qualsiasi momento.

Il ritiro del consenso non pregiudica la liceità del trattamento basato sul consenso prima del suo ritiro, articolo 7, paragrafo 3, frase 2 GDPR. Deve essere facile ritirare il consenso, art. 7 (3) Frase 4 GDPR. Pertanto, il ritiro del consenso può sempre avvenire nello stesso modo in cui è stato dato il consenso o in qualsiasi altro modo, che è considerato dall'interessato essere più semplice. Nella società dell'informazione di oggi, probabilmente il modo più semplice per ritirare il consenso è una semplice email. Se l'interessato desidera ritirare il suo consenso, ci è sufficiente una semplice email. In alternativa, l'interessato può scegliere qualsiasi altro modo per comunicare il suo ritiro del consenso a noi.

## K. Diritto di presentare un reclamo all'autorità di controllo (articolo 14, paragrafo 2, lett. e), 77, paragrafo 1 del GDPR)

Come titolare del trattamento, siamo obbligati a comunicare all'interessato il diritto di presentare un reclamo all'autorità di controllo, articolo 13, paragrafo 2, lett. d) GDPR. Il diritto di presentare un reclamo presso un'autorità di controllo è regolato dall'articolo 77, paragrafo 1 del GDPR. In base a tale disposizione, fatto salvo ogni altro rimedio amministrativo o giudiziario, ogni interessato ha il diritto di presentare un reclamo all'autorità di controllo, in particolare nello Stato membro della sua residenza abituale, luogo di lavoro o luogo di la presunta violazione se l'interessato ritiene che il trattamento di dati personali che lo riguardano violino il regolamento generale sulla protezione dei dati. Il diritto di presentare una denuncia presso un'autorità di controllo era limitato dal diritto dell'Unione solo in tal modo, che poteva essere esercitato solo dinanzi a un'unica autorità di vigilanza (Considerando 141, frase 1, del GDPR). Questa regola è intesa ad evitare i doppi reclami della stessa persona interessata nella stessa materia. Se una persona interessata desidera presentare un reclamo su di noi, abbiamo quindi chiesto di contattare solo una singola autorità di controllo.

## L. Fonte: i dati personali provengono e, se del caso, se provengono da fonti accessibili al pubblico (articolo 14, paragrafo 2, lett. f) GDPR)

In linea di principio, i dati personali vengono raccolti direttamente dall'interessato o in collaborazione con un'autorità (ad esempio, il recupero di dati da un registro ufficiale). Altri dati sugli interessati sono derivati da trasferimenti di società del gruppo. Nel contesto di queste informazioni generali, la denominazione delle fonti esatte da cui provengono i dati personali è impossibile o comporterebbe uno sforzo sproporzionato ai sensi dell'Art. 14 (5) lett. b) GDPR. In linea di principio, non raccogliamo dati personali da fonti accessibili pubblicamente.

Qualsiasi soggetto interessato può contattarci in qualsiasi momento per ottenere informazioni più dettagliate sulle esatte fonti dei dati personali che lo riguardano. Qualora l'origine dei dati personali non


© All rights reserved by Heiko Maniero.

possa essere fornita all'interessato in quanto sono state utilizzate varie fonti, è opportuno fornire informazioni generali (considerando 61, frase 4, GDPR).

### M. Esistenza di processi decisionali automatizzati, inclusa la profilazione, di cui all'articolo 22, paragrafi 1 e 4, del GDPR e, almeno in tali casi, informazioni significative sulla logica in questione, nonché sulla significatività e le conseguenze previste di tale trattamento per l'interessato (articolo 14, paragrafo 2, lett. g) GDPR)

In quanto azienda responsabile, di solito non utilizziamo il processo decisionale automatizzato o la profilazione. Se, in casi eccezionali, effettuiamo un processo decisionale o di profilazione automatizzato, informeremo l'interessato separatamente o tramite una sottosezione della nostra informativa sulla privacy (sul nostro sito web). In tal caso, si applica quanto segue:

Il processo decisionale automatizzato - compresa la profilazione - può avvenire se (1) è necessario per la stipula o l'esecuzione di un contratto tra l'interessato e noi, oppure (2) è autorizzato dal diritto dell'Unione o degli Stati membri a cui siamo soggetti e che prevede anche misure idonee a salvaguardare i diritti e le libertà dell'interessato e i suoi legittimi interessi, oppure (3) si basa sul consenso esplicito dell'interessato.

Nei casi di cui all'articolo 22, paragrafo 2, lettere a) e c), del GDPR, attueremo misure adeguate per salvaguardare i diritti e le libertà dell'interessato e i suoi legittimi interessi. In questi casi, l'interessato ha il diritto di ottenere l'intervento umano da parte del responsabile del trattamento, di esprimere il proprio punto di vista e di contestare la decisione.

Informazioni significative sulla logica, l'importanza e le conseguenze previste di tale trattamento per l'interessato sono contenute nella nostra politica sulla privacy.

## III. EU-U.S. Data Privacy Framework (EU-U.S. DPF), UK Extension to the EU-U.S. DPF, Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF)

Se la nostra organizzazione è un membro certificato dell'EU-U.S. Data Privacy Framework (EU-U.S. DPF) e/o della UK Extension to the EU-U.S. DPF e/o del Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF), si applica quanto segue:

Ci atteniamo all'EU-U.S. Data Privacy Framework (EU-U.S. DPF) e alla UK Extension to the EU-U.S. DPF, così come al Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF), come stabilito dal U.S. Department of Commerce. La nostra azienda ha confermato al Dipartimento del Commercio degli Stati Uniti che rispetta gli EU-U.S. Data Privacy Framework Principles (EU-U.S. DPF Principles) relativamente al trattamento dei dati personali che riceve dall'Unione Europea e dal Regno Unito in base all'EU-U.S.


© All rights reserved by Heiko Maniero.

DPF e alla UK Extension to the EU-U.S. DPF. La nostra azienda ha anche confermato di rispettare i Swiss-U.S. Data Privacy Framework Principles (Swiss-U.S. DPF Principles) per quanto riguarda il trattamento dei dati personali ricevuti dalla Svizzera in base al Swiss-U.S. DPF. In caso di contraddizione tra le disposizioni della nostra politica sulla privacy e gli EU-U.S. DPF Principles e/o i Swiss-U.S. DPF Principles, i Principles prevarranno.

Per saperne di più sul programma Data Privacy Framework (DPF) e per visualizzare la nostra certificazione, si prega di visitare https://www.dataprivacyframework.gov/.

Le altre unità statunitensi o le filiali della nostra azienda che aderiscono anche agli EU-U.S. DPF Principals, inclusa la UK Extension to the EU-U.S. DPF e i Swiss-U.S. DPF Principals, se presenti, sono elencate nella nostra politica sulla privacy.

In conformità con l'EU-U.S. DPF, la UK Extension to the EU-U.S. DPF e il Swiss-U.S. DPF, la nostra azienda si impegna a collaborare con il comitato istituito dalle autorità europee per la protezione dei dati, l'Information Commissioner's Office (ICO) del Regno Unito e il Commissario federale per la protezione dei dati e la trasparenza (EDÖB) della Svizzera, e a seguire i loro consigli riguardo alle lamentele irrisolte sul nostro trattamento dei dati personali che riceviamo in base all'EU-U.S. DPF, alla UK Extension to the EU-U.S. DPF e al Swiss-U.S. DPF.

Informiamo le persone interessate riguardo alle autorità europee per la protezione dei dati competenti per gestire le lamentele sul trattamento dei dati personali da parte della nostra organizzazione, nella parte superiore di questo documento di trasparenza, e che offriamo un rimedio legale adeguato e gratuito.

Informiamo tutte le persone interessate che la nostra azienda è soggetta ai poteri di indagine e di enforcement della Federal Trade Commission (FTC).

Le persone interessate hanno la possibilità, in determinate condizioni, di richiedere un arbitrato vincolante. La nostra organizzazione è obbligata a risolvere le richieste e ad aderire alle condizioni dell'Allegato I dei DPF-Principals, a condizione che la persona interessata abbia richiesto un arbitrato vincolante notificando la nostra organizzazione e che le procedure e le condizioni dell'Allegato I dei Principals siano state rispettate.

Informiamo qui tutte le persone interessate sulla responsabilità della nostra organizzazione in caso di trasferimento di dati personali a terzi.

Per domande delle persone interessate o delle autorità di controllo della protezione dei dati, abbiamo nominato i rappresentanti locali menzionati nella parte superiore di questo documento di trasparenza.

Offriamo la possibilità di scegliere (Opt-out) se i dati personali (i) devono essere condivisi con terzi o (ii) utilizzati per scopi sostanzialmente diversi da quelli per i quali sono stati originariamente raccolti o successivamente autorizzati. Il meccanismo chiaro, ben visibile e facilmente accessibile per esercitare il proprio diritto di scelta consiste nel contattare il nostro Data Protection Officer (DSB) via email. Non si ha alcuna possibilità di scelta e non siamo obbligati quando i dati sono condivisi con un terzo che agisce


© All rights reserved by Heiko Maniero.

come agente o processore per nostro conto e secondo le nostre istruzioni. Tuttavia, stipuliamo sempre un contratto con tale agente o processore.

Per i dati sensibili (ovvero dati personali che includono informazioni sulla salute, l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale o informazioni sulla vita sessuale della persona interessata), otteniamo il vostro consenso esplicito (Opt-in) se tali dati (i) devono essere condivisi o (ii) utilizzati per scopi diversi da quelli per cui sono stati originariamente raccolti o per cui avete successivamente dato il vostro consenso, facendo la vostra scelta di Opt-in. Inoltre, trattiamo tutti i dati personali che riceviamo da terzi come sensibili se il terzo li ha identificati e trattati come tali.

Vi informiamo qui sulla necessità di divulgare dati personali in risposta a richieste legali dalle autorità, inclusa l'esecuzione delle richieste di sicurezza nazionale o di applicazione della legge.

Nel trasferimento di dati personali a un terzo che agisce come responsabile, ci atteniamo ai Principals di notifica e scelta. Inoltre, stipuliamo un contratto con il terzo responsabile del trattamento che prevede che questi dati possano essere trattati solo per scopi limitati e specifici in conformità con il consenso fornito e che il destinatario offra lo stesso livello di protezione dei Principals del DPF e ci notifichi se determina di non poter più soddisfare questo obbligo. Il contratto prevede che il terzo, che agisce come responsabile, interrompa il trattamento o adotti altre misure ragionevoli e appropriate per rimediare se tale determinazione viene fatta.

Nel trasferimento di dati personali a un terzo che agisce come agente o processore, (i) trasferiamo questi dati solo per scopi limitati e specifici; (ii) ci assicuriamo che l'agente o il processore sia obbligato a fornire almeno lo stesso livello di protezione dei dati richiesto dai DPF-Principals; (iii) adottiamo misure ragionevoli e appropriate per garantire che l'agente o il processore tratti effettivamente i dati personali trasferiti in modo conforme ai nostri obblighi ai sensi dei DPF-Principals; (iv) richiediamo che l'agente o il processore ci notifichi se determina di non poter più soddisfare il suo obbligo di fornire lo stesso livello di protezione richiesto dai DPF-Principals; (v) dopo tale notifica, anche sotto (iv), adottiamo misure ragionevoli e appropriate per interrompere il trattamento non autorizzato e rimediare; e (vi) forniamo al DPF Department, su richiesta, un riassunto o un esemplare rappresentativo delle disposizioni pertinenti sulla privacy del nostro contratto con tale agente.

In conformità con l'EU-U.S. DPF e/o la UK Extension to the EU-U.S. DPF e/o il Swiss-U.S. DPF, la nostra organizzazione si impegna a cooperare con il comitato istituito dalle autorità di protezione dei dati dell'UE e dall'Information Commissioner's Office (ICO) del Regno Unito e dal Commissario federale per la protezione dei dati e la trasparenza (EDÖB) della Svizzera, e a seguire i loro consigli riguardo le lamentele irrisolte sul nostro trattamento dei dati personali che riceviamo in relazione al lavoro sotto l'EU-U.S. DPF, la UK Extension to the EU-U.S. DPF e il Swiss-U.S. DPF.

Tutti gli interessati che si trovano temporaneamente nell'Unione Europea (UE), nello Spazio Economico Europeo (SEE) o nel Regno Unito, o che vi hanno il domicilio o la residenza abituale, hanno diritto ai


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

diritti e alle prerogative degli interessati pubblicati nel nostro Documento sulla trasparenza, che derivano anche dagli articoli da 15 a 22 del GDPR, compreso il diritto di accesso ai dati personali. Abbiamo reso disponibili queste informazioni in tutte le lingue dell'UE e del SEE. La versione in lingua inglese si applica al Regno Unito.

Tutti gli interessati che risiedono temporaneamente in Svizzera o che vi hanno il domicilio o la residenza abituale hanno diritto ai diritti e alle prerogative degli interessati ai sensi della Legge svizzera sulla protezione dei dati (LPD) e del Regolamento svizzero sulla protezione dei dati (RGPD), pubblicati nel nostro Documento sulla trasparenza, compreso il diritto di accesso ai dati personali. Abbiamo fornito queste informazioni nelle tre lingue ufficiali della Svizzera (tedesco, italiano e francese).


© All rights reserved by Heiko Maniero.

# ITALIAN: Informazioni sul trattamento dei dati personali per dipendenti e richiedenti (articolo 13, 14 GDPR)

Gentile signore o signora,

I dati personali di dipendenti e candidati meritano una protezione speciale. Il nostro obiettivo è di mantenere il nostro livello di protezione dei dati ad un alto livello. Pertanto, sviluppiamo ordinariamente i nostri concetti di protezione dei dati e sicurezza dei dati.

Ovviamente, rispettiamo le disposizioni legali sulla protezione dei dati. Ai sensi dell'articolo 13, 14 GDPR, i titolari del trattamento soddisfano specifici requisiti di informazione nel trattamento dei dati personali. Questo documento soddisfa questi obblighi.

La terminologia della regolamentazione legale è complicata. Sfortunatamente, l'uso di termini legali non può essere evitato nella preparazione di questo documento. Pertanto, vorremmo sottolineare che siete sempre i benvenuti a contattarci per tutte le domande riguardanti questo documento, i termini usati o le formulazioni.

## I. Rispetto dei requisiti in materia di informazione quando i dati personali sono raccolti dall'interessato (articolo 13 del GDPR)

### A. Identità e recapiti del titolare del trattamento (articolo 13, paragrafo 1, lett. a) del GDPR)

Vedi sopra

### B. Dati di contatto del responsabile della protezione dei dati (articolo 13, paragrafo 1, lett. b) del GDPR)

Vedi sopra

### C. Finalità del trattamento al quale sono destinati i dati personali nonché base legale per il trattamento (articolo 13, paragrafo 1, lett. c) GDPR)

Per i dati del richiedente, lo scopo del trattamento dei dati è di condurre un esame dell'applicazione durante il processo di assunzione. A tale scopo, elaboriamo tutti i dati forniti dall'utente. Sulla base dei dati presentati durante il processo di assunzione, verificheremo se sei stato invitato a un colloquio di


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

lavoro (parte del processo di selezione). Nel caso di candidati generalmente idonei, in particolare nel contesto del colloquio di lavoro, elaboriamo alcuni altri dati personali forniti da voi, che è essenziale per la nostra decisione di selezione. Se sei assunto da noi, i dati del candidato cambieranno automaticamente in dati dei dipendenti. Come parte del processo di reclutamento, elaboreremo altri dati personali che ti richiediamo e che sono necessari per avviare o soddisfare il tuo contratto (come numeri di identificazione personale o numeri di imposta). Per i dati dei dipendenti, lo scopo del trattamento dei dati è l'esecuzione del contratto di lavoro o l'adempimento ad altre disposizioni legali applicabili al rapporto di lavoro (es. Diritto tributario), nonché l'uso dei dati personali per eseguire il contratto di lavoro concluso con voi (es. pubblicazione del tuo nome e delle informazioni di contatto all'interno dell'azienda o ai clienti). I dati dei dipendenti vengono archiviati dopo la cessazione del rapporto di lavoro per rispettare i periodi di conservazione legale.

La base giuridica per l'elaborazione dei dati è l'articolo 6, paragrafo 1, lett. b) GDPR, articolo 9, paragrafo 2, lett. b) e h) GDPR, articolo 88 (1) del GDPR e legislazione nazionale, come per la Germania Sezione 26 BDSG (Legge federale sulla protezione dei dati).

## D. Categorie di destinatari dei dati personali (articolo 13, paragrafo 1, lett. e) GDPR)

Autorità pubbliche

Entità esterne

Ulteriori entità esterne

Elaborazione interna

Elaborazione intragruppo

Altre entità

L'elenco dei nostri responsabili del trattamento e dei destinatari dei dati nei Paesi terzi e, se del caso, delle organizzazioni internazionali è pubblicato sul nostro sito web o può essere richiesto gratuitamente. Per richiedere tale elenco, si prega di contattare il nostro responsabile della protezione dei dati.

## E. Destinatari in un paese terzo e garanzie appropriate o adeguate e i mezzi con cui ottenerne una copia o quando sono stati resi disponibili (articolo 13, paragrafo 1, lett. f), 46, paragrafo 1, articolo 46, paragrafo 2, lett. c) GDPR)

Tutte le società e le filiali che fanno parte del nostro gruppo (in seguito denominate "società del gruppo") che hanno la loro sede di attività o un ufficio in un paese terzo possono appartenere ai destinatari dei dati personali. Un elenco di tutte le società del gruppo o dei destinatari può essere richiesto a noi.


© All rights reserved by Heiko Maniero.

Ai sensi dell'articolo 46, paragrafo 1, del GDPR, un titolare del trattamento o un responsabile del trattamento può trasferire dati personali solo a un paese terzo se il titolare del trattamento o il responsabile del trattamento ha fornito garanzie appropriate e a condizione che siano disponibili diritti soggetti a diritti esecutivi e rimedi giuridici efficaci per le persone interessate. Possono essere fornite appropriate misure di salvaguardia senza richiedere un'autorizzazione specifica da parte di un'autorità di controllo mediante clausole contrattuali standard, articolo 46, paragrafo 2, lett. c) GDPR.

Le clausole contrattuali standard dell'Unione europea o altre garanzie appropriate sono concordate con tutti i beneficiari di paesi terzi prima della prima trasmissione di dati personali. Di conseguenza, è garantito che siano garantite garanzie appropriate, diritti soggetti a diritti esecutivi e rimedi giuridici efficaci per gli interessati. Ogni persona interessata può ottenere da noi una copia delle clausole contrattuali standard. Le clausole contrattuali standard sono inoltre disponibili nella Gazzetta ufficiale dell'Unione europea.

L'articolo 45, paragrafo 3, del Regolamento generale sulla protezione dei dati (GDPR) conferisce alla Commissione europea il potere di decidere, mediante un atto di esecuzione, che un Paese non appartenente all'UE garantisce un livello di protezione adeguato. Ciò significa un livello di protezione dei dati personali sostanzialmente equivalente al livello di protezione all'interno dell'UE. L'effetto delle decisioni di adeguatezza è che i dati personali possono fluire liberamente dall'UE (e da Norvegia, Liechtenstein e Islanda) verso un Paese terzo senza ulteriori ostacoli. Regole simili esistono anche per il Regno Unito, la Svizzera e alcuni altri Paesi.

Laddove la Commissione Europea o il governo di un altro Paese abbia deciso che un Paese terzo garantisce un livello di protezione adeguato e sia in vigore un quadro normativo valido (ad esempio, EU-U.S. Data Privacy Framework, Swiss-U.S. Data Privacy Framework, UK Extension to the EU-U.S. Data Privacy Framework), tutti i trasferimenti da parte nostra ai membri di tali quadri normativi (ad esempio, entità autocertificate) si basano esclusivamente sull'appartenenza di tali entità al rispettivo quadro normativo. Nel caso in cui noi o una delle entità del nostro gruppo sia membro di tale quadro, tutti i trasferimenti a noi o alla nostra entità del gruppo si basano esclusivamente sull'appartenenza dell'entità a tale quadro.

Ogni interessato può ottenere da noi una copia dei quadri normativi. Inoltre, i quadri sono disponibili anche nella Gazzetta ufficiale dell'Unione europea o nei materiali legali pubblicati o sui siti web delle autorità di controllo o di altre autorità o istituzioni competenti.

## F. Periodo per il quale saranno conservati i dati personali o, se ciò non fosse possibile, i criteri utilizzati per determinare tale periodo (articolo 13, paragrafo 2, lett. a), GDPR)

La durata della conservazione dei dati personali dei candidati è di 6 mesi. Per i dati dei dipendenti si applica il rispettivo periodo di conservazione previsto dalla legge. Dopo la scadenza di tale periodo, i dati


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

corrispondenti vengono regolarmente cancellati, a condizione che non siano più necessari per l'adempimento del contratto o l'inizio di un contratto.

## G. Esistenza del diritto di richiedere al titolare del trattamento l'accesso e la rettifica o cancellazione di dati personali o la limitazione del trattamento della persona interessata o di opporsi al trattamento nonché il diritto alla portabilità dei dati (articolo 13, paragrafo 2, lett. b) del GDPR)

Tutte le persone interessate hanno i seguenti diritti:

***Diritto di accesso***

Ogni soggetto interessato ha il diritto di accedere ai dati personali che lo riguardano. Il diritto di accesso si estende a tutti i dati elaborati da noi. Il diritto può essere esercitato facilmente e ad intervalli ragionevoli, al fine di essere a conoscenza e verificare la liceità del trattamento (Considerando 63 GDPR). Questo diritto deriva dall'art. 15 GDPR. L'interessato può contattarci per esercitare il diritto di accesso.

***Diritto di rettifica***

Ai sensi dell'articolo 16, paragrafo 1, del GDPR, l'interessato ha il diritto di ottenere dal titolare del trattamento, senza indebito ritardo, la rettifica di dati personali inesatti che lo riguardano. Inoltre, l'articolo 16, paragrafo 2 del GDPR prevede che l'interessato abbia diritto, in considerazione delle finalità del trattamento, a che i dati personali siano incompleti, anche mediante la presentazione di una dichiarazione integrativa. L'interessato può contattarci per esercitare il diritto di rettifica.

***Diritto alla cancellazione (diritto di essere dimenticato)***

Inoltre, l'interessato ha il diritto alla cancellazione e all'oblio ai sensi dell'art. 17 GDPR. Questo diritto può essere esercitato anche contattandoci. A questo punto, tuttavia, vorremmo sottolineare che questo diritto non si applica nella misura in cui il trattamento è necessario per adempiere a un obbligo legale a cui è soggetta la nostra società, articolo 17, paragrafo 3, lett. b) GDPR. Ciò significa che possiamo approvare un'applicazione da cancellare solo dopo la scadenza del periodo di conservazione previsto dalla legge.

***Diritto alla restrizione dell'elaborazione***

Ai sensi dell'articolo 18 del GDPR, ogni interessato ha diritto a una restrizione del trattamento. La restrizione del trattamento può essere richiesta se una delle condizioni di cui all'articolo 18, paragrafo 1, lettere a)-d) GDPR è soddisfatto. L'interessato può contattarci per esercitare il diritto alla restrizione del trattamento.

***Diritto di obiettare***

Inoltre, l'art. 21 GDPR garantisce il diritto di obiettare. L'interessato può contattarci per esercitare il diritto di obiettare.


© All rights reserved by Heiko Maniero.

***Diritto alla portabilità dei dati***

L'articolo 20 del GDPR conferisce all'interessato il diritto alla portabilità dei dati. Ai sensi di questa disposizione, la persona interessata ha le condizioni di cui all'articolo 20, paragrafo 1, lett. a) e b) GDPR il diritto di ricevere i dati personali che lo riguardano, che lui o lei ha fornito a un titolare del trattamento, in un formato strutturato, comunemente usato e leggibile da una macchina e ha il diritto di trasmettere tali dati a un altro titolare del trattamento senza impedimenti dal controllore a cui sono stati forniti i dati personali. L'interessato può contattarci per esercitare il diritto alla portabilità dei dati.

## H. L'esistenza del diritto di revocare il consenso in qualsiasi momento, senza pregiudizio della liceità del trattamento basato sul consenso prima del suo ritiro, qualora il trattamento si basi sull'articolo 6, paragrafo 1, lett. a) GDPR o l'Articolo 9 (2) lett. a) GDPR (articolo 13, paragrafo 2, lett. c) del GDPR)

Se il trattamento dei dati personali è basato sull'art. 6 (1) lett. a) GDPR, che è il caso, se l'interessato ha acconsentito al trattamento dei dati personali per uno o più scopi specifici o è basato sull'articolo 9, paragrafo 2, lett. a) GDPR, che regola il consenso esplicito al trattamento di categorie speciali di dati personali, l'interessato ha in base all'articolo 7 (3) Frase 1 GDPR il diritto di revocare il proprio consenso in qualsiasi momento.

Il ritiro del consenso non pregiudica la liceità del trattamento basato sul consenso prima del suo ritiro, articolo 7, paragrafo 3, frase 2 GDPR. Deve essere facile ritirare il consenso, art. 7 (3) Frase 4 GDPR. Pertanto, il ritiro del consenso può sempre avvenire nello stesso modo in cui è stato dato il consenso o in qualsiasi altro modo, che è considerato dall'interessato essere più semplice. Nella società dell'informazione di oggi, probabilmente il modo più semplice per ritirare il consenso è una semplice email. Se l'interessato desidera ritirare il suo consenso, ci è sufficiente una semplice email. In alternativa, l'interessato può scegliere qualsiasi altro modo per comunicare il suo ritiro del consenso a noi.

## I. Diritto di presentare un reclamo all'autorità di controllo (articolo 13, paragrafo 2, lett. d), 77, paragrafo 1 del GDPR)

Come titolare del trattamento, siamo obbligati a comunicare all'interessato il diritto di presentare un reclamo all'autorità di controllo, articolo 13, paragrafo 2, lett. d) GDPR. Il diritto di presentare un reclamo presso un'autorità di controllo è regolato dall'articolo 77, paragrafo 1 del GDPR. In base a tale disposizione, fatto salvo ogni altro rimedio amministrativo o giudiziario, ogni interessato ha il diritto di presentare un reclamo all'autorità di controllo, in particolare nello Stato membro della sua residenza abituale, luogo di lavoro o luogo di la presunta violazione se l'interessato ritiene che il trattamento di dati personali che lo riguardano violino il regolamento generale sulla protezione dei dati. Il diritto di presentare una denuncia presso un'autorità di controllo era limitato dal diritto dell'Unione solo in tal modo, che poteva essere esercitato solo dinanzi a un'unica autorità di vigilanza (Considerando 141, frase 1, del GDPR).


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

Questa regola è intesa ad evitare i doppi reclami della stessa persona interessata nella stessa materia. Se una persona interessata desidera presentare un reclamo su di noi, abbiamo quindi chiesto di contattare solo una singola autorità di controllo.

## J. Fornitura di dati personali come requisito legale o contrattuale; Requisito necessario per stipulare un contratto; Obbligo dell'interessato di fornire i dati personali; possibili conseguenze del mancato conferimento di tali dati (articolo 13, paragrafo 2, lett. e) GDPR)

Chiariamo che la fornitura di dati personali è in parte richiesta dalla legge (ad es. Regolamenti fiscali) o può anche derivare da disposizioni contrattuali (ad esempio informazioni sul partner contrattuale).

A volte può essere necessario concludere un contratto che l'interessato fornisca dati personali, che devono successivamente essere elaborati da noi. L'interessato è, per esempio, obbligato a fornire dati personali quando la nostra azienda firma un contratto con lui o lei. La mancata fornitura dei dati personali avrebbe come conseguenza che il contratto con l'interessato non poteva essere concluso.

Prima che i dati personali siano forniti dall'interessato, l'interessato deve contattarci. Chiariamo all'interessato se la fornitura dei dati personali è richiesta dalla legge o dal contratto o è necessaria per la conclusione del contratto, se esiste l'obbligo di fornire i dati personali e le conseguenze della mancata fornitura dei dati personali.

## K. Esistenza di processi decisionali automatizzati, inclusa la profilazione, di cui all'articolo 22, paragrafi 1 e 4, del GDPR e, almeno in tali casi, informazioni significative sulla logica in questione, nonché sulla significatività e le conseguenze previste di tale trattamento per l'interessato (articolo 13, paragrafo 2, lett. f) GDPR)

In quanto azienda responsabile, di solito non utilizziamo il processo decisionale automatizzato o la profilazione. Se, in casi eccezionali, effettuiamo un processo decisionale o di profilazione automatizzato, informeremo l'interessato separatamente o tramite una sottosezione della nostra informativa sulla privacy (sul nostro sito web). In tal caso, si applica quanto segue:

Il processo decisionale automatizzato - compresa la profilazione - può avvenire se (1) è necessario per la stipula o l'esecuzione di un contratto tra l'interessato e noi, oppure (2) è autorizzato dal diritto dell'Unione o degli Stati membri a cui siamo soggetti e che prevede anche misure idonee a salvaguardare i diritti e le libertà dell'interessato e i suoi legittimi interessi, oppure (3) si basa sul consenso esplicito dell'interessato.

Nei casi di cui all'articolo 22, paragrafo 2, lettere a) e c), del GDPR, attueremo misure adeguate per salvaguardare i diritti e le libertà dell'interessato e i suoi legittimi interessi. In questi casi, l'interessato ha


© All rights reserved by Heiko Maniero.

il diritto di ottenere l'intervento umano da parte del responsabile del trattamento, di esprimere il proprio punto di vista e di contestare la decisione.

Informazioni significative sulla logica, l'importanza e le conseguenze previste di tale trattamento per l'interessato sono contenute nella nostra politica sulla privacy.

## II. Rispetto dei requisiti di informazione quando i dati personali non sono raccolti dall'interessato (articolo 14 del GDPR)

### A. Identità e recapiti del titolare del trattamento (articolo 14, paragrafo 1, lett. a), del GDPR)

Vedi sopra

### B. Dati di contatto del responsabile della protezione dei dati (articolo 14, paragrafo 1, lett. b) del GDPR)

Vedi sopra

### C. Finalità del trattamento per il quale sono destinati i dati personali nonché base legale per il trattamento (articolo 14, paragrafo 1, lett. c) GDPR)

Per i dati del richiedente non raccolti dall'interessato, lo scopo del trattamento dei dati è di condurre un esame dell'applicazione durante il processo di assunzione. A tal fine, potremmo elaborare dati non raccolti da te. Sulla base dei dati elaborati durante il processo di assunzione, verificheremo se sei stato invitato a un colloquio di lavoro (parte del processo di selezione). Se sei assunto da noi, i dati del candidato si convertiranno automaticamente in dati dei dipendenti. Per i dati dei dipendenti, lo scopo del trattamento dei dati è l'esecuzione del contratto di lavoro o l'osservanza di altre disposizioni legali applicabili al rapporto di lavoro. I dati dei dipendenti vengono archiviati dopo la cessazione del rapporto di lavoro per rispettare i periodi di conservazione legale.

La base giuridica per l'elaborazione dei dati è l'articolo 6, paragrafo 1, lett. b) e f) GDPR, articolo 9, paragrafo 2, lett. b) e h) GDPR, articolo 88 (1) del GDPR e legislazione nazionale, come per la Germania Sezione 26 BDSG (Legge federale sulla protezione dei dati).

### D. Categorie di dati personali interessati (articolo 14, paragrafo 1, lett. d) GDPR)


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

Dati del richiedente

Dati dei dipendenti

## E. Categorie di destinatari dei dati personali (articolo 14, paragrafo 1, lett. e) GDPR)

Autorità pubbliche

Entità esterne

Ulteriori entità esterne

Elaborazione interna

Elaborazione intragruppo

Altre entità

L'elenco dei nostri responsabili del trattamento e dei destinatari dei dati nei Paesi terzi e, se del caso, delle organizzazioni internazionali è pubblicato sul nostro sito web o può essere richiesto gratuitamente. Per richiedere tale elenco, si prega di contattare il nostro responsabile della protezione dei dati.

## F. Destinatari in un paese terzo e garanzie appropriate o adeguate e mezzi per ottenerne una copia o quando sono stati resi disponibili (articolo 14, paragrafo 1, lett. f), 46, paragrafo 1, articolo 46, paragrafo 2, lett. c) GDPR)

Tutte le società e le filiali che fanno parte del nostro gruppo (in seguito denominate "società del gruppo") che hanno la loro sede di attività o un ufficio in un paese terzo possono appartenere ai destinatari dei dati personali. Un elenco di tutte le società del gruppo o dei destinatari può essere richiesto a noi.

Ai sensi dell'articolo 46, paragrafo 1 del GDPR, un titolare del trattamento o un responsabile del trattamento può trasferire dati personali solo a un paese terzo se il titolare del trattamento o il responsabile del trattamento ha fornito garanzie appropriate e a condizione che siano disponibili diritti soggetti a diritti esecutivi e rimedi giuridici efficaci per le persone interessate. Possono essere fornite opportune salvaguardie senza richiedere un'autorizzazione specifica da parte di un'autorità di controllo mediante clausole standard di protezione dei dati, articolo 46, paragrafo 2, lett. c) GDPR.

Le clausole contrattuali standard dell'Unione europea o altre garanzie appropriate sono concordate con tutti i beneficiari di paesi terzi prima della prima trasmissione di dati personali. Di conseguenza, è garantito che siano garantite garanzie appropriate, diritti soggetti a diritti esecutivi e rimedi giuridici efficaci per gli


© All rights reserved by Heiko Maniero.

interessati. Ogni persona interessata può ottenere da noi una copia delle clausole contrattuali standard. Le clausole contrattuali standard sono inoltre disponibili nella Gazzetta ufficiale dell'Unione europea.

L'articolo 45, paragrafo 3, del Regolamento generale sulla protezione dei dati (GDPR) conferisce alla Commissione europea il potere di decidere, mediante un atto di esecuzione, che un Paese non appartenente all'UE garantisce un livello di protezione adeguato. Ciò significa un livello di protezione dei dati personali sostanzialmente equivalente al livello di protezione all'interno dell'UE. L'effetto delle decisioni di adeguatezza è che i dati personali possono fluire liberamente dall'UE (e da Norvegia, Liechtenstein e Islanda) verso un Paese terzo senza ulteriori ostacoli. Regole simili esistono anche per il Regno Unito, la Svizzera e alcuni altri Paesi.

Laddove la Commissione Europea o il governo di un altro Paese abbia deciso che un Paese terzo garantisce un livello di protezione adeguato e sia in vigore un quadro normativo valido (ad esempio, EU-U.S. Data Privacy Framework, Swiss-U.S. Data Privacy Framework, UK Extension to the EU-U.S. Data Privacy Framework), tutti i trasferimenti da parte nostra ai membri di tali quadri normativi (ad esempio, entità autocertificate) si basano esclusivamente sull'appartenenza di tali entità al rispettivo quadro normativo. Nel caso in cui noi o una delle entità del nostro gruppo sia membro di tale quadro, tutti i trasferimenti a noi o alla nostra entità del gruppo si basano esclusivamente sull'appartenenza dell'entità a tale quadro.

Ogni interessato può ottenere da noi una copia dei quadri normativi. Inoltre, i quadri sono disponibili anche nella Gazzetta ufficiale dell'Unione europea o nei materiali legali pubblicati o sui siti web delle autorità di controllo o di altre autorità o istituzioni competenti.

## G. Periodo per il quale saranno conservati i dati personali o, se ciò non fosse possibile, i criteri utilizzati per determinare tale periodo (articolo 14, paragrafo 2, lett. a) GDPR)

La durata della conservazione dei dati personali dei candidati è di 6 mesi. Per i dati dei dipendenti si applica il rispettivo periodo di conservazione previsto dalla legge. Dopo la scadenza di tale periodo, i dati corrispondenti vengono regolarmente cancellati, a condizione che non siano più necessari per l'adempimento del contratto o l'inizio di un contratto.

## H. Notifica degli interessi legittimi perseguiti dal titolare del trattamento o da un terzo se il trattamento si basa sull'articolo 6, paragrafo 1, lett. f) GDPR (Art. 14 (2) lett. b) GDPR)

Ai sensi dell'articolo 6, paragrafo 1, lett. f) GDPR, il trattamento è lecito solo se il trattamento è necessario ai fini di interessi legittimi perseguiti dal titolare del trattamento o da un terzo, eccetto laddove tali interessi siano superati dagli interessi o dai diritti e dalle libertà fondamentali dell'interessato che richiedono


© All rights reserved by Heiko Maniero.

protezione di dati personali. Secondo il considerando 47, frase 2, GDPR, potrebbe esistere un interesse legittimo qualora esista una relazione pertinente e appropriata tra l'interessato e il titolare del trattamento, ad es. in situazioni in cui l'interessato è un cliente del titolare del trattamento. In tutti i casi in cui la nostra società elabora i dati del richiedente in base all'articolo 6, paragrafo 1, lett. a). Per GDPR, il nostro legittimo interesse è l'impiego di personale e professionisti adatti.

## I. Esistenza del diritto di richiedere al titolare del trattamento accesso e rettifica o cancellazione di dati personali o restrizione del trattamento in relazione all'interessato e di opporsi al trattamento nonché al diritto alla portabilità dei dati (articolo 14, paragrafo 2, lett. c) del GDPR)

Tutte le persone interessate hanno i seguenti diritti:

***Diritto di accesso***

Ogni soggetto interessato ha il diritto di accedere ai dati personali che lo riguardano. Il diritto di accesso si estende a tutti i dati elaborati da noi. Il diritto può essere esercitato facilmente e ad intervalli ragionevoli, al fine di essere a conoscenza e verificare la liceità del trattamento (Considerando 63 GDPR). Questo diritto deriva dall'art. 15 GDPR. L'interessato può contattarci per esercitare il diritto di accesso.

***Diritto di rettifica***

Ai sensi dell'articolo 16, paragrafo 1, del GDPR, l'interessato ha il diritto di ottenere dal titolare del trattamento, senza indebito ritardo, la rettifica di dati personali inesatti che lo riguardano. Inoltre, l'articolo 16, paragrafo 2 del GDPR prevede che l'interessato abbia diritto, in considerazione delle finalità del trattamento, a che i dati personali siano incompleti, anche mediante la presentazione di una dichiarazione integrativa. L'interessato può contattarci per esercitare il diritto di rettifica.

***Diritto alla cancellazione (diritto di essere dimenticato)***

Inoltre, l'interessato ha il diritto alla cancellazione e all'oblio ai sensi dell'art. 17 GDPR. Questo diritto può essere esercitato anche contattandoci. A questo punto, tuttavia, vorremmo sottolineare che questo diritto non si applica nella misura in cui il trattamento è necessario per adempiere a un obbligo legale a cui è soggetta la nostra società, articolo 17, paragrafo 3, lett. b GDPR. Ciò significa che possiamo approvare un'applicazione da cancellare solo dopo la scadenza del periodo di conservazione previsto dalla legge.

***Diritto alla restrizione dell'elaborazione***

Ai sensi dell'articolo 18 del GDPR, ogni interessato ha diritto a una restrizione del trattamento. La restrizione del trattamento può essere richiesta se una delle condizioni di cui all'articolo 18, paragrafo 1, lettere a-d GDPR è soddisfatto. L'interessato può contattarci per esercitare il diritto alla restrizione del trattamento.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

***Diritto di obiettare***

Inoltre, l'art. 21 GDPR garantisce il diritto di obiettare. L'interessato può contattarci per esercitare il diritto di obiettare.

***Diritto alla portabilità dei dati***

L'articolo 20 del GDPR conferisce all'interessato il diritto alla portabilità dei dati. Ai sensi di questa disposizione, la persona interessata ha le condizioni di cui all'articolo 20, paragrafo 1, lett. a e b GDPR il diritto di ricevere i dati personali che lo riguardano, che lui o lei ha fornito a un titolare del trattamento, in un formato strutturato, comunemente usato e leggibile da una macchina e ha il diritto di trasmettere tali dati a un altro titolare del trattamento senza impedimenti dal controllore a cui sono stati forniti i dati personali. L'interessato può contattarci per esercitare il diritto alla portabilità dei dati.

## J. L'esistenza del diritto di revocare il consenso in qualsiasi momento, senza pregiudizio della liceità del trattamento basato sul consenso prima del suo ritiro, qualora il trattamento si basi sull'articolo 6, paragrafo 1, lett. a o l'articolo 9, paragrafo 2, lett. a GDPR (articolo 14, paragrafo 2, lett. d GDPR)

Se il trattamento dei dati personali è basato sull'art. 6 (1) lett. a GDPR, che è il caso, se l'interessato ha acconsentito al trattamento dei dati personali per uno o più scopi specifici o è basato sull'articolo 9, paragrafo 2, lett. la GDPR, che regola il consenso esplicito al trattamento di categorie speciali di dati personali, l'interessato ha in base all'articolo 7 (3) Frase 1 GDPR il diritto di revocare il proprio consenso in qualsiasi momento.

Il ritiro del consenso non pregiudica la liceità del trattamento basato sul consenso prima del suo ritiro, articolo 7, paragrafo 3, frase 2 GDPR. Deve essere facile ritirare il consenso, art. 7 (3) Frase 4 GDPR. Pertanto, il ritiro del consenso può sempre avvenire nello stesso modo in cui è stato dato il consenso o in qualsiasi altro modo, che è considerato dall'interessato essere più semplice. Nella società dell'informazione di oggi, probabilmente il modo più semplice per ritirare il consenso è una semplice email. Se l'interessato desidera ritirare il suo consenso, ci è sufficiente una semplice email. In alternativa, l'interessato può scegliere qualsiasi altro modo per comunicare il suo ritiro del consenso a noi.

## K. Diritto di presentare un reclamo all'autorità di controllo (articolo 13, paragrafo 2, lett. d), 77, paragrafo 1 del GDPR)

Come titolare del trattamento, siamo obbligati a comunicare all'interessato il diritto di presentare un reclamo all'autorità di controllo, articolo 13, paragrafo 2, lett. d GDPR. Il diritto di presentare un reclamo presso un'autorità di controllo è regolato dall'articolo 77, paragrafo 1 del GDPR. In base a tale disposizione, fatto salvo ogni altro rimedio amministrativo o giudiziario, ogni interessato ha il diritto di presentare un reclamo all'autorità di controllo, in particolare nello Stato membro della sua residenza abituale, luogo di lavoro o luogo di la presunta violazione se l'interessato ritiene che il trattamento di dati


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

personali che lo riguardano violino il regolamento generale sulla protezione dei dati. Il diritto di presentare una denuncia presso un'autorità di controllo era limitato dal diritto dell'Unione solo in tal modo, che poteva essere esercitato solo dinanzi a un'unica autorità di vigilanza (Considerando 141, frase 1, del GDPR). Questa regola è intesa ad evitare i doppi reclami della stessa persona interessata nella stessa materia. Se una persona interessata desidera presentare un reclamo su di noi, abbiamo quindi chiesto di contattare solo una singola autorità di controllo.

## L. I dati personali provengono e, se del caso, provengono da fonti accessibili al pubblico (articolo 14, paragrafo 2, lett. g) del GDPR)

In linea di principio, i dati personali vengono raccolti direttamente dall'interessato o in collaborazione con un'autorità (ad esempio, il recupero di dati da un registro ufficiale). Altri dati sugli interessati sono derivati da trasferimenti di società del gruppo. Nel contesto di queste informazioni generali, la denominazione delle fonti esatte da cui provengono i dati personali è impossibile o comporterebbe uno sforzo sproporzionato ai sensi dell'Art. 14 (5) lett. b_ GDPR. In linea di principio, non raccogliamo dati personali da fonti accessibili pubblicamente.

Qualsiasi soggetto interessato può contattarci in qualsiasi momento per ottenere informazioni più dettagliate sulle esatte fonti dei dati personali che lo riguardano. Qualora l'origine dei dati personali non possa essere fornita all'interessato in quanto sono state utilizzate varie fonti, è opportuno fornire informazioni generali (considerando 61, frase 4, GDPR).

## M. Esistenza di processi decisionali automatizzati, inclusa la profilazione, di cui all'articolo 22, paragrafi 1 e 4, del GDPR e, almeno in tali casi, informazioni significative sulla logica in questione, nonché sulla significatività e le conseguenze previste di tale trattamento per l'interessato (articolo 14, paragrafo 2, lett. g) GDPR)

In quanto azienda responsabile, di solito non utilizziamo il processo decisionale automatizzato o la profilazione. Se, in casi eccezionali, effettuiamo un processo decisionale o di profilazione automatizzato, informeremo l'interessato separatamente o tramite una sottosezione della nostra informativa sulla privacy (sul nostro sito web). In tal caso, si applica quanto segue:

Il processo decisionale automatizzato - compresa la profilazione - può avvenire se (1) è necessario per la stipula o l'esecuzione di un contratto tra l'interessato e noi, oppure (2) è autorizzato dal diritto dell'Unione o degli Stati membri a cui siamo soggetti e che prevede anche misure idonee a salvaguardare i diritti e le libertà dell'interessato e i suoi legittimi interessi, oppure (3) si basa sul consenso esplicito dell'interessato.

Nei casi di cui all'articolo 22, paragrafo 2, lettere a) e c), del GDPR, attueremo misure adeguate per salvaguardare i diritti e le libertà dell'interessato e i suoi legittimi interessi. In questi casi, l'interessato ha


© All rights reserved by Heiko Maniero.

il diritto di ottenere l'intervento umano da parte del responsabile del trattamento, di esprimere il proprio punto di vista e di contestare la decisione.

Informazioni significative sulla logica, l'importanza e le conseguenze previste di tale trattamento per l'interessato sono contenute nella nostra politica sulla privacy.

## III. EU-U.S. Data Privacy Framework (EU-U.S. DPF), UK Extension to the EU-U.S. DPF, Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF)

Se la nostra organizzazione è un membro certificato dell'EU-U.S. Data Privacy Framework (EU-U.S. DPF) e/o della UK Extension to the EU-U.S. DPF e/o del Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF), si applica quanto segue:

Ci atteniamo all'EU-U.S. Data Privacy Framework (EU-U.S. DPF) e alla UK Extension to the EU-U.S. DPF, così come al Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF), come stabilito dal U.S. Department of Commerce. La nostra azienda ha confermato al Dipartimento del Commercio degli Stati Uniti che rispetta gli EU-U.S. Data Privacy Framework Principles (EU-U.S. DPF Principles) relativamente al trattamento dei dati personali che riceve dall'Unione Europea e dal Regno Unito in base all'EU-U.S. DPF e alla UK Extension to the EU-U.S. DPF. La nostra azienda ha anche confermato di rispettare i Swiss-U.S. Data Privacy Framework Principles (Swiss-U.S. DPF Principles) per quanto riguarda il trattamento dei dati personali ricevuti dalla Svizzera in base al Swiss-U.S. DPF. In caso di contraddizione tra le disposizioni della nostra politica sulla privacy e gli EU-U.S. DPF Principles e/o i Swiss-U.S. DPF Principles, i Principles prevarranno.

Per saperne di più sul programma Data Privacy Framework (DPF) e per visualizzare la nostra certificazione, si prega di visitare https://www.dataprivacyframework.gov/.

Le altre unità statunitensi o le filiali della nostra azienda che aderiscono anche agli EU-U.S. DPF Principals, inclusa la UK Extension to the EU-U.S. DPF e i Swiss-U.S. DPF Principals, se presenti, sono elencate nella nostra politica sulla privacy.

In conformità con l'EU-U.S. DPF, la UK Extension to the EU-U.S. DPF e il Swiss-U.S. DPF, la nostra azienda si impegna a collaborare con il comitato istituito dalle autorità europee per la protezione dei dati, l'Information Commissioner's Office (ICO) del Regno Unito e il Commissario federale per la protezione dei dati e la trasparenza (EDÖB) della Svizzera, e a seguire i loro consigli riguardo alle lamentele irrisolte sul nostro trattamento dei dati personali che riceviamo in base all'EU-U.S. DPF, alla UK Extension to the EU-U.S. DPF e al Swiss-U.S. DPF.


© All rights reserved by Heiko Maniero.

Informiamo le persone interessate riguardo alle autorità europee per la protezione dei dati competenti per gestire le lamentele sul trattamento dei dati personali da parte della nostra organizzazione, nella parte superiore di questo documento di trasparenza, e che offriamo un rimedio legale adeguato e gratuito.

Informiamo tutte le persone interessate che la nostra azienda è soggetta ai poteri di indagine e di enforcement della Federal Trade Commission (FTC).

Le persone interessate hanno la possibilità, in determinate condizioni, di richiedere un arbitrato vincolante. La nostra organizzazione è obbligata a risolvere le richieste e ad aderire alle condizioni dell'Allegato I dei DPF-Principals, a condizione che la persona interessata abbia richiesto un arbitrato vincolante notificando la nostra organizzazione e che le procedure e le condizioni dell'Allegato I dei Principals siano state rispettate.

Informiamo qui tutte le persone interessate sulla responsabilità della nostra organizzazione in caso di trasferimento di dati personali a terzi.

Per domande delle persone interessate o delle autorità di controllo della protezione dei dati, abbiamo nominato i rappresentanti locali menzionati nella parte superiore di questo documento di trasparenza.

Offriamo la possibilità di scegliere (Opt-out) se i dati personali (i) devono essere condivisi con terzi o (ii) utilizzati per scopi sostanzialmente diversi da quelli per i quali sono stati originariamente raccolti o successivamente autorizzati. Il meccanismo chiaro, ben visibile e facilmente accessibile per esercitare il proprio diritto di scelta consiste nel contattare il nostro Data Protection Officer (DSB) via email. Non si ha alcuna possibilità di scelta e non siamo obbligati quando i dati sono condivisi con un terzo che agisce come agente o processore per nostro conto e secondo le nostre istruzioni. Tuttavia, stipuliamo sempre un contratto con tale agente o processore.

Per i dati sensibili (ovvero dati personali che includono informazioni sulla salute, l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale o informazioni sulla vita sessuale della persona interessata), otteniamo il vostro consenso esplicito (Opt-in) se tali dati (i) devono essere condivisi o (ii) utilizzati per scopi diversi da quelli per cui sono stati originariamente raccolti o per cui avete successivamente dato il vostro consenso, facendo la vostra scelta di Opt-in. Inoltre, trattiamo tutti i dati personali che riceviamo da terzi come sensibili se il terzo li ha identificati e trattati come tali.

Vi informiamo qui sulla necessità di divulgare dati personali in risposta a richieste legali dalle autorità, inclusa l'esecuzione delle richieste di sicurezza nazionale o di applicazione della legge.

Nel trasferimento di dati personali a un terzo che agisce come responsabile, ci atteniamo ai Principals di notifica e scelta. Inoltre, stipuliamo un contratto con il terzo responsabile del trattamento che prevede che questi dati possano essere trattati solo per scopi limitati e specifici in conformità con il consenso fornito e che il destinatario offra lo stesso livello di protezione dei Principals del DPF e ci notifichi se determina di non poter più soddisfare questo obbligo. Il contratto prevede che il terzo, che agisce come


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

responsabile, interrompa il trattamento o adotti altre misure ragionevoli e appropriate per rimediare se tale determinazione viene fatta.

Nel trasferimento di dati personali a un terzo che agisce come agente o processore, (i) trasferiamo questi dati solo per scopi limitati e specifici; (ii) ci assicuriamo che l'agente o il processore sia obbligato a fornire almeno lo stesso livello di protezione dei dati richiesto dai DPF-Principals; (iii) adottiamo misure ragionevoli e appropriate per garantire che l'agente o il processore tratti effettivamente i dati personali trasferiti in modo conforme ai nostri obblighi ai sensi dei DPF-Principals; (iv) richiediamo che l'agente o il processore ci notifichi se determina di non poter più soddisfare il suo obbligo di fornire lo stesso livello di protezione richiesto dai DPF-Principals; (v) dopo tale notifica, anche sotto (iv), adottiamo misure ragionevoli e appropriate per interrompere il trattamento non autorizzato e rimediare; e (vi) forniamo al DPF Department, su richiesta, un riassunto o un esemplare rappresentativo delle disposizioni pertinenti sulla privacy del nostro contratto con tale agente.

In conformità con l'EU-U.S. DPF e/o la UK Extension to the EU-U.S. DPF e/o il Swiss-U.S. DPF, la nostra organizzazione si impegna a cooperare con il comitato istituito dalle autorità di protezione dei dati dell'UE e dall'Information Commissioner's Office (ICO) del Regno Unito e dal Commissario federale per la protezione dei dati e la trasparenza (EDÖB) della Svizzera, e a seguire i loro consigli riguardo le lamentele irrisolte sul nostro trattamento dei dati personali che riceviamo in relazione al lavoro sotto l'EU-U.S. DPF, la UK Extension to the EU-U.S. DPF e il Swiss-U.S. DPF.

Tutti gli interessati che si trovano temporaneamente nell'Unione Europea (UE), nello Spazio Economico Europeo (SEE) o nel Regno Unito, o che vi hanno il domicilio o la residenza abituale, hanno diritto ai diritti e alle prerogative degli interessati pubblicati nel nostro Documento sulla trasparenza, che derivano anche dagli articoli da 15 a 22 del GDPR, compreso il diritto di accesso ai dati personali. Abbiamo reso disponibili queste informazioni in tutte le lingue dell'UE e del SEE. La versione in lingua inglese si applica al Regno Unito.

Tutti gli interessati che risiedono temporaneamente in Svizzera o che vi hanno il domicilio o la residenza abituale hanno diritto ai diritti e alle prerogative degli interessati ai sensi della Legge svizzera sulla protezione dei dati (LPD) e del Regolamento svizzero sulla protezione dei dati (RGPD), pubblicati nel nostro Documento sulla trasparenza, compreso il diritto di accesso ai dati personali. Abbiamo fornito queste informazioni nelle tre lingue ufficiali della Svizzera (tedesco, italiano e francese).


© All rights reserved by Heiko Maniero.

# DUTCH: Informatie over de verwerking van persoonsgegevens (Artikel 13, 14 AVG)

Geachte heer, geachte mevrouw,

De persoonsgegevens van elke persoon die een contractuele, precontractuele of andere relatie met ons bedrijf heeft, verdienen speciale bescherming. Ons doel is ons gegevensbeschermingsniveau aan een hoge standaard te laten voldoen. Daarom zorgen wij voor een routinematig ontwikkeling van onze concepten voor gegevensbescherming en gegevensbeveiliging.

Uiteraard voldoen wij aan de wettelijke bepalingen inzake gegevensbescherming. Volgens de artikelen 13 en 14 van de AVG moeten bedrijven aan specifieke informatievereisten voldoen bij het verzamelen van persoonsgegevens. Dit document voldoet aan deze verplichtingen.

De terminologie van wettelijke regelgeving is gecompliceerd. Helaas kon het gebruik van wettelijke termen niet worden voorkomen bij de voorbereiding van dit document. Daarom willen we u er graag op wijzen dat u altijd contact kunt opnemen met onze functionaris voor gegevensbescherming voor alle vragen die u hebt over dit document en de gebruikte termen of formuleringen.

## I. Te verstrekken informatie wanneer persoonsgegevens bij de betrokkene worden verzameld (artikel 13 AVG)

### A. Identiteit en contactgegevens van de verwerkingsverantwoordelijke (artikel 13, lid 1, punt a AVG)

Zie bovenstaande

### B. Contactgegevens van de functionaris voor gegevensbescherming (artikel 13, lid 1, punt b AVG)

Zie bovenstaande

### C. De verwerkingsdoeleinden waarvoor de persoonsgegevens zijn bestemd, en de rechtsgrond voor de verwerking (artikel 13, lid 1, punt c AVG)

Het doel van het verwerken van persoonsgegevens is de uitvoer van alle activiteiten die verwerkingsverantwoordelijke, klanten, prospecten, zakelijke partners of andere contractuele of


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

precontractuele relaties tussen de genoemde groepen (in de breedste zin van het woord) betreffen of wettelijke verplichtingen van de verwerkingsverantwoordelijke.

Artikel 6, lid 1, punt a AVG dient als de wettelijke basis voor verwerkingsactiviteiten waarvoor wij toestemming vragen voor een specifiek verwerkingsdoel. Als de verwerking van persoonsgegevens nodig is voor het uitvoeren van een contract waarvan de betrokkene partij is, zoals het geval bijvoorbeeld bij verwerkingsactiviteiten die nodig zijn voor de levering van goederen of van enige andere dienst, is de verwerking gebaseerd op artikel 6, lid 1, punt b AVG. Hetzelfde is van toepassing bij verwerkingsactiviteiten die noodzakelijk zijn voor het uitvoeren van precontractuele maatregelen, bijvoorbeeld in het geval van vragen over onze producten of diensten. Als ons bedrijf onderworpen is aan een wettelijke verplichting die de verwerking van persoonsgegevens vereist, zoals voor het uitvoeren van belastingverplichtingen, is de verwerking gebaseerd op artikel 6, lid 1, punt c AVG.

In zeldzame gevallen kan de verwerking van persoonsgegevens nodig zijn om de vitale belangen van betrokkene of van een andere natuurlijke persoon te beschermen. Dit zou het geval zijn als bijvoorbeeld een bezoeker gewond zou raken in ons bedrijf en zijn naam, leeftijd, verzekeringsnummer of andere belangrijke informatie doorgegeven zouden moeten worden doorgegeven aan een arts, ziekenhuis of andere derde. De verwerking zou dan gebaseerd zijn op artikel 6, lid 1, punt d AVG.

Wanneer de verwerking noodzakelijk is voor de vervulling van een taak van algemeen belang of die deel uitmaakt van de uitoefening van het openbaar gezag die aan de verwerkingsverantwoordelijke is opgedragen, is de rechtsgrondslag artikel 6, lid 1, punt e AVG.

En verder kunnen verwerkingsactiviteiten gebaseerd zijn op artikel 6, lid 1, punt f AVG. Deze wettelijke basis wordt gebruikt voor verwerkingsactiviteiten die niet worden gedekt door enige bovengenoemde wettelijke reden, als de verwerking nodig is voor de gerechtvaardigde belangen die ons bedrijf of een derde nastreeft, behalve wanneer dergelijke belangen worden overschreven door de belangen van fundamentele rechten en vrijheden van de betrokkene die de bescherming van persoonsgegevens vereisen. Dergelijke verwerkingsactiviteiten zijn met name toegestaan omdat ze specifiek worden genoemd door de Europese wetgever. Deze overwoog dat een legitiem belang kon worden aangenomen indien betrokkene een klant van de verwerkingsverantwoordelijke is (Overweging 47 zin 2 AVG).

## D. De gerechtvaardigde belangen van de verwerkingsverantwoordelijke of van een derde, indien de verwerking op artikel 6, lid 1, punt f), is gebaseerd

Waar het verwerken van persoonsgegevens is gebaseerd op artikel 6, lid 1, punt f AVG is het legitiem belang om ons bedrijf uit te voeren in het belang van het welzijn van al onze medewerkers en aandeelhouders.

## E. Categorieën ontvangers van de persoonsgegevens (artikel 13, lid 1, punt e AVG)


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

Overheidsinstanties

Externe instanties

Andere externe instanties

Interne verwerking

Verwerking binnen een groep

Andere instanties

Een lijst van onze verwerkers en ontvangers van gegevens in derde landen en, indien van toepassing, internationale organisaties wordt gepubliceerd op onze website of kan kosteloos bij ons worden aangevraagd. Neem contact op met onze functionaris voor gegevensbescherming om deze lijst op te vragen.

## F. Ontvangers in een derde land en passende of geschikte waarborgen en de manieren waarop een kopie hiervan kan worden verkregen of waar ze beschikbaar zijn gemaakt (artikel 13, lid 1, punt e, 46, lid 1, 46, lid 2, punt c AVG)

Alle bedrijven en organisaties die onderdeel zijn van onze groep (hierna "groepsbedrijven") die hun bedrijfslocatie voeren of een kantoor hebben in een derde land kunnen behoren tot de ontvangers van persoonsgegevens.

Volgens artikel 46, lid 1 AVG kan een verwerkingsverantwoordelijke of verwerker persoonsgegevens uitsluitend naar een derde land doorgeven wanneer de verwerkingsverantwoordelijke of verwerker passende waarborgen heeft ingesteld en op voorwaarde dat betrokkenen over afdwingbare rechten en doeltreffende rechtsmiddelen beschikken. Passende waarborgen kunnen worden geleverd zonder dat hier een specifieke autorisatie van een toezichthoudende autoriteit door standaard contractclausules, artikel 46 lid 2, punt c AVG.

De standaard contractclausules van de Europese Unie worden overeengekomen met alle ontvangers uit derde landen vóór de eerste overdracht van persoonlijke gegevens. Bijgevolg is gewaarborgd dat passende garanties, afdwingbare rechten van betrokkenen en doeltreffende rechtsmiddelen voor betrokkenen die voortvloeien uit de standaard contractclausules van de EU worden gewaarborgd. Elke betrokkene kan een exemplaar van de standaard contractclausules verkrijgen van onze functionaris voor gegevensbescherming. De standaard contractclausules zijn ook beschikbaar in het Publicatieblad van de Europese Unie.

Artikel 45, lid 3, van de Algemene Verordening Gegevensbescherming (GDPR) geeft de Europese Commissie de bevoegdheid om door middel van een uitvoeringshandeling te besluiten dat een niet-EU-land een passend beschermingsniveau waarborgt. Dit betekent een beschermingsniveau voor


© All rights reserved by Heiko Maniero.

persoonsgegevens dat in wezen gelijkwaardig is aan het beschermingsniveau binnen de EU. Het gevolg van adequaatheidsbesluiten is dat persoonsgegevens zonder verdere belemmeringen vrij van de EU (en Noorwegen, Liechtenstein en IJsland) naar een derde land kunnen stromen. Soortgelijke regels bestaan voor het Verenigd Koninkrijk, Zwitserland en enkele andere landen.

Wanneer de Europese Commissie of de regering van een ander land heeft besloten dat een derde land een passend beschermingsniveau waarborgt en er een geldig kader van kracht is (bijv. EU-U.S. Data Privacy Framework, Swiss-U.S. Data Privacy Framework, UK Extension to the EU-U.S. Data Privacy Framework), zijn alle overdrachten door ons aan de leden van dergelijke kaders (bijv. zelfgecertificeerde entiteiten) uitsluitend gebaseerd op het lidmaatschap van die entiteiten van het respectieve kader. Wanneer wij of een van onze groepsentiteiten lid is van een dergelijk kader, zijn alle overdrachten aan ons of onze groepsentiteit uitsluitend gebaseerd op het lidmaatschap van de entiteit in het betreffende kader.

Elke betrokkene kan een kopie van de kaders bij ons opvragen. Daarnaast zijn de kaders ook beschikbaar in het Publicatieblad van de Europese Unie of in de gepubliceerde wettelijke materialen of op de websites van toezichthoudende autoriteiten of andere bevoegde autoriteiten of instellingen.

## G. Periode gedurende welke de persoonsgegevens worden opgeslagen, of indien dat niet nodig is de criteria die worden gebruikt om die periode te bepalen (artikel 13, lid 2, punt a AVG)

De criteria die worden gebruikt om de periode van opslag van persoonsgegevens te bepalen is de respectievelijke bewaarperiode. Na verloop van die periode worden de betreffende gegevens routinematig verwijderd, zo lang ze niet langer nodig zijn voor het voldoen aan het contract of het initiëren van een contract.

Als er geen wettelijke bewaartermijn is, is het criterium de contractuele of interne bewaartermijn.

## H. Het bestaan van het recht de verwerkingsverantwoordelijke te verzoeken om inzage van en rectificatie of wissing van de persoonsgegevens of beperking van de hem of haar betreffende verwerking, alsmede het recht tegen de verwerking bezwaar te maken en het recht op gegevensoverdraagbaarheid (artikel 13, lid 2, punt b AVG)

Alle betrokkenen hebben de volgende rechten:

***Recht op toegang***

Elke betrokkene heeft het recht tot toegang tot de hem betreffende persoonsgegevens. Het recht op toegang geldt voor alle gegevens die door ons worden verwerkt. Het recht kan gemakkelijk en met redelijke intervallen worden uitgeoefend om bewust te zijn van de rechtmatigheid van de werking en deze


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

te controleren (Overweging 63 AVG). Dit recht resulteert uit artikel 15 GDPR. De betrokkene mag contact opnemen met onze verwerkingsverantwoordelijke om het recht op toegang uit te oefenen.

***Recht op rectificatie***

Volgens artikel 16 zin 1 AVG heeft de betrokkene het recht zonder onnodige vertraging van de verwerkingsverantwoordelijke de rectificatie van incorrecte persoonsgegevens hemzelf betreffende te verkrijgen. Bovendien heeft, volgens artikel 16 zin 2 AVG, de betrokkene het recht, met inachtneming van de doelen van de verwerking, op vervolledigen van onvolledige persoonsgegevens, inclusief door een aanvullende verklaring te verstrekken. De betrokkene mag contact opnemen met onze functionaris voor gegevensverwerking om het recht op rectificatie uit te oefenen.

***Recht op wissing (recht op vergetelheid)***

Daarnaast hebben betrokkenen het recht op wissing en vergetelheid onder artikel 17 AVG. Dit recht kan ook worden uitgeoefend door contact op te nemen met de functionaris voor gegevensverwerking. Bij dit punt willen wij er echter op wijzen dat dit recht niet van toepassing is als de verwerking noodzakelijk is om te voldoen aan een wettelijke verplichting waar ons bedrijf zich aan moet houden, artikel 17, lid 3, punt b AVG. Dit betekent dat we een verzoek om wissing alleen kunnen goedkeuren na het vervallen van de wettelijke bewaartermijn.

***Recht op beperking van verwerking***

Volgens artikel 18 AVG heeft elke betrokkene het recht op beperking van de verwerking. De beperking van de verwerking kan worden gevraagd als wordt voldaan aan een van de voorwaarden in artikel 18, lid 1, punt a - d AVG. De betrokkene mag contact opnemen met onze functionaris voor gegevensverwerking om het recht op beperking van de verwerking uit te oefenen.

***Recht van bezwaar***

Verder garandeert artikel 21 AVG het recht van bezwaar. De betrokkene mag contact opnemen met onze functionaris voor gegevensverwerking om het recht van bezwaar uit te oefenen.

***Recht op overdraagbaarheid van gegevens***

Artikel 20 AVG garandeert de betrokkene het recht op overdraagbaarheid van gegevens. Onder deze voorziening heeft de betrokkene onder de voorwaarden die zijn vastgelegd in artikel 20, lid 1, punt a en b AVG het recht de hem betreffende persoonsgegevens, die hij aan een verwerkingsverantwoordelijke heeft verstrekt, in een gestructureerde, gangbare en machine leesbare vorm te verkrijgen, en hij heeft het recht die gegevens aan een andere verwerkingsverantwoordelijke over te dragen, zonder daarbij te worden gehinderd door de verwerkingsverantwoordelijke aan wie de persoonsgegevens waren verstrekt De betrokkene mag contact opnemen met onze functionaris voor gegevensverwerking om het recht op overdraagbaarheid van gegevens uit te oefenen.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

### I. Het bestaan van het recht om de toestemming te allen tijde in te trekken, zonder dat dit afbreuk doet aan de rechtmatigheid van de verwerking op basis van de toestemming vóór de intrekking daarvan, waar de verwerking is gebaseerd op artikel 6, lid 1, punt a of artikel 9, lid 2, punt a AVG (artikel 13, lid 2, punt c AVG)

Als het verwerken van persoonsgegevens is gebaseerd op artikel 6, lid 1, punt a AVG, wat het geval is, als de betrokkene heeft ingestemd met de verwerking van persoonsgegevens voor één of meerdere specifieke doelen of als het is gebaseerd op artikel 9, lid 2, punt a AVG, die de expliciete toestemming voor het verwerken van speciale categorieën persoonsgegevens, heeft de betrokkene volgens artikel 7, lid 3, zin 1 AVG het recht om zijn toestemming te allen tijde in te trekken.

Het intrekken van de toestemming laat de rechtmatigheid van de verwerking op basis van de toestemming vóór de intrekking daarvan, onverlet, artikel 7, lid 3, zin 2 AVG. Het intrekken van de toestemming is even eenvoudig als het geven ervan, artikel 7, lid 3, zin 4 AVG. Daarom kan het intrekken van toestemming altijd op dezelfde manier gebeuren als de toestemming is gegeven, of op enig andere manier die de betrokkene als eenvoudiger beschouwt. In de informatiemaatschappij van vandaag de dag is een eenvoudige e-mail de eenvoudigste manier om toestemming in te trekken. Als de betrokkene zijn aan ons verleende toestemming wil intrekken, is een eenvoudige e-mail naar onze functionaris voor gegevensverwerking voldoende. Het is de betrokkene vrij elke andere manier te kiezen om het intrekken van zijn toestemming aan ons te communiceren.

## J. Het recht om een klacht in te dienen bij een toezichthoudende autoriteit (artikel 13, lid 2, punt d, 77, lid 1 AVG)

Als verwerkingsverantwoordelijke zijn wij verplicht de betrokkene te informeren dat de betrokkene het recht heeft klacht in te dienen bij een toezichthoudende autoriteit, artikel 13, lid 2, punt d AVG. Het recht om een klacht in te dienen bij een toezichthoudende autoriteit is geregeld in artikel 77, lid 1 AVG. Onverminderd andere mogelijkheden van administratief of buitengerechtelijk beroep, heeft iedere natuurlijke persoon of rechtspersoon het recht om tegen een hem betreffend juridisch bindend besluit van een toezichthoudende autoriteit, met name in de lidstaat van zijn of haar woonplaats, werkplaats of plaats van de vermoede inbreuk, als de betrokkene vindt dat de verwerking van zijn persoonsgegevens inbreuk maakt op de Algemene verordening gegevensbescherming. Het recht een klacht in te dienen bij een toezichthoudende autoriteit was enkel als zodanig beperkt door de wet van de Unie, dat het uitsluitend kan worden uitgeoefend voor een enkele toezichthoudende autoriteit (Overweging 141, zin 1 AVG. Deze regel is bedoeld om dubbele klachten van dezelfde betrokkene op dezelfde manier te voorkomen. Als de betrokkene een klacht over ons wil indienen, hebben wij daarom gevraagd om contact op te nemen met slechts één toezichthoudende autoriteit.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## K. De verstrekking van persoonsgegevens als wettelijke of contractuele verplichting; Noodzakelijke voorwaarde om een overeenkomst te sluiten; Verplichting van de betrokkene de persoonsgegevens te verstrekken; Mogelijke gevolgen wanneer deze gegevens niet worden verstrekt (artikel 13, lid 2, punt e AVG)

Wij lichten toe dat de voorziening van persoonsgegevens deels voor de wet vereist is (bijvoorbeeld belastingregels) of ook het resultaat kan zijn van contractuele voorzieningen (bijvoorbeeld informatie over de contractpartner).

Soms kan het nodig zijn om een contract te sluiten waarvoor de betrokkene ons persoonsgegevens verstrekt, die vervolgens door ons verwerkt moeten worden. De betrokkene is, bijvoorbeeld, verplicht ons persoonsgegevens toe te sturen wanneer ons bedrijf een contract met hem of haar tekent. Het niet verstrekken van persoonsgegevens zou tot gevolg hebben dat het contract met de betrokkene niet getekend zou kunnen worden.

Voordat persoonsgegevens worden verstrekt door de betrokkene, moet de betrokkene contact opnemen met onze functionaris gegevensbescherming. Onze functionaris gegevensbescherming licht aan de betrokkene toe of het verstrekken van de persoonsgegevens wettelijk vereist is, of voor het tekenen van een contract nodig is, of er een verplichting bestaat de persoonsgegevens te verstrekken en wat de gevolgen zijn van het niet verstrekken van de persoonsgegevens.

## L. Het bestaan van geautomatiseerde besluitvorming, waaronder profilering, zoals opgenomen in artikel 22, lid 1 en 4 AVG en, in ieder geval in deze situaties, belangrijke informatie over de betrokken logica, evenals het belang en de beoogde gevolgen van dergelijke verwerking voor betrokkene (artikel 13, lid 2, punt f AVG)

Als verantwoordelijk bedrijf maken we gewoonlijk geen gebruik van geautomatiseerde besluitvorming of profilering. Als we in uitzonderlijke gevallen geautomatiseerde besluitvorming of profilering toepassen, informeren we de betrokkene hierover afzonderlijk of via een subrubriek in ons privacybeleid (op onze website). In dit geval is het volgende van toepassing:

Geautomatiseerde besluitvorming - met inbegrip van profilering - kan plaatsvinden indien (1) dit noodzakelijk is voor het aangaan of uitvoeren van een overeenkomst tussen de betrokkene en ons, of (2) dit is toegestaan door wetgeving van de Unie of de lidstaat waaraan wij zijn onderworpen en waarin ook passende maatregelen zijn vastgelegd om de rechten en vrijheden en legitieme belangen van de betrokkene te waarborgen; of (3) dit is gebaseerd op de uitdrukkelijke toestemming van de betrokkene.

In de gevallen waarnaar wordt verwezen in artikel 22, lid 2, onder a) en c) GDPR, zullen wij passende maatregelen treffen om de rechten en vrijheden en legitieme belangen van de betrokkene te waarborgen.


© All rights reserved by Heiko Maniero.

In deze gevallen heeft u het recht op menselijke tussenkomst van de verwerkingsverantwoordelijke, om uw standpunt kenbaar te maken en om de beslissing te betwisten.

Betekenisvolle informatie over de betrokken logica, evenals het belang en de beoogde gevolgen van een dergelijke verwerking voor de betrokkene wordt uiteengezet in ons privacybeleid.

## II. Voldoen aan de informatievereisten bij het niet verzamelen van persoonsgegevens van de betrokkene (artikel 14 AVG)

### A. Identiteit en contactgegevens van de verwerkingsverantwoordelijke (artikel 14, lid 1, punt a AVG)

Zie bovenstaande

### B. Contactgegevens van de functionaris voor gegevensbescherming (artikel 14, lid 1, punt b AVG)

Zie bovenstaande

### C. Verwerkingsdoeleinden waarvoor de persoonsgegevens zijn bestemd en de rechtsgrond voor de verwerking (artikel 14, lid 1, punt c AVG)

Het doel van het verwerken van persoonsgegevens is de uitvoer van alle activiteiten die verwerkingsverantwoordelijke, klanten, prospecten, zakelijke partners of andere contractuele of precontractuele relaties tussen de genoemde groepen (in de breedste zin van het woord) betreffen of wettelijke verplichtingen van de verwerkingsverantwoordelijke.

Als de verwerking van persoonsgegevens nodig is voor het uitvoeren van een contract waarvan de betrokkene partij is, zoals het geval bijvoorbeeld bij verwerkingsactiviteiten die nodig zijn voor de levering van goederen of van enige andere dienst, is de verwerking gebaseerd op artikel 6, lid 1, punt b AVG. Hetzelfde is van toepassing bij verwerkingsactiviteiten die noodzakelijk zijn voor het uitvoeren van pre-contractuele maatregelen, bijvoorbeeld in het geval van vragen over onze producten of diensten. Als ons bedrijf onderworpen is aan een wettelijke verplichting die de verwerking van persoonsgegevens vereist, zoals voor het uitvoeren van belastingverplichtingen, is de verwerking gebaseerd op artikel 6, lid 1, punt c AVG.

In zeldzame gevallen kan de verwerking van persoonsgegevens nodig zijn om de vitale belangen van betrokkene of van een andere natuurlijke persoon te beschermen. Dit zou het geval zijn als bijvoorbeeld een bezoeker gewond zou raken in ons bedrijf en zijn naam, leeftijd, verzekeringsnummer of andere


© All rights reserved by Heiko Maniero.

belangrijke informatie doorgegeven zouden moeten worden doorgegeven aan een arts, ziekenhuis of andere derde. De verwerking zou dan gebaseerd zijn op artikel 6, lid 1, punt d AVG.

Wanneer de verwerking noodzakelijk is voor de vervulling van een taak van algemeen belang of die deel uitmaakt van de uitoefening van het openbaar gezag die aan de verwerkingsverantwoordelijke is opgedragen, is de rechtsgrondslag artikel 6, lid 1, punt e AVG.

En verder kunnen verwerkingsactiviteiten gebaseerd zijn op artikel 6, lid 1, punt f AVG. Deze wettelijke basis wordt gebruikt voor verwerkingsactiviteiten die niet worden gedekt door enige bovengenoemde wettelijke reden, als de verwerking nodig is voor de gerechtvaardigde belangen die ons bedrijf of een derde nastreeft, behalve wanneer dergelijke belangen worden overschreven door de belangen van fundamentele rechten en vrijheden van de betrokkene die de bescherming van persoonsgegevens vereisen. Dergelijke verwerkingsactiviteiten zijn met name toegestaan omdat ze specifiek worden genoemd door de Europese wetgever. Deze overwoog dat een legitiem belang kon worden aangenomen indien betrokkene een klant van de verwerkingsverantwoordelijke is (Overweging 47 zin 2 AVG).

## D. Betrokken categorieën van persoonsgegevens (artikel 14(, lid 1, punt d AVG)

Klantgegevens

Gegevens van mogelijke klanten

Gegevens van medewerkers

Gegevens van leveranciers

## E. Categorieën ontvangers van de persoonsgegevens (artikel 14, lid 1, punt e AVG)

Overheidsinstanties

Externe instanties

Andere externe instanties

Interne verwerking

Verwerking binnen een groep

Andere instanties


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

Een lijst van onze verwerkers en ontvangers van gegevens in derde landen en, indien van toepassing, internationale organisaties wordt gepubliceerd op onze website of kan kosteloos bij ons worden aangevraagd. Neem contact op met onze functionaris voor gegevensbescherming om deze lijst op te vragen.

## F. Ontvangers in een derde land en passende of geschikte waarborgen en de manieren waarop een kopie hiervan kan worden verkregen of waar ze beschikbaar zijn gemaakt (artikel 14, lid 1, punt f, 46, lid 1, 46, lid 2, punt c AVG)

Alle bedrijven en organisaties die onderdeel zijn van onze groep (hierna "groepsbedrijven") die hun bedrijfslocatie voeren of een kantoor hebben in een derde land kunnen behoren tot de ontvangers van persoonsgegevens.

Volgens artikel 46, lid 1 AVG kan een verwerkingsverantwoordelijke of verwerker persoonsgegevens uitsluitend naar een derde land doorgeven wanneer de verwerkingsverantwoordelijke of verwerker passende waarborgen heeft ingesteld en op voorwaarde dat betrokkenen over afdwingbare rechten en doeltreffende rechtsmiddelen beschikken. Passende waarborgen kunnen worden geleverd zonder dat hier een specifieke autorisatie van een toezichthoudende autoriteit door standaard contractclausules, artikel 46 lid 2, punt c AVG.

De standaard contractclausules van de Europese Unie worden overeengekomen met alle ontvangers uit derde landen vóór de eerste overdracht van persoonlijke gegevens. Bijgevolg is gewaarborgd dat passende garanties, afdwingbare rechten van betrokkenen en doeltreffende rechtsmiddelen voor betrokkenen die voortvloeien uit de standaard contractclausules van de EU worden gewaarborgd. Elke betrokkene kan een exemplaar van de standaard contractclausules verkrijgen van onze functionaris voor gegevensbescherming. De standaard contractclausules zijn ook beschikbaar in het Publicatieblad van de Europese Unie.

Artikel 45, lid 3, van de Algemene Verordening Gegevensbescherming (GDPR) geeft de Europese Commissie de bevoegdheid om door middel van een uitvoeringshandeling te besluiten dat een niet-EU-land een passend beschermingsniveau waarborgt. Dit betekent een beschermingsniveau voor persoonsgegevens dat in wezen gelijkwaardig is aan het beschermingsniveau binnen de EU. Het gevolg van adequaatheidsbesluiten is dat persoonsgegevens zonder verdere belemmeringen vrij van de EU (en Noorwegen, Liechtenstein en IJsland) naar een derde land kunnen stromen. Soortgelijke regels bestaan voor het Verenigd Koninkrijk, Zwitserland en enkele andere landen.

Wanneer de Europese Commissie of de regering van een ander land heeft besloten dat een derde land een passend beschermingsniveau waarborgt en er een geldig kader van kracht is (bijv. EU-U.S. Data Privacy Framework, Swiss-U.S. Data Privacy Framework, UK Extension to the EU-U.S. Data Privacy Framework), zijn alle overdrachten door ons aan de leden van dergelijke kaders (bijv. zelfgecertificeerde entiteiten) uitsluitend gebaseerd op het lidmaatschap van die entiteiten van het respectieve kader.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

Wanneer wij of een van onze groepsentiteiten lid is van een dergelijk kader, zijn alle overdrachten aan ons of onze groepsentiteit uitsluitend gebaseerd op het lidmaatschap van de entiteit in het betreffende kader.

Elke betrokkene kan een kopie van de kaders bij ons opvragen. Daarnaast zijn de kaders ook beschikbaar in het Publicatieblad van de Europese Unie of in de gepubliceerde wettelijke materialen of op de websites van toezichthoudende autoriteiten of andere bevoegde autoriteiten of instellingen.

## G. Periode gedurende welke de persoonsgegevens worden opgeslagen, of indien dat niet mogelijk is, de criteria die worden gebruikt om die periode te bepalen (artikel 14, lid 2, punt a AVG)

De criteria die worden gebruikt om de periode van opslag van persoonsgegevens te bepalen is de respectievelijke bewaarperiode. Na verloop van die periode worden de betreffende gegevens routinematig verwijderd, zo lang ze niet langer nodig zijn voor het voldoen aan het contract of het initiëren van een contract.

Als er geen wettelijke bewaartermijn is, is het criterium de contractuele of interne bewaartermijn.

## H. Melding van de legitieme belangen nagestreefd door de verwerkingsverantwoordelijke of door een derde is gebaseerd op (artikel 6, lid 1, punt f AVG) (artikel 14, lid 2, punt b AVG)

Volgens artikel 6, lid 1, punt f AVG, is de verwerking alleen gewettigd als de verwerking nodig is voor de gerechtvaardigde belangen die de verwerkingsverantwoordelijke of een derde nastreeft, behalve wanneer dergelijke belangen worden overschreven door de belangen van fundamentele rechten en vrijheden van de betrokkene die de bescherming van persoonsgegevens vereisen. Volgens Overweging 47 zin 2 AVG kan een legitiem belang bestaan wanneer er een relevante en passende relatie bestaat tussen de betrokkene en de verwerkingsverantwoordelijke, bijvoorbeeld in situaties waar de betrokkene een klant is van de verwerkingsverantwoordelijke. Waar het verwerken van persoonsgegevens is gebaseerd op artikel 6, lid 1, punt f AVG is ons legitiem belang om ons bedrijf uit te voeren in het belang van het welzijn van al onze medewerkers en aandeelhouders.

## I. Het bestaan van het recht de verwerkingsverantwoordelijke te verzoeken om inzage van en rectificatie of wissing van de persoonsgegevens of beperking van de hem of haar betreffende verwerking, alsmede het recht tegen de verwerking bezwaar te maken en het recht op gegevensoverdraagbaarheid (artikel 13, lid 2, punt b AVG)

Alle betrokkenen hebben de volgende rechten:


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

***Recht op toegang***

Elke betrokkene heeft het recht tot toegang tot de hem betreffende persoonsgegevens. Het recht op toegang geldt voor alle gegevens die door ons worden verwerkt. Het recht kan gemakkelijk en met redelijke intervallen worden uitgeoefend om bewust te zijn van de rechtmatigheid van de werking en deze te controleren (Overweging 63 AVG). Dit recht resulteert uit artikel 15 GDPR. De betrokkene mag contact opnemen met onze verwerkingsverantwoordelijke om het recht op toegang uit te oefenen.

***Recht op rectificatie***

Volgens artikel 16 zin 1 AVG heeft de betrokkene het recht zonder onnodige vertraging van de verwerkingsverantwoordelijke de rectificatie van incorrecte persoonsgegevens hemzelf betreffende te verkrijgen. Bovendien heeft, volgens artikel 16 zin 2 AVG, de betrokkene het recht, met inachtneming van de doelen van de verwerking, op vervolledigen van onvolledige persoonsgegevens, inclusief door een aanvullende verklaring te verstrekken. De betrokkene mag contact opnemen met onze functionaris voor gegevensverwerking om het recht op rectificatie uit te oefenen.

***Recht op wissing (recht op vergetelheid)***

Daarnaast hebben betrokkenen het recht op wissing en vergetelheid onder artikel 17 AVG. Dit recht kan ook worden uitgeoefend door contact op te nemen met de functionaris voor gegevensverwerking. Bij dit punt willen wij er echter op wijzen dat dit recht niet van toepassing is als de verwerking noodzakelijk is om te voldoen aan een wettelijke verplichting waar ons bedrijf zich aan moet houden, artikel 17, lid 3, punt b AVG. Dit betekent dat we een verzoek om wissing alleen kunnen goedkeuren na het vervallen van de wettelijke bewaartermijn.

***Recht op beperking van verwerking***

Volgens artikel 18 AVG heeft elke betrokkene het recht op beperking van de verwerking. De beperking van de verwerking kan worden gevraagd als wordt voldaan aan een van de voorwaarden in artikel 18, lid 1, punt a - d AVG. De betrokkene mag contact opnemen met onze functionaris voor gegevensverwerking om het recht op beperking van de verwerking uit te oefenen.

***Recht van bezwaar***

Verder garandeert artikel 21 AVG het recht van bezwaar. De betrokkene mag contact opnemen met onze functionaris voor gegevensverwerking om het recht van bezwaar uit te oefenen.

***Recht op overdraagbaarheid van gegevens***

Artikel 20 AVG garandeert de betrokkene het recht op overdraagbaarheid van gegevens. Onder deze voorziening heeft de betrokkene onder de voorwaarden die zijn vastgelegd in artikel 20, lid 1, punt a en b AVG het recht de hem betreffende persoonsgegevens, die hij aan een verwerkingsverantwoordelijke heeft verstrekt, in een gestructureerde, gangbare en machine leesbare vorm te verkrijgen, en hij heeft het recht die gegevens aan een andere verwerkingsverantwoordelijke over te dragen, zonder daarbij te worden gehinderd door de verwerkingsverantwoordelijke aan wie de persoonsgegevens waren verstrekt De betrokkene mag contact opnemen met onze functionaris voor gegevensverwerking om het recht op overdraagbaarheid van gegevens uit te oefenen.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## J. Het bestaan van het recht om toestemming in te trekken op elk moment, zonder de wettigheid van de verwerking op basis van toestemming voordat deze werd ingetrokken, waar de verwerking is gebaseerd op artikel 6, lid 1, punt a of artikel 9, lid 2, punt a AVG (artikel 14, lid 2, punt d AVG)

Als het verwerken van persoonsgegevens is gebaseerd op artikel 6, lid 1, punt a AVG, wat het geval is, als de betrokkene heeft ingestemd met de verwerking van persoonsgegevens voor één of meerdere specifieke doelen of als het is gebaseerd op artikel 9, lid 2, punt a AVG, die de expliciete toestemming voor het verwerken van speciale categorieën persoonsgegevens, heeft de betrokkene volgens artikel 7, lid 3, zin 1 AVG het recht om zijn toestemming te allen tijde in te trekken.

Het intrekken van de toestemming laat de rechtmatigheid van de verwerking op basis van de toestemming vóór de intrekking daarvan, onverlet, artikel 7, lid 3, zin 2 AVG. Het intrekken van de toestemming is even eenvoudig als het geven ervan, artikel 7, lid 3, zin 4 AVG. Daarom kan het intrekken van toestemming altijd op dezelfde manier gebeuren als de toestemming is gegeven, of op enig andere manier die de betrokkene als eenvoudiger beschouwt. In de informatiemaatschappij van vandaag de dag is een eenvoudige e-mail de eenvoudigste manier om toestemming in te trekken. Als de betrokkene zijn aan ons verleende toestemming wil intrekken, is een eenvoudige e-mail naar onze functionaris voor gegevensverwerking voldoende. Het is de betrokkene vrij elke andere manier te kiezen om het intrekken van zijn toestemming aan ons te communiceren.

## K. Het recht om een klacht in te dienen bij een toezichthoudende autoriteit (artikel 14, lid 2, punt e, 77, lid 1 AVG)

Als verwerkingsverantwoordelijke zijn wij verplicht de betrokkene te informeren dat de betrokkene het recht heeft klacht in te dienen bij een toezichthoudende autoriteit, artikel 13, lid 2, punt d AVG. Het recht om een klacht in te dienen bij een toezichthoudende autoriteit is geregeld in artikel 77, lid 1 AVG. Onverminderd andere mogelijkheden van administratief of buitengerechtelijk beroep, heeft iedere natuurlijke persoon of rechtspersoon het recht om tegen een hem betreffend juridisch bindend besluit van een toezichthoudende autoriteit, met name in de lidstaat van zijn of haar woonplaats, werkplaats of plaats van de vermoede inbreuk, als de betrokkene vindt dat de verwerking van zijn persoonsgegevens inbreuk maakt op de Algemene verordening gegevensbescherming. Het recht een klacht in te dienen bij een toezichthoudende autoriteit was enkel als zodanig beperkt door de wet van de Unie, dat het uitsluitend kan worden uitgeoefend voor een enkele toezichthoudende autoriteit (Overweging 141, zin 1 AVG. Deze regel is bedoeld om dubbele klachten van dezelfde betrokkene op dezelfde manier te voorkomen. Als de betrokkene een klacht over ons wil indienen, hebben wij daarom gevraagd om contact op te nemen met slechts één toezichthoudende autoriteit.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## L. De bron waar de persoonsgegevens vandaan komen, en in voorkomend geval, of zij afkomstig zijn van openbare bronnen (artikel 14, lid 2, punt f AVG)

In principe worden de persoonsgegevens rechtstreeks verzameld van de betrokkene of in samenwerking met een autoriteit (bijvoorbeeld het opzoeken van gegevens in een officieel register). Andere gegevens over betrokkenen worden afgeleid van overschrijvingen van groepsbedrijven. In de context van deze algemene informatie, is het noemen van de exacte bronnen waarvan de persoonsgegevens afkomstig zijn ofwel onmogelijk of zou dit onevenredig veel inspanning vergen binnen de betekenis van artikel 14, lid 5, punt b AVG. In principe verzamelen wij geen persoonsgegevens van openbaar toegankelijke diensten.

Elke betrokkene kan te allen tijde contact opnemen met onze functionaris gegevensbescherming om meer gedetailleerde informatie te krijgen over de exacte bronnen van de persoonsgegevens die hem of haar betreffen. Waar de oorsprong van de persoonsgegevens niet kan worden verstrekt aan de betrokkene omdat verschillende bronnen gebruikt zijn, moet algemene informatie worden verstrekt (Overweging 61, zin 4 AVG).

## M. Het bestaan van geautomatiseerde besluitvorming, waaronder profilering, zoals opgenomen in artikel 22, lid 1 en 4 AVG en, in ieder geval in deze situaties, belangrijke informatie over de betrokken logica, evenals het belang en de beoogde gevolgen van dergelijke verwerking voor betrokkene (artikel 14, lid 2, punt g AVG)

Als verantwoordelijk bedrijf maken we gewoonlijk geen gebruik van geautomatiseerde besluitvorming of profilering. Als we in uitzonderlijke gevallen geautomatiseerde besluitvorming of profilering toepassen, informeren we de betrokkene hierover afzonderlijk of via een subrubriek in ons privacybeleid (op onze website). In dit geval is het volgende van toepassing:

Geautomatiseerde besluitvorming - met inbegrip van profilering - kan plaatsvinden indien (1) dit noodzakelijk is voor het aangaan of uitvoeren van een overeenkomst tussen de betrokkene en ons, of (2) dit is toegestaan door wetgeving van de Unie of de lidstaat waaraan wij zijn onderworpen en waarin ook passende maatregelen zijn vastgelegd om de rechten en vrijheden en legitieme belangen van de betrokkene te waarborgen; of (3) dit is gebaseerd op de uitdrukkelijke toestemming van de betrokkene.

In de gevallen waarnaar wordt verwezen in artikel 22, lid 2, onder a) en c) GDPR, zullen wij passende maatregelen treffen om de rechten en vrijheden en legitieme belangen van de betrokkene te waarborgen. In deze gevallen heeft u het recht op menselijke tussenkomst van de verwerkingsverantwoordelijke, om uw standpunt kenbaar te maken en om de beslissing te betwisten.

Betekenisvolle informatie over de betrokken logica, evenals het belang en de beoogde gevolgen van een dergelijke verwerking voor de betrokkene wordt uiteengezet in ons privacybeleid.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## III. EU-U.S. Data Privacy Framework (EU-U.S. DPF), UK Extension to the EU-U.S. DPF, Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF)

Als onze organisatie een gecertificeerd lid is van het EU-U.S. Data Privacy Framework (EU-U.S. DPF) en/of de UK Extension to the EU-U.S. DPF en/of het Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF), dan geldt het volgende:

Wij houden ons aan het EU-U.S. Data Privacy Framework (EU-U.S. DPF) en de UK Extension to the EU-U.S. DPF, evenals aan het Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF), zoals vastgesteld door het U.S. Department of Commerce. Ons bedrijf heeft tegenover het Amerikaanse Ministerie van Handel bevestigd dat het de EU-U.S. Data Privacy Framework Principles (EU-U.S. DPF Principles) naleeft met betrekking tot de verwerking van persoonsgegevens die het ontvangt uit de Europese Unie en het Verenigd Koninkrijk op basis van het EU-U.S. DPF en de UK Extension to the EU-U.S. DPF. Ons bedrijf heeft ook bevestigd aan het Amerikaanse Ministerie van Handel dat het de Swiss-U.S. Data Privacy Framework Principles (Swiss-U.S. DPF Principles) naleeft met betrekking tot de verwerking van persoonsgegevens die het uit Zwitserland ontvangt op basis van de Swiss-U.S. DPF. In het geval van een tegenstrijdigheid tussen de bepalingen van ons privacybeleid en de EU-U.S. DPF Principles en/of de Swiss-U.S. DPF Principles, zijn de Principles leidend.

Om meer te weten te komen over het Data Privacy Framework (DPF) programma en om onze certificering te bekijken, bezoek alstublieft https://www.dataprivacyframework.gov/.

Andere Amerikaanse entiteiten of dochterondernemingen van ons bedrijf die zich ook houden aan de EU-U.S. DPF Principals, inclusief de UK Extension to the EU-U.S. DPF en de Swiss-U.S. DPF Principals, indien aanwezig, worden genoemd in ons privacybeleid.

In overeenstemming met het EU-U.S. DPF, de UK Extension to the EU-U.S. DPF en het Swiss-U.S. DPF, verbindt ons bedrijf zich ertoe samen te werken met het panel opgericht door de EU-gegevensbeschermingsautoriteiten, het Britse Information Commissioner's Office (ICO) en de Zwitserse Federale Gegevensbeschermings- en Informatiecommissaris (EDÖB), en hun advies op te volgen met betrekking tot onopgeloste klachten over onze omgang met persoonsgegevens die we ontvangen op basis van het EU-U.S. DPF, de UK Extension to the EU-U.S. DPF en de Swiss-U.S. DPF.

We informeren de betrokken personen over de bevoegde Europese gegevensbeschermingsautoriteiten die verantwoordelijk zijn voor het behandelen van klachten over hoe onze organisatie met persoonsgegevens omgaat, bovenaan dit transparantiedocument, en dat we de betrokken personen een passend en gratis juridisch middel bieden.

We informeren alle betrokken personen dat ons bedrijf onderworpen is aan de onderzoeks- en handhavingsbevoegdheden van de Federal Trade Commission (FTC).


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

Betrokken personen hebben onder bepaalde voorwaarden de mogelijkheid om een bindende arbitrageprocedure aan te vragen. Onze organisatie is verplicht om claims te regelen en de voorwaarden volgens Bijlage I van de DPF-Principals na te leven, mits de betrokken persoon een bindende arbitrage heeft aangevraagd door onze organisatie hiervan op de hoogte te stellen en de procedures en voorwaarden volgens Bijlage I van de Principals zijn nageleefd.

Wij informeren hierbij alle betrokken personen over de aansprakelijkheid van onze organisatie in het geval van het doorgeven van persoonsgegevens aan derden.

Voor vragen van betrokken personen of de gegevensbeschermingsautoriteiten hebben wij de lokale vertegenwoordigers genoemd aan de bovenkant van dit transparantiedocument.

Wij bieden u de keuze (Opt-out) of uw persoonsgegevens (i) aan derden worden doorgegeven of (ii) worden gebruikt voor een doel dat wezenlijk verschilt van het doel/de doelen waarvoor ze oorspronkelijk zijn verzameld of later door u zijn goedgekeurd. Het duidelijke, goed zichtbare en gemakkelijk toegankelijke mechanisme om uw keuze uit te oefenen, is door contact op te nemen met onze Data Protection Officer (DSB) via e-mail. U heeft geen keuzemogelijkheid en wij zijn niet verplicht wanneer de gegevens aan een derde worden doorgegeven die als agent of verwerker namens ons en op onze instructie handelt. We sluiten echter altijd een contract af met zo'n agent of verwerker.

Voor gevoelige gegevens (dat wil zeggen persoonsgegevens die informatie bevatten over de gezondheidstoestand, de raciale of etnische afkomst, politieke meningen, religieuze of filosofische overtuigingen, vakbondslidmaatschap, of gegevens over het seksleven van de betrokkene) verkrijgen wij uw uitdrukkelijke toestemming (Opt-in) indien deze gegevens (i) worden doorgegeven aan derden of (ii) worden gebruikt voor een ander doel dan waarvoor ze oorspronkelijk zijn verzameld of waarvoor u later uw toestemming heeft gegeven door uw Opt-in keuze te maken. Bovendien behandelen we alle persoonsgegevens die we van derden ontvangen als gevoelig, als de derde partij deze als zodanig heeft geïdentificeerd en behandeld.

Wij informeren u hierbij over de noodzaak om persoonsgegevens bekend te maken in reactie op wettige verzoeken van autoriteiten, inclusief het voldoen aan eisen van nationale veiligheid of rechtshandhaving.

Bij het overdragen van persoonsgegevens aan een derde die als verantwoordelijke optreedt, houden we ons aan de Principals van kennisgeving en keuze. Bovendien sluiten we een contract af met de derde die verantwoordelijk is voor de verwerking, dat bepaalt dat deze gegevens alleen voor beperkte en gespecificeerde doeleinden mogen worden verwerkt in overeenstemming met de toestemming die u heeft verleend en dat de ontvanger hetzelfde beschermingsniveau biedt als de Principals van het DPF en ons informeert als hij vaststelt dat hij deze verplichting niet langer kan nakomen. Het contract bepaalt dat de derde die als verantwoordelijke optreedt, de verwerking staakt of andere redelijke en geschikte maatregelen neemt om een oplossing te bieden, indien een dergelijke vaststelling wordt gedaan.

Bij het overdragen van persoonsgegevens aan een derde die als agent of verwerker optreedt, (i) dragen we deze gegevens alleen over voor beperkte en gespecificeerde doeleinden; (ii) zorgen we ervoor dat


© All rights reserved by Heiko Maniero.

de agent of verwerker verplicht is om ten minste hetzelfde niveau van gegevensbescherming te bieden als vereist door de DPF-Principals; (iii) nemen we redelijke en geschikte maatregelen om ervoor te zorgen dat de agent of verwerker de overgedragen persoonsgegevens daadwerkelijk verwerkt op een manier die in overeenstemming is met onze verplichtingen volgens de DPF-Principals; (iv) vereisen we dat de agent of verwerker ons informeert als hij vaststelt dat hij niet langer in staat is om hetzelfde beschermingsniveau te bieden als vereist door de DPF-Principals; (v) ondernemen we na een dergelijke kennisgeving, ook onder (iv), redelijke en geschikte stappen om de ongeautoriseerde verwerking te stoppen en een oplossing te bieden; en (vi) verstrekken we het DPF Department op verzoek een samenvatting of een representatief voorbeeld van de relevante privacybepalingen van ons contract met die agent.

In overeenstemming met het EU-U.S. DPF en/of de UK Extension to the EU-U.S. DPF en/of de Swiss-U.S. DPF, verbindt onze organisatie zich ertoe samen te werken met het panel opgericht door de EU-gegevensbeschermingsautoriteiten en het Information Commissioner's Office (ICO) van het Verenigd Koninkrijk en de Zwitserse Federale Commissaris voor Gegevensbescherming en Openbaarheid (EDÖB), en hun adviezen op te volgen met betrekking tot onopgeloste klachten over onze omgang met persoonsgegevens die we ontvangen in verband met werk onder het EU-U.S. DPF, de UK Extension to the EU-U.S. DPF en het Swiss-U.S. DPF.

Alle betrokkenen die zich tijdelijk in de Europese Unie (EU), de Europese Economische Ruimte (EER) of het Verenigd Koninkrijk bevinden, of die daar hun domicilie of gewone verblijfplaats hebben, hebben recht op de rechten en rechten van de betrokkenen die zijn gepubliceerd in ons Transparantiedocument, die ook voortvloeien uit artikel 15 tot en met 22 GDPR, waaronder het recht op toegang tot persoonsgegevens. We hebben deze informatie beschikbaar gesteld in alle talen van de EU en de EER. De Engelstalige versie geldt voor het Verenigd Koninkrijk.

Alle betrokkenen die tijdelijk in Zwitserland wonen of daar hun domicilie of gewone verblijfplaats hebben, hebben recht op de rechten en de rechten van de betrokkenen volgens de Zwitserse Wet Bescherming Persoonsgegevens (DPA) en de Zwitserse Verordening Bescherming Persoonsgegevens (DPR) die zijn gepubliceerd in ons Transparantiedocument, inclusief het recht op toegang tot persoonsgegevens. We hebben deze informatie verstrekt in de drie officiële talen van Zwitserland (Duits, Italiaans en Frans).


© All rights reserved by Heiko Maniero.

# DUTCH: Informatie over de verwerking van persoonsgegevens voor werknemers en sollicitanten (artikel 13, 14 AVG)

Geachte heer, geachte mevrouw,

Persoonsgegevens van werknemers en sollicitanten verdienen speciale bescherming. Ons doel is om gegevensbescherming aan een hoge standaard te laten voldoen. Daarom scherpen wij onze visie op gegevensbescherming en gegevensbeveiliging routinematig aan.

Uiteraard voldoen wij aan de wettelijke bepalingen inzake gegevensbescherming. Volgens de artikelen 13 en 14 van de AVG moeten verwerkingsverantwoordelijken aan specifieke informatievereisten voldoen bij het verzamelen van persoonsgegevens. Dit document voldoet aan deze verplichtingen.

De terminologie van wettelijke regelgeving is ingewikkeld. Helaas kon het gebruik van wettelijke termen niet worden voorkomen bij de voorbereiding van dit document. Daarom willen we u er graag op wijzen dat u altijd contact kunt opnemen met ons voor alle vragen die u hebt over dit document en de gebruikte termen of formuleringen.

## I. Te verstrekken informatie wanneer persoonsgegevens bij de betrokkene worden verzameld (artikel 13 AVG)

### A. Identiteit en contactgegevens van de verwerkingsverantwoordelijke (artikel 13, lid 1, punt a AVG)

Zie bovenstaande

### B. Contactgegevens van de functionaris voor gegevensbescherming (artikel 13, lid 1, punt b AVG)

Zie bovenstaande

### C. De verwerkingsdoeleinden waarvoor de persoonsgegevens zijn bestemd, alsook de rechtsgrond voor de verwerking (artikel 13, lid 1, punt c AVG)

Voor de gegevens van de sollicitant is het doel van gegevensverwerking het onderzoeken van de sollicitatie tijdens het wervingsproces. Voor dit doel verwerken wij alle gegevens die door u zijn verstrekt.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

Op basis van de gegevens die tijdens het wervingsproces zijn verstrekt, gaan we na of we u al dan niet uitnodigen voor een sollicitatiegesprek (onderdeel van de selectieprocedure). In het geval van algemeen geschikte kandidaten, in het bijzonder in de context van het sollicitatiegesprek, verwerken wij bepaalde andere persoonsgegevens die door u zijn verstrekt, wat essentieel is voor de beslissing die wij voor de selectie nemen. Als u door ons wordt aangenomen, worden de gegevens die u als sollicitant opgaf automatisch omgezet in werknemersgegevens. Als onderdeel van het rekruteringsproces zullen wij andere persoonsgegevens vragen en die vervolgens verwerken. Deze gegevens zijn nodig om uw contract op te stellen of uit te voeren (zoals persoonlijk identificatienummer of belastingnummer). Voor werknemersgegevens is het doel van gegevensverwerking de uitvoering van de arbeidsovereenkomst of de naleving van andere wettelijke bepalingen die van toepassing zijn op de arbeidsrelatie (bijvoorbeeld belastingwetgeving). Uw persoonsgegevens zullen dus eveneens gebruikt worden voor het uitvoeren van de met u gesloten arbeidsovereenkomst (bijv. publicatie van uw naam en de contactinformatie binnen het bedrijf of aan klanten). Werknemer gegevens worden na beëindiging van de arbeidsrelatie opgeslagen om te voldoen aan wettelijke bewaartermijnen.

De rechtsgrondslag voor gegevensverwerking is artikel 6(1) punt b AVG, artikel 9(2) punt. b en h AVG, artikel 88 (1) AVG en nationale wetgeving, zoals voor Duitsland, artikel 26 BDSG (Federale Wet Bescherming Persoonsgegevens).

## D. Categorieën ontvangers van de persoonsgegevens (artikel 13, lid 1, punt e AVG)

Overheidsinstanties

Externe instanties

Andere externe instanties

Interne verwerking

Verwerking binnen een groep

Andere instanties

Een lijst van onze verwerkers en ontvangers van gegevens in derde landen en, indien van toepassing, internationale organisaties wordt gepubliceerd op onze website of kan kosteloos bij ons worden aangevraagd. Neem contact op met onze functionaris voor gegevensbescherming om deze lijst op te vragen.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## E. Ontvangers in een derde land en passende of geschikte waarborgen en de manieren waarop een kopie hiervan kan worden verkregen of waar ze beschikbaar zijn gemaakt (artikel 14, lid 1, punt f, 46, lid 1, 46, lid 2, punt c AVG)

Alle bedrijven en organisaties die onderdeel zijn van onze groep (hierna "groepsbedrijven") die hun bedrijfslocatie voeren of een kantoor hebben in een derde land kunnen behoren tot de ontvangers van persoonsgegevens.

Volgens artikel 46, lid 1 AVG kan een verwerkingsverantwoordelijke of verwerker persoonsgegevens uitsluitend naar een derde land doorgeven wanneer de verwerkingsverantwoordelijke of verwerker passende waarborgen heeft ingesteld en op voorwaarde dat betrokkenen over afdwingbare rechten en doeltreffende rechtsmiddelen beschikken. Passende waarborgen kunnen worden geleverd zonder dat hier een specifieke autorisatie van een toezichthoudende autoriteit door standaard contractclausules, artikel 46 lid 2, punt c AVG.

De standaard contractclausules van de Europese Unie worden overeengekomen met alle ontvangers uit derde landen vóór de eerste overdracht van persoonlijke gegevens. Bijgevolg is gewaarborgd dat passende garanties, afdwingbare rechten van betrokkenen en doeltreffende rechtsmiddelen voor betrokkenen die voortvloeien uit de standaard contractclausules van de EU worden gewaarborgd. Elke betrokkene kan een exemplaar van de standaard contractclausules verkrijgen van onze functionaris voor gegevensbescherming. De standaard contractclausules zijn ook beschikbaar in het Publicatieblad van de Europese Unie.

Artikel 45, lid 3, van de Algemene Verordening Gegevensbescherming (GDPR) geeft de Europese Commissie de bevoegdheid om door middel van een uitvoeringshandeling te besluiten dat een niet-EU-land een passend beschermingsniveau waarborgt. Dit betekent een beschermingsniveau voor persoonsgegevens dat in wezen gelijkwaardig is aan het beschermingsniveau binnen de EU. Het gevolg van adequaatheidsbesluiten is dat persoonsgegevens zonder verdere belemmeringen vrij van de EU (en Noorwegen, Liechtenstein en IJsland) naar een derde land kunnen stromen. Soortgelijke regels bestaan voor het Verenigd Koninkrijk, Zwitserland en enkele andere landen.

Wanneer de Europese Commissie of de regering van een ander land heeft besloten dat een derde land een passend beschermingsniveau waarborgt en er een geldig kader van kracht is (bijv. EU-U.S. Data Privacy Framework, Swiss-U.S. Data Privacy Framework, UK Extension to the EU-U.S. Data Privacy Framework), zijn alle overdrachten door ons aan de leden van dergelijke kaders (bijv. zelfgecertificeerde entiteiten) uitsluitend gebaseerd op het lidmaatschap van die entiteiten van het respectieve kader. Wanneer wij of een van onze groepsentiteiten lid is van een dergelijk kader, zijn alle overdrachten aan ons of onze groepsentiteit uitsluitend gebaseerd op het lidmaatschap van de entiteit in het betreffende kader.

Elke betrokkene kan een kopie van de kaders bij ons opvragen. Daarnaast zijn de kaders ook beschikbaar in het Publicatieblad van de Europese Unie of in de gepubliceerde wettelijke materialen of op de websites van toezichthoudende autoriteiten of andere bevoegde autoriteiten of instellingen.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## F. Periode gedurende welke de persoonsgegevens worden opgeslagen, of indien dat niet nodig, is de criteria die worden gebruikt om die periode te bepalen (artikel 13(2) sub a AVG)

De duur van de opslag van persoonsgegevens van sollicitanten is 6 maanden. Voor werknemersgegevens is de respectieve wettelijke bewaartermijn van toepassing. Na verloop van die periode worden de betreffende gegevens routinematig verwijderd, zo lang ze niet langer nodig zijn om aan de overeenkomst of aan de opstelling daarvan te voldoen.

## G. Het bestaan van het recht de verwerkingsverantwoordelijke te verzoeken om inzage van en rectificatie of wissing van de persoonsgegevens of beperking van de hem of haar betreffende verwerking, alsmede het recht tegen de verwerking bezwaar te maken en het recht op gegevensoverdraagbaarheid (artikel 13, lid 2, punt b AVG)

Alle betrokkenen hebben de volgende rechten:

***Recht op toegang***

Elke betrokkene heeft het recht tot toegang tot de hem betreffende persoonsgegevens. Het recht op toegang geldt voor alle gegevens die door ons worden verwerkt. Het recht kan gemakkelijk en met redelijke intervallen worden uitgeoefend om bewust te zijn van de rechtmatigheid van de werking en deze te controleren (Overweging 63 AVG). Dit recht resulteert uit artikel 15 GDPR. De betrokkene mag contact opnemen met onze verwerkingsverantwoordelijke om het recht op toegang uit te oefenen.

***Recht op rectificatie***

Volgens artikel 16 zin 1 AVG heeft de betrokkene het recht zonder onnodige vertraging van de verwerkingsverantwoordelijke de rectificatie van incorrecte persoonsgegevens hemzelf betreffende te verkrijgen. Bovendien heeft, volgens artikel 16 zin 2 AVG, de betrokkene het recht, met inachtneming van de doelen van de verwerking, op vervolledigen van onvolledige persoonsgegevens, inclusief door een aanvullende verklaring te verstrekken. De betrokkene mag contact opnemen met onze functionaris voor gegevensverwerking om het recht op rectificatie uit te oefenen.

***Recht op wissing (recht op vergetelheid)***

Daarnaast hebben betrokkenen het recht op wissing en vergetelheid onder artikel 17 AVG. Dit recht kan ook worden uitgeoefend door contact op te nemen met de functionaris voor gegevensverwerking. Bij dit punt willen wij er echter op wijzen dat dit recht niet van toepassing is als de verwerking noodzakelijk is om te voldoen aan een wettelijke verplichting waar ons bedrijf zich aan moet houden, artikel 17, lid 3, punt b AVG. Dit betekent dat we een verzoek om wissing alleen kunnen goedkeuren na het vervallen van de wettelijke bewaartermijn.


© All rights reserved by Heiko Maniero.

***Recht op beperking van verwerking***

Volgens artikel 18 AVG heeft elke betrokkene het recht op beperking van de verwerking. De beperking van de verwerking kan worden gevraagd als wordt voldaan aan een van de voorwaarden in artikel 18, lid 1, punt a - d AVG. De betrokkene mag contact opnemen met onze functionaris voor gegevensverwerking om het recht op beperking van de verwerking uit te oefenen.

***Recht van bezwaar***

Verder garandeert artikel 21 AVG het recht van bezwaar. De betrokkene mag contact opnemen met onze functionaris voor gegevensverwerking om het recht van bezwaar uit te oefenen.

***Recht op overdraagbaarheid van gegevens***

Artikel 20 AVG garandeert de betrokkene het recht op overdraagbaarheid van gegevens. Onder deze voorziening heeft de betrokkene onder de voorwaarden die zijn vastgelegd in artikel 20, lid 1, punt a en b AVG het recht de hem betreffende persoonsgegevens, die hij aan een verwerkingsverantwoordelijke heeft verstrekt, in een gestructureerde, gangbare en machine leesbare vorm te verkrijgen, en hij heeft het recht die gegevens aan een andere verwerkingsverantwoordelijke over te dragen, zonder daarbij te worden gehinderd door de verwerkingsverantwoordelijke aan wie de persoonsgegevens waren verstrekt De betrokkene mag contact opnemen met onze functionaris voor gegevensverwerking om het recht op overdraagbaarheid van gegevens uit te oefenen.

## H. Het bestaan van het recht om de toestemming te allen tijde in te trekken, zonder dat dit afbreuk doet aan de rechtmatigheid van de verwerking op basis van de toestemming vóór de intrekking daarvan, waar de verwerking is gebaseerd op artikel 6, lid 1, punt a of artikel 9, lid 2, punt a AVG (artikel 13, lid 2, punt c AVG)

Als het verwerken van persoonsgegevens is gebaseerd op artikel 6, lid 1, punt a AVG, wat het geval is, als de betrokkene heeft ingestemd met de verwerking van persoonsgegevens voor één of meerdere specifieke doelen of als het is gebaseerd op artikel 9, lid 2, punt a AVG, die de expliciete toestemming voor het verwerken van speciale categorieën persoonsgegevens, heeft de betrokkene volgens artikel 7, lid 3, zin 1 AVG het recht om zijn toestemming te allen tijde in te trekken.

Het intrekken van de toestemming laat de rechtmatigheid van de verwerking op basis van de toestemming vóór de intrekking daarvan, onverlet, artikel 7, lid 3, zin 2 AVG. Het intrekken van de toestemming is even eenvoudig als het geven ervan, artikel 7, lid 3, zin 4 AVG. Daarom kan het intrekken van toestemming altijd op dezelfde manier gebeuren als de toestemming is gegeven, of op enig andere manier die de betrokkene als eenvoudiger beschouwt. In de informatiemaatschappij van vandaag de dag is een eenvoudige e-mail de eenvoudigste manier om toestemming in te trekken. Als de betrokkene zijn aan ons verleende toestemming wil intrekken, is een eenvoudige e-mail naar onze functionaris voor gegevensverwerking voldoende. Het is de betrokkene vrij elke andere manier te kiezen om het intrekken van zijn toestemming aan ons te communiceren.


© All rights reserved by Heiko Maniero.

## I. Het recht om een klacht in te dienen bij een toezichthoudende autoriteit (artikel 13, lid 2, punt d, 77, lid 1 AVG)

Als verwerkingsverantwoordelijke zijn wij verplicht de betrokkene te informeren dat de betrokkene het recht heeft klacht in te dienen bij een toezichthoudende autoriteit, artikel 13, lid 2, punt d AVG. Het recht om een klacht in te dienen bij een toezichthoudende autoriteit is geregeld in artikel 77, lid 1 AVG. Onverminderd andere mogelijkheden van administratief of buitengerechtelijk beroep, heeft iedere natuurlijke persoon of rechtspersoon het recht om tegen een hem betreffend juridisch bindend besluit van een toezichthoudende autoriteit, met name in de lidstaat van zijn of haar woonplaats, werkplaats of plaats van de vermoede inbreuk, als de betrokkene vindt dat de verwerking van zijn persoonsgegevens inbreuk maakt op de Algemene verordening gegevensbescherming. Het recht een klacht in te dienen bij een toezichthoudende autoriteit was enkel als zodanig beperkt door de wet van de Unie, dat het uitsluitend kan worden uitgeoefend voor een enkele toezichthoudende autoriteit (Overweging 141, zin 1 AVG. Deze regel is bedoeld om dubbele klachten van dezelfde betrokkene op dezelfde manier te voorkomen. Als de betrokkene een klacht over ons wil indienen, hebben wij daarom gevraagd om contact op te nemen met slechts één toezichthoudende autoriteit.

## J. De verstrekking van persoonsgegevens als wettelijke of contractuele verplichting; Noodzakelijke voorwaarde om een overeenkomst te sluiten; Verplichting van de betrokkene de persoonsgegevens te verstrekken; Mogelijke gevolgen wanneer deze gegevens niet worden verstrekt (artikel 13, lid 2, punt e AVG)

Wij lichten toe dat de voorziening van persoonsgegevens deels voor de wet vereist is (bijvoorbeeld belastingregels) of ook het resultaat kan zijn van contractuele voorzieningen (bijvoorbeeld informatie over de contractpartner).

Soms kan het nodig zijn om een contract te sluiten waarvoor de betrokkene ons persoonsgegevens verstrekt, die vervolgens door ons verwerkt moeten worden. De betrokkene is, bijvoorbeeld, verplicht ons persoonsgegevens toe te sturen wanneer ons bedrijf een contract met hem of haar tekent. Het niet verstrekken van persoonsgegevens zou tot gevolg hebben dat het contract met de betrokkene niet getekend zou kunnen worden.

Voordat persoonsgegevens worden verstrekt door de betrokkene, moet de betrokkene contact opnemen met onze functionaris gegevensbescherming. Onze functionaris gegevensbescherming licht aan de betrokkene toe of het verstrekken van de persoonsgegevens wettelijk vereist is, of voor het tekenen van een contract nodig is, of er een verplichting bestaat de persoonsgegevens te verstrekken en wat de gevolgen zijn van het niet verstrekken van de persoonsgegevens.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

### K. Het bestaan van geautomatiseerde besluitvorming, waaronder profilering, zoals opgenomen in artikel 22, lid 1 en 4 AVG en, in ieder geval in deze situaties, belangrijke informatie over de betrokken logica, evenals het belang en de beoogde gevolgen van dergelijke verwerking voor betrokkene (artikel 13, lid 2, punt f AVG)

Als verantwoordelijk bedrijf maken we gewoonlijk geen gebruik van geautomatiseerde besluitvorming of profilering. Als we in uitzonderlijke gevallen geautomatiseerde besluitvorming of profilering toepassen, informeren we de betrokkene hierover afzonderlijk of via een subrubriek in ons privacybeleid (op onze website). In dit geval is het volgende van toepassing:

Geautomatiseerde besluitvorming - met inbegrip van profilering - kan plaatsvinden indien (1) dit noodzakelijk is voor het aangaan of uitvoeren van een overeenkomst tussen de betrokkene en ons, of (2) dit is toegestaan door wetgeving van de Unie of de lidstaat waaraan wij zijn onderworpen en waarin ook passende maatregelen zijn vastgelegd om de rechten en vrijheden en legitieme belangen van de betrokkene te waarborgen; of (3) dit is gebaseerd op de uitdrukkelijke toestemming van de betrokkene.

In de gevallen waarnaar wordt verwezen in artikel 22, lid 2, onder a) en c) GDPR, zullen wij passende maatregelen treffen om de rechten en vrijheden en legitieme belangen van de betrokkene te waarborgen. In deze gevallen heeft u het recht op menselijke tussenkomst van de verwerkingsverantwoordelijke, om uw standpunt kenbaar te maken en om de beslissing te betwisten.

Betekenisvolle informatie over de betrokken logica, evenals het belang en de beoogde gevolgen van een dergelijke verwerking voor de betrokkene wordt uiteengezet in ons privacybeleid.

## II. Voldoen aan de informatievereisten bij het niet verzamelen van persoonsgegevens van de betrokkene (artikel 14 AVG)

### A. Identiteit en contactgegevens van de verwerkingsverantwoordelijke (artikel 14, lid 1, punt a AVG)

Zie bovenstaande

### B. Contactgegevens van de functionaris voor gegevensbescherming (artikel 14, lid 1, punt b AVG)

Zie bovenstaande


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## C. Doelen van het verwerken waarvoor de persoonsgegevens zijn bedoeld en de wettelijke basis voor het verwerken (artikel 14, lid 1, punt c AVG)

Voor sollicitantgegevens die niet door de betrokkene zelf zijn verstrekt, is het doel van de gegevensverwerking het onderzoek van de sollicitatie tijdens het wervingsproces. Voor dit doel kunnen we gegevens verwerken die niet door uzelf verstrekt zijn. Op basis van de gegevens die tijdens het wervingsproces zijn verwerkt, gaan we na of we u al dan niet uitnodigen voor een sollicitatiegesprek (onderdeel van de selectieprocedure). Als u door ons wordt aangenomen, worden de gegevens die u als sollicitant opgaf automatisch omgezet in werknemersgegevens. Voor werknemersgegevens is het doel van gegevensverwerking de uitvoering van de arbeidsovereenkomst of de naleving van andere wettelijke bepalingen die van toepassing zijn op de arbeidsrelatie. Werknemer gegevens worden na beëindiging van de arbeidsrelatie opgeslagen om te voldoen aan wettelijke bewaartermijnen.

De rechtsgrondslag voor gegevensverwerking is artikel 6(1) punt b en f AVG, artikel 9(2) punt. b en h AVG, artikel 88 (1) AVG en nationale wetgeving, zoals voor Duitsland, artikel 26 BDSG (Federale Wet Bescherming Persoonsgegevens).

## D. Betrokken categorieën van persoonsgegevens (artikel 14(, lid 1, punt d AVG)

Sollicitantgegevens

Werknemer gegevens

## E. Categorieën ontvangers van de persoonsgegevens (artikel 14, lid 1, punt e AVG)

Overheidsinstanties

Externe instanties

Andere externe instanties

Interne verwerking

Verwerking binnen een groep

Andere instanties

Een lijst van onze verwerkers en ontvangers van gegevens in derde landen en, indien van toepassing, internationale organisaties wordt gepubliceerd op onze website of kan kosteloos bij ons worden


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

aangevraagd. Neem contact op met onze functionaris voor gegevensbescherming om deze lijst op te vragen.

## F. Ontvangers in een derde land en passende of geschikte waarborgen en de manieren waarop een kopie hiervan kan worden verkregen of waar ze beschikbaar zijn gemaakt (artikel 14, lid 1, punt f, 46, lid 1, 46, lid 2, punt c AVG)

Alle bedrijven en organisaties die onderdeel zijn van onze groep (hierna "groepsbedrijven") die hun bedrijfslocatie voeren of een kantoor hebben in een derde land kunnen behoren tot de ontvangers van persoonsgegevens.

Volgens artikel 46, lid 1 AVG kan een verwerkingsverantwoordelijke of verwerker persoonsgegevens uitsluitend naar een derde land doorgeven wanneer de verwerkingsverantwoordelijke of verwerker passende waarborgen heeft ingesteld en op voorwaarde dat betrokkenen over afdwingbare rechten en doeltreffende rechtsmiddelen beschikken. Passende waarborgen kunnen worden geleverd zonder dat hier een specifieke autorisatie van een toezichthoudende autoriteit door standaard contractclausules, artikel 46 lid 2, punt c AVG.

De standaard contractclausules van de Europese Unie worden overeengekomen met alle ontvangers uit derde landen vóór de eerste overdracht van persoonlijke gegevens. Bijgevolg is gewaarborgd dat passende garanties, afdwingbare rechten van betrokkenen en doeltreffende rechtsmiddelen voor betrokkenen die voortvloeien uit de standaard contractclausules van de EU worden gewaarborgd. Elke betrokkene kan een exemplaar van de standaard contractclausules verkrijgen van onze functionaris voor gegevensbescherming. De standaard contractclausules zijn ook beschikbaar in het Publicatieblad van de Europese Unie.

Artikel 45, lid 3, van de Algemene Verordening Gegevensbescherming (GDPR) geeft de Europese Commissie de bevoegdheid om door middel van een uitvoeringshandeling te besluiten dat een niet-EU-land een passend beschermingsniveau waarborgt. Dit betekent een beschermingsniveau voor persoonsgegevens dat in wezen gelijkwaardig is aan het beschermingsniveau binnen de EU. Het gevolg van adequaatheidsbesluiten is dat persoonsgegevens zonder verdere belemmeringen vrij van de EU (en Noorwegen, Liechtenstein en IJsland) naar een derde land kunnen stromen. Soortgelijke regels bestaan voor het Verenigd Koninkrijk, Zwitserland en enkele andere landen.

Wanneer de Europese Commissie of de regering van een ander land heeft besloten dat een derde land een passend beschermingsniveau waarborgt en er een geldig kader van kracht is (bijv. EU-U.S. Data Privacy Framework, Swiss-U.S. Data Privacy Framework, UK Extension to the EU-U.S. Data Privacy Framework), zijn alle overdrachten door ons aan de leden van dergelijke kaders (bijv. zelfgecertificeerde entiteiten) uitsluitend gebaseerd op het lidmaatschap van die entiteiten van het respectieve kader. Wanneer wij of een van onze groepsentiteiten lid is van een dergelijk kader, zijn alle overdrachten aan


© All rights reserved by Heiko Maniero.

ons of onze groepsentiteit uitsluitend gebaseerd op het lidmaatschap van de entiteit in het betreffende kader.

Elke betrokkene kan een kopie van de kaders bij ons opvragen. Daarnaast zijn de kaders ook beschikbaar in het Publicatieblad van de Europese Unie of in de gepubliceerde wettelijke materialen of op de websites van toezichthoudende autoriteiten of andere bevoegde autoriteiten of instellingen.

## G. Periode gedurende welke de persoonsgegevens worden opgeslagen, of indien dat niet mogelijk is, de criteria die worden gebruikt om die periode te bepalen (artikel 14(2), punt a AVG)

De duur van de opslag van persoonsgegevens van sollicitanten is 6 maanden. Voor werknemersgegevens is de respectieve wettelijke bewaartermijn van toepassing. Na verloop van die periode worden de betreffende gegevens routinematig verwijderd, zo lang ze niet langer nodig zijn om aan de overeenkomst of aan de opstelling daarvan te voldoen.

## H. Melding van de gerechtvaardigde belangen die door een verwerkingsverantwoordelijke of door een derde wordt behartigd, is gebaseerd op (artikel 6(1) sub f AVG) (artikel 14(2) sub b AVG)

Volgens artikel 6(1) sub f AVG, is de verwerking alleen rechtmatig indien voor de behartiging van de gerechtvaardigde belangen van de verwerkingsverantwoordelijke of van een derde, behalve wanneer de belangen of de grondrechten en de fundamentele vrijheden van de betrokkene die tot bescherming van persoonsgegevens nopen, zwaarder wegen dan die belangen. Volgens Overweging 47 zin 2 AVG kan een dergelijk gerechtvaardigd belang aanwezig zijn wanneer sprake is van een relevante en passende verhouding tussen de betrokkene en de verwerkingsverantwoordelijke, bijvoorbeeld in situaties waarin de betrokkene een klant is van de verwerkingsverantwoordelijke. In alle gevallen waarin ons bedrijf de gegevens van de sollicitant verwerkt op basis van artikel 6(1) punt f AVG, is ons gerechtvaardigd belang het tewerkstellen van geschikt personeel en professionals.

## I. Het bestaan van het recht de verwerkingsverantwoordelijke te verzoeken om inzage van en rectificatie of wissing van de persoonsgegevens of beperking van de hem of haar betreffende verwerking, alsmede het recht tegen de verwerking bezwaar te maken en het recht op gegevensoverdraagbaarheid (artikel 13, lid 2, punt b AVG)

Alle betrokkenen hebben de volgende rechten:


© All rights reserved by Heiko Maniero.

***Recht op toegang***

Elke betrokkene heeft het recht tot toegang tot de hem betreffende persoonsgegevens. Het recht op toegang geldt voor alle gegevens die door ons worden verwerkt. Het recht kan gemakkelijk en met redelijke intervallen worden uitgeoefend om bewust te zijn van de rechtmatigheid van de werking en deze te controleren (Overweging 63 AVG). Dit recht resulteert uit artikel 15 GDPR. De betrokkene mag contact opnemen met onze verwerkingsverantwoordelijke om het recht op toegang uit te oefenen.

***Recht op rectificatie***

Volgens artikel 16 zin 1 AVG heeft de betrokkene het recht zonder onnodige vertraging van de verwerkingsverantwoordelijke de rectificatie van incorrecte persoonsgegevens hemzelf betreffende te verkrijgen. Bovendien heeft, volgens artikel 16 zin 2 AVG, de betrokkene het recht, met inachtneming van de doelen van de verwerking, op vervolledigen van onvolledige persoonsgegevens, inclusief door een aanvullende verklaring te verstrekken. De betrokkene mag contact opnemen met onze functionaris voor gegevensverwerking om het recht op rectificatie uit te oefenen.

***Recht op wissing (recht op vergetelheid)***

Daarnaast hebben betrokkenen het recht op wissing en vergetelheid onder artikel 17 AVG. Dit recht kan ook worden uitgeoefend door contact op te nemen met de functionaris voor gegevensverwerking. Bij dit punt willen wij er echter op wijzen dat dit recht niet van toepassing is als de verwerking noodzakelijk is om te voldoen aan een wettelijke verplichting waar ons bedrijf zich aan moet houden, artikel 17, lid 3, punt b AVG. Dit betekent dat we een verzoek om wissing alleen kunnen goedkeuren na het vervallen van de wettelijke bewaartermijn.

***Recht op beperking van verwerking***

Volgens artikel 18 AVG heeft elke betrokkene het recht op beperking van de verwerking. De beperking van de verwerking kan worden gevraagd als wordt voldaan aan een van de voorwaarden in artikel 18, lid 1, punt a - d AVG. De betrokkene mag contact opnemen met onze functionaris voor gegevensverwerking om het recht op beperking van de verwerking uit te oefenen.

***Recht van bezwaar***

Verder garandeert artikel 21 AVG het recht van bezwaar. De betrokkene mag contact opnemen met onze functionaris voor gegevensverwerking om het recht van bezwaar uit te oefenen.

***Recht op overdraagbaarheid van gegevens***

Artikel 20 AVG garandeert de betrokkene het recht op overdraagbaarheid van gegevens. Onder deze voorziening heeft de betrokkene onder de voorwaarden die zijn vastgelegd in artikel 20, lid 1, punt a en b AVG het recht de hem betreffende persoonsgegevens, die hij aan een verwerkingsverantwoordelijke heeft verstrekt, in een gestructureerde, gangbare en machine leesbare vorm te verkrijgen, en hij heeft het recht die gegevens aan een andere verwerkingsverantwoordelijke over te dragen, zonder daarbij te worden gehinderd door de verwerkingsverantwoordelijke aan wie de persoonsgegevens waren verstrekt De betrokkene mag contact opnemen met onze functionaris voor gegevensverwerking om het recht op overdraagbaarheid van gegevens uit te oefenen.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## J. Het bestaan van het recht om toestemming in te trekken op elk moment, zonder de wettigheid van de verwerking op basis van toestemming voordat deze werd ingetrokken, waar de verwerking is gebaseerd op artikel 6, lid 1, punt a of artikel 9, lid 2, punt a AVG (artikel 14, lid 2, punt d AVG)

Als het verwerken van persoonsgegevens is gebaseerd op artikel 6, lid 1, punt a AVG, wat het geval is, als de betrokkene heeft ingestemd met de verwerking van persoonsgegevens voor één of meerdere specifieke doelen of als het is gebaseerd op artikel 9, lid 2, punt a AVG, die de expliciete toestemming voor het verwerken van speciale categorieën persoonsgegevens, heeft de betrokkene volgens artikel 7, lid 3, zin 1 AVG het recht om zijn toestemming te allen tijde in te trekken.

Het intrekken van de toestemming laat de rechtmatigheid van de verwerking op basis van de toestemming vóór de intrekking daarvan, onverlet, artikel 7, lid 3, zin 2 AVG. Het intrekken van de toestemming is even eenvoudig als het geven ervan, artikel 7, lid 3, zin 4 AVG. Daarom kan het intrekken van toestemming altijd op dezelfde manier gebeuren als de toestemming is gegeven, of op enig andere manier die de betrokkene als eenvoudiger beschouwt. In de informatiemaatschappij van vandaag de dag is een eenvoudige e-mail de eenvoudigste manier om toestemming in te trekken. Als de betrokkene zijn aan ons verleende toestemming wil intrekken, is een eenvoudige e-mail naar onze functionaris voor gegevensverwerking voldoende. Het is de betrokkene vrij elke andere manier te kiezen om het intrekken van zijn toestemming aan ons te communiceren.

## K. Het recht om een klacht in te dienen bij een toezichthoudende autoriteit (artikel 14, lid 2, punt e, 77, lid 1 AVG)

Als verwerkingsverantwoordelijke zijn wij verplicht de betrokkene te informeren dat de betrokkene het recht heeft klacht in te dienen bij een toezichthoudende autoriteit, artikel 13, lid 2, punt d AVG. Het recht om een klacht in te dienen bij een toezichthoudende autoriteit is geregeld in artikel 77, lid 1 AVG. Onverminderd andere mogelijkheden van administratief of buitengerechtelijk beroep, heeft iedere natuurlijke persoon of rechtspersoon het recht om tegen een hem betreffend juridisch bindend besluit van een toezichthoudende autoriteit, met name in de lidstaat van zijn of haar woonplaats, werkplaats of plaats van de vermoede inbreuk, als de betrokkene vindt dat de verwerking van zijn persoonsgegevens inbreuk maakt op de Algemene verordening gegevensbescherming. Het recht een klacht in te dienen bij een toezichthoudende autoriteit was enkel als zodanig beperkt door de wet van de Unie, dat het uitsluitend kan worden uitgeoefend voor een enkele toezichthoudende autoriteit (Overweging 141, zin 1 AVG. Deze regel is bedoeld om dubbele klachten van dezelfde betrokkene op dezelfde manier te voorkomen. Als de betrokkene een klacht over ons wil indienen, hebben wij daarom gevraagd om contact op te nemen met slechts één toezichthoudende autoriteit.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## L. De bron waar de persoonsgegevens vandaan komen, en in voorkomend geval, of zij afkomstig zijn van openbare bronnen (artikel 14, lid 2, punt f AVG)

In principe worden de persoonsgegevens rechtstreeks verzameld van de betrokkene of in samenwerking met een autoriteit (bijvoorbeeld het opzoeken van gegevens in een officieel register). Andere gegevens over betrokkenen worden afgeleid van overschrijvingen van groepsbedrijven. In de context van deze algemene informatie, is het noemen van de exacte bronnen waarvan de persoonsgegevens afkomstig zijn ofwel onmogelijk of zou dit onevenredig veel inspanning vergen binnen de betekenis van artikel 14, lid 5, punt b AVG. In principe verzamelen wij geen persoonsgegevens van openbaar toegankelijke diensten.

Elke betrokkene kan te allen tijde contact opnemen met onze functionaris gegevensbescherming om meer gedetailleerde informatie te krijgen over de exacte bronnen van de persoonsgegevens die hem of haar betreffen. Waar de oorsprong van de persoonsgegevens niet kan worden verstrekt aan de betrokkene omdat verschillende bronnen gebruikt zijn, moet algemene informatie worden verstrekt (Overweging 61, zin 4 AVG).

## M. Het bestaan van geautomatiseerde besluitvorming, waaronder profilering, zoals opgenomen in artikel 22, lid 1 en 4 AVG en, in ieder geval in deze situaties, belangrijke informatie over de betrokken logica, evenals het belang en de beoogde gevolgen van dergelijke verwerking voor betrokkene (artikel 14, lid 2, punt g AVG)

Als verantwoordelijk bedrijf maken we gewoonlijk geen gebruik van geautomatiseerde besluitvorming of profilering. Als we in uitzonderlijke gevallen geautomatiseerde besluitvorming of profilering toepassen, informeren we de betrokkene hierover afzonderlijk of via een subrubriek in ons privacybeleid (op onze website). In dit geval is het volgende van toepassing:

Geautomatiseerde besluitvorming - met inbegrip van profilering - kan plaatsvinden indien (1) dit noodzakelijk is voor het aangaan of uitvoeren van een overeenkomst tussen de betrokkene en ons, of (2) dit is toegestaan door wetgeving van de Unie of de lidstaat waaraan wij zijn onderworpen en waarin ook passende maatregelen zijn vastgelegd om de rechten en vrijheden en legitieme belangen van de betrokkene te waarborgen; of (3) dit is gebaseerd op de uitdrukkelijke toestemming van de betrokkene.

In de gevallen waarnaar wordt verwezen in artikel 22, lid 2, onder a) en c) GDPR, zullen wij passende maatregelen treffen om de rechten en vrijheden en legitieme belangen van de betrokkene te waarborgen. In deze gevallen heeft u het recht op menselijke tussenkomst van de verwerkingsverantwoordelijke, om uw standpunt kenbaar te maken en om de beslissing te betwisten.

Betekenisvolle informatie over de betrokken logica, evenals het belang en de beoogde gevolgen van een dergelijke verwerking voor de betrokkene wordt uiteengezet in ons privacybeleid.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## III. EU-U.S. Data Privacy Framework (EU-U.S. DPF), UK Extension to the EU-U.S. DPF, Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF)

Als onze organisatie een gecertificeerd lid is van het EU-U.S. Data Privacy Framework (EU-U.S. DPF) en/of de UK Extension to the EU-U.S. DPF en/of het Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF), dan geldt het volgende:

Wij houden ons aan het EU-U.S. Data Privacy Framework (EU-U.S. DPF) en de UK Extension to the EU-U.S. DPF, evenals aan het Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF), zoals vastgesteld door het U.S. Department of Commerce. Ons bedrijf heeft tegenover het Amerikaanse Ministerie van Handel bevestigd dat het de EU-U.S. Data Privacy Framework Principles (EU-U.S. DPF Principles) naleeft met betrekking tot de verwerking van persoonsgegevens die het ontvangt uit de Europese Unie en het Verenigd Koninkrijk op basis van het EU-U.S. DPF en de UK Extension to the EU-U.S. DPF. Ons bedrijf heeft ook bevestigd aan het Amerikaanse Ministerie van Handel dat het de Swiss-U.S. Data Privacy Framework Principles (Swiss-U.S. DPF Principles) naleeft met betrekking tot de verwerking van persoonsgegevens die het uit Zwitserland ontvangt op basis van de Swiss-U.S. DPF. In het geval van een tegenstrijdigheid tussen de bepalingen van ons privacybeleid en de EU-U.S. DPF Principles en/of de Swiss-U.S. DPF Principles, zijn de Principles leidend.

Om meer te weten te komen over het Data Privacy Framework (DPF) programma en om onze certificering te bekijken, bezoek alstublieft https://www.dataprivacyframework.gov/.

Andere Amerikaanse entiteiten of dochterondernemingen van ons bedrijf die zich ook houden aan de EU-U.S. DPF Principals, inclusief de UK Extension to the EU-U.S. DPF en de Swiss-U.S. DPF Principals, indien aanwezig, worden genoemd in ons privacybeleid.

In overeenstemming met het EU-U.S. DPF, de UK Extension to the EU-U.S. DPF en het Swiss-U.S. DPF, verbindt ons bedrijf zich ertoe samen te werken met het panel opgericht door de EU-gegevensbeschermingsautoriteiten, het Britse Information Commissioner's Office (ICO) en de Zwitserse Federale Gegevensbeschermings- en Informatiecommissaris (EDÖB), en hun advies op te volgen met betrekking tot onopgeloste klachten over onze omgang met persoonsgegevens die we ontvangen op basis van het EU-U.S. DPF, de UK Extension to the EU-U.S. DPF en de Swiss-U.S. DPF.

We informeren de betrokken personen over de bevoegde Europese gegevensbeschermingsautoriteiten die verantwoordelijk zijn voor het behandelen van klachten over hoe onze organisatie met persoonsgegevens omgaat, bovenaan dit transparantiedocument, en dat we de betrokken personen een passend en gratis juridisch middel bieden.

We informeren alle betrokken personen dat ons bedrijf onderworpen is aan de onderzoeks- en handhavingsbevoegdheden van de Federal Trade Commission (FTC).


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

Betrokken personen hebben onder bepaalde voorwaarden de mogelijkheid om een bindende arbitrageprocedure aan te vragen. Onze organisatie is verplicht om claims te regelen en de voorwaarden volgens Bijlage I van de DPF-Principals na te leven, mits de betrokken persoon een bindende arbitrage heeft aangevraagd door onze organisatie hiervan op de hoogte te stellen en de procedures en voorwaarden volgens Bijlage I van de Principals zijn nageleefd.

Wij informeren hierbij alle betrokken personen over de aansprakelijkheid van onze organisatie in het geval van het doorgeven van persoonsgegevens aan derden.

Voor vragen van betrokken personen of de gegevensbeschermingsautoriteiten hebben wij de lokale vertegenwoordigers genoemd aan de bovenkant van dit transparantiedocument.

Wij bieden u de keuze (Opt-out) of uw persoonsgegevens (i) aan derden worden doorgegeven of (ii) worden gebruikt voor een doel dat wezenlijk verschilt van het doel/de doelen waarvoor ze oorspronkelijk zijn verzameld of later door u zijn goedgekeurd. Het duidelijke, goed zichtbare en gemakkelijk toegankelijke mechanisme om uw keuze uit te oefenen, is door contact op te nemen met onze Data Protection Officer (DSB) via e-mail. U heeft geen keuzemogelijkheid en wij zijn niet verplicht wanneer de gegevens aan een derde worden doorgegeven die als agent of verwerker namens ons en op onze instructie handelt. We sluiten echter altijd een contract af met zo'n agent of verwerker.

Voor gevoelige gegevens (dat wil zeggen persoonsgegevens die informatie bevatten over de gezondheidstoestand, de raciale of etnische afkomst, politieke meningen, religieuze of filosofische overtuigingen, vakbondslidmaatschap, of gegevens over het seksleven van de betrokkene) verkrijgen wij uw uitdrukkelijke toestemming (Opt-in) indien deze gegevens (i) worden doorgegeven aan derden of (ii) worden gebruikt voor een ander doel dan waarvoor ze oorspronkelijk zijn verzameld of waarvoor u later uw toestemming heeft gegeven door uw Opt-in keuze te maken. Bovendien behandelen we alle persoonsgegevens die we van derden ontvangen als gevoelig, als de derde partij deze als zodanig heeft geïdentificeerd en behandeld.

Wij informeren u hierbij over de noodzaak om persoonsgegevens bekend te maken in reactie op wettige verzoeken van autoriteiten, inclusief het voldoen aan eisen van nationale veiligheid of rechtshandhaving.

Bij het overdragen van persoonsgegevens aan een derde die als verantwoordelijke optreedt, houden we ons aan de Principals van kennisgeving en keuze. Bovendien sluiten we een contract af met de derde die verantwoordelijk is voor de verwerking, dat bepaalt dat deze gegevens alleen voor beperkte en gespecificeerde doeleinden mogen worden verwerkt in overeenstemming met de toestemming die u heeft verleend en dat de ontvanger hetzelfde beschermingsniveau biedt als de Principals van het DPF en ons informeert als hij vaststelt dat hij deze verplichting niet langer kan nakomen. Het contract bepaalt dat de derde die als verantwoordelijke optreedt, de verwerking staakt of andere redelijke en geschikte maatregelen neemt om een oplossing te bieden, indien een dergelijke vaststelling wordt gedaan.

Bij het overdragen van persoonsgegevens aan een derde die als agent of verwerker optreedt, (i) dragen we deze gegevens alleen over voor beperkte en gespecificeerde doeleinden; (ii) zorgen we ervoor dat


© All rights reserved by Heiko Maniero.

de agent of verwerker verplicht is om ten minste hetzelfde niveau van gegevensbescherming te bieden als vereist door de DPF-Principals; (iii) nemen we redelijke en geschikte maatregelen om ervoor te zorgen dat de agent of verwerker de overgedragen persoonsgegevens daadwerkelijk verwerkt op een manier die in overeenstemming is met onze verplichtingen volgens de DPF-Principals; (iv) vereisen we dat de agent of verwerker ons informeert als hij vaststelt dat hij niet langer in staat is om hetzelfde beschermingsniveau te bieden als vereist door de DPF-Principals; (v) ondernemen we na een dergelijke kennisgeving, ook onder (iv), redelijke en geschikte stappen om de ongeautoriseerde verwerking te stoppen en een oplossing te bieden; en (vi) verstrekken we het DPF Department op verzoek een samenvatting of een representatief voorbeeld van de relevante privacybepalingen van ons contract met die agent.

In overeenstemming met het EU-U.S. DPF en/of de UK Extension to the EU-U.S. DPF en/of de Swiss-U.S. DPF, verbindt onze organisatie zich ertoe samen te werken met het panel opgericht door de EU-gegevensbeschermingsautoriteiten en het Information Commissioner's Office (ICO) van het Verenigd Koninkrijk en de Zwitserse Federale Commissaris voor Gegevensbescherming en Openbaarheid (EDÖB), en hun adviezen op te volgen met betrekking tot onopgeloste klachten over onze omgang met persoonsgegevens die we ontvangen in verband met werk onder het EU-U.S. DPF, de UK Extension to the EU-U.S. DPF en het Swiss-U.S. DPF.

Alle betrokkenen die zich tijdelijk in de Europese Unie (EU), de Europese Economische Ruimte (EER) of het Verenigd Koninkrijk bevinden, of die daar hun domicilie of gewone verblijfplaats hebben, hebben recht op de rechten en rechten van de betrokkenen die zijn gepubliceerd in ons Transparantiedocument, die ook voortvloeien uit artikel 15 tot en met 22 GDPR, waaronder het recht op toegang tot persoonsgegevens. We hebben deze informatie beschikbaar gesteld in alle talen van de EU en de EER. De Engelstalige versie geldt voor het Verenigd Koninkrijk.

Alle betrokkenen die tijdelijk in Zwitserland wonen of daar hun domicilie of gewone verblijfplaats hebben, hebben recht op de rechten en de rechten van de betrokkenen volgens de Zwitserse Wet Bescherming Persoonsgegevens (DPA) en de Zwitserse Verordening Bescherming Persoonsgegevens (DPR) die zijn gepubliceerd in ons Transparantiedocument, inclusief het recht op toegang tot persoonsgegevens. We hebben deze informatie verstrekt in de drie officiële talen van Zwitserland (Duits, Italiaans en Frans).


© All rights reserved by Heiko Maniero.

# GREEK: Πληροφορίες σχετικά με την επεξεργασία δεδομένων προσωπικού χαρακτήρα (Άρθρα 13, 14 ΓΚΠΔ)

Αγαπητέ κύριε, κυρία,

Τα δεδομένα προσωπικού χαρακτήρα κάθε ιδιώτη που είναι σε συμβατική, προσυμβατική ή άλλη σχέση με την εταιρεία μας χαίρει ειδικής προστασίας. Σκοπός μας είναι να διατηρήσουμε το υψηλό επίπεδο προστασίας δεδομένων μας. Για το σκοπό αυτό, αναπτύσσουμε συστηματικά τους μηχανισμούς προστασίας και ασφάλειας δεδομένων.

Ασφαλώς τηρούμε τις νόμιμες διατάξεις προστασίας δεδομένων. Σύμφωνα με τα άρθρα 13 και 14 ΓΚΠΔ, οι υπεύθυνοι επεξεργασίας θα πρέπει να πληρούν ειδικές προϋποθέσεις κατά τη συλλογή δεδομένων προσωπικού χαρακτήρα. Το έγγραφο αυτό πληρεί αυτές τις προϋποθέσεις.

Η ορολογία των νομικών ρυθμίσεων είναι περίπλοκη. Δυστυχώς, η χρήση νομικών εννοιών δεν μπορούσε να αποφευχθεί κατά τη σύνταξη του παρόντος εγγράφου. Για το λόγο αυτό, θα θέλαμε να τονίσουμε ότι μπορείτε ανά πάσα στιγμή να επικοινωνήσετε μαζί μας για κάθε ερώτηση σχετικά με το παρόν έγγραφο, τους χρησιμοποιούμενους όρους και τη διατύπωση.

## I. Πληροφορίες που παρέχονται εάν τα δεδομένα προσωπικού χαρακτήρα συλλέγονται από το υποκείμενο των δεδομένων (Άρθρο 13 ΓΚΠΔ)

### A. Ταυτότητα και στοιχεία επικοινωνίας του υπεύθυνου επεξεργασίας (αρ. 13 παρ. 1 περ. α΄ ΓΚΠΔ)

Βλέπε ανωτέρω

### B. Στοιχεία επικοινωνίας του Υπεύθυνου Προστασίας Δεδομένων(αρ. 13 παρ. 1 περ. β’ ΓΚΠΔ)

Βλέπε ανωτέρω


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## C. Σκοπός της επιχειρούμενης επεξεργασίας δεδομένων προσωπικού χαρακτήρα και νόμιμη βάση επεξεργασίας (αρ. 13 (1) περ. γ' ΓΚΠΔ)

Σκοπός επεξεργασίας των δεδομένων προσωπικού χαρακτήρα είναι η διαχείριση όλων των εργασιών που αφορούν τον υπεύθυνο επεξεργασίας, τους πελάτες, τους πιθανούς πελάτες, εμπορικούς συνεργάτες ή άλλες συμβατικές ή μη συμβατικές σχέσεις μεταξύ των αναφερόμενων μερών (εν ευρεία έννοια) ή άλλη νόμιμη υποχρέωση του υπεύθυνου επεξεργασίας.

Το αρ. 6 παρ. 1 περ. α' ΓΚΠΔ λειτουργεί ως η νόμιμη βάση για τις εργασίες επεξεργασίας για τις οποίες λαμβάνουμε τη συναίνεση επεξεργασίας. Σε περίπτωση που η επεξεργασία των δεδομένων προσωπικού χαρακτήρα είναι απαραίτητη για την εκτέλεση σύμβασης στην οποία συμβαλλόμενο μέρος είναι το υποκείμενο των δεδομένων, όπως, για παράδειγμα, όταν η επεξεργασία είναι απαραίτητη για την παροχή προϊόντων ή υπηρεσιών, η επεξεργασία βασίζεται στο άρθρο 6 παρ. 1 περ. β' ΓΚΠΔ. Το ίδιο ισχύει για την επεξεργασία που είναι απαραίτητη για τη λήψη μέτρων πριν τη σύναψη σύμβασης, όπως για παράδειγμα στην περίπτωση παροχής πληροφοριών που αφορούν τα προϊόντα ή τις υπηρεσίες μας. Στην περίπτωση που η εταιρεία μας υπέχει νόμιμη υποχρέωση επεξεργασίας δεδομένων προσωπικού χαρακτήρα, όπως για την εκπλήρωση φορολογικών υποχρεώσεων, η επεξεργασία βασίζεται στο αρ. 6 παρ. 1 περ. γ' ΓΚΠΔ.

Σε σπάνιες περιπτώσεις, η επεξεργασίας δεδομένων προσωπικού χαρακτήρα μπορεί να είναι απαραίτητη για τη διαφύλαξη ζωτικού συμφέροντος του υποκειμένου των δεδομένων ή άλλου φυσικού προσώπου. Τέτοια είναι η περίπτωση, για παράδειγμα, όταν επισκέπτης τραυματίζεται στην εταιρεία μας και το όνομα, η ηλικία του, δεδομένα ασφάλειας υγείας ή άλλα ζωτικές πληροφορίες διαβιβάζονται σε ιατρό, νοσοκομείο ή τρίτο πρόσωπο. Τότε η επεξεργασία βασίζεται στο αρ. 6 παρ. 1 περ. δ' ΓΚΠΔ.

Όταν η επεξεργασία είναι απαραίτητη για την εκτέλεση καθήκοντος που εκτελείται προς το δημόσιο συμφέρον ή κατά την άσκηση δημόσιας εξουσίας που έχει ανατεθεί στον υπεύθυνο επεξεργασίας, η νομική βάση είναι το αρ. 6 παρ. 1 περ. e ΓΚΠΔ.

Τέλος, οι εργασίες επεξεργασίας μπορούν να έχουν τη βάση τους στο αρ. 6 παρ. 1 ΓΚΠΔ. Λειτουργεί ως νόμιμη βάση για τις εργασίες επεξεργασίας που δεν καλύπτονται από τις προαναφερθείσες βάσεις, εφόσον η επεξεργασία είναι απαραίτητη για το σκοπό της εξυπηρέτησης των εννόμων συμφερόντων της εταιρείας μας ή τρίτου μέρους, υπό τον όρο ότι δεν υπερισχύουν των συμφερόντων ή των θεμελιωδών δικαιωμάτων και ελευθεριών του υποκειμένου του οποίου τα δεδομένα προσωπικού χαρακτήρα υπόκεινται σε προστασία. Τέτοιες εργασίες επεξεργασίας επιτρέπονται ιδίως στις περιπτώσεις που αναφέρονται από τον ευρωπαίο νομοθέτη. Σύμφωνα με αυτόν, τέτοιο έννομο συμφέρον θα μπορούσε να υπάρχει όταν το υποκείμενο των δεδομένων είναι πελάτης του υπεύθυνου επεξεργασίας (Προοίμιο παρ. 47 εδ. β' ΓΚΠΔ).


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## D. Ενημέρωση σχετικά με τα έννομα συμφέροντα που επιδιώκονται από τον υπεύθυνο επεξεργασίας ή από τρίτο, σε περίπτωση που η επεξεργασία βασίζεται στο αρ.6 παρ.1 περ. στ' ΓΚΠΔ

Όταν η επεξεργασία δεδομένων προσωπικού χαρακτήρα βασίζεται στο άρθρο 6 παράγραφος 1 στοιχείο στ) του ΓΚΠΔ, το έννομο συμφέρον μας είναι να διεξάγουμε την επιχείρησή μας προς όφελος της ευημερίας όλων των εργαζομένων μας και των μετόχων.

## E. Κατηγορίες αποδεκτών δεδομένων προσωπικού χαρακτήρα (αρ. 13 παρ. 1 περ. ε' ΓΚΠΔ)

Δημόσιες αρχές

Εξωτερικά όργανα

Εσωτερική επεξεργασία

Ενδοομιλική επεξεργασία

Άλλα όργανα κι οργανισμοί

Κατάλογος των εκτελούντων την επεξεργασία και των αποδεκτών των δεδομένων μας σε τρίτες χώρες και, κατά περίπτωση, διεθνών οργανισμών δημοσιεύεται στον ιστότοπό μας ή μπορεί να ζητηθεί από εμάς δωρεάν. Παρακαλούμε επικοινωνήστε με τον υπεύθυνο προστασίας δεδομένων μας για να ζητήσετε αυτόν τον κατάλογο.

## F. Αποδέκτες σε τρίτες χώρες και κατάλληλα μέτρα προστασίας και μέσα για τη λήψη αντιγράφων των δεδομένων ή των αποδεκτών τους (αρ. 13 παρ. 1 περ. στ', 46 παρ. 1, 46 παρ. 2 περ. γ' ΓΚΔΠ)

Όλες οι εταιρείες και τα υποκαταστήματα που είναι μέρος του ομίλου μας (στο εξής αναφερόμενες ως «όμιλος εταιρειών») και έχουν τη δική τους έδρα ή γραφείο σε τρίτη χώρα μπορεί να αποτελούν αποδέκτες δεδομένων προσωπικού χαρακτήρα. Μπορείτε να ζητήσετε λίστα των εταιρειών του ομίλου ή των αποδεκτών από εμάς.

Σύμφωνα με το αρ. 46 παρ. 1 ΓΚΠΔ, ο υπεύθυνος επεξεργασίας ή εκτελών την επεξεργασία μπορεί να διαβιβάζει δεδομένων προσωπικού χαρακτήρα σε τρίτη χώρα μόνο εάν ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία παρέχει κατάλληλες εγγυήσεις και υπό την προϋπόθεση ότι υφίστανται εκτελεστά δικαιώματα και αποτελεσματικά ένδικα μέσα διαθέσιμα για το υποκείμενο των δεδομένων. Οι κατάλληλες εγγυήσεις μπορούν να προβλέπονται χωρίς να απαιτείται ειδική άδεια εποπτικής αρχής μέσω τυποποιημένων συμβατικών ρητρών (αρ. 46 παρ. 2 περ. γ' ΓΚΠΔ).


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

Οι τυποποιημένες συμβατικές ρήτρες της Ευρωπαϊκής Ένωσης ή άλλες κατάλληλες εγγυήσεις συμφωνούνται με κάθε αποδέκτη σε τρίτη χώρα πριν την πρώτη διαβίβαση δεδομένων προσωπικού χαρακτήρα. Συνεπώς, διασφαλίζονται κατάλληλες εγγυήσεις, αλλά και εκτελεστά δικαιώματα και αποτελεσματικά ένδικα μέσα για τα υποκείμενα των δεδομένων. Κάθε υποκείμενο των δεδομένων μπορεί να παραλαμβάνει αντίγραφο των τυποποιημένων συμβατικών ρητρών από εμάς. Οι τυποποιημένες συμβατικές ρήτρες είναι επίσης διαθέσιμες στην Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης.

Το άρθρο 45 παράγραφος 3 του Γενικού Κανονισμού για την Προστασία Δεδομένων (ΓΚΠΔ) παρέχει στην Ευρωπαϊκή Επιτροπή την εξουσία να αποφασίζει, μέσω εκτελεστικής πράξης, ότι μια χώρα εκτός ΕΕ εξασφαλίζει επαρκές επίπεδο προστασίας. Αυτό σημαίνει επίπεδο προστασίας των δεδομένων προσωπικού χαρακτήρα που είναι ουσιαστικά ισοδύναμο με το επίπεδο προστασίας εντός της ΕΕ. Οι αποφάσεις περί επάρκειας έχουν ως αποτέλεσμα τα δεδομένα προσωπικού χαρακτήρα να μπορούν να διακινούνται ελεύθερα από την ΕΕ (και τη Νορβηγία, το Λιχτενστάιν και την Ισλανδία) προς μια τρίτη χώρα χωρίς περαιτέρω εμπόδια. Παρόμοιοι κανόνες υπάρχουν για το Ηνωμένο Βασίλειο, την Ελβετία και ορισμένες άλλες χώρες.

Σε περίπτωση που η Ευρωπαϊκή Επιτροπή ή η κυβέρνηση άλλης χώρας αποφασίσει ότι μια τρίτη χώρα εξασφαλίζει επαρκές επίπεδο προστασίας και υπάρχει έγκυρο πλαίσιο (π.χ. EU-U.S. Data Privacy Framework, Swiss-U.S. Data Privacy Framework, UK Extension to the EU-U.S. Data Privacy Framework), όλες οι διαβιβάσεις από εμάς προς τα μέλη αυτών των πλαισίων (π.χ. αυτοπιστοποιημένες οντότητες) βασίζονται αποκλειστικά στη συμμετοχή της εν λόγω οντότητας στο αντίστοιχο πλαίσιο. Όταν εμείς ή μία από τις οντότητες του ομίλου μας είναι μέλος τέτοιου πλαισίου, όλες οι διαβιβάσεις προς εμάς ή την οντότητα του ομίλου μας βασίζονται αποκλειστικά στη συμμετοχή της οντότητας στο εν λόγω πλαίσιο.

Κάθε υποκείμενο των δεδομένων μπορεί να λάβει αντίγραφο των πλαισίων από εμάς. Επιπλέον, τα πλαίσια είναι επίσης διαθέσιμα στην Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης ή στο δημοσιευμένο νομικό υλικό ή στους δικτυακούς τόπους των εποπτικών αρχών ή άλλων αρμόδιων αρχών ή φορέων.

## G. Περίοδος αποθήκευσης των δεδομένων προσωπικού χαρακτήρα ή, όταν αυτό είναι αδύνατο, κριτήρια καθορισμού της περιόδου (αρ. 14 παρ. 2 περ. α' ΓΚΠΔ)

Κριτήριο για τον καθορισμό της περιόδου αποθήκευσης των δεδομένων προσωπικού χαρακτήρα είναι η νόμιμη περίοδος διακράτησης. Μετά το πέρας της περιόδου αυτής, τα σχετικά δεδομένα διαγράφονται, στην έκταση που δεν είναι πλέον αναγκαία η διατήρησή τους για την εκπλήρωση της σύμβασης ή τη σύναψή της.

Εάν δεν υπάρχει νόμιμη περίοδος διατήρησης, το κριτήριο είναι η συμβατική ή εσωτερική περίοδος διατήρησης.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## Η. Δικαίωμα υποβολής αιτήματος στον υπεύθυνο επεξεργασίας για πρόσβαση και διόρθωση ή διαγραφή των δεδομένων προσωπικού χαρακτήρα ή περιορισμό της επεξεργασίας που αφορούν το υποκείμενο των δεδομένων ή αντίταξης στην επεξεργασία και φορητότητα των δεδομένων (αρ. 13 παρ. 2 περ. β' ΓΚΠΔ)

Κάθε υποκείμενο των δεδομένων έχει τα ακόλουθα δικαιώματα:

***Δικαίωμα πρόσβασης***

Το υποκείμενο των δεδομένων έχει δικαίωμα πρόσβασης σε δεδομένα προσωπικού χαρακτήρα που το αφορούν. Το δικαίωμα πρόσβασης εκτείνεται σε όλα τα δεδομένα που επεξεργάζονται από εμάς. Το δικαίωμα ασκείται ευχερώς και σε εύλογα τακτά χρονικά διαστήματα, προκειμένου το υποκείμενο των δεδομένων να έχει επίγνωση και να επαληθεύει τη νομιμότητα της επεξεργασίας (Προοίμιο 63 ΓΚΠΔ). Το δικαίωμα αυτό απορρέει από το άρθρο 15 ΓΚΠΔ. Το υποκείμενο των δεδομένων μπορεί να επικοινωνεί μαζί μας για την άσκηση του δικαιώματός του.

***Δικαίωμα διόρθωσης***

Σύμφωνα με το αρ. 16 εδ. α' ΓΚΠΔ, το υποκείμενο των δεδομένων έχει το δικαίωμα να απαιτήσει από τον υπεύθυνο επεξεργασίας χωρίς αδικαιολόγητη καθυστέρηση τη διόρθωση ανακριβών δεδομένων προσωπικού χαρακτήρα που το αφορούν. Επιπλέον το αρ. 16 εδ. β' ΓΚΠΔ τονίζει ότι, έχοντας υπόψη τους σκοπούς της επεξεργασίας, το υποκείμενο των δεδομένων έχει το δικαίωμα να απαιτήσει τη συμπλήρωση ελλιπών δεδομένων προσωπικού χαρακτήρα, μεταξύ άλλων μέσω συμπληρωματικής δήλωσης. Το υποκείμενο των δεδομένων μπορεί να επικοινωνήσει μαζί μας για την άσκηση του δικαιώματός του για διόρθωση.

***Δικαίωμα διαγραφής («δικαίωμα στη λήθη»)***

Επιπλέον, το υποκείμενο των δεδομένων έχει δικαίωμα διαγραφής των δεδομένων («δικαίωμα στη λήθη») σύμφωνα με το αρ. 17 ΓΚΠΔ. Και το δικαίωμα αυτό ασκείται μετά από επικοινωνία μαζί μας. Στο σημείο αυτό, ωστόσο, θα θέλαμε να σημειώσουμε ότι το δικαίωμα αυτό δεν μπορεί να ασκηθεί στο βαθμο που η επεξεργασία είναι απαραίτητη για την τήρηση νομικής υποχρέωσης στην οποία υπόκειται η εταιρεία μας (αρ. 17 παρ. 3 περ. β' ΓΚΠΔ). Αυτό σημαίνει ότι μπορούμε να κάνουμε δεκτή αίτηση διαγραφής μόνο μετά το πέρας της νόμιμης περιόδου διατήρησης.

***Δικαίωμα περιορισμού της επεξεργασίας***

Σύμφωνα με το αρ. 18 ΓΚΠΔ, το υποκείμενο των δεδομένων μπορεί να ζητήσει τον περιορισμό της επεξεργασίας. Ο περιορισμός της επεξεργασίας μπορεί να ζητηθεί αν πληρείται μία από τις προϋποθέσεις που ορίζει το αρ. 18 παρ. 1 στις περιπτώσεις α' έως δ' ΓΚΠΔ. Το υποκείμενο των δεδομένων μπορεί να επικοινωνήσει μαζί μας για την άσκηση του δικαιώματός του για περιορισμό της επεξεργασίας.

***Δικαίωμα εναντίωσης***

Επιπλέον, το αρ. 21 ΓΚΠΔ παρέχει το δικαίωμα εναντίωσης. Το υποκείμενο των δεδομένων μπορεί να επικοινωνήσει μαζί μας για την άσκηση του δικαιώματός του για εναντίωση.


© All rights reserved by Heiko Maniero.

***Δικαίωμα στη φορητότητα των δεδομένων***

Το αρ. 20 ΓΚΠΔ παρέχει στο υποκείμενο των δεδομένων το δικαίωμα στη φορητότητα των δεδομένων. Σύμφωνα με την παρούσα διάταξη, το υποκείμενο των δεδομένων έχει υπό τις προϋποθέσεις του αρ. 20 παρ. 1 περ. α' και β' ΓΚΠΔ το δικαίωμα να λαμβάνει τα δεδομένα προσωπικού χαρακτήρα που το αφορούν, και τα οποία έχει παράσχει σε υπεύθυνο επεξεργασίας, σε δομημένο, κοινώς χρησιμοποιούμενο και αναγνώσιμο από μηχανήματα μορφότυπο, καθώς και το δικαίωμα να διαβιβάζει τα εν λόγω δεδομένα σε άλλον υπεύθυνο επεξεργασίας χωρίς αντίρρηση από τον υπεύθυνο επεξεργασίας στον οποίο παρασχέθηκαν τα δεδομένα προσωπικού χαρακτήρα. Το υποκείμενο των δεδομένων μπορεί να επικοινωνήσει μαζί μας για την άσκηση του δικαιώματός του στη φορητότητα των δεδομένων.

## I. Το δικαίωμα ανάκλησης της συγκατάθεσης οποτεδήποτε, χωρίς να θιγεί η νομιμότητα της επεξεργασίας επί τη βάσει προηγούμενης συγκατάθεσης, όταν η επεξεργασία βασίζεται στο αρ. 6 παρ. 1 περ. α' ΓΚΠΔ ή στο αρ. 9 παρ. 2 περ. α' ΓΚΠΔ (αρ. 13 παρ. 2 περ. γ' ΓΚΠΔ)

Εάν η επεξεργασία των δεδομένων προσωπικού χαρακτήρα βασίζεται στο αρ. 6 παρ. 1 περ. γ' ΓΚΠΔ, δηλαδή το υποκείμενο των δεδομένων έχει δώσει τη συγκατάθεσή του στην επεξεργασία των δεδομένων για έναν ή περισσότερους σκοπούς, ή στο αρ. 9 παρ. 2 περ. α' ΓΚΠΔ, που ρυθμίζει την παροχή συναίνεσης για την επεξεργασία ειδικών κατηγοριών δεδομένων προσωπικού χαρακτήρα, το υποκείμενο έχει σύμφωνα με το αρ. 7 παρ. 3 εδ. α' ΓΚΠΔ το δικαίωμα ανάκλησης της συγκατάθεσής του ανά πάσα στιγμή.

Η ανάκληση της συναίνεσης δεν θίγει τη νομιμότητα της επεξεργασίας που βασίζεται στη συγκατάθεση πριν την ανάκλησή της (αρ. 7 παρ. 3 εδ. β' ΓΚΠΔ). Η ανάκληση της συγκατάθεσης είναι εξίσου εύκολη με την παροχή της (αρ. 7 παρ. 3 εδ. δ' ΓΚΠΔ). Έτσι, η άρση της συγκατάθεσης μπορεί να γίνει με τον ίδιο τρόπο όπως η χορήγησή της ή με οποιονδήποτε άλλο τρόπο το υποκείμενο των δεδομένων θεωρεί ευκολότερο. Στη σημερινή κοινότητα της πληροφορίας, ο πιο εύκολος τρόπος ανάκλησης της συναίνεσης είναι πιθανότατα μέσω email. Αν το υποκείμενο των δεδομένων επιθυμεί να ανακαλέσει τη συγκατάθεσή του προς εμάς, ένα απλό email θα ήταν αποτελεσματικό. Εναλλακτικά, το υποκείμενο των δεδομένων μπορεί να επιλέξει οποιονδήποτε άλλο τρόπο γνωστοποίησης της ανάκλησής του προς εμάς.

## J. Δικαίωμα υποβολής καταγγελίας σε εποπτική αρχή (αρ. 13 παρ. 2 περ. δ', 77 παρ. 1 ΓΚΠΔ)

Ως υπεύθυνος επεξεργασίας, είμαστε υποχρεωμένοι να ενημερώνουμε το υποκείμενο των δεδομένων σχετικά με το δικαίωμα υποβολής καταγγελίας σε εποπτική αρχή (αρ. 13 παρ. 2 περ. δ' ΓΚΠΔ). Το δικαίωμα υποβολής καταγγελίας σε εποπτική αρχή ρυθμίζεται από το αρ. 77 παρ. 1 ΓΚΠΔ. Σύμφωνα με αυτή τη διάταξη, με την επιφύλαξη τυχόν άλλων διοικητικών ή δικαστικών προσφυγών, κάθε υποκείμενο


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

των δεδομένων έχει το δικαίωμα να υποβάλει καταγγελία σε εποπτική αρχή, ιδίως στο κράτος μέλος στο οποίο έχει τη συνήθη διαμονή του ή τον τόπο εργασίας του ή τον τόπο της εικαζόμενης παράβασης, εάν το υποκείμενο των δεδομένων θεωρεί ότι η επεξεργασία των δεδομένων προσωπικού χαρακτήρα που το αφορά παραβαίνει το Γενικό Κανονισμό Προστασίας Δεδομένων. Το δικαίωμα υποβολής καταγγελίας έχει περιοριστεί από το ενωσιακό δίκαιο με τέτοιο τρόπο ώστε να μπορεί να ασκηθεί μόνο ενώπιον μίας εποπτικής αρχής (Προοίμιο 141 εδ. α' ΓΚΠΔ). Σκοπός του κανόνα αυτού είναι η αποφυγή υποβολής διπλών καταγγελιών από το ίδιο υποκείμενο δεδομένων και για το ίδιο αντικείμενο. Σε περίπτωση που υποκείμενο των δεδομένων επιθυμεί να υποβάλει καταγγελία εναντίον μας, παρακαλούμε όπως επικοινωνήσει μόνο με μία εποπτική αρχή.

## K. Παροχή δεδομένων προσωπικού χαρακτήρα στη βάση νομικής ή συμβατικής υποχρέωσης ή απαίτησης για τη σύναψη σύμβασης, υποχρέωση του υποκειμένου των δεδομένων να παρέχει τα δεδομένα προσωπικού χαρακτήρα και ενδεχόμενες συνέπειες της μη παροχή των δεδομένων (αρ. 13 παρ. 2 περ. ε' ΓΚΠΔ)

Θα θέλαμε να διευκρινίσουμε ότι η παροχή δεδομένων προσωπικού χαρακτήρα απαιτείται εν μέρει από το νόμο (πχ. από φορολογικές διατάξεις), αλλά μπορεί να προκύπτει και από συμβατικές διατάξεις (π.χ. πληροφορίες σχετικά με το άλλο συμβαλλόμενο μέρος).

Μερικές φορές θα είναι ίσως απαραίτητη η σύναψη σύμβασης μέσω της οποίας το υποκείμενο των δεδομένων μας παρέχει δεδομένα προσωπικού χαρακτήρα, τα οποία θα επεξεργαστούμε εμείς στη συνέχεια. Το υποκείμενο των δεδομένων υποχρεούται, για παράδειγμα, να μας παρέχει δεδομένα προσωπικού χαρακτήρα όταν συνάπτουμε σύμβαση μαζί του. Η μη παροχή αυτών των δεδομένων μπορεί να έχει ως συνέπεια την αδυναμία σύναψης της σύμβασης.

Πριν την παροχή των δεδομένων προσωπικού χαρακτήρα από το υποκείμενο των δεδομένων, το υποκείμενο οφείλει να επικοινωνήσει μαζί μας. Με τον τρόπο αυτό, διευκρινίζουμε στο υποκείμενο αν η παροχή των δεδομένων είναι υποχρεωτική από το νόμο ή τη σύμβαση ή είναι απαραίτητη για τη σύναψη της σύμβασης, καθώς και αν υπάρχει υποχρέωση παροχής τους και συνέπειες από τη μη παροχή.

## L. Αυτοματοποιημένη λήψη αποφάσεων, περιλαμβανομένης της κατάρτισης προφίλ, σύμφωνα με το αρ. 22 παρ. 1 και 4 ΓΚΠΔ και, τουλάχιστον στις περιπτώσεις αυτές, σημαντικές πληροφορίες σχετικά με τη λογική που ακολουθείται, καθώς και τη σημασία και τις προβλεπόμενες συνέπειες της εν λόγω επεξεργασίας για το υποκείμενο των δεδομένων

Ως υπεύθυνη εταιρεία, συνήθως δεν χρησιμοποιούμε αυτοματοποιημένη λήψη αποφάσεων ή κατάρτιση προφίλ. Εάν, σε εξαιρετικές περιπτώσεις, προβούμε σε αυτοματοποιημένη λήψη αποφάσεων ή


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

κατάρτιση προφίλ, θα ενημερώσουμε το υποκείμενο των δεδομένων είτε ξεχωριστά είτε μέσω υποενότητας στην πολιτική απορρήτου μας (στον ιστότοπό μας). Σε αυτή την περίπτωση, ισχύουν τα εξής:

Η αυτοματοποιημένη λήψη αποφάσεων - συμπεριλαμβανομένης της κατάρτισης προφίλ - μπορεί να πραγματοποιηθεί εάν (1) αυτό είναι απαραίτητο για τη σύναψη ή την εκτέλεση σύμβασης μεταξύ του υποκειμένου των δεδομένων και εμάς, ή (2) αυτό επιτρέπεται από το δίκαιο της Ένωσης ή του κράτους μέλους στο οποίο υπαγόμαστε και το οποίο προβλέπει επίσης κατάλληλα μέτρα για τη διασφάλιση των δικαιωμάτων και των ελευθεριών και των έννομων συμφερόντων του υποκειμένου των δεδομένων, ή (3) αυτό βασίζεται στη ρητή συγκατάθεση του υποκειμένου των δεδομένων.

Στις περιπτώσεις που αναφέρονται στο άρθρο 22 παράγραφος 2 στοιχεία α) και γ) του ΓΚΠΔ, εφαρμόζουμε κατάλληλα μέτρα για τη διασφάλιση των δικαιωμάτων και ελευθεριών και των έννομων συμφερόντων του υποκειμένου των δεδομένων. Σε αυτές τις περιπτώσεις, έχετε το δικαίωμα να ζητήσετε την ανθρώπινη παρέμβαση εκ μέρους του υπεύθυνου επεξεργασίας, να εκφράσετε την άποψή σας και να αμφισβητήσετε την απόφαση.

Σημαντικές πληροφορίες σχετικά με τη λογική που εμπλέκεται, καθώς και τη σημασία και τις προβλεπόμενες συνέπειες της εν λόγω επεξεργασίας για το υποκείμενο των δεδομένων παρατίθενται στην πολιτική απορρήτου μας.

## II. Συμμόρφωση με τις προϋποθέσεις για την περίπτωση που τα δεδομένα προσωπικού χαρακτήρα δεν έχουν συλλεγεί από το υποκείμενο των δεδομένων (αρ.14 ΓΚΠΔ)

### A. Ταυτότητα και στοιχεία επικοινωνίας του υπεύθυνου επεξεργασίας (αρ. 14 παρ. 1 περ. α΄ ΓΚΠΔ)

Βλέπε ανωτέρω

### B. Στοιχεία επικοινωνία του Υπεύθυνου Προστασίας Δεδομένων (αρ. 14 παρ. 1 περ. β’ ΓΚΠΔ)

Βλέπε ανωτέρω


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## C. Σκοπός επεξεργασίας των δεδομένων προσωπικού χαρακτήρα καθώς και νόμιμη βάση επεξεργασίας (αρ. 14 παρ. 1 περ. γ' ΓΚΠΔ)

Σκοπός επεξεργασίας των δεδομένων προσωπικού χαρακτήρα είναι η διαχείριση όλων των εργασιών που αφορούν τον υπεύθυνο επεξεργασίας, τους πελάτες, τους πιθανούς πελάτες, εμπορικούς συνεργάτες ή άλλες συμβατικές ή μη συμβατικές σχέσεις μεταξύ των αναφερόμενων μερών (εν ευρεία έννοια) ή άλλη νόμιμη υποχρέωση του υπεύθυνου επεξεργασίας.

Το αρ. 6 παρ. 1 περ. α' ΓΚΠΔ λειτουργεί ως η νόμιμη βάση για τις εργασίες επεξεργασίας για τις οποίες λαμβάνουμε τη συναίνεση επεξεργασίας. Σε περίπτωση που η επεξεργασία των δεδομένων προσωπικού χαρακτήρα είναι απαραίτητη για την εκτέλεση σύμβασης στην οποία συμβαλλόμενο μέρος είναι το υποκείμενο των δεδομένων, όπως, για παράδειγμα, όταν η επεξεργασία είναι απαραίτητη για την παροχή προϊόντων ή υπηρεσιών, η επεξεργασία βασίζεται στο άρθρο 6 παρ. 1 περ. β' ΓΚΠΔ. Το ίδιο ισχύει για την επεξεργασία που είναι απαραίτητη για τη λήψη μέτρων πριν τη σύναψη σύμβασης, όπως για παράδειγμα στην περίπτωση παροχής πληροφοριών που αφορούν τα προϊόντα ή τις υπηρεσίες μας. Στην περίπτωση που η εταιρεία μας υπέχει νόμιμη υποχρέωση επεξεργασίας δεδομένων προσωπικού χαρακτήρα, όπως για την εκπλήρωση φορολογικών υποχρεώσεων, η επεξεργασία βασίζεται στο αρ. 6 παρ. 1 περ. γ' ΓΚΠΔ.

Σε σπάνιες περιπτώσεις, η επεξεργασίας δεδομένων προσωπικού χαρακτήρα μπορεί να είναι απαραίτητη για τη διαφύλαξη ζωτικού συμφέροντος του υποκειμένου των δεδομένων ή άλλου φυσικού προσώπου. Τέτοια είναι η περίπτωση, για παράδειγμα, όταν επισκέπτης τραυματίζεται στην εταιρεία μας και το όνομα, η ηλικία του, δεδομένα ασφάλειας υγείας ή άλλα ζωτικές πληροφορίες διαβιβάζονται σε ιατρό, νοσοκομείο ή τρίτο πρόσωπο. Τότε η επεξεργασία βασίζεται στο αρ. 6 παρ. 1 περ. δ' ΓΚΠΔ.

Όταν η επεξεργασία είναι απαραίτητη για την εκτέλεση καθήκοντος που εκτελείται προς το δημόσιο συμφέρον ή κατά την άσκηση δημόσιας εξουσίας που έχει ανατεθεί στον υπεύθυνο επεξεργασίας, η νομική βάση είναι το αρ. 6 παρ. 1 περ. e ΓΚΠΔ.

Τέλος, οι εργασίες επεξεργασίας μπορούν να έχουν τη βάση τους στο αρ. 6 παρ. 1 ΓΚΠΔ. Λειτουργεί ως νόμιμη βάση για τις εργασίες επεξεργασίας που δεν καλύπτονται από τις προαναφερθείσες βάσεις, εφόσον η επεξεργασία είναι απαραίτητη για το σκοπό της εξυπηρέτησης των εννόμων συμφερόντων της εταιρείας μας ή τρίτου μέρους, υπό τον όρο ότι δεν υπερισχύουν των συμφερόντων ή των θεμελιωδών δικαιωμάτων και ελευθεριών του υποκειμένου του οποίου τα δεδομένα προσωπικού χαρακτήρα υπόκεινται σε προστασία. Τέτοιες εργασίες επεξεργασίας επιτρέπονται ιδίως στις περιπτώσεις που αναφέρονται από τον ευρωπαίο νομοθέτη. Σύμφωνα με αυτόν, τέτοιο έννομο συμφέρον θα μπορούσε να υπάρχει όταν το υποκείμενο των δεδομένων είναι πελάτης του υπεύθυνου επεξεργασίας (Προοίμιο παρ. 47 εδ. β' ΓΚΠΔ).

## D. Κατηγορίες δεδομένων προσωπικού χαρακτήρα (αρ. 14 παρ. 1 περ. δ' ΓΚΠΔ)


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

Δεδομένα πελατών

Δεδομένα δυνητικών πελατών

Δεδομένα εργαζομένων

Δεδομένα προμηθευτών

## Ε. Κατηγορίες αποδεκτών δεδομένων προσωπικού χαρακτήρα (αρ. 13 παρ. 1 περ. ε' ΓΚΠΔ)

Δημόσιες αρχές

Εξωτερικά όργανα

Εσωτερική επεξεργασία

Ενδοομιλική επεξεργασία

Άλλα όργανα κι οργανισμοί

Κατάλογος των εκτελούντων την επεξεργασία και των αποδεκτών των δεδομένων μας σε τρίτες χώρες και, κατά περίπτωση, διεθνών οργανισμών δημοσιεύεται στον ιστότοπό μας ή μπορεί να ζητηθεί από εμάς δωρεάν. Παρακαλούμε επικοινωνήστε με τον υπεύθυνο προστασίας δεδομένων μας για να ζητήσετε αυτόν τον κατάλογο.

## F. Αποδέκτες σε τρίτες χώρες και κατάλληλα μέτρα προστασίας και μέσα για τη λήψη αντιγράφων των δεδομένων ή των αποδεκτών τους (αρ. 14 παρ. 1 περ. στ', 46 παρ. 1, 46 παρ. 2 περ. γ' ΓΚΔΠ)

Όλες οι εταιρείες και τα υποκαταστήματα που είναι μέρος του ομίλου μας (στο εξής αναφερόμενες ως «όμιλος εταιρειών») και έχουν τη δική τους έδρα ή γραφείο σε τρίτη χώρα μπορεί να αποτελούν αποδέκτες δεδομένων προσωπικού χαρακτήρα. Μπορείτε να ζητήσετε λίστα των εταιρειών του ομίλου ή των αποδεκτών από εμάς.

Σύμφωνα με το αρ. 46 παρ. 1 ΓΚΠΔ, ο υπεύθυνος επεξεργασίας ή εκτελών την επεξεργασία μπορεί να διαβιβάζει δεδομένων προσωπικού χαρακτήρα σε τρίτη χώρα μόνο εάν ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία παρέχει κατάλληλες εγγυήσεις και υπό την προϋπόθεση ότι υφίστανται εκτελεστά δικαιώματα και αποτελεσματικά ένδικα μέσα διαθέσιμα για το υποκείμενο των δεδομένων. Οι κατάλληλες εγγυήσεις μπορούν να προβλέπονται χωρίς να απαιτείται ειδική άδεια εποπτικής αρχής μέσω τυποποιημένων συμβατικών ρητρών (αρ. 46 παρ. 2 περ. γ' ΓΚΠΔ).


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

Οι τυποποιημένες συμβατικές ρήτρες της Ευρωπαϊκής Ένωσης ή άλλες κατάλληλες εγγυήσεις συμφωνούνται με κάθε αποδέκτη σε τρίτη χώρα πριν την πρώτη διαβίβαση δεδομένων προσωπικού χαρακτήρα. Συνεπώς, διασφαλίζονται κατάλληλες εγγυήσεις, αλλά και εκτελεστά δικαιώματα και αποτελεσματικά ένδικα μέσα για τα υποκείμενα των δεδομένων. Κάθε υποκείμενο των δεδομένων μπορεί να παραλαμβάνει αντίγραφο των τυποποιημένων συμβατικών ρητρών από εμάς. Οι τυποποιημένες συμβατικές ρήτρες είναι επίσης διαθέσιμες στην Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης.

Το άρθρο 45 παράγραφος 3 του Γενικού Κανονισμού για την Προστασία Δεδομένων (ΓΚΠΔ) παρέχει στην Ευρωπαϊκή Επιτροπή την εξουσία να αποφασίζει, μέσω εκτελεστικής πράξης, ότι μια χώρα εκτός ΕΕ εξασφαλίζει επαρκές επίπεδο προστασίας. Αυτό σημαίνει επίπεδο προστασίας των δεδομένων προσωπικού χαρακτήρα που είναι ουσιαστικά ισοδύναμο με το επίπεδο προστασίας εντός της ΕΕ. Οι αποφάσεις περί επάρκειας έχουν ως αποτέλεσμα τα δεδομένα προσωπικού χαρακτήρα να μπορούν να διακινούνται ελεύθερα από την ΕΕ (και τη Νορβηγία, το Λιχτενστάιν και την Ισλανδία) προς μια τρίτη χώρα χωρίς περαιτέρω εμπόδια. Παρόμοιοι κανόνες υπάρχουν για το Ηνωμένο Βασίλειο, την Ελβετία και ορισμένες άλλες χώρες.

Σε περίπτωση που η Ευρωπαϊκή Επιτροπή ή η κυβέρνηση άλλης χώρας αποφασίσει ότι μια τρίτη χώρα εξασφαλίζει επαρκές επίπεδο προστασίας και υπάρχει έγκυρο πλαίσιο (π.χ. EU-U.S. Data Privacy Framework, Swiss-U.S. Data Privacy Framework, UK Extension to the EU-U.S. Data Privacy Framework), όλες οι διαβιβάσεις από εμάς προς τα μέλη αυτών των πλαισίων (π.χ. αυτοπιστοποιημένες οντότητες) βασίζονται αποκλειστικά στη συμμετοχή της εν λόγω οντότητας στο αντίστοιχο πλαίσιο. Όταν εμείς ή μία από τις οντότητες του ομίλου μας είναι μέλος τέτοιου πλαισίου, όλες οι διαβιβάσεις προς εμάς ή την οντότητα του ομίλου μας βασίζονται αποκλειστικά στη συμμετοχή της οντότητας στο εν λόγω πλαίσιο.

Κάθε υποκείμενο των δεδομένων μπορεί να λάβει αντίγραφο των πλαισίων από εμάς. Επιπλέον, τα πλαίσια είναι επίσης διαθέσιμα στην Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης ή στο δημοσιευμένο νομικό υλικό ή στους δικτυακούς τόπους των εποπτικών αρχών ή άλλων αρμόδιων αρχών ή φορέων.

## G. Περίοδος αποθήκευσης των δεδομένων προσωπικού χαρακτήρα ή, όταν αυτό είναι αδύνατο, κριτήρια καθορισμού της περιόδου (αρ. 14 παρ. 2 περ. α' ΓΚΠΔ)

Κριτήριο για τον καθορισμό της περιόδου αποθήκευσης των δεδομένων προσωπικού χαρακτήρα είναι η νόμιμη περίοδος διακράτησης. Μετά το πέρας της περιόδου αυτής, τα σχετικά δεδομένα διαγράφονται, στην έκταση που δεν είναι πλέον αναγκαία η διατήρησή τους για την εκπλήρωση της σύμβασης ή τη σύναψή της.

Εάν δεν υπάρχει νόμιμη περίοδος διατήρησης, το κριτήριο είναι η συμβατική ή εσωτερική περίοδος διατήρησης.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## Η. Ενημέρωση σχετικά με τα έννομα συμφέροντα που επιδιώκονται από τον υπεύθυνο επεξεργασίας ή από τρίτο, σε περίπτωση που η επεξεργασία βασίζεται στο αρ.6 παρ.1 περ. στ' ΓΚΠΔ (Αρ. 14 παρ. 2 περ. γ' ΓΚΠΔ)

Σε περίπτωση που η επεξεργασία δεδομένων προσωπικού χαρακτήρα βασίζεται στο αρ. 6 παρ. 1 περ. στ' ΓΚΠΔ, η επεξεργασία είναι νόμιμη μόνο όταν είναι απαραίτητη για τους σκοπούς των έννομων συμφερόντων που επιδιώκει ο υπεύθυνος επεξεργασίας ή τρίτος, εκτός εάν έναντι των συμφερόντων αυτών υπερισχύει το συμφέρον ή τα θεμελιώδη δικαιώματα και οι ελευθερίες του υποκειμένου των δεδομένων που επιβάλλουν την προστασία των δεδομένων προσωπικού χαρακτήρα. Σύμφωνα με την παράγραφο 47 εδ. β' του Προοιμίου, τέτοιο έννομο συμφέρον μπορεί να υπάρχει όταν υφίσταται σχετική και κατάλληλη σχέση μεταξύ του υποκειμένου των δεδομένων και του υπευθύνου επεξεργασίας, όπως π.χ. αν το υποκείμενο των δεδομένων είναι πελάτης του υπευθύνου επεξεργασίας. Σε κάθε περίπτωση επεξεργασίας δεδομένων προσωπικού χαρακτήρα από την εταιρεία μας στη βάση του αρ. 6 παρ. 1 περ. στ' ΓΚΠΔ, το έννομο συμφέρον μας είναι η άσκηση των δραστηριοτήτων μας υπέρ της ευημερίας όλων των εργαζομένων και των μετόχων μας.

## Ι. 'Υπαρξη δικαιώματος υποβολής αιτήματος στον υπεύθυνο επεξεργασίας για πρόσβαση και διόρθωση ή διαγραφή των δεδομένων προσωπικού χαρακτήρα ή περιορισμό της επεξεργασίας που αφορά το υποκείμενο των δεδομένων και δικαιώματος αντίταξης στην επεξεργασία, καθώς και δικαιώματος στη φορητότητα των δεδομένων (αρ. 14 παρ. 2 περ. γ' ΓΚΠΔ)

Κάθε υποκείμενο των δεδομένων έχει τα ακόλουθα δικαιώματα:

***Δικαίωμα πρόσβασης***

Το υποκείμενο των δεδομένων έχει δικαίωμα πρόσβασης σε δεδομένα προσωπικού χαρακτήρα που το αφορούν. Το δικαίωμα πρόσβασης εκτείνεται σε όλα τα δεδομένα που επεξεργάζονται από εμάς. Το δικαίωμα ασκείται ευχερώς και σε εύλογα τακτά χρονικά διαστήματα, προκειμένου το υποκείμενο των δεδομένων να έχει επίγνωση και να επαληθεύει τη νομιμότητα της επεξεργασίας (Προοίμιο 63 ΓΚΠΔ). Το δικαίωμα αυτό απορρέει από το άρθρο 15 ΓΚΠΔ. Το υποκείμενο των δεδομένων μπορεί να επικοινωνεί μαζί μας για την άσκηση του δικαιώματός του.

***Δικαίωμα διόρθωσης***

Σύμφωνα με το αρ. 16 εδ. α' ΓΚΠΔ, το υποκείμενο των δεδομένων έχει το δικαίωμα να απαιτήσει από τον υπεύθυνο επεξεργασίας χωρίς αδικαιολόγητη καθυστέρηση τη διόρθωση ανακριβών δεδομένων προσωπικού χαρακτήρα που το αφορούν. Επιπλέον το αρ. 16 εδ. β' ΓΚΠΔ τονίζει ότι, έχοντας υπόψη τους σκοπούς της επεξεργασίας, το υποκείμενο των δεδομένων έχει το δικαίωμα να απαιτήσει τη συμπλήρωση ελλιπών δεδομένων προσωπικού χαρακτήρα, μεταξύ άλλων μέσω συμπληρωματικής δήλωσης. Το υποκείμενο των δεδομένων μπορεί να επικοινωνήσει μαζί μας για την άσκηση του δικαιώματός του για διόρθωση.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

***Δικαίωμα διαγραφής («δικαίωμα στη λήθη»)***

Επιπλέον, το υποκείμενο των δεδομένων έχει δικαίωμα διαγραφής των δεδομένων («δικαίωμα στη λήθη») σύμφωνα με το αρ. 17 ΓΚΠΔ. Και το δικαίωμα αυτό ασκείται μετά από επικοινωνία μαζί μας. Στο σημείο αυτό, ωστόσο, θα θέλαμε να σημειώσουμε ότι το δικαίωμα αυτό δεν μπορεί να ασκηθεί στο βαθμο που η επεξεργασία είναι απαραίτητη για την τήρηση νομικής υποχρέωσης στην οποία υπόκειται η εταιρεία μας (αρ. 17 παρ. 3 περ. β' ΓΚΠΔ). Αυτό σημαίνει ότι μπορούμε να κάνουμε δεκτή αίτηση διαγραφής μόνο μετά το πέρας της νόμιμης περιόδου διατήρησης.

***Δικαίωμα περιορισμού της επεξεργασίας***

Σύμφωνα με το αρ. 18 ΓΚΠΔ, το υποκείμενο των δεδομένων μπορεί να ζητήσει τον περιορισμό της επεξεργασίας. Ο περιορισμός της επεξεργασίας μπορεί να ζητηθεί αν πληρείται μία από τις προϋποθέσεις που ορίζει το αρ. 18 παρ. 1 στις περιπτώσεις α' έως δ' ΓΚΠΔ. Το υποκείμενο των δεδομένων μπορεί να επικοινωνήσει μαζί μας για την άσκηση του δικαιώματός του για περιορισμό της επεξεργασίας.

***Δικαίωμα εναντίωσης***

Επιπλέον, το αρ. 21 ΓΚΠΔ παρέχει το δικαίωμα εναντίωσης. Το υποκείμενο των δεδομένων μπορεί να επικοινωνήσει μαζί μας για την άσκηση του δικαιώματός του για εναντίωση.

***Δικαίωμα στη φορητότητα των δεδομένων***

Το αρ. 20 ΓΚΠΔ παρέχει στο υποκείμενο των δεδομένων το δικαίωμα στη φορητότητα των δεδομένων. Σύμφωνα με την παρούσα διάταξη, το υποκείμενο των δεδομένων έχει υπό τις προϋποθέσεις του αρ. 20 παρ. 1 περ. α' και β' ΓΚΠΔ το δικαίωμα να λαμβάνει τα δεδομένα προσωπικού χαρακτήρα που το αφορούν, και τα οποία έχει παράσχει σε υπεύθυνο επεξεργασίας, σε δομημένο, κοινώς χρησιμοποιούμενο και αναγνώσιμο από μηχανήματα μορφότυπο, καθώς και το δικαίωμα να διαβιβάζει τα εν λόγω δεδομένα σε άλλον υπεύθυνο επεξεργασίας χωρίς αντίρρηση από τον υπεύθυνο επεξεργασίας στον οποίο παρασχέθηκαν τα δεδομένα προσωπικού χαρακτήρα. Το υποκείμενο των δεδομένων μπορεί να επικοινωνήσει μαζί μας για την άσκηση του δικαιώματός του στη φορητότητα των δεδομένων.

## J. Ύπαρξη του δικαιώματος ανάκλησης της συγκατάθεσής του οποτεδήποτε, χωρίς να θίγεται η νομιμότητα της επεξεργασίας που βασίστηκε στη συγκατάθεση πριν από την ανάκλησή της, όταν η επεξεργασία βασίζεται στ ααρ. 6 παρ. 1 περ. α' ή αρ. 9 παρ. 2 περ. α' ΓΚΠΔ (αρ. 14 παρ. 2 περ. δ' ΓΚΠΔ)

Εάν η επεξεργασία βασίζεται στο αρ. 6 παρ. 1 περ. α' ΓΚΠΔ, δηλαδή το υποκείμενο των δεδομένων έχει συναινέσει στην επεξεργασία των δεδομένων προσωπικού χαρακτήρα του για έναν ή περισσότερους συγκεκριμένους σκοπούς, ή στο αρ. 9 παρ. 2 περ. α' ΓΚΠΔ, που ρυθμίζει την παροχή ρητής συγκατάθεσης για την επεξεργασία ειδικών κατηγοριών δεδομένων προσωπικού χαρακτήρα, το υποκείμενο των δεδομένων έχει σύμφωνα με το αρ. 7 παρ. 3 εδ. α' ΓΚΠΔ το δικαίωμα ανάκλησης της συγκατάθεσης του ανά πάσα στιγμή.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

Η ανάκληση της συγκατάθεσης δεν θίγει τη νομιμότητα της επεξεργασίας που βασίστηκε στη συγκατάθεση προ της ανάκλησής της (αρ. 7 παρ. 3 εδ. β' ΓΚΠΔ). Η ανάκληση της συγκατάθεσης είναι εξίσου εύκολη με την παροχή της (αρ. 7 παρ. 3 εδ. δ' ΓΚΠΔ). Έτσι, η άρση της συγκατάθεσης μπορεί να γίνει με τον ίδιο τρόπο όπως η χορήγησή της ή με οποιονδήποτε άλλο τρόπο το υποκείμενο των δεδομένων θεωρεί ευκολότερο. Στη σημερινή κοινότητα της πληροφορίας, ο πιο εύκολος τρόπος ανάκλησης της συναίνεσης είναι πιθανότατα μέσω email. Αν το υποκείμενο των δεδομένων επιθυμεί να ανακαλέσει τη συγκατάθεσή του προς εμάς, ένα απλό email θα ήταν αποτελεσματικό. Εναλλακτικά, το υποκείμενο των δεδομένων μπορεί να επιλέξει οποιονδήποτε άλλο τρόπο γνωστοποίησης της ανάκλησής του προς εμάς.

## K. Δικαίωμα υποβολής καταγγελίας σε εποπτική αρχή (αρ. 14 παρ. 2 περ. ε', 77 παρ. 1 ΓΚΠΔ)

Ως υπεύθυνος επεξεργασίας, είμαστε υποχρεωμένοι να ενημερώνουμε το υποκείμενο των δεδομένων σχετικά με το δικαίωμα υποβολής καταγγελίας σε εποπτική αρχή (αρ. 14 παρ. 2 περ. ε' ΓΚΠΔ). Το δικαίωμα υποβολής καταγγελίας σε εποπτική αρχή ρυθμίζεται από το αρ. 77 παρ. 1 ΓΚΠΔ. Σύμφωνα με αυτή τη διάταξη, με την επιφύλαξη τυχόν άλλων διοικητικών ή δικαστικών προσφυγών, κάθε υποκείμενο των δεδομένων έχει το δικαίωμα να υποβάλει καταγγελία σε εποπτική αρχή, ιδίως στο κράτος μέλος στο οποίο έχει τη συνήθη διαμονή του ή τον τόπο εργασίας του ή τον τόπο της εικαζόμενης παράβασης, εάν το υποκείμενο των δεδομένων θεωρεί ότι η επεξεργασία των δεδομένων προσωπικού χαρακτήρα που το αφορά παραβαίνει το Γενικό Κανονισμό Προστασίας Δεδομένων. Το δικαίωμα υποβολής καταγγελίας έχει περιοριστεί από το ενωσιακό δίκαιο με τέτοιο τρόπο ώστε να μπορεί να ασκηθεί μόνο ενώπιον μίας εποπτικής αρχής (Προοίμιο 141 εδ. α' ΓΚΠΔ). Σκοπός του κανόνα αυτού είναι η αποφυγή υποβολής διπλών καταγγελιών από το ίδιο υποκείμενο δεδομένων και για το ίδιο αντικείμενο. Σε περίπτωση που υποκείμενο των δεδομένων επιθυμεί να υποβάλει καταγγελία εναντίον μας, παρακαλούμε όπως επικοινωνήσει μόνο με μία εποπτική αρχή.

## L. Πηγή των δεδομένων προσωπικού χαρακτήρα και, ανάλογα με την περίπτωση, προέλευση των δεδομένων από πηγές στις οποίες έχει πρόσβαση το κοινό (αρ. 14 παρ. 2 εδ. στ' ΓΚΠΔ)

Κατά κανόνα, τα δεδομένα προσωπικού χαρακτήρα συλλέγονται άμεσα από το υποκείμενο των δεδομένων ή σε συνδυασμό με ορισμένη αρχή (π.χ. ανάκτηση δεδομένων από επίσημο μητρώο). Άλλα δεδομένα προσωπικού χαρακτήρα των υποκειμένων των δεδομένων προέρτχονται από διαβιβάσεις μεταξύ ομίλων εταιρειών. Στο πλαίσιο αυτών των γενικών πληροφοριών, η ακριβής καταγραφή των πηγών από τις οποίες προέρχονται τα δεδομένα προσωπικού χαρακτήρα είτε είναι αδύνατη είτε συνεπάγεται δυσανάλογη προσπάθεια σσύμφωνα με την έννοια του αρ. 14 παρ. 5 περ. β' ΓΚΠΔ. Κατά κανόνα, δεν συλλέγουμαι δεδομένα προσωπικού χαρακτήρα από δημόσια διαθέσιμες πηγές.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

Κάθε υποκείμενο των δεδομένων μπορεί να επικοινωνήσει μαζί μας ανά πάσα στιγμή για να λάβει περισσότερες, λεπτομερείς πληροφορίες σχετικά με τις ακριβείς πηγές των δεδομένων προσωπικού χαρακτήρα που το αφορούν. Σε περιπτώσει που δεν μπορούν να παρασχεθούν πληροφορίες σχετικά με την προέλευση των δεδομένων προσωπικού χαρακτήρα στο υποκείμενο των δεδομένων καθώς έχουν χρησιμοποιηθεί περισσότερες πηγές, θα πρέπει να παρέχονται γενικές πληροφορίες (Παράγραφο 61 εδ. δ' Προοίμιο ΓΚΠΔ).

## Μ. Αυτοματοποιημένη λήψη αποφάσεων, συμπεριλαμβανομένης της κατάρτισης προφίλ, σύμφωνα με το άρθρο 22 παράγραφοι 1 και 4 και, τουλάχιστον στις περιπτώσεις αυτές, σημαντικές πληροφορίες σχετικά με τη λογική που ακολουθείται, καθώς και τη σημασία και τις προβλεπόμενες συνέπειες της εν λόγω επεξεργασίας για το υποκείμενο των δεδομένων (αρ. 14 παρ. 2 εδ. ζ' ΓΚΠΔ)

Ως υπεύθυνη εταιρεία, συνήθως δεν χρησιμοποιούμε αυτοματοποιημένη λήψη αποφάσεων ή κατάρτιση προφίλ. Εάν, σε εξαιρετικές περιπτώσεις, προβούμε σε αυτοματοποιημένη λήψη αποφάσεων ή κατάρτιση προφίλ, θα ενημερώσουμε το υποκείμενο των δεδομένων είτε ξεχωριστά είτε μέσω υποενότητας στην πολιτική απορρήτου μας (στον ιστότοπό μας). Σε αυτή την περίπτωση, ισχύουν τα εξής:

Η αυτοματοποιημένη λήψη αποφάσεων - συμπεριλαμβανομένης της κατάρτισης προφίλ - μπορεί να πραγματοποιηθεί εάν (1) αυτό είναι απαραίτητο για τη σύναψη ή την εκτέλεση σύμβασης μεταξύ του υποκειμένου των δεδομένων και εμάς, ή (2) αυτό επιτρέπεται από το δίκαιο της Ένωσης ή του κράτους μέλους στο οποίο υπαγόμαστε και το οποίο προβλέπει επίσης κατάλληλα μέτρα για τη διασφάλιση των δικαιωμάτων και των ελευθεριών και των έννομων συμφερόντων του υποκειμένου των δεδομένων, ή (3) αυτό βασίζεται στη ρητή συγκατάθεση του υποκειμένου των δεδομένων.

Στις περιπτώσεις που αναφέρονται στο άρθρο 22 παράγραφος 2 στοιχεία α) και γ) του ΓΚΠΔ, εφαρμόζουμε κατάλληλα μέτρα για τη διασφάλιση των δικαιωμάτων και ελευθεριών και των έννομων συμφερόντων του υποκειμένου των δεδομένων. Σε αυτές τις περιπτώσεις, έχετε το δικαίωμα να ζητήσετε την ανθρώπινη παρέμβαση εκ μέρους του υπεύθυνου επεξεργασίας, να εκφράσετε την άποψή σας και να αμφισβητήσετε την απόφαση.

Σημαντικές πληροφορίες σχετικά με τη λογική που εμπλέκεται, καθώς και τη σημασία και τις προβλεπόμενες συνέπειες της εν λόγω επεξεργασίας για το υποκείμενο των δεδομένων παρατίθενται στην πολιτική απορρήτου μας.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## III. EU-U.S. Data Privacy Framework (EU-U.S. DPF), UK Extension to the EU-U.S. DPF, Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF)

Εάν ο οργανισμός μας είναι πιστοποιημένο μέλος του EU-U.S. Data Privacy Framework (EU-U.S. DPF) και/ή του UK Extension to the EU-U.S. DPF και/ή του Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF), ισχύουν τα ακόλουθα:

Συμμορφωνόμαστε με το EU-U.S. Data Privacy Framework (EU-U.S. DPF) και το UK Extension to the EU-U.S. DPF καθώς και με το Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF), όπως έχει καθοριστεί από το U.S. Department of Commerce. Η εταιρεία μας έχει επιβεβαιώσει στο Υπουργείο Εμπορίου των ΗΠΑ ότι τηρεί τις EU-U.S. Data Privacy Framework Principles (EU-U.S. DPF Principles) όσον αφορά την επεξεργασία προσωπικών δεδομένων που λαμβάνει από την Ευρωπαϊκή Ένωση και το Ηνωμένο Βασίλειο αναφερόμενη στο EU-U.S. DPF και το UK Extension to the EU-U.S. DPF. Η εταιρεία μας έχει επιβεβαιώσει στο Υπουργείο Εμπορίου των ΗΠΑ ότι τηρεί τις Swiss-U.S. Data Privacy Framework Principles (Swiss-U.S. DPF Principles) όσον αφορά την επεξεργασία προσωπικών δεδομένων που λαμβάνει από την Ελβετία αναφερόμενη στο Swiss-U.S. DPF. Σε περίπτωση αντίθεσης μεταξύ των διατάξεων της πολιτικής απορρήτου μας και των EU-U.S. DPF Principles και/ή των Swiss-U.S. DPF Principles, οι Principles είναι αυτές που υπερισχύουν.

Για να μάθετε περισσότερα σχετικά με το Data Privacy Framework (DPF) πρόγραμμα και για να δείτε την πιστοποίησή μας, επισκεφθείτε τη διεύθυνση https://www.dataprivacyframework.gov/.

Οι άλλες αμερικανικές μονάδες ή θυγατρικές της εταιρείας μας που επίσης συμμορφώνονται με τις EU-U.S. DPF Principles, συμπεριλαμβανομένου του UK Extension to the EU-U.S. DPF και των Swiss-U.S. DPF Principles, εάν υπάρχουν, αναφέρονται στην πολιτική απορρήτου μας.

Σύμφωνα με το EU-U.S. DPF και το UK Extension to the EU-U.S. DPF καθώς και το Swiss-U.S. DPF, η εταιρεία μας δεσμεύεται να συνεργάζεται με τις ευρωπαϊκές αρχές προστασίας δεδομένων και το Information Commissioner's Office (ICO) του Ηνωμένου Βασιλείου καθώς και το Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) της Ελβετίας και να ακολουθεί τις συμβουλές τους σχετικά με άλυτες καταγγελίες για τον χειρισμό προσωπικών δεδομένων που λαμβάνουμε αναφερόμενοι στο EU-U.S. DPF και το UK Extension to the EU-U.S. DPF και το Swiss-U.S. DPF.

Ενημερώνουμε τα υποκείμενα των δεδομένων σχετικά με τις αρμόδιες ευρωπαϊκές αρχές προστασίας δεδομένων που είναι υπεύθυνες για την επεξεργασία καταγγελιών σχετικά με τον χειρισμό προσωπικών δεδομένων από τον οργανισμό μας στο πάνω μέρος αυτού του εγγράφου διαφάνειας και ότι παρέχουμε στα υποκείμενα των δεδομένων κατάλληλη και δωρεάν προσφυγή.

Ενημερώνουμε όλα τα υποκείμενα των δεδομένων ότι η εταιρεία μας υπόκειται στις ερευνητικές και εκτελεστικές εξουσίες της Federal Trade Commission (FTC).


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

Τα υποκείμενα των δεδομένων έχουν υπό ορισμένες προϋποθέσεις τη δυνατότητα να υποβληθούν σε δεσμευτική διαιτησία. Ο οργανισμός μας υποχρεούται να επιλύσει αξιώσεις και να τηρεί τις συνθήκες του Παραρτήματος I των DPF Principles, εάν το υποκείμενο των δεδομένων έχει ζητήσει δεσμευτική διαιτησία ενημερώνοντας τον οργανισμό μας και ακολουθώντας τις διαδικασίες και συνθήκες του Παραρτήματος I των Principles.

Ενημερώνουμε εδώ όλα τα υποκείμενα των δεδομένων σχετικά με την ευθύνη του οργανισμού μας σε περίπτωση διαβίβασης προσωπικών δεδομένων σε τρίτους.

Για ερωτήσεις των υποκειμένων των δεδομένων ή των αρχών προστασίας δεδομένων, έχουμε ορίσει τους τοπικούς εκπροσώπους που αναφέρονται στο πάνω μέρος αυτού του εγγράφου διαφάνειας.

Σας προσφέρουμε τη δυνατότητα επιλογής (Opt-out), αν τα προσωπικά σας δεδομένα (i) διαβιβαστούν σε τρίτους ή (ii) χρησιμοποιηθούν για σκοπό που διαφέρει ουσιαστικά από τον/τους σκοπό/ούς για τον/τους οποίους αρχικά συλλέχθηκαν ή αργότερα εγκρίθηκαν από εσάς. Ο σαφής, ευδιάκριτος και εύκολα προσβάσιμος μηχανισμός για την άσκηση του δικαιώματός σας επιλογής είναι η επικοινωνία μέσω ηλεκτρονικού ταχυδρομείου με τον υπεύθυνο προστασίας δεδομένων (DSB). Δεν έχετε δικαίωμα επιλογής και δεν είμαστε υποχρεωμένοι, εάν τα δεδομένα διαβιβαστούν σε τρίτο που ενεργεί ως εντολέας ή επεξεργαστής για λογαριασμό μας και σύμφωνα με τις οδηγίες μας. Ωστόσο, πάντα συνάπτουμε σύμβαση με τέτοιον εντολέα ή επεξεργαστή.

Για ευαίσθητα δεδομένα (π.χ. προσωπικά δεδομένα που περιέχουν πληροφορίες για την υγεία, τη φυλετική ή εθνική καταγωγή, πολιτικές απόψεις, θρησκευτικές ή φιλοσοφικές πεποιθήσεις, μέλη σε συνδικαλιστική οργάνωση ή δεδομένα για τη σεξουαλική ζωή του ατόμου), λαμβάνουμε τη ρητή συγκατάθεσή σας (Opt-in) αν αυτά τα δεδομένα (i) διαβιβαστούν σε τρίτους ή (ii) χρησιμοποιηθούν για σκοπό διαφορετικό από αυτόν για τον οποίο αρχικά συλλέχθηκαν ή για τον οποίο αργότερα δώσατε τη συγκατάθεσή σας επιλέγοντας Opt-in. Επιπλέον, αντιμετωπίζουμε όλα τα προσωπικά δεδομένα που λαμβάνουμε από τρίτους ως ευαίσθητα, αν ο τρίτος τα έχει χαρακτηρίσει και αντιμετωπίσει ως ευαίσθητα.

Σας ενημερώνουμε εδώ σχετικά με την ανάγκη αποκάλυψης προσωπικών δεδομένων ως απάντηση σε νόμιμα αιτήματα αρχών, συμπεριλαμβανομένης της συμμόρφωσης με τις απαιτήσεις εθνικής ασφάλειας ή επιβολής του νόμου.

Κατά τη διαβίβαση προσωπικών δεδομένων σε τρίτο που ενεργεί ως υπεύθυνος επεξεργασίας, συμμορφωνόμαστε με τις Principals της ειδοποίησης και της επιλογής. Επιπλέον, συνάπτουμε σύμβαση με τον τρίτο που είναι υπεύθυνος για την επεξεργασία, η οποία προβλέπει ότι αυτά τα δεδομένα μπορούν να υποβληθούν σε επεξεργασία μόνο για περιορισμένους και καθορισμένους σκοπούς σύμφωνα με τη συγκατάθεση που έχετε δώσει και ότι ο παραλήπτης παρέχει το ίδιο επίπεδο προστασίας όπως οι Principals του DPF και μας ειδοποιεί αν διαπιστώσει ότι δεν μπορεί πλέον να εκπληρώσει αυτή τη δέσμευση. Η σύμβαση προβλέπει ότι ο τρίτος που είναι υπεύθυνος επεξεργασίας θα σταματήσει την επεξεργασία ή θα λάβει άλλα κατάλληλα και κατάλληλα μέτρα για την παροχή λύσης, εάν διαπιστωθεί ότι δεν μπορεί να εκπληρώσει τη δέσμευσή του.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

Κατά τη διαβίβαση προσωπικών δεδομένων σε τρίτο που ενεργεί ως εντολέας ή επεξεργαστής, (i) διαβιβάζουμε αυτά τα δεδομένα μόνο για περιορισμένους και καθορισμένους σκοπούς, (ii) διασφαλίζουμε ότι ο εντολέας ή επεξεργαστής δεσμεύεται να παρέχει τουλάχιστον το ίδιο επίπεδο προστασίας δεδομένων όπως απαιτούν οι DPF Principles, (iii) λαμβάνουμε κατάλληλα και κατάλληλα μέτρα για να διασφαλίσουμε ότι ο εντολέας ή επεξεργαστής επεξεργάζεται τα προσωπικά δεδομένα που διαβιβάζονται με τρόπο που συμφωνεί με τις δεσμεύσεις μας σύμφωνα με τις DPF Principles, (iv) απαιτούμε από τον εντολέα ή επεξεργαστή να μας ειδοποιήσει αν διαπιστώσει ότι δεν μπορεί να εκπληρώσει τη δέσμευσή του να παρέχει το ίδιο επίπεδο προστασίας όπως απαιτούν οι DPF Principles, (v) λαμβάνουμε κατάλληλα και κατάλληλα μέτρα για να σταματήσουμε την ανεπίτρεπτη επεξεργασία και να παρέχουμε λύση σε περίπτωση που ληφθεί ειδοποίηση, συμπεριλαμβανομένης της ειδοποίησης υπό (iv), και (vi) παρέχουμε στο DPF Department, κατόπιν αιτήματος, μια περίληψη ή ένα αντιπροσωπευτικό αντίγραφο των σχετικών διατάξεων προστασίας δεδομένων της σύμβασής μας με αυτόν τον εντολέα.

Σύμφωνα με το EU-U.S. DPF και/ή το UK Extension to the EU-U.S. DPF και/ή το Swiss-U.S. DPF, η εταιρεία μας δεσμεύεται να συνεργάζεται με το σώμα που έχει συσταθεί από τις ευρωπαϊκές αρχές προστασίας δεδομένων και το Information Commissioner's Office (ICO) του Ηνωμένου Βασιλείου ή το Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) της Ελβετίας και να ακολουθεί τις συμβουλές τους σχετικά με άλυτες καταγγελίες για τον χειρισμό προσωπικών δεδομένων που λαμβάνουμε αναφερόμενοι στο EU-U.S. DPF και την UK Extension to the EU-U.S. DPF και το Swiss-U.S. DPF στο πλαίσιο της εργασιακής σχέσης.

Όλα τα υποκείμενα των δεδομένων που βρίσκονται προσωρινά στην Ευρωπαϊκή Ένωση (ΕΕ), στον Ευρωπαϊκό Οικονομικό Χώρο (ΕΟΧ) ή στο Ηνωμένο Βασίλειο ή που έχουν την κατοικία ή τη συνήθη διαμονή τους εκεί, δικαιούνται τα δικαιώματα και τα δικαιώματα των υποκειμένων των δεδομένων που δημοσιεύονται στο Έγγραφο Διαφάνειας, τα οποία απορρέουν επίσης από τα άρθρα 15 έως 22 του ΓΚΠΔ, συμπεριλαμβανομένου του δικαιώματος πρόσβασης σε δεδομένα προσωπικού χαρακτήρα. Έχουμε καταστήσει τις πληροφορίες αυτές διαθέσιμες σε όλες τις γλώσσες της ΕΕ και του ΕΟΧ. Η έκδοση στην αγγλική γλώσσα ισχύει για το Ηνωμένο Βασίλειο.

Όλα τα υποκείμενα των δεδομένων που διαμένουν προσωρινά στην Ελβετία ή έχουν την κατοικία τους ή τη συνήθη διαμονή τους εκεί, δικαιούνται τα δικαιώματα και τα δικαιώματα των υποκειμένων των δεδομένων σύμφωνα με τον ελβετικό νόμο περί προστασίας δεδομένων (DPA) και τον ελβετικό κανονισμό περί προστασίας δεδομένων (DPR), τα οποία δημοσιεύονται στο έγγραφο διαφάνειας, συμπεριλαμβανομένου του δικαιώματος πρόσβασης σε δεδομένα προσωπικού χαρακτήρα. Έχουμε παράσχει αυτές τις πληροφορίες στις τρεις επίσημες γλώσσες της Ελβετίας (γερμανικά, ιταλικά και γαλλικά).


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

# GREEK: Πληροφορίες σχετικά με την επεξεργασία δεδομένων προσωπικού χαρακτήρα Εργαζομένων και Υποψηφίων (Άρθρα 13, 14 ΓΚΠΔ)

Αγαπητέ κύριε, κυρία,

Τα δεδομένα προσωπικού χαρακτήρα εργαζομένων και υποψηφίων χαίρουν ειδικής προστασίας. Σκοπός μας είναι να διατηρήσουμε το υψηλό επίπεδο προστασίας δεδομένων μας. Για το σκοπό αυτό, αναπτύσσουμε συστηματικά τους μηχανισμούς προστασίας και ασφάλειας δεδομένων.

Ασφαλώς τηρούμε τις νόμιμες διατάξεις προστασίας δεδομένων. Σύμφωνα με τα άρθρα 13 και 14 ΓΚΠΔ, οι υπεύθυνοι επεξεργασίας θα πρέπει να πληρούν ειδικές προϋποθέσεις κατά την επεξεργασία δεδομένων προσωπικού χαρακτήρα. Το έγγραφο αυτό πληρεί τις σχετικές προϋποθέσεις.

Η ορολογία των νομικών ρυθμίσεων είναι περίπλοκη. Δυστυχώς, η χρήση νομικών εννοιών δεν μπορούσε να αποφευχθεί κατά τη σύνταξη του παρόντος εγγράφου. Για το λόγο αυτό, θα θέλαμε να τονίσουμε ότι μπορείτε ανά πάσα στιγμή να επικοινωνήσετε μαζί μας για κάθε ερώτηση σχετικά με το παρόν έγγραφο, τους χρησιμοποιούμενους όρους και τη διατύπωση.

## I. Πληροφορίες που παρέχονται εάν τα δεδομένα προσωπικού χαρακτήρα συλλέγονται από το υποκείμενο των δεδομένων (Άρθρο 13 ΓΚΠΔ)

### A. Ταυτότητα και στοιχεία επικοινωνίας του υπεύθυνου επεξεργασίας (Αρ. 13 παρ. 1 περ. α΄ ΓΚΠΔ)

Βλέπε ανωτέρω

### B. Στοιχεία επικοινωνίας του Υπεύθυνου Προστασίας Δεδομένων (Αρ. 13 παρ. 1 περ. β’ ΓΚΠΔ)

Βλέπε ανωτέρω


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## C. Σκοπός της επιχειρούμενης επεξεργασίας δεδομένων προσωπικού χαρακτήρα και νόμιμη βάση επεξεργασίας (αρ. 13 (1) περ. γ' ΓΚΠΔ)

Σε ό,τι αφορά τα δεδομένα των υποψηφίων, σκοπός της επεξεργασίας δεδομένων είναι η διενέργεια ελέγχου της αίτησης κατά τη διάρκεια της διαδικασίας πρόσληψης. Για το σκοπό αυτό, επεξεργαζόμαστε όλα τα δεδομένα που μας παρέχετε. Με βάση τα δεδομένα που παρέχετε κατά τη διάρκεια της διαδικασίας πρόσληψης, εξετάζουμε αν θα κληθείτε σε συνέντευξη εργασίας (μλερος της διαδικασίας επιλογής). Στην περίπτωση υποψηφίων που πληρούν τις γενικές προϋποθέσεις, συγκεκριμένα στο πλαίσιο της συνέντευξης, επεξεργαζόμαστε συγκεκριμένα δεδομένα προσωπικού χαρακτήρα που μας παρέχετε και είναι απαραίτητα για την επιλογή. Αν προσληφθείτε, τα δεδομένα υποψηφίου μετατρέπονται αυτόματα σε δεδομένα εργαζόμενου. Ως μέρος της διαδικασίας πρόσληψης, επεξεργαζόμαστε και άλλα δεδομένα προσωπικού χαρακτήρα σχετικά με εσάς που σας ζητούμε και είναι απαραίτητα για τη σύναψη ή την εκτέλεση της σύμβασής μας (όπως δεδομένα τυατοποίησης ή αριθμό φορολογικού μητρώου). Σχετικά με τα δεδομένα εργαζομένων, σκοπός της επεξεργασίας είναι η εκτέλεση της σύμβασης εργασίας ή η συμμόρφωση με άλλες διατάξεις εφαρμοστέες στην εργασιακή σχέση (π.χ. φορολογικό δίκαιο), καθώς και για την εκτέλεση της σύμβασης εργασίας (π.χ. δημοσιοποίηση του ονόματος και των στοιχείων επικοινωνίας στην εταιρεία ή τους πελάτες). Τα δεδομένα εργαζομένων διατηρούνται μετά τη λύση της εργασιακής σχέσης σύμφωνα με τις νόμιμες διατάξεις σχετικά με την περίοδο διακράτησής τους.

Νόμιμη βάση για την επεξεργασία των δεδομένων είναι το αρ. 6 παρ. 1 περ. β' ΓΚΠΔ, το αρ. 9 παρ. 2 περ. β' και η΄ΓΚΠΔ, το αρ. 88 παρ. 1 ΓΚΠΔ και η εθνική νομοθεσία.

## D. Κατηγορίες αποδεκτών δεδομένων προσωπικού χαρακτήρα (αρ. 13 παρ. 1 περ. ε' ΓΚΠΔ)

Δημόσιες αρχές

Εξωτερικά όργανα

Εσωτερική επεξεργασία

Ενδοομιλική επεξεργασία

Άλλα όργανα κι οργανισμοί

Κατάλογος των εκτελούντων την επεξεργασία και των αποδεκτών των δεδομένων μας σε τρίτες χώρες και, κατά περίπτωση, διεθνών οργανισμών δημοσιεύεται στον ιστότοπό μας ή μπορεί να ζητηθεί από εμάς δωρεάν. Παρακαλούμε επικοινωνήστε με τον υπεύθυνο προστασίας δεδομένων μας για να ζητήσετε αυτόν τον κατάλογο.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## E. Αποδέκτες σε τρίτες χώρες και κατάλληλα μέτρα προστασίας και μέσα για τη λήψη αντιγράφων των δεδομένων ή των αποδεκτών τους (αρ. 13 παρ. 1 περ. στ', 46 παρ. 1, 46 παρ. 2 περ. γ' ΓΚΔΠ)

Όλες οι εταιρείες και τα υποκαταστήματα που είναι μέρος του ομίλου μας (στο εξής αναφερόμενες ως «όμιλος εταιρειών») και έχουν τη δική τους έδρα ή γραφείο σε τρίτη χώρα μπορεί να αποτελούν αποδέκτες δεδομένων προσωπικού χαρακτήρα. Μπορείτε να ζητήσετε λίστα των εταιρειών του ομίλου ή των αποδεκτών από εμάς.

Σύμφωνα με το αρ. 46 παρ. 1 ΓΚΠΔ, ο υπεύθυνος επεξεργασίας ή εκτελών την επεξεργασία μπορεί να διαβιβάζει δεδομένων προσωπικού χαρακτήρα σε τρίτη χώρα μόνο εάν ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία παρέχει κατάλληλες εγγυήσεις και υπό την προϋπόθεση ότι υφίστανται εκτελεστά δικαιώματα και αποτελεσματικά ένδικα μέσα διαθέσιμα για το υποκείμενο των δεδομένων. Οι κατάλληλες εγγυήσεις μπορούν να προβλέπονται χωρίς να απαιτείται ειδική άδεια εποπτικής αρχής μέσω τυποποιημένων συμβατικών ρητρών (αρ. 46 παρ. 2 περ. γ' ΓΚΠΔ).

Οι τυποποιημένες συμβατικές ρήτρες της Ευρωπαϊκής Ένωσης ή άλλες κατάλληλες εγγυήσεις συμφωνούνται με κάθε αποδέκτη σε τρίτη χώρα πριν την πρώτη διαβίβαση δεδομένων προσωπικού χαρακτήρα. Συνεπώς, διασφαλίζονται κατάλληλες εγγυήσεις, αλλά και εκτελεστά δικαιώματα και αποτελεσματικά ένδικα μέσα για τα υποκείμενα των δεδομένων. Κάθε υποκείμενο των δεδομένων μπορεί να παραλαμβάνει αντίγραφο των τυποποιημένων συμβατικών ρητρών από εμάς. Οι τυποποιημένες συμβατικές ρήτρες είναι επίσης διαθέσιμες στην Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης.

Το άρθρο 45 παράγραφος 3 του Γενικού Κανονισμού για την Προστασία Δεδομένων (ΓΚΠΔ) παρέχει στην Ευρωπαϊκή Επιτροπή την εξουσία να αποφασίζει, μέσω εκτελεστικής πράξης, ότι μια χώρα εκτός ΕΕ εξασφαλίζει επαρκές επίπεδο προστασίας. Αυτό σημαίνει επίπεδο προστασίας των δεδομένων προσωπικού χαρακτήρα που είναι ουσιαστικά ισοδύναμο με το επίπεδο προστασίας εντός της ΕΕ. Οι αποφάσεις περί επάρκειας έχουν ως αποτέλεσμα τα δεδομένα προσωπικού χαρακτήρα να μπορούν να διακινούνται ελεύθερα από την ΕΕ (και τη Νορβηγία, το Λιχτενστάιν και την Ισλανδία) προς μια τρίτη χώρα χωρίς περαιτέρω εμπόδια. Παρόμοιοι κανόνες υπάρχουν για το Ηνωμένο Βασίλειο, την Ελβετία και ορισμένες άλλες χώρες.

Σε περίπτωση που η Ευρωπαϊκή Επιτροπή ή η κυβέρνηση άλλης χώρας αποφασίσει ότι μια τρίτη χώρα εξασφαλίζει επαρκές επίπεδο προστασίας και υπάρχει έγκυρο πλαίσιο (π.χ. EU-U.S. Data Privacy Framework, Swiss-U.S. Data Privacy Framework, UK Extension to the EU-U.S. Data Privacy Framework), όλες οι διαβιβάσεις από εμάς προς τα μέλη αυτών των πλαισίων (π.χ. αυτοπιστοποιημένες οντότητες) βασίζονται αποκλειστικά στη συμμετοχή της εν λόγω οντότητας στο αντίστοιχο πλαίσιο. Όταν εμείς ή μία από τις οντότητες του ομίλου μας είναι μέλος τέτοιου πλαισίου, όλες οι διαβιβάσεις προς εμάς ή την οντότητα του ομίλου μας βασίζονται αποκλειστικά στη συμμετοχή της οντότητας στο εν λόγω πλαίσιο.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

Κάθε υποκείμενο των δεδομένων μπορεί να λάβει αντίγραφο των πλαισίων από εμάς. Επιπλέον, τα πλαίσια είναι επίσης διαθέσιμα στην Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης ή στο δημοσιευμένο νομικό υλικό ή στους δικτυακούς τόπους των εποπτικών αρχών ή άλλων αρμόδιων αρχών ή φορέων.

## F. Περίοδος αποθήκευσης των δεδομένων προσωπικού χαρακτήρα ή, όταν αυτό είναι αδύνατο, κριτήρια καθορισμού της περιόδου (αρ. 14 παρ. 2 περ. α' ΓΚΠΔ)

Κριτήριο για τον καθορισμό της περιόδου αποθήκευσης των δεδομένων προσωπικού χαρακτήρα είναι η νόμιμη περίοδος διακράτησης. Μετά το πέρας της περιόδου αυτής, τα σχετικά δεδομένα διαγράφονται, στην έκταση που δεν είναι πλέον αναγκαία η διατήρησή τους για την εκπλήρωση της σύμβασης ή τη σύναψή της.

## G. Δικαίωμα υποβολής αιτήματος στον υπεύθυνο επεξεργασίας για πρόσβαση και διόρθωση ή διαγραφή των δεδομένων προσωπικού χαρακτήρα ή περιορισμό της επεξεργασίας που αφορούν το υποκείμενο των δεδομένων ή αντίταξης στην επεξεργασία και φορητότητα των δεδομένων (αρ. 13 παρ. 2 περ. β' ΓΚΠΔ)

Κάθε υποκείμενο των δεδομένων έχει τα ακόλουθα δικαιώματα:

***Δικαίωμα πρόσβασης***

Το υποκείμενο των δεδομένων έχει δικαίωμα πρόσβασης σε δεδομένα προσωπικού χαρακτήρα που το αφορούν. Το δικαίωμα πρόσβασης εκτείνεται σε όλα τα δεδομένα που επεξεργάζονται από εμάς. Το δικαίωμα ασκείται ευχερώς και σε εύλογα τακτά χρονικά διαστήματα, προκειμένου το υποκείμενο των δεδομένων να έχει επίγνωση και να επαληθεύει τη νομιμότητα της επεξεργασίας (Προοίμιο 63 ΓΚΠΔ). Το δικαίωμα αυτό απορρέει από το άρθρο 15 ΓΚΠΔ. Το υποκείμενο των δεδομένων μπορεί να επικοινωνεί μαζί μας για την άσκηση του δικαιώματός του.

***Δικαίωμα διόρθωσης***

Σύμφωνα με το αρ. 16 εδ. α' ΓΚΠΔ, το υποκείμενο των δεδομένων έχει το δικαίωμα να απαιτήσει από τον υπεύθυνο επεξεργασίας χωρίς αδικαιολόγητη καθυστέρηση τη διόρθωση ανακριβών δεδομένων προσωπικού χαρακτήρα που το αφορούν. Επιπλέον το αρ. 16 εδ. β' ΓΚΠΔ τονίζει ότι, έχοντας υπόψη τους σκοπούς της επεξεργασίας, το υποκείμενο των δεδομένων έχει το δικαίωμα να απαιτήσει τη συμπλήρωση ελλιπών δεδομένων προσωπικού χαρακτήρα, μεταξύ άλλων μέσω συμπληρωματικής δήλωσης. Το υποκείμενο των δεδομένων μπορεί να επικοινωνήσει μαζί μας για την άσκηση του δικαιώματός του για διόρθωση.

***Δικαίωμα διαγραφής («δικαίωμα στη λήθη»)***

Επιπλέον, το υποκείμενο των δεδομένων έχει δικαίωμα διαγραφής των δεδομένων («δικαίωμα στη λήθη») σύμφωνα με το αρ. 17 ΓΚΠΔ. Και το δικαίωμα αυτό ασκείται μετά από επικοινωνία μαζί μας. Στο σημείο αυτό, ωστόσο, θα θέλαμε να σημειώσουμε ότι το δικαίωμα αυτό δεν μπορεί να ασκηθεί στο βαθμο


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

που η επεξεργασία είναι απαραίτητη για την τήρηση νομικής υποχρέωσης στην οποία υπόκειται η εταιρεία μας (αρ. 17 παρ. 3 περ. β' ΓΚΠΔ). Αυτό σημαίνει ότι μπορούμε να κάνουμε δεκτή αίτηση διαγραφής μόνο μετά το πέρας της νόμιμης περιόδου διατήρησης.

***Δικαίωμα περιορισμού της επεξεργασίας***

Σύμφωνα με το αρ. 18 ΓΚΠΔ, το υποκείμενο των δεδομένων μπορεί να ζητήσει τον περιορισμό της επεξεργασίας. Ο περιορισμός της επεξεργασίας μπορεί να ζητηθεί αν πληρείται μία από τις προϋποθέσεις που ορίζει το αρ. 18 παρ. 1 στις περιπτώσεις α' έως δ' ΓΚΠΔ. Το υποκείμενο των δεδομένων μπορεί να επικοινωνήσει μαζί μας για την άσκηση του δικαιώματός του για περιορισμό της επεξεργασίας.

***Δικαίωμα εναντίωσης***

Επιπλέον, το αρ. 21 ΓΚΠΔ παρέχει το δικαίωμα εναντίωσης. Το υποκείμενο των δεδομένων μπορεί να επικοινωνήσει μαζί μας για την άσκηση του δικαιώματός του για εναντίωση.

***Δικαίωμα στη φορητότητα των δεδομένων***

Το αρ. 20 ΓΚΠΔ παρέχει στο υποκείμενο των δεδομένων το δικαίωμα στη φορητότητα των δεδομένων. Σύμφωνα με την παρούσα διάταξη, το υποκείμενο των δεδομένων έχει υπό τις προϋποθέσεις του αρ. 20 παρ. 1 περ. α' και β' ΓΚΠΔ το δικαίωμα να λαμβάνει τα δεδομένα προσωπικού χαρακτήρα που το αφορούν, και τα οποία έχει παράσχει σε υπεύθυνο επεξεργασίας, σε δομημένο, κοινώς χρησιμοποιούμενο και αναγνώσιμο από μηχανήματα μορφότυπο, καθώς και το δικαίωμα να διαβιβάζει τα εν λόγω δεδομένα σε άλλον υπεύθυνο επεξεργασίας χωρίς αντίρρηση από τον υπεύθυνο επεξεργασίας στον οποίο παρασχέθηκαν τα δεδομένα προσωπικού χαρακτήρα. Το υποκείμενο των δεδομένων μπορεί να επικοινωνήσει μαζί μας για την άσκηση του δικαιώματός του στη φορητότητα των δεδομένων.

## Η. Το δικαίωμα ανάκλησης της συγκατάθεσης οποτεδήποτε, χωρίς να θιγεί η νομιμότητα της επεξεργασίας επί τη βάσει προηγούμενης συγκατάθεσης, όταν η επεξεργασία βασίζεται στο αρ. 6 παρ. 1 περ. α' ΓΚΠΔ ή στο αρ. 9 παρ. 2 περ. α' ΓΚΠΔ (αρ. 13 παρ. 2 περ. γ' ΓΚΠΔ)

Εάν η επεξεργασία των δεδομένων προσωπικού χαρακτήρα βασίζεται στο αρ. 6 παρ. 1 περ. α' ΓΚΠΔ, δηλαδή το υποκείμενο των δεδομένων έχει δώσει τη συγκατάθεσή του στην επεξεργασία των δεδομένων για έναν ή περισσότερους σκοπούς, ή στο αρ. 9 παρ. 2 περ. α' ΓΚΠΔ, που ρυθμίζει την παροχή συναίνεσης για την επεξεργασία ειδικών κατηγοριών δεδομένων προσωπικού χαρακτήρα, το υποκείμενο έχει σύμφωνα με το αρ. 7 παρ. 3 εδ. α' ΓΚΠΔ το δικαίωμα ανάκλησης της συγκατάθεσής του ανά πάσα στιγμή.

Η ανάκληση της συναίνεσης δεν θίγει τη νομιμότητα της επεξεργασίας που βασίζεται στη συγκατάθεση πριν την ανάκλησή της (αρ. 7 παρ. 3 εδ. β' ΓΚΠΔ). Η ανάκληση της συγκατάθεσης είναι εξίσου εύκολη με την παροχή της (αρ. 7 παρ. 3 εδ. δ' ΓΚΠΔ). Έτσι, η άρση της συγκατάθεσης μπορεί να γίνει με τον


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

ίδιο τρόπο όπως η χορήγησή της ή με οποιονδήποτε άλλο τρόπο το υποκείμενο των δεδομένων θεωρεί ευκολότερο. Στη σημερινή κοινότητα της πληροφορίας, ο πιο εύκολος τρόπος ανάκλησης της συναίνεσης είναι πιθανότατα μέσω email. Αν το υποκείμενο των δεδομένων επιθυμεί να ανακαλέσει τη συγκατάθεσή του προς εμάς, ένα απλό email θα ήταν αποτελεσματικό. Εναλλακτικά, το υποκείμενο των δεδομένων μπορεί να επιλέξει οποιονδήποτε άλλο τρόπο γνωστοποίησης της ανάκλησής του προς εμάς.

## I. Δικαίωμα υποβολής καταγγελίας σε εποπτική αρχή (αρ. 13 παρ. 2 περ. δ', 77 παρ. 1 ΓΚΠΔ)

Ως υπεύθυνος επεξεργασίας, είμαστε υποχρεωμένοι να ενημερώνουμε το υποκείμενο των δεδομένων σχετικά με το δικαίωμα υποβολής καταγγελίας σε εποπτική αρχή (αρ. 13 παρ. 2 περ. δ' ΓΚΠΔ). Το δικαίωμα υποβολής καταγγελίας σε εποπτική αρχή ρυθμίζεται από το αρ. 77 παρ. 1 ΓΚΠΔ. Σύμφωνα με αυτή τη διάταξη, με την επιφύλαξη τυχόν άλλων διοικητικών ή δικαστικών προσφυγών, κάθε υποκείμενο των δεδομένων έχει το δικαίωμα να υποβάλει καταγγελία σε εποπτική αρχή, ιδίως στο κράτος μέλος στο οποίο έχει τη συνήθη διαμονή του ή τον τόπο εργασίας του ή τον τόπο της εικαζόμενης παράβασης, εάν το υποκείμενο των δεδομένων θεωρεί ότι η επεξεργασία των δεδομένων προσωπικού χαρακτήρα που το αφορά παραβαίνει το Γενικό Κανονισμό Προστασίας Δεδομένων. Το δικαίωμα υποβολής καταγγελίας έχει περιοριστεί από το ενωσιακό δίκαιο με τέτοιο τρόπο ώστε να μπορεί να ασκηθεί μόνο ενώπιον μίας εποπτικής αρχής (Προοίμιο 141 εδ. α' ΓΚΠΔ). Σκοπός του κανόνα αυτού είναι η αποφυγή υποβολής διπλών καταγγελιών από το ίδιο υποκείμενο δεδομένων και για το ίδιο αντικείμενο. Σε περίπτωση που υποκείμενο των δεδομένων επιθυμεί να υποβάλει καταγγελία εναντίον μας, παρακαλούμε όπως επικοινωνήσει μόνο με μία εποπτική αρχή.

## J. Παροχή δεδομένων προσωπικού χαρακτήρα στη βάση νομικής ή συμβατικής υποχρέωσης ή απαίτησης για τη σύναψη σύμβασης, υποχρέωση του υποκειμένου των δεδομένων να παρέχει τα δεδομένα προσωπικού χαρακτήρα και ενδεχόμενες συνέπειες της μη παροχή των δεδομένων (αρ. 13 παρ. 2 περ. ε' ΓΚΠΔ)

Θα θέλαμε να διευκρινίσουμε ότι η παροχή δεδομένων προσωπικού χαρακτήρα απαιτείται εν μέρει από το νόμο (π.χ. από φορολογικές διατάξεις), αλλά μπορεί να προκύπτει και από συμβατικές διατάξεις (π.χ. πληροφορίες σχετικά με το άλλο συμβαλλόμενο μέρος).

Μερικές φορές είναι ίσως απαραίτητη η σύναψη σύμβασης μέσω της οποίας το υποκείμενο των δεδομένων μας παρέχει δεδομένα προσωπικού χαρακτήρα, τα οποία θα επεξεργαστούμε εμείς στη συνέχεια. Το υποκείμενο των δεδομένων υποχρεούται, για παράδειγμα, να μας παρέχει δεδομένα προσωπικού χαρακτήρα όταν συνάπτουμε σύμβαση μαζί του. Η μη παροχή αυτών των δεδομένων μπορεί να έχει ως συνέπεια την αδυναμία σύναψης της σύμβασης.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

Πριν την παροχή των δεδομένων προσωπικού χαρακτήρα από το υποκείμενο των δεδομένων, το υποκείμενο οφείλει να επικοινωνήσει μαζί μας. Με τον τρόπο αυτό, διευκρινίζουμε στο υποκείμενο αν η παροχή των δεδομένων είναι υποχρεωτική από το νόμο ή τη σύμβαση ή είναι απαραίτητη για τη σύναψη της σύμβασης, καθώς και αν υπάρχει υποχρέωση παροχής τους και συνέπειες από τη μη παροχή.

### K. Αυτοματοποιημένη λήψη αποφάσεων, περιλαμβανομένης της κατάρτισης προφίλ, σύμφωνα με το αρ. 22 παρ. 1 και 4 ΓΚΠΔ και, τουλάχιστον στις περιπτώσεις αυτές, σημαντικές πληροφορίες σχετικά με τη λογική που ακολουθείται, καθώς και τη σημασία και τις προβλεπόμενες συνέπειες της εν λόγω επεξεργασίας για το υποκείμενο των δεδομένων

Ως υπεύθυνη εταιρεία, συνήθως δεν χρησιμοποιούμε αυτοματοποιημένη λήψη αποφάσεων ή κατάρτιση προφίλ. Εάν, σε εξαιρετικές περιπτώσεις, προβούμε σε αυτοματοποιημένη λήψη αποφάσεων ή κατάρτιση προφίλ, θα ενημερώσουμε το υποκείμενο των δεδομένων είτε ξεχωριστά είτε μέσω υποενότητας στην πολιτική απορρήτου μας (στον ιστότοπό μας). Σε αυτή την περίπτωση, ισχύουν τα εξής:

Η αυτοματοποιημένη λήψη αποφάσεων - συμπεριλαμβανομένης της κατάρτισης προφίλ - μπορεί να πραγματοποιηθεί εάν (1) αυτό είναι απαραίτητο για τη σύναψη ή την εκτέλεση σύμβασης μεταξύ του υποκειμένου των δεδομένων και εμάς, ή (2) αυτό επιτρέπεται από το δίκαιο της Ένωσης ή του κράτους μέλους στο οποίο υπαγόμαστε και το οποίο προβλέπει επίσης κατάλληλα μέτρα για τη διασφάλιση των δικαιωμάτων και των ελευθεριών και των έννομων συμφερόντων του υποκειμένου των δεδομένων, ή (3) αυτό βασίζεται στη ρητή συγκατάθεση του υποκειμένου των δεδομένων.

Στις περιπτώσεις που αναφέρονται στο άρθρο 22 παράγραφος 2 στοιχεία α) και γ) του ΓΚΠΔ, εφαρμόζουμε κατάλληλα μέτρα για τη διασφάλιση των δικαιωμάτων και ελευθεριών και των έννομων συμφερόντων του υποκειμένου των δεδομένων. Σε αυτές τις περιπτώσεις, έχετε το δικαίωμα να ζητήσετε την ανθρώπινη παρέμβαση εκ μέρους του υπεύθυνου επεξεργασίας, να εκφράσετε την άποψή σας και να αμφισβητήσετε την απόφαση.

Σημαντικές πληροφορίες σχετικά με τη λογική που εμπλέκεται, καθώς και τη σημασία και τις προβλεπόμενες συνέπειες της εν λόγω επεξεργασίας για το υποκείμενο των δεδομένων παρατίθενται στην πολιτική απορρήτου μας.

## II. Συμμόρφωση με τις προϋποθέσεις για την περίπτωση που τα δεδομένα προσωπικού χαρακτήρα δεν έχουν συλλεγεί από το υποκείμενο των δεδομένων (αρ.14 ΓΚΠΔ)


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## A. Ταυτότητα και στοιχεία επικοινωνίας του υπεύθυνου επεξεργασίας (αρ. 14 παρ. 1 περ. α΄ ΓΚΠΔ)

Βλέπε ανωτέρω

## B. Στοιχεία επικοινωνία του Υπεύθυνου Προστασίας Δεδομένων (αρ. 14 παρ. 1 περ. β’ ΓΚΠΔ)

Βλέπε ανωτέρω

## C. Σκοπός επεξεργασίας των δεδομένων προσωπικού χαρακτήρα καθώς και νόμιμη βάση επεξεργασίας (αρ. 14 παρ. 1 περ. γ’ ΓΚΠΔ)

Σε ό,τι αφορά τα δεδομένα των υποψηφίων που δεν συλλέγησαν μέσω του υποκειμένου των δεδομένων, σκοπός της επεξεργασίας είναι η διενέργεια ελέγχου της αίτησης κατά τη διάρκεια της διαδικασίας πρόσληψης. Για το σκοπό αυτό, ενδέχεται να επεξεργαζόμαστε δεδομένα που δεν έχουμε συλλέξει από εσάς. Με βάση τα δεδομένα που επεξεργαζόμαστε κατά τη διάρκεια της διαδικασίας πρόσληψης, εξετάζουμε αν θα κληθείτε σε συνέντευξη εργασίας (μέρος της διαδικασίας επιλογής). Αν προσληφθείτε, τα δεδομένα υποψηφίου μετατρέπονται αυτόματα σε δεδομένα εργαζόμενου. Σχετικά με τα δεδομένα εργαζομένων, σκοπός της επεξεργασίας είναι η εκτέλεση της σύμβασης εργασίας ή η συμμόρφωση με άλλες διατάξεις εφαρμοστέες στην εργασιακή σχέση. Τα δεδομένα εργαζομένων διατηρούνται μετά τη λύση της εργασιακής σχέσης σύμφωνα με τις νόμιμες διατάξεις σχετικά με την περίοδο διακράτησης..

Νόμιμη βάση για την επεξεργασία των δεδομένων είναι το αρ. 6 παρ. 1 περ. β’ ΓΚΠΔ, το αρ. 9 παρ. 2 περ. β’ και η’ ΓΚΠΔ, το αρ. 88 παρ. 1 ΓΚΠΔ και η εθνική νομοθεσία.

## D. Κατηγορίες δεδομένων προσωπικού χαρακτήρα (αρ. 14 παρ. 1 περ. δ’ ΓΚΠΔ)

Δεδομένα υποψηδίων

Δεδομένα εργαζομένων

## E. Κατηγορίες αποδεκτών δεδομένων προσωπικού χαρακτήρα (αρ. 13 παρ. 1 περ. ε’ ΓΚΠΔ)

Δημόσιες αρχές

Εξωτερικά όργανα


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

Εσωτερική επεξεργασία

Ενδοομιλική επεξεργασία

Άλλα όργανα κι οργανισμοί

Κατάλογος των εκτελούντων την επεξεργασία και των αποδεκτών των δεδομένων μας σε τρίτες χώρες και, κατά περίπτωση, διεθνών οργανισμών δημοσιεύεται στον ιστότοπό μας ή μπορεί να ζητηθεί από εμάς δωρεάν. Παρακαλούμε επικοινωνήστε με τον υπεύθυνο προστασίας δεδομένων μας για να ζητήσετε αυτόν τον κατάλογο.

## F. Αποδέκτες σε τρίτες χώρες και κατάλληλα μέτρα προστασίας και μέσα για τη λήψη αντιγράφων των δεδομένων ή των αποδεκτών τους (αρ. 14 παρ. 1 περ. στ', 46 παρ. 1, 46 παρ. 2 περ. γ' ΓΚΔΠ)

Όλες οι εταιρείες και τα υποκαταστήματα που είναι μέρος του ομίλου μας (στο εξής αναφερόμενες ως «όμιλος εταιρειών») και έχουν τη δική τους έδρα ή γραφείο σε τρίτη χώρα μπορεί να αποτελούν αποδέκτες δεδομένων προσωπικού χαρακτήρα. Μπορείτε να ζητήσετε λίστα των εταιρειών του ομίλου ή των αποδεκτών από εμάς.

Σύμφωνα με το αρ. 46 παρ. 1 ΓΚΠΔ, ο υπεύθυνος επεξεργασίας ή εκτελών την επεξεργασία μπορεί να διαβιβάζει δεδομένων προσωπικού χαρακτήρα σε τρίτη χώρα μόνο εάν ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία παρέχει κατάλληλες εγγυήσεις και υπό την προϋπόθεση ότι υφίστανται εκτελεστά δικαιώματα και αποτελεσματικά ένδικα μέσα διαθέσιμα για το υποκείμενο των δεδομένων. Οι κατάλληλες εγγυήσεις μπορούν να προβλέπονται χωρίς να απαιτείται ειδική άδεια εποπτικής αρχής μέσω τυποποιημένων συμβατικών ρητρών (αρ. 46 παρ. 2 περ. γ' ΓΚΠΔ).

Οι τυποποιημένες συμβατικές ρήτρες της Ευρωπαϊκής Ένωσης ή άλλες κατάλληλες εγγυήσεις συμφωνούνται με κάθε αποδέκτη σε τρίτη χώρα πριν την πρώτη διαβίβαση δεδομένων προσωπικού χαρακτήρα. Συνεπώς, διασφαλίζονται κατάλληλες εγγυήσεις, αλλά και εκτελεστά δικαιώματα και αποτελεσματικά ένδικα μέσα για τα υποκείμενα των δεδομένων. Κάθε υποκείμενο των δεδομένων μπορεί να παραλαμβάνει αντίγραφο των τυποποιημένων συμβατικών ρητρών από εμάς. Οι τυποποιημένες συμβατικές ρήτρες είναι επίσης διαθέσιμες στην Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης.

Το άρθρο 45 παράγραφος 3 του Γενικού Κανονισμού για την Προστασία Δεδομένων (ΓΚΠΔ) παρέχει στην Ευρωπαϊκή Επιτροπή την εξουσία να αποφασίζει, μέσω εκτελεστικής πράξης, ότι μια χώρα εκτός ΕΕ εξασφαλίζει επαρκές επίπεδο προστασίας. Αυτό σημαίνει επίπεδο προστασίας των δεδομένων προσωπικού χαρακτήρα που είναι ουσιαστικά ισοδύναμο με το επίπεδο προστασίας εντός της ΕΕ. Οι αποφάσεις περί επάρκειας έχουν ως αποτέλεσμα τα δεδομένα προσωπικού χαρακτήρα να μπορούν να διακινούνται ελεύθερα από την ΕΕ (και τη Νορβηγία, το Λιχτενστάιν και την Ισλανδία) προς μια τρίτη χώρα χωρίς περαιτέρω εμπόδια. Παρόμοιοι κανόνες υπάρχουν για το Ηνωμένο Βασίλειο, την Ελβετία και ορισμένες άλλες χώρες.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

Σε περίπτωση που η Ευρωπαϊκή Επιτροπή ή η κυβέρνηση άλλης χώρας αποφασίσει ότι μια τρίτη χώρα εξασφαλίζει επαρκές επίπεδο προστασίας και υπάρχει έγκυρο πλαίσιο (π.χ. EU-U.S. Data Privacy Framework, Swiss-U.S. Data Privacy Framework, UK Extension to the EU-U.S. Data Privacy Framework), όλες οι διαβιβάσεις από εμάς προς τα μέλη αυτών των πλαισίων (π.χ. αυτοπιστοποιημένες οντότητες) βασίζονται αποκλειστικά στη συμμετοχή της εν λόγω οντότητας στο αντίστοιχο πλαίσιο. Όταν εμείς ή μία από τις οντότητες του ομίλου μας είναι μέλος τέτοιου πλαισίου, όλες οι διαβιβάσεις προς εμάς ή την οντότητα του ομίλου μας βασίζονται αποκλειστικά στη συμμετοχή της οντότητας στο εν λόγω πλαίσιο.

Κάθε υποκείμενο των δεδομένων μπορεί να λάβει αντίγραφο των πλαισίων από εμάς. Επιπλέον, τα πλαίσια είναι επίσης διαθέσιμα στην Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης ή στο δημοσιευμένο νομικό υλικό ή στους δικτυακούς τόπους των εποπτικών αρχών ή άλλων αρμόδιων αρχών ή φορέων.

## G. Περίοδος αποθήκευσης των δεδομένων προσωπικού χαρακτήρα ή, όταν αυτό είναι αδύνατο, κριτήρια καθορισμού της περιόδου (αρ. 14 παρ. 2 περ. α' ΓΚΠΔ)

Η περίοδος διατήρησης των δεδομένων των υποψηφίων είναι 6 μήνες. Για τα δεδομένα εργαζομένων εφαρμόζεται η αντίστοιχη νόμιμη περίοδος διακράτησης. Μετά το πέρας της περιόδου αυτής, τα αντίστοιχα δεδομένα διαγράφονται, εφόσον δεν είναι πλέον απαραίτητα για την εκτέλεση της σύμβασης ή για τη σύναψή της.

## H. Ενημέρωση σχετικά με τα έννομα συμφέροντα που επιδιώκονται από τον υπεύθυνο επεξεργασίας ή από τρίτο, σε περίπτωση που η επεξεργασία βασίζεται στο αρ. 6 παρ. 1 περ. στ' ΓΚΠΔ (Αρ. 14 παρ. 2 περ. β' ΓΚΠΔ)

Σύμφωνα με το αρ. 6 παρ. 1 περ. στ' ΓΚΠΔ, η επεξεργασία είναι νόμιμη μόνο όταν είναι απαραίτητη για τους σκοπούς των έννομων συμφερόντων που επιδιώκει ο υπεύθυνος επεξεργασίας ή τρίτος, εκτός εάν έναντι των συμφερόντων αυτών υπερισχύει το συμφέρον ή τα θεμελιώδη δικαιώματα και οι ελευθερίες του υποκειμένου των δεδομένων που επιβάλλουν την προστασία των δεδομένων προσωπικού χαρακτήρα. Σύμφωνα με την παράγραφο 47 εδ. β' του Προοιμίου, τέτοιο έννομο συμφέρον μπορεί να υπάρχει όταν υφίσταται σχετική και κατάλληλη σχέση μεταξύ του υποκειμένου των δεδομένων και του υπευθύνου επεξεργασίας, όπως π.χ. αν το υποκείμενο των δεδομένων είναι πελάτης του υπευθύνου επεξεργασίας. Σε κάθε περίπτωση επεξεργασίας δεδομένων προσωπικού χαρακτήρα από την εταιρεία μας στη βάση του αρ. 6 παρ. 1 περ. στ' ΓΚΠΔ, το έννομο συμφέρον μας είναι η άσκηση των δραστηριοτήτων μας υπέρ της ευημερίας όλων των εργαζομένων και των μετόχων μας.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## I. Ύπαρξη δικαιώματος υποβολής αιτήματος στον υπεύθυνο επεξεργασίας για πρόσβαση και διόρθωση ή διαγραφή των δεδομένων προσωπικού χαρακτήρα ή περιορισμό της επεξεργασίας που αφορά το υποκείμενο των δεδομένων και δικαιώματος αντίταξης στην επεξεργασία, καθώς και δικαιώματος στη φορητότητα των δεδομένων (αρ. 14 παρ. 2 περ. γ' ΓΚΠΔ)

Κάθε υποκείμενο των δεδομένων έχει τα ακόλουθα δικαιώματα:

***Δικαίωμα πρόσβασης***

Το υποκείμενο των δεδομένων έχει δικαίωμα πρόσβασης σε δεδομένα προσωπικού χαρακτήρα που το αφορούν. Το δικαίωμα πρόσβασης εκτείνεται σε όλα τα δεδομένα που επεξεργάζονται από εμάς. Το δικαίωμα ασκείται ευχερώς και σε εύλογα τακτά χρονικά διαστήματα, προκειμένου το υποκείμενο των δεδομένων να έχει επίγνωση και να επαληθεύει τη νομιμότητα της επεξεργασίας (Προοίμιο 63 ΓΚΠΔ). Το δικαίωμα αυτό απορρέει από το άρθρο 15 ΓΚΠΔ. Το υποκείμενο των δεδομένων μπορεί να επικοινωνεί μαζί μας για την άσκηση του δικαιώματός του.

***Δικαίωμα διόρθωσης***

Σύμφωνα με το αρ. 16 εδ. α' ΓΚΠΔ, το υποκείμενο των δεδομένων έχει το δικαίωμα να απαιτήσει από τον υπεύθυνο επεξεργασίας χωρίς αδικαιολόγητη καθυστέρηση τη διόρθωση ανακριβών δεδομένων προσωπικού χαρακτήρα που το αφορούν. Επιπλέον το αρ. 16 εδ. β' ΓΚΠΔ τονίζει ότι, έχοντας υπόψη τους σκοπούς της επεξεργασίας, το υποκείμενο των δεδομένων έχει το δικαίωμα να απαιτήσει τη συμπλήρωση ελλιπών δεδομένων προσωπικού χαρακτήρα, μεταξύ άλλων μέσω συμπληρωματικής δήλωσης. Το υποκείμενο των δεδομένων μπορεί να επικοινωνήσει μαζί μας για την άσκηση του δικαιώματός του για διόρθωση.

***Δικαίωμα διαγραφής («δικαίωμα στη λήθη»)***

Επιπλέον, το υποκείμενο των δεδομένων έχει δικαίωμα διαγραφής των δεδομένων («δικαίωμα στη λήθη») σύμφωνα με το αρ. 17 ΓΚΠΔ. Και το δικαίωμα αυτό ασκείται μετά από επικοινωνία μαζί μας. Στο σημείο αυτό, ωστόσο, θα θέλαμε να σημειώσουμε ότι το δικαίωμα αυτό δεν μπορεί να ασκηθεί στο βαθμο που η επεξεργασία είναι απαραίτητη για την τήρηση νομικής υποχρέωσης στην οποία υπόκειται η εταιρεία μας (αρ. 17 παρ. 3 περ. β' ΓΚΠΔ). Αυτό σημαίνει ότι μπορούμε να κάνουμε δεκτή αίτηση διαγραφής μόνο μετά το πέρας της νόμιμης περιόδου διατήρησης.

***Δικαίωμα περιορισμού της επεξεργασίας***

Σύμφωνα με το αρ. 18 ΓΚΠΔ, το υποκείμενο των δεδομένων μπορεί να ζητήσει τον περιορισμό της επεξεργασίας. Ο περιορισμός της επεξεργασίας μπορεί να ζητηθεί αν πληρείται μία από τις προϋποθέσεις που ορίζει το αρ. 18 παρ. 1 στις περιπτώσεις α' έως δ' ΓΚΠΔ. Το υποκείμενο των δεδομένων μπορεί να επικοινωνήσει μαζί μας για την άσκηση του δικαιώματός του για περιορισμό της επεξεργασίας.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

***Δικαίωμα εναντίωσης***

Επιπλέον, το αρ. 21 ΓΚΠΔ παρέχει το δικαίωμα εναντίωσης. Το υποκείμενο των δεδομένων μπορεί να επικοινωνήσει μαζί μας για την άσκηση του δικαιώματός του για εναντίωση.

***Δικαίωμα στη φορητότητα των δεδομένων***

Το αρ. 20 ΓΚΠΔ παρέχει στο υποκείμενο των δεδομένων το δικαίωμα στη φορητότητα των δεδομένων. Σύμφωνα με την παρούσα διάταξη, το υποκείμενο των δεδομένων έχει υπό τις προϋποθέσεις του αρ. 20 παρ. 1 περ. α' και β' ΓΚΠΔ το δικαίωμα να λαμβάνει τα δεδομένα προσωπικού χαρακτήρα που το αφορούν, και τα οποία έχει παράσχει σε υπεύθυνο επεξεργασίας, σε δομημένο, κοινώς χρησιμοποιούμενο και αναγνώσιμο από μηχανήματα μορφότυπο, καθώς και το δικαίωμα να διαβιβάζει τα εν λόγω δεδομένα σε άλλον υπεύθυνο επεξεργασίας χωρίς αντίρρηση από τον υπεύθυνο επεξεργασίας στον οποίο παρασχέθηκαν τα δεδομένα προσωπικού χαρακτήρα. Το υποκείμενο των δεδομένων μπορεί να επικοινωνήσει μαζί μας για την άσκηση του δικαιώματός του στη φορητότητα των δεδομένων.

## J. Ύπαρξη του δικαιώματος ανάκλησης της συγκατάθεσής του οποτεδήποτε, χωρίς να θίγεται η νομιμότητα της επεξεργασίας που βασίστηκε στη συγκατάθεση πριν από την ανάκλησή της, όταν η επεξεργασία βασίζεται στ ααρ. 6 παρ. 1 περ. α' ή αρ. 9 παρ. 2 περ. α' ΓΚΠΔ (αρ. 14 παρ. 2 περ. δ' ΓΚΠΔ)

Εάν η επεξεργασία βασίζεται στο αρ. 6 παρ. 1 περ. α' ΓΚΠΔ, δηλαδή το υποκείμενο των δεδομένων έχει συναινέσει στην επεξεργασία των δεδομένων προσωπικού χαρακτήρα για έναν ή περισσότερους συγκεκριμένους σκοπούς, ή στο αρ. 9 παρ. 2 περ. α' ΓΚΠΔ, που ρυθμίζει την παροχή ρητής συγκατάθεσης για την επεξεργασία ειδικών κατηγοριών δεδομένων προσωπικού χαρακτήρα, το υποκείμενο των δεδομένων έχει σύμφωνα με το αρ. 7 παρ. 3 εδ. α' ΓΚΠΔ το δικαίωμα ανάκλησης της συγκατάθεσης του ανά πάσα στιγμή.

Η ανάκληση της συγκατάθεσης δεν θίγει τη νομιμότητα της επεξεργασίας που βασίστηκε στη συγκατάθεση προ της ανάκλησής της (αρ. 7 παρ. 3 εδ. β' ΓΚΠΔ). Η ανάκληση της συγκατάθεσης είναι εξίσου εύκολη με την παροχή της (αρ. 7 παρ. 3 εδ. δ' ΓΚΠΔ). Έτσι, η άρση της συγκατάθεσης μπορεί να γίνει με τον ίδιο τρόπο όπως η χορήγησή της ή με οποιονδήποτε άλλο τρόπο το υποκείμενο των δεδομένων θεωρεί ευκολότερο. Στη σημερινή κοινότητα της πληροφορίας, ο πιο εύκολος τρόπος ανάκλησης της συναίνεσης είναι πιθανότατα μέσω email. Αν το υποκείμενο των δεδομένων επιθυμεί να ανακαλέσει τη συγκατάθεσή του προς εμάς, ένα απλό email θα ήταν αποτελεσματικό. Εναλλακτικά, το υποκείμενο των δεδομένων μπορεί να επιλέξει οποιονδήποτε άλλο τρόπο γνωστοποίησης της πρόθεσης ανάκλησης προς εμάς.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## K. Δικαίωμα υποβολής καταγγελίας σε εποπτική αρχή (αρ. 14 παρ. 2 περ. ε', 77 παρ. 1 ΓΚΠΔ)

Ως υπεύθυνος επεξεργασίας, είμαστε υποχρεωμένοι να ενημερώνουμε το υποκείμενο των δεδομένων σχετικά με το δικαίωμα υποβολής καταγγελίας σε εποπτική αρχή (αρ. 14 παρ. 2 περ. ε' ΓΚΠΔ). Το δικαίωμα υποβολής καταγγελίας σε εποπτική αρχή ρυθμίζεται από το αρ. 77 παρ. 1 ΓΚΠΔ. Σύμφωνα με αυτή τη διάταξη, με την επιφύλαξη τυχόν άλλων διοικητικών ή δικαστικών προσφυγών, κάθε υποκείμενο των δεδομένων έχει το δικαίωμα να υποβάλει καταγγελία σε εποπτική αρχή, ιδίως στο κράτος μέλος στο οποίο έχει τη συνήθη διαμονή του ή τον τόπο εργασίας του ή τον τόπο της εικαζόμενης παράβασης, εάν το υποκείμενο των δεδομένων θεωρεί ότι η επεξεργασία των δεδομένων προσωπικού χαρακτήρα που το αφορά παραβαίνει το Γενικό Κανονισμό Προστασίας Δεδομένων. Το δικαίωμα υποβολής καταγγελίας έχει περιοριστεί από το ενωσιακό δίκαιο με τέτοιο τρόπο ώστε να μπορεί να ασκηθεί μόνο ενώπιον μίας εποπτικής αρχής (Προοίμιο 141 εδ. α' ΓΚΠΔ). Σκοπός του κανόνα αυτού είναι η αποφυγή υποβολής διπλών καταγγελιών από το ίδιο υποκείμενο δεδομένων και για το ίδιο αντικείμενο. Σε περίπτωση που υποκείμενο των δεδομένων επιθυμεί να υποβάλει καταγγελία εναντίον μας, παρακαλούμε όπως επικοινωνήσει μόνο με μία εποπτική αρχή.

## L. Πηγή των δεδομένων προσωπικού χαρακτήρα και, ανάλογα με την περίπτωση, προέλευση των δεδομένων από πηγές στις οποίες έχει πρόσβαση το κοινό (αρ. 14 παρ. 2 εδ. στ' ΓΚΠΔ)

Κατά κανόνα, τα δεδομένα προσωπικού χαρακτήρα συλλέγονται άμεσα από το υποκείμενο των δεδομένων ή σε συνδυασμό με ορισμένη αρχή (π.χ. ανάκτηση δεδομένων από επίσημο μητρώο). Άλλα δεδομένα προσωπικού χαρακτήρα των υποκειμένων των δεδομένων προέρτχονται από διαβιβάσεις μεταξύ ομίλων εταιρειών. Στο πλαίσιο αυτών των γενικών πληροφοριών, η ακριβής καταγραφή των πηγών από τις οποίες προέρχονται τα δεδομένα προσωπικού χαρακτήρα είτε είναι αδύνατη είτε συνεπάγεται δυσανάλογη προσπάθεια σσύμφωνα με την έννοια του αρ. 14 παρ. 5 περ. β' ΓΚΠΔ. Κατά κανόνα, δεν συλλέγουμαι δεδομένα προσωπικού χαρακτήρα από δημόσια διαθέσιμες πηγές.

Κάθε υποκείμενο των δεδομένων μπορεί να επικοινωνήσει μαζί μας ανά πάσα στιγμή για να λάβει περισσότερες, λεπτομερείς πληροφορίες σχετικά με τις ακριβείς πηγές των δεδομένων προσωπικού χαρακτήρα που το αφορούν. Σε περιπτώσει που δεν μπορούν να παρασχεθούν πληροφορίες σχετικά με την προέλευση των δεδομένων προσωπικού χαρακτήρα στο υποκείμενο των δεδομένων καθώς έχουν χρησιμοποιηθεί περισσότερες πηγές, θα πρέπει να παρέχονται γενικές πληροφορίες (Παράγραφο 61 εδ. δ' Προοίμιο ΓΚΠΔ).


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

### M. Αυτοματοποιημένη λήψη αποφάσεων, συμπεριλαμβανομένης της κατάρτισης προφίλ, σύμφωνα με το άρθρο 22 παράγραφοι 1 και 4 και, τουλάχιστον στις περιπτώσεις αυτές, σημαντικές πληροφορίες σχετικά με τη λογική που ακολουθείται, καθώς και τη σημασία και τις προβλεπόμενες συνέπειες της εν λόγω επεξεργασίας για το υποκείμενο των δεδομένων (αρ. 14 παρ. 2 εδ. ζ' ΓΚΠΔ)

Ως υπεύθυνη εταιρεία, συνήθως δεν χρησιμοποιούμε αυτοματοποιημένη λήψη αποφάσεων ή κατάρτιση προφίλ. Εάν, σε εξαιρετικές περιπτώσεις, προβούμε σε αυτοματοποιημένη λήψη αποφάσεων ή κατάρτιση προφίλ, θα ενημερώσουμε το υποκείμενο των δεδομένων είτε ξεχωριστά είτε μέσω υποενότητας στην πολιτική απορρήτου μας (στον ιστότοπό μας). Σε αυτή την περίπτωση, ισχύουν τα εξής:

Η αυτοματοποιημένη λήψη αποφάσεων - συμπεριλαμβανομένης της κατάρτισης προφίλ - μπορεί να πραγματοποιηθεί εάν (1) αυτό είναι απαραίτητο για τη σύναψη ή την εκτέλεση σύμβασης μεταξύ του υποκειμένου των δεδομένων και εμάς, ή (2) αυτό επιτρέπεται από το δίκαιο της Ένωσης ή του κράτους μέλους στο οποίο υπαγόμαστε και το οποίο προβλέπει επίσης κατάλληλα μέτρα για τη διασφάλιση των δικαιωμάτων και των ελευθεριών και των έννομων συμφερόντων του υποκειμένου των δεδομένων, ή (3) αυτό βασίζεται στη ρητή συγκατάθεση του υποκειμένου των δεδομένων.

Στις περιπτώσεις που αναφέρονται στο άρθρο 22 παράγραφος 2 στοιχεία α) και γ) του ΓΚΠΔ, εφαρμόζουμε κατάλληλα μέτρα για τη διασφάλιση των δικαιωμάτων και ελευθεριών και των έννομων συμφερόντων του υποκειμένου των δεδομένων. Σε αυτές τις περιπτώσεις, έχετε το δικαίωμα να ζητήσετε την ανθρώπινη παρέμβαση εκ μέρους του υπεύθυνου επεξεργασίας, να εκφράσετε την άποψή σας και να αμφισβητήσετε την απόφαση.

Σημαντικές πληροφορίες σχετικά με τη λογική που εμπλέκεται, καθώς και τη σημασία και τις προβλεπόμενες συνέπειες της εν λόγω επεξεργασίας για το υποκείμενο των δεδομένων παρατίθενται στην πολιτική απορρήτου μας.

## III. EU-U.S. Data Privacy Framework (EU-U.S. DPF), UK Extension to the EU-U.S. DPF, Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF)

Εάν ο οργανισμός μας είναι πιστοποιημένο μέλος του EU-U.S. Data Privacy Framework (EU-U.S. DPF) και/ή του UK Extension to the EU-U.S. DPF και/ή του Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF), ισχύουν τα ακόλουθα:

Συμμορφωνόμαστε με το EU-U.S. Data Privacy Framework (EU-U.S. DPF) και το UK Extension to the EU-U.S. DPF καθώς και με το Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF), όπως έχει


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

καθοριστεί από το U.S. Department of Commerce. Η εταιρεία μας έχει επιβεβαιώσει στο Υπουργείο Εμπορίου των ΗΠΑ ότι τηρεί τις EU-U.S. Data Privacy Framework Principles (EU-U.S. DPF Principles) όσον αφορά την επεξεργασία προσωπικών δεδομένων που λαμβάνει από την Ευρωπαϊκή Ένωση και το Ηνωμένο Βασίλειο αναφερόμενη στο EU-U.S. DPF και το UK Extension to the EU-U.S. DPF. Η εταιρεία μας έχει επιβεβαιώσει στο Υπουργείο Εμπορίου των ΗΠΑ ότι τηρεί τις Swiss-U.S. Data Privacy Framework Principles (Swiss-U.S. DPF Principles) όσον αφορά την επεξεργασία προσωπικών δεδομένων που λαμβάνει από την Ελβετία αναφερόμενη στο Swiss-U.S. DPF. Σε περίπτωση αντίθεσης μεταξύ των διατάξεων της πολιτικής απορρήτου μας και των EU-U.S. DPF Principles και/ή των Swiss-U.S. DPF Principles, οι Principles είναι αυτές που υπερισχύουν.

Για να μάθετε περισσότερα σχετικά με το Data Privacy Framework (DPF) πρόγραμμα και για να δείτε την πιστοποίησή μας, επισκεφθείτε τη διεύθυνση https://www.dataprivacyframework.gov/.

Οι άλλες αμερικανικές μονάδες ή θυγατρικές της εταιρείας μας που επίσης συμμορφώνονται με τις EU-U.S. DPF Principles, συμπεριλαμβανομένου του UK Extension to the EU-U.S. DPF και των Swiss-U.S. DPF Principles, εάν υπάρχουν, αναφέρονται στην πολιτική απορρήτου μας.

Σύμφωνα με το EU-U.S. DPF και το UK Extension to the EU-U.S. DPF καθώς και το Swiss-U.S. DPF, η εταιρεία μας δεσμεύεται να συνεργάζεται με τις ευρωπαϊκές αρχές προστασίας δεδομένων και το Information Commissioner's Office (ICO) του Ηνωμένου Βασιλείου καθώς και το Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) της Ελβετίας και να ακολουθεί τις συμβουλές τους σχετικά με άλυτες καταγγελίες για τον χειρισμό προσωπικών δεδομένων που λαμβάνουμε αναφερόμενοι στο EU-U.S. DPF και το UK Extension to the EU-U.S. DPF και το Swiss-U.S. DPF.

Ενημερώνουμε τα υποκείμενα των δεδομένων σχετικά με τις αρμόδιες ευρωπαϊκές αρχές προστασίας δεδομένων που είναι υπεύθυνες για την επεξεργασία καταγγελιών σχετικά με τον χειρισμό προσωπικών δεδομένων από τον οργανισμό μας στο πάνω μέρος αυτού του εγγράφου διαφάνειας και ότι παρέχουμε στα υποκείμενα των δεδομένων κατάλληλη και δωρεάν προσφυγή.

Ενημερώνουμε όλα τα υποκείμενα των δεδομένων ότι η εταιρεία μας υπόκειται στις ερευνητικές και εκτελεστικές εξουσίες της Federal Trade Commission (FTC).

Τα υποκείμενα των δεδομένων έχουν υπό ορισμένες προϋποθέσεις τη δυνατότητα να υποβληθούν σε δεσμευτική διαιτησία. Ο οργανισμός μας υποχρεούται να επιλύσει αξιώσεις και να τηρεί τις συνθήκες του Παραρτήματος I των DPF Principles, εάν το υποκείμενο των δεδομένων έχει ζητήσει δεσμευτική διαιτησία ενημερώνοντας τον οργανισμό μας και ακολουθώντας τις διαδικασίες και συνθήκες του Παραρτήματος I των Principles.

Ενημερώνουμε εδώ όλα τα υποκείμενα των δεδομένων σχετικά με την ευθύνη του οργανισμού μας σε περίπτωση διαβίβασης προσωπικών δεδομένων σε τρίτους.

Για ερωτήσεις των υποκειμένων των δεδομένων ή των αρχών προστασίας δεδομένων, έχουμε ορίσει τους τοπικούς εκπροσώπους που αναφέρονται στο πάνω μέρος αυτού του εγγράφου διαφάνειας.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

Σας προσφέρουμε τη δυνατότητα επιλογής (Opt-out), αν τα προσωπικά σας δεδομένα (i) διαβιβαστούν σε τρίτους ή (ii) χρησιμοποιηθούν για σκοπό που διαφέρει ουσιαστικά από τον/τους σκοπό/ούς για τον/τους οποίους αρχικά συλλέχθηκαν ή αργότερα εγκρίθηκαν από εσάς. Ο σαφής, ευδιάκριτος και εύκολα προσβάσιμος μηχανισμός για την άσκηση του δικαιώματός σας επιλογής είναι η επικοινωνία μέσω ηλεκτρονικού ταχυδρομείου με τον υπεύθυνο προστασίας δεδομένων (DSB). Δεν έχετε δικαίωμα επιλογής και δεν είμαστε υποχρεωμένοι, εάν τα δεδομένα διαβιβαστούν σε τρίτο που ενεργεί ως εντολέας ή επεξεργαστής για λογαριασμό μας και σύμφωνα με τις οδηγίες μας. Ωστόσο, πάντα συνάπτουμε σύμβαση με τέτοιον εντολέα ή επεξεργαστή.

Για ευαίσθητα δεδομένα (π.χ. προσωπικά δεδομένα που περιέχουν πληροφορίες για την υγεία, τη φυλετική ή εθνική καταγωγή, πολιτικές απόψεις, θρησκευτικές ή φιλοσοφικές πεποιθήσεις, μέλη σε συνδικαλιστική οργάνωση ή δεδομένα για τη σεξουαλική ζωή του ατόμου), λαμβάνουμε τη ρητή συγκατάθεσή σας (Opt-in) αν αυτά τα δεδομένα (i) διαβιβαστούν σε τρίτους ή (ii) χρησιμοποιηθούν για σκοπό διαφορετικό από αυτόν για τον οποίο αρχικά συλλέχθηκαν ή για τον οποίο αργότερα δώσατε τη συγκατάθεσή σας επιλέγοντας Opt-in. Επιπλέον, αντιμετωπίζουμε όλα τα προσωπικά δεδομένα που λαμβάνουμε από τρίτους ως ευαίσθητα, αν ο τρίτος τα έχει χαρακτηρίσει και αντιμετωπίσει ως ευαίσθητα.

Σας ενημερώνουμε εδώ σχετικά με την ανάγκη αποκάλυψης προσωπικών δεδομένων ως απάντηση σε νόμιμα αιτήματα αρχών, συμπεριλαμβανομένης της συμμόρφωσης με τις απαιτήσεις εθνικής ασφάλειας ή επιβολής του νόμου.

Κατά τη διαβίβαση προσωπικών δεδομένων σε τρίτο που ενεργεί ως υπεύθυνος επεξεργασίας, συμμορφωνόμαστε με τις Principals της ειδοποίησης και της επιλογής. Επιπλέον, συνάπτουμε σύμβαση με τον τρίτο που είναι υπεύθυνος για την επεξεργασία, η οποία προβλέπει ότι αυτά τα δεδομένα μπορούν να υποβληθούν σε επεξεργασία μόνο για περιορισμένους και καθορισμένους σκοπούς σύμφωνα με τη συγκατάθεση που έχετε δώσει και ότι ο παραλήπτης παρέχει το ίδιο επίπεδο προστασίας όπως οι Principals του DPF και μας ειδοποιεί αν διαπιστώσει ότι δεν μπορεί πλέον να εκπληρώσει αυτή τη δέσμευση. Η σύμβαση προβλέπει ότι ο τρίτος που είναι υπεύθυνος επεξεργασίας θα σταματήσει την επεξεργασία ή θα λάβει άλλα κατάλληλα και κατάλληλα μέτρα για την παροχή λύσης, εάν διαπιστωθεί ότι δεν μπορεί να εκπληρώσει τη δέσμευσή του.

Κατά τη διαβίβαση προσωπικών δεδομένων σε τρίτο που ενεργεί ως εντολέας ή επεξεργαστής, (i) διαβιβάζουμε αυτά τα δεδομένα μόνο για περιορισμένους και καθορισμένους σκοπούς, (ii) διασφαλίζουμε ότι ο εντολέας ή επεξεργαστής δεσμεύεται να παρέχει τουλάχιστον το ίδιο επίπεδο προστασίας δεδομένων όπως απαιτούν οι DPF Principles, (iii) λαμβάνουμε κατάλληλα και κατάλληλα μέτρα για να διασφαλίσουμε ότι ο εντολέας ή επεξεργαστής επεξεργάζεται τα προσωπικά δεδομένα που διαβιβάζονται με τρόπο που συμφωνεί με τις δεσμεύσεις μας σύμφωνα με τις DPF Principles, (iv) απαιτούμε από τον εντολέα ή επεξεργαστή να μας ειδοποιήσει αν διαπιστώσει ότι δεν μπορεί να εκπληρώσει τη δέσμευσή του να παρέχει το ίδιο επίπεδο προστασίας όπως απαιτούν οι DPF Principles, (v) λαμβάνουμε κατάλληλα και κατάλληλα μέτρα για να σταματήσουμε την ανεπίτρεπτη επεξεργασία και να παρέχουμε λύση σε περίπτωση που ληφθεί ειδοποίηση, συμπεριλαμβανομένης της ειδοποίησης υπό (iv), και (vi) παρέχουμε


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

στο DPF Department, κατόπιν αιτήματος, μια περίληψη ή ένα αντιπροσωπευτικό αντίγραφο των σχετικών διατάξεων προστασίας δεδομένων της σύμβασής μας με αυτόν τον εντολέα.

Σύμφωνα με το EU-U.S. DPF και/ή το UK Extension to the EU-U.S. DPF και/ή το Swiss-U.S. DPF, η εταιρεία μας δεσμεύεται να συνεργάζεται με το σώμα που έχει συσταθεί από τις ευρωπαϊκές αρχές προστασίας δεδομένων και το Information Commissioner's Office (ICO) του Ηνωμένου Βασιλείου ή το Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) της Ελβετίας και να ακολουθεί τις συμβουλές τους σχετικά με άλυτες καταγγελίες για τον χειρισμό προσωπικών δεδομένων που λαμβάνουμε αναφερόμενοι στο EU-U.S. DPF και την UK Extension to the EU-U.S. DPF και το Swiss-U.S. DPF στο πλαίσιο της εργασιακής σχέσης.

Όλα τα υποκείμενα των δεδομένων που βρίσκονται προσωρινά στην Ευρωπαϊκή Ένωση (ΕΕ), στον Ευρωπαϊκό Οικονομικό Χώρο (ΕΟΧ) ή στο Ηνωμένο Βασίλειο ή που έχουν την κατοικία ή τη συνήθη διαμονή τους εκεί, δικαιούνται τα δικαιώματα και τα δικαιώματα των υποκειμένων των δεδομένων που δημοσιεύονται στο Έγγραφο Διαφάνειας, τα οποία απορρέουν επίσης από τα άρθρα 15 έως 22 του ΓΚΠΔ, συμπεριλαμβανομένου του δικαιώματος πρόσβασης σε δεδομένα προσωπικού χαρακτήρα. Έχουμε καταστήσει τις πληροφορίες αυτές διαθέσιμες σε όλες τις γλώσσες της ΕΕ και του ΕΟΧ. Η έκδοση στην αγγλική γλώσσα ισχύει για το Ηνωμένο Βασίλειο.

Όλα τα υποκείμενα των δεδομένων που διαμένουν προσωρινά στην Ελβετία ή έχουν την κατοικία τους ή τη συνήθη διαμονή τους εκεί, δικαιούνται τα δικαιώματα και τα δικαιώματα των υποκειμένων των δεδομένων σύμφωνα με τον ελβετικό νόμο περί προστασίας δεδομένων (DPA) και τον ελβετικό κανονισμό περί προστασίας δεδομένων (DPR), τα οποία δημοσιεύονται στο έγγραφο διαφάνειας, συμπεριλαμβανομένου του δικαιώματος πρόσβασης σε δεδομένα προσωπικού χαρακτήρα. Έχουμε παράσχει αυτές τις πληροφορίες στις τρεις επίσημες γλώσσες της Ελβετίας (γερμανικά, ιταλικά και γαλλικά).


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

# POLISH: Informacja o przetwarzaniu danych osobowych (Artykuł 13 i 14 RODO)

Szanowni Państwo,

Dane osobowe każdej osoby fizycznej pozostającej w relacji związanej z umową, która została lub będzie zawarta lub w innej relacji z naszą firmą, zasługują na szczególną ochronę. Naszym celem jest utrzymanie wysokiego poziomu ochrony danych. Dlatego regularnie rozwijamy nasze koncepcje ochrony i bezpieczeństwa danych.

Oczywiście przestrzegamy ustawowych przepisów dotyczących ochrony danych. Zgodnie z art. 13 i 14 RODO firmy gromadząc dane osobowe muszą spełniać określone wymogi informacyjne. Niniejszy dokument spełnia te obowiązki.

Słownictwo stosowane w przepisach prawnych jest skomplikowane. Niestety, przy opracowywaniu tego dokumentu nie można było uniknąć stosowania terminów prawnych. Dlatego pragniemy zwrócić uwagę, że zawsze mogą Państwo skontaktować się z naszym inspektorem ochrony danych w przypadku jakichkolwiek pytań dotyczących niniejszego dokumentu, używanych terminów lub sformułowań.

## I. Zgodność z wymogami informacyjnymi w przypadku zbierania danych osobowych od osoby, której dane dotyczą (art. 13 RODO)

### A. Tożsamość i dane kontaktowe administratora (art. 13 ust. 1 lit. a) RODO)

Patrz wyżej

### B. Dane kontaktowe inspektora ochrony danych (art. 13 ust. 1 lit. b) RODO)

Patrz wyżej

### C. Cele przetwarzania danych osobowych oraz podstawa prawna przetwarzania (art. 13 ust. 1 lit. c RODO)

Celem przetwarzania danych osobowych jest obsługa wszystkich operacji dotyczących administratora, klientów, potencjalnych klientów, partnerów biznesowych lub innych relacji związanych z umową już zawartą lub zawieraną między wymienionymi grupami (w najszerszym tego słowa znaczeniu) lub prawnych obowiązków administratora danych.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

Art. 6 ust. 1 lit. a RODO służy jako podstawa prawna przeprowadzania operacji przetwarzania, dla których uzyskujemy zgodę na konkretny cel przetwarzania. Jeżeli przetwarzanie danych osobowych jest konieczne do wykonania umowy, której stroną jest osoba, której dane dotyczą, jak ma to miejsce na przykład w przypadku, gdy operacje przetwarzania są niezbędne do dostarczania towarów lub świadczenia jakiejkolwiek innej usługi, przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. b RODO. To samo dotyczy operacji przetwarzania, które są niezbędne do realizacji czynności przed zawarciem umowy, na przykład w przypadku zapytań dotyczących naszych produktów lub usług. Jeśli nasza firma podlega prawnemu obowiązkowi, zgodnie z którym wymagane jest przetwarzanie danych osobowych, np. w celu wypełnienia obowiązków podatkowych, podstawą przetwarzania jest art. 6 ust. 1 lit. c RODO.

W rzadkich przypadkach przetwarzanie danych osobowych może być konieczne do ochrony żywotnych interesów osoby, których dane dotyczą, lub innej osoby fizycznej. Taka sytuacja wystąpiłaby na przykład wtedy, gdyby odwiedzający naszą firmę został ranny, a jego imię i nazwisko, wiek, dane dotyczące ubezpieczenia zdrowotnego lub inne istotne informacje musiałyby zostać przekazane lekarzowi, szpitalowi lub innej stronie trzeciej. Wówczas podstawą przetwarzania byłby art. 6 ust. 1 lit. d RODO.

Jeżeli przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi, podstawą prawną jest art. 6 ust. 1 lit. e RODO.

Podstawą operacji przetwarzania mógłby również być art. 6 ust. 1 lit. f RODO. Tę podstawę prawną stosuje się do operacji przetwarzania nieuwzględnionych w powyżej wymienionych podstawach prawnych, jeżeli przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez naszą firmę lub stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osób, których dane dotyczą, wymagające ochrony danych osobowych. Takie operacje przetwarzania są szczególnie dopuszczalne, ponieważ zostały wyraźnie wymienione przez europejskiego prawodawcę, który uznał, że można założyć uzasadniony interes, jeżeli osoba, której dane dotyczą, jest klientem administratora (ust. 47 zdanie 2 preambuły RODO).

## D. Uzasadnione interesy administratora lub strony trzeciej, jeżeli podstawą przetwarzania jest art. 6 ust. 1 lit. f RODO, (art. 13 ust. 1 lit. d) RODO)

Jeżeli podstawą przetwarzania danych osobowych jest art. 6 ust. 1 lit. f RODO, naszym uzasadnionym interesem jest prowadzenie naszej działalności na rzecz dobra wszystkich naszych pracowników i udziałowców.

## E. Kategorie odbiorców danych osobowych (art. 13 ust. 1 lit. e RODO)


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

Władze publiczne

Organy zewnętrzne

Dalsze organy zewnętrzne

Przetwarzanie wewnętrzne

Przetwarzanie wewnątrzgrupowe

Inne organy

Lista naszych podmiotów przetwarzających i odbiorców danych w państwach trzecich oraz, w stosownych przypadkach, organizacji międzynarodowych jest publikowana na naszej stronie internetowej lub można ją bezpłatnie uzyskać od nas. Aby poprosić o taką listę, należy skontaktować się z naszym inspektorem ochrony danych.

## F. Odbiorcy w państwie trzecim, jak również odpowiednie lub właściwe zabezpieczenia oraz możliwości uzyskania kopii danych lub miejsca udostępnienia danych (art. 13 ust. 1 lit. f, art. 46 ust. 1, art. 46 ust. 2 lit. c RODO)

Wszystkie firmy i oddziały należące do naszej grupy (zwane dalej „spółkami grupy"), które mają swoje miejsce prowadzenia działalności lub biuro w państwie trzecim, mogą być odbiorcami danych osobowych.

Na mocy art. 46 ust. 1 RODO administrator lub podmiot przetwarzający mogą przekazać dane osobowe do państwa trzeciego wyłącznie, gdy zapewnią odpowiednie zabezpieczenia, i pod warunkiem, że obowiązują egzekwowalne prawa osób, których dane dotyczą, i skuteczne środki ochrony prawnej. Odpowiednie zabezpieczenia można zapewnić bez konieczności uzyskania specjalnego zezwolenia organu nadzorczego za pomocą standardowych klauzul umownych (art. 46 ust. 2 lit. c RODO).

Przed pierwszym przekazaniem danych osobowych uzgadniane są z wszystkimi odbiorcami z państw trzecich standardowe klauzule umowne Unii Europejskiej. W związku z tym zapewniono, że zagwarantowane zostaną odpowiednie zabezpieczenia, egzekwowalne prawa osób, których dane dotyczą, oraz skuteczne środki prawne dla osób, których dane dotyczą, wynikające ze standardowych klauzul umownych UE. Każda osoba, której dane dotyczą, może uzyskać kopię standardowych klauzul umownych od naszego inspektora ochrony danych. Standardowe klauzule umowne są również dostępne w Dzienniku Urzędowym Unii Europejskiej.

Artykuł 45 ust. 3 ogólnego rozporządzenia o ochronie danych (RODO) przyznaje Komisji Europejskiej prawo do podjęcia decyzji, w drodze aktu wykonawczego, że państwo spoza UE zapewnia odpowiedni poziom ochrony. Oznacza to poziom ochrony danych osobowych, który jest zasadniczo równoważny poziomowi ochrony w UE. Skutkiem decyzji stwierdzających odpowiedni poziom ochrony jest to, że dane


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

osobowe mogą swobodnie przepływać z UE (oraz Norwegii, Liechtensteinu i Islandii) do państwa trzeciego bez dalszych przeszkód. Podobne zasady obowiązują w Wielkiej Brytanii, Szwajcarii i niektórych innych krajach.

W przypadku, gdy Komisja Europejska lub rząd innego kraju zdecyduje, że kraj trzeci zapewnia odpowiedni poziom ochrony, a obowiązujące ramy (np. EU-U.S. Data Privacy Framework, Swiss-U.S. Data Privacy Framework, UK Extension to the EU-U.S. Data Privacy Framework), wszystkie transfery dokonywane przez nas do członków takich ram (np. podmiotów samocertyfikowanych) opierają się wyłącznie na członkostwie tych podmiotów w odpowiednich ramach. W przypadku, gdy my lub jeden z podmiotów należących do naszej grupy jest członkiem takich ram, wszystkie transfery do nas lub naszego podmiotu należącego do grupy opierają się wyłącznie na członkostwie podmiotu w takich ramach.

Każda osoba, której dane dotyczą, może uzyskać od nas kopię tych ram. Ponadto ramy są również dostępne w Dzienniku Urzędowym Unii Europejskiej lub w opublikowanych materiałach prawnych lub na stronach internetowych organów nadzorczych lub innych właściwych organów lub instytucji.

## G. Okres, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalania tego okresu (art. 13 ust. 2 lit. a RODO)

Kryteriami stosowanymi do określenia okresu przechowywania danych osobowych są odpowiednie ustawowe okresy zatrzymywania. Po upływie tego okresu odpowiednie dane są rutynowo usuwane, o ile nie są już konieczne do wypełnienia umowy lub rozpoczęcia umowy.

Jeśli nie ma ustawowego okresu przechowywania, kryterium jest umowny lub wewnętrzny okres przechowywania.

## H. Informacje o prawie do żądania od administratora dostępu do danych osobowych osoby, której dane dotyczą, ich sprostowania, usunięcia lub ograniczenia przetwarzania lub o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych (art. 13 ust. 2 lit. b RODO)

Wszystkie osoby, których dane dotyczą, mają następujące prawa:

***Prawo dostępu***

Każda osoba, której dane dotyczą, ma prawo dostępu do danych osobowych, które jej dotyczą. Prawo dostępu obejmuje wszystkie przetwarzane przez nas dane. Istnieje możliwość łatwego wykonywania tego prawa w rozsądnych odstępach czasu, by mieć świadomość przetwarzania i móc zweryfikować zgodność przetwarzania z prawem (ust. 63 preambuły RODO). To prawo wynika z art. 15


© All rights reserved by Heiko Maniero.

RODO. Osoba, której dane dotyczą, może skontaktować się z naszym inspektorem ochrony danych, aby skorzystać z prawa dostępu.

***Prawo do sprostowania***

Zgodnie z art. 16 zdanie 1 RODO osoba, której dane dotyczą, ma prawo żądania od administratora niezwłocznego sprostowania dotyczących jej danych osobowych, które są nieprawidłowe. Ponadto zgodnie z art. 16 zdanie 2 RODO osoba, której dane dotyczą, ma prawo, biorąc pod uwagę cele przetwarzania, żądania uzupełnienia niekompletnych danych osobowych, w tym poprzez przedstawienie dodatkowego oświadczenia. Osoba, której dane dotyczą, może skontaktować się z naszym inspektorem ochrony danych, aby skorzystać z prawa do sprostowania.

***Prawo do usunięcia danych (prawo do bycia zapomnianym)***

Ponadto osoby, których dane dotyczą, mają prawo do usunięcia danych i do bycia zapomnianym na mocy art. 17 RODO. Z tego prawa można również skorzystać, kontaktując się z naszym inspektorem ochrony danych. W tym miejscu chcielibyśmy jednak zwrócić uwagę, że to prawo nie ma zastosowania, o ile przetwarzanie jest konieczne do wypełnienia obowiązku prawnego, któremu podlega nasza firma (art. 17 ust. 3 lit. b RODO). Oznacza to, że możemy zaakceptować wniosek o usunięcie danych tylko po upływie ustawowego okresu zatrzymywania.

***Prawo do ograniczenia przetwarzania danych***

Zgodnie z art. 18 RODO osoba, której dane dotyczą, jest uprawniona do ograniczenia przetwarzania danych. Można domagać się ograniczenia przetwarzania, jeżeli spełniony jest jeden z warunków określonych w art. 18 ust. 1 lit. a-d RODO. Osoba, której dane dotyczą, może skontaktować się z naszym inspektorem ochrony danych, aby skorzystać z prawa ograniczenia przetwarzania..

***Prawo do sprzeciwu***

Ponadto art. 21 RODO gwarantuje prawo do sprzeciwu. Osoba, której dane dotyczą, może skontaktować się z naszym inspektorem ochrony danych, aby skorzystać z prawa do sprzeciwu.

***Prawo do przenoszenia danych***

Art. Art. 20 RODO gwarantuje osobie, której dane dotyczą, prawo do przenoszenia danych. Zgodnie z tym postanowieniem, osoba, której dane dotyczą, ma prawo na warunkach określonych w art. 20 ust. 1 lit. a i b RODO otrzymać w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego dane osobowe jej dotyczące, które dostarczyła administratorowi, oraz ma prawo przesłać te dane osobowe innemu administratorowi bez przeszkód ze strony administratora, któremu dostarczono te dane osobowe. Osoba, której dane dotyczą, może skontaktować się z naszym inspektorem ochrony danych, aby skorzystać z prawa do przenoszenia danych.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## I. Informacje o prawie do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem, jeśli podstawą przetwarzania jest art. 6 ust. 1 lit. a RODO lub art. 9 ust. 2 lit. a RODO (art. 13 ust. 2 lit. c) RODO)

Jeśli podstawą przetwarzania danych osobowych jest art. 6 ust. 1 lit. a RODO, jak ma to miejsce w sytuacji, gdy osoba, której dane dotyczą wyraziła zgodę na przetwarzanie danych osobowych dla jednego lub więcej konkretnych celów, lub art. 9 ust. 2 lit. a RODO, który reguluje wyraźną zgodę na przetwarzanie szczególnych kategorii danych osobowych, osoba, której dane dotyczą, zgodnie z art. 7 ust. 3 zdanie 1 RODO, ma prawo do wycofania swojej zgody w dowolnym czasie.

Wycofanie zgody nie wpływa na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej wycofaniem (art. 7 ust. 3 zdanie 2 RODO). Wycofanie zgody musi być równie łatwe jak jej wyrażenie (art. 7 ust. 3 zdanie 4 RODO. W związku z powyższym wycofanie zgody może zawsze nastąpić w taki sam sposób, jak udzielono zgody lub w jakikolwiek inny sposób, który jest uważany przez osobę, której dane dotyczą, za prostszy. W dzisiejszym społeczeństwie informacyjnym najprawdopodobniej najprostszym sposobem na wycofanie zgody jest zwykła wiadomość e-mail. Jeżeli osoba, której dane dotyczą, pragnie wycofać udzieloną nam zgodę, wystarczy zwykła wiadomość e-mail wysłana do naszego inspektora ochrony danych. Alternatywnie osoba, której dane dotyczą, może wybrać inny sposób powiadomienia nas o wycofaniu swojej zgody.

## J. Informacje o prawie wniesienia skargi do organu nadzorczego (art. 13 ust. 2 lit. d, art. 77 ust. 1 RODO)

Jako administrator jesteśmy zobowiązani powiadomić osobę, której dane dotyczą, o prawie do wniesienia skargi do organu nadzorczego (art. 13 ust. 2. lit. d RODO). Prawo do wniesienia skargi do organu nadzorczego reguluje art. 77 ust. 1 RODO. Zgodnie z jego treścią, bez uszczerbku dla innych administracyjnych lub środków ochrony prawnej przed sądem każda osoba, której dane dotyczą, ma prawo wnieść skargę do organu nadzorczego, w szczególności w państwie członkowskim swojego zwykłego pobytu, swojego miejsca pracy lub miejsca popełnienia domniemanego naruszenia, jeżeli sądzi, że przetwarzanie danych osobowych jej dotyczące narusza rozporządzenie ogólne rozporządzenie o ochronie danych. Prawo do wniesienia skargi do organu nadzorczego zostało ograniczone prawem Unii w taki sposób, że może ono być wykonywane tylko przed jednym organem nadzorującym (ust. 141 zdanie 1 preambuły RODO). Ta reguła ma na celu uniknięcie podwójnych skarg niniejszej samej osoby, której dane dotyczą, w niniejszej samej sprawie. Jeżeli osoba, której dane dotyczą, chce złożyć na nas skargę, prosimy o kontakt tylko z jednym organem nadzorczym.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## K. Udostępnianie danych osobowych jako wymóg ustawowy lub umowny; warunek zawarcia umowy; obowiązek osoby, której dane dotyczą, do podania danych osobowych; ewentualne konsekwencje niepodania danych (art. art. 13 ust. 2 lit. e RODO)

Wyjaśniamy, że udostępnianie danych osobowych jest częściowo wymagane przez prawo (np. przepisy podatkowe) lub może wynikać z postanowień umownych (np. informacje o partnerze umownym).

Czasami może być konieczne do zawarcia umowy podanie przez osobę, której dane dotyczą, danych osobowych, które następnie muszą zostać przez nas przetwarzane. Osoba, której dane dotyczą jest na przykład zobowiązana do przekazania nam danych osobowych podczas zawierania z nami umowy. Konsekwencją niedostarczenia danych osobowych byłby brak możliwości zawarcia umowy z osobą, której dane dotyczą.

Zanim dane osobowe zostaną przekazane przez osobę, której dane dotyczą, osoba ta musi skontaktować się z naszym inspektorem ochrony danych. Nasz inspektor ochrony danych wyjaśnia osobie, której dane dotyczą, czy podanie danych osobowych jest wymagane przez prawo lub umowę lub jest konieczne do zawarcia umowy, czy istnieje obowiązek dostarczenia danych osobowych i konsekwencje niedostarczenia danych osobowych.

## L. Informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, o którym mowa w art. 22 ust. 1 i 4 RODO, oraz – przynajmniej w tych przypadkach – istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą (art. 13 ust. 2 lit. f RODO)

Jako odpowiedzialna firma zazwyczaj nie stosujemy zautomatyzowanego podejmowania decyzji ani profilowania. Jeśli w wyjątkowych przypadkach przeprowadzimy zautomatyzowane podejmowanie decyzji lub profilowanie, poinformujemy o tym osobę, której dane dotyczą, osobno lub za pośrednictwem podsekcji w naszej polityce prywatności (na naszej stronie internetowej). W takim przypadku obowiązują następujące zasady:

Zautomatyzowane podejmowanie decyzji - w tym profilowanie - może mieć miejsce, jeżeli (1) jest to niezbędne do zawarcia lub wykonania umowy między osobą, której dane dotyczą, a nami lub (2) jest to dozwolone prawem Unii lub prawem państwa członkowskiego, któremu podlegamy i które przewiduje również odpowiednie środki ochrony praw i wolności oraz prawnie uzasadnionych interesów osoby, której dane dotyczą; lub (3) odbywa się to na podstawie wyraźnej zgody osoby, której dane dotyczą.

W przypadkach, o których mowa w art. 22 ust. 2 lit. a) i c) RODO, wdrażamy odpowiednie środki w celu ochrony praw i wolności oraz uzasadnionych interesów osoby, której dane dotyczą. W takich


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

przypadkach użytkownik ma prawo do uzyskania interwencji ludzkiej ze strony administratora, wyrażenia swojego punktu widzenia i zakwestionowania decyzji.

Istotne informacje na temat zastosowanej logiki, a także znaczenia i przewidywanych konsekwencji takiego przetwarzania dla osoby, której dane dotyczą, są określone w naszej polityce prywatności.

## II. Zgodność z wymogami informacyjnymi w przypadku niezbierania danych osobowych od osoby, której dane dotyczą (art. 14 RODO)

### A. Tożsamość i dane kontaktowe administratora (art. 14 ust. 1 lit. a) RODO)

Patrz wyżej

### B. Dane kontaktowe inspektora ochrony danych (art. 14 ust. 1 lit. b) RODO)

Patrz wyżej

### C. Cele przetwarzania danych osobowych oraz podstawa prawna przetwarzania (art. 14 ust. 1 lit. c RODO)

Celem przetwarzania danych osobowych jest obsługa wszystkich operacji dotyczących administratora, klientów, potencjalnych klientów, partnerów biznesowych lub innych relacji związanych z umową już zawartą lub zawieraną między wymienionymi grupami (w najszerszym tego słowa znaczeniu) lub prawnych obowiązków administratora danych.

Jeżeli przetwarzanie danych osobowych jest konieczne do wykonania umowy, której stroną jest osoba, której dane dotyczą, jak ma to miejsce na przykład w przypadku, gdy operacje przetwarzania są niezbędne do dostarczania towarów lub świadczenia jakiejkolwiek innej usługi, przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. b RODO. To samo dotyczy operacji przetwarzania, które są niezbędne do realizacji czynności przed zawarciem umowy, na przykład w przypadku zapytań dotyczących naszych produktów lub usług. Jeśli nasza firma podlega prawnemu obowiązkowi, zgodnie z którym wymagane jest przetwarzanie danych osobowych, np. w celu wypełnienia obowiązków podatkowych, podstawą przetwarzania jest art. 6 ust. 1 lit. c RODO.

W rzadkich przypadkach przetwarzanie danych osobowych może być konieczne do ochrony żywotnych interesów osoby, których dane dotyczą, lub innej osoby fizycznej. Taka sytuacja wystąpiłaby na przykład wtedy, gdyby odwiedzający naszą firmę został ranny, a jego imię i nazwisko, wiek, dane dotyczące ubezpieczenia zdrowotnego lub inne istotne informacje musiałyby zostać przekazane lekarzowi, szpitalowi lub innej stronie trzeciej. Wówczas podstawą przetwarzania byłby art. 6 ust. 1 lit. d RODO.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

Jeżeli przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi, podstawą prawną jest art. 6 ust. 1 lit. e RODO.

Podstawą operacji przetwarzania mógłby również być art. 6 ust. 1 lit. f RODO. Tę podstawę prawną stosuje się do operacji przetwarzania nieuwzględnionych w powyżej wymienionych podstawach prawnych, jeżeli przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez naszą firmę lub stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osób, których dane dotyczą, wymagające ochrony danych osobowych. Takie operacje przetwarzania są szczególnie dopuszczalne, ponieważ zostały wyraźnie wymienione przez europejskiego prawodawcę, który uznał, że można założyć prawnie uzasadniony interes, jeżeli osoba, której dane dotyczą, jest klientem administratora (ust. 47 zdanie 2 preambuły RODO).

## D. Kategorie odnośnych danych osobowych (art. 14 ust. 1 lit. d RODO)

Dane klienta

Dane potencjalnych klientów

Dane pracowników

Dane dostawców

## E. Kategorie odbiorców danych (art. 14 ust. 1 lit. e RODO)

Władze publiczne

Organy zewnętrzne

Dalsze organy zewnętrzne

Przetwarzanie wewnętrzne

Przetwarzanie wewnątrzgrupowe

Inne organy

Lista naszych podmiotów przetwarzających i odbiorców danych w państwach trzecich oraz, w stosownych przypadkach, organizacji międzynarodowych jest publikowana na naszej stronie


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

internetowej lub można ją bezpłatnie uzyskać od nas. Aby poprosić o taką listę, należy skontaktować się z naszym inspektorem ochrony danych.

## F. Odbiorcy w państwie trzecim, jak również odpowiednie lub właściwe zabezpieczenia oraz możliwości uzyskania kopii danych lub miejsca udostępnienia danych (art. 14 ust. 1 lit. f, art. 46 ust. 1, art. 46 ust. 2 lit. c RODO)

Wszystkie firmy i oddziały należące do naszej grupy (zwane dalej „spółkami grupy"), które mają swoje miejsce prowadzenia działalności lub biuro w państwie trzecim, mogą być odbiorcami danych osobowych.

Na mocy art. 46 ust. 1 RODO administrator lub podmiot przetwarzający mogą przekazać dane osobowe do państwa trzeciego wyłącznie, gdy zapewnią odpowiednie zabezpieczenia, i pod warunkiem, że obowiązują egzekwowalne prawa osób, których dane dotyczą, i skuteczne środki ochrony prawnej. Odpowiednie zabezpieczenia można zapewnić bez konieczności uzyskania specjalnego zezwolenia organu nadzorczego za pomocą standardowych klauzul umownych (art. 46 ust. 2 lit. c RODO).

Przed pierwszym przekazaniem danych osobowych uzgadniane są z wszystkimi odbiorcami z państw trzecich standardowe klauzule umowne Unii Europejskiej. W związku z tym zapewniono, że zagwarantowane zostaną odpowiednie zabezpieczenia, egzekwowalne prawa osób, których dane dotyczą, oraz skuteczne środki prawne dla osób, których dane dotyczą, wynikające ze standardowych klauzul umownych UE. Każda osoba, której dane dotyczą, może uzyskać kopię standardowych klauzul umownych od naszego inspektora ochrony danych. Standardowe klauzule umowne są również dostępne w Dzienniku Urzędowym Unii Europejskiej.

Artykuł 45 ust. 3 ogólnego rozporządzenia o ochronie danych (RODO) przyznaje Komisji Europejskiej prawo do podjęcia decyzji, w drodze aktu wykonawczego, że państwo spoza UE zapewnia odpowiedni poziom ochrony. Oznacza to poziom ochrony danych osobowych, który jest zasadniczo równoważny poziomowi ochrony w UE. Skutkiem decyzji stwierdzających odpowiedni poziom ochrony jest to, że dane osobowe mogą swobodnie przepływać z UE (oraz Norwegii, Liechtensteinu i Islandii) do państwa trzeciego bez dalszych przeszkód. Podobne zasady obowiązują w Wielkiej Brytanii, Szwajcarii i niektórych innych krajach.

W przypadku, gdy Komisja Europejska lub rząd innego kraju zdecyduje, że kraj trzeci zapewnia odpowiedni poziom ochrony, a obowiązujące ramy (np. EU-U.S. Data Privacy Framework, Swiss-U.S. Data Privacy Framework, UK Extension to the EU-U.S. Data Privacy Framework), wszystkie transfery dokonywane przez nas do członków takich ram (np. podmiotów samocertyfikowanych) opierają się wyłącznie na członkostwie tych podmiotów w odpowiednich ramach. W przypadku, gdy my lub jeden z podmiotów należących do naszej grupy jest członkiem takich ram, wszystkie transfery do nas lub naszego podmiotu należącego do grupy opierają się wyłącznie na członkostwie podmiotu w takich ramach.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

Każda osoba, której dane dotyczą, może uzyskać od nas kopię tych ram. Ponadto ramy są również dostępne w Dzienniku Urzędowym Unii Europejskiej lub w opublikowanych materiałach prawnych lub na stronach internetowych organów nadzorczych lub innych właściwych organów lub instytucji.

## G. Okres, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalania tego okresu (art. 14 ust. 2 lit. a RODO)

Kryteriami stosowanymi do określenia okresu przechowywania danych osobowych są odpowiednie ustawowe okresy zatrzymywania. Po upływie tego okresu odpowiednie dane są rutynowo usuwane, o ile nie są już konieczne do wypełnienia umowy lub rozpoczęcia umowy.

Jeśli nie ma ustawowego okresu przechowywania, kryterium jest umowny lub wewnętrzny okres przechowywania.

## H. Powiadomienie o prawnie uzasadnionych interesach realizowanych przez administratora lub przez stronę trzecią, jeżeli podstawą przetwarzania jest art. 6 ust. 1 lit. f RODO (art. 14 ust. 2. b RODO)

Zgodnie z art. 6 ust. 1 lit. f RODO przetwarzanie jest zgodne z prawem tylko wtedy, gdy jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osób, których dane dotyczą, wymagające ochrony danych osobowych. Zgodnie z ust. 47 zdanie 2 preambuły RODO uzasadniony interes może istnieć wtedy, gdy występuje odpowiedni i właściwy związek między osobą, której dane dotyczą, a administratorem, np. w sytuacjach, w których osoba, której dane dotyczą, jest klientem administratora. We wszystkich przypadkach, w których nasza firma przetwarza dane na podstawie art. 6 ust. 1 lit. f RODO, naszym uzasadnionym interesem jest prowadzenie naszej działalności na rzecz dobra wszystkich naszych pracowników i udziałowców.

## I. Informacje o prawie do żądania od administratora dostępu do danych osobowych dotyczących osoby, której dane dotyczą, ich sprostowania, usunięcia lub ograniczenia przetwarzania oraz o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych (art. 14 ust. 2 lit. c RODO)

Wszystkie osoby, których dane dotyczą, mają następujące prawa:

***Prawo dostępu***

Każda osoba, której dane dotyczą, ma prawo dostępu do danych osobowych, które jej dotyczą. Prawo dostępu obejmuje wszystkie przetwarzane przez nas dane. Istnieje możliwość łatwego


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

wykonywania tego prawa w rozsądnych odstępach czasu, by mieć świadomość przetwarzania i móc zweryfikować zgodność przetwarzania z prawem (ust. 63 preambuły RODO). To prawo wynika z art. 15 RODO. Osoba, której dane dotyczą, może skontaktować się z naszym inspektorem ochrony danych, aby skorzystać z prawa dostępu.

***Prawo do sprostowania***

Zgodnie z art. 16 zdanie 1 RODO osoba, której dane dotyczą, ma prawo żądania od administratora niezwłocznego sprostowania dotyczących jej danych osobowych, które są nieprawidłowe. Osoba, której dane dotyczą, może skontaktować się z naszym inspektorem ochrony danych, aby skorzystać z prawa do sprostowania. Zgodnie z art. 16 zdanie 1 RODO osoba, której dane dotyczą, ma prawo żądania od administratora niezwłocznego sprostowania dotyczących jej danych osobowych, które są nieprawidłowe.

***Prawo do usunięcia danych (prawo do bycia zapomnianym)***

Ponadto osoby, których dane dotyczą, mają prawo do usunięcia danych i do bycia zapomnianym na mocy art. 17 RODO. Z tego prawa można również skorzystać, kontaktując się z naszym inspektorem ochrony danych. W tym miejscu chcielibyśmy jednak zwrócić uwagę, że to prawo nie ma zastosowania, o ile przetwarzanie jest konieczne do wypełnienia obowiązku prawnego, któremu podlega nasza firma (art. 17 ust. 3 lit. b RODO). Oznacza to, że możemy zaakceptować wniosek o usunięcie danych tylko po upływie ustawowego okresu zatrzymywania.

***Prawo do ograniczenia przetwarzania danych***

Zgodnie z art. 18 RODO osoba, której dane dotyczą, jest uprawniona do ograniczenia przetwarzania danych. Można domagać się ograniczenia przetwarzania, jeżeli spełniony jest jeden z warunków określonych w art. 18 ust. 1 lit. a-d RODO. Można domagać się ograniczenia przetwarzania, jeżeli spełniony jest jeden z warunków określonych w art. 18 ust. 1 lit. a-d RODO.

***Prawo do sprzeciwu***

Ponadto art. 21 RODO gwarantuje prawo do sprzeciwu. Osoba, której dane dotyczą, może skontaktować się z naszym inspektorem ochrony danych, aby skorzystać z prawa do sprzeciwu.

***Prawo do przenoszenia danych***

Art. 20 RODO gwarantuje osobie, której dane dotyczą, prawo do przenoszenia danych. Zgodnie z tym postanowieniem, osoba, której dane dotyczą, ma prawo na warunkach określonych w art. 20 ust. 1 lit. a i b RODO otrzymać w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego dane osobowe jej dotyczące, które dostarczyła administratorowi, oraz ma prawo przesłać te dane osobowe innemu administratorowi bez przeszkód ze strony administratora, któremu dostarczono te dane osobowe. Osoba, której dane dotyczą, może skontaktować się z naszym inspektorem ochrony danych, aby skorzystać z prawa do przenoszenia danych.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## J. Informacje o prawie do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem, jeśli podstawą przetwarzania jest art. 6 ust. 1 lit. a lub art. 9 ust. 2 lit. a RODO (art. 14 ust. 2 lit. d RODO)

Jeśli podstawą przetwarzania danych osobowych jest art. 6 ust. 1 lit. a RODO, jak ma to miejsce w sytuacji, gdy osoba, której dane dotyczą wyraziła zgodę na przetwarzanie danych osobowych dla jednego lub więcej konkretnych celów, lub art. 9 ust. 2 lit. a RODO, który reguluje wyraźną zgodę na przetwarzanie szczególnych kategorii danych osobowych, osoba, której dane dotyczą, zgodnie z art. 7 ust. 3 zdanie 1 RODO, ma prawo do wycofania swojej zgody w dowolnym czasie.

Wycofanie zgody nie wpływa na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej wycofaniem (art. 7 ust. 3 zdanie 2 RODO). Wycofanie zgody musi być równie łatwe jak jej wyrażenie (art. 7 ust. 3 zdanie 4 RODO. W związku z powyższym wycofanie zgody może zawsze nastąpić w taki sam sposób, jak udzielono zgody lub w jakikolwiek inny sposób, który jest uważany przez osobę, której dane dotyczą, za prostszy. W dzisiejszym społeczeństwie informacyjnym najprawdopodobniej najprostszym sposobem na wycofanie zgody jest zwykła wiadomość e-mail. Jeżeli osoba, której dane dotyczą, pragnie wycofać udzieloną nam zgodę, wystarczy zwykła wiadomość e-mail wysłana do naszego inspektora ochrony danych. Alternatywnie osoba, której dane dotyczą, może wybrać inny sposób powiadomienia nas o wycofaniu swojej zgody.

## K. Informacje o prawie wniesienia skargi do organu nadzorczego (art. 14 ust. 2 lit. e, art. 77 ust. 1 RODO)

Jako administrator jesteśmy zobowiązani powiadomić osobę, której dane dotyczą, o prawie do wniesienia skargi do organu nadzorczego (art. 13 ust. 2. lit. d RODO). Prawo do wniesienia skargi do organu nadzorczego reguluje art. 77 ust. 1 RODO. Zgodnie z jego treścią, bez uszczerbku dla innych administracyjnych lub środków ochrony prawnej przed sądem każda osoba, której dane dotyczą, ma prawo wnieść skargę do organu nadzorczego, w szczególności w państwie członkowskim swojego zwykłego pobytu, swojego miejsca pracy lub miejsca popełnienia domniemanego naruszenia, jeżeli sądzi, że przetwarzanie danych osobowych jej dotyczące narusza rozporządzenie ogólne rozporządzenie o ochronie danych. Prawo do wniesienia skargi do organu nadzorczego zostało ograniczone prawem Unii w taki sposób, że może ono być wykonywane tylko przed jednym organem nadzorującym (ust. 141 zdanie 1 preambuły RODO). Ta reguła ma na celu uniknięcie podwójnych skarg niniejszej samej osoby, której dane dotyczą, w niniejszej samej sprawie. Jeżeli osoba, której dane dotyczą, chce złożyć na nas skargę, prosimy o kontakt tylko z jednym organem nadzorczym.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## L. Źródło pochodzenia danych osobowych, a gdy ma to zastosowanie – czy pochodzą one ze źródeł publicznie dostępnych (art. 14 ust. 2 lit. f RODO)

Zasadniczo dane osobowe są gromadzone bezpośrednio od osoby, której dane dotyczą lub we współpracy z organem (np. pobieranie danych z rejestru urzędowego). Inne dane osób, których dane dotyczą, pochodzą z przeniesień w ramach spółek grupy. W kontekście tych ogólnych informacji wskazanie z nazwy dokładnych źródeł pochodzenia danych osobowych jest niemożliwe lub wymagałoby nieproporcjonalnego wysiłku w rozumieniu art. 14 ust. 5 lit. b RODO. Co do zasady nie zbieramy danych osobowych z publicznie dostępnych źródeł.

Każda osoba, której dane dotyczą, może w każdej chwili skontaktować się z naszym inspektorem ochrony danych w celu uzyskania bardziej szczegółowych informacji na temat dokładnych źródeł danych osobowych, które jej dotyczą. Jeżeli osobie, której dane dotyczą, nie można podać pochodzenia danych osobowych, ponieważ korzystano z różnych źródeł, informacje należy przedstawić w sposób ogólny (ust. 61 zdanie 4 preambuły RODO).

## M. Informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, o którym mowa w art. 22 ust. 1 i 4, oraz – przynajmniej w tych przypadkach – istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą (art. 14 ust. 2 lit. g RODO)

Jako odpowiedzialna firma zazwyczaj nie stosujemy zautomatyzowanego podejmowania decyzji ani profilowania. Jeśli w wyjątkowych przypadkach przeprowadzimy zautomatyzowane podejmowanie decyzji lub profilowanie, poinformujemy o tym osobę, której dane dotyczą, osobno lub za pośrednictwem podsekcji w naszej polityce prywatności (na naszej stronie internetowej). W takim przypadku obowiązują następujące zasady:

Zautomatyzowane podejmowanie decyzji - w tym profilowanie - może mieć miejsce, jeżeli (1) jest to niezbędne do zawarcia lub wykonania umowy między osobą, której dane dotyczą, a nami lub (2) jest to dozwolone prawem Unii lub prawem państwa członkowskiego, któremu podlegamy i które przewiduje również odpowiednie środki ochrony praw i wolności oraz prawnie uzasadnionych interesów osoby, której dane dotyczą; lub (3) odbywa się to na podstawie wyraźnej zgody osoby, której dane dotyczą.

W przypadkach, o których mowa w art. 22 ust. 2 lit. a) i c) RODO, wdrażamy odpowiednie środki w celu ochrony praw i wolności oraz uzasadnionych interesów osoby, której dane dotyczą. W takich przypadkach użytkownik ma prawo do uzyskania interwencji ludzkiej ze strony administratora, wyrażenia swojego punktu widzenia i zakwestionowania decyzji.

Istotne informacje na temat zastosowanej logiki, a także znaczenia i przewidywanych konsekwencji takiego przetwarzania dla osoby, której dane dotyczą, są określone w naszej polityce prywatności.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## III. EU-U.S. Data Privacy Framework (EU-U.S. DPF), UK Extension to the EU-U.S. DPF, Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF)

Jeśli nasza organizacja jest certyfikowanym członkiem EU-U.S. Data Privacy Framework (EU-U.S. DPF) i/lub UK Extension to the EU-U.S. DPF i/lub Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF), obowiązują następujące zasady:

Przestrzegamy EU-U.S. Data Privacy Framework (EU-U.S. DPF) i UK Extension to the EU-U.S. DPF oraz Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF), jak określono przez U.S. Department of Commerce. Nasza firma potwierdziła w Departamencie Handlu USA, że przestrzega EU-U.S. Data Privacy Framework Principles (EU-U.S. DPF Principles) w odniesieniu do przetwarzania danych osobowych, które otrzymuje z Unii Europejskiej i Wielkiej Brytanii, odwołując się do EU-U.S. DPF i UK Extension to the EU-U.S. DPF. Nasza firma potwierdziła w Departamencie Handlu USA, że przestrzega Swiss-U.S. Data Privacy Framework Principles (Swiss-U.S. DPF Principles) w odniesieniu do przetwarzania danych osobowych, które otrzymuje ze Szwajcarii, odwołując się do Swiss-U.S. DPF. W przypadku sprzeczności między postanowieniami naszej polityki prywatności a EU-U.S. DPF Principles i/lub Swiss-U.S. DPF Principles, nadrzędne są Principles.

Aby dowiedzieć się więcej o programie Data Privacy Framework (DPF) oraz aby zobaczyć nasze certyfikaty, prosimy odwiedzić stronę https://www.dataprivacyframework.gov/.

Inne jednostki lub spółki zależne naszej firmy w USA, które również przestrzegają EU-U.S. DPF Principles, w tym UK Extension to the EU-U.S. DPF oraz Swiss-U.S. DPF Principles, jeśli istnieją, są wymienione w naszej polityce prywatności.

Zgodnie z EU-U.S. DPF i UK Extension to the EU-U.S. DPF oraz Swiss-U.S. DPF, nasza firma zobowiązuje się do współpracy z organami ochrony danych UE oraz Information Commissioner's Office (ICO) w Wielkiej Brytanii oraz Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) w Szwajcarii, i do przestrzegania ich zaleceń w odniesieniu do nierozwiązanych skarg dotyczących naszego postępowania z danymi osobowymi, które otrzymaliśmy, odwołując się do EU-U.S. DPF oraz UK Extension to the EU-U.S. DPF i Swiss-U.S. DPF.

Informujemy osoby, których dane dotyczą, o odpowiednich europejskich organach ochrony danych, które są odpowiedzialne za przetwarzanie skarg dotyczących postępowania naszej organizacji z danymi osobowymi, w górnej części tego dokumentu przejrzystości oraz o tym, że oferujemy odpowiednie i bezpłatne środki ochrony prawnej.

Informujemy wszystkie osoby, których dane dotyczą, że nasza firma podlega uprawnieniom dochodzeniowym i egzekucyjnym Federal Trade Commission (FTC).


© All rights reserved by Heiko Maniero.

Osoby, których dane dotyczą, mają pod pewnymi warunkami możliwość skorzystania z wiążącego arbitrażu. Nasza organizacja zobowiązana jest do rozstrzygania roszczeń i przestrzegania warunków zgodnie z załącznikiem I DPF Principles, jeśli osoba, której dane dotyczą, zażądała wiążącego arbitrażu, powiadamiając naszą organizację i przestrzegając procedur oraz warunków zgodnie z załącznikiem I Principles.

Informujemy tutaj wszystkie osoby, których dane dotyczą, o odpowiedzialności naszej organizacji w przypadku przekazania danych osobowych stronom trzecim.

W przypadku pytań osób, których dane dotyczą, lub organów ochrony danych, wyznaczyliśmy lokalnych przedstawicieli, których nazwy znajdują się w górnej części tego dokumentu przejrzystości.

Oferujemy Państwu możliwość wyboru (Opt-out), czy Państwa dane osobowe (i) mają zostać przekazane stronom trzecim, czy (ii) mają zostać użyte do celu, który znacząco różni się od celu/ów, dla którego/których zostały pierwotnie zebrane lub później zatwierdzone przez Państwa. Wyraźny, dobrze widoczny i łatwo dostępny mechanizm do wykonania prawa wyboru polega na skontaktowaniu się z naszym Inspektorem Ochrony Danych (DSB) poprzez e-mail. Nie mają Państwo możliwości wyboru i nie jesteśmy do tego zobowiązani, jeśli dane są przekazywane stronie trzeciej, która działa jako pełnomocnik lub przetwarzający na naszą rzecz i zgodnie z naszymi instrukcjami. Zawsze jednak zawieramy umowę z takim pełnomocnikiem lub przetwarzającym.

W przypadku danych wrażliwych (tj. danych osobowych zawierających informacje o stanie zdrowia, pochodzeniu rasowym lub etnicznym, poglądach politycznych, przekonaniach religijnych lub filozoficznych, członkostwie w związkach zawodowych lub danych dotyczących życia seksualnego osoby, której dane dotyczą), uzyskujemy Państwa wyraźną zgodę (Opt-in), jeśli te dane (i) mają zostać przekazane stronom trzecim, czy (ii) mają zostać użyte do innego celu niż ten, dla którego zostały pierwotnie zebrane lub dla którego później wyrazili Państwo zgodę, dokonując wyboru Opt-in. Ponadto, traktujemy wszystkie dane osobowe, które otrzymujemy od stron trzecich, jako wrażliwe, jeśli strona trzecia je zidentyfikowała i traktowała jako wrażliwe.

Informujemy Państwa o konieczności ujawnienia danych osobowych w odpowiedzi na legalne żądania władz, w tym w celu spełnienia wymogów bezpieczeństwa narodowego lub egzekwowania prawa.

Podczas przekazywania danych osobowych stronie trzeciej, która działa jako administrator, przestrzegamy Principles powiadamiania i wyboru. Ponadto, zawieramy umowę z administratorem, która przewiduje, że dane te mogą być przetwarzane wyłącznie do ograniczonych i określonych celów zgodnie z Państwa zgodą, i że odbiorca zapewnia ten sam poziom ochrony, co Principles DPF, i powiadamia nas, jeśli stwierdzi, że nie jest już w stanie spełnić tego zobowiązania. Umowa przewiduje, że administrator zaprzestanie przetwarzania lub podejmie inne odpowiednie i właściwe środki zaradcze, jeśli stwierdzi, że nie jest w stanie spełnić swojego zobowiązania.

Podczas przekazywania danych osobowych stronie trzeciej, która działa jako pełnomocnik lub przetwarzający, (i) przekazujemy te dane wyłącznie do ograniczonych i określonych celów; (ii)


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

upewniamy się, że pełnomocnik lub przetwarzający zobowiązany jest zapewnić co najmniej ten sam poziom ochrony danych, jaki wymagają DPF Principles; (iii) podejmujemy odpowiednie i właściwe środki, aby upewnić się, że pełnomocnik lub przetwarzający faktycznie przetwarza przekazane dane osobowe w sposób zgodny z naszymi zobowiązaniami zgodnie z DPF Principles; (iv) wymagamy od pełnomocnika lub przetwarzającego, aby powiadomił naszą organizację, jeśli stwierdzi, że nie może już spełnić swojego zobowiązania do zapewnienia tego samego poziomu ochrony, jaki wymagają DPF Principles; (v) po otrzymaniu powiadomienia, w tym zgodnie z (iv), podejmujemy odpowiednie i właściwe kroki, aby zatrzymać nieautoryzowane przetwarzanie i zapewnić środki zaradcze; oraz (vi) dostarczamy DPF Department na żądanie streszczenie lub reprezentatywny egzemplarz odpowiednich postanowień umowy dotyczących ochrony danych z tym pełnomocnikiem.

Zgodnie z EU-U.S. DPF i/lub UK Extension to the EU-U.S. DPF i/lub Swiss-U.S. DPF, nasza firma zobowiązuje się do współpracy z organem utworzonym przez europejskie organy ochrony danych oraz Information Commissioner's Office (ICO) w Wielkiej Brytanii lub Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) w Szwajcarii oraz do przestrzegania ich zaleceń w odniesieniu do nierozwiązanych skarg dotyczących naszego postępowania z danymi osobowymi, które otrzymujemy, odwołując się do EU-U.S. DPF oraz UK Extension to the EU-U.S. DPF i Swiss-U.S. DPF w kontekście relacji pracowniczych.

Wszystkim osobom, których dane dotyczą, przebywającym tymczasowo w Unii Europejskiej (UE), Europejskim Obszarze Gospodarczym (EOG) lub Zjednoczonym Królestwie lub mającym tam miejsce zamieszkania lub zwykłego pobytu, przysługują prawa i uprawnienia osoby, której dane dotyczą, opublikowane w naszym dokumencie dotyczącym przejrzystości, które wynikają również z art. 15-22 RODO, w tym prawo dostępu do danych osobowych. Udostępniliśmy te informacje we wszystkich językach UE i EOG. Angielska wersja językowa dotyczy Wielkiej Brytanii.

Wszystkim osobom, których dane dotyczą, które tymczasowo przebywają w Szwajcarii lub mają tam miejsce zamieszkania lub zwykłego pobytu, przysługują prawa i uprawnienia osoby, której dane dotyczą, wynikające ze szwajcarskiej ustawy o ochronie danych (DPA) i szwajcarskiego rozporządzenia o ochronie danych (DPR), które zostały opublikowane w naszym Dokumencie przejrzystości, w tym prawo dostępu do danych osobowych. Udostępniliśmy te informacje w trzech językach urzędowych Szwajcarii (niemieckim, włoskim i francuskim).


© All rights reserved by Heiko Maniero.

# POLISH: Informacja o przetwarzaniu danych osobowych pracowników i kandydatów (art. 13 i 14 RODO)

Szanowni Państwo!

Dane osobowe pracowników i kandydatów zasługują na szczególną ochronę. Naszym celem jest utrzymanie wysokiego poziomu ochrony danych osobowych. Dlatego regularnie rozwijamy nasze koncepcje ochrony i bezpieczeństwa danych.

Oczywiście przestrzegamy ustawowych przepisów w zakresie ochrony danych. Zgodnie z art. 13 i art. 14 RODO przetwarzając dane osobowe, administratorzy muszą spełnić określone wymogi udzielania informacji. Ten dokument spełnia ten obowiązek.

Terminologia regulacji prawnych jest skomplikowana. Niestety przygotowanie tego dokumentu nie obyło się bez użycia konkretnych terminów prawnych. Chcielibyśmy zatem podkreślić, że zawsze mogą się Państwo z nami skontaktować, aby zapytać o ten dokument, terminy lub sformułowania w nim użyte.

## I. Zgodność z wymogami informacyjnymi w przypadku zbierania danych osobowych od osoby, której dane dotyczą (art. 13 RODO)

### A. Tożsamość i dane kontaktowe administratora (art. 13 ust. 1 lit. a) RODO)

Patrz wyżej

### B. Dane kontaktowe inspektora ochrony danych (art. 13 ust. 1 lit. b) RODO)

Patrz wyżej

### C. Cele przetwarzania danych osobowych oraz podstawa prawna przetwarzania (art. 13 ust. 1 lit. c RODO)

W przypadku danych kandydatów są one przetwarzane w celu weryfikacji zgłoszenia w procesie rekrutacji. W tym celu przetwarzamy wszystkie dane podane przez kandydata. Na podstawie danych przekazanych w trakcie procesu rekrutacji sprawdzimy, czy dana osoba została zaproszona na rozmowę kwalifikacyjną (jest to część procesu selekcji). W przypadku osób, które spełniają ogólne kryteria, w szczególności w kontekście rozmowy kwalifikacyjnej, przetwarzamy określone inne dane osobowe podane przez kandydata niezbędne do podjęcia przez nas decyzji o wyborze. W przypadku zatrudnienia kandydata jego dane zmienią się automatycznie na dane pracownika. W ramach procesu rekrutacji


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

będziemy przetwarzać inne dane osobowe pracownika, których od niego zażądamy, a które są niezbędne do zawarcia lub realizacji umowy (np. osobiste numery identyfikacyjne lub numery identyfikacji podatkowej). W przypadku danych pracowników są one przetwarzane w celu realizacji umowy zawartej z pracownikiem lub spełnienia innych wymogów prawnych w zakresie stosunku pracy (np. przepisów podatkowych); dane osobowe pracownika są również wykorzystane w celu realizacji jego umowy o pracę (np. publikacja imienia i nazwiska oraz danych kontaktowych pracownika w spółce lub przekazanie ich klientom). Dane pracownika przechowywane są po rozwiązaniu jego stosunku pracy przez okres wymagany prawem.

Podstawą prawną przetwarzania danych jest art. 6 ust. 1 lit. b RODO, art. 9 ust. 2 lit. b i lit. h RODO, art. 88 ust. 1 RODO oraz ustawodawstwo krajowe, w tym art. 26 niemieckiej ustawy BDSG (federalnej ustawy o ochronie danych osobowych).

## D. Kategorie odbiorców danych osobowych (art. 13 ust. 1 lit. e RODO)

Władze publiczne

Organy zewnętrzne

Dalsze organy zewnętrzne

Przetwarzanie wewnętrzne

Przetwarzanie wewnątrzgrupowe

Inne organy

Lista naszych podmiotów przetwarzających i odbiorców danych w państwach trzecich oraz, w stosownych przypadkach, organizacji międzynarodowych jest publikowana na naszej stronie internetowej lub można ją bezpłatnie uzyskać od nas. Aby poprosić o taką listę, należy skontaktować się z naszym inspektorem ochrony danych.

## E. Odbiorcy w państwie trzecim, jak również odpowiednie lub właściwe zabezpieczenia oraz możliwości uzyskania kopii danych lub miejsca udostępnienia danych (art. 13 ust. 1 lit. f, art. 46 ust. 1, art. 46 ust. 2 lit. c RODO)

Wszystkie firmy i oddziały należące do naszej grupy (zwane dalej „spółkami grupy”), które mają swoje miejsce prowadzenia działalności lub biuro w państwie trzecim, mogą być odbiorcami danych osobowych.


© All rights reserved by Heiko Maniero.

Na mocy art. 46 ust. 1 RODO administrator lub podmiot przetwarzający mogą przekazać dane osobowe do państwa trzeciego wyłącznie, gdy zapewnią odpowiednie zabezpieczenia, i pod warunkiem, że obowiązują egzekwowalne prawa osób, których dane dotyczą, i skuteczne środki ochrony prawnej. Odpowiednie zabezpieczenia można zapewnić bez konieczności uzyskania specjalnego zezwolenia organu nadzorczego za pomocą standardowych klauzul umownych (art. 46 ust. 2 lit. c RODO).

Przed pierwszym przekazaniem danych osobowych uzgadniane są z wszystkimi odbiorcami z państw trzecich standardowe klauzule umowne Unii Europejskiej. W związku z tym zapewniono, że zagwarantowane zostaną odpowiednie zabezpieczenia, egzekwowalne prawa osób, których dane dotyczą, oraz skuteczne środki prawne dla osób, których dane dotyczą, wynikające ze standardowych klauzul umownych UE. Każda osoba, której dane dotyczą, może uzyskać kopię standardowych klauzul umownych od naszego inspektora ochrony danych. Standardowe klauzule umowne są również dostępne w Dzienniku Urzędowym Unii Europejskiej.

Artykuł 45 ust. 3 ogólnego rozporządzenia o ochronie danych (RODO) przyznaje Komisji Europejskiej prawo do podjęcia decyzji, w drodze aktu wykonawczego, że państwo spoza UE zapewnia odpowiedni poziom ochrony. Oznacza to poziom ochrony danych osobowych, który jest zasadniczo równoważny poziomowi ochrony w UE. Skutkiem decyzji stwierdzających odpowiedni poziom ochrony jest to, że dane osobowe mogą swobodnie przepływać z UE (oraz Norwegii, Liechtensteinu i Islandii) do państwa trzeciego bez dalszych przeszkód. Podobne zasady obowiązują w Wielkiej Brytanii, Szwajcarii i niektórych innych krajach.

W przypadku, gdy Komisja Europejska lub rząd innego kraju zdecyduje, że kraj trzeci zapewnia odpowiedni poziom ochrony, a obowiązujące ramy (np. EU-U.S. Data Privacy Framework, Swiss-U.S. Data Privacy Framework, UK Extension to the EU-U.S. Data Privacy Framework), wszystkie transfery dokonywane przez nas do członków takich ram (np. podmiotów samocertyfikowanych) opierają się wyłącznie na członkostwie tych podmiotów w odpowiednich ramach. W przypadku, gdy my lub jeden z podmiotów należących do naszej grupy jest członkiem takich ram, wszystkie transfery do nas lub naszego podmiotu należącego do grupy opierają się wyłącznie na członkostwie podmiotu w takich ramach.

Każda osoba, której dane dotyczą, może uzyskać od nas kopię tych ram. Ponadto ramy są również dostępne w Dzienniku Urzędowym Unii Europejskiej lub w opublikowanych materiałach prawnych lub na stronach internetowych organów nadzorczych lub innych właściwych organów lub instytucji.

## F. Okres, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalania tego okresu (art. 13 ust. 2 lit. a RODO)

Okres przechowywania danych osobowych kandydatów wynosi 6 miesięcy. Do danych osobowych pracowników stosuje się odpowiednie ustawowe okresy przechowywania danych. Po upływie tego


© All rights reserved by Heiko Maniero.

okresu odpowiednie dane są standardowo usuwane, o ile nie będę jeszcze potrzebne do realizacji lub zawarcia umowy.

## G. Informacje o prawie do żądania od administratora dostępu do danych osobowych osoby, której dane dotyczą, ich sprostowania, usunięcia lub ograniczenia przetwarzania lub o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych (art. 13 ust. 2 lit. b RODO)

Wszystkie osoby, których dane dotyczą, mają następujące prawa:

***Prawo dostępu***

Każda osoba, której dane dotyczą, ma prawo dostępu do danych osobowych, które jej dotyczą. Prawo dostępu obejmuje wszystkie przetwarzane przez nas dane. Istnieje możliwość łatwego wykonywania tego prawa w rozsądnych odstępach czasu, by mieć świadomość przetwarzania i móc zweryfikować zgodność przetwarzania z prawem (ust. 63 preambuły RODO). To prawo wynika z art. 15 RODO. Osoba, której dane dotyczą, może skontaktować się z naszym inspektorem ochrony danych, aby skorzystać z prawa dostępu.

***Prawo do sprostowania***

Zgodnie z art. 16 zdanie 1 RODO osoba, której dane dotyczą, ma prawo żądania od administratora niezwłocznego sprostowania dotyczących jej danych osobowych, które są nieprawidłowe. Ponadto zgodnie z art. 16 zdanie 2 RODO osoba, której dane dotyczą, ma prawo, biorąc pod uwagę cele przetwarzania, żądania uzupełnienia niekompletnych danych osobowych, w tym poprzez przedstawienie dodatkowego oświadczenia. Osoba, której dane dotyczą, może skontaktować się z naszym inspektorem ochrony danych, aby skorzystać z prawa do sprostowania.

***Prawo do usunięcia danych (prawo do bycia zapomnianym)***

Ponadto osoby, których dane dotyczą, mają prawo do usunięcia danych i do bycia zapomnianym na mocy art. 17 RODO. Z tego prawa można również skorzystać, kontaktując się z naszym inspektorem ochrony danych. W tym miejscu chcielibyśmy jednak zwrócić uwagę, że to prawo nie ma zastosowania, o ile przetwarzanie jest konieczne do wypełnienia obowiązku prawnego, któremu podlega nasza firma (art. 17 ust. 3 lit. b RODO). Oznacza to, że możemy zaakceptować wniosek o usunięcie danych tylko po upływie ustawowego okresu zatrzymywania.

***Prawo do ograniczenia przetwarzania danych***

Zgodnie z art. 18 RODO osoba, której dane dotyczą, jest uprawniona do ograniczenia przetwarzania danych. Można domagać się ograniczenia przetwarzania, jeżeli spełniony jest jeden z warunków określonych w art. 18 ust. 1 lit. a-d RODO. Osoba, której dane dotyczą, może skontaktować się z naszym inspektorem ochrony danych, aby skorzystać z prawa ograniczenia przetwarzania..


© All rights reserved by Heiko Maniero.

***Prawo do sprzeciwu***

Ponadto art. 21 RODO gwarantuje prawo do sprzeciwu. Osoba, której dane dotyczą, może skontaktować się z naszym inspektorem ochrony danych, aby skorzystać z prawa do sprzeciwu.

***Prawo do przenoszenia danych***

Art. Art. 20 RODO gwarantuje osobie, której dane dotyczą, prawo do przenoszenia danych. Zgodnie z tym postanowieniem, osoba, której dane dotyczą, ma prawo na warunkach określonych w art. 20 ust. 1 lit. a i b RODO otrzymać w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego dane osobowe jej dotyczące, które dostarczyła administratorowi, oraz ma prawo przesłać te dane osobowe innemu administratorowi bez przeszkód ze strony administratora, któremu dostarczono te dane osobowe. Osoba, której dane dotyczą, może skontaktować się z naszym inspektorem ochrony danych, aby skorzystać z prawa do przenoszenia danych.

## H. Informacje o prawie do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem, jeśli podstawą przetwarzania jest art. 6 ust. 1 lit. a RODO lub art. 9 ust. 2 lit. a RODO (art. 13 ust. 2 lit. c) RODO)

Jeśli podstawą przetwarzania danych osobowych jest art. 6 ust. 1 lit. a RODO, jak ma to miejsce w sytuacji, gdy osoba, której dane dotyczą wyraziła zgodę na przetwarzanie danych osobowych dla jednego lub więcej konkretnych celów, lub art. 9 ust. 2 lit. a RODO, który reguluje wyraźną zgodę na przetwarzanie szczególnych kategorii danych osobowych, osoba, której dane dotyczą, zgodnie z art. 7 ust. 3 zdanie 1 RODO, ma prawo do wycofania swojej zgody w dowolnym czasie.

Wycofanie zgody nie wpływa na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej wycofaniem (art. 7 ust. 3 zdanie 2 RODO). Wycofanie zgody musi być równie łatwe jak jej wyrażenie (art. 7 ust. 3 zdanie 4 RODO. W związku z powyższym wycofanie zgody może zawsze nastąpić w taki sam sposób, jak udzielono zgody lub w jakikolwiek inny sposób, który jest uważany przez osobę, której dane dotyczą, za prostszy. W dzisiejszym społeczeństwie informacyjnym najprawdopodobniej najprostszym sposobem na wycofanie zgody jest zwykła wiadomość e-mail. Jeżeli osoba, której dane dotyczą, pragnie wycofać udzieloną nam zgodę, wystarczy zwykła wiadomość e-mail wysłana do naszego inspektora ochrony danych. Alternatywnie osoba, której dane dotyczą, może wybrać inny sposób powiadomienia nas o wycofaniu swojej zgody.

## I. Informacje o prawie wniesienia skargi do organu nadzorczego (art. 13 ust. 2 lit. d, art. 77 ust. 1 RODO)

Jako administrator jesteśmy zobowiązani powiadomić osobę, której dane dotyczą, o prawie do wniesienia skargi do organu nadzorczego (art. 13 ust. 2. lit. d RODO). Prawo do wniesienia skargi do organu nadzorczego reguluje art. 77 ust. 1 RODO. Zgodnie z jego treścią, bez uszczerbku dla innych


© All rights reserved by Heiko Maniero.

administracyjnych lub środków ochrony prawnej przed sądem każda osoba, której dane dotyczą, ma prawo wnieść skargę do organu nadzorczego, w szczególności w państwie członkowskim swojego zwykłego pobytu, swojego miejsca pracy lub miejsca popełnienia domniemanego naruszenia, jeżeli sądzi, że przetwarzanie danych osobowych jej dotyczące narusza rozporządzenie ogólne rozporządzenie o ochronie danych. Prawo do wniesienia skargi do organu nadzorczego zostało ograniczone prawem Unii w taki sposób, że może ono być wykonywane tylko przed jednym organem nadzorującym (ust. 141 zdanie 1 preambuły RODO). Ta reguła ma na celu uniknięcie podwójnych skarg niniejszej samej osoby, której dane dotyczą, w niniejszej samej sprawie. Jeżeli osoba, której dane dotyczą, chce złożyć na nas skargę, prosimy o kontakt tylko z jednym organem nadzorczym.

## J. Udostępnianie danych osobowych jako wymóg ustawowy lub umowny; warunek zawarcia umowy; obowiązek osoby, której dane dotyczą, do podania danych osobowych; ewentualne konsekwencje niepodania danych (art. art. 13 ust. 2 lit. e RODO)

Wyjaśniamy, że udostępnianie danych osobowych jest częściowo wymagane przez prawo (np. przepisy podatkowe) lub może wynikać z postanowień umownych (np. informacje o partnerze umownym).

Czasami może być konieczne do zawarcia umowy podanie przez osobę, której dane dotyczą, danych osobowych, które następnie muszą zostać przez nas przetwarzane. Osoba, której dane dotyczą jest na przykład zobowiązana do przekazania nam danych osobowych podczas zawierania z nami umowy. Konsekwencją niedostarczenia danych osobowych byłby brak możliwości zawarcia umowy z osobą, której dane dotyczą.

Zanim dane osobowe zostaną przekazane przez osobę, której dane dotyczą, osoba ta musi skontaktować się z naszym inspektorem ochrony danych. Nasz inspektor ochrony danych wyjaśnia osobie, której dane dotyczą, czy podanie danych osobowych jest wymagane przez prawo lub umowę lub jest konieczne do zawarcia umowy, czy istnieje obowiązek dostarczenia danych osobowych i konsekwencje niedostarczenia danych osobowych.

## K. Informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, o którym mowa w art. 22 ust. 1 i 4 RODO, oraz – przynajmniej w tych przypadkach – istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą (art. 13 ust. 2 lit. f RODO)

Jako odpowiedzialna firma zazwyczaj nie stosujemy zautomatyzowanego podejmowania decyzji ani profilowania. Jeśli w wyjątkowych przypadkach przeprowadzimy zautomatyzowane podejmowanie decyzji lub profilowanie, poinformujemy o tym osobę, której dane dotyczą, osobno lub za pośrednictwem


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

podsekcji w naszej polityce prywatności (na naszej stronie internetowej). W takim przypadku obowiązują następujące zasady:

Zautomatyzowane podejmowanie decyzji - w tym profilowanie - może mieć miejsce, jeżeli (1) jest to niezbędne do zawarcia lub wykonania umowy między osobą, której dane dotyczą, a nami lub (2) jest to dozwolone prawem Unii lub prawem państwa członkowskiego, któremu podlegamy i które przewiduje również odpowiednie środki ochrony praw i wolności oraz prawnie uzasadnionych interesów osoby, której dane dotyczą; lub (3) odbywa się to na podstawie wyraźnej zgody osoby, której dane dotyczą.

W przypadkach, o których mowa w art. 22 ust. 2 lit. a) i c) RODO, wdrażamy odpowiednie środki w celu ochrony praw i wolności oraz uzasadnionych interesów osoby, której dane dotyczą. W takich przypadkach użytkownik ma prawo do uzyskania interwencji ludzkiej ze strony administratora, wyrażenia swojego punktu widzenia i zakwestionowania decyzji.

Istotne informacje na temat zastosowanej logiki, a także znaczenia i przewidywanych konsekwencji takiego przetwarzania dla osoby, której dane dotyczą, są określone w naszej polityce prywatności.

## II. Zgodność z wymogami informacyjnymi w przypadku niezbierania danych osobowych od osoby, której dane dotyczą (art. 14 RODO)

### A. Tożsamość i dane kontaktowe administratora (art. 14 ust. 1 lit. a) RODO)

Patrz wyżej

### B. Dane kontaktowe inspektora ochrony danych (art. 14 ust. 1 lit. b) RODO)

Patrz wyżej

### C. Cele przetwarzania danych osobowych oraz podstawa prawna przetwarzania (art. 14 ust. 1 lit. c RODO)

Dane kandydatów pozyskane z innych źródeł, niż od osoby, których dane dotyczą, są przetwarzane w celu weryfikacji zgłoszenia w procesie rekrutacji. W tym celu możemy przetwarzać dane zgromadzone z innych źródeł niż od kandydata. Na podstawie danych przetwarzanych w trakcie procesu rekrutacji sprawdzimy, czy dana osoba została zaproszona na rozmowę kwalifikacyjną (jest to część procesu selekcji). W przypadku zatrudnienia kandydata jego dane zostaną zamienione automatycznie na dane pracownika. W przypadku danych pracowników są one przetwarzane w celu realizacji umowy zawartej z pracownikiem lub spełnienia innych wymogów prawnych w zakresie stosunku pracy. Dane pracownika przechowywane są po rozwiązaniu jego stosunku pracy przez okres wymagany prawem.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

Podstawą prawną przetwarzania danych jest art. 6 ust. 1 lit. b i lit. f RODO, art. 9 ust. 2 lit. b i lit. h RODO, art. 88 ust. 1 RODO oraz ustawodawstwo krajowe, w tym art. 26 niemieckiej ustawy BDSG (federalnej ustawy o ochronie danych osobowych).

## D. Kategorie danych osobowych (art. 14 ust. 1 lit. d RODO)

Dane kandydatów

Dane pracowników

## E. Kategorie odbiorców danych (art. 14 ust. 1 lit. e RODO)

Władze publiczne

Organy zewnętrzne

Dalsze organy zewnętrzne

Przetwarzanie wewnętrzne

Przetwarzanie wewnątrzgrupowe

Inne organy

Lista naszych podmiotów przetwarzających i odbiorców danych w państwach trzecich oraz, w stosownych przypadkach, organizacji międzynarodowych jest publikowana na naszej stronie internetowej lub można ją bezpłatnie uzyskać od nas. Aby poprosić o taką listę, należy skontaktować się z naszym inspektorem ochrony danych.

## F. Odbiorcy w państwie trzecim, jak również odpowiednie lub właściwe zabezpieczenia oraz możliwości uzyskania kopii danych lub miejsca udostępnienia danych (art. 14 ust. 1 lit. f, art. 46 ust. 1, art. 46 ust. 2 lit. c RODO)

Wszystkie firmy i oddziały należące do naszej grupy (zwane dalej „spółkami grupy”), które mają swoje miejsce prowadzenia działalności lub biuro w państwie trzecim, mogą być odbiorcami danych osobowych.

Na mocy art. 46 ust. 1 RODO administrator lub podmiot przetwarzający mogą przekazać dane osobowe do państwa trzeciego wyłącznie, gdy zapewnią odpowiednie zabezpieczenia, i pod warunkiem, że


© All rights reserved by Heiko Maniero.

obowiązują egzekwowalne prawa osób, których dane dotyczą, i skuteczne środki ochrony prawnej. Odpowiednie zabezpieczenia można zapewnić bez konieczności uzyskania specjalnego zezwolenia organu nadzorczego za pomocą standardowych klauzul umownych (art. 46 ust. 2 lit. c RODO).

Przed pierwszym przekazaniem danych osobowych uzgadniane są z wszystkimi odbiorcami z państw trzecich standardowe klauzule umowne Unii Europejskiej. W związku z tym zapewniono, że zagwarantowane zostaną odpowiednie zabezpieczenia, egzekwowalne prawa osób, których dane dotyczą, oraz skuteczne środki prawne dla osób, których dane dotyczą, wynikające ze standardowych klauzul umownych UE. Każda osoba, której dane dotyczą, może uzyskać kopię standardowych klauzul umownych od naszego inspektora ochrony danych. Standardowe klauzule umowne są również dostępne w Dzienniku Urzędowym Unii Europejskiej.

Artykuł 45 ust. 3 ogólnego rozporządzenia o ochronie danych (RODO) przyznaje Komisji Europejskiej prawo do podjęcia decyzji, w drodze aktu wykonawczego, że państwo spoza UE zapewnia odpowiedni poziom ochrony. Oznacza to poziom ochrony danych osobowych, który jest zasadniczo równoważny poziomowi ochrony w UE. Skutkiem decyzji stwierdzających odpowiedni poziom ochrony jest to, że dane osobowe mogą swobodnie przepływać z UE (oraz Norwegii, Liechtensteinu i Islandii) do państwa trzeciego bez dalszych przeszkód. Podobne zasady obowiązują w Wielkiej Brytanii, Szwajcarii i niektórych innych krajach.

W przypadku, gdy Komisja Europejska lub rząd innego kraju zdecyduje, że kraj trzeci zapewnia odpowiedni poziom ochrony, a obowiązujące ramy (np. EU-U.S. Data Privacy Framework, Swiss-U.S. Data Privacy Framework, UK Extension to the EU-U.S. Data Privacy Framework), wszystkie transfery dokonywane przez nas do członków takich ram (np. podmiotów samocertyfikowanych) opierają się wyłącznie na członkostwie tych podmiotów w odpowiednich ramach. W przypadku, gdy my lub jeden z podmiotów należących do naszej grupy jest członkiem takich ram, wszystkie transfery do nas lub naszego podmiotu należącego do grupy opierają się wyłącznie na członkostwie podmiotu w takich ramach.

Każda osoba, której dane dotyczą, może uzyskać od nas kopię tych ram. Ponadto ramy są również dostępne w Dzienniku Urzędowym Unii Europejskiej lub w opublikowanych materiałach prawnych lub na stronach internetowych organów nadzorczych lub innych właściwych organów lub instytucji.

## G. Okres, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalania tego okresu (art. 14 ust. 2 lit. a RODO)

Okres przechowywania danych osobowych kandydatów wynosi 6 miesięcy. Do danych osobowych pracowników stosuje się odpowiednie ustawowe okresy przechowywania danych. Po upływie tego okresu odpowiednie dane są standardowo usuwane, o ile nie będę jeszcze potrzebne do realizacji lub zawarcia umowy.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## H. Powiadomienie o uzasadnionych interesach administratora lub strony trzeciej, jeżeli podstawą przetwarzania jest art. 6 ust. 1 lit. f RODO (art. 14 ust. 2. b RODO)

Zgodnie z art. 6 ust. 1 lit. f RODO przetwarzanie jest zgodne z prawem tylko wtedy, gdy jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osób, których dane dotyczą, wymagające ochrony danych osobowych. Zgodnie z ust. 47 zdanie 2 preambuły RODO uzasadniony interes może istnieć wtedy, gdy występuje odpowiedni i właściwy związek między osobą, której dane dotyczą, a administratorem, np. w sytuacjach, w których osoba, której dane dotyczą, jest klientem administratora. We wszystkich przypadkach, w których nasza firma przetwarza dane na podstawie art. 6 ust. 1 lit (f) RODO, naszym uzasadnionym interesem jest zatrudnienie odpowiedniego personelu i specjalistów.

## I. Informacje o prawie do żądania od administratora dostępu do danych osobowych dotyczących osoby, której dane dotyczą, ich sprostowania, usunięcia lub ograniczenia przetwarzania oraz o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych (art. 14 ust. 2 lit. c RODO)

Wszystkie osoby, których dane dotyczą, mają następujące prawa:

***Prawo dostępu***

Każda osoba, której dane dotyczą, ma prawo dostępu do danych osobowych, które jej dotyczą. Prawo dostępu obejmuje wszystkie przetwarzane przez nas dane. Istnieje możliwość łatwego wykonywania tego prawa w rozsądnych odstępach czasu, by mieć świadomość przetwarzania i móc zweryfikować zgodność przetwarzania z prawem (ust. 63 preambuły RODO). To prawo wynika z art. 15 RODO. Osoba, której dane dotyczą, może skontaktować się z naszym inspektorem ochrony danych, aby skorzystać z prawa dostępu.

***Prawo do sprostowania***

Zgodnie z art. 16 zdanie 1 RODO osoba, której dane dotyczą, ma prawo żądania od administratora niezwłocznego sprostowania dotyczących jej danych osobowych, które są nieprawidłowe. Osoba, której dane dotyczą, może skontaktować się z naszym inspektorem ochrony danych, aby skorzystać z prawa do sprostowania. Zgodnie z art. 16 zdanie 1 RODO osoba, której dane dotyczą, ma prawo żądania od administratora niezwłocznego sprostowania dotyczących jej danych osobowych, które są nieprawidłowe.

***Prawo do usunięcia danych (prawo do bycia zapomnianym)***

Ponadto osoby, których dane dotyczą, mają prawo do usunięcia danych i do bycia zapomnianym na mocy art. 17 RODO. Z tego prawa można również skorzystać, kontaktując się z naszym inspektorem ochrony danych. W tym miejscu chcielibyśmy jednak zwrócić uwagę, że to prawo nie ma zastosowania, o ile przetwarzanie jest konieczne do wypełnienia obowiązku prawnego, któremu podlega nasza firma


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

(art. 17 ust. 3 lit. b RODO). Oznacza to, że możemy zaakceptować wniosek o usunięcie danych tylko po upływie ustawowego okresu zatrzymywania.

***Prawo do ograniczenia przetwarzania danych***

Zgodnie z art. 18 RODO osoba, której dane dotyczą, jest uprawniona do ograniczenia przetwarzania danych. Można domagać się ograniczenia przetwarzania, jeżeli spełniony jest jeden z warunków określonych w art. 18 ust. 1 lit. a-d RODO. Można domagać się ograniczenia przetwarzania, jeżeli spełniony jest jeden z warunków określonych w art. 18 ust. 1 lit. a-d RODO.

***Prawo do sprzeciwu***

Ponadto art. 21 RODO gwarantuje prawo do sprzeciwu. Osoba, której dane dotyczą, może skontaktować się z naszym inspektorem ochrony danych, aby skorzystać z prawa do sprzeciwu.

***Prawo do przenoszenia danych***

Art. 20 RODO gwarantuje osobie, której dane dotyczą, prawo do przenoszenia danych. Zgodnie z tym postanowieniem, osoba, której dane dotyczą, ma prawo na warunkach określonych w art. 20 ust. 1 lit. a i b RODO otrzymać w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego dane osobowe jej dotyczące, które dostarczyła administratorowi, oraz ma prawo przesłać te dane osobowe innemu administratorowi bez przeszkód ze strony administratora, któremu dostarczono te dane osobowe. Osoba, której dane dotyczą, może skontaktować się z naszym inspektorem ochrony danych, aby skorzystać z prawa do przenoszenia danych.

## J. Informacje o prawie do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem, jeśli podstawą przetwarzania jest art. 6 ust. 1 lit. a lub art. 9 ust. 2 lit. a RODO (art. 14 ust. 2 lit. d RODO)

Jeśli podstawą przetwarzania danych osobowych jest art. 6 ust. 1 lit. a RODO, jak ma to miejsce w sytuacji, gdy osoba, której dane dotyczą wyraziła zgodę na przetwarzanie danych osobowych dla jednego lub więcej konkretnych celów, lub art. 9 ust. 2 lit. a RODO, który reguluje wyraźną zgodę na przetwarzanie szczególnych kategorii danych osobowych, osoba, której dane dotyczą, zgodnie z art. 7 ust. 3 zdanie 1 RODO, ma prawo do wycofania swojej zgody w dowolnym czasie.

Wycofanie zgody nie wpływa na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej wycofaniem (art. 7 ust. 3 zdanie 2 RODO). Wycofanie zgody musi być równie łatwe jak jej wyrażenie (art. 7 ust. 3 zdanie 4 RODO. W związku z powyższym wycofanie zgody może zawsze nastąpić w taki sam sposób, jak udzielono zgody lub w jakikolwiek inny sposób, który jest uważany przez osobę, której dane dotyczą, za prostszy. W dzisiejszym społeczeństwie informacyjnym najprawdopodobniej najprostszym sposobem na wycofanie zgody jest zwykła wiadomość e-mail. Jeżeli osoba, której dane dotyczą, pragnie wycofać udzieloną nam zgodę, wystarczy zwykła wiadomość e-mail


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

wysłana do naszego inspektora ochrony danych. Alternatywnie osoba, której dane dotyczą, może wybrać inny sposób powiadomienia nas o wycofaniu swojej zgody.

## K. Informacje o prawie wniesienia skargi do organu nadzorczego (art. 14 ust. 2 lit. e, art. 77 ust. 1 RODO)

Jako administrator jesteśmy zobowiązani powiadomić osobę, której dane dotyczą, o prawie do wniesienia skargi do organu nadzorczego (art. 13 ust. 2. lit. d RODO). Prawo do wniesienia skargi do organu nadzorczego reguluje art. 77 ust. 1 RODO. Zgodnie z jego treścią, bez uszczerbku dla innych administracyjnych lub środków ochrony prawnej przed sądem każda osoba, której dane dotyczą, ma prawo wnieść skargę do organu nadzorczego, w szczególności w państwie członkowskim swojego zwykłego pobytu, swojego miejsca pracy lub miejsca popełnienia domniemanego naruszenia, jeżeli sądzi, że przetwarzanie danych osobowych jej dotyczące narusza rozporządzenie ogólne rozporządzenie o ochronie danych. Prawo do wniesienia skargi do organu nadzorczego zostało ograniczone prawem Unii w taki sposób, że może ono być wykonywane tylko przed jednym organem nadzorującym (ust. 141 zdanie 1 preambuły RODO). Ta reguła ma na celu uniknięcie podwójnych skarg niniejszej samej osoby, której dane dotyczą, w niniejszej samej sprawie. Jeżeli osoba, której dane dotyczą, chce złożyć na nas skargę, prosimy o kontakt tylko z jednym organem nadzorczym.

## L. Źródło pochodzenia danych osobowych, a gdy ma to zastosowanie – czy pochodzą one ze źródeł publicznie dostępnych (art. 14 ust. 2 lit. f RODO)

Zasadniczo dane osobowe są gromadzone bezpośrednio od osoby, której dane dotyczą lub we współpracy z organem (np. pobieranie danych z rejestru urzędowego). Inne dane osób, których dane dotyczą, pochodzą z przeniesień w ramach spółek grupy. W kontekście tych ogólnych informacji wskazanie z nazwy dokładnych źródeł pochodzenia danych osobowych jest niemożliwe lub wymagałoby nieproporcjonalnego wysiłku w rozumieniu art. 14 ust. 5 lit. b RODO. Co do zasady nie zbieramy danych osobowych z publicznie dostępnych źródeł.

Każda osoba, której dane dotyczą, może w każdej chwili skontaktować się z naszym inspektorem ochrony danych w celu uzyskania bardziej szczegółowych informacji na temat dokładnych źródeł danych osobowych, które jej dotyczą. Jeżeli osobie, której dane dotyczą, nie można podać pochodzenia danych osobowych, ponieważ korzystano z różnych źródeł, informacje należy przedstawić w sposób ogólny (ust. 61 zdanie 4 preambuły RODO).


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

### M. Informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, o którym mowa w art. 22 ust. 1 i 4, oraz – przynajmniej w tych przypadkach – istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą (art. 14 ust. 2 lit. g RODO)

Jako odpowiedzialna firma zazwyczaj nie stosujemy zautomatyzowanego podejmowania decyzji ani profilowania. Jeśli w wyjątkowych przypadkach przeprowadzimy zautomatyzowane podejmowanie decyzji lub profilowanie, poinformujemy o tym osobę, której dane dotyczą, osobno lub za pośrednictwem podsekcji w naszej polityce prywatności (na naszej stronie internetowej). W takim przypadku obowiązują następujące zasady:

Zautomatyzowane podejmowanie decyzji - w tym profilowanie - może mieć miejsce, jeżeli (1) jest to niezbędne do zawarcia lub wykonania umowy między osobą, której dane dotyczą, a nami lub (2) jest to dozwolone prawem Unii lub prawem państwa członkowskiego, któremu podlegamy i które przewiduje również odpowiednie środki ochrony praw i wolności oraz prawnie uzasadnionych interesów osoby, której dane dotyczą; lub (3) odbywa się to na podstawie wyraźnej zgody osoby, której dane dotyczą.

W przypadkach, o których mowa w art. 22 ust. 2 lit. a) i c) RODO, wdrażamy odpowiednie środki w celu ochrony praw i wolności oraz uzasadnionych interesów osoby, której dane dotyczą. W takich przypadkach użytkownik ma prawo do uzyskania interwencji ludzkiej ze strony administratora, wyrażenia swojego punktu widzenia i zakwestionowania decyzji.

Istotne informacje na temat zastosowanej logiki, a także znaczenia i przewidywanych konsekwencji takiego przetwarzania dla osoby, której dane dotyczą, są określone w naszej polityce prywatności.

## III. EU-U.S. Data Privacy Framework (EU-U.S. DPF), UK Extension to the EU-U.S. DPF, Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF)

Jeśli nasza organizacja jest certyfikowanym członkiem EU-U.S. Data Privacy Framework (EU-U.S. DPF) i/lub UK Extension to the EU-U.S. DPF i/lub Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF), obowiązują następujące zasady:

Przestrzegamy EU-U.S. Data Privacy Framework (EU-U.S. DPF) i UK Extension to the EU-U.S. DPF oraz Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF), jak określono przez U.S. Department of Commerce. Nasza firma potwierdziła w Departamencie Handlu USA, że przestrzega EU-U.S. Data Privacy Framework Principles (EU-U.S. DPF Principles) w odniesieniu do przetwarzania danych osobowych, które otrzymuje z Unii Europejskiej i Wielkiej Brytanii, odwołując się do EU-U.S. DPF i UK Extension to the EU-U.S. DPF. Nasza firma potwierdziła w Departamencie Handlu USA, że przestrzega Swiss-U.S. Data Privacy Framework Principles (Swiss-U.S. DPF Principles) w odniesieniu do


© All rights reserved by Heiko Maniero.

przetwarzania danych osobowych, które otrzymuje ze Szwajcarii, odwołując się do Swiss-U.S. DPF. W przypadku sprzeczności między postanowieniami naszej polityki prywatności a EU-U.S. DPF Principles i/lub Swiss-U.S. DPF Principles, nadrzędne są Principles.

Aby dowiedzieć się więcej o programie Data Privacy Framework (DPF) oraz aby zobaczyć nasze certyfikaty, prosimy odwiedzić stronę https://www.dataprivacyframework.gov/.

Inne jednostki lub spółki zależne naszej firmy w USA, które również przestrzegają EU-U.S. DPF Principles, w tym UK Extension to the EU-U.S. DPF oraz Swiss-U.S. DPF Principles, jeśli istnieją, są wymienione w naszej polityce prywatności.

Zgodnie z EU-U.S. DPF i UK Extension to the EU-U.S. DPF oraz Swiss-U.S. DPF, nasza firma zobowiązuje się do współpracy z organami ochrony danych UE oraz Information Commissioner's Office (ICO) w Wielkiej Brytanii oraz Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) w Szwajcarii, i do przestrzegania ich zaleceń w odniesieniu do nierozwiązanych skarg dotyczących naszego postępowania z danymi osobowymi, które otrzymaliśmy, odwołując się do EU-U.S. DPF oraz UK Extension to the EU-U.S. DPF i Swiss-U.S. DPF.

Informujemy osoby, których dane dotyczą, o odpowiednich europejskich organach ochrony danych, które są odpowiedzialne za przetwarzanie skarg dotyczących postępowania naszej organizacji z danymi osobowymi, w górnej części tego dokumentu przejrzystości oraz o tym, że oferujemy odpowiednie i bezpłatne środki ochrony prawnej.

Informujemy wszystkie osoby, których dane dotyczą, że nasza firma podlega uprawnieniom dochodzeniowym i egzekucyjnym Federal Trade Commission (FTC).

Osoby, których dane dotyczą, mają pod pewnymi warunkami możliwość skorzystania z wiążącego arbitrażu. Nasza organizacja zobowiązana jest do rozstrzygania roszczeń i przestrzegania warunków zgodnie z załącznikiem I DPF Principles, jeśli osoba, której dane dotyczą, zażądała wiążącego arbitrażu, powiadamiając naszą organizację i przestrzegając procedur oraz warunków zgodnie z załącznikiem I Principles.

Informujemy tutaj wszystkie osoby, których dane dotyczą, o odpowiedzialności naszej organizacji w przypadku przekazania danych osobowych stronom trzecim.

W przypadku pytań osób, których dane dotyczą, lub organów ochrony danych, wyznaczyliśmy lokalnych przedstawicieli, których nazwy znajdują się w górnej części tego dokumentu przejrzystości.

Oferujemy Państwu możliwość wyboru (Opt-out), czy Państwa dane osobowe (i) mają zostać przekazane stronom trzecim, czy (ii) mają zostać użyte do celu, który znacząco różni się od celu/ów, dla którego/których zostały pierwotnie zebrane lub później zatwierdzone przez Państwa. Wyraźny, dobrze widoczny i łatwo dostępny mechanizm do wykonania prawa wyboru polega na skontaktowaniu się z naszym Inspektorem Ochrony Danych (DSB) poprzez e-mail. Nie mają Państwo możliwości wyboru i nie jesteśmy do tego zobowiązani, jeśli dane są przekazywane stronie trzeciej, która działa jako pełnomocnik


© All rights reserved by Heiko Maniero.

lub przetwarzający na naszą rzecz i zgodnie z naszymi instrukcjami. Zawsze jednak zawieramy umowę z takim pełnomocnikiem lub przetwarzającym.

W przypadku danych wrażliwych (tj. danych osobowych zawierających informacje o stanie zdrowia, pochodzeniu rasowym lub etnicznym, poglądach politycznych, przekonaniach religijnych lub filozoficznych, członkostwie w związkach zawodowych lub danych dotyczących życia seksualnego osoby, której dane dotyczą), uzyskujemy Państwa wyraźną zgodę (Opt-in), jeśli te dane (i) mają zostać przekazane stronom trzecim, czy (ii) mają zostać użyte do innego celu niż ten, dla którego zostały pierwotnie zebrane lub dla którego później wyrazili Państwo zgodę, dokonując wyboru Opt-in. Ponadto, traktujemy wszystkie dane osobowe, które otrzymujemy od stron trzecich, jako wrażliwe, jeśli strona trzecia je zidentyfikowała i traktowała jako wrażliwe.

Informujemy Państwa o konieczności ujawnienia danych osobowych w odpowiedzi na legalne żądania władz, w tym w celu spełnienia wymogów bezpieczeństwa narodowego lub egzekwowania prawa.

Podczas przekazywania danych osobowych stronie trzeciej, która działa jako administrator, przestrzegamy Principles powiadamiania i wyboru. Ponadto, zawieramy umowę z administratorem, która przewiduje, że dane te mogą być przetwarzane wyłącznie do ograniczonych i określonych celów zgodnie z Państwa zgodą, i że odbiorca zapewnia ten sam poziom ochrony, co Principles DPF, i powiadamia nas, jeśli stwierdzi, że nie jest już w stanie spełnić tego zobowiązania. Umowa przewiduje, że administrator zaprzestanie przetwarzania lub podejmie inne odpowiednie i właściwe środki zaradcze, jeśli stwierdzi, że nie jest w stanie spełnić swojego zobowiązania.

Podczas przekazywania danych osobowych stronie trzeciej, która działa jako pełnomocnik lub przetwarzający, (i) przekazujemy te dane wyłącznie do ograniczonych i określonych celów; (ii) upewniamy się, że pełnomocnik lub przetwarzający zobowiązany jest zapewnić co najmniej ten sam poziom ochrony danych, jaki wymagają DPF Principles; (iii) podejmujemy odpowiednie i właściwe środki, aby upewnić się, że pełnomocnik lub przetwarzający faktycznie przetwarza przekazane dane osobowe w sposób zgodny z naszymi zobowiązaniami zgodnie z DPF Principles; (iv) wymagamy od pełnomocnika lub przetwarzającego, aby powiadomił naszą organizację, jeśli stwierdzi, że nie może już spełnić swojego zobowiązania do zapewnienia tego samego poziomu ochrony, jaki wymagają DPF Principles; (v) po otrzymaniu powiadomienia, w tym zgodnie z (iv), podejmujemy odpowiednie i właściwe kroki, aby zatrzymać nieautoryzowane przetwarzanie i zapewnić środki zaradcze; oraz (vi) dostarczamy DPF Department na żądanie streszczenie lub reprezentatywny egzemplarz odpowiednich postanowień umowy dotyczących ochrony danych z tym pełnomocnikiem.

Zgodnie z EU-U.S. DPF i/lub UK Extension to the EU-U.S. DPF i/lub Swiss-U.S. DPF, nasza firma zobowiązuje się do współpracy z organem utworzonym przez europejskie organy ochrony danych oraz Information Commissioner's Office (ICO) w Wielkiej Brytanii lub Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) w Szwajcarii oraz do przestrzegania ich zaleceń w odniesieniu do nierozwiązanych skarg dotyczących naszego postępowania z danymi osobowymi, które otrzymujemy,


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

odwołując się do EU-U.S. DPF oraz UK Extension to the EU-U.S. DPF i Swiss-U.S. DPF w kontekście relacji pracowniczych.

Wszystkim osobom, których dane dotyczą, przebywającym tymczasowo w Unii Europejskiej (UE), Europejskim Obszarze Gospodarczym (EOG) lub Zjednoczonym Królestwie lub mającym tam miejsce zamieszkania lub zwykłego pobytu, przysługują prawa i uprawnienia osoby, której dane dotyczą, opublikowane w naszym dokumencie dotyczącym przejrzystości, które wynikają również z art. 15-22 RODO, w tym prawo dostępu do danych osobowych. Udostępniliśmy te informacje we wszystkich językach UE i EOG. Angielska wersja językowa dotyczy Wielkiej Brytanii.

Wszystkim osobom, których dane dotyczą, które tymczasowo przebywają w Szwajcarii lub mają tam miejsce zamieszkania lub zwykłego pobytu, przysługują prawa i uprawnienia osoby, której dane dotyczą, wynikające ze szwajcarskiej ustawy o ochronie danych (DPA) i szwajcarskiego rozporządzenia o ochronie danych (DPR), które zostały opublikowane w naszym Dokumencie przejrzystości, w tym prawo dostępu do danych osobowych. Udostępniliśmy te informacje w trzech językach urzędowych Szwajcarii (niemieckim, włoskim i francuskim).


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

# HUNGARIAN: Információk személyes adatok kezeléséről (GDPR 13., 14. cikk)

Kedves Hölgyem/Uram!

Minden olyan személy személyes adata, aki szerződéses, szerződésen kívüli vagy egyéb kapcsolatban áll vállalatunkkal, különleges védelmet érdemel. A célunk az, hogy magas szintű adatvédelmet biztosítsunk. Ezért rutinszerűen fejlesztjük adatvédelmi és adatbiztonsági elveinket.

Természetesen megfelelünk az adatvédelemre vonatkozó jogszabályi előírásoknak. A GDPR 13., 14. cikke értelmében a vállatok specifikus tájékoztatási követelményeket teljesítenek személyes adatok gyűjtésekor. Ez a dokumentum teljesíti ezt a kötelezettséget.

A jogszabályok terminológiája bonyolult. Sajnos a jogi szakkifejezések használata elengedhetetlen jelen dokumentum elkészítésekor. Ezért szeretnénk felhívni a figyelmet arra, hogy mindig bátran lépjen kapcsolatba az adatvédelmi tisztviselővel a jelen dokumentummal, a használt kifejezésekkel vagy megfogalmazásokkal kapcsolatos minden kérdésben.

## I. Az adatszolgáltatási követelményeknek való megfelelés, ha a személyes adatokat az érintettől gyűjtik (a GDPR 13. cikke)

### A. Az adatkezelő személyazonossága és kapcsolattartási adatai (GDPR 13. cikk (1) bekezdés a) pont)

Lásd feljebb

### B. Az adatvédelmi tisztviselő kapcsolattartási adatai (GDPR 13. cikk (1) bekezdés b) pont)

Lásd feljebb

### C. Az adatkezelés célja, amelyre a személyes adatok szolgálnak, valamint az adatkezelés jogalapja (a GDPR 13. cikk (1) bekezdésének c) pontja)

A személyes adatok kezelésének célja minden olyan művelet, amely az adatkezelőre, az ügyfelekre, a leendő ügyfelekre, az üzleti partnerekre, a (legtágabb értelemben vett) csoportok között létrejövő más


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

szerződéses vagy szerződésen kívüli kapcsolatokra, vagy az adatkezelő jogi kötelezettségeire vonatkozik.

A GDPR 6. cikkének (1) bekezdése szolgál jogalapként az adatkezelési műveletekhez, amelyekhez az adott adatkezelési cél vonatkozásában hozzájárulást kaptunk. Ha a személyes adatok feldolgozása szükséges a szerződés teljesítéséhez, amelynek az érintett is részese, például az adatkezelés az áruk kiszállításához vagy más szolgáltatásnyújtáshoz szükséges, akkor az adatkezelés alapja a GDPR 6. cikkének (1) bekezdése. Ugyanez vonatkozik a szerződést megelőző intézkedések biztosításához szükséges adatkezelési műveletekre is, például a termékeinket vagy szolgáltatásainkat érintő érdeklődés esetén. Vállalatunkra vonatkozó jogi kötelezettség miatt a személyes adatok kezelése kötelező, például adózási kötelezettségeink teljesítéséhez, az adatkezelés jogalapja ebben az esetben a GDPR 6. cikk (1) bekezdés c) pontja.

Ritka esetekben a személyes adatok feldolgozása az érintett vagy más természetes személy létfontosságú érdekeinek védelme érdekében szükséges. Ez állna fenn például akkor, ha egy látogató megsérülne a vállalatunknál, és nevét, életkorát, egészségbiztosítási adatait vagy egyéb fontos információkat továbbítanánk az orvosnak, kórháznak vagy más harmadik félnek. Majd az adatkezelés a GDPR 6. cikk (1) bekezdés d) pontja alapján történne.

Amennyiben az adatkezelés közérdekből vagy az adatkezelőre ruházott közhatalmi jogosítványok gyakorlása során végzett feladat végrehajtásához szükséges, a jogalap az GDPR 6. cikk (1) bekezdés e) pontja.

Végül az adatkezelési műveletek a GDPR 6. cikk (1) bekezdés f) pontjában foglaltakon alapulnának. Ez a jogalap azon adatkezelési műveletekre vonatkozik, amelyekre a fent említett jogalapok egyike sem, amennyiben az adatkezelés vállalatunk vagy egy harmadik fél jogos érdekében szükséges, kivéve, ha azok az érdekek felülírják annak az érintettnek az érdekeit, alapvető jogait és szabadságát, akinek személyes adatait meg kell védeni. Az ilyen adatkezelési műveletek különösen megengedhetők, mivel azokat az európai jogalkotó kifejezetten említi. Úgy ítéli meg, hogy jogos érdeket feltételezhet, ha az érintett az adatkezelő ügyfele (GDPR bevezetés 47. pont 2. mondat).

## D. Ha az adatkezelés a GDPR 6. cikk (1) bekezdésének f) pontján alapul az adatkezelő vagy harmadik fél jogos érdekei alapján (GDPR 13. cikk (1) bekezdés d) pont)

Ha a személyes adatok kezelése a GDPR 6. cikk (1) bekezdés f) pontján alapul, a mi jogos érdekünk az üzleti tevékenység folytatása alkalmazottaink és részvényeseink jóléte érdekében.

## E. Személyes adatok címzettjeinek kategóriái (GDPR 13. cikk (1) bekezdés e) pont)


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

Közhatalmi szervek

Külső szervek

További külső szervek

Belső adatkezelés

Csoportok közötti adatkezelés

Egyéb szervek

A harmadik országokban működő adatfeldolgozóink és adatátvevőink, valamint adott esetben nemzetközi szervezetek listáját vagy közzétesszük a weboldalunkon, vagy ingyenesen kérhető tőlünk. Kérjük, lépjen kapcsolatba adatvédelmi tisztviselőnkkel a lista igényléséhez.

## F. Harmadik országban lévő címzettek és megfelelő vagy alkalmas biztosítékok és eszközök, amelyekkel másolatot lehet szerezni róluk, vagy ahol rendelkezésre bocsájtották őket (GDPR 13. cikk (1) bek. f) pont, 46. cikk (1) bek., 46. cikk (2) bek. c) pont)

Minden olyan csoportunkat alkotó vállalat és fiókiroda (továbbiakban „csoportvállalatok”), amely harmadik országban folytat üzleti tevékenységet vagy ott tart fenn irodát, lehet címzettje a személyes adatoknak.

A GDPR 46. cikk (1) bekezdése szerint az adatkezelő vagy adatfeldolgozó csak akkor továbbíthat személyes adatokat harmadik országba, ha az adatkezelő vagy adatfeldolgozó megfelelő biztosítékokat nyújt, ha az érintett jogai kikényszeríthetők és rendelkezésre állnak jogorvoslati lehetőségek az érintettek részére. Megfelelő biztosítékokat lehet nyújtani a felügyeleti hatóság külön engedélye nélkül is szabványos szerződéses záradékok segítségével (GDPR 46. cikk (2) bek. c) pont).

Az Európai Unió szabványos szerződéses záradékait a személyes adatok első továbbítása előtt kötött megállapodás biztosítja minden harmadik országban tartózkodó címzett esetén. Ennek következtében megfelelő biztosítékok, az érintett kikényszeríthető jogai és hatályos jogorvoslati lehetőségek biztosíthatók az érintett számára, amelyeket az EU szabványos szerződéses záradékai garantálnak. Az érintettek a szabványos szerződéses záradékokról másolatot kaphatnak az adatvédelmi tisztviselőtől. A szabványos szerződéses záradékok elérhetők az Európai Unió hivatalos lapjában.

Az általános adatvédelmi rendelet (GDPR) 45. cikkének (3) bekezdése biztosítja az Európai Bizottság számára azt a jogot, hogy végrehajtási jogi aktus útján döntsön arról, hogy egy Unión kívüli ország megfelelő szintű védelmet biztosít-e. Ez a személyes adatok védelmének olyan szintjét jelenti, amely nagyjából egyenértékű az uniós védelemmel. A megfelelő szintű védelmet megállapító határozatok azt eredményezik, hogy a személyes adatok szabadon, további akadályok nélkül áramolhatnak az EU-ból


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

(valamint Norvégiából, Liechtensteinből és Izlandról) egy harmadik országba. Hasonló szabályok vonatkoznak az Egyesült Királyságban, Svájcban és néhány más országban is.

Abban az esetben, ha az Európai Bizottság vagy egy másik ország kormánya úgy dönt, hogy egy harmadik ország megfelelő szintű védelmet biztosít, és az alkalmazandó keretrendszer (pl. az EU-U.S. Data Privacy Framework, Swiss-U.S. Data Privacy Framework, UK Extension to the EU-U.S. Data Privacy Framework), az ilyen keretrendszerek tagjainak (pl. önhitelesített szervezetek) történő valamennyi adattovábbításunk kizárólag az adott szervezetek adott keretrendszerben való tagságán alapul. Abban az esetben, ha mi vagy csoportunk valamelyik tagja tagja az ilyen keretrendszereknek, a nekünk vagy csoportunk valamelyik tagjának történő minden adattovábbítás kizárólag a tagságon alapul.

A keretrendszerek egy példányát bármely érintett megkaphatja tőlünk. A keretszabályok ezen túlmenően az Európai Unió Hivatalos Lapjában vagy a közzétett jogi anyagokban, illetve a felügyeleti hatóságok vagy más illetékes hatóságok vagy intézmények weboldalain is elérhetők.

## G. A személyes adatok tárolásának időtartama, vagy ha az nem lehetséges, az időtartam meghatározására szolgáló kritériumok (GDPR 13. cikk (2) bek. a) pont)

A személyes adatok tárolási időtartamának megadására vonatkozó kritériumokat a törvény által előírt megőrzési idő határozza meg. Az adott időtartamot követően az adatok rutinszerűen törlésre kerülnek, amennyiben azok már nem szükségesek a szerződés teljesítéséhez vagy a szerződés megkötéséhez.

Ha nincs jogszabályban előírt megőrzési időszak, akkor a kritérium a szerződéses vagy belső megőrzési időszak.

## H. Az érintett joga a személyes adatok hozzáférését, helyesbítését vagy törlését, azok korlátozott feldolgozását kérni az adatkezelőtől, tiltakozni az adatkezelés ellen, illetve az adathordozhatósághoz való jog (GDPR 13. cikk (2) bek. b) pont)

Minden érintett az alábbi jogokkal rendelkezik:

***Hozzáféréshez való jog***

Minden érintettnek joga van hozzáférni az őt érintő személyes adatokhoz. A hozzáférés joga kiterjed minden általunk kezelt adatra. Ez a jog könnyen és ésszerű időközönként gyakorolható az adatkezelés megismerése, és törvényességének ellenőrzése érdekében (GDPR Bevezetés 63. pont) Ezt a jogot a GDPR 15. cikke biztosítja. Az érintett felveheti a kapcsolatot az adatvédelmi tisztviselőnkkel, ha szeretne élni a hozzáférés jogával.

***Helyesbítés joga***

A GDPR 16. cikk 1. mondata értelmében az érintettnek joga van, hogy kérje az adatkezelőt, hogy indokolatlan késedelem nélkül helyesbítse az őt érintő pontatlan személyes adatokat. Ezen kívül a GDPR


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

16. cikk 2. mondata biztosítja, hogy az érintett jogosult – figyelembe véve az adatkezelés céljait – a hiányos adatok pótlását kérni beleértve a kiegészítő nyilatkozattal való biztosítást is. Az érintett felveheti a kapcsolatot az adatvédelmi tisztviselőnkkel, ha szeretne élni a helyesbítés jogával.

***Törléshez való jog („elfeledtetéshez való jog")***

Ezen kívül az érintettek jogosultak a törléshez és elfeledtetéshez való jog gyakorlására a a GDPR 17. cikke értelmében. Az érintett élhet ezzel a jogával, ha felveszi a kapcsolatot adatvédelmi tisztviselőnkkel. Ezen a ponton azonban szeretnénk rámutatni arra, hogy ez a jog nem alkalmazandó, amennyiben az adatkezelés ránk vonatkozó jogi kötelezettség teljesítéséhez szükséges GDPR 17. cikk (3) bek. b) pont. Ez azt jelenti, hogy a törlésre vonatkozó kérelmet csak a törvényi előírás szerinti megőrzési időszak lejáratát követően tudjuk jóváhagyni.

***Adatkezelés korlátozásához való jog***

A GDPR 18. cikke szerint minden érintett jogosult az adatkezelés korlátozására. Ha az adatkezelés korlátozását akkor lehet kérni, ha a GDPR 18. cikk (1) bek. a-d) pontjában meghatározott feltételek valamelyike teljesül. Az érintett felveheti a kapcsolatot az adatvédelmi tisztviselőnkkel, ha szeretne élni az adatkezelés korlátozásának jogával.

***Tiltakozáshoz való jog***

Továbbá a GDPR 21. cikke biztosítja a tiltakozáshoz való jogot. Az érintett felveheti a kapcsolatot az adatvédelmi tisztviselőnkkel, ha szeretne élni a tiltakozáshoz való jogával.

***Adathordozhatóság joga***

A GDPR 20. cikke biztosítja az adathordozhatóság jogát az érintettnek. E rendelkezés értelmében az érintettnek a GDPR 20. cikk (1) bekezdésének a) és b) pontjában meghatározott feltételek szerint joga van, hogy megkapja az őt érintő, adatkezelő részére átadott személyes adatokat egy strukturált, általánosan használt és gépileg olvasható formában, és joga van arra, hogy ezeket az adatokat egy másik adatkezelőnek akadály nélkül továbbítsa attól az adatkezelőtől, akinek a személyes adatokat megadta. Az érintett felveheti a kapcsolatot az adatvédelmi tisztviselőnkkel, ha szeretne élni az adathordozhatóság jogával.

## I. A hozzájárulás bármikor történő visszavonásának joga a hozzájáruláson alapuló adatfeldolgozás törvényességét a visszavonás előtt nem érintve, ahol az adatkezelés a GDPR 6. cikk (1) bekezdés a) pontján vagy a GDPR 9. cikk (2) bekezdés a) pontján (GDPR 13. cikk (2) bek. c) pontja) alapul

Ha a személyes adatok kezelése a GDPR 6. cikk (1) bekezdés a) pontja szerint történik, amennyiben az érintett hozzájárulását adta a személyes adatok kezeléséhez egy vagy több célból, vagy a GDPR 9. cikk (2) bekezdés a) pontján alapul, amely a személyes adatok speciális kategóriáinak kezeléséhez való kifejezett hozzájárulást szabályozza, akkor az érintettnek joga van a GDPR 7. cikk (3) bek. 1. mondat értelmében bármikor visszavonni a hozzájárulását.


© All rights reserved by Heiko Maniero.

A hozzájárulás visszavonása nem érinti a visszavonás előtti, hozzájáruláson alapuló adatkezelés törvényességét a GDPR 7. cikk (3) bek. 2. mondat értelmében. A hozzájárulás visszavonása olyan egyszerű, mint a hozzájárulás megadása (GDPR 7. cikk (3) bekezdés 4. mondat). Ezért a hozzájárulás visszavonása mindig a hozzájárulás megadásával megegyező módon történik, vagy más módon, ha az érintett számára az egyszerűbb. Napjaink információs társadalmában talán a hozzájárulás visszavonásának legegyszerűbb módja az e-mail küldés. Ha az érintett szeretné visszavonni a nekünk megadott hozzájárulását, akkor elegendő, ha küld egy e-mail üzenetet az adatvédelmi tisztviselőnknek. De az érintett választhat más módot is a hozzájárulása visszavonásához.

## J. Panasz felügyeleti hatósághoz való benyújtásának joga (GDPR 13. cikk (2) bekezdés d) pont, 77. cikk (1) bekezdés)

Adatkezelőként kötelesek vagyunk értesíteni az érintettet arról, hogy joga van panaszt benyújtani a felügyeleti hatósághoz (GDPR 13. cikk (2) bek. d) pont). A panasz felügyeleti hatósághoz való benyújtásának jogát a GDPR 77. cikk (1) bekezdése szabályozza. E rendelkezés értelmében bármely más közigazgatási vagy bírósági jogorvoslat sérelme nélkül minden érintettnek joga van panaszt benyújtani egy felügyeleti hatósághoz, a szokásos tartózkodási helye, munkahelye vagy az állítólagos jogsértés helye szerinti tagállamban, ha az érintett úgy ítéli meg, hogy az őt érintő személyes adatok feldolgozása sérti az Általános adatvédelmi szabályozást. A panasz felügyeleti hatósághoz való benyújtásának jogát az Unió törvénye szabályozza olyan módon, hogy az kizárólag egyetlen felügyeleti hatósággal szemben gyakorolható (GDPR Bevezetés 141. pont, 1. mondat). Ennek a szabálynak a célja, hogy kizárja, hogy az ugyanaz az érintett ugyanabban az ügyben dupla panaszt nyújtson be. Ha az érintett panaszt szeretne benyújtani velünk szemben, kérjük, hogy azt csak egyetlen felügyeleti hatóságnál tegye meg.

## K. Személyes adatok biztosítása törvényi vagy szerződéses követelményként; A szerződés megkötéséhez szükséges követelmény; Az érintett kötelezettsége a személyes adatok biztosítása érdekében; az ilyen adatok nem teljesítésének lehetséges következményei (GDPR 13. cikk (2) bekezdés e) pontja).

Tisztázzuk, hogy a személyes adatok megadása részben törvényi okokból (pl.: adószabályok), vagy részben szerződéses rendelkezések miatt szükséges (pl.: a szerződő fél adatai).

Néha szükséges lehet szerződés kötésére, hogy az érintett személyes adatokat adjon át nekünk, amelyeket később mi kezelünk. Az érintett például személyes adatokat ad át vállalatunknak, amikor aláírunk vele egy szerződést. Ha az érintett nem adna át személyes adatokat, akkor a szerződést nem tudnánk megkötni.

Mielőtt az érintett személyes adatokat adna meg, az érintettnek fel kell vennie a kapcsolatot az adatvédelmi tisztviselővel. Adatvédelmi tisztviselőnk tisztázza az érintettel, hogy a személyes adatok


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

megadására törvényi vagy szerződéses okokból van szükség, vagy a szerződés megkötéséhez szükséges, illetve, hogy kötelezettsége van a személyes adatok megadására, és milyen következményekkel jár a személyes adatok megadásának megtagadása.

### L. A GDPR 22. cikkének (1) és (4) bekezdésében említett automatizált döntéshozatal, ideértve a profilalkotást is, és legalábbis ezekben az esetekben az értelmezhető logikával kapcsolatos lényeges információk, valamint az ilyen adatkezelés megvalósításának jelentősége és tervezett következményei az érintett számára (GDPR 13. cikk (2) bekezdés f) pont).

Felelős vállalatként általában nem alkalmazunk automatizált döntéshozatalt vagy profilalkotást. Ha kivételes esetekben automatizált döntéshozatalt vagy profilalkotást végzünk, erről külön vagy az adatvédelmi szabályzatunkban (a weboldalunkon) található alfejezeten keresztül tájékoztatjuk az érintettet. Ebben az esetben a következők érvényesek:

Automatizált döntéshozatalra - ideértve a profilalkotást is - akkor kerülhet sor, ha (1) ez szükséges az érintett és köztünk létrejött szerződés megkötéséhez vagy teljesítéséhez, vagy (2) ezt az érintett jogainak és szabadságainak, valamint jogos érdekeinek védelmét szolgáló megfelelő intézkedéseket is előíró uniós vagy tagállami jog engedélyezi, amelynek hatálya alá tartozunk; vagy (3) ez az érintett kifejezett hozzájárulásán alapul.

A GDPR 22. cikk (2) bekezdésének a) és c) pontjában említett esetekben megfelelő intézkedéseket hajtunk végre az érintett jogainak és szabadságainak, valamint jogos érdekeinek védelme érdekében. Ezekben az esetekben Ön jogosult arra, hogy az adatkezelő részéről emberi beavatkozást kérjen, kifejtse álláspontját és megtámadja a döntést.

Az érintett logikáról, valamint az adatkezelés jelentőségéről és az érintettre gyakorolt várható következményeiről az adatvédelmi szabályzatunkban találhatók érdemi információk.

## II. Az adatszolgáltatási követelményeknek való megfelelés, ha a személyes adatokat nem az érintettől gyűjtik (a GDPR 14. cikke)

### A. Az adatkezelő személyazonossága és kapcsolattartási adatai (GDPR 14. cikk (1) bekezdés a) pont)

Lásd feljebb


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## B. Az adatvédelmi tisztviselő kapcsolattartási adatai (GDPR 14. cikk (1) bekezdés b) pont)

Lásd feljebb

## C. Az adatkezelés célja, amelyre a személyes adatok szolgálnak, valamint az adatkezelés jogalapja (a GDPR 14. cikk (1) bekezdésének c) pontja)

A személyes adatok kezelésének célja minden olyan művelet, amely az adatkezelőre, az ügyfelekre, a leendő ügyfelekre, az üzleti partnerekre, a (legtágabb értelemben vett) csoportok között létrejövő más szerződéses vagy szerződésen kívüli kapcsolatokra, vagy az adatkezelő jogi kötelezettségeire vonatkozik.

Ha a személyes adatok feldolgozása szükséges a szerződés teljesítéséhez, amelynek az érintett is részese, például az adatkezelés az áruk kiszállításához vagy más szolgáltatásnyújtáshoz szükséges, akkor az adatkezelés alapja a GDPR 6. cikkének (1) bekezdése. Ugyanez vonatkozik a szerződést megelőző intézkedések biztosításához szükséges adatkezelési műveletekre is, például a termékeinket vagy szolgáltatásainkat érintő érdeklődés esetén. Vállalatunkra vonatkozó jogi kötelezettség miatt a személyes adatok kezelése kötelező, például adózási kötelezettségeink teljesítéséhez, az adatkezelés jogalapja ebben az esetben a GDPR 6. cikk (1) bekezdés c) pontja.

Ritka esetekben a személyes adatok feldolgozása az érintett vagy más természetes személy létfontosságú érdekeinek védelme érdekében szükséges. Ez állna fenn például akkor, ha egy látogató megsérülne a vállalatunknál, és nevét, életkorát, egészségbiztosítási adatait vagy egyéb fontos információkat továbbítanánk az orvosnak, kórháznak vagy más harmadik félnek. Majd az adatkezelés a GDPR 6. cikk (1) bekezdés d) pontja alapján történne.

Amennyiben az adatkezelés közérdekből vagy az adatkezelőre ruházott közhatalmi jogosítványok gyakorlása során végzett feladat végrehajtásához szükséges, a jogalap az GDPR 6. cikk (1) bekezdés e) pontja.

Végül az adatkezelési műveletek a GDPR 6. cikk (1) bekezdés f) pontjában foglaltakon alapulnának. Ez a jogalap azon adatkezelési műveletekre vonatkozik, amelyekre a fent említett jogalapok egyike sem, amennyiben az adatkezelés vállalatunk vagy egy harmadik fél jogos érdekében szükséges, kivéve, ha azok az érdekek felülírják annak az érintettnek az érdekeit, alapvető jogait és szabadságát, akinek személyes adatait meg kell védeni. Az ilyen adatkezelési műveletek különösen megengedhetők, mivel azokat az európai jogalkotó kifejezetten említi. Úgy ítéli meg, hogy jogos érdeket feltételezhet, ha az érintett az adatkezelő ügyfele (GDPR bevezetés 47. pont 2. mondat).

## D. Érintett személyes adatok kategóriái (GDPR 14. cikk (1) bekezdés d) pont)


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

Ügyfél adatai

Potenciális ügyfelek adatai

Alkalmazottak adatai

Beszállítók adatai

## E. Személyes adatok címzettjeinek kategóriái (GDPR 14. cikk (1) bekezdés e) pont)

Közhatalmi szervek

Külső szervek

További külső szervek

Belső adatkezelés

Csoportok közötti adatkezelés

Egyéb szervek

A harmadik országokban működő adatfeldolgozóink és adatátvevőink, valamint adott esetben nemzetközi szervezetek listáját vagy közzétesszük a weboldalunkon, vagy ingyenesen kérhető tőlünk. Kérjük, lépjen kapcsolatba adatvédelmi tisztviselőnkkel a lista igényléséhez.

## F. Harmadik országban lévő címzettek és megfelelő vagy alkalmas biztosítékok és eszközök, amelyekkel másolatot lehet szerezni róluk, vagy ahol rendelkezésre bocsájtották őket (GDPR 14. cikk (1) bek. f) pont, 46. cikk (1) bek., 46. cikk (2) bek. c) pont)

Minden olyan csoportunkat alkotó vállalat és fiókiroda (továbbiakban „csoportvállalatok”), amely harmadik országban folytat üzleti tevékenységet vagy ott tart fenn irodát, lehet címzettje a személyes adatoknak. Minden csoportvállalat címe megtalálható a weboldalunkon www.osigroup.com.

A GDPR 46. cikk (1) bekezdése szerint az adatkezelő vagy adatfeldolgozó csak akkor továbbíthat személyes adatokat harmadik országba, ha az adatkezelő vagy adatfeldolgozó megfelelő biztosítékokat nyújt, ha az érintett jogai kikényszeríthetők és rendelkezésre állnak jogorvoslati lehetőségek az érintettek részére. Megfelelő biztosítékokat lehet nyújtani a felügyeleti hatóság külön engedélye nélkül is szabványos szerződéses záradékok segítségével (GDPR 46. cikk (2) bek. c) pont).


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

Az Európai Unió szabványos szerződéses záradékait a személyes adatok első továbbítása előtt kötött megállapodás biztosítja minden harmadik országban tartózkodó címzett esetén. Ennek következtében megfelelő biztosítékok, az érintett kikényszeríthető jogai és hatályos jogorvoslati lehetőségek biztosíthatók az érintett számára, amelyeket az EU szabványos szerződéses záradékai garantálnak. Az érintettek a szabványos szerződéses záradékokról másolatot kaphatnak az adatvédelmi tisztviselőtől. A szabványos szerződéses záradékok elérhetők az Európai Unió hivatalos lapjában.

Az általános adatvédelmi rendelet (GDPR) 45. cikkének (3) bekezdése biztosítja az Európai Bizottság számára azt a jogot, hogy végrehajtási jogi aktus útján döntsön arról, hogy egy Unión kívüli ország megfelelő szintű védelmet biztosít-e. Ez a személyes adatok védelmének olyan szintjét jelenti, amely nagyjából egyenértékű az uniós védelemmel. A megfelelő szintű védelmet megállapító határozatok azt eredményezik, hogy a személyes adatok szabadon, további akadályok nélkül áramolhatnak az EU-ból (valamint Norvégiából, Liechtensteinből és Izlandról) egy harmadik országba. Hasonló szabályok vonatkoznak az Egyesült Királyságban, Svájcban és néhány más országban is.

Abban az esetben, ha az Európai Bizottság vagy egy másik ország kormánya úgy dönt, hogy egy harmadik ország megfelelő szintű védelmet biztosít, és az alkalmazandó keretrendszer (pl. az EU-U.S. Data Privacy Framework, Swiss-U.S. Data Privacy Framework, UK Extension to the EU-U.S. Data Privacy Framework), az ilyen keretrendszerek tagjainak (pl. önhitelesített szervezetek) történő valamennyi adattovábbításunk kizárólag az adott szervezetek adott keretrendszerben való tagságán alapul. Abban az esetben, ha mi vagy csoportunk valamelyik tagja tagja az ilyen keretrendszereknek, a nekünk vagy csoportunk valamelyik tagjának történő minden adattovábbítás kizárólag a tagságon alapul.

A keretrendszerek egy példányát bármely érintett megkaphatja tőlünk. A keretszabályok ezen túlmenően az Európai Unió Hivatalos Lapjában vagy a közzétett jogi anyagokban, illetve a felügyeleti hatóságok vagy más illetékes hatóságok vagy intézmények weboldalain is elérhetők.

## G. A személyes adatok tárolásának időtartama, vagy ha az nem lehetséges, az időtartam meghatározására szolgáló kritériumok (GDPR 14. cikk (2) bek. a) pont)

A személyes adatok tárolási időtartamának megadására vonatkozó kritériumokat a törvény által előírt megőrzési idő határozza meg. Az adott időtartamot követően az adatok rutinszerűen törlésre kerülnek, amennyiben azok már nem szükségesek a szerződés teljesítéséhez vagy a szerződés megkötéséhez.

Ha nincs jogszabályban előírt megőrzési időszak, akkor a kritérium a szerződéses vagy belső megőrzési időszak.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## H. Értesítés az adatkezelő vagy harmadik jogos érdekeiről, amennyiben az adatkezelés a GDPR 6. cikk (1) bekezdés f) pontja alapján történik (GDPR 14. cikk (2) bekezdés b) pontja).

A GDPR 6. cikk (1) bekezdés f) pontja szerinti adatkezelés csak akkor lehet törvényes, amennyiben az adatkezelés az adatkezelő vagy egy harmadik fél jogos érdekében szükséges, kivéve, ha azok az érdekek felülírják annak az érintettnek az érdekeit, alapvető jogait és szabadságát, akinek személyes adatait meg kell védeni. A GDPR Bevezetés 47. pontjának 2. mondata szerint a jogos érdek fennállhat, ha az érintett és az adatkezelő között releváns és megfelelő kapcsolat van, például ha az érintett az adatkezelő ügyfele. Minden esetben, amikor vállaltunk a személyes adatokat a GDPR 6. cikk (1) bekezdés f) pontja szerint kezeli, a mi jogos érdekünk az üzleti tevékenység folytatása alkalmazottaink és részvényeseink jóléte érdekében.

## I. Az érintett joga a személyes adatok hozzáférését, helyesbítését vagy törlését, azok korlátozott feldolgozását kérni az adatkezelőtől, tiltakozni az adatkezelés ellen, illetve az adathordozhatósághoz való jogát gyakorolni (GDPR 14. cikk (2) bek. c) pont)

Minden érintett az alábbi jogokkal rendelkezik:

***Hozzáféréshez való jog***

Minden érintettnek joga van hozzáférni az őt érintő személyes adatokhoz. A hozzáférés joga kiterjed minden általunk kezelt adatra. Ez a jog könnyen és ésszerű időközönként gyakorolható az adatkezelés megismerése, és törvényességének ellenőrzése érdekében (GDPR Bevezetés 63. pont) Ezt a jogot a GDPR 15. cikke biztosítja. Az érintett felveheti a kapcsolatot az adatvédelmi tisztviselőnkkel, ha szeretne élni a hozzáférés jogával.

***Helyesbítés joga***

A GDPR 16. cikk 1. mondata értelmében az érintettnek joga van, hogy kérje az adatkezelőt, hogy indokolatlan késedelem nélkül helyesbítse az őt érintő pontatlan személyes adatokat. Ezen kívül a GDPR 16. cikk 2. mondata biztosítja, hogy az érintett jogosult – figyelembe véve az adatkezelés céljait – a hiányos adatok pótlását kérni beleértve a kiegészítő nyilatkozattal való biztosítást is. Az érintett felveheti a kapcsolatot az adatvédelmi tisztviselőnkkel, ha szeretne élni a helyesbítés jogával.

***Törléshez való jog („elfeledtetéshez való jog")***

Ezen kívül az érintettek jogosultak a törléshez és elfeledtetéshez való jog gyakorlására a a GDPR 17. cikke értelmében. Az érintett élhet ezzel a jogával, ha felveszi a kapcsolatot adatvédelmi tisztviselőnkkel. Ezen a ponton azonban szeretnénk rámutatni arra, hogy ez a jog nem alkalmazandó, amennyiben az adatkezelés ránk vonatkozó jogi kötelezettség teljesítéséhez szükséges GDPR 17. cikk (3) bek. b) pont. Ez azt jelenti, hogy a törlésre vonatkozó kérelmet csak a törvényi előírás szerinti megőrzési időszak lejáratát követően tudjuk jóváhagyni.


© All rights reserved by Heiko Maniero.

***Adatkezelés korlátozásához való jog***

A GDPR 18. cikke szerint minden érintett jogosult az adatkezelés korlátozására. Ha az adatkezelés korlátozását akkor lehet kérni, ha a GDPR 18. cikk (1) bek. a-d) pontjában meghatározott feltételek valamelyike teljesül. Az érintett felveheti a kapcsolatot az adatvédelmi tisztviselőnkkel, ha szeretne élni az adatkezelés korlátozásának jogával.

***Tiltakozáshoz való jog***

Továbbá a GDPR 21. cikke biztosítja a tiltakozáshoz való jogot. Az érintett felveheti a kapcsolatot az adatvédelmi tisztviselőnkkel, ha szeretne élni a tiltakozáshoz való jogával.

***Adathordozhatóság joga***

A GDPR 20. cikke biztosítja az adathordozhatóság jogát az érintettnek. E rendelkezés értelmében az érintettnek a GDPR 20. cikk (1) bekezdésének a) és b) pontjában meghatározott feltételek szerint joga van, hogy megkapja az őt érintő, adatkezelő részére átadott személyes adatokat egy strukturált, általánosan használt és gépileg olvasható formában, és joga van arra, hogy ezeket az adatokat egy másik adatkezelőnek akadály nélkül továbbítsa attól az adatkezelőtől, akinek a személyes adatokat megadta. Az érintett felveheti a kapcsolatot az adatvédelmi tisztviselőnkkel, ha szeretne élni az adathordozhatóság jogával.

## J. A hozzájárulás bármikor történő visszavonásának joga a hozzájáruláson alapuló adatfeldolgozás törvényességét a visszavonás előtt nem érintve, ahol az adatkezelés a GDPR 6. cikk (1) bekezdés a) pontján vagy a GDPR 9. cikk (2) bekezdés a) pontján alapul (GDPR 14. cikk (2) bekezdés d) pontja)

Ha a személyes adatok kezelése a GDPR 6. cikk (1) bekezdés a) pontja szerint történik, amennyiben az érintett hozzájárulását adta a személyes adatok kezeléséhez egy vagy több célból, vagy a GDPR 9. cikk (2) bekezdés a) pontján alapul, amely a személyes adatok speciális kategóriáinak kezeléséhez való kifejezett hozzájárulást szabályozza, akkor az érintettnek joga van a GDPR 7. cikk (3) bek. 1. mondat értelmében bármikor visszavonni a hozzájárulását.

A hozzájárulás visszavonása nem érinti a visszavonás előtti, hozzájáruláson alapuló adatkezelés törvényességét a GDPR 7. cikk (3) bek. 2. mondat értelmében. A hozzájárulás visszavonása olyan egyszerű, mint a hozzájárulás megadása (GDPR 7. cikk (3) bekezdés 4. mondat). Ezért a hozzájárulás visszavonása mindig a hozzájárulás megadásával megegyező módon történik, vagy más módon, ha az érintett számára az egyszerűbb. Napjaink információs társadalmában talán a hozzájárulás visszavonásának legegyszerűbb módja az e-mail küldés. Ha az érintett szeretné visszavonni a nekünk megadott hozzájárulását, akkor elegendő, ha küld egy e-mail üzenetet az adatvédelmi tisztviselőnknek. De az érintett választhat más módot is a hozzájárulása visszavonásához.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## K. Panasz felügyeleti hatósághoz való benyújtásának joga (GDPR 14. cikk (2) bekezdés e) pont, 77. cikk (1) bekezdés)

Adatkezelőként kötelesek vagyunk értesíteni az érintettet arról, hogy joga van panaszt benyújtani a felügyeleti hatósághoz (GDPR 13. cikk (2) bek. d) pont). A panasz felügyeleti hatósághoz való benyújtásának jogát a GDPR 77. cikk (1) bekezdése szabályozza. E rendelkezés értelmében bármely más közigazgatási vagy bírósági jogorvoslat sérelme nélkül minden érintettnek joga van panaszt benyújtani egy felügyeleti hatósághoz, a szokásos tartózkodási helye, munkahelye vagy az állítólagos jogsértés helye szerinti tagállamban, ha az érintett úgy ítéli meg, hogy az őt érintő személyes adatok feldolgozása sérti az Általános adatvédelmi szabályozást. A panasz felügyeleti hatósághoz való benyújtásának jogát az Unió törvénye szabályozza olyan módon, hogy az kizárólag egyetlen felügyeleti hatósággal szemben gyakorolható (GDPR Bevezetés 141. pont, 1. mondat). Ennek a szabálynak a célja, hogy kizárja, hogy az ugyanaz az érintett ugyanabban az ügyben dupla panaszt nyújtson be. Ha az érintett panaszt szeretne benyújtani velünk szemben, kérjük, hogy azt csak egyetlen felügyeleti hatóságnál tegye meg.

## L. Forrás ahonnan a személyes adatok származnak, és adott esetben a nyilvános elérhető források (ha az adatok onnan származnak) (GDPR 14. cikk (2) bekezdés f) pont)

Elviekben a személyes adatokat közvetlenül az érintettől vagy egy hatósággal együttműködésben gyűjtik (pl.: adatok kinyerése egy hivatalos nyilvántartásból) Az érintettek egyéb adatai a csoportvállalatoktól adattovábbítással érkeznek. Ezen általános információkkal összefüggésben a pontos források megnevezése, amelyekből a személyes adatok származnak, lehetetlen vagy aránytalan erőfeszítéssel járna a GDPR 14. cikk (5) bekezdés b) pontja értelmében. Elméletileg nem gyűjtünk személyes adatokat nyilvánosan hozzáférhető forrásokból.

Az érintettek bármikor felvehetik a kapcsolatot az adatvédelmi tisztviselőnkkel, hogy további információt kapjanak az őket érintő személyes adatok pontos forrásáról. Ha a személyes adatok eredetét nem tudjuk megmondani az érintettnek, mivel több forrásból származnak, akkor általános tájékoztatást kell adnunk (GDPR Bevezetés 61. pont 4. mondat).


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

### M. A GDPR 22. cikkének (1) és (4) bekezdésében említett automatizált döntéshozatal, ideértve a profilalkotást is, és legalábbis ezekben az esetekben az értelmezhető logikával kapcsolatos lényeges információk, valamint az ilyen adatkezelés megvalósításának jelentősége és tervezett következményei az érintett számára (GDPR 14. cikk (2) bekezdés g) pont).

Felelős vállalatként általában nem alkalmazunk automatizált döntéshozatalt vagy profilalkotást. Ha kivételes esetekben automatizált döntéshozatalt vagy profilalkotást végzünk, erről külön vagy az adatvédelmi szabályzatunkban (a weboldalunkon) található alfejezeten keresztül tájékoztatjuk az érintettet. Ebben az esetben a következők érvényesek:

Automatizált döntéshozatalra - ideértve a profilalkotást is - akkor kerülhet sor, ha (1) ez szükséges az érintett és köztünk létrejött szerződés megkötéséhez vagy teljesítéséhez, vagy (2) ezt az érintett jogainak és szabadságainak, valamint jogos érdekeinek védelmét szolgáló megfelelő intézkedéseket is előíró uniós vagy tagállami jog engedélyezi, amelynek hatálya alá tartozunk; vagy (3) ez az érintett kifejezett hozzájárulásán alapul.

A GDPR 22. cikk (2) bekezdésének a) és c) pontjában említett esetekben megfelelő intézkedéseket hajtunk végre az érintett jogainak és szabadságainak, valamint jogos érdekeinek védelme érdekében. Ezekben az esetekben Ön jogosult arra, hogy az adatkezelő részéről emberi beavatkozást kérjen, kifejtse álláspontját és megtámadja a döntést.

Az érintett logikáról, valamint az adatkezelés jelentőségéről és az érintettre gyakorolt várható következményeiről az adatvédelmi szabályzatunkban találhatók érdemi információk.

## III. EU-U.S. Data Privacy Framework (EU-U.S. DPF), UK Extension to the EU-U.S. DPF, Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF)

Amennyiben szervezetünk tanúsított tagja az EU-U.S. Data Privacy Framework (EU-U.S. DPF) és/vagy a UK Extension to the EU-U.S. DPF és/vagy a Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF), az alábbiak érvényesek:

Betartjuk az EU-U.S. Data Privacy Framework (EU-U.S. DPF) és a UK Extension to the EU-U.S. DPF, valamint a Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF) előírásait, ahogyan azt az U.S. Department of Commerce meghatározta. Vállalatunk megerősítette az amerikai kereskedelmi minisztérium számára, hogy betartja az EU-U.S. Data Privacy Framework Principles (EU-U.S. DPF Principles) elveit a személyes adatok feldolgozásával kapcsolatban, amelyeket az Európai Unióból és az Egyesült Királyságból kap az EU-U.S. DPF és a UK Extension to the EU-U.S. DPF alapján. Vállalatunk megerősítette az amerikai kereskedelmi minisztérium számára, hogy betartja a Swiss-U.S. Data Privacy Framework Principles (Swiss-U.S. DPF Principles) elveit a személyes adatok feldolgozásával


© All rights reserved by Heiko Maniero.

kapcsolatban, amelyeket Svájcból kap a Swiss-U.S. DPF alapján. Amennyiben ellentmondás van adatvédelmi nyilatkozatunk és az EU-U.S. DPF Principles és/vagy a Swiss-U.S. DPF Principles rendelkezései között, az elvek az irányadók.

A Data Privacy Framework (DPF) programról és tanúsítványunkról további információkat a https://www.dataprivacyframework.gov/ oldalon talál.

Azok az egyéb amerikai egységek vagy amerikai leányvállalatok, amelyek szintén betartják az EU-U.S. DPF Principles elveit, beleértve a UK Extension to the EU-U.S. DPF és a Swiss-U.S. DPF Principles elveit, amennyiben vannak, adatvédelmi nyilatkozatunkban kerülnek megnevezésre.

Az EU-U.S. DPF, a UK Extension to the EU-U.S. DPF és a Swiss-U.S. DPF előírásaival összhangban vállalatunk kötelezi magát arra, hogy együttműködik az EU adatvédelmi hatóságaival, a brit Information Commissioner's Office-szal (ICO), valamint a svájci Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) hivatallal, és követi azok tanácsait a személyes adatok kezelésével kapcsolatos, megoldatlan panaszok tekintetében, amelyeket az EU-U.S. DPF, a UK Extension to the EU-U.S. DPF és a Swiss-U.S. DPF alapján kapunk.

Tájékoztatjuk az érintett személyeket az illetékes európai adatvédelmi hatóságokról, amelyek felelősek szervezetünk személyes adatok kezelésével kapcsolatos panaszainak feldolgozásáért, ezen átláthatósági dokumentum tetején, valamint arról, hogy megfelelő és ingyenes jogorvoslati lehetőséget kínálunk az érintett személyek számára.

Tájékoztatjuk az összes érintett személyt, hogy vállalatunk a Federal Trade Commission (FTC) vizsgálati és végrehajtási hatáskörébe tartozik.

Az érintett személyek bizonyos körülmények között lehetőséget kapnak kötelező érvényű választottbíráskodás igénybevételére. Szervezetünk köteles rendezni a követeléseket és betartani az I. mellékletben szereplő DPF Principles feltételeit, amennyiben az érintett személy kötelező érvényű választottbíráskodást kér, értesítve szervezetünket és betartva az I. melléklet elveiben szereplő eljárásokat és feltételeket.

Ezúton tájékoztatjuk az összes érintett személyt szervezetünk felelősségéről a személyes adatok harmadik félnek történő továbbítása esetén.

Az érintett személyek vagy adatvédelmi hatóságok kérdései esetén kijelöltük a helyi képviselőket, akiknek neve ezen átláthatósági dokumentum tetején található.

Lehetőséget kínálunk Önnek, hogy döntsön (Opt-out), hogy személyes adatait (i) harmadik félnek továbbítják, vagy (ii) olyan célra használják, amely jelentősen eltér az eredeti céloktól, amelyekre azokat gyűjtötték, vagy később Ön által jóváhagyták. Az Ön választási jogának gyakorlására szolgáló egyértelmű, jól látható és könnyen hozzáférhető mechanizmus az, hogy e-mailben felvegye a kapcsolatot adatvédelmi tisztviselőnkkel (DSB). Nincs választási lehetősége, és nem vagyunk kötelesek erre, ha az


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

adatokat olyan harmadik félnek továbbítják, aki megbízottként vagy feldolgozóként jár el a nevünkben és utasításaink szerint. Mindig szerződést kötünk egy ilyen megbízottal vagy feldolgozóval.

Az érzékeny adatok (azaz az egészségügyi állapotra, a faji vagy etnikai származásra, a politikai véleményekre, a vallási vagy filozófiai meggyőződésekre, a szakszervezeti tagságra vagy a szexuális életre vonatkozó személyes adatok) esetében kifejezett hozzájárulását (Opt-in) kérjük, ha ezeket az adatokat (i) harmadik félnek továbbítják, vagy (ii) más célra használják, mint amelyre eredetileg gyűjtötték, vagy amelyhez később az Opt-in választásával hozzájárult. Ezenkívül minden személyes adatot, amelyet harmadik féltől kapunk, érzékenyként kezelünk, ha a harmadik fél azokat érzékenyként azonosította és kezelte.

Ezúton tájékoztatjuk Önt a személyes adatok hatósági kérésre történő közzétételének szükségességéről, beleértve a nemzetbiztonsági vagy bűnüldözési követelmények teljesítését.

Amikor személyes adatokat harmadik félnek továbbítunk, aki adatkezelőként jár el, betartjuk az értesítési és választási elveket. Emellett szerződést kötünk az adatkezelővel, amely előírja, hogy ezeket az adatokat csak korlátozott és meghatározott célokra szabad feldolgozni az Ön hozzájárulásával összhangban, és hogy a címzett ugyanolyan szintű védelmet biztosít, mint a DPF elvei, és értesít minket, ha úgy találja, hogy már nem tudja teljesíteni ezt a kötelezettséget. A szerződés előírja, hogy az adatkezelő beszünteti az adatkezelést, vagy más megfelelő és megfelelő intézkedéseket tesz a helyrehozás érdekében, ha megállapítást nyer, hogy nem tudja teljesíteni kötelezettségét.

Amikor személyes adatokat továbbítunk harmadik félnek, aki megbízottként vagy feldolgozóként jár el, (i) ezeket az adatokat csak korlátozott és meghatározott célokra továbbítjuk; (ii) meggyőződünk arról, hogy a megbízott vagy feldolgozó köteles biztosítani a DPF elveinek megfelelő adatvédelmi szintet; (iii) megfelelő és megfelelő intézkedéseket teszünk annak biztosítására, hogy a megbízott vagy feldolgozó ténylegesen olyan módon dolgozza fel a továbbított személyes adatokat, amely megfelel a DPF elveinek való megfelelésünkkel; (iv) megköveteljük a megbízottól vagy feldolgozótól, hogy értesítse szervezetünket, ha úgy találja, hogy már nem tudja teljesíteni kötelezettségét a DPF elveinek megfelelő szintű védelem biztosítására; (v) értesítés, beleértve a (iv) pontot, esetén megfelelő és megfelelő lépéseket teszünk az engedély nélküli adatkezelés leállítására és a helyreállítás érdekében; és (vi) a DPF Department kérésére összefoglalót vagy reprezentatív példányt nyújtunk a megbízottal kötött szerződésünk releváns adatvédelmi rendelkezéseiről.

Az EU-U.S. DPF és/vagy a UK Extension to the EU-U.S. DPF és/vagy a Swiss-U.S. DPF előírásainak megfelelően vállalatunk kötelezi magát arra, hogy együttműködik az EU adatvédelmi hatóságaival és a brit Information Commissioner's Office-szal (ICO), valamint a svájci Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) hivatallal, és követi azok tanácsait a személyes adatok kezelésével kapcsolatos, megoldatlan panaszok tekintetében, amelyeket az EU-U.S. DPF, a UK Extension to the EU-U.S. DPF és a Swiss-U.S. DPF alapján kapunk munkaviszonyban.


© All rights reserved by Heiko Maniero.

Minden olyan érintettet, aki ideiglenesen az Európai Unióban (EU), az Európai Gazdasági Térségben (EGT) vagy az Egyesült Királyságban tartózkodik, vagy ott rendelkezik lakóhellyel vagy szokásos tartózkodási hellyel, megilletik az átláthatósági dokumentumunkban közzétett jogok és az érintettek jogai, amelyek a GDPR 15-22. cikkéből is következnek, beleértve a személyes adatokhoz való hozzáférés jogát. Ezt a tájékoztatást az EU és az EGT valamennyi nyelvén elérhetővé tettük. Az angol nyelvű változat az Egyesült Királyságra vonatkozik.

Minden olyan érintettet, aki ideiglenesen Svájcban tartózkodik, vagy ott rendelkezik lakóhellyel vagy szokásos tartózkodási hellyel, megilletnek a svájci adatvédelmi törvény (DPA) és a svájci adatvédelmi rendelet (DPR) szerinti jogok és az érintettek jogai, amelyeket az átláthatósági dokumentumunkban teszünk közzé, beleértve a személyes adatokhoz való hozzáférés jogát. Ezt a tájékoztatást Svájc három hivatalos nyelvén (németül, olaszul és franciául) adtuk meg.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

# HUNGARIAN: A munkavállalók és pályázók személyes adatainak feldolgozásáról szóló információk (GDPR, 13. és 14. cikk)

Tisztelt Hölgyem/Uram!

A munkavállalók és pályázók személyes adatai fokozott védelmet érdemelnek. A célunk az, hogy magas szintű adatvédelmet biztosítsunk. Ezért rutinszerűen fejlesztjük az adatvédelmi és adatbiztonsági gyakorlatainkat.

Természetesen megfelelünk az adatvédelemre vonatkozó jogszabályi előírásoknak. A GDPR 13. és 14. cikke szerint az adatkezelőknek a személyes adatok feldolgozása során speciális tájékoztatási követelményeknek kell megfelelniük. Ez a dokumentum teljesíti az ilyen jellegű kötelezettségeket.

A jogi szabályozás terminológiája meglehetősen bonyolult. Sajnos a jogi szakkifejezések használata elengedhetetlen a jelen dokumentum elkészítésekor. Ezért szeretnénk felhívni a figyelmét arra, hogy mindig szívesen vesszük, ha felkeres bennünket bármilyen, a jelen dokumentummal, a fogalmakkal vagy a megfogalmazással kapcsolatos kérdéssel.

## I. Az adatszolgáltatási követelményeknek való megfelelés, ha a személyes adatokat az érintettől gyűjtik (a GDPR 13. cikke)

### A. Az adatkezelő személyazonossága és kapcsolattartási adatai (GDPR 13. cikk (1) bekezdés a) pont)

Lásd feljebb

### B. Az adatvédelmi tisztviselő kapcsolattartási adatai (GDPR 13. cikk (1) bekezdés b) pont)

Lásd feljebb


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## C. Az adatkezelés célja, amelyre a személyes adatok szolgálnak, valamint az adatkezelés jogalapja (a GDPR 13. cikk (1) bekezdésének c) pontja)

A pályázó adataira vonatkozóan az adatfeldolgozás célja a jelentkezés vizsgálatának lefolytatása a munkaerő-felvételi folyamat során. Ezen célból az összes, Ön által biztosított adatot feldolgozzuk. A munkaerő-felvételi folyamat során benyújtott adatok alapján eldöntjük, hogy behívjuk-e állásinterjúra (ez része a kiválasztási folyamatnak). Az általánosságban véve alkalmas pályázók esetében, főként az állásinterjú kapcsán feldolgozunk bizonyos egyéb, Ön által biztosított személyes adatokat, mely létfontosságú a választási döntésünk meghozatalában. Ha felvesszük Önt, a pályázói adatok automatikusan munkavállalói adatokká válnak. A munkaerő-felvételi folyamat részeként feldolgozunk egyéb, Önhöz kapcsolódó, általunk bekért személyes adatokat is, amelyek a szerződés megkötéséhez vagy teljesítéséhez szükségesek (például személyazonosító okmány száma vagy adószám). A munkavállaló adataira vonatkozóan az adatfeldolgozás célja a munkaszerződés teljesítése, illetve az egyéb, munkaviszony szempontjából alkalmazandó, jogi rendelkezéseknek (pl. adótörvény) való megfelelés, valamint az Ön személyes adatainak felhasználása az Önnel kötött munkaszerződés teljesítése céljából (pl. az Ön nevének és elérhetőségének közzététele a vállalaton belül vagy az ügyfelek számára). A munkavállalói adatok tárolása a munkaviszony megszűnését követően a jogilag előírt adatmegőrzési időszak teljesítésével történik.

Az adatfeldolgozás jogalapja a GDPR 6. cikk (1) bekezdés b) pontja, a GDPR 9. cikk (2) bekezdés b) és h) pontja, a GDPR 88. cikk (1) bekezdése, valamint az olyan nemzeti jogszabályok, mint a német szövetségi adatvédelmi törvény (BDSG) 26. szakasza.

## D. Személyes adatok címzettjeinek kategóriái (GDPR 13. cikk (1) bekezdés e) pont)

Közhatalmi szervek

Külső szervek

További külső szervek

Belső adatkezelés

Csoportok közötti adatkezelés

Egyéb szervek

A harmadik országokban működő adatfeldolgozóink és adatátvevőink, valamint adott esetben nemzetközi szervezetek listáját vagy közzétesszük a weboldalunkon, vagy ingyenesen kérhető tőlünk. Kérjük, lépjen kapcsolatba adatvédelmi tisztviselőnkkel a lista igényléséhez.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## E. Harmadik országban lévő címzettek és megfelelő vagy alkalmas biztosítékok és eszközök, amelyekkel másolatot lehet szerezni róluk, vagy ahol rendelkezésre bocsájtották őket (GDPR 13. cikk (1) bek. f) pont, 46. cikk (1) bek., 46. cikk (2) bek. c) pont)

Minden olyan csoportunkat alkotó vállalat és fiókiroda (továbbiakban „csoportvállalatok”), amely harmadik országban folytat üzleti tevékenységet vagy ott tart fenn irodát, lehet címzettje a személyes adatoknak.

A GDPR 46. cikk (1) bekezdése szerint az adatkezelő vagy adatfeldolgozó csak akkor továbbíthat személyes adatokat harmadik országba, ha az adatkezelő vagy adatfeldolgozó megfelelő biztosítékokat nyújt, ha az érintett jogai kikényszeríthetők és rendelkezésre állnak jogorvoslati lehetőségek az érintettek részére. Megfelelő biztosítékokat lehet nyújtani a felügyeleti hatóság külön engedélye nélkül is szabványos szerződéses záradékok segítségével (GDPR 46. cikk (2) bek. c) pont).

Az Európai Unió szabványos szerződéses záradékait a személyes adatok első továbbítása előtt kötött megállapodás biztosítja minden harmadik országban tartózkodó címzett esetén. Ennek következtében megfelelő biztosítékok, az érintett kikényszeríthető jogai és hatályos jogorvoslati lehetőségek biztosíthatók az érintett számára, amelyeket az EU szabványos szerződéses záradékai garantálnak. Az érintettek a szabványos szerződéses záradékokról másolatot kaphatnak az adatvédelmi tisztviselőtől. A szabványos szerződéses záradékok elérhetők az Európai Unió hivatalos lapjában.

Az általános adatvédelmi rendelet (GDPR) 45. cikkének (3) bekezdése biztosítja az Európai Bizottság számára azt a jogot, hogy végrehajtási jogi aktus útján döntsön arról, hogy egy Unión kívüli ország megfelelő szintű védelmet biztosít-e. Ez a személyes adatok védelmének olyan szintjét jelenti, amely nagyjából egyenértékű az uniós védelemmel. A megfelelő szintű védelmet megállapító határozatok azt eredményezik, hogy a személyes adatok szabadon, további akadályok nélkül áramolhatnak az EU-ból (valamint Norvégiából, Liechtensteinből és Izlandról) egy harmadik országba. Hasonló szabályok vonatkoznak az Egyesült Királyságban, Svájcban és néhány más országban is.

Abban az esetben, ha az Európai Bizottság vagy egy másik ország kormánya úgy dönt, hogy egy harmadik ország megfelelő szintű védelmet biztosít, és az alkalmazandó keretrendszer (pl. az EU-U.S. Data Privacy Framework, Swiss-U.S. Data Privacy Framework, UK Extension to the EU-U.S. Data Privacy Framework), az ilyen keretrendszerek tagjainak (pl. önhitelesített szervezetek) történő valamennyi adattovábbításunk kizárólag az adott szervezetek adott keretrendszerben való tagságán alapul. Abban az esetben, ha mi vagy csoportunk valamelyik tagja tagja az ilyen keretrendszereknek, a nekünk vagy csoportunk valamelyik tagjának történő minden adattovábbítás kizárólag a tagságon alapul.

A keretrendszerek egy példányát bármely érintett megkaphatja tőlünk. A keretszabályok ezen túlmenően az Európai Unió Hivatalos Lapjában vagy a közzétett jogi anyagokban, illetve a felügyeleti hatóságok vagy más illetékes hatóságok vagy intézmények weboldalain is elérhetők.


© All rights reserved by Heiko Maniero.

## F. A személyes adatok tárolásának időtartama, vagy ha az nem lehetséges, az időtartam meghatározására szolgáló kritériumok (GDPR 13. cikk (2) bek. a) pont)

A pályázók személyes adatainak tárolási időtartama 6 hónap. A munkavállalók adataira a törvény által előírt adatmegőrzési időszak érvényes. Az adott időtartamot követően az adatok rutinszerűen törlésre kerülnek, amennyiben azok már nem szükségesek a szerződés teljesítéséhez vagy a szerződés megkötéséhez.

## G. Az érintett joga a személyes adatok hozzáférését, helyesbítését vagy törlését, azok korlátozott feldolgozását kérni az adatkezelőtől, tiltakozni az adatkezelés ellen, illetve az adathordozhatósághoz való jog (GDPR 13. cikk (2) bek. b) pont)

Minden érintett az alábbi jogokkal rendelkezik:

***Hozzáféréshez való jog***

Minden érintettnek joga van hozzáférni az őt érintő személyes adatokhoz. A hozzáférés joga kiterjed minden általunk kezelt adatra. Ez a jog könnyen és ésszerű időközönként gyakorolható az adatkezelés megismerése, és törvényességének ellenőrzése érdekében (GDPR Bevezetés 63. pont) Ezt a jogot a GDPR 15. cikke biztosítja. Az érintett felveheti a kapcsolatot az adatvédelmi tisztviselőnkkel, ha szeretne élni a hozzáférés jogával.

***Helyesbítés joga***

A GDPR 16. cikk 1. mondata értelmében az érintettnek joga van, hogy kérje az adatkezelőt, hogy indokolatlan késedelem nélkül helyesbítse az őt érintő pontatlan személyes adatokat. Ezen kívül a GDPR 16. cikk 2. mondata biztosítja, hogy az érintett jogosult – figyelembe véve az adatkezelés céljait – a hiányos adatok pótlását kérni beleértve a kiegészítő nyilatkozattal való biztosítást is. Az érintett felveheti a kapcsolatot az adatvédelmi tisztviselőnkkel, ha szeretne élni a helyesbítés jogával.

***Törléshez való jog („elfeledtetéshez való jog")***

Ezen kívül az érintettek jogosultak a törléshez és elfeledtetéshez való jog gyakorlására a a GDPR 17. cikke értelmében. Az érintett élhet ezzel a jogával, ha felveszi a kapcsolatot adatvédelmi tisztviselőnkkel. Ezen a ponton azonban szeretnénk rámutatni arra, hogy ez a jog nem alkalmazandó, amennyiben az adatkezelés ránk vonatkozó jogi kötelezettség teljesítéséhez szükséges GDPR 17. cikk (3) bek. b) pont. Ez azt jelenti, hogy a törlésre vonatkozó kérelmet csak a törvényi előírás szerinti megőrzési időszak lejáratát követően tudjuk jóváhagyni.

***Adatkezelés korlátozásához való jog***

A GDPR 18. cikke szerint minden érintett jogosult az adatkezelés korlátozására. Ha az adatkezelés korlátozását akkor lehet kérni, ha a GDPR 18. cikk (1) bek. a-d) pontjában meghatározott feltételek valamelyike teljesül. Az érintett felveheti a kapcsolatot az adatvédelmi tisztviselőnkkel, ha szeretne élni az adatkezelés korlátozásának jogával.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

***Tiltakozáshoz való jog***

Továbbá a GDPR 21. cikke biztosítja a tiltakozáshoz való jogot. Az érintett felveheti a kapcsolatot az adatvédelmi tisztviselőnkkel, ha szeretne élni a tiltakozáshoz való jogával.

***Adathordozhatóság joga***

A GDPR 20. cikke biztosítja az adathordozhatóság jogát az érintettnek. E rendelkezés értelmében az érintettnek a GDPR 20. cikk (1) bekezdésének a) és b) pontjában meghatározott feltételek szerint joga van, hogy megkapja az őt érintő, adatkezelő részére átadott személyes adatokat egy strukturált, általánosan használt és gépileg olvasható formában, és joga van arra, hogy ezeket az adatokat egy másik adatkezelőnek akadály nélkül továbbítsa attól az adatkezelőtől, akinek a személyes adatokat megadta. Az érintett felveheti a kapcsolatot az adatvédelmi tisztviselőnkkel, ha szeretne élni az adathordozhatóság jogával.

## H. A hozzájárulás bármikor történő visszavonásának joga a hozzájáruláson alapuló adatfeldolgozás törvényességét a visszavonás előtt nem érintve, ahol az adatkezelés a GDPR 6. cikk (1) bekezdés a) pontján vagy a GDPR 9. cikk (2) bekezdés a) pontján (GDPR 13. cikk (2) bek. c) pontja) alapul

Ha a személyes adatok kezelése a GDPR 6. cikk (1) bekezdés a) pontja szerint történik, amennyiben az érintett hozzájárulását adta a személyes adatok kezeléséhez egy vagy több célból, vagy a GDPR 9. cikk (2) bekezdés a) pontján alapul, amely a személyes adatok speciális kategóriáinak kezeléséhez való kifejezett hozzájárulást szabályozza, akkor az érintettnek joga van a GDPR 7. cikk (3) bek. 1. mondat értelmében bármikor visszavonni a hozzájárulását.

A hozzájárulás visszavonása nem érinti a visszavonás előtti, hozzájáruláson alapuló adatkezelés törvényességét a GDPR 7. cikk (3) bek. 2. mondat értelmében. A hozzájárulás visszavonása olyan egyszerű, mint a hozzájárulás megadása (GDPR 7. cikk (3) bekezdés 4. mondat). Ezért a hozzájárulás visszavonása mindig a hozzájárulás megadásával megegyező módon történik, vagy más módon, ha az érintett számára az egyszerűbb. Napjaink információs társadalmában talán a hozzájárulás visszavonásának legegyszerűbb módja az e-mail küldés. Ha az érintett szeretné visszavonni a nekünk megadott hozzájárulását, akkor elegendő, ha küld egy e-mail üzenetet az adatvédelmi tisztviselőnknek. De az érintett választhat más módot is a hozzájárulása visszavonásához.

## I. Panasz felügyeleti hatósághoz való benyújtásának joga (GDPR 13. cikk (2) bekezdés d) pont, 77. cikk (1) bekezdés)

Adatkezelőként kötelesek vagyunk értesíteni az érintettet arról, hogy joga van panaszt benyújtani a felügyeleti hatósághoz (GDPR 13. cikk (2) bek. d) pont). A panasz felügyeleti hatósághoz való benyújtásának jogát a GDPR 77. cikk (1) bekezdése szabályozza. E rendelkezés értelmében bármely más közigazgatási vagy bírósági jogorvoslat sérelme nélkül minden érintettnek joga van panaszt


© All rights reserved by Heiko Maniero.

benyújtani egy felügyeleti hatósághoz, a szokásos tartózkodási helye, munkahelye vagy az állítólagos jogsértés helye szerinti tagállamban, ha az érintett úgy ítéli meg, hogy az őt érintő személyes adatok feldolgozása sérti az Általános adatvédelmi szabályozást. A panasz felügyeleti hatósághoz való benyújtásának jogát az Unió törvénye szabályozza olyan módon, hogy az kizárólag egyetlen felügyeleti hatósággal szemben gyakorolható (GDPR Bevezetés 141. pont, 1. mondat). Ennek a szabálynak a célja, hogy kizárja, hogy az ugyanaz az érintett ugyanabban az ügyben dupla panaszt nyújtson be. Ha az érintett panaszt szeretne benyújtani velünk szemben, kérjük, hogy azt csak egyetlen felügyeleti hatóságnál tegye meg.

## J. Személyes adatok biztosítása törvényi vagy szerződéses követelményként; A szerződés megkötéséhez szükséges követelmény; Az érintett kötelezettsége a személyes adatok biztosítása érdekében; az ilyen adatok nem teljesítésének lehetséges következményei (GDPR 13. cikk (2) bekezdés e) pontja).

Tisztázzuk, hogy a személyes adatok megadása részben törvényi okokból (pl.: adószabályok), vagy részben szerződéses rendelkezések miatt szükséges (pl.: a szerződő fél adatai).

Néha szükséges lehet szerződés kötésére, hogy az érintett személyes adatokat adjon át nekünk, amelyeket később mi kezelünk. Az érintett például személyes adatokat ad át vállalatunknak, amikor aláírunk vele egy szerződést. Ha az érintett nem adna át személyes adatokat, akkor a szerződést nem tudnánk megkötni.

Mielőtt az érintett személyes adatokat adna meg, az érintettnek fel kell vennie a kapcsolatot az adatvédelmi tisztviselővel. Adatvédelmi tisztviselőnk tisztázza az érintettel, hogy a személyes adatok megadására törvényi vagy szerződéses okokból van szükség, vagy a szerződés megkötéséhez szükséges, illetve, hogy kötelezettsége van a személyes adatok megadására, és milyen következményekkel jár a személyes adatok megadásának megtagadása.

## K. A GDPR 22. cikkének (1) és (4) bekezdésében említett automatizált döntéshozatal, ideértve a profilalkotást is, és legalábbis ezekben az esetekben az értelmezhető logikával kapcsolatos lényeges információk, valamint az ilyen adatkezelés megvalósításának jelentősége és tervezett következményei az érintett számára (GDPR 13. cikk (2) bekezdés f) pont).

Felelős vállalatként általában nem alkalmazunk automatizált döntéshozatalt vagy profilalkotást. Ha kivételes esetekben automatizált döntéshozatalt vagy profilalkotást végzünk, erről külön vagy az adatvédelmi szabályzatunkban (a weboldalunkon) található alfejezeten keresztül tájékoztatjuk az érintettet. Ebben az esetben a következők érvényesek:


© All rights reserved by Heiko Maniero.

Automatizált döntéshozatalra - ideértve a profilalkotást is - akkor kerülhet sor, ha (1) ez szükséges az érintett és köztünk létrejött szerződés megkötéséhez vagy teljesítéséhez, vagy (2) ezt az érintett jogainak és szabadságainak, valamint jogos érdekeinek védelmét szolgáló megfelelő intézkedéseket is előíró uniós vagy tagállami jog engedélyezi, amelynek hatálya alá tartozunk; vagy (3) ez az érintett kifejezett hozzájárulásán alapul.

A GDPR 22. cikk (2) bekezdésének a) és c) pontjában említett esetekben megfelelő intézkedéseket hajtunk végre az érintett jogainak és szabadságainak, valamint jogos érdekeinek védelme érdekében. Ezekben az esetekben Ön jogosult arra, hogy az adatkezelő részéről emberi beavatkozást kérjen, kifejtse álláspontját és megtámadja a döntést.

Az érintett logikáról, valamint az adatkezelés jelentőségéről és az érintettre gyakorolt várható következményeiről az adatvédelmi szabályzatunkban találhatók érdemi információk.

## II. Az adatszolgáltatási követelményeknek való megfelelés, ha a személyes adatokat nem az érintettől gyűjtik (a GDPR 14. cikke)

### A. Az adatkezelő személyazonossága és kapcsolattartási adatai (GDPR 14. cikk (1) bekezdés a) pont)

Lásd feljebb

### B. Az adatvédelmi tisztviselő kapcsolattartási adatai (GDPR 14. cikk (1) bekezdés b) pont)

Lásd feljebb

### C. Az adatkezelés célja, amelyre a személyes adatok szolgálnak, valamint az adatkezelés jogalapja (a GDPR 14. cikk (1) bekezdésének c) pontja)

A nem az érintett felektől begyűjtött pályázói adatokra vonatkozóan az adatfeldolgozás célja a jelentkezés vizsgálatának lefolytatása a munkaerő-felvételi folyamat során. Ebből a célból feldolgozhatunk nem Öntől begyűjtött adatokat is. A munkaerő-felvételi folyamat során feldolgozott adatok alapján eldöntjük, hogy behívjuk-e állásinterjúra (ez része a kiválasztási folyamatnak). Ha felvesszük Önt, a pályázói adatok automatikusan munkavállalói adatokká változnak. A munkavállalók adataira vonatkozóan az adatfeldolgozás célja a munkaszerződés teljesítése, illetve az egyéb, munkaviszony szempontjából alkalmazandó, jogi rendelkezéseknek való megfelelés A munkavállalói adatok tárolása a munkaviszony megszűnését követően a jogilag előírt adatmegőrzési időszak teljesítésével történik.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

Az adatfeldolgozás jogalapja a GDPR 6. cikk (1) bekezdés b) és f) pontja, a GDPR 9. cikk (2) bekezdés b) és h) pontja, a GDPR 88. cikk (1) bekezdése, valamint az olyan nemzeti jogszabályok, mint a német szövetségi adatvédelmi törvény (BDSG) 26. szakasza.

## D. Érintett személyes adatok kategóriái (GDPR 14. cikk (1) bekezdés d) pont)

Pályázói adatok

Munkavállalói adatok

## E. Személyes adatok címzettjeinek kategóriái (GDPR 14. cikk (1) bekezdés e) pont)

Közhatalmi szervek

Külső szervek

További külső szervek

Belső adatkezelés

Csoportok közötti adatkezelés

Egyéb szervek

A harmadik országokban működő adatfeldolgozóink és adatátvevőink, valamint adott esetben nemzetközi szervezetek listáját vagy közzétesszük a weboldalunkon, vagy ingyenesen kérhető tőlünk. Kérjük, lépjen kapcsolatba adatvédelmi tisztviselőnkkel a lista igényléséhez.

## F. Harmadik országban lévő címzettek és megfelelő vagy alkalmas biztosítékok és eszközök, amelyekkel másolatot lehet szerezni róluk, vagy ahol rendelkezésre bocsájtották őket (GDPR 14. cikk (1) bek. f) pont, 46. cikk (1) bek., 46. cikk (2) bek. c) pont)

Minden olyan csoportunkat alkotó vállalat és fiókiroda (továbbiakban „csoportvállalatok”), amely harmadik országban folytat üzleti tevékenységet vagy ott tart fenn irodát, lehet címzettje a személyes adatoknak. Minden csoportvállalat címe megtalálható a weboldalunkon www.osigroup.com.

A GDPR 46. cikk (1) bekezdése szerint az adatkezelő vagy adatfeldolgozó csak akkor továbbíthat személyes adatokat harmadik országba, ha az adatkezelő vagy adatfeldolgozó megfelelő biztosítékokat


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

nyújt, ha az érintett jogai kikényszeríthetők és rendelkezésre állnak jogorvoslati lehetőségek az érintettek részére. Megfelelő biztosítékokat lehet nyújtani a felügyeleti hatóság külön engedélye nélkül is szabványos szerződéses záradékok segítségével (GDPR 46. cikk (2) bek. c) pont).

Az Európai Unió szabványos szerződéses záradékait a személyes adatok első továbbítása előtt kötött megállapodás biztosítja minden harmadik országban tartózkodó címzett esetén. Ennek következtében megfelelő biztosítékok, az érintett kikényszeríthető jogai és hatályos jogorvoslati lehetőségek biztosíthatók az érintett számára, amelyeket az EU szabványos szerződéses záradékai garantálnak. Az érintettek a szabványos szerződéses záradékokról másolatot kaphatnak az adatvédelmi tisztviselőtől. A szabványos szerződéses záradékok elérhetők az Európai Unió hivatalos lapjában.

Az általános adatvédelmi rendelet (GDPR) 45. cikkének (3) bekezdése biztosítja az Európai Bizottság számára azt a jogot, hogy végrehajtási jogi aktus útján döntsön arról, hogy egy Unión kívüli ország megfelelő szintű védelmet biztosít-e. Ez a személyes adatok védelmének olyan szintjét jelenti, amely nagyjából egyenértékű az uniós védelemmel. A megfelelő szintű védelmet megállapító határozatok azt eredményezik, hogy a személyes adatok szabadon, további akadályok nélkül áramolhatnak az EU-ból (valamint Norvégiából, Liechtensteinből és Izlandról) egy harmadik országba. Hasonló szabályok vonatkoznak az Egyesült Királyságban, Svájcban és néhány más országban is.

Abban az esetben, ha az Európai Bizottság vagy egy másik ország kormánya úgy dönt, hogy egy harmadik ország megfelelő szintű védelmet biztosít, és az alkalmazandó keretrendszer (pl. az EU-U.S. Data Privacy Framework, Swiss-U.S. Data Privacy Framework, UK Extension to the EU-U.S. Data Privacy Framework), az ilyen keretrendszerek tagjainak (pl. önhitelesített szervezetek) történő valamennyi adattovábbításunk kizárólag az adott szervezetek adott keretrendszerben való tagságán alapul. Abban az esetben, ha mi vagy csoportunk valamelyik tagja tagja az ilyen keretrendszereknek, a nekünk vagy csoportunk valamelyik tagjának történő minden adattovábbítás kizárólag a tagságon alapul.

A keretrendszerek egy példányát bármely érintett megkaphatja tőlünk. A keretszabályok ezen túlmenően az Európai Unió Hivatalos Lapjában vagy a közzétett jogi anyagokban, illetve a felügyeleti hatóságok vagy más illetékes hatóságok vagy intézmények weboldalain is elérhetők.

## G. A személyes adatok tárolásának időtartama, vagy ha az nem lehetséges, az időtartam meghatározására szolgáló kritériumok (GDPR 14. cikk (2) bek. a) pont)

A pályázók személyes adatainak tárolási időtartama 6 hónap. A munkavállalók adataira a törvény által előírt adatmegőrzési időszak érvényes. Az adott időtartamot követően az adatok rutinszerűen törlésre kerülnek, amennyiben azok már nem szükségesek a szerződés teljesítéséhez vagy a szerződés megkötéséhez.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## H. Értesítés az adatkezelő vagy harmadik jogos érdekeiről, amennyiben az adatkezelés a GDPR 6. cikk (1) bekezdés f) pontja alapján történik (GDPR 14. cikk (2) bekezdés b) pontja).

A GDPR 6. cikk (1) bekezdés f) pontja szerinti adatkezelés csak akkor lehet törvényes, amennyiben az adatkezelés az adatkezelő vagy egy harmadik fél jogos érdekében szükséges, kivéve, ha azok az érdekek felülírják annak az érintettnek az érdekeit, alapvető jogait és szabadságát, akinek személyes adatait meg kell védeni. A GDPR Bevezetés 47. pontjának 2. mondata szerint a jogos érdek fennállhat, ha az érintett és az adatkezelő között releváns és megfelelő kapcsolat van, például ha az érintett az adatkezelő ügyfele. Minden esetben, melynek során vállalatunk a GDPR 6. cikk (1) bekezdés f) pontja alapján dolgozza fel a pályázói adatokat, a jogos érdekünk a megfelelő személyzet és szakemberek alkalmazása.

## I. Az érintett joga a személyes adatok hozzáférését, helyesbítését vagy törlését, azok korlátozott feldolgozását kérni az adatkezelőtől, tiltakozni az adatkezelés ellen, illetve az adathordozhatósághoz való jogát gyakorolni (GDPR 14. cikk (2) bek. c) pont)

Minden érintett az alábbi jogokkal rendelkezik:

***Hozzáféréshez való jog***

Minden érintettnek joga van hozzáférni az őt érintő személyes adatokhoz. A hozzáférés joga kiterjed minden általunk kezelt adatra. Ez a jog könnyen és ésszerű időközönként gyakorolható az adatkezelés megismerése, és törvényességének ellenőrzése érdekében (GDPR Bevezetés 63. pont) Ezt a jogot a GDPR 15. cikke biztosítja. Az érintett felveheti a kapcsolatot az adatvédelmi tisztviselőnkkel, ha szeretne élni a hozzáférés jogával.

***Helyesbítés joga***

A GDPR 16. cikk 1. mondata értelmében az érintettnek joga van, hogy kérje az adatkezelőt, hogy indokolatlan késedelem nélkül helyesbítse az őt érintő pontatlan személyes adatokat. Ezen kívül a GDPR 16. cikk 2. mondata biztosítja, hogy az érintett jogosult – figyelembe véve az adatkezelés céljait – a hiányos adatok pótlását kérni beleértve a kiegészítő nyilatkozattal való biztosítást is. Az érintett felveheti a kapcsolatot az adatvédelmi tisztviselőnkkel, ha szeretne élni a helyesbítés jogával.

***Törléshez való jog („elfeledtetéshez való jog")***

Ezen kívül az érintettek jogosultak a törléshez és elfeledtetéshez való jog gyakorlására a a GDPR 17. cikke értelmében. Az érintett élhet ezzel a jogával, ha felveszi a kapcsolatot adatvédelmi tisztviselőnkkel. Ezen a ponton azonban szeretnénk rámutatni arra, hogy ez a jog nem alkalmazandó, amennyiben az adatkezelés ránk vonatkozó jogi kötelezettség teljesítéséhez szükséges GDPR 17. cikk (3) bek. b) pont. Ez azt jelenti, hogy a törlésre vonatkozó kérelmet csak a törvényi előírás szerinti megőrzési időszak lejáratát követően tudjuk jóváhagyni.


© All rights reserved by Heiko Maniero.

***Adatkezelés korlátozásához való jog***

A GDPR 18. cikke szerint minden érintett jogosult az adatkezelés korlátozására. Ha az adatkezelés korlátozását akkor lehet kérni, ha a GDPR 18. cikk (1) bek. a-d) pontjában meghatározott feltételek valamelyike teljesül. Az érintett felveheti a kapcsolatot az adatvédelmi tisztviselőnkkel, ha szeretne élni az adatkezelés korlátozásának jogával.

***Tiltakozáshoz való jog***

Továbbá a GDPR 21. cikke biztosítja a tiltakozáshoz való jogot. Az érintett felveheti a kapcsolatot az adatvédelmi tisztviselőnkkel, ha szeretne élni a tiltakozáshoz való jogával.

***Adathordozhatóság joga***

A GDPR 20. cikke biztosítja az adathordozhatóság jogát az érintettnek. E rendelkezés értelmében az érintettnek a GDPR 20. cikk (1) bekezdésének a) és b) pontjában meghatározott feltételek szerint joga van, hogy megkapja az őt érintő, adatkezelő részére átadott személyes adatokat egy strukturált, általánosan használt és gépileg olvasható formában, és joga van arra, hogy ezeket az adatokat egy másik adatkezelőnek akadály nélkül továbbítsa attól az adatkezelőtől, akinek a személyes adatokat megadta. Az érintett felveheti a kapcsolatot az adatvédelmi tisztviselőnkkel, ha szeretne élni az adathordozhatóság jogával.

## J. A hozzájárulás bármikor történő visszavonásának joga a hozzájáruláson alapuló adatfeldolgozás törvényességét a visszavonás előtt nem érintve, ahol az adatkezelés a GDPR 6. cikk (1) bekezdés a) pontján vagy a GDPR 9. cikk (2) bekezdés a) pontján alapul (GDPR 14. cikk (2) bekezdés d) pontja)

Ha a személyes adatok kezelése a GDPR 6. cikk (1) bekezdés a) pontja szerint történik, amennyiben az érintett hozzájárulását adta a személyes adatok kezeléséhez egy vagy több célból, vagy a GDPR 9. cikk (2) bekezdés a) pontján alapul, amely a személyes adatok speciális kategóriáinak kezeléséhez való kifejezett hozzájárulást szabályozza, akkor az érintettnek joga van a GDPR 7. cikk (3) bek. 1. mondat értelmében bármikor visszavonni a hozzájárulását.

A hozzájárulás visszavonása nem érinti a visszavonás előtti, hozzájáruláson alapuló adatkezelés törvényességét a GDPR 7. cikk (3) bek. 2. mondat értelmében. A hozzájárulás visszavonása olyan egyszerű, mint a hozzájárulás megadása (GDPR 7. cikk (3) bekezdés 4. mondat). Ezért a hozzájárulás visszavonása mindig a hozzájárulás megadásával megegyező módon történik, vagy más módon, ha az érintett számára az egyszerűbb. Napjaink információs társadalmában talán a hozzájárulás visszavonásának legegyszerűbb módja az e-mail küldés. Ha az érintett szeretné visszavonni a nekünk megadott hozzájárulását, akkor elegendő, ha küld egy e-mail üzenetet az adatvédelmi tisztviselőnknek. De az érintett választhat más módot is a hozzájárulása visszavonásához.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## K. Panasz felügyeleti hatósághoz való benyújtásának joga (GDPR 14. cikk (2) bekezdés e) pont, 77. cikk (1) bekezdés)

Adatkezelőként kötelesek vagyunk értesíteni az érintettet arról, hogy joga van panaszt benyújtani a felügyeleti hatósághoz (GDPR 13. cikk (2) bek. d) pont). A panasz felügyeleti hatósághoz való benyújtásának jogát a GDPR 77. cikk (1) bekezdése szabályozza. E rendelkezés értelmében bármely más közigazgatási vagy bírósági jogorvoslat sérelme nélkül minden érintettnek joga van panaszt benyújtani egy felügyeleti hatósághoz, a szokásos tartózkodási helye, munkahelye vagy az állítólagos jogsértés helye szerinti tagállamban, ha az érintett úgy ítéli meg, hogy az őt érintő személyes adatok feldolgozása sérti az Általános adatvédelmi szabályozást. A panasz felügyeleti hatósághoz való benyújtásának jogát az Unió törvénye szabályozza olyan módon, hogy az kizárólag egyetlen felügyeleti hatósággal szemben gyakorolható (GDPR Bevezetés 141. pont, 1. mondat). Ennek a szabálynak a célja, hogy kizárja, hogy az ugyanaz az érintett ugyanabban az ügyben dupla panaszt nyújtson be. Ha az érintett panaszt szeretne benyújtani velünk szemben, kérjük, hogy azt csak egyetlen felügyeleti hatóságnál tegye meg.

## L. Forrás ahonnan a személyes adatok származnak, és adott esetben a nyilvános elérhető források (ha az adatok onnan származnak) (GDPR 14. cikk (2) bekezdés f) pont)

Elviekben a személyes adatokat közvetlenül az érintettől vagy egy hatósággal együttműködésben gyűjtik (pl.: adatok kinyerése egy hivatalos nyilvántartásból) Az érintettek egyéb adatai a csoportvállalatoktól adattovábbítással érkeznek. Ezen általános információkkal összefüggésben a pontos források megnevezése, amelyekből a személyes adatok származnak, lehetetlen vagy aránytalan erőfeszítéssel járna a GDPR 14. cikk (5) bekezdés b) pontja értelmében. Elméletileg nem gyűjtünk személyes adatokat nyilvánosan hozzáférhető forrásokból.

Az érintettek bármikor felvehetik a kapcsolatot az adatvédelmi tisztviselőnkkel, hogy további információt kapjanak az őket érintő személyes adatok pontos forrásáról. Ha a személyes adatok eredetét nem tudjuk megmondani az érintettnek, mivel több forrásból származnak, akkor általános tájékoztatást kell adnunk (GDPR Bevezetés 61. pont 4. mondat).


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

M. A GDPR 22. cikkének (1) és (4) bekezdésében említett automatizált döntéshozatal, ideértve a profilalkotást is, és legalábbis ezekben az esetekben az értelmezhető logikával kapcsolatos lényeges információk, valamint az ilyen adatkezelés megvalósításának jelentősége és tervezett következményei az érintett számára (GDPR 14. cikk (2) bekezdés g) pont).

Felelős vállalatként általában nem alkalmazunk automatizált döntéshozatalt vagy profilalkotást. Ha kivételes esetekben automatizált döntéshozatalt vagy profilalkotást végzünk, erről külön vagy az adatvédelmi szabályzatunkban (a weboldalunkon) található alfejezeten keresztül tájékoztatjuk az érintettet. Ebben az esetben a következők érvényesek:

Automatizált döntéshozatalra - ideértve a profilalkotást is - akkor kerülhet sor, ha (1) ez szükséges az érintett és köztünk létrejött szerződés megkötéséhez vagy teljesítéséhez, vagy (2) ezt az érintett jogainak és szabadságainak, valamint jogos érdekeinek védelmét szolgáló megfelelő intézkedéseket is előíró uniós vagy tagállami jog engedélyezi, amelynek hatálya alá tartozunk; vagy (3) ez az érintett kifejezett hozzájárulásán alapul.

A GDPR 22. cikk (2) bekezdésének a) és c) pontjában említett esetekben megfelelő intézkedéseket hajtunk végre az érintett jogainak és szabadságainak, valamint jogos érdekeinek védelme érdekében. Ezekben az esetekben Ön jogosult arra, hogy az adatkezelő részéről emberi beavatkozást kérjen, kifejtse álláspontját és megtámadja a döntést.

Az érintett logikáról, valamint az adatkezelés jelentőségéről és az érintettre gyakorolt várható következményeiről az adatvédelmi szabályzatunkban találhatók érdemi információk.

## III. EU-U.S. Data Privacy Framework (EU-U.S. DPF), UK Extension to the EU-U.S. DPF, Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF)

Amennyiben szervezetünk tanúsított tagja az EU-U.S. Data Privacy Framework (EU-U.S. DPF) és/vagy a UK Extension to the EU-U.S. DPF és/vagy a Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF), az alábbiak érvényesek:

Betartjuk az EU-U.S. Data Privacy Framework (EU-U.S. DPF) és a UK Extension to the EU-U.S. DPF, valamint a Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF) előírásait, ahogyan azt az U.S. Department of Commerce meghatározta. Vállalatunk megerősítette az amerikai kereskedelmi minisztérium számára, hogy betartja az EU-U.S. Data Privacy Framework Principles (EU-U.S. DPF Principles) elveit a személyes adatok feldolgozásával kapcsolatban, amelyeket az Európai Unióból és az Egyesült Királyságból kap az EU-U.S. DPF és a UK Extension to the EU-U.S. DPF alapján. Vállalatunk megerősítette az amerikai kereskedelmi minisztérium számára, hogy betartja a Swiss-U.S. Data Privacy Framework Principles (Swiss-U.S. DPF Principles) elveit a személyes adatok feldolgozásával


© All rights reserved by Heiko Maniero.

kapcsolatban, amelyeket Svájcból kap a Swiss-U.S. DPF alapján. Amennyiben ellentmondás van adatvédelmi nyilatkozatunk és az EU-U.S. DPF Principles és/vagy a Swiss-U.S. DPF Principles rendelkezései között, az elvek az irányadók.

A Data Privacy Framework (DPF) programról és tanúsítványunkról további információkat a https://www.dataprivacyframework.gov/ oldalon talál.

Azok az egyéb amerikai egységek vagy amerikai leányvállalatok, amelyek szintén betartják az EU-U.S. DPF Principles elveit, beleértve a UK Extension to the EU-U.S. DPF és a Swiss-U.S. DPF Principles elveit, amennyiben vannak, adatvédelmi nyilatkozatunkban kerülnek megnevezésre.

Az EU-U.S. DPF, a UK Extension to the EU-U.S. DPF és a Swiss-U.S. DPF előírásaival összhangban vállalatunk kötelezi magát arra, hogy együttműködik az EU adatvédelmi hatóságaival, a brit Information Commissioner's Office-szal (ICO), valamint a svájci Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) hivatallal, és követi azok tanácsait a személyes adatok kezelésével kapcsolatos, megoldatlan panaszok tekintetében, amelyeket az EU-U.S. DPF, a UK Extension to the EU-U.S. DPF és a Swiss-U.S. DPF alapján kapunk.

Tájékoztatjuk az érintett személyeket az illetékes európai adatvédelmi hatóságokról, amelyek felelősek szervezetünk személyes adatok kezelésével kapcsolatos panaszainak feldolgozásáért, ezen átláthatósági dokumentum tetején, valamint arról, hogy megfelelő és ingyenes jogorvoslati lehetőséget kínálunk az érintett személyek számára.

Tájékoztatjuk az összes érintett személyt, hogy vállalatunk a Federal Trade Commission (FTC) vizsgálati és végrehajtási hatáskörébe tartozik.

Az érintett személyek bizonyos körülmények között lehetőséget kapnak kötelező érvényű választottbíráskodás igénybevételére. Szervezetünk köteles rendezni a követeléseket és betartani az I. mellékletben szereplő DPF Principles feltételeit, amennyiben az érintett személy kötelező érvényű választottbíráskodást kér, értesítve szervezetünket és betartva az I. melléklet elveiben szereplő eljárásokat és feltételeket.

Ezúton tájékoztatjuk az összes érintett személyt szervezetünk felelősségéről a személyes adatok harmadik félnek történő továbbítása esetén.

Az érintett személyek vagy adatvédelmi hatóságok kérdései esetén kijelöltük a helyi képviselőket, akiknek neve ezen átláthatósági dokumentum tetején található.

Lehetőséget kínálunk Önnek, hogy döntsön (Opt-out), hogy személyes adatait (i) harmadik félnek továbbítják, vagy (ii) olyan célra használják, amely jelentősen eltér az eredeti céloktól, amelyekre azokat gyűjtötték, vagy később Ön által jóváhagyták. Az Ön választási jogának gyakorlására szolgáló egyértelmű, jól látható és könnyen hozzáférhető mechanizmus az, hogy e-mailben felvegye a kapcsolatot adatvédelmi tisztviselőnkkel (DSB). Nincs választási lehetősége, és nem vagyunk kötelesek erre, ha az


© All rights reserved by Heiko Maniero.

adatokat olyan harmadik félnek továbbítják, aki megbízottként vagy feldolgozóként jár el a nevünkben és utasításaink szerint. Mindig szerződést kötünk egy ilyen megbízottal vagy feldolgozóval.

Az érzékeny adatok (azaz az egészségügyi állapotra, a faji vagy etnikai származásra, a politikai véleményekre, a vallási vagy filozófiai meggyőződésekre, a szakszervezeti tagságra vagy a szexuális életre vonatkozó személyes adatok) esetében kifejezett hozzájárulását (Opt-in) kérjük, ha ezeket az adatokat (i) harmadik félnek továbbítják, vagy (ii) más célra használják, mint amelyre eredetileg gyűjtötték, vagy amelyhez később az Opt-in választásával hozzájárult. Ezenkívül minden személyes adatot, amelyet harmadik féltől kapunk, érzékenyként kezelünk, ha a harmadik fél azokat érzékenyként azonosította és kezelte.

Ezúton tájékoztatjuk Önt a személyes adatok hatósági kérésre történő közzétételének szükségességéről, beleértve a nemzetbiztonsági vagy bűnüldözési követelmények teljesítését.

Amikor személyes adatokat harmadik félnek továbbítunk, aki adatkezelőként jár el, betartjuk az értesítési és választási elveket. Emellett szerződést kötünk az adatkezelővel, amely előírja, hogy ezeket az adatokat csak korlátozott és meghatározott célokra szabad feldolgozni az Ön hozzájárulásával összhangban, és hogy a címzett ugyanolyan szintű védelmet biztosít, mint a DPF elvei, és értesít minket, ha úgy találja, hogy már nem tudja teljesíteni ezt a kötelezettséget. A szerződés előírja, hogy az adatkezelő beszünteti az adatkezelést, vagy más megfelelő és megfelelő intézkedéseket tesz a helyrehozás érdekében, ha megállapítást nyer, hogy nem tudja teljesíteni kötelezettségét.

Amikor személyes adatokat továbbítunk harmadik félnek, aki megbízottként vagy feldolgozóként jár el, (i) ezeket az adatokat csak korlátozott és meghatározott célokra továbbítjuk; (ii) meggyőződünk arról, hogy a megbízott vagy feldolgozó köteles biztosítani a DPF elveinek megfelelő adatvédelmi szintet; (iii) megfelelő és megfelelő intézkedéseket teszünk annak biztosítására, hogy a megbízott vagy feldolgozó ténylegesen olyan módon dolgozza fel a továbbított személyes adatokat, amely megfelel a DPF elveinek való megfelelésünkkel; (iv) megköveteljük a megbízottól vagy feldolgozótól, hogy értesítse szervezetünket, ha úgy találja, hogy már nem tudja teljesíteni kötelezettségét a DPF elveinek megfelelő szintű védelem biztosítására; (v) értesítés, beleértve a (iv) pontot, esetén megfelelő és megfelelő lépéseket teszünk az engedély nélküli adatkezelés leállítására és a helyreállítás érdekében; és (vi) a DPF Department kérésére összefoglalót vagy reprezentatív példányt nyújtunk a megbízottal kötött szerződésünk releváns adatvédelmi rendelkezéseiről.

Az EU-U.S. DPF és/vagy a UK Extension to the EU-U.S. DPF és/vagy a Swiss-U.S. DPF előírásainak megfelelően vállalatunk kötelezi magát arra, hogy együttműködik az EU adatvédelmi hatóságaival és a brit Information Commissioner's Office-szal (ICO), valamint a svájci Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) hivatallal, és követi azok tanácsait a személyes adatok kezelésével kapcsolatos, megoldatlan panaszok tekintetében, amelyeket az EU-U.S. DPF, a UK Extension to the EU-U.S. DPF és a Swiss-U.S. DPF alapján kapunk munkaviszonyban.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

Minden olyan érintettet, aki ideiglenesen az Európai Unióban (EU), az Európai Gazdasági Térségben (EGT) vagy az Egyesült Királyságban tartózkodik, vagy ott rendelkezik lakóhellyel vagy szokásos tartózkodási hellyel, megilletik az átláthatósági dokumentumunkban közzétett jogok és az érintettek jogai, amelyek a GDPR 15-22. cikkéből is következnek, beleértve a személyes adatokhoz való hozzáférés jogát. Ezt a tájékoztatást az EU és az EGT valamennyi nyelvén elérhetővé tettük. Az angol nyelvű változat az Egyesült Királyságra vonatkozik.

Minden olyan érintettet, aki ideiglenesen Svájcban tartózkodik, vagy ott rendelkezik lakóhellyel vagy szokásos tartózkodási hellyel, megilletnek a svájci adatvédelmi törvény (DPA) és a svájci adatvédelmi rendelet (DPR) szerinti jogok és az érintettek jogai, amelyeket az átláthatósági dokumentumunkban teszünk közzé, beleértve a személyes adatokhoz való hozzáférés jogát. Ezt a tájékoztatást Svájc három hivatalos nyelvén (németül, olaszul és franciául) adtuk meg.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

# ROMANIAN: Informații despre prelucrarea datelor cu caracter personal (Articolul 13, 14 GDPR)

Stimate domnule sau doamnă,

Datele personale ale fiecărei persoane care are o relație contractuală, precontractuală sau de altă natură cu compania noastră merită o protecție specială. Scopul nostru este să păstrăm nivelul de protecție a datelor la un nivel înalt. Prin urmare, dezvoltăm în mod curent conceptele noastre privind protecția datelor și securitatea datelor.

Desigur, respectăm prevederile legale privind protecția datelor. În conformitate cu articolul 13, 14 GDPR, operatorii îndeplinesc cerințele specifice privind informațiile atunci când colectează date cu caracter personal. Acest document îndeplinește aceste obligații.

Terminologia privind reglementările legale este complicată. Din păcate, utilizarea termenilor legali nu a putut fi eliminată în pregătirea acestui document. Prin urmare, am dori să subliniem că sunteți întotdeauna bineveniți să ne contactați pentru toate întrebările referitoare la acest document, termenii sau formulările folosite.

## I. Respectarea cerințelor de informare în cazul în care datele cu caracter personal sunt colectate de la persoana vizată (articolul 13 GDPR)

### A. Identitatea și datele de contact ale operatorului (articolul 13 alineatul (1) lit. a GDPR)

Vezi deasupra

### B. Datele de contact ale responsabilului cu protecția datelor (articolul 13 alineatul (1) lit. b. GDPR)

Vezi deasupra


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## C. Scopurile prelucrării pentru care sunt destinate datele cu caracter personal, precum și temeiul juridic al prelucrării (articolul 13 alineatul (1) lit. c din GDPR)

Scopul prelucrării datelor cu caracter personal este gestionarea tuturor operațiunilor care privesc operatorul, clienții, potențialii clienți, partenerii de afaceri sau alte relații contractuale sau precontractuale dintre grupurile numite (în sensul cel mai larg) sau obligațiile legale ale operatorului.

Art. 6 (1) lit. a GDPR servește ca bază legală pentru operațiunile de procesare pentru care obținem consimțământul pentru un anumit scop al prelucrării. Dacă prelucrarea datelor cu caracter personal este necesară pentru executarea unui contract la care este parte persoana vizată, cum este cazul, de exemplu, atunci când operațiunile de prelucrare sunt necesare pentru furnizarea de bunuri sau pentru furnizarea oricărui alt serviciu, prelucrarea este în temeiul articolului 6 alineatul (1) lit. b GDPR. Același lucru este valabil și pentru operațiunile de prelucrare care sunt necesare pentru efectuarea măsurilor precontractuale, de exemplu în cazul anchetelor referitoare la produsele sau serviciile noastre. Compania noastră este supusă obligației legale prin care este necesară prelucrarea datelor cu caracter personal, cum ar fi îndeplinirea obligațiilor fiscale, prelucrarea se face pe baza art. 6 (1) lit. c GDPR.

În cazuri rare, prelucrarea datelor cu caracter personal poate fi necesară pentru a proteja interesele vitale ale persoanei vizate sau ale unei alte persoane fizice. Acesta ar fi cazul, de exemplu, în cazul în care un vizitator a fost rănit în compania noastră și numele, vârsta, datele de asigurare de sănătate sau alte informații vitale ar trebui să fie transmise unui medic, spital sau unei alte terțe părți. Apoi, prelucrarea se va baza pe Art. 6 (1) lit. d GDPR.

În cazul în care prelucrarea este necesară pentru îndeplinirea unei sarcini de interes public sau în exercitarea autorității publice cu care este învestit operatorul, temeiul juridic este Art. 6 (1) lit. e GDPR.

În cele din urmă, operațiunile de prelucrare s-ar putea baza pe articolul 6 alineatul (1) lit. f GDPR. Acest temei juridic este utilizat pentru operațiunile de prelucrare care nu sunt acoperite de niciunul dintre motivele juridice menționate mai sus, dacă prelucrarea este necesară pentru interesele legitime urmărite de compania noastră sau de o terță parte, cu excepția cazului în care aceste interese sunt în contradicție cu alte drepturi și libertăți fundamentale ale persoanei vizate care necesită protecție a datelor cu caracter personal. Astfel de operațiuni de prelucrare sunt în mod special permise deoarece au fost menționate în mod specific de legiuitorul european. El a considerat că ar putea fi asumat un interes legitim dacă persoana vizată este clientul operatorului (Considerentul 47 din propoziția 2 GDPR).

## D. În cazul în care prelucrarea se bazează pe articolul 6 alineatul (1) lit. f GDPR interesele legitime urmărite de operator sau de o terță parte (Articolul 13 (1) lit. d GDPR)

În cazul în care prelucrarea datelor cu caracter personal se bazează pe articolul 6 alineatul (1) lit. f GDPR interesul nostru legitim este să ne desfășurăm afacerea în favoarea bunăstării tuturor angajaților și acționarilor noștri.


© All rights reserved by Heiko Maniero.

## E. Categorii de destinatari ai datelor cu caracter personal (Articolul 13 (1) lit. e GDPR)

Autoritățile publice

Organismele externe

Alte organisme externe

Procesare internă

Procesare în cadrul grupului

Alte organisme

O listă a persoanelor împuternicite de către noi și a destinatarilor de date din țări terțe și, dacă este cazul, a organizațiilor internaționale este publicată pe site-ul nostru web sau poate fi solicitată gratuit de la noi. Vă rugăm să contactați responsabilul nostru cu protecția datelor pentru a solicita această listă.

## F. Destinatarii dintr-o țară terță și garanțiile corespunzătoare adecvate și mijloacele prin care se obțin o copie a acestora sau în cazul în care acestea au fost puse la dispoziție [articolul 13 alineatul (1) lit. f, articolul 46 alineatul (1), articolul 46 alineatul (2) lit. c GDPR)

Toate companiile și sucursalele care fac parte din grupul nostru (denumite în continuare "societăți grup") care își au sediul sau un birou într-o țară terță pot aparține destinatarilor datelor cu caracter personal. O listă a tuturor companiilor din grup sau a destinatarilor poate fi solicitată de la noi.

În conformitate cu articolul 46 alineatul (1) din GDPR, un operator sau o persoana împuternicită de operator poate transfera date cu caracter personal numai unei țări terțe, în cazul în care operatorul sau persoana împuternicită de operator a furnizat garanții adecvate și cu condiția ca drepturile persoanelor vizate aplicabile și căile de atac efective să fie disponibile pentru persoanele vizate. Pot fi furnizate garanții adecvate fără a necesita o autorizare specifică din partea unei autorități de supraveghere prin intermediul unor clauze contractuale standard, articolul 46 alineatul (2) lit. c GDPR.

Clauzele contractuale standard ale Uniunii Europene sau alte garanții adecvate sunt convenite cu toți beneficiarii din țările terțe înainte de prima transmitere a datelor cu caracter personal. În consecință, se asigură garanțiile adecvate, drepturile aplicabile ale persoanelor vizate și căile de atac eficiente pentru persoanele vizate. Fiecare persoană vizată poate obține de la noi o copie a clauzelor contractuale


© All rights reserved by Heiko Maniero.

standard. Clauzele contractuale standard sunt, de asemenea, disponibile în Jurnalul Oficial al Uniunii Europene.

Articolul 45 alineatul (3) din Regulamentul general privind protecția datelor (RGPD) acordă Comisiei Europene dreptul de a decide, prin intermediul unui act de punere în aplicare, că o țară din afara UE oferă un nivel de protecție adecvat. Acest lucru înseamnă un nivel de protecție a datelor cu caracter personal care este, în linii mari, echivalent cu cel din UE. Efectul deciziilor prin care se constată un nivel de protecție adecvat este că datele cu caracter personal pot circula liber din UE (și din Norvegia, Liechtenstein și Islanda) către o țară terță fără alte obstacole. Reguli similare se aplică în Regatul Unit, în Elveția și în alte câteva țări.

În cazul în care Comisia Europeană sau guvernul unei alte țări decide că o țară terță oferă un nivel adecvat de protecție, iar cadrul aplicabil (de exemplu, EU-U.S. Data Privacy Framework, Swiss-U.S. Data Privacy Framework, UK Extension to the EU-U.S. Data Privacy Framework), toate transferurile efectuate de noi către membrii acestor cadre (de exemplu, entități autocertificate) se bazează exclusiv pe apartenența acestor entități la cadrul relevant. În cazul în care noi sau una dintre entitățile din grupul nostru este membră a unui astfel de cadru, toate transferurile către noi sau către entitatea din grupul nostru se bazează exclusiv pe apartenența entității respective la un astfel de cadru.

Orice persoană vizată poate obține o copie a cadrelor de la noi. În plus, cadrele sunt, de asemenea, disponibile în Jurnalul Oficial al Uniunii Europene sau în materialele juridice publicate sau pe site-urile web ale autorităților de supraveghere sau ale altor autorități sau instituții competente.

## G. Perioada pentru care datele cu caracter personal vor fi stocate sau, dacă acest lucru nu este posibil, criteriile utilizate pentru stabilirea acestei perioade (articolul 13 alineatul (2) lit. a GDPR)

Criteriile utilizate pentru a determina perioada de stocare a datelor cu caracter personal sunt perioada de păstrare legală respectivă. După expirarea perioadei respective, datele corespunzătoare sunt șterse în mod curent, atât timp cât nu mai sunt necesare pentru îndeplinirea contractului sau inițierea unui contract.

În cazul în care nu există o perioadă de păstrare legală, criteriul este perioada de păstrare contractuală sau internă.

## H. Existența dreptului de a solicita operatorului accesul la rectificarea sau ștergerea datelor cu caracter personal sau limitarea prelucrării cu privire la persoana vizată sau de a se opune prelucrării, precum și dreptul la portabilitatea datelor (articolul 13 alineatul (2) lit. b GDPR)

Toate persoanele vizate au următoarele drepturi:


© All rights reserved by Heiko Maniero.

***Dreptul de acces***

Fiecare persoană vizată are dreptul de a accesa datele personale pe care o privesc. Dreptul de acces se extinde la toate datele procesate de noi. Dreptul poate fi exercitat cu ușurință și la intervale rezonabile, pentru a cunoaște și verifica legalitatea procesării (Considerentul 63 din GDPR). Acest drept rezultă din Art. 15 GDPR. Persoana vizată ne poate contacta pentru a-și exercita dreptul de acces.

***Dreptul la rectificare***

În conformitate cu articolul 16 alineatul (1) din GDPR, persoana vizată are dreptul de a obține de la operator, fără întârzieri nejustificate, rectificarea datelor personale inexacte cu privire la acesta. Mai mult, articolul 16 din GDPR prevede că persoana vizată are dreptul, ținând cont de scopurile prelucrării, de a avea aceste date personale incomplete completate, inclusiv prin furnizarea unei declarații suplimentare. Persoana vizată ne poate contacta pentru a-și exercita dreptul de rectificare.

***Dreptul de ștergere (dreptul de a fi uitat)***

În plus, persoanele vizate au dreptul la ștergerea datelor și de a fi uitate conform art. 17 GDPR. Acest drept poate fi, de asemenea, exercitat prin contactarea noastră. Cu toate acestea, în acest moment, am dori să subliniem că acest drept nu se aplică în măsura în care prelucrarea este necesară pentru a îndeplini o obligație legală la care se supune societatea noastră, articolul 17 alineatul (3) lit. b GDPR. Aceasta înseamnă că putem aproba o cerere de ștergere numai după expirarea perioadei legale de păstrare.

***Dreptul la restricționarea prelucrării***

Conform articolului 18 GDPR, orice persoană vizată are dreptul la o restricționare a prelucrării. Limitarea prelucrării poate fi cerută dacă una dintre condițiile prevăzute la articolul 18 alineatul (1) lit. a- d GDPR este îndeplinită. Persoana vizată ne poate contacta pentru a exercita dreptul la restricționarea prelucrării.

***Dreptul de a obiecta***

Mai mult, art. 21 GDPR garantează dreptul de a obiecta. Persoana vizată ne poate contacta pentru a-și exercita dreptul de a prezenta obiecții.

***Dreptul la portabilitatea datelor***

Art. 20 GDPR acordă persoanei vizate dreptul la portabilitatea datelor. În conformitate cu această dispoziție, persoana vizată are, în condițiile prevăzute la articolul 20 alineatul (1) litera a și b GDPR dreptul de a primi datele personale cu privire la el sau ea, pe care le-a furnizat unui operator, într-un format structurat, utilizat în mod obișnuit și care poate fi citit și are dreptul să transmită aceste date altui operator fără să împiedice operatorul la care au fost furnizate datele cu caracter personal. Persoana vizată ne poate contacta pentru a-și exercita dreptul la transferabilitatea datelor.


© All rights reserved by Heiko Maniero.

## I. Existența dreptului de retragere a consimțământului în orice moment, fără a afecta legalitatea prelucrării bazate pe consimțământ înainte de retragerea sa, în cazul în care prelucrarea se bazează pe articolul 6 alineatul (1) lit. a GDPR sau articolul 9 alineatul (2) lit. a GDPR (articolul 13 alineatul (2) lit. c GDPR)

Dacă prelucrarea datelor cu caracter personal se bazează pe Art. 6 (1) lit. a GDPR, în cazul în care persoana vizată și-a dat acordul pentru prelucrarea datelor cu caracter personal în unul sau mai multe scopuri specifice sau se bazează pe articolul 9 alineatul (2) lit. a GDPR care reglementează consimțământul explicit pentru prelucrarea categoriilor speciale de date cu caracter personal, persoana vizată are dreptul de a-și retrage consimțământul în orice moment în conformitate cu articolul 7 alineatul (3) punctul 1 GDPR.

Retragerea consimțământului nu afectează legalitatea prelucrării pe baza consimțământului înainte de retragerea sa, articolul 7 alineatul (3) din propoziția 2 GDPR. Este la fel de ușor să se retragă și să dea consimțământul, Art. 7 (3) Propoziția 4 GDPR. Prin urmare, retragerea consimțământului poate avea loc întotdeauna în același mod în care a fost acordat consimțământul sau în orice alt mod, care este considerat de către persoana vizată ca fiind mai simplu. În societatea informațională de astăzi, probabil cea mai simplă modalitate de retragere a consimțământului este un simplu e-mail. Dacă persoana vizată dorește să-și retragă consimțământul acordat nouă, este suficient să ne trimiteți un e-mail. În mod alternativ, persoana vizată poate alege orice alt mod de a comunica retragerea consimțământului.

## J. Dreptul de a depune o plângere la o autoritate de supraveghere (articolul 13 alineatul (2) lit. d, articolul 77 alineatul (1) din GDPR)

În calitate de operator, suntem obligați să notificăm persoanei vizate dreptul de a depune o plângere la o autoritate de supraveghere, articolul 13 alineatul (2) lit. d GDPR. Dreptul de a depune o plângere la o autoritate de supraveghere este reglementat de articolul 77 alineatul (1) din GDPR. Conform acestei dispoziții, fără a aduce atingere oricărei alte căi de atac administrative sau judiciare, fiecare persoană vizată are dreptul de a depune o plângere la o autoritate de supraveghere, în special în statul membru în care își are reședința obișnuită, locul de muncă sau locul de muncă unde s-a desfășurat presupusa încălcare în cazul în care persoana vizată consideră că prelucrarea datelor cu caracter personal care o privesc încalcă regulamentul general privind protecția datelor. Dreptul de a depune o plângere la o autoritate de supraveghere a fost limitat doar de legea Uniunii astfel încât să poată fi exercitat numai în fața unei autorități unice de supraveghere (considerentul 141 din propunerea 1 GDPR). Această regulă vizează evitarea plângerilor duble ale aceluiași subiect de date în aceeași chestiune. Dacă un subiect de date dorește să depună o plângere în legătură cu noi, am solicitat, prin urmare, să contactați numai o singură autoritate de supraveghere.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

### K. Furnizarea de date cu caracter personal ca cerință statutară sau contractuală; Cerința necesară pentru a încheia un contract; Obligația persoanei vizate de a furniza datele cu caracter personal; consecințele posibile ale neîndeplinirii furnizării cestor date [articolul 13 alineatul (2) lit. e din GDPR]

Clarificăm că furnizarea de date cu caracter personal este cerută parțial de lege (de ex. Reglementări fiscale) sau poate rezulta și din dispoziții contractuale (de exemplu, informații despre partenerul contractual).

Uneori poate fi necesar să se încheie un contract conform căruia persoana vizată ne furnizează date cu caracter personal, care trebuie prelucrate ulterior de noi. Persoana vizată este, de exemplu, obligată să ne furnizeze date cu caracter personal atunci când compania noastră semnează un contract cu el sau ea. Nefurnizarea datelor cu caracter personal ar avea drept consecință faptul că persoana vizată nu a putut încheia contractul respectiv.

Înainte de a furniza date cu caracter personal către persoana vizată, aceasta trebuie să ne contacteze. Vom clarifica persoanei vizate dacă furnizarea datelor cu caracter personal este prevăzută de lege sau contract sau este necesară pentru încheierea contractului, dacă există o obligație de a furniza datele cu caracter personal, precum și consecințele nefurnizării datelor cu caracter personal.

### L. Existența unui proces automat de luare a deciziilor, inclusiv profilarea, menționat la articolul 22 alineatele (1) și (4) din GDPR și, cel puțin în acele cazuri, informațiile semnificative cu privire la logica implicată, precum și semnificația și consecințele preconizate ale unei astfel de procesări pentru persoana vizată (articolul 13 alineatul (2) lit. f GDPR)

În calitate de companie responsabilă, de obicei nu folosim procesul decizional automatizat sau crearea de profiluri. Dacă, în cazuri excepționale, efectuăm luarea automată a deciziilor sau crearea de profiluri, vom informa persoana vizată fie separat, fie printr-o subsecțiune din politica noastră de confidențialitate (pe site-ul nostru web). În acest caz, se aplică următoarele:

Luarea automată a deciziilor - inclusiv crearea de profiluri - poate avea loc dacă (1) acest lucru este necesar pentru încheierea sau executarea unui contract între persoana vizată și noi sau (2) acest lucru este autorizat de legislația Uniunii sau a unui stat membru căreia îi suntem supuși și care stabilește, de asemenea, măsuri adecvate pentru a proteja drepturile și libertățile și interesele legitime ale persoanei vizate; sau (3) acest lucru se bazează pe consimțământul explicit al persoanei vizate.

În cazurile menționate la articolul 22 alineatul (2) literele (a) și (c) din GDPR, vom pune în aplicare măsuri adecvate pentru a proteja drepturile și libertățile și interesele legitime ale persoanei vizate. În aceste cazuri, aveți dreptul de a obține o intervenție umană din partea operatorului, de a vă exprima punctul de vedere și de a contesta decizia.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

Informații semnificative despre logica implicată, precum și despre semnificația și consecințele preconizate ale unei astfel de prelucrări pentru persoana vizată sunt prezentate în politica noastră de confidențialitate.

## II. Respectarea cerințelor privind informațiile în cazul în care datele cu caracter personal nu sunt colectate de la persoana vizată (articolul 14 din GDPR)

### A. Identitatea și datele de contact ale operatorului (articolul 14 alineatul (1) lit. a GDPR)

Vezi deasupra

### B. Datele de contact ale responsabilului cu protecția datelor (articolul 14 alineatul (1) lit. b GDPR)

Vezi deasupra

### C. Scopurile prelucrării pentru care sunt destinate datele cu caracter personal, precum și temeiul juridic al prelucrării (articolul 14 alineatul (1) lit. c din GDPR)

Scopul prelucrării datelor cu caracter personal este gestionarea tuturor operațiunilor care privesc operatorul, clienții, potențialii clienți, partenerii de afaceri sau alte relații contractuale sau precontractuale dintre grupurile numite (în sensul cel mai larg) sau obligațiile legale ale operatorului.

Dacă prelucrarea datelor cu caracter personal este necesară pentru executarea unui contract la care este parte persoana vizată, cum este cazul, de exemplu, atunci când operațiunile de prelucrare sunt necesare pentru furnizarea de bunuri sau pentru furnizarea oricărui alt serviciu, prelucrarea este în temeiul articolului 6 alineatul (1) lit. b GDPR. Același lucru este valabil și pentru operațiunile de prelucrare care sunt necesare pentru efectuarea măsurilor precontractuale, de exemplu în cazul anchetelor referitoare la produsele sau serviciile noastre. Compania noastră este supusă obligației legale care se referă la necesitatea prelucrării datelor cu caracter personal, cum ar fi îndeplinirea obligațiilor fiscale; prelucrarea se face pe baza art. 6 (1) lit. c GDPR.

În cazuri rare, prelucrarea datelor cu caracter personal poate fi necesară pentru a proteja interesele vitale ale persoanei vizate sau ale unei alte persoane fizice. Acesta ar fi cazul, de exemplu, în cazul în care un vizitator a fost rănit în compania noastră și numele, vârsta, datele de asigurare de sănătate sau alte


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

informații vitale ar trebui să fie transmise unui medic, spital sau unei alte terțe părți. Apoi, prelucrarea se va baza pe Art. 6 (1) lit. d GDPR.

În cazul în care prelucrarea este necesară pentru îndeplinirea unei sarcini de interes public sau în exercitarea autorității publice cu care este învestit operatorul, temeiul juridic este Art. 6 (1) lit. e GDPR.

În cele din urmă, operațiunile de prelucrare s-ar putea baza pe articolul 6 alineatul (1) lit. f GDPR. Acest temei juridic este utilizat pentru operațiunile de prelucrare care nu sunt acoperite de niciunul dintre motivele juridice menționate mai sus, dacă prelucrarea este necesară pentru interesele legitime urmărite de compania noastră sau de o terță parte, cu excepția cazului în care aceste interese sunt înlăturate de interesele sau drepturile și libertățile fundamentale ale persoanei vizate care necesită protecția datelor cu caracter personal. Astfel de operațiuni de prelucrare sunt în mod special permise deoarece au fost menționate în mod specific de legiuitorul european. El a considerat că ar putea fi asumat un interes legitim dacă persoana vizată este clientul operatorului (Considerentul 47 din propoziția 2 GDPR).

## D. Categoriile de date cu caracter personal vizate (articolul 14 alineatul (1) lit. d GDPR)

Datele despre consumator

Datele potențialilor clienți

Datele furnizorilor

## E. Categorii de destinatari ai datelor cu caracter personal (Articolul 14 (1) lit. e GDPR)

Autorități publice

Organismele externe

Alte organisme externe

Procesare internă

Procesare în cadrul grupului

Alte organisme


© All rights reserved by Heiko Maniero.

O listă a persoanelor împuternicite de către noi și a destinatarilor de date din țări terțe și, dacă este cazul, a organizațiilor internaționale este publicată pe site-ul nostru web sau poate fi solicitată gratuit de la noi. Vă rugăm să contactați responsabilul nostru cu protecția datelor pentru a solicita această listă.

## F. Beneficiarii dintr-o țară terță și garanțiile adecvate precum și mijloacele prin care să se obțină o copie a acestora sau în cazul în care acestea au fost puse la dispoziție [articolul 14 alineatul (1) lit. f, articolul 46 alineatul (1), articolul 46 alineatul (2) lit. c GDPR)

Toate companiile și sucursalele care fac parte din grupul nostru (denumite în continuare "societăți de grup") care își au sediul sau un birou într-o țară terță pot aparține destinatarilor datelor cu caracter personal. O listă a tuturor companiilor din grup poate fi solicitată de la noi.

În conformitate cu articolul 46 alineatul (1) din GDPR, un operator sau o persoană împuternicită de operator poate transfera datele cu caracter personal numai unei țări terțe, în cazul în care operatorul sau persoana împuternicită de operator a furnizat garanții adecvate și cu condiția ca drepturile persoanelor vizate aplicabile și căile de atac efective să fie disponibile pentru persoanele vizate. Pot fi furnizate garanții adecvate fără a solicita o autorizare specifică din partea unei autorități de supraveghere prin intermediul unor clauze standard de protecție a datelor, articolul 46 alineatul (2) lit. c GDPR.

Clauzele contractuale standard ale Uniunii Europene sau alte garanții adecvate sunt convenite cu toți beneficiarii din țările terțe înainte de prima transmitere a datelor cu caracter personal. În consecință, se asigură garanțiile adecvate, drepturile aplicabile ale persoanelor vizate și căile de atac eficiente pentru persoanele vizate. Fiecare persoană vizată poate obține de la noi o copie a clauzelor contractuale standard. Clauzele contractuale standard sunt, de asemenea, disponibile în Jurnalul Oficial al Uniunii Europene.

Articolul 45 alineatul (3) din Regulamentul general privind protecția datelor (RGPD) acordă Comisiei Europene dreptul de a decide, prin intermediul unui act de punere în aplicare, că o țară din afara UE oferă un nivel de protecție adecvat. Acest lucru înseamnă un nivel de protecție a datelor cu caracter personal care este, în linii mari, echivalent cu cel din UE. Efectul deciziilor prin care se constată un nivel de protecție adecvat este că datele cu caracter personal pot circula liber din UE (și din Norvegia, Liechtenstein și Islanda) către o țară terță fără alte obstacole. Reguli similare se aplică în Regatul Unit, în Elveția și în alte câteva țări.

În cazul în care Comisia Europeană sau guvernul unei alte țări decide că o țară terță oferă un nivel adecvat de protecție, iar cadrul aplicabil (de exemplu, EU-U.S. Data Privacy Framework, Swiss-U.S. Data Privacy Framework, UK Extension to the EU-U.S. Data Privacy Framework), toate transferurile efectuate de noi către membrii acestor cadre (de exemplu, entități autocertificate) se bazează exclusiv pe apartenența acestor entități la cadrul relevant. În cazul în care noi sau una dintre entitățile din grupul


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

nostru este membră a unui astfel de cadru, toate transferurile către noi sau către entitatea din grupul nostru se bazează exclusiv pe apartenența entității respective la un astfel de cadru.

Orice persoană vizată poate obține o copie a cadrelor de la noi. În plus, cadrele sunt, de asemenea, disponibile în Jurnalul Oficial al Uniunii Europene sau în materialele juridice publicate sau pe site-urile web ale autorităților de supraveghere sau ale altor autorități sau instituții competente.

## G. Perioada pentru care datele cu caracter personal vor fi stocate sau, dacă acest lucru nu este posibil, criteriile utilizate pentru a determina acea perioadă (Articolul 14 (2) lit. a GDPR)

Criteriile utilizate pentru a determina perioada de stocare a datelor cu caracter personal sunt perioada de păstrare legală respectivă. După expirarea perioadei respective, datele corespunzătoare sunt șterse în mod curent, atât timp cât nu mai sunt necesare pentru îndeplinirea contractului sau inițierea unui contract.

În cazul în care nu există o perioadă de păstrare legală, criteriul este perioada de păstrare contractuală sau internă.

## H. Notificarea intereselor legitime urmărite de operator sau de o terță parte în cazul în care prelucrarea se bazează pe articolul 6 alineatul (1) lit. f GDPR (articolul 14 alineatul (2) lit. b GDPR)

În conformitate cu articolul 6 alineatul (1) lit. f, prelucrarea este legală numai dacă aceasta este necesară în scopul îndeplinirii intereselor legitime urmărite de operator sau de o terță parte, cu excepția cazului în care aceste interese sunt înlăturate de interesele sau de drepturile și libertățile fundamentale ale persoanei vizate care necesită protecția datelor cu caracter personal. În conformitate cu Considerentul 47 din propunerea 2 GDPR, ar putea exista un interes legitim în cazul în care există o relație relevantă și adecvată între persoana vizată și operator, de ex. în situațiile în care persoana vizată este clientul operatorului. În toate cazurile în care societatea noastră procesează date personale în baza articolului 6 alineatul (1) lit. f GDPR, interesul nostru legitim este să ne desfășurăm afacerea în favoarea bunăstării tuturor angajaților și a acționarilor.

## I. Existența dreptului de a solicita operatorului accesul la rectificarea sau ștergerea datelor cu caracter personal sau limitarea prelucrării cu privire la persoana vizată sau de a se opune prelucrării, precum și dreptul la portabilitatea datelor (articolul 13 alineatul (2) lit. b GDPR)

Toate persoanele vizate au următoarele drepturi:


© All rights reserved by Heiko Maniero.

***Dreptul de acces***

Fiecare persoană vizată are dreptul de a accesa datele personale pe care o privesc. Dreptul de acces se extinde la toate datele procesate de noi. Dreptul poate fi exercitat cu ușurință și la intervale rezonabile, pentru a cunoaște și verifica legalitatea procesării (Considerentul 63 din GDPR). Acest drept rezultă din Art. 15 GDPR. Persoana vizată ne poate contacta pentru a-și exercita dreptul de acces.

***Dreptul la rectificare***

În conformitate cu articolul 16 alineatul (1) din GDPR, persoana vizată are dreptul de a obține de la operator, fără întârzieri nejustificate, rectificarea datelor personale inexacte cu privire la acesta. Mai mult, articolul 16 din GDPR prevede că persoana vizată are dreptul, ținând cont de scopurile prelucrării, de a avea aceste date personale incomplete completate, inclusiv prin furnizarea unei declarații suplimentare. Persoana vizată ne poate contacta pentru a-și exercita dreptul de rectificare.

***Dreptul de ștergere (dreptul de a fi uitat)***

În plus, persoanele vizate au dreptul la ștergerea datelor și de a fi uitate conform art. 17 GDPR. Acest drept poate fi, de asemenea, exercitat prin contactarea noastră. Cu toate acestea, în acest moment, am dori să subliniem că acest drept nu se aplică în măsura în care prelucrarea este necesară pentru a îndeplini o obligație legală la care se supune societatea noastră, articolul 17 alineatul (3) lit. b GDPR. Aceasta înseamnă că putem aproba o cerere de ștergere numai după expirarea perioadei legale de păstrare.

***Dreptul la restricționarea prelucrării***

Conform articolului 18 GDPR, orice persoană vizată are dreptul la o restricționare a prelucrării. Limitarea prelucrării poate fi cerută dacă una dintre condițiile prevăzute la articolul 18 alineatul (1) lit. a- d GDPR este îndeplinită. Persoana vizată ne poate contacta pentru a exercita dreptul la restricționarea prelucrării.

***Dreptul de a obiecta***

Mai mult, art. 21 GDPR garantează dreptul de a obiecta. Persoana vizată ne poate contacta pentru a-și exercita dreptul de a prezenta obiecții.

***Dreptul la portabilitatea datelor***

Art. 20 GDPR acordă persoanei vizate dreptul la portabilitatea datelor. În conformitate cu această dispoziție, persoana vizată are, în condițiile prevăzute la articolul 20 alineatul (1) litera a și b GDPR dreptul de a primi datele personale cu privire la el sau ea, pe care le-a furnizat unui operator, într-un format structurat, utilizat în mod obișnuit și care poate fi citit și are dreptul să transmită aceste date altui operator fără să împiedice operatorul la care au fost furnizate datele cu caracter personal. Persoana vizată ne poate contacta pentru a-și exercita dreptul la transferabilitatea datelor.


© All rights reserved by Heiko Maniero.

## J. Existența dreptului de retragere a consimțământului în orice moment, fără a afecta legalitatea prelucrării pe baza consimțământului înainte de retragerea acestuia, în cazul în care prelucrarea se bazează pe articolul 6 alineatul (1) lit. a sau articolul 9 alineatul (2) lit. a GDPR (articolul 14 alineatul (2) lit. d GDPR)

Dacă prelucrarea datelor cu caracter personal se bazează pe Art. 6 (1) lit. a GDPR, în cazul în care persoana vizată și-a dat acordul pentru prelucrarea datelor cu caracter personal în unul sau mai multe scopuri specifice sau se bazează pe articolul 9 alineatul (2) litera a GDPR care reglementează consimțământul explicit pentru prelucrarea categoriilor speciale de date cu caracter personal, persoana vizată are dreptul de a-și retrage consimțământul în orice moment în conformitate cu articolul 7 alineatul (3) punctul 1. GDPR.

Retragerea consimțământului nu afectează legalitatea prelucrării pe baza consimțământului înainte de retragerea sa, articolul 7 alineatul (3) din propoziția 2 GDPR. Este la fel de ușor să se retragă și să dea consimțământul, Art. 7 (3) Propoziția 4 GDPR. Prin urmare, retragerea consimțământului poate avea loc întotdeauna în același mod în care a fost acordat consimțământul sau în orice alt mod, care este considerat de către persoana vizată ca fiind mai simplu. În societatea informațională de astăzi, probabil cea mai simplă modalitate de retragere a consimțământului este un simplu e-mail. Dacă persoana vizată dorește să-și retragă consimțământul acordat nouă, este suficient să ne trimiteți un e-mail. În mod alternativ, persoana vizată poate alege orice alt mod de a ne comunica retragerea consimțământului.

## K. Dreptul de a depune o plângere la o autoritate de supraveghere [articolul 14 alineatul (2) lit. e, articolul 77 alineatul (1) din GDPR]

În calitate de operator, suntem obligați să notificăm persoanei vizate dreptul de a depune o plângere la o autoritate de supraveghere, articolul 13 alineatul (2) lit. d GDPR. Dreptul de a depune o plângere la o autoritate de supraveghere este reglementat de articolul 77 alineatul (1) din GDPR. Conform acestei dispoziții, fără a aduce atingere oricărei alte căi de atac administrative sau judiciare, fiecare persoană vizată are dreptul de a depune o plângere la o autoritate de supraveghere, în special în statul membru în care își are reședința obișnuită, locul de muncă sau locul de muncă unde s-a desfășurat presupusa încălcare în cazul în care persoana vizată consideră că prelucrarea datelor cu caracter personal care o privesc încalcă regulamentul general privind protecția datelor. Dreptul de a depune o plângere la o autoritate de supraveghere a fost limitat doar de legea Uniunii astfel încât să poată fi exercitat numai în fața unei autorități unice de supraveghere (considerentul 141 din propunerea 1 GDPR). Această regulă vizează evitarea plângerilor duble ale aceluiași subiect de date în aceeași chestiune. Dacă un subiect de date dorește să depună o plângere în legătură cu noi, am solicitat, prin urmare, să contactați numai o singură autoritate de supraveghere.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## L. Sursa datelor cu caracter personal provine din surse accesibile publicului [articolul 14 alineatul (2) lit. f GDPR]

În principiu, datele cu caracter personal sunt colectate direct de la persoana vizată sau în cooperare cu o autoritate (de exemplu, recuperarea datelor dintr-un registru oficial). Alte date privind persoanele vizate provin din transferurile companiilor din grup. În contextul acestor informații generale, denumirea surselor exacte din care provin datele personale este fie imposibilă, fie ar implica un efort disproporționat în sensul art. 14 (5) lit. b GDPR. În principiu, nu colectăm date cu caracter personal din surse accesibile publicului.

Orice persoană vizată ne poate contacta în orice moment pentru a obține informații mai detaliate despre sursele exacte privind datele cu caracter personal care o privesc. În cazul în care originea datelor cu caracter personal nu poate fi furnizată persoanei vizate deoarece s-au folosit diverse surse, ar trebui să se furnizeze informații generale (considerentul 61 din propunerea 4 din GDPR).

## M. Existența unui proces automat de luare a deciziilor, inclusiv profilare, menționat la articolul 22 alineatele (1) și (4) din GDPR și, cel puțin în acele cazuri, informații semnificative cu privire la logica implicată, precum și semnificația și consecințele preconizate ale unei astfel de procesări pentru persoana vizată (articolul 14 alineatul (2) lit. g GDPR)

În calitate de companie responsabilă, de obicei nu folosim procesul decizional automatizat sau crearea de profiluri. Dacă, în cazuri excepționale, efectuăm luarea automată a deciziilor sau crearea de profiluri, vom informa persoana vizată fie separat, fie printr-o subsecțiune din politica noastră de confidențialitate (pe site-ul nostru web). În acest caz, se aplică următoarele:

Luarea automată a deciziilor - inclusiv crearea de profiluri - poate avea loc dacă (1) acest lucru este necesar pentru încheierea sau executarea unui contract între persoana vizată și noi sau (2) acest lucru este autorizat de legislația Uniunii sau a unui stat membru căreia îi suntem supuși și care stabilește, de asemenea, măsuri adecvate pentru a proteja drepturile și libertățile și interesele legitime ale persoanei vizate; sau (3) acest lucru se bazează pe consimțământul explicit al persoanei vizate.

În cazurile menționate la articolul 22 alineatul (2) literele (a) și (c) din GDPR, vom pune în aplicare măsuri adecvate pentru a proteja drepturile și libertățile și interesele legitime ale persoanei vizate. În aceste cazuri, aveți dreptul de a obține o intervenție umană din partea operatorului, de a vă exprima punctul de vedere și de a contesta decizia.

Informații semnificative despre logica implicată, precum și despre semnificația și consecințele preconizate ale unei astfel de prelucrări pentru persoana vizată sunt prezentate în politica noastră de confidențialitate.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## III. EU-U.S. Data Privacy Framework (EU-U.S. DPF), UK Extension to the EU-U.S. DPF, Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF)

Dacă organizația noastră este un membru certificat al EU-U.S. Data Privacy Framework (EU-U.S. DPF) și/sau al UK Extension to the EU-U.S. DPF și/sau al Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF), se aplică următoarele:

Ne conformăm EU-U.S. Data Privacy Framework (EU-U.S. DPF) și UK Extension to the EU-U.S. DPF, precum și Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF), așa cum este stabilit de U.S. Department of Commerce. Compania noastră a confirmat către Departamentul de Comerț al SUA că respectă EU-U.S. Data Privacy Framework Principles (EU-U.S. DPF Principles) în ceea ce privește procesarea datelor personale pe care le primește din Uniunea Europeană și Regatul Unit, invocând EU-U.S. DPF și UK Extension to the EU-U.S. DPF. Compania noastră a confirmat către Departamentul de Comerț al SUA că respectă Swiss-U.S. Data Privacy Framework Principles (Swiss-U.S. DPF Principles) în ceea ce privește procesarea datelor personale pe care le primește din Elveția, invocând Swiss-U.S. DPF. În cazul unei contradicții între prevederile politicii noastre de confidențialitate și EU-U.S. DPF Principles și/sau Swiss-U.S. DPF Principles, prevalează Principiile.

Pentru a afla mai multe despre programul Data Privacy Framework (DPF) și pentru a vedea certificarea noastră, vă rugăm să vizitați https://www.dataprivacyframework.gov/.

Celelalte unități sau filiale americane ale companiei noastre, care respectă de asemenea EU-U.S. DPF Principles, inclusiv UK Extension to the EU-U.S. DPF și Swiss-U.S. DPF Principles, dacă există, sunt menționate în politica noastră de confidențialitate.

În conformitate cu EU-U.S. DPF și UK Extension to the EU-U.S. DPF, precum și Swiss-U.S. DPF, compania noastră se angajează să colaboreze cu autoritățile europene de protecție a datelor și cu Information Commissioner's Office (ICO) din Marea Britanie, precum și cu Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) din Elveția, și să urmeze sfaturile acestora cu privire la reclamațiile nerezolvate legate de gestionarea datelor personale pe care le primim invocând EU-U.S. DPF și UK Extension to the EU-U.S. DPF și Swiss-U.S. DPF.

Informăm persoanele vizate despre autoritățile europene de protecție a datelor competente, responsabile pentru gestionarea reclamațiilor legate de modul în care organizația noastră gestionează datele personale, în partea superioară a acestui document de transparență și despre faptul că oferim persoanelor vizate o cale de atac adecvată și gratuită.

Informăm toate persoanele vizate că compania noastră este supusă competențelor de investigație și de aplicare ale Federal Trade Commission (FTC).

Persoanele vizate au, în anumite condiții, posibilitatea de a recurge la arbitraj obligatoriu. Organizația noastră este obligată să soluționeze cererile și să respecte condițiile prevăzute în Anexa I a DPF


© All rights reserved by Heiko Maniero.

Principles, în cazul în care persoana vizată a solicitat arbitraj obligatoriu, notificând organizația noastră și respectând procedurile și condițiile prevăzute în Anexa I a Principiilor.

Informăm aici toate persoanele vizate despre responsabilitatea organizației noastre în cazul transferului datelor personale către terți.

Pentru întrebările persoanelor vizate sau ale autorităților de supraveghere a protecției datelor, am desemnat reprezentanții locali menționați mai sus în acest document de transparență.

Vă oferim posibilitatea de a alege (Opt-out) dacă datele dumneavoastră personale (i) sunt transferate către terți sau (ii) sunt utilizate în scopuri care diferă substanțial de scopurile pentru care au fost colectate inițial sau ulterior autorizate de dumneavoastră. Mecanismul clar, vizibil și ușor accesibil pentru exercitarea dreptului dumneavoastră de alegere constă în contactarea prin e-mail a responsabilului nostru cu protecția datelor (DSB). Nu aveți posibilitatea de a alege și nu suntem obligați să o facem, dacă datele sunt transferate către un terț care acționează ca agent sau procesator în numele nostru și conform instrucțiunilor noastre. Totuși, încheiem întotdeauna un contract cu un astfel de agent sau procesator.

Pentru datele sensibile (adică datele personale care conțin informații despre starea de sănătate, originea rasială sau etnică, opiniile politice, convingerile religioase sau filozofice, apartenența la sindicate sau informații despre viața sexuală a persoanei vizate), obținem consimțământul dumneavoastră explicit (Opt-in) dacă aceste date (i) sunt transferate către terți sau (ii) sunt utilizate în alte scopuri decât cele pentru care au fost colectate inițial sau pentru care ați acordat ulterior consimțământul dumneavoastră prin alegerea Opt-in. În plus, tratăm toate datele personale pe care le primim de la terți ca fiind sensibile, dacă terțul le-a identificat și tratat ca fiind sensibile.

Vă informăm aici despre necesitatea dezvăluirii datelor personale ca răspuns la solicitările legitime ale autorităților, inclusiv pentru îndeplinirea cerințelor de securitate națională sau de aplicare a legii.

La transferul datelor personale către un terț care acționează ca operator, respectăm Principiile notificării și alegerii. În plus, încheiem un contract cu operatorul, care prevede că aceste date pot fi prelucrate numai în scopuri limitate și specificate, în conformitate cu consimțământul dumneavoastră, și că destinatarul oferă același nivel de protecție ca Principiile DPF și ne notifică în cazul în care constată că nu mai poate îndeplini această obligație. Contractul prevede că operatorul va înceta prelucrarea sau va lua alte măsuri adecvate și corespunzătoare pentru a remedia situația, în cazul în care se constată că nu poate îndeplini această obligație.

La transferul datelor personale către un terț care acționează ca agent sau procesator, (i) transferăm aceste date numai în scopuri limitate și specificate; (ii) ne asigurăm că agentul sau procesatorul este obligat să asigure cel puțin același nivel de protecție a datelor ca cel cerut de DPF Principles; (iii) luăm măsuri adecvate și corespunzătoare pentru a ne asigura că agentul sau procesatorul prelucrează efectiv datele personale transferate într-un mod care să fie conform cu obligațiile noastre în temeiul DPF Principles; (iv) cerem agentului sau procesatorului să notifice organizația noastră dacă constată că nu mai poate îndeplini obligația de a oferi același nivel de protecție ca cel cerut de DPF Principles; (v) după


© All rights reserved by Heiko Maniero.

notificare, inclusiv conform punctului (iv), luăm măsuri adecvate și corespunzătoare pentru a opri prelucrarea neautorizată și a remedia situația; și (vi) punem la dispoziția DPF Department, la cerere, un rezumat sau un exemplar reprezentativ al prevederilor relevante privind protecția datelor din contractul nostru cu acest agent.

În conformitate cu EU-U.S. DPF și/sau UK Extension to the EU-U.S. DPF și/sau Swiss-U.S. DPF, compania noastră se angajează să colaboreze cu autoritățile europene de protecție a datelor și cu Information Commissioner's Office (ICO) din Marea Britanie, precum și cu Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) din Elveția, și să urmeze sfaturile acestora cu privire la reclamațiile nerezolvate legate de gestionarea datelor personale pe care le primim invocând EU-U.S. DPF și UK Extension to the EU-U.S. DPF și Swiss-U.S. DPF în contextul relațiilor de muncă.

Toate persoanele vizate care se află temporar în Uniunea Europeană (UE), în Spațiul Economic European (SEE) sau în Regatul Unit, sau care își au domiciliul sau reședința obișnuită în aceste țări, beneficiază de drepturile și drepturile persoanelor vizate care sunt publicate în Documentul nostru de transparență, care decurg, de asemenea, din articolele 15-22 din RGPD, inclusiv dreptul de acces la datele cu caracter personal. Am pus la dispoziție aceste informații în toate limbile UE și SEE. Versiunea în limba engleză se aplică în Regatul Unit.

Toate persoanele vizate care au reședința temporară în Elveția sau care își au domiciliul sau reședința obișnuită în această țară beneficiază de drepturile și drepturile persoanelor vizate în temeiul Legii elvețiene privind protecția datelor (DPA) și al Regulamentului elvețian privind protecția datelor (DPR), care sunt publicate în documentul nostru de transparență, inclusiv dreptul de acces la datele cu caracter personal. Am furnizat aceste informații în cele trei limbi oficiale ale Elveției (germană, italiană și franceză).


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

# ROMANIAN: Informații privind prelucrarea datelor cu caracter personal pentru angajați și solicitanți (articolul 13, 14 GDPR)

Stimate domnule sau doamnă,

Datele personale ale angajaților și ale solicitanților merită o protecție specială. Scopul nostru este să păstrăm protecția datelor la un nivel înalt. Prin urmare, dezvoltăm în mod curent conceptele noastre privind protecția datelor și securitatea datelor.

Desigur, respectăm prevederile legale privind protecția datelor. În conformitate cu articolul 13, 14 GDPR, operatori îndeplinesc cerințele specifice de informare atunci când procesează date cu caracter personal. Acest document îndeplinește aceste obligații.

Terminologia privind reglementările juridice este complicată. Din păcate, utilizarea termenilor legali nu a putut fi eliminată în pregătirea acestui document. Prin urmare, am dori să subliniem că sunteți întotdeauna bineveniți să ne contactați pentru toate întrebările referitoare la acest document, termenii utilizați sau formulările.

## I. Respectarea cerințelor de informare în cazul în care datele cu caracter personal sunt colectate de la persoana vizată (articolul 13 GDPR)

### A. Identitatea și datele de contact ale operatorului (articolul 13 alineatul (1) lit. a GDPR)

Vezi deasupra

### B. Datele de contact ale responsabilului cu protecția datelor (articolul 13 alineatul (1) lit. b GDPR)

Vezi deasupra

### C. Scopurile prelucrării pentru care sunt destinate datele cu caracter personal, precum și temeiul juridic al prelucrării (articolul 13 alineatul (1) lit. c din GDPR)

Pentru datele solicitantului, scopul prelucrării datelor este de a efectua o examinare a cererii în timpul procesului de recrutare. În acest scop, procesăm toate datele furnizate de dvs. Pe baza datelor furnizate în timpul procesului de recrutare, vom verifica dacă sunteți invitat la un interviu de angajare (parte a


© All rights reserved by Heiko Maniero.

procesului de selecție). În cazul candidaților în general potriviți, în special în contextul interviului de angajare, procesăm anumite date personale furnizate de dvs., ceea ce este esențial pentru decizia noastră de selecție. Dacă sunteți angajat de noi, datele solicitantului se vor schimba automat în datele angajaților. Ca parte a procesului de recrutare, vom procesa alte date personale despre dvs. pe care le cerem de la dvs. și care trebuie să inițieze sau să vă îndeplinească contractul (cum ar fi numerele de identificare personale). În ceea ce privește datele angajaților, scopul prelucrării datelor este executarea contractului de muncă sau respectarea altor dispoziții legale aplicabile relației de muncă (de exemplu, dreptul fiscal), precum și utilizarea datelor dvs. personale pentru a încheia un contract de muncă (de exemplu, publicarea numelui dvs. și a informațiilor de contact din cadrul companiei sau clienților). Datele angajatului sunt stocate după încetarea raportului de muncă pentru a îndeplini perioadele de păstrare legală.

Temeiul juridic pentru prelucrarea datelor este articolul 6 alineatul (1) lit. b și f GDPR, articolul 9 alineatul (2) lit. b și h GDPR, articolul 88 (1) GDPR și legislația națională, cum ar fi pentru Germania Secțiunea 26 BDSG (Legea federală privind protecția datelor).

## D. Categorii de destinatari ai datelor cu caracter personal (Articolul 13 (1) lit. e GDPR)

Autorități publice

Organismele externe

Alte organisme externe

Procesare internă

Procesare în cadrul grupului

Alte organisme

O listă a persoanelor împuternicite de către noi și a destinatarilor de date din țări terțe și, dacă este cazul, a organizațiilor internaționale este publicată pe site-ul nostru web sau poate fi solicitată gratuit de la noi. Vă rugăm să contactați responsabilul nostru cu protecția datelor pentru a solicita această listă.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## E. Destinatarii dintr-o țară terță și garanțiile corespunzătoare adecvate și mijloacele prin care se obțin o copie a acestora sau în cazul în care acestea au fost puse la dispoziție [articolul 13 alineatul (1) lit. f, articolul 46 alineatul (1), articolul 46 alineatul (2) lit. c GDPR)

Toate companiile și sucursalele care fac parte din grupul nostru (denumite în continuare "societăți grup") care își au sediul sau un birou într-o țară terță pot aparține destinatarilor datelor cu caracter personal. O listă a tuturor companiilor din grup sau a destinatarilor poate fi solicitată de la noi.

În conformitate cu articolul 46 alineatul (1) din GDPR, un operator sau o persoana împuternicită de operator poate transfera date cu caracter personal numai unei țări terțe, în cazul în care operatorul sau persoana împuternicită de operator a furnizat garanții adecvate și cu condiția ca drepturile persoanelor vizate aplicabile și căile de atac efective să fie disponibile pentru persoanele vizate. Pot fi furnizate garanții adecvate fără a necesita o autorizare specifică din partea unei autorități de supraveghere prin intermediul unor clauze contractuale standard, articolul 46 alineatul (2) lit. c GDPR.

Clauzele contractuale standard ale Uniunii Europene sau alte garanții adecvate sunt convenite cu toți beneficiarii din țările terțe înainte de prima transmitere a datelor cu caracter personal. În consecință, se asigură garanțiile adecvate, drepturile aplicabile ale persoanelor vizate și căile de atac eficiente pentru persoanele vizate. Fiecare persoană vizată poate obține de la noi o copie a clauzelor contractuale standard. Clauzele contractuale standard sunt, de asemenea, disponibile în Jurnalul Oficial al Uniunii Europene.

Articolul 45 alineatul (3) din Regulamentul general privind protecția datelor (RGPD) acordă Comisiei Europene dreptul de a decide, prin intermediul unui act de punere în aplicare, că o țară din afara UE oferă un nivel de protecție adecvat. Acest lucru înseamnă un nivel de protecție a datelor cu caracter personal care este, în linii mari, echivalent cu cel din UE. Efectul deciziilor prin care se constată un nivel de protecție adecvat este că datele cu caracter personal pot circula liber din UE (și din Norvegia, Liechtenstein și Islanda) către o țară terță fără alte obstacole. Reguli similare se aplică în Regatul Unit, în Elveția și în alte câteva țări.

În cazul în care Comisia Europeană sau guvernul unei alte țări decide că o țară terță oferă un nivel adecvat de protecție, iar cadrul aplicabil (de exemplu, EU-U.S. Data Privacy Framework, Swiss-U.S. Data Privacy Framework, UK Extension to the EU-U.S. Data Privacy Framework), toate transferurile efectuate de noi către membrii acestor cadre (de exemplu, entități autocertificate) se bazează exclusiv pe apartenența acestor entități la cadrul relevant. În cazul în care noi sau una dintre entitățile din grupul nostru este membră a unui astfel de cadru, toate transferurile către noi sau către entitatea din grupul nostru se bazează exclusiv pe apartenența entității respective la un astfel de cadru.

Orice persoană vizată poate obține o copie a cadrelor de la noi. În plus, cadrele sunt, de asemenea, disponibile în Jurnalul Oficial al Uniunii Europene sau în materialele juridice publicate sau pe site-urile web ale autorităților de supraveghere sau ale altor autorități sau instituții competente.


© All rights reserved by Heiko Maniero.

## F. Perioada pentru care datele cu caracter personal vor fi stocate sau, dacă acest lucru nu este posibil, criteriile utilizate pentru stabilirea acestei perioade (articolul 13 alineatul (2) lit. a GDPR)

Durata păstrării datelor personale ale solicitanților este de 6 luni. Pentru datele despre salariați, se aplică respectiva perioadă de păstrare legală. După expirarea perioadei respective, datele corespunzătoare sunt șterse în mod curent, atât timp cât nu mai sunt necesare pentru îndeplinirea contractului sau inițierea unui contract.

## G. Existența dreptului de a solicita operatorului accesul la rectificarea sau ștergerea datelor cu caracter personal sau limitarea prelucrării cu privire la persoana vizată sau de a se opune prelucrării, precum și dreptul la portabilitatea datelor (articolul 13 alineatul (2) lit. b GDPR)

Toate persoanele vizate au următoarele drepturi:

***Dreptul de acces***

Fiecare persoană vizată are dreptul de a accesa datele personale pe care o privesc. Dreptul de acces se extinde la toate datele procesate de noi. Dreptul poate fi exercitat cu ușurință și la intervale rezonabile, pentru a cunoaște și verifica legalitatea procesării (Considerentul 63 din GDPR). Acest drept rezultă din Art. 15 GDPR. Persoana vizată ne poate contacta pentru a-și exercita dreptul de acces.

***Dreptul la rectificare***

În conformitate cu articolul 16 alineatul (1) din GDPR, persoana vizată are dreptul de a obține de la operator, fără întârzieri nejustificate, rectificarea datelor personale inexacte cu privire la acesta. Mai mult, articolul 16 din GDPR prevede că persoana vizată are dreptul, ținând cont de scopurile prelucrării, de a avea aceste date personale incomplete completate, inclusiv prin furnizarea unei declarații suplimentare. Persoana vizată ne poate contacta pentru a-și exercita dreptul de rectificare.

***Dreptul de ştergere (dreptul de a fi uitat)***

În plus, persoanele vizate au dreptul la ștergerea datelor și de a fi uitate conform art. 17 GDPR. Acest drept poate fi, de asemenea, exercitat prin contactarea noastră. Cu toate acestea, în acest moment, am dori să subliniem că acest drept nu se aplică în măsura în care prelucrarea este necesară pentru a îndeplini o obligație legală la care se supune societatea noastră, articolul 17 alineatul (3) lit. b GDPR. Aceasta înseamnă că putem aproba o cerere de ștergere numai după expirarea perioadei legale de păstrare.


© All rights reserved by Heiko Maniero.

***Dreptul la restricționarea prelucrării***

Conform articolului 18 GDPR, orice persoană vizată are dreptul la o restricționare a prelucrării. Limitarea prelucrării poate fi cerută dacă una dintre condițiile prevăzute la articolul 18 alineatul (1) lit. a- d GDPR este îndeplinită. Persoana vizată ne poate contacta pentru a exercita dreptul la restricționarea prelucrării.

***Dreptul de a obiecta***

Mai mult, art. 21 GDPR garantează dreptul de a obiecta. Persoana vizată ne poate contacta pentru a-și exercita dreptul de a prezenta obiecții.

***Dreptul la portabilitatea datelor***

Art. 20 GDPR acordă persoanei vizate dreptul la portabilitatea datelor. În conformitate cu această dispoziție, persoana vizată are, în condițiile prevăzute la articolul 20 alineatul (1) litera a și b GDPR dreptul de a primi datele personale cu privire la el sau ea, pe care le-a furnizat unui operator, într-un format structurat, utilizat în mod obișnuit și care poate fi citit și are dreptul să transmită aceste date altui operator fără să împiedice operatorul la care au fost furnizate datele cu caracter personal. Persoana vizată ne poate contacta pentru a-și exercita dreptul la transferabilitatea datelor.

## H. Existența dreptului de retragere a consimțământului în orice moment, fără a afecta legalitatea prelucrării bazate pe consimțământ înainte de retragerea sa, în cazul în care prelucrarea se bazează pe articolul 6 alineatul (1) lit. a GDPR sau articolul 9 alineatul (2) lit. a GDPR (articolul 13 alineatul (2) lit. c GDPR)

Dacă prelucrarea datelor cu caracter personal se bazează pe Art. 6 (1) lit. a GDPR, în cazul în care persoana vizată și-a dat acordul pentru prelucrarea datelor cu caracter personal în unul sau mai multe scopuri specifice sau se bazează pe articolul 9 alineatul (2) lit. a GDPR care reglementează consimțământul explicit pentru prelucrarea categoriilor speciale de date cu caracter personal, persoana vizată are dreptul de a-și retrage consimțământul în orice moment în conformitate cu articolul 7 alineatul (3) punctul 1 GDPR.

Retragerea consimțământului nu afectează legalitatea prelucrării pe baza consimțământului înainte de retragerea sa, articolul 7 alineatul (3) din propoziția 2 GDPR. Este la fel de ușor să se retragă și să dea consimțământul, Art. 7 (3) Propoziția 4 GDPR. Prin urmare, retragerea consimțământului poate avea loc întotdeauna în același mod în care a fost acordat consimțământul sau în orice alt mod, care este considerat de către persoana vizată ca fiind mai simplu. În societatea informațională de astăzi, probabil cea mai simplă modalitate de retragere a consimțământului este un simplu e-mail. Dacă persoana vizată dorește să-și retragă consimțământul acordat nouă, este suficient să ne trimiteți un e-mail. În mod alternativ, persoana vizată poate alege orice alt mod de a comunica retragerea consimțământului.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## I. Dreptul de a depune o plângere la o autoritate de supraveghere (articolul 13 alineatul (2) lit. d, articolul 77 alineatul (1) din GDPR)

În calitate de operator, suntem obligați să notificăm persoanei vizate dreptul de a depune o plângere la o autoritate de supraveghere, articolul 13 alineatul (2) lit. d GDPR. Dreptul de a depune o plângere la o autoritate de supraveghere este reglementat de articolul 77 alineatul (1) din GDPR. Conform acestei dispoziții, fără a aduce atingere oricărei alte căi de atac administrative sau judiciare, fiecare persoană vizată are dreptul de a depune o plângere la o autoritate de supraveghere, în special în statul membru în care își are reședința obișnuită, locul de muncă sau locul de muncă unde s-a desfășurat presupusa încălcare în cazul în care persoana vizată consideră că prelucrarea datelor cu caracter personal care o privesc încalcă regulamentul general privind protecția datelor. Dreptul de a depune o plângere la o autoritate de supraveghere a fost limitat doar de legea Uniunii astfel încât să poată fi exercitat numai în fața unei autorități unice de supraveghere (considerentul 141 din propunerea 1 GDPR). Această regulă vizează evitarea plângerilor duble ale aceluiași subiect de date în aceeași chestiune. Dacă un subiect de date dorește să depună o plângere în legătură cu noi, am solicitat, prin urmare, să contactați numai o singură autoritate de supraveghere.

## J. Furnizarea de date cu caracter personal ca cerință statutară sau contractuală; Cerința necesară pentru a încheia un contract; Obligația persoanei vizate de a furniza datele cu caracter personal; consecințele posibile ale neîndeplinirii furnizării cestor date [articolul 13 alineatul (2) lit. e din GDPR]

Clarificăm că furnizarea de date cu caracter personal este cerută parțial de lege (de ex. Reglementări fiscale) sau poate rezulta și din dispoziții contractuale (de exemplu, informații despre partenerul contractual).

Uneori poate fi necesar să se încheie un contract conform căruia persoana vizată ne furnizează date cu caracter personal, care trebuie prelucrate ulterior de noi. Persoana vizată este, de exemplu, obligată să ne furnizeze date cu caracter personal atunci când compania noastră semnează un contract cu el sau ea. Nefurnizarea datelor cu caracter personal ar avea drept consecință faptul că persoana vizată nu a putut încheia contractul respectiv..

Înainte de a furniza date cu caracter personal către persoana vizată, aceasta trebuie să ne contacteze. Vom clarifica persoanei vizate dacă furnizarea datelor cu caracter personal este prevăzută de lege sau contract sau este necesară pentru încheierea contractului, dacă există o obligație de a furniza datele cu caracter personal, precum și consecințele nefurnizării datelor cu caracter personal.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

### K. Existența unui proces automat de luare a deciziilor, inclusiv profilarea, menționat la articolul 22 alineatele (1) și (4) din GDPR și, cel puțin în acele cazuri, informațiile semnificative cu privire la logica implicată, precum și semnificația și consecințele preconizate ale unei astfel de procesări pentru persoana vizată (articolul 13 alineatul (2) lit. f GDPR)

În calitate de companie responsabilă, de obicei nu folosim procesul decizional automatizat sau crearea de profiluri. Dacă, în cazuri excepționale, efectuăm luarea automată a deciziilor sau crearea de profiluri, vom informa persoana vizată fie separat, fie printr-o subsecțiune din politica noastră de confidențialitate (pe site-ul nostru web). În acest caz, se aplică următoarele:

Luarea automată a deciziilor - inclusiv crearea de profiluri - poate avea loc dacă (1) acest lucru este necesar pentru încheierea sau executarea unui contract între persoana vizată și noi sau (2) acest lucru este autorizat de legislația Uniunii sau a unui stat membru căreia îi suntem supuși și care stabilește, de asemenea, măsuri adecvate pentru a proteja drepturile și libertățile și interesele legitime ale persoanei vizate; sau (3) acest lucru se bazează pe consimțământul explicit al persoanei vizate.

În cazurile menționate la articolul 22 alineatul (2) literele (a) și (c) din GDPR, vom pune în aplicare măsuri adecvate pentru a proteja drepturile și libertățile și interesele legitime ale persoanei vizate. În aceste cazuri, aveți dreptul de a obține o intervenție umană din partea operatorului, de a vă exprima punctul de vedere și de a contesta decizia.

Informații semnificative despre logica implicată, precum și despre semnificația și consecințele preconizate ale unei astfel de prelucrări pentru persoana vizată sunt prezentate în politica noastră de confidențialitate.

## II. Respectarea cerințelor privind informațiile în cazul în care datele cu caracter personal nu sunt colectate de la persoana vizată (articolul 14 din GDPR)

### A. Identitatea și datele de contact ale operatorului (articolul 14 alineatul (1) lit. a GDPR)

Vezi deasupra

### B. Datele de contact ale responsabilului cu protecția datelor (articolul 14 alineatul (1) lit. b GDPR)

Vezi deasupra


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## C. Scopurile prelucrării pentru care sunt destinate datele cu caracter personal, precum și temeiul juridic al prelucrării (articolul 14 alineatul (1) lit. c din GDPR)

Pentru datele solicitantului care nu au fost colectate de la persoana vizată, scopul prelucrării datelor este de a efectua o examinare a cererii în timpul procesului de recrutare. În acest scop, este posibil să procesăm date care nu au fost colectate de la dvs. Pe baza datelor procesate în timpul procesului de recrutare, vom verifica dacă sunteți invitat la un interviu de angajare (parte a procesului de selecție). Dacă sunteți angajat de noi, datele solicitantului vor fi convertite automat în datele angajaților. Pentru datele furnizate de angajați, scopul prelucrării datelor este executarea contractului de muncă sau respectarea altor dispoziții legale aplicabile relației de muncă. Datele angajatului sunt stocate după încetarea raportului de muncă pentru a îndeplini perioadele de păstrare legală.

Temeiul juridic pentru prelucrarea datelor este articolul 6 alineatul (1) lit. b și f GDPR, articolul 9 alineatul (2) lit. b și h GDPR, articolul 88 (1) GDPR și legislația națională, cum ar fi pentru Germania Secțiunea 26 BDSG (Legea federală privind protecția datelor).

## D. Categoriile de date cu caracter personal vizate (articolul 14 alineatul (1) lit. d GDPR)

Datele solicitantului

Datele angajatului

## E. Categorii de destinatari ai datelor cu caracter personal (Articolul 14 (1) lit. e GDPR)

Autorități publice

Organismele externe

Alte organisme externe

Procesare internă

Procesare în cadrul grupului

Alte organisme


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

O listă a persoanelor împuternicite de către noi și a destinatarilor de date din țări terțe și, dacă este cazul, a organizațiilor internaționale este publicată pe site-ul nostru web sau poate fi solicitată gratuit de la noi. Vă rugăm să contactați responsabilul nostru cu protecția datelor pentru a solicita această listă.

## F. Destinatarii dintr-o țară terță și garanțiile corespunzătoare adecvate și mijloacele prin care se obțin o copie a acestora sau în cazul în care acestea au fost puse la dispoziție [articolul 13 alineatul (1) lit. f, articolul 46 alineatul (1), articolul 46 alineatul (2) lit. c GDPR)

Toate companiile și sucursalele care fac parte din grupul nostru (denumite în continuare "societăți grup") care își au sediul sau un birou într-o țară terță pot aparține destinatarilor datelor cu caracter personal. O listă a tuturor companiilor din grup sau a destinatarilor poate fi solicitată de la noi.

În conformitate cu articolul 46 alineatul (1) din GDPR, un operator sau o persoana împuternicită de operator poate transfera date cu caracter personal numai unei țări terțe, în cazul în care operatorul sau persoana împuternicită de operator a furnizat garanții adecvate și cu condiția ca drepturile persoanelor vizate aplicabile și căile de atac efective să fie disponibile pentru persoanele vizate. Pot fi furnizate garanții adecvate fără a necesita o autorizare specifică din partea unei autorități de supraveghere prin intermediul unor clauze contractuale standard, articolul 46 alineatul (2) lit. c GDPR.

Clauzele contractuale standard ale Uniunii Europene sau alte garanții adecvate sunt convenite cu toți beneficiarii din țările terțe înainte de prima transmitere a datelor cu caracter personal. În consecință, se asigură garanțiile adecvate, drepturile aplicabile ale persoanelor vizate și căile de atac eficiente pentru persoanele vizate. Fiecare persoană vizată poate obține de la noi o copie a clauzelor contractuale standard. Clauzele contractuale standard sunt, de asemenea, disponibile în Jurnalul Oficial al Uniunii Europene.

Articolul 45 alineatul (3) din Regulamentul general privind protecția datelor (RGPD) acordă Comisiei Europene dreptul de a decide, prin intermediul unui act de punere în aplicare, că o țară din afara UE oferă un nivel de protecție adecvat. Acest lucru înseamnă un nivel de protecție a datelor cu caracter personal care este, în linii mari, echivalent cu cel din UE. Efectul deciziilor prin care se constată un nivel de protecție adecvat este că datele cu caracter personal pot circula liber din UE (și din Norvegia, Liechtenstein și Islanda) către o țară terță fără alte obstacole. Reguli similare se aplică în Regatul Unit, în Elveția și în alte câteva țări.

În cazul în care Comisia Europeană sau guvernul unei alte țări decide că o țară terță oferă un nivel adecvat de protecție, iar cadrul aplicabil (de exemplu, EU-U.S. Data Privacy Framework, Swiss-U.S. Data Privacy Framework, UK Extension to the EU-U.S. Data Privacy Framework), toate transferurile efectuate de noi către membrii acestor cadre (de exemplu, entități autocertificate) se bazează exclusiv pe apartenența acestor entități la cadrul relevant. În cazul în care noi sau una dintre entitățile din grupul


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

nostru este membră a unui astfel de cadru, toate transferurile către noi sau către entitatea din grupul nostru se bazează exclusiv pe apartenența entității respective la un astfel de cadru.

Orice persoană vizată poate obține o copie a cadrelor de la noi. În plus, cadrele sunt, de asemenea, disponibile în Jurnalul Oficial al Uniunii Europene sau în materialele juridice publicate sau pe site-urile web ale autorităților de supraveghere sau ale altor autorități sau instituții competente.

## G. Perioada pentru care datele cu caracter personal vor fi stocate sau, dacă acest lucru nu este posibil, criteriile utilizate pentru a determina acea perioadă (Articolul 14 (2) lit. a GDPR)

Durata păstrării datelor personale ale solicitanților este de 6 luni. Pentru datele despre salariați, se aplică respectiva perioadă de păstrare legală. După expirarea perioadei respective, datele corespunzătoare sunt șterse în mod curent, atât timp cât nu mai sunt necesare pentru îndeplinirea contractului sau inițierea unui contract.

## H. Notificarea intereselor legitime urmărite de operator sau de o terță parte în cazul în care prelucrarea se bazează pe articolul 6 alineatul (1) lit. f GDPR (articolul 14 alineatul (2) lit. b GDPR)

În conformitate cu articolul 6 alineatul (1) lit. f, prelucrarea este legală numai dacă prelucrarea este necesară în scopul intereselor legitime urmărite de operator sau de o terță parte, cu excepția cazului în care aceste interese sunt înlăturate de interesele sau de drepturile și libertățile fundamentale ale persoanei vizate care necesită protecția datele cu caracter personal. În conformitate cu considerentul 47 din propunerea 2 GDPR, ar putea exista un interes legitim în cazul în care există o relație relevantă și adecvată între persoana vizată și operator, de ex. în situațiile în care persoana vizată este clientul operatorului. În toate cazurile în care societatea noastră procesează datele solicitantului în baza articolului 6 alineatul (1) lit. f GDPR, interesul nostru legitim este angajarea personalului și a profesioniștilor adecvați.

## I. Existența dreptului de a solicita operatorului accesul la rectificarea sau ștergerea datelor cu caracter personal sau limitarea prelucrării cu privire la persoana vizată sau de a se opune prelucrării, precum și dreptul la portabilitatea datelor (articolul 13 alineatul (2) lit. b GDPR)

Toate persoanele vizate au următoarele drepturi:


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

***Dreptul de acces***

Fiecare persoană vizată are dreptul de a accesa datele personale pe care o privesc. Dreptul de acces se extinde la toate datele procesate de noi. Dreptul poate fi exercitat cu ușurință și la intervale rezonabile, pentru a cunoaște și verifica legalitatea procesării (Considerentul 63 din GDPR). Acest drept rezultă din Art. 15 GDPR. Persoana vizată ne poate contacta pentru a-și exercita dreptul de acces.

***Dreptul la rectificare***

În conformitate cu articolul 16 alineatul (1) din GDPR, persoana vizată are dreptul de a obține de la operator, fără întârzieri nejustificate, rectificarea datelor personale inexacte cu privire la acesta. Mai mult, articolul 16 din GDPR prevede că persoana vizată are dreptul, ținând cont de scopurile prelucrării, de a avea aceste date personale incomplete completate, inclusiv prin furnizarea unei declarații suplimentare. Persoana vizată ne poate contacta pentru a-și exercita dreptul de rectificare.

***Dreptul de ştergere (dreptul de a fi uitat)***

În plus, persoanele vizate au dreptul la ștergerea datelor și de a fi uitate conform art. 17 GDPR. Acest drept poate fi, de asemenea, exercitat prin contactarea noastră. Cu toate acestea, în acest moment, am dori să subliniem că acest drept nu se aplică în măsura în care prelucrarea este necesară pentru a îndeplini o obligație legală la care se supune societatea noastră, articolul 17 alineatul (3) lit. b GDPR. Aceasta înseamnă că putem aproba o cerere de ștergere numai după expirarea perioadei legale de păstrare.

***Dreptul la restricționarea prelucrării***

Conform articolului 18 GDPR, orice persoană vizată are dreptul la o restricționare a prelucrării. Limitarea prelucrării poate fi cerută dacă una dintre condițiile prevăzute la articolul 18 alineatul (1) lit. a - d GDPR este îndeplinită. Persoana vizată ne poate contacta pentru a exercita dreptul la restricționarea prelucrării.

***Dreptul de a obiecta***

Mai mult, art. 21 GDPR garantează dreptul de a obiecta. Persoana vizată ne poate contacta pentru a-și exercita dreptul de a prezenta obiecții.

***Dreptul la portabilitatea datelor***

Art. 20 GDPR acordă persoanei vizate dreptul la portabilitatea datelor. În conformitate cu această dispoziție, persoana vizată are, în condițiile prevăzute la articolul 20 alineatul (1) litera a și b GDPR dreptul de a primi datele personale cu privire la el sau ea, pe care le-a furnizat unui operator, într-un format structurat, utilizat în mod obișnuit și care poate fi citit și are dreptul să transmită aceste date altui operator fără să împiedice operatorul la care au fost furnizate datele cu caracter personal. Persoana vizată ne poate contacta pentru a-și exercita dreptul la transferabilitatea datelor.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## J. Existența dreptului de retragere a consimțământului în orice moment, fără a afecta legalitatea prelucrării bazate pe consimțământ înainte de retragerea sa, în cazul în care prelucrarea se bazează pe articolul 6 alineatul (1) lit. a sau articolul 9 alineatul (2) lit. a GDPR (articolul 14 alineatul (2) lit. d GDPR)

Dacă prelucrarea datelor cu caracter personal se bazează pe Art. 6 (1) lit. a GDPR, în cazul în care persoana vizată și-a dat acordul pentru prelucrarea datelor cu caracter personal în unul sau mai multe scopuri specifice sau se bazează pe articolul 9 alineatul (2) lit. a GDPR care reglementează consimțământul explicit pentru prelucrarea categoriilor speciale de date cu caracter personal, persoana vizată are dreptul de a-și retrage consimțământul în orice moment în conformitate cu articolul 7 alineatul (3) punctul 1 GDPR.

Retragerea consimțământului nu afectează legalitatea prelucrării pe baza consimțământului înainte de retragerea sa, articolul 7 alineatul (3) din propoziția 2 GDPR. Este la fel de ușor să se retragă și să dea consimțământul, Art. 7 (3) Propoziția 4 GDPR. Prin urmare, retragerea consimțământului poate avea loc întotdeauna în același mod în care a fost acordat consimțământul sau în orice alt mod, care este considerat de către persoana vizată ca fiind mai simplu. În societatea informațională de astăzi, probabil cea mai simplă modalitate de retragere a consimțământului este un simplu e-mail. Dacă persoana vizată dorește să-și retragă consimțământul acordat nouă, este suficient să ne trimiteți un e-mail. În mod alternativ, persoana vizată poate alege orice alt mod de a comunica retragerea consimțământului.

## K. Dreptul de a depune o plângere la o autoritate de supraveghere (articolul 14 alineatul (2) lit. e, articolul 77 alineatul (1) din GDPR)

În calitate de operator, suntem obligați să notificăm persoanei vizate dreptul de a depune o plângere la o autoritate de supraveghere, articolul 14 alineatul (2) lit. e GDPR. Dreptul de a depune o plângere la o autoritate de supraveghere este reglementat de articolul 77 alineatul (1) din GDPR. Conform acestei dispoziții, fără a aduce atingere oricărei alte căi de atac administrative sau judiciare, fiecare persoană vizată are dreptul de a depune o plângere la o autoritate de supraveghere, în special în statul membru în care își are reședința obișnuită, locul de muncă sau locul de muncă unde presupusa încălcare în cazul în care persoana vizată consideră că prelucrarea datelor cu caracter personal pe care o privesc încalcă regulamentul general privind protecția datelor. Dreptul de a depune o plângere la o autoritate de supraveghere a fost limitat doar de legea Uniunii astfel încât să poată fi exercitat numai în fața unei autorități unice de supraveghere (Considerentul 141 din propunerea 1 GDPR). Această regulă vizează evitarea plângerilor duble ale aceluiași subiect de date în aceeași chestiune. Dacă un subiect de date dorește să depună o plângere, am solicitat contactarea numai unei singure autorități de supraveghere.


© All rights reserved by Heiko Maniero.

## L. Sursa datelor cu caracter personal provine din surse accesibile publicului (articolul 14 alineatul (2) lit. f GDPR)

În principiu, datele cu caracter personal sunt colectate direct de la persoana vizată sau în cooperare cu o autoritate (de exemplu, recuperarea datelor dintr-un registru oficial). Alte date privind persoanele vizate provin din transferurile companiilor din grup. În contextul acestor informații generale, denumirea surselor exacte din care provin datele personale este fie imposibilă, fie ar implica un efort disproporționat în sensul art. 14 (5) lit. b GDPR. În principiu, nu colectăm date cu caracter personal din surse accesibile publicului.

Orice persoană vizată ne poate contacta în orice moment pentru a obține informații mai detaliate despre sursele exacte de date cu caracter personal pe care o privesc. În cazul în care originea datelor cu caracter personal nu poate fi furnizată persoanei vizate deoarece s-au folosit diverse surse, ar trebui să se furnizeze informații generale (Considerentul 61 din propunerea 4 din GDPR).

## M. Existența unui proces automat de luare a deciziilor, inclusiv a profilării, menționat la articolul 22 alineatele (1) și (4) din GDPR și, cel puțin în acele cazuri, informații semnificative cu privire la logica implicată, precum și semnificația și consecințele preconizate ale unei astfel de procesări pentru persoana vizată (articolul 14 alineatul (2) lit. g GDPR)

În calitate de companie responsabilă, de obicei nu folosim procesul decizional automatizat sau crearea de profiluri. Dacă, în cazuri excepționale, efectuăm luarea automată a deciziilor sau crearea de profiluri, vom informa persoana vizată fie separat, fie printr-o subsecțiune din politica noastră de confidențialitate (pe site-ul nostru web). În acest caz, se aplică următoarele:

Luarea automată a deciziilor - inclusiv crearea de profiluri - poate avea loc dacă (1) acest lucru este necesar pentru încheierea sau executarea unui contract între persoana vizată și noi sau (2) acest lucru este autorizat de legislația Uniunii sau a unui stat membru căreia îi suntem supuși și care stabilește, de asemenea, măsuri adecvate pentru a proteja drepturile și libertățile și interesele legitime ale persoanei vizate; sau (3) acest lucru se bazează pe consimțământul explicit al persoanei vizate.

În cazurile menționate la articolul 22 alineatul (2) literele (a) și (c) din GDPR, vom pune în aplicare măsuri adecvate pentru a proteja drepturile și libertățile și interesele legitime ale persoanei vizate. În aceste cazuri, aveți dreptul de a obține o intervenție umană din partea operatorului, de a vă exprima punctul de vedere și de a contesta decizia.

Informații semnificative despre logica implicată, precum și despre semnificația și consecințele preconizate ale unei astfel de prelucrări pentru persoana vizată sunt prezentate în politica noastră de confidențialitate.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## III. EU-U.S. Data Privacy Framework (EU-U.S. DPF), UK Extension to the EU-U.S. DPF, Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF)

Dacă organizația noastră este un membru certificat al EU-U.S. Data Privacy Framework (EU-U.S. DPF) și/sau al UK Extension to the EU-U.S. DPF și/sau al Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF), se aplică următoarele:

Ne conformăm EU-U.S. Data Privacy Framework (EU-U.S. DPF) și UK Extension to the EU-U.S. DPF, precum și Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF), așa cum este stabilit de U.S. Department of Commerce. Compania noastră a confirmat către Departamentul de Comerț al SUA că respectă EU-U.S. Data Privacy Framework Principles (EU-U.S. DPF Principles) în ceea ce privește procesarea datelor personale pe care le primește din Uniunea Europeană și Regatul Unit, invocând EU-U.S. DPF și UK Extension to the EU-U.S. DPF. Compania noastră a confirmat către Departamentul de Comerț al SUA că respectă Swiss-U.S. Data Privacy Framework Principles (Swiss-U.S. DPF Principles) în ceea ce privește procesarea datelor personale pe care le primește din Elveția, invocând Swiss-U.S. DPF. În cazul unei contradicții între prevederile politicii noastre de confidențialitate și EU-U.S. DPF Principles și/sau Swiss-U.S. DPF Principles, prevalează Principiile.

Pentru a afla mai multe despre programul Data Privacy Framework (DPF) și pentru a vedea certificarea noastră, vă rugăm să vizitați https://www.dataprivacyframework.gov/.

Celelalte unități sau filiale americane ale companiei noastre, care respectă de asemenea EU-U.S. DPF Principles, inclusiv UK Extension to the EU-U.S. DPF și Swiss-U.S. DPF Principles, dacă există, sunt menționate în politica noastră de confidențialitate.

În conformitate cu EU-U.S. DPF și UK Extension to the EU-U.S. DPF, precum și Swiss-U.S. DPF, compania noastră se angajează să colaboreze cu autoritățile europene de protecție a datelor și cu Information Commissioner's Office (ICO) din Marea Britanie, precum și cu Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) din Elveția, și să urmeze sfaturile acestora cu privire la reclamațiile nerezolvate legate de gestionarea datelor personale pe care le primim invocând EU-U.S. DPF și UK Extension to the EU-U.S. DPF și Swiss-U.S. DPF.

Informăm persoanele vizate despre autoritățile europene de protecție a datelor competente, responsabile pentru gestionarea reclamațiilor legate de modul în care organizația noastră gestionează datele personale, în partea superioară a acestui document de transparență și despre faptul că oferim persoanelor vizate o cale de atac adecvată și gratuită.

Informăm toate persoanele vizate că compania noastră este supusă competențelor de investigație și de aplicare ale Federal Trade Commission (FTC).

Persoanele vizate au, în anumite condiții, posibilitatea de a recurge la arbitraj obligatoriu. Organizația noastră este obligată să soluționeze cererile și să respecte condițiile prevăzute în Anexa I a DPF


© All rights reserved by Heiko Maniero.

Principles, în cazul în care persoana vizată a solicitat arbitraj obligatoriu, notificând organizația noastră și respectând procedurile și condițiile prevăzute în Anexa I a Principiilor.

Informăm aici toate persoanele vizate despre responsabilitatea organizației noastre în cazul transferului datelor personale către terți.

Pentru întrebările persoanelor vizate sau ale autorităților de supraveghere a protecției datelor, am desemnat reprezentanții locali menționați mai sus în acest document de transparență.

Vă oferim posibilitatea de a alege (Opt-out) dacă datele dumneavoastră personale (i) sunt transferate către terți sau (ii) sunt utilizate în scopuri care diferă substanțial de scopurile pentru care au fost colectate inițial sau ulterior autorizate de dumneavoastră. Mecanismul clar, vizibil și ușor accesibil pentru exercitarea dreptului dumneavoastră de alegere constă în contactarea prin e-mail a responsabilului nostru cu protecția datelor (DSB). Nu aveți posibilitatea de a alege și nu suntem obligați să o facem, dacă datele sunt transferate către un terț care acționează ca agent sau procesator în numele nostru și conform instrucțiunilor noastre. Totuși, încheiem întotdeauna un contract cu un astfel de agent sau procesator.

Pentru datele sensibile (adică datele personale care conțin informații despre starea de sănătate, originea rasială sau etnică, opiniile politice, convingerile religioase sau filozofice, apartenența la sindicate sau informații despre viața sexuală a persoanei vizate), obținem consimțământul dumneavoastră explicit (Opt-in) dacă aceste date (i) sunt transferate către terți sau (ii) sunt utilizate în alte scopuri decât cele pentru care au fost colectate inițial sau pentru care ați acordat ulterior consimțământul dumneavoastră prin alegerea Opt-in. În plus, tratăm toate datele personale pe care le primim de la terți ca fiind sensibile, dacă terțul le-a identificat și tratat ca fiind sensibile.

Vă informăm aici despre necesitatea dezvăluirii datelor personale ca răspuns la solicitările legitime ale autorităților, inclusiv pentru îndeplinirea cerințelor de securitate națională sau de aplicare a legii.

La transferul datelor personale către un terț care acționează ca operator, respectăm Principiile notificării și alegerii. În plus, încheiem un contract cu operatorul, care prevede că aceste date pot fi prelucrate numai în scopuri limitate și specificate, în conformitate cu consimțământul dumneavoastră, și că destinatarul oferă același nivel de protecție ca Principiile DPF și ne notifică în cazul în care constată că nu mai poate îndeplini această obligație. Contractul prevede că operatorul va înceta prelucrarea sau va lua alte măsuri adecvate și corespunzătoare pentru a remedia situația, în cazul în care se constată că nu poate îndeplini această obligație.

La transferul datelor personale către un terț care acționează ca agent sau procesator, (i) transferăm aceste date numai în scopuri limitate și specificate; (ii) ne asigurăm că agentul sau procesatorul este obligat să asigure cel puțin același nivel de protecție a datelor ca cel cerut de DPF Principles; (iii) luăm măsuri adecvate și corespunzătoare pentru a ne asigura că agentul sau procesatorul prelucrează efectiv datele personale transferate într-un mod care să fie conform cu obligațiile noastre în temeiul DPF Principles; (iv) cerem agentului sau procesatorului să notifice organizația noastră dacă constată că nu mai poate îndeplini obligația de a oferi același nivel de protecție ca cel cerut de DPF Principles; (v) după


© All rights reserved by Heiko Maniero.

notificare, inclusiv conform punctului (iv), luăm măsuri adecvate și corespunzătoare pentru a opri prelucrarea neautorizată și a remedia situația; și (vi) punem la dispoziția DPF Department, la cerere, un rezumat sau un exemplar reprezentativ al prevederilor relevante privind protecția datelor din contractul nostru cu acest agent.

În conformitate cu EU-U.S. DPF și/sau UK Extension to the EU-U.S. DPF și/sau Swiss-U.S. DPF, compania noastră se angajează să colaboreze cu autoritățile europene de protecție a datelor și cu Information Commissioner's Office (ICO) din Marea Britanie, precum și cu Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) din Elveția, și să urmeze sfaturile acestora cu privire la reclamațiile nerezolvate legate de gestionarea datelor personale pe care le primim invocând EU-U.S. DPF și UK Extension to the EU-U.S. DPF și Swiss-U.S. DPF în contextul relațiilor de muncă.

Toate persoanele vizate care se află temporar în Uniunea Europeană (UE), în Spațiul Economic European (SEE) sau în Regatul Unit, sau care își au domiciliul sau reședința obișnuită în aceste țări, beneficiază de drepturile și drepturile persoanelor vizate care sunt publicate în Documentul nostru de transparență, care decurg, de asemenea, din articolele 15-22 din RGPD, inclusiv dreptul de acces la datele cu caracter personal. Am pus la dispoziție aceste informații în toate limbile UE și SEE. Versiunea în limba engleză se aplică în Regatul Unit.

Toate persoanele vizate care au reședința temporară în Elveția sau care își au domiciliul sau reședința obișnuită în această țară beneficiază de drepturile și drepturile persoanelor vizate în temeiul Legii elvețiene privind protecția datelor (DPA) și al Regulamentului elvețian privind protecția datelor (DPR), care sunt publicate în documentul nostru de transparență, inclusiv dreptul de acces la datele cu caracter personal. Am furnizat aceste informații în cele trei limbi oficiale ale Elveției (germană, italiană și franceză).


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

# CROATIAN: Informacije o obradi osobnih podataka (članak 13, 14 GDPR)

Poštovani,

Osobni podaci svakog pojedinca koji je u ugovornom, pred-ugovornom ili drugom odnosu s našom tvrtkom zaslužuje posebnu zaštitu. Naš je cilj zadržati razinu zaštite podataka na visokom nivou. Stoga rutinski razvijamo koncepte zaštite podataka i sigurnosti podataka.

Naravno, poštujemo zakonske odredbe o zaštiti podataka. Prema člancima 13, 14. GDPR, kontrolori ispunjavaju posebne zahtjeve obavješćivanja pri prikupljanju osobnih podataka. Ovaj dokument ispunjava te obveze.

Terminologija pravnih propisa je složena. Nažalost, korištenje pravnih izraza nije se moglo izostaviti u pripremi ovog dokumenta. Stoga želimo naglasiti da nas uvijek možete kontaktirati za sva pitanja koja se tiču ovog dokumenta, korištenih termina ili formulacija.

## I. Usklađenost sa zahtjevima obavješćivanja kada se osobni podaci prikupljaju od nositelja podataka (članak 13. GDPR)

### A. Identitet i kontaktni podaci kontrolora (članak 13. stavak 1. točka (a) GDPR)

Vidi gore

### B. Kontaktni podaci službenika za zaštitu podataka (članak 13. stavak 1. točka (b) GDPR)

Vidi gore

### C. Svrha obrade za koju su osobni podaci namijenjeni, kao i pravna osnova za obradu (članak 13. stavak 1. točka (c) GDPR)

Svrha obrade osobnih podataka je rukovanje svim operacijama koje se tiču kontrolora, klijenata, potencijalnih klijenata, poslovnih partnera ili drugih ugovornih ili predugovornih odnosa između navedenih skupina (u najširem smislu) ili zakonskih obveza kontrolora.

Članak 6 (1) točka (a) GDPR služi kao pravna osnova za operacije obrade za koje dobivamo pristanak za određenu svrhu obrade. Ako je obrada osobnih podataka nužna za izvršenje ugovora u kojem je


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

subjekt podataka stranka, kao što je, na primjer, kada su operacije obrade potrebne za isporuku robe ili pružanje bilo koje druge usluge, obrada je na temelju članka 6. stavka 1 točka (b) GDPR. Isto se odnosi i na postupke obrade koji su potrebni za provedbu predugovornih mjera, primjerice u slučaju upita o našim proizvodima ili uslugama. Kada je naša tvrtka podložna zakonskoj obavezi kojom se traži obrada osobnih podataka, kao što je ispunjenje poreznih obveza, obrada se temelji na čl. 6 (1) točka (c) GDPR.

U rijetkim slučajevima, obrada osobnih podataka može biti potrebna za zaštitu vitalnih interesa nositelja podataka ili druge fizičke osobe. To bi bio slučaj, na primjer, ako bi se posjetitelj ozlijedio u našoj tvrtki i njegovo ime, dob, podaci o zdravstvenom osiguranju ili druge vitalne informacije trebali bi se prenijeti liječniku, bolnici ili drugoj trećoj osobi. Tada bi se obrada temeljila na čl. 6 (1) točka (d) GDPR.

Ako je obrada nužna za obavljanje zadaće koja se provodi u javnom interesu ili u izvršavanju službenih ovlasti dodijeljenih voditelju obrade, pravna osnova je čl. 6 (1) točka (e) GDPR.

Konačno, postupci obrade mogu se temeljiti na članku 6. stavku 1. točka (f) GDPR. Ova se pravna osnova koristi za postupke obrade koji nisu obuhvaćeni ni jednom od gore navedenih pravnih osnova, ako je obrada potrebna u svrhu legitimnih interesa koje naša tvrtka ili treća strana nastoje ostvariti, osim ako su interesi nadjačani interesima ili pravima i slobodama nositelja podataka koji zahtijevaju zaštitu osobnih podataka. Takvi postupci obrade posebno su dopušteni jer ih je europski zakonodavac posebno spomenuo. Smatrao je da se legitimni interes može pretpostaviti ako je subjekt podataka klijent kontrolora (uvodna izjava 47, rečenica 2 GDPR).

## D. Kada se obrada temelji na članku 6 (1) točka (f) GDPR, legitimni interesi koje provodi kontrolor ili treća strana (članak 13. stavak 1. točka (d) GDPR)

Kada se obrada osobnih podataka temelji na članku 6. stavku 1. točka (f) GDPR, naš legitimni interes je obavljanje našeg poslovanja u korist dobrobiti svih naših zaposlenika i dioničara.

## E. Kategorije primatelja osobnih podataka (članak 13. stavak 1. točka (e) GDPR)

Javne vlasti

Vanjska tijela

Daljnja vanjska tijela

Interna obrada

Obrada unutar grupe

Ostala tijela


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

Popis naših izvršitelja obrade i primatelja podataka u trećim zemljama i, ako je primjenjivo, međunarodnim organizacijama objavljen je na našoj web stranici ili se može zatražiti od nas besplatno. Obratite se našem službeniku za zaštitu podataka kako biste zatražili ovaj popis.

## F. Primatelji u trećoj zemlji i odgovarajuće ili prikladne mjere zaštite i sredstva za njihovo pribavljanje ili njihovo stavljanje na raspolaganje (članak 13 (1) točka (f); 46(1), 46 (2) točka (c) GDPR)

Sve tvrtke i podružnice koje su dio naše grupe (u daljnjem tekstu: tvrtke grupe) koje imaju sjedište ili ured u trećoj zemlji mogu pripadati primateljima osobnih podataka. Od nas se može zatražiti popis svih tvrtki ili primatelja grupe.

U skladu s člankom 46. stavkom 1. GDPR, kontrolor ili obrađivač može prenijeti osobne podatke samo trećoj zemlji ako je kontrolor ili obrađivač osigurao odgovarajuće zaštitne mjere i pod uvjetom da su na raspolaganju provediva prava subjekta podataka i učinkoviti pravni lijekovi za subjekte podataka. Odgovarajuće zaštitne mjere mogu se pružiti bez potrebe za posebnim odobrenjem nadzornog tijela putem standardnih ugovornih klauzula, članak 46 (2) točka (c) GDPR.

Standardne ugovorne klauzule Europske unije ili druge odgovarajuće mjere zaštite dogovorene su sa svim primateljima iz trećih zemalja prije prvog prijenosa osobnih podataka. Slijedom toga, osigurano je da su zajamčeni odgovarajući zaštitni mehanizmi, primjenjiva prava subjekata podataka i djelotvorni pravni lijekovi za subjekte podataka. Svaki subjekt podataka može od nas dobiti kopiju standardnih ugovornih klauzula. Standardne ugovorne klauzule također su dostupne u Službenom listu Europske unije.

Članak 45. stavak 3. Opće uredbe o zaštiti podataka (GDPR) daje Europskoj komisiji ovlast da putem provedbenog akta odluči da zemlja koja nije članica EU-a osigurava odgovarajuću razinu zaštite. To znači razinu zaštite osobnih podataka koja je u biti jednaka razini zaštite unutar EU-a. Učinak odluka o primjerenosti je da osobni podaci mogu slobodno teći iz EU (i Norveške, Lihtenštajna i Islanda) u treću zemlju bez daljnjih prepreka. Slična pravila postoje za Ujedinjeno Kraljevstvo, Švicarsku i neke druge zemlje.

Kada je Europska komisija ili vlada druge zemlje odlučila da treća zemlja osigurava odgovarajuću razinu zaštite, a postoji važeći okvir (npr. EU-U.S. Data Privacy Framework, Swiss-U.S. Data Privacy Framework, UK Extension to the EU-U.S. Data Privacy Framework), svi naši prijenosi članovima takvih okvira (npr. samocertificirani subjekti) temelje se isključivo na članstvu tih subjekata u dotičnom okviru. Tamo gdje smo mi ili jedan od entiteta naše grupe član takvog okvira, svi prijenosi nama ili entitetu naše grupe temelje se isključivo na članstvu entiteta u takvom okviru.

Svaki subjekt podataka može od nas dobiti kopiju okvira. Osim toga, okviri su također dostupni u Službenom listu Europske unije ili u objavljenim pravnim materijalima ili na web stranicama nadzornih tijela ili drugih nadležnih tijela ili institucija.


© All rights reserved by Heiko Maniero.

## G. Razdoblje za koje će osobni podaci biti pohranjeni, ili ako to nije moguće odrediti, kriteriji koji se koriste za određivanje tog razdoblja (članak 13. stavak 2. točka (a) GDPR)

Kriterij koji se koristi za određivanje razdoblja čuvanja osobnih podataka je odgovarajuće zakonsko razdoblje čuvanja podataka. Nakon isteka tog razdoblja, odgovarajući podaci se rutinski brišu, sve dok više nisu potrebni za ispunjenje ugovora ili pokretanje ugovora.

Ako ne postoji zakonski rok čuvanja, kriterij je ugovorni ili interni rok čuvanja.

## H. Postojanje prava da se od kontrolora zatraži pristup i ispravak ili brisanje osobnih podataka ili ograničenje obrade u odnosu na nositelja podataka ili da se uloži prigovor na obradu, kao i pravo na prenosivost podataka (članak 13. stavak 2. točka (b) GDPR)

Svi subjekti podataka imaju sljedeća prava:

***Pravo na pristup***

Svaki nosilac podataka ima pravo pristupa osobnim podacima koji se odnose na njega. Pravo na pristup proteže se na sve podatke koje obrađujemo. Pravo se može ostvariti jednostavno i u razumnim vremenskim intervalima kako bi se zadovoljili i provjerili zakonitost obrade (uvodna izjava 63 GDPR-a). Ovo pravo proizlazi iz čl. 15 GDPR. Subjekt podataka može nas kontaktirati kako bi ostvario pravo pristupa.

***Pravo na ispravak***

U skladu s člankom 16. rečenica 1 GDPR, osoba čiji se podaci obrađuju ima pravo od kontrolora bez nepotrebnog odgađanja dobiti ispravak netočnih osobnih podataka koji se odnose na njega. Nadalje, člankom 16. rečenica 2 GDPR predviđeno je da subjekt podataka ima pravo, uzimajući u obzir svrhu obrade, imati dovršene nepotpune osobne podatke, uključujući i pružanje dodatne izjave. Subjekt podataka može nas kontaktirati kako bi ostvario pravo na ispravak.

***Pravo na brisanje (pravo na zaborav)***

Osim toga, osobe čiji se podaci obrađuju imaju pravo na brisanje i pravo da podaci budu zaboravljeni na temelju čl. 17 GDPR. To se pravo može ostvariti ako nas kontaktirate. U ovom trenutku, međutim, želimo naglasiti da se to pravo ne primjenjuje u onoj mjeri u kojoj je obrada potrebna kako bi se ispunila zakonska obveza na koju je naša tvrtka podložna, članak 17 (3) točka (b) GDPR. To znači da možemo odobriti zahtjev za brisanje samo nakon isteka zakonskog roka zadržavanja.

***Pravo na ograničenje obrade***

Prema članku 18. GDPR, svaki subjekt podataka ima pravo na ograničenje obrade. Ograničenje obrade može se zahtijevati ako je jedan od uvjeta iz članka 18. stavka 1 točke a-d GDPR je ispunjen. Subjekt podataka može nas kontaktirati kako bi ostvario pravo na ograničenje obrade.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

***Pravo na prigovor***

Nadalje, čl. 21 GDPR jamči pravo na prigovor. Subjekt podataka može nas kontaktirati kako bi ostvario pravo na prigovor.

***Pravo na prenosivost podataka***

Članak 20 GDPR daje subjektu podataka pravo na prenosivost podataka. Prema ovoj odredbi, subjekt podataka pod uvjetima iz članka 20. stavka 1. točke a i b GDPR ima pravo na primanje osobnih podataka koji se odnose na njega ili nju, koje je on ili ona pružio kontroloru, u strukturiranom, uobičajeno korištenom i strojno čitljivom formatu i imaju pravo na nesmetani prijenos tih podataka drugom kontroloru od kontrolora kojem su dostavljeni osobni podaci. Subjekt podataka može nas kontaktirati radi ostvarivanja prava na prenosivost podataka.

## I. Postojanje prava na povlačenje pristanka u bilo kojem trenutku, bez utjecaja na zakonitost obrade na temelju suglasnosti prije njegovog povlačenja, ako se obrada temelji na članku 6. stavku 1. točka (a) GDPR ili članak 9 (2) točka (a) GDPR (članak 13. stavak 2. točka c GDPR)

Ako se obrada osobnih podataka temelji na čl. 6 (1) točka (a) GDPR, što je slučaj, ako je subjekt podataka dao pristanak na obradu osobnih podataka za jednu ili više posebnih svrha ili se temelji na članku 9 (2) točka (a) GDPR, koji regulira izričitu suglasnost za obradu posebnih kategorija osobnih podataka, subjekt podataka ima u skladu s člankom 7. stavkom 3. rečenice 1 GDPR-a pravo povući svoj pristanak u bilo kojem trenutku.

Povlačenje suglasnosti ne utječe na zakonitost obrade na temelju suglasnosti prije njezina povlačenja, članak 7. stavak 3. rečenica 2 GDPR. Povlačenje je jednako lako kao i davanje pristanka, čl. 7 (3) rečenica 4 GDPR. Stoga se povlačenje suglasnosti uvijek može dogoditi na isti način kao što je pristanak dan ili na bilo koji drugi način, što subjekt podataka smatra jednostavnijim. U današnjem informacijskom društvu, vjerojatno je najjednostavniji način povlačenja pristanka jednostavna e-pošta. Ako subjekt podataka želi povući svoj odobreni pristanak, dovoljan nam je jednostavan e-mail. Alternativno, subjekt podataka može odabrati bilo koji drugi način da nam priopći svoje povlačenje pristanka.

## J. Pravo na podnošenje pritužbe nadzornom tijelu (članak 13. stavak 2. točka (d), članak 77. stavak 1. GDPR)

Kao kontrolor, dužni smo obavijestiti nositelja podataka o pravu na podnošenje pritužbe nadzornom tijelu, članak 13 (2) točka (d) GDPR. Pravo na podnošenje pritužbe nadzornom tijelu regulirano je člankom 77. stavkom 1. GDPR. U skladu s ovom odredbom, pre ulaganja bilo kojeg drugog administrativnog ili pravnog lijeka, svaki subjekt podataka ima pravo podnijeti pritužbu nadzornom tijelu, posebno u državi članici u kojoj ima prebivalište, radno mjesto ili mjesto navodne povrede ako subjekt podataka smatra da obrada osobnih podataka koji se odnose na njega ili nju krši Opću uredbu o zaštiti podataka. Pravo na


© All rights reserved by Heiko Maniero.

podnošenje pritužbe nadzornom tijelu bilo je ograničeno samo pravom Unije na takav način, da se može ostvariti samo pred jednim nadzornim tijelom (uvodna izjava 141, rečenica 1 GDPR). Cilj ovog pravila je izbjegavanje dvostrukih pritužbi istog subjekta podataka u istom predmetu. Ako subjekt podataka želi podnijeti pritužbu na nas, tražimo da kontaktira samo jedno nadzorno tijelo.

## K. Pružanje osobnih podataka kao zakonski ili ugovorni zahtjev; Zahtjev potreban za sklapanje ugovora; Obveza nositelja podataka da dostavi osobne podatke; moguće posljedice nepružanja takvih podataka (čl. 13. stavak 2. točka (e) GDPR)

Pojašnjavamo da je davanje osobnih podataka djelomično zahtijevano zakonom (npr. Porezni propisi) ili također može proizaći iz ugovornih odredbi (npr. Informacija o ugovornom partneru).

Ponekad može biti potrebno sklopiti ugovor kojim nam subjekt podataka daje osobne podatke, koje moramo naknadno obraditi. Subjekt podataka je, primjerice, dužan da nam dostavi osobne podatke kada naša tvrtka s njim ili njom potpiše ugovor. Nepružanje osobnih podataka imalo bi za posljedicu da se ugovor s subjektom podataka ne može zaključiti.

Prije davanja osobnih podataka od strane nositelja podataka, osoba na koju se podaci odnose mora nas kontaktirati. Obavjestićemo osobu na koju se podaci odnose je li pružanje osobnih podataka obvezno po zakonu ili ugovoru ili je potrebno za sklapanje ugovora, postoji li obveza pružanja osobnih podataka i posljedica nepružanja osobnih podataka.

## L. Postojanje automatiziranog odlučivanja, uključujući profiliranje, iz članka 22. (1) i (4) GDPR i barem u tim slučajevima, značajne informacije o logici koja je uključena, kao i značaj i predviđene posljedice takve obrade za osobe čiji se podaci obrađuju (članak 13. stavak 2. točka (f) GDPR)

Kao odgovorna tvrtka, obično ne koristimo automatizirano donošenje odluka ili profiliranje. Ako, u iznimnim slučajevima, provodimo automatizirano donošenje odluka ili profiliranje, o tome ćemo obavijestiti nositelja podataka zasebno ili putem pododjeljka u našim pravilima o privatnosti (na našoj web stranici). U ovom slučaju vrijedi sljedeće:

Automatizirano donošenje odluka - uključujući profiliranje - može se dogoditi ako (1) je to potrebno za sklapanje ili izvršenje ugovora između ispitanika i nas, ili (2) je to dopušteno zakonom Unije ili države članice prema kojem se pridržavamo su predmet i koji također utvrđuje odgovarajuće mjere za zaštitu prava i sloboda i legitimnih interesa ispitanika; ili (3) to se temelji na izričitom pristanku nositelja podataka.

U slučajevima iz članka 22. stavka 2. (a) i (c) GDPR-a, provest ćemo odgovarajuće mjere za zaštitu prava i sloboda i legitimnih interesa ispitanika. U tim slučajevima imate pravo zatražiti ljudsku intervenciju od strane kontrolora, izraziti svoje stajalište i osporiti odluku.


© All rights reserved by Heiko Maniero.

Značajne informacije o uključenoj logici, kao i značaju i predviđenim posljedicama takve obrade za subjekta podataka navedene su u našim pravilima o privatnosti.

## II. Usklađenost sa zahtjevima obavješćivanja kada se osobni podaci ne prikupljaju od nositelja podataka (članak 14.GDPR)

### A. Identitet i kontaktni podaci kontrolora (članak 14. stavak 1. točka (a) GDPR)

Vidi gore

### B. Kontaktni podaci službenika za zaštitu podataka (članak 14. stavak 1. točka (b) GDPR)

Vidi gore

### C. Svrha obrade za koju su osobni podaci namijenjeni, kao i pravna osnova za obradu (članak 14 (1) točka (c) GDPR)

Svrha obrade osobnih podataka je rukovanje svim operacijama koje se tiču kontrolora, kupaca, potencijalnih kupaca, poslovnih partnera ili drugih ugovornih ili predugovornih odnosa između navedenih skupina (u najširem smislu) ili zakonskih obaveza kontrolora.

Ako je obrada osobnih podataka nužna za izvršenje ugovora u kojem je subjekt podataka stranka, kao što je, na primjer, kada su operacije obrade potrebne za isporuku robe ili pružanje bilo koje druge usluge, obrada je na temelju članka 6. stavka 1. točka (b) GDPR. Isto se odnosi i na postupke obrade koji su potrebni za provedbu predugovornih mjera, primjerice u slučaju upita o našim proizvodima ili uslugama. Da li je naša tvrtka podložna zakonskoj obavezi kojom se traži obrada osobnih podataka, kao što je ispunjenje poreznih obveza, obrada se temelji na čl. 6 (1) točka (c) GDPR.

U rijetkim slučajevima, obrada osobnih podataka može biti potrebna za zaštitu vitalnih interesa nositelja podataka ili druge fizičke osobe. To bi bio slučaj, na primjer, ako bi se posjetitelj ozlijedio u našoj tvrtki i njegovo ime, dob, podaci o zdravstvenom osiguranju ili druge vitalne informacije trebali bi se prenijeti liječniku, bolnici ili drugoj trećoj osobi. Tada bi se obrada temeljila na čl. 6 (1) točka (d) GDPR.

Ako je obrada nužna za obavljanje zadaće koja se provodi u javnom interesu ili u izvršavanju službenih ovlasti dodijeljenih voditelju obrade, pravna osnova je čl. 6 (1) točka (e) GDPR.

Konačno, postupci obrade mogu se temeljiti na članku 6. stavku 1. točka (f) GDPR. Ova se pravna osnova koristi za postupke obrade koji nisu obuhvaćeni ni jednom od gore navedenih pravnih osnova, ako je


© All rights reserved by Heiko Maniero.

obrada potrebna u svrhu legitimnih interesa koje naša tvrtka ili treća strana nastoje ostvariti, osim ako su interesi nadjačani interesima ili temeljna prava i slobode nositelja podataka koji zahtijevaju zaštitu osobnih podataka. Takvi postupci obrade posebno su dopušteni jer ih je europski zakonodavac posebno spomenuo. Smatrao je da se legitimni interes može pretpostaviti ako je subjekt podataka klijent kontrolora (uvodna izjava 47, rečenica 2 GDPR).

## D. Kategorije dotičnih osobnih podataka (članak 14. stavak 1. točka (d) GDPR)

Korisnički podaci

Podaci potencijalnih kupaca

Podaci zaposlenika

Podaci dobavljača

## E. Kategorije primatelja osobnih podataka (članak 14. stavak 1. točka (e) GDPR)

Javne vlasti

Vanjska tijela

Daljnja vanjska tijela

Interna obrada

Obrada unutar grupe

Ostala tijela

Popis naših izvršitelja obrade i primatelja podataka u trećim zemljama i, ako je primjenjivo, međunarodnim organizacijama objavljen je na našoj web stranici ili se može zatražiti od nas besplatno. Obratite se našem službeniku za zaštitu podataka kako biste zatražili ovaj popis.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## F. Primatelji u trećoj zemlji i odgovarajuće ili prikladne mjere zaštite i sredstva za njihovo pribavljanje ili njihovo stavljanje na raspolaganje (članak 14. stavak 1. točka (f), 46 (1), 46 (2) točka (c) GDPR)

Sve tvrtke i podružnice koje su dio naše grupe (u daljnjem tekstu: tvrtke grupe) koje imaju sjedište ili ured u trećoj zemlji mogu pripadati primateljima osobnih podataka. Od nas se može zatražiti popis svih tvrtki iz grupe.

U skladu s člankom 46. stavkom 1. GDPR, kontrolor ili obrađivač može prenijeti osobne podatke samo trećoj zemlji ako je kontrolor ili obrađivač osigurao odgovarajuće zaštitne mjere i pod uvjetom da su na raspolaganju provediva prava subjekta podataka i učinkoviti pravni lijekovi za subjekte podataka. Odgovarajuće zaštitne mjere mogu se pružiti bez potrebe za posebnim odobrenjem nadzornog tijela pomoću standardnih klauzula o zaštiti podataka, članak 46 (2) točka (c) GDPR.

Standardne ugovorne klauzule Europske unije ili druge odgovarajuće mjere zaštite dogovorene su sa svim primateljima iz trećih zemalja prije prvog prijenosa osobnih podataka. Slijedom toga, osigurano je da su zajamčeni odgovarajući zaštitni mehanizmi, primjenjiva prava subjekata podataka i djelotvorni pravni lijekovi za subjekte podataka. Svaki subjekt podataka može od nas dobiti kopiju standardnih ugovornih klauzula. Standardne ugovorne klauzule također su dostupne u Službenom listu Europske unije.

Članak 45. stavak 3. Opće uredbe o zaštiti podataka (GDPR) daje Europskoj komisiji ovlast da putem provedbenog akta odluči da zemlja koja nije članica EU-a osigurava odgovarajuću razinu zaštite. To znači razinu zaštite osobnih podataka koja je u biti jednaka razini zaštite unutar EU-a. Učinak odluka o primjerenosti je da osobni podaci mogu slobodno teći iz EU (i Norveške, Lihtenštajna i Islanda) u treću zemlju bez daljnjih prepreka. Slična pravila postoje za Ujedinjeno Kraljevstvo, Švicarsku i neke druge zemlje.

Kada je Europska komisija ili vlada druge zemlje odlučila da treća zemlja osigurava odgovarajuću razinu zaštite, a postoji važeći okvir (npr. EU-U.S. Data Privacy Framework, Swiss-U.S. Data Privacy Framework, UK Extension to the EU-U.S. Data Privacy Framework), svi naši prijenosi članovima takvih okvira (npr. samocertificirani subjekti) temelje se isključivo na članstvu tih subjekata u dotičnom okviru. Tamo gdje smo mi ili jedan od entiteta naše grupe član takvog okvira, svi prijenosi nama ili entitetu naše grupe temelje se isključivo na članstvu entiteta u takvom okviru.

Svaki subjekt podataka može od nas dobiti kopiju okvira. Osim toga, okviri su također dostupni u Službenom listu Europske unije ili u objavljenim pravnim materijalima ili na web stranicama nadzornih tijela ili drugih nadležnih tijela ili institucija.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## G. Razdoblje za koje će osobni podaci biti pohranjeni ili, ako to nije moguće odrediti, kriteriji koji se koriste za određivanje tog razdoblja (članak 14. stavak 2. točka (a) GDPR)

Kriterij koji se koristi za određivanje razdoblja čuvanja osobnih podataka je odgovarajuće zakonsko razdoblje čuvanja podataka. Nakon isteka tog razdoblja, odgovarajući podaci se rutinski brišu, sve dok više nisu potrebni za ispunjenje ugovora ili pokretanje ugovora.

Ako ne postoji zakonski rok čuvanja, kriterij je ugovorni ili interni rok čuvanja.

## H. Obavijest o legitimnim interesima koje provodi kontrolor ili treća strana ako se obrada temelji na članku 6 (1) točka (f) GDPR (čl. 14 (2) točka (b) GDPR)

Prema članku 6 (1) točka (f) GDPR, obrada će biti zakonita samo ako je obrada potrebna u svrhe legitimnih interesa koje ostvaruje kontrolor ili treća strana, osim ako su ti interesi nadjačani interesima ili temeljnim pravima i slobodama nositelja podataka koji zahtijevaju zaštitu osobnih podataka. U skladu s uvodnom izjavom 47. stavka 2. GDPR legitiman interes može postojati tamo gdje postoji relevantan i odgovarajući odnos između ispitanika i kontrolora, npr. u situacijama u kojima je subjekt podataka klijent kontrolora. U svim slučajevima u kojima naša tvrtka obrađuje osobne podatke na temelju članka 6 (1) točka (f) GDPR, naš legitimni interes je u obavljanju našeg poslovanja u korist dobrobiti svih naših zaposlenika i dioničara.

## I. Postojanje prava da se od kontrolora zatraži pristup i ispravak ili brisanje osobnih podataka ili ograničenje obrade u vezi s nositeljem podataka te da se uloži prigovor na obradu, kao i pravo na prenosivost podataka (članak 14. stavak 2. točka (c) GDPR)

Svi subjekti podataka imaju sljedeća prava:

***Pravo na pristup***

Svaki subjekt podataka ima pravo pristupa osobnim podacima koji se odnose na njega. Pravo na pristup proteže se na sve podatke koje obrađujemo. Pravo se može ostvariti lako i u razumnim vremenskim razmacima, kako bi bio svjestan i provjerio zakonitost obrade (uvodna izjava 63 GDPR). Ovo pravo proizlazi iz čl. 15 GDPR. Subjekt podataka može nas kontaktirati kako bi ostvario pravo pristupa.

***Pravo na ispravak***

U skladu s člankom 16. rečenica 1 GDPR, osoba čiji se podaci obrađuju ima pravo od kontrolora bez nepotrebnog odgađanja dobiti ispravak netočnih osobnih podataka koji se odnose na njega. Nadalje, člankom 16. rečenica 2 GDPR predviđeno je da subjekt podataka ima pravo, uzimajući u obzir svrhu obrade, imati dovršene nepotpune osobne podatke, uključujući i pružanje dodatne izjave. Subjekt podataka može nas kontaktirati kako bi ostvario pravo na ispravak.


© All rights reserved by Heiko Maniero.

***Pravo na brisanje (pravo na zaborav)***

Osim toga, osobe čiji se podaci obrađuju imaju pravo na brisanje i pravo da podaci budu zaboravljeni na temelju čl. 17 GDPR. To se pravo može ostvariti ako nas kontaktirate. U ovom trenutku, međutim, želimo naglasiti da se to pravo ne primjenjuje u onoj mjeri u kojoj je obrada potrebna kako bi se ispunila zakonska obveza na koju je naša tvrtka podložna, članak 17 (3) točka (b) GDPR. To znači da možemo odobriti zahtjev za brisanje samo nakon isteka zakonskog roka zadržavanja.

***Pravo na ograničenje obrade***

Prema članku 18. GDPR, svaki subjekt podataka ima pravo na ograničenje obrade. Ograničenje obrade može se zahtijevati ako je jedan od uvjeta iz članka 18. stavka 1. točke a-d GDPR je ispunjen. Subjekt podataka može nas kontaktirati kako bi ostvario pravo na ograničenje obrade.

***Pravo na prigovor***

Nadalje, čl. 21 GDPR jamči pravo na prigovor. Subjekt podataka može nas kontaktirati kako bi ostvario pravo na prigovor.

***Pravo na prenosivost podataka***

Članak 20 GDPR daje subjektu podataka pravo na prenosivost podataka. Prema ovoj odredbi, subjekt podataka pod uvjetima iz članka 20. stavka 1. točke a i b GDPR ima pravo na primanje osobnih podataka koji se odnose na njega ili nju, koje je on ili ona pružio kontroloru, u strukturiranom, uobičajeno korištenom i strojno čitljivom formatu i imaju pravo na nesmetani prijenos tih podataka drugom kontroloru od kontrolora kojem su dostavljeni osobni podaci. Subjekt podataka može nas kontaktirati radi ostvarivanja prava na prenosivost podataka.

## J. Postojanje prava na povlačenje pristanka u bilo kojem trenutku, bez utjecaja na zakonitost obrade na temelju suglasnosti prije njegovog povlačenja, ako se obrada temelji na članku 6. stavku 1. točka (a) ili članak 9. (2) točka (a) GDPR (čl. 14 (2) točka (d) GDPR)

Ako se obrada osobnih podataka temelji na čl. 6 (1) točka (a) GDPR, što je slučaj, ako je subjekt podataka dao pristanak na obradu osobnih podataka za jednu ili više posebnih svrha ili se temelji na članku 9 (2) točka (a) GDPR, koji regulira izričitu suglasnost za obradu posebnih kategorija osobnih podataka, subjekt podataka ima u skladu s člankom 7. stavkom 3. rečenice 1 GDPR pravo povući svoj pristanak u bilo kojem trenutku.

Povlačenje suglasnosti ne utječe na zakonitost obrade na temelju suglasnosti prije njenog povlačenja, članak 7. stavak 3. rečenica 2 GDPR. Povlačenje je jednako lako kao i davanje pristanka, čl. 7 (3) rečenica 4 GDPR. Stoga se povlačenje suglasnosti uvijek može dogoditi na isti način kao što je pristanak dan ili na bilo koji drugi način, što subjekt podataka smatra jednostavnijim. U današnjem informacijskom društvu, vjerojatno je najjednostavniji način povlačenja pristanka jednostavna e-pošta. Ako subjekt


© All rights reserved by Heiko Maniero.

podataka želi povući svoj odobreni pristanak, dovoljan nam je jednostavan e-mail. Alternativno, subjekt podataka može odabrati bilo koji drugi način da nam priopći svoje povlačenje pristanka.

## K. Pravo na podnošenje pritužbe nadzornom tijelu (članak 14. stavak 2. točka (e), članak 77. stavak 1. GDPR)

Kao kontrolor, dužni smo obavijestiti nositelja podataka o pravu podnošenja pritužbe nadzornom tijelu, članak 14 (2) točka (e) GDPR. Pravo na podnošenje pritužbe nadzornom tijelu regulirano je člankom 77. stavkom 1. GDPR. U skladu s ovom odredbom, pre ulaganja bilo kojeg drugog administrativnog ili pravnog lijeka, svaki subjekt podataka ima pravo podnijeti pritužbu nadzornom tijelu, posebno u državi članici u kojoj ima prebivalište, radno mjesto ili mjesto navodne povrede ako subjekt podataka smatra da obrada osobnih podataka koji se odnose na njega ili nju krši Opću uredbu o zaštiti podataka. Pravo na podnošenje pritužbe nadzornom tijelu bilo je ograničeno samo pravom Unije na takav način, da se može ostvariti samo pred jednim nadzornim tijelom (uvodna izjava 141, rečenica 1 GDPR). Cilj ovog pravila je izbjegavanje dvostrukih pritužbi istog subjekta podataka u istom predmetu. Ako subjekt podataka želi podnijeti pritužbu na nas, tražimo da kontaktira samo jedno nadzorno tijelo.

## L. Izvor iz kog osobni podatci potječu, i ako je primjenjivo, jesu li došli iz javno dostupnih izvora (članak 14. stavak 2. točka (f) GDPR)

U načelu, osobni se podaci prikupljaju izravno od nositelja podataka ili u suradnji s nadležnim tijelom (npr. Dohvat podataka iz službenog registra). Ostali podaci o subjektima podataka proizlaze iz transfera društava grupe. U kontekstu ove opće informacije, imenovanje točnih izvora iz kojih su osobni podaci nastali ili je nemoguće ili bi uključivalo nerazmjerne napore u smislu čl. 14 (5) točka (b) GDPR. U načelu, ne prikupljamo osobne podatke iz javno dostupnih izvora.

Svaki subjekt podataka može nas kontaktirati u bilo koje vrijeme kako bi dobili detaljnije informacije o točnim izvorima osobnih podataka koji se odnose na njega. Ako se podrijetlo osobnih podataka ne može dati subjektu podataka jer su korišteni različiti izvori, potrebno je dostaviti opće informacije (uvodna izjava 61, rečenica 4 GDPR).

## M. Postojanje automatiziranog odlučivanja, uključujući profiliranje, iz članka 22. (1) i (4) GDPR, i barem u tim slučajevima, značajne informacije o logici koja je uključena, kao i značaj i predviđene posljedice takve obrade za osobe čiji se podaci obrađuju (članak 14. stavak 2. točka g)

Kao odgovorna tvrtka, obično ne koristimo automatizirano donošenje odluka ili profiliranje. Ako, u iznimnim slučajevima, provodimo automatizirano donošenje odluka ili profiliranje, o tome ćemo


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

obavijestiti nositelja podataka zasebno ili putem pododjeljka u našim pravilima o privatnosti (na našoj web stranici). U ovom slučaju vrijedi sljedeće:

Automatizirano donošenje odluka - uključujući profiliranje - može se dogoditi ako (1) je to potrebno za sklapanje ili izvršenje ugovora između ispitanika i nas, ili (2) je to dopušteno zakonom Unije ili države članice prema kojem se pridržavamo su predmet i koji također utvrđuje odgovarajuće mjere za zaštitu prava i sloboda i legitimnih interesa ispitanika; ili (3) to se temelji na izričitom pristanku nositelja podataka.

U slučajevima iz članka 22. stavka 2. (a) i (c) GDPR-a, provest ćemo odgovarajuće mjere za zaštitu prava i sloboda i legitimnih interesa ispitanika. U tim slučajevima imate pravo zatražiti ljudsku intervenciju od strane kontrolora, izraziti svoje stajalište i osporiti odluku.

Značajne informacije o uključenoj logici, kao i značaju i predviđenim posljedicama takve obrade za subjekta podataka navedene su u našim pravilima o privatnosti.

## III. EU-U.S. Data Privacy Framework (EU-U.S. DPF), UK Extension to the EU-U.S. DPF, Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF)

Ako je naša organizacija certificirani član EU-U.S. Data Privacy Framework (EU-U.S. DPF) i/ili UK Extension to the EU-U.S. DPF i/ili Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF), vrijedi sljedeće:

Mi se pridržavamo EU-U.S. Data Privacy Framework (EU-U.S. DPF) i UK Extension to the EU-U.S. DPF, kao i Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF), kako je određeno od strane U.S. Department of Commerce. Naša kompanija je potvrdila Ministarstvu trgovine SAD-a da se pridržava EU-U.S. Data Privacy Framework Principles (EU-U.S. DPF Principles) u vezi s obradom osobnih podataka koje prima iz Europske unije i Ujedinjenog Kraljevstva pozivajući se na EU-U.S. DPF i UK Extension to the EU-U.S. DPF. Naša kompanija je potvrdila Ministarstvu trgovine SAD-a da se pridržava Swiss-U.S. Data Privacy Framework Principles (Swiss-U.S. DPF Principles) u vezi s obradom osobnih podataka koje prima iz Švicarske pozivajući se na Swiss-U.S. DPF. U slučaju sukoba između odredbi naše politike privatnosti i EU-U.S. DPF Principles i/ili Swiss-U.S. DPF Principles, Principles su mjerodavne.

Za više informacija o Data Privacy Framework (DPF) programu i za pregled naše certifikacije, posjetite https://www.dataprivacyframework.gov/.

Ostale američke jedinice ili američke podružnice naše kompanije, koje se također pridržavaju EU-U.S. DPF Principles, uključujući UK Extension to the EU-U.S. DPF i Swiss-U.S. DPF Principles, ako postoje, navedene su u našoj politici privatnosti.

U skladu s EU-U.S. DPF i UK Extension to the EU-U.S. DPF, kao i Swiss-U.S. DPF, naša kompanija se obvezuje surađivati s tijelom koje su osnovale europske nadzorne vlasti za zaštitu podataka i britanski Information Commissioner's Office (ICO), kao i sa švicarskim Federal Data Protection and Information


© All rights reserved by Heiko Maniero.

Commissioner (EDÖB), te slijediti njihove savjete u vezi s neriješenim pritužbama o našem rukovanju osobnim podacima koje primamo pozivajući se na EU-U.S. DPF i UK Extension to the EU-U.S. DPF i Swiss-U.S. DPF.

Obavještavamo pogođene osobe o nadležnim europskim tijelima za zaštitu podataka koja su odgovorna za rješavanje pritužbi u vezi s rukovanjem osobnim podacima naše organizacije u gornjem dijelu ovog transparentnog dokumenta te da pogođenim osobama pružamo odgovarajuće i besplatno pravno sredstvo.

Obavještavamo sve pogođene osobe da naša kompanija podliježe istražnim i izvršnim ovlastima Federal Trade Commission (FTC).

Pogođene osobe imaju pravo, pod određenim uvjetima, zatražiti obvezujuću arbitražu. Naša organizacija je obvezna riješiti zahtjeve i pridržavati se uvjeta prema Prilogu I DPF-Principles, ako je pogođena osoba zatražila obvezujuću arbitražu tako što je obavijestila našu organizaciju i pridržavala se postupaka i uvjeta prema Prilogu I Principles.

Ovdje obavještavamo sve pogođene osobe o odgovornosti naše organizacije u slučaju prijenosa osobnih podataka trećim stranama.

Za pitanja pogođenih osoba ili tijela za zaštitu podataka imenovali smo lokalne predstavnike navedene u gornjem dijelu ovog transparentnog dokumenta.

Pružamo vam mogućnost izbora (Opt-out) da li želite da vaši osobni podaci (i) budu proslijeđeni trećim stranama ili (ii) korišteni u svrhu koja se bitno razlikuje od one za koju su izvorno prikupljeni ili koju ste kasnije odobrili. Jasan, vidljiv i lako dostupan mehanizam za ostvarivanje vašeg prava izbora je kontaktiranje našeg službenika za zaštitu podataka (DSB) putem e-pošte. Nemate mogućnost izbora i nismo obvezni to učiniti ako se podaci prosljeđuju trećoj strani koja djeluje kao agent ili obrađivač podataka u naše ime i prema našim uputama. Međutim, uvijek sklapamo ugovor s takvim agentom ili obrađivačem podataka.

Za osjetljive podatke (tj. osobne podatke koji sadrže informacije o zdravstvenom stanju, rasnom ili etničkom porijeklu, političkim mišljenjima, vjerskim ili filozofskim uvjerenjima, članstvu u sindikatu ili informacije o seksualnom životu pogođene osobe) tražimo vašu izričitu suglasnost (Opt-in) kada se ti podaci (i) prosljeđuju trećim stranama ili (ii) koriste u svrhu koja se razlikuje od one za koju su izvorno prikupljeni ili za koju ste kasnije dali svoju suglasnost odabirom Opt-in. Osim toga, sve osobne podatke koje primimo od trećih strana tretiramo kao osjetljive ako ih treća strana identificira i tretira kao osjetljive.

Ovdje vas obavještavamo o potrebi otkrivanja osobnih podataka kao odgovor na zakonite zahtjeve vlasti, uključujući ispunjavanje zahtjeva za nacionalnu sigurnost ili provođenje zakona.

Prilikom prijenosa osobnih podataka trećoj strani koja djeluje kao voditelj obrade, pridržavamo se Principles obavještavanja i izbora. Također sklapamo ugovor s trećom stranom koja je odgovorna za obradu, koji predviđa da se ti podaci smiju obrađivati samo za ograničene i određene svrhe u skladu s


© All rights reserved by Heiko Maniero.

vašom danom suglasnošću i da primatelj pruža istu razinu zaštite kao Principles DPF te nas obavještava ako utvrdi da više ne može ispunjavati tu obvezu. Ugovor predviđa da treća strana, koja je voditelj obrade, prekine obradu ili poduzme druge odgovarajuće i prikladne mjere kako bi se otklonio problem kada se takva situacija utvrdi.

Prilikom prijenosa osobnih podataka trećoj strani koja djeluje kao agent ili obrađivač podataka (i) prenosimo te podatke samo za ograničene i određene svrhe; (ii) uvjeravamo se da je agent ili obrađivač podataka obvezan osigurati najmanje istu razinu zaštite podataka kao što to zahtijevaju DPF-Principles; (iii) poduzimamo odgovarajuće i prikladne mjere kako bismo osigurali da agent ili obrađivač podataka stvarno obrađuje prenesene osobne podatke na način koji je u skladu s našim obvezama prema DPF-Principles; (iv) zahtijevamo od agenta ili obrađivača podataka da obavijesti našu organizaciju ako utvrdi da više ne može ispunjavati obvezu pružanja iste razine zaštite kao što to predviđaju DPF-Principles; (v) nakon obavijesti, uključujući onu pod (iv), poduzimamo odgovarajuće i prikladne korake kako bismo zaustavili neovlaštenu obradu i otklonili problem; i (vi) DPF Departmentu na zahtjev pružamo sažetak ili reprezentativni primjerak relevantnih odredbi ugovora o zaštiti podataka s tim agentom.

U skladu s EU-U.S. DPF i/ili UK Extension to the EU-U.S. DPF i/ili Swiss-U.S. DPF, naša organizacija se obvezuje surađivati s tijelom koje su osnovale europske nadzorne vlasti za zaštitu podataka i britanski Information Commissioner's Office (ICO), odnosno sa švicarskim Federal Data Protection and Information Commissioner (EDÖB), te slijediti njihove savjete u vezi s neriješenim pritužbama o našem rukovanju osobnim podacima u vezi s radnim odnosom koje primamo pozivajući se na EU-U.S. DPF i UK Extension to the EU-U.S. DPF i Swiss-U.S. DPF.

Svi subjekti podataka koji se privremeno nalaze u Europskoj uniji (EU), Europskom gospodarskom prostoru (EGP) ili Ujedinjenom Kraljevstvu, ili koji tamo imaju prebivalište ili uobičajeno boravište, imaju pravo na prava i prava ispitanika koji su objavljeni u našem Dokumenta o transparentnosti, koji također proizlaze iz članaka 15. do 22. GDPR-a, uključujući pravo na pristup osobnim podacima. Učinili smo ove informacije dostupnima na svim jezicima EU i EGP. Verzija na engleskom jeziku odnosi se na Ujedinjeno Kraljevstvo.

Svi subjekti podataka koji privremeno borave u Švicarskoj ili tamo imaju prebivalište ili uobičajeno boravište imaju pravo na prava i prava ispitanika prema švicarskom Zakonu o zaštiti podataka (DPA) i Švicarskoj uredbi o zaštiti podataka (DPR) koji su objavljeni u našoj Transparentnosti Dokument, uključujući pravo na pristup osobnim podacima. Ove smo informacije dali na tri službena jezika Švicarske (njemačkom, talijanskom i francuskom).


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

# CROATIAN: Informacije o obradi osobnih podataka za zaposlenike i podnositelje zahtjeva (članak 13, 14 GDPR)

Poštovani,

Osobni podaci zaposlenika i podnositelja zahtjeva zaslužuju posebnu zaštitu. Naš je cilj zadržati razinu zaštite podataka na visokom nivou. Stoga rutinski razvijamo koncepte zaštite podataka i sigurnosti podataka.

Naravno, poštujemo zakonske odredbe o zaštiti podataka. Prema člancima 13, 14 GDPR, kontroleri ispunjavaju posebne zahtjeve obavješćivanja pri obradi osobnih podataka. Ovaj dokument ispunjava te obveze.

Terminologija pravne regulacije je složena. Nažalost, korištenje pravnih izraza nije se moglo izostaviti u pripremi ovog dokumenta. Stoga želimo naglasiti da nas uvijek možete kontaktirati za sva pitanja vezana uz ovaj dokument, korištene pojmove ili formulacije.

## I. Usklađenost sa zahtjevima obavješćivanja kada se osobni podaci prikupljaju od nositelja podataka (članak 13. GDPR)

### A. Identitet i kontaktni podaci kontrolora (članak 13. stavak 1. točka (a) GDPR)

Vidi gore

### B. Kontaktni podaci službenika za zaštitu podataka (članak 13. stavak 1. točka (b) GDPR)

Vidi gore

### C. Svrha obrade za koju su osobni podaci namijenjeni, kao i pravna osnova za obradu (članak 13. stavak 1. točka (c) GDPR)

Za podatke podnositelja zahtjeva, svrha obrade podataka je provesti ispitivanje zahtjeva tijekom procesa zapošljavanja. U tu svrhu obrađujemo sve vaše podatke. Na temelju podataka dostavljenih tijekom procesa zapošljavanja, provjerit ćemo da li ste pozvani na razgovor za posao (dio postupka odabira). U


© All rights reserved by Heiko Maniero.

slučaju općenito prikladnih kandidata, posebno u kontekstu intervjua za posao, obrađujemo i neke druge osobne podatke koje ste dali, što je ključno za našu odluku o odabiru. Ako nas unajmite, podaci podnositelja zahtjeva automatski će se promijeniti u podatke zaposlenika. Kao dio procesa zapošljavanja, obradit ćemo druge osobne podatke o vama koje tražimo od vas i koji su potrebni za pokretanje ili ispunjenje vašeg ugovora (kao što su osobni identifikacijski brojevi ili porezni brojevi). Za podatke zaposlenika, svrha obrade podataka je izvršenje ugovora o radu ili poštivanje drugih zakonskih odredbi koje se primjenjuju na radni odnos (npr. Porezni zakon), kao i korištenje vaših osobnih podataka za izvršenje ugovora o radu sklopljenog s vama (npr. objavljivanje vašeg imena i kontaktne informacije unutar tvrtke ili klijentima). Podaci o zaposlenicima pohranjuju se nakon prestanka radnog odnosa radi ispunjenja zakonskog razdoblja zadržavanja.

Pravna osnova za obradu podataka je članak 6. stavak 1. točka (b) GDPR, članak 9 (2) točke (b) i (h) GDPR, članak 88 (1) GDPR i nacionalno zakonodavstvo, kao što je za Njemačku Odjeljak 26 BDSG (Savezni zakon o zaštiti podataka).

## D. Kategorije primatelja osobnih podataka (članak 13. stavak 1. točka (e) GDPR)

Javne vlasti

Vanjska tijela

Daljnja vanjska tijela

Interna obrada

Obrada unutar grupe

Ostala tijela

Popis naših izvršitelja obrade i primatelja podataka u trećim zemljama i, ako je primjenjivo, međunarodnim organizacijama objavljen je na našoj web stranici ili se može zatražiti od nas besplatno. Obratite se našem službeniku za zaštitu podataka kako biste zatražili ovaj popis.

## E. Primatelji u trećoj zemlji i odgovarajuće ili prikladne mjere zaštite i sredstva za njihovo pribavljanje ili njihovo stavljanje na raspolaganje (članak 13 (1) točka (f); 46(1), 46 (2) točka (c) GDPR)

Sve tvrtke i podružnice koje su dio naše grupe (u daljnjem tekstu: tvrtke grupe) koje imaju sjedište ili ured u trećoj zemlji mogu pripadati primateljima osobnih podataka. Od nas se može zatražiti popis svih tvrtki ili primatelja grupe.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

U skladu s člankom 46. stavkom 1. GDPR, kontrolor ili obrađivač može prenijeti osobne podatke samo trećoj zemlji ako je kontrolor ili obrađivač osigurao odgovarajuće zaštitne mjere i pod uvjetom da su na raspolaganju provediva prava subjekta podataka i učinkoviti pravni lijekovi za subjekte podataka. Odgovarajuće zaštitne mjere mogu se pružiti bez potrebe za posebnim odobrenjem nadzornog tijela putem standardnih ugovornih klauzula, članak 46 (2) točka (c) GDPR.

Standardne ugovorne klauzule Europske unije ili druge odgovarajuće mjere zaštite dogovorene su sa svim primateljima iz trećih zemalja prije prvog prijenosa osobnih podataka. Slijedom toga, osigurano je da su zajamčeni odgovarajući zaštitni mehanizmi, primjenjiva prava subjekata podataka i djelotvorni pravni lijekovi za subjekte podataka. Svaki subjekt podataka može od nas dobiti kopiju standardnih ugovornih klauzula. Standardne ugovorne klauzule također su dostupne u Službenom listu Europske unije.

Članak 45. stavak 3. Opće uredbe o zaštiti podataka (GDPR) daje Europskoj komisiji ovlast da putem provedbenog akta odluči da zemlja koja nije članica EU-a osigurava odgovarajuću razinu zaštite. To znači razinu zaštite osobnih podataka koja je u biti jednaka razini zaštite unutar EU-a. Učinak odluka o primjerenosti je da osobni podaci mogu slobodno teći iz EU (i Norveške, Lihtenštajna i Islanda) u treću zemlju bez daljnjih prepreka. Slična pravila postoje za Ujedinjeno Kraljevstvo, Švicarsku i neke druge zemlje.

Kada je Europska komisija ili vlada druge zemlje odlučila da treća zemlja osigurava odgovarajuću razinu zaštite, a postoji važeći okvir (npr. EU-U.S. Data Privacy Framework, Swiss-U.S. Data Privacy Framework, UK Extension to the EU-U.S. Data Privacy Framework), svi naši prijenosi članovima takvih okvira (npr. samocertificirani subjekti) temelje se isključivo na članstvu tih subjekata u dotičnom okviru. Tamo gdje smo mi ili jedan od entiteta naše grupe član takvog okvira, svi prijenosi nama ili entitetu naše grupe temelje se isključivo na članstvu entiteta u takvom okviru.

Svaki subjekt podataka može od nas dobiti kopiju okvira. Osim toga, okviri su također dostupni u Službenom listu Europske unije ili u objavljenim pravnim materijalima ili na web stranicama nadzornih tijela ili drugih nadležnih tijela ili institucija.

## F. Razdoblje za koje će osobni podaci biti pohranjeni, ili ako to nije moguće odrediti, kriteriji koji se koriste za određivanje tog razdoblja (članak 13. stavak 2. točka (a) GDPR)

Trajanje pohrane osobnih podataka podnositelja zahtjeva je 6 mjeseci. Za podatke zaposlenika primjenjuje se odgovarajuće razdoblje zadržavanja. Nakon isteka tog razdoblja, odgovarajući podaci se rutinski brišu, sve dok više nisu potrebni za ispunjenje ugovora ili pokretanje ugovora.


© All rights reserved by Heiko Maniero.

## G. Postojanje prava da se od kontrolora zatraži pristup i ispravak ili brisanje osobnih podataka ili ograničenje obrade u odnosu na nositelja podataka ili da se uloži prigovor na obradu, kao i pravo na prenosivost podataka (članak 13. stavak 2. točka (b) GDPR)

Svi subjekti podataka imaju sljedeća prava:

***Pravo na pristup***

Svaki subjekt podataka ima pravo pristupa osobnim podacima koji se odnose na njega. Pravo na pristup proteže se na sve podatke koje obrađujemo. Pravo se može ostvariti lako i u razumnim vremenskim razmacima, kako bi bio svjestan i provjerio zakonitost obrade (uvodna izjava 63 GDPR). Ovo pravo proizlazi iz čl. 15 GDPR. Subjekt podataka može nas kontaktirati kako bi ostvario pravo pristupa.

***Pravo na ispravak***

U skladu s člankom 16. rečenica 1 GDPR, osoba čiji se podaci obrađuju ima pravo od kontrolora bez nepotrebnog odgađanja dobiti ispravak netočnih osobnih podataka koji se odnose na njega. Nadalje, člankom 16. rečenica 2 GDPR predviđeno je da subjekt podataka ima pravo, uzimajući u obzir svrhu obrade, imati dovršene nepotpune osobne podatke, uključujući i pružanje dodatne izjave. Subjekt podataka može nas kontaktirati kako bi ostvario pravo na ispravak.

***Pravo na brisanje (pravo na zaborav)***

Osim toga, osobe čiji se podaci obrađuju imaju pravo na brisanje i pravo da podaci budu zaboravljeni na temelju čl. 17 GDPR. To se pravo može ostvariti ako nas kontaktirate. U ovom trenutku, međutim, želimo naglasiti da se to pravo ne primjenjuje u onoj mjeri u kojoj je obrada potrebna kako bi se ispunila zakonska obveza na koju je naša tvrtka podložna, članak 17 (3) točka (b) GDPR. To znači da možemo odobriti zahtjev za brisanje samo nakon isteka zakonskog roka zadržavanja.

***Pravo na ograničenje obrade***

Prema članku 18. GDPR, svaki subjekt podataka ima pravo na ograničenje obrade. Ograničenje obrade može se zahtijevati ako je jedan od uvjeta iz članka 18. stavka 1 točke a-d GDPR je ispunjen. Subjekt podataka može nas kontaktirati kako bi ostvario pravo na ograničenje obrade.

***Pravo na prigovor***

Nadalje, čl. 21 GDPR jamči pravo na prigovor. Subjekt podataka može nas kontaktirati kako bi ostvario pravo na prigovor.

***Pravo na prenosivost podataka***

Članak 20 GDPR daje subjektu podataka pravo na prenosivost podataka. Prema ovoj odredbi, subjekt podataka pod uvjetima iz članka 20. stavka 1. točke a i b GDPR ima pravo na primanje osobnih podataka koji se odnose na njega ili nju, koje je on ili ona pružio kontroloru, u strukturiranom, uobičajeno korištenom i strojno čitljivom formatu i imaju pravo na nesmetani prijenos tih podataka drugom kontroloru od kontrolora kojem su dostavljeni osobni podaci. Subjekt podataka može nas kontaktirati radi ostvarivanja prava na prenosivost podataka.


© All rights reserved by Heiko Maniero.

## H. Postojanje prava na povlačenje pristanka u bilo kojem trenutku, bez utjecaja na zakonitost obrade na temelju suglasnosti prije njegovog povlačenja, ako se obrada temelji na članku 6. stavku 1. točka (a) GDPR ili članak 9 (2) točka (a) GDPR (članak 13. stavak 2. točka c GDPR)

Ako se obrada osobnih podataka temelji na čl. 6 (1) točka (a) GDPR, što je slučaj, ako je subjekt podataka dao pristanak na obradu osobnih podataka za jednu ili više posebnih svrha ili se temelji na članku 9 (2) točka (a) GDPR, koji regulira izričitu suglasnost za obradu posebnih kategorija osobnih podataka, subjekt podataka ima u skladu s člankom 7. stavkom 3. rečenice 1 GDPR-a pravo povući svoj pristanak u bilo kojem trenutku.

Povlačenje suglasnosti ne utječe na zakonitost obrade na temelju suglasnosti prije njezina povlačenja, članak 7. stavak 3. rečenica 2 GDPR. Povlačenje je jednako lako kao i davanje pristanka, čl. 7 (3) rečenica 4 GDPR. Stoga se povlačenje suglasnosti uvijek može dogoditi na isti način kao što je pristanak dan ili na bilo koji drugi način, što subjekt podataka smatra jednostavnijim. U današnjem informacijskom društvu, vjerojatno je najjednostavniji način povlačenja pristanka jednostavna e-pošta. Ako subjekt podataka želi povući svoj odobreni pristanak, dovoljan nam je jednostavan e-mail. Alternativno, subjekt podataka može odabrati bilo koji drugi način da nam priopći svoje povlačenje pristanka.

## I. Pravo na podnošenje pritužbe nadzornom tijelu (članak 13. stavak 2. točka (d), članak 77. stavak 1. GDPR)

Kao kontrolor, dužni smo obavijestiti nositelja podataka o pravu na podnošenje pritužbe nadzornom tijelu, članak 13 (2) točka (d) GDPR. Pravo na podnošenje pritužbe nadzornom tijelu regulirano je člankom 77. stavkom 1. GDPR. U skladu s ovom odredbom, pre ulaganja bilo kojeg drugog administrativnog ili pravnog lijeka, svaki subjekt podataka ima pravo podnijeti pritužbu nadzornom tijelu, posebno u državi članici u kojoj ima prebivalište, radno mjesto ili mjesto navodne povrede ako subjekt podataka smatra da obrada osobnih podataka koji se odnose na njega ili nju krši Opću uredbu o zaštiti podataka. Pravo na podnošenje pritužbe nadzornom tijelu bilo je ograničeno samo pravom Unije na takav način, da se može ostvariti samo pred jednim nadzornim tijelom (uvodna izjava 141, rečenica 1 GDPR). Cilj ovog pravila je izbjegavanje dvostrukih pritužbi istog subjekta podataka u istom predmetu. Ako subjekt podataka želi podnijeti pritužbu na nas, tražimo da kontaktira samo jedno nadzorno tijelo.

## J. Pružanje osobnih podataka kao zakonski ili ugovorni zahtjev; Zahtjev potreban za sklapanje ugovora; Obveza nositelja podataka da dostavi osobne podatke; moguće posljedice nepružanja takvih podataka (čl. 13. stavak 2. točka (e) GDPR)

Pojašnjavamo da je davanje osobnih podataka djelomično zahtijevano zakonom (npr. Porezni propisi) ili također može proizaći iz ugovornih odredbi (npr. Informacija o ugovornom partneru).


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

Ponekad može biti potrebno sklopiti ugovor kojim nam subjekt podataka daje osobne podatke, koje moramo naknadno obraditi. Subjekt podataka je, primjerice, dužan da nam dostavi osobne podatke kada naša tvrtka s njim ili njom potpiše ugovor. Nepružanje osobnih podataka imalo bi za posljedicu da se ugovor s subjektom podataka ne može zaključiti.

Prije davanja osobnih podataka od strane nositelja podataka, osoba na koju se podaci odnose mora nas kontaktirati. Obavjestićemo osobu na koju se podaci odnose je li pružanje osobnih podataka obvezno po zakonu ili ugovoru ili je potrebno za sklapanje ugovora, postoji li obaveza pružanja osobnih podataka i posljedica nepružanja osobnih podataka.

### K. Postojanje automatiziranog odlučivanja, uključujući profiliranje, iz članka 22. (1) i (4) GDPR i barem u tim slučajevima, značajne informacije o logici koja je uključena, kao i značaj i predviđene posljedice takve obrade za osobe čiji se podaci obrađuju (članak 13. stavak 2. točka (f) GDPR)

Kao odgovorna tvrtka, obično ne koristimo automatizirano donošenje odluka ili profiliranje. Ako, u iznimnim slučajevima, provodimo automatizirano donošenje odluka ili profiliranje, o tome ćemo obavijestiti nositelja podataka zasebno ili putem pododjeljka u našim pravilima o privatnosti (na našoj web stranici). U ovom slučaju vrijedi sljedeće:

Automatizirano donošenje odluka - uključujući profiliranje - može se dogoditi ako (1) je to potrebno za sklapanje ili izvršenje ugovora između ispitanika i nas, ili (2) je to dopušteno zakonom Unije ili države članice prema kojem se pridržavamo su predmet i koji također utvrđuje odgovarajuće mjere za zaštitu prava i sloboda i legitimnih interesa ispitanika; ili (3) to se temelji na izričitom pristanku nositelja podataka.

U slučajevima iz članka 22. stavka 2. (a) i (c) GDPR-a, provest ćemo odgovarajuće mjere za zaštitu prava i sloboda i legitimnih interesa ispitanika. U tim slučajevima imate pravo zatražiti ljudsku intervenciju od strane kontrolora, izraziti svoje stajalište i osporiti odluku.

Značajne informacije o uključenoj logici, kao i značaju i predviđenim posljedicama takve obrade za subjekta podataka navedene su u našim pravilima o privatnosti.

## II. Usklađenost sa zahtjevima obavješćivanja kada se osobni podaci ne prikupljaju od nositelja podataka (članak 14.GDPR)

### A. Identitet i kontaktni podaci kontrolora (članak 14. stavak 1. točka (a) GDPR)

Vidi gore


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## B. Kontaktni podaci službenika za zaštitu podataka (članak 14. stavak 1. točka (b) GDPR)

Vidi gore

## C. Svrha obrade za koju su osobni podaci namijenjeni, kao i pravna osnova za obradu (članak 14 (1) točka (c) GDPR)

Za podatke podnositelja zahtjeva koji nisu prikupljeni od nositelja podataka, svrha obrade podataka je provesti ispitivanje zahtjeva tijekom postupka zapošljavanja. U tu svrhu možemo obrađivati podatke koji nisu prikupljeni od vas. Na temelju podataka obrađenih tijekom procesa zapošljavanja, provjerit ćemo da li ste pozvani na razgovor za posao (dio postupka odabira). Ako vas unajmimo, podaci podnositelja zahtjeva automatski će se pretvoriti u podatke zaposlenika. Za podatke zaposlenika, svrha obrade podataka je izvršenje ugovora o radu ili poštivanje drugih zakonskih odredbi koje se primjenjuju na radni odnos. Podaci o zaposlenicima pohranjuju se nakon prestanka radnog odnosa radi ispunjenja zakonskog razdoblja zadržavanja.

Pravna osnova za obradu podataka je članak 6. stavak 1. točke b i f GDPR, članak 9 (2) točke b i h GDPR, članak 88 (1) GDPR i nacionalno zakonodavstvo, kao što je za Njemačku Odjeljak 26 BDSG (Savezni zakon o zaštiti podataka).

## D. Kategorije dotičnih osobnih podataka (članak 14. stavak 1. točka (d) GDPR)

Podaci podnositelja zahtjeva

Podaci o zaposlenicima

## E. Kategorije primatelja osobnih podataka (članak 14. stavak 1. točka (e) GDPR)

Javne vlasti

Vanjska tijela

Daljnja vanjska tijela

Interna obrada

Obrada unutar grupe


© All rights reserved by Heiko Maniero.

Ostala tijela

Popis naših izvršitelja obrade i primatelja podataka u trećim zemljama i, ako je primjenjivo, međunarodnim organizacijama objavljen je na našoj web stranici ili se može zatražiti od nas besplatno. Obratite se našem službeniku za zaštitu podataka kako biste zatražili ovaj popis.

## F. Primatelji u trećoj zemlji i odgovarajuće ili prikladne mjere zaštite i sredstva za njihovo pribavljanje ili njihovo stavljanje na raspolaganje (članak 14. stavak 1. točka (f), 46 (1), 46 (2) točka (c) GDPR)

Sve tvrtke i podružnice koje su dio naše grupe (u daljnjem tekstu: tvrtke grupe) koje imaju sjedište ili ured u trećoj zemlji mogu pripadati primateljima osobnih podataka. Od nas se može zatražiti popis svih tvrtki ili primatelja grupe.

U skladu s člankom 46. stavkom 1. GDPR, kontrolor ili obrađivač može prenijeti osobne podatke samo trećoj zemlji ako je kontrolor ili obrađivač osigurao odgovarajuće zaštitne mjere i pod uvjetom da su na raspolaganju provediva prava subjekta podataka i učinkoviti pravni lijekovi za subjekte podataka. Odgovarajuće zaštitne mjere mogu se pružiti bez potrebe za posebnim odobrenjem nadzornog tijela pomoću standardnih klauzula o zaštiti podataka, članak 46 (2) točka (c) GDPR.

Standardne ugovorne klauzule Europske unije ili druge odgovarajuće mjere zaštite dogovorene su sa svim primateljima iz trećih zemalja prije prvog prijenosa osobnih podataka. Slijedom toga, osigurano je da su zajamčeni odgovarajući zaštitni mehanizmi, primjenjiva prava subjekata podataka i djelotvorni pravni lijekovi za subjekte podataka. Svaki subjekt podataka može od nas dobiti kopiju standardnih ugovornih klauzula. Standardne ugovorne klauzule također su dostupne u Službenom listu Europske unije.

Članak 45. stavak 3. Opće uredbe o zaštiti podataka (GDPR) daje Europskoj komisiji ovlast da putem provedbenog akta odluči da zemlja koja nije članica EU-a osigurava odgovarajuću razinu zaštite. To znači razinu zaštite osobnih podataka koja je u biti jednaka razini zaštite unutar EU-a. Učinak odluka o primjerenosti je da osobni podaci mogu slobodno teći iz EU (i Norveške, Lihtenštajna i Islanda) u treću zemlju bez daljnjih prepreka. Slična pravila postoje za Ujedinjeno Kraljevstvo, Švicarsku i neke druge zemlje.

Kada je Europska komisija ili vlada druge zemlje odlučila da treća zemlja osigurava odgovarajuću razinu zaštite, a postoji važeći okvir (npr. EU-U.S. Data Privacy Framework, Swiss-U.S. Data Privacy Framework, UK Extension to the EU-U.S. Data Privacy Framework), svi naši prijenosi članovima takvih okvira (npr. samocertificirani subjekti) temelje se isključivo na članstvu tih subjekata u dotičnom okviru. Tamo gdje smo mi ili jedan od entiteta naše grupe član takvog okvira, svi prijenosi nama ili entitetu naše grupe temelje se isključivo na članstvu entiteta u takvom okviru.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

Svaki subjekt podataka može od nas dobiti kopiju okvira. Osim toga, okviri su također dostupni u Službenom listu Europske unije ili u objavljenim pravnim materijalima ili na web stranicama nadzornih tijela ili drugih nadležnih tijela ili institucija.

## G. Razdoblje za koje će osobni podaci biti pohranjeni ili, ako to nije moguće odrediti, kriteriji koji se koriste za određivanje tog razdoblja (članak 14. stavak 2. točka (a) GDPR)

Trajanje pohrane osobnih podataka podnositelja zahtjeva je 6 mjeseci. Za podatke zaposlenika primjenjuje se odgovarajuće razdoblje zadržavanja. Nakon isteka tog razdoblja, odgovarajući podaci se rutinski brišu, sve dok više nisu potrebni za ispunjenje ugovora ili pokretanje ugovora.

## H. Obavijest o legitimnim interesima koje provodi kontrolor ili treća strana ako se obrada temelji na članku 6 (1) točka (f) GDPR (čl. 14 (2) točka (b) GDPR)

Prema članku 6 (1) točka (f) GDPR, obrada će biti zakonita samo ako je obrada potrebna u svrhe legitimnih interesa koje ostvaruje kontrolor ili treća strana, osim ako su ti interesi nadjačani interesima ili temeljnim pravima i slobodama nositelja podataka koji zahtijevaju zaštitu osobnih podataka. U skladu s uvodnom izjavom 47. rečenica 2. GDPR legitiman interes može postojati tamo gdje postoji relevantan i odgovarajući odnos između ispitanika i kontrolora, npr. u situacijama u kojima je subjekt podataka klijent kontrolora. U svim slučajevima u kojima naša tvrtka obrađuje podatke podnositelja zahtjeva na temelju članka 6 (1) točka (f) GDPR, naš legitimni interes je zapošljavanje odgovarajućeg osoblja i stručnjaka.

## I. Postojanje prava da se od kontrolora zatraži pristup i ispravak ili brisanje osobnih podataka ili ograničenje obrade u vezi s nositeljem podataka te da se uloži prigovor na obradu, kao i pravo na prenosivost podataka (članak 14. stavak 2. točka (c) GDPR)

Svi subjekti podataka imaju sljedeća prava:

***Pravo na pristup***

Svaki subjekt podataka ima pravo pristupa osobnim podacima koji se odnose na njega. Pravo na pristup proteže se na sve podatke koje obrađujemo. Pravo se može ostvariti lako i u razumnim vremenskim razmacima, kako bi bio svjestan i provjerio zakonitost obrade (uvodna izjava 63 GDPR). Ovo pravo proizlazi iz čl. 15 GDPR. Subjekt podataka može nas kontaktirati kako bi ostvario pravo pristupa.

***Pravo na ispravak***

U skladu s člankom 16. rečenica 1 GDPR, osoba čiji se podaci obrađuju ima pravo od kontrolora bez nepotrebnog odgađanja dobiti ispravak netočnih osobnih podataka koji se odnose na njega. Nadalje, člankom 16. rečenica 2 GDPR predviđeno je da subjekt podataka ima pravo, uzimajući u obzir svrhu


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

obrade, imati dovršene nepotpune osobne podatke, uključujući i pružanje dodatne izjave. Subjekt podataka može nas kontaktirati kako bi ostvario pravo na ispravak.

***Pravo na brisanje (pravo na zaborav)***

Osim toga, osobe čiji se podaci obrađuju imaju pravo na brisanje i pravo da podaci budu zaboravljeni na temelju čl. 17 GDPR. To se pravo može ostvariti ako nas kontaktirate. U ovom trenutku, međutim, želimo naglasiti da se to pravo ne primjenjuje u onoj mjeri u kojoj je obrada potrebna kako bi se ispunila zakonska obveza na koju je naša tvrtka podložna, članak 17 (3) točka (b) GDPR. To znači da možemo odobriti zahtjev za brisanje samo nakon isteka zakonskog roka zadržavanja.

***Pravo na ograničenje obrade***

Prema članku 18. GDPR, svaki subjekt podataka ima pravo na ograničenje obrade. Ograničenje obrade može se zahtijevati ako je jedan od uvjeta iz članka 18. stavka 1. točke a-d GDPR je ispunjen. Subjekt podataka može nas kontaktirati kako bi ostvario pravo na ograničenje obrade.

***Pravo na prigovor***

Nadalje, čl. 21 GDPR jamči pravo na prigovor. Subjekt podataka može nas kontaktirati kako bi ostvario pravo na prigovor.

***Pravo na prenosivost podataka***

Članak 20 GDPR daje subjektu podataka pravo na prenosivost podataka. Prema ovoj odredbi, subjekt podataka pod uvjetima iz članka 20. stavka 1. točke a i b GDPR ima pravo na primanje osobnih podataka koji se odnose na njega ili nju, koje je on ili ona pružio kontroloru, u strukturiranom, uobičajeno korištenom i strojno čitljivom formatu i imaju pravo na nesmetani prijenos tih podataka drugom kontroloru od kontrolora kojem su dostavljeni osobni podaci. Subjekt podataka može nas kontaktirati radi ostvarivanja prava na prenosivost podataka.

## J. Postojanje prava na povlačenje pristanka u bilo kojem trenutku, bez utjecaja na zakonitost obrade na temelju suglasnosti prije njegovog povlačenja, ako se obrada temelji na članku 6. stavku 1. točka (a) ili članak 9. (2) točka (a) GDPR (čl. 14 (2) točka (d) GDPR)

Ako se obrada osobnih podataka temelji na čl. 6 (1) točka (a) GDPR, što je slučaj, ako je subjekt podataka dao pristanak na obradu osobnih podataka za jednu ili više posebnih svrha ili se temelji na članku 9 (2) točka (a) GDPR, koji regulira izričitu suglasnost za obradu posebnih kategorija osobnih podataka, subjekt podataka ima u skladu s člankom 7. stavkom 3. rečenice 1 GDPR pravo povući svoj pristanak u bilo kojem trenutku.

Povlačenje suglasnosti ne utječe na zakonitost obrade na temelju suglasnosti prije njenog povlačenja, članak 7. stavak 3. rečenica 2 GDPR. Povlačenje je jednako lako kao i davanje pristanka, čl. 7 (3) rečenica 4 GDPR. Stoga se povlačenje suglasnosti uvijek može dogoditi na isti način kao što je pristanak


© All rights reserved by Heiko Maniero.

dan ili na bilo koji drugi način, što subjekt podataka smatra jednostavnijim. U današnjem informacijskom društvu, vjerojatno je najjednostavniji način povlačenja pristanka jednostavna e-pošta. Ako subjekt podataka želi povući svoj odobreni pristanak, dovoljan nam je jednostavan e-mail. Alternativno, subjekt podataka može odabrati bilo koji drugi način da nam priopći svoje povlačenje pristanka.

## K. Pravo na podnošenje pritužbe nadzornom tijelu (članak 14. stavak 2. točka (e), članak 77. stavak 1. GDPR)

Kao kontrolor, dužni smo obavijestiti nositelja podataka o pravu podnošenja pritužbe nadzornom tijelu, članak 14 (2) točka (e) GDPR. Pravo na podnošenje pritužbe nadzornom tijelu regulirano je člankom 77. stavkom 1. GDPR. U skladu s ovom odredbom, pre ulaganja bilo kojeg drugog administrativnog ili pravnog lijeka, svaki subjekt podataka ima pravo podnijeti pritužbu nadzornom tijelu, posebno u državi članici u kojoj ima prebivalište, radno mjesto ili mjesto navodne povrede ako subjekt podataka smatra da obrada osobnih podataka koji se odnose na njega ili nju krši Opću uredbu o zaštiti podataka. Pravo na podnošenje pritužbe nadzornom tijelu bilo je ograničeno samo pravom Unije na takav način, da se može ostvariti samo pred jednim nadzornim tijelom (uvodna izjava 141, rečenica 1 GDPR). Cilj ovog pravila je izbjegavanje dvostrukih pritužbi istog subjekta podataka u istom predmetu. Ako subjekt podataka želi podnijeti pritužbu na nas, tražimo da kontaktira samo jedno nadzorno tijelo.

## L. Izvor iz kog osobni podatci potječu, i ako je primjenjivo, jesu li došli iz javno dostupnih izvora (članak 14. stavak 2. točka (f) GDPR)

U načelu, osobni se podaci prikupljaju izravno od nositelja podataka ili u suradnji s nadležnim tijelom (npr. Dohvat podataka iz službenog registra). Ostali podaci o subjektima podataka proizlaze iz transfera društava grupe. U kontekstu ove opće informacije, imenovanje točnih izvora iz kojih su osobni podaci nastali ili je nemoguće ili bi uključivalo nerazmjerne napore u smislu čl. 14 (5) točka (b) GDPR. U načelu, ne prikupljamo osobne podatke iz javno dostupnih izvora.

Svaki subjekt podataka može nas kontaktirati u bilo koje vrijeme kako bi dobili detaljnije informacije o točnim izvorima osobnih podataka koji se odnose na njega. Ako se podrijetlo osobnih podataka ne može dati subjektu podataka jer su korišteni različiti izvori, potrebno je dostaviti opće informacije (uvodna izjava 61, rečenica 4 GDPR).


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

### M. Postojanje automatiziranog odlučivanja, uključujući profiliranje, iz članka 22. (1) i (4) GDPR, i barem u tim slučajevima, značajne informacije o logici koja je uključena, kao i značaj i predviđene posljedice takve obrade za osobe čiji se podaci obrađuju (članak 14. stavak 2. točka g)

Kao odgovorna tvrtka, obično ne koristimo automatizirano donošenje odluka ili profiliranje. Ako, u iznimnim slučajevima, provodimo automatizirano donošenje odluka ili profiliranje, o tome ćemo obavijestiti nositelja podataka zasebno ili putem pododjeljka u našim pravilima o privatnosti (na našoj web stranici). U ovom slučaju vrijedi sljedeće:

Automatizirano donošenje odluka - uključujući profiliranje - može se dogoditi ako (1) je to potrebno za sklapanje ili izvršenje ugovora između ispitanika i nas, ili (2) je to dopušteno zakonom Unije ili države članice prema kojem se pridržavamo su predmet i koji također utvrđuje odgovarajuće mjere za zaštitu prava i sloboda i legitimnih interesa ispitanika; ili (3) to se temelji na izričitom pristanku nositelja podataka.

U slučajevima iz članka 22. stavka 2. (a) i (c) GDPR-a, provest ćemo odgovarajuće mjere za zaštitu prava i sloboda i legitimnih interesa ispitanika. U tim slučajevima imate pravo zatražiti ljudsku intervenciju od strane kontrolora, izraziti svoje stajalište i osporiti odluku.

Značajne informacije o uključenoj logici, kao i značaju i predviđenim posljedicama takve obrade za subjekta podataka navedene su u našim pravilima o privatnosti.

## III. EU-U.S. Data Privacy Framework (EU-U.S. DPF), UK Extension to the EU-U.S. DPF, Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF)

Ako je naša organizacija certificirani član EU-U.S. Data Privacy Framework (EU-U.S. DPF) i/ili UK Extension to the EU-U.S. DPF i/ili Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF), vrijedi sljedeće:

Mi se pridržavamo EU-U.S. Data Privacy Framework (EU-U.S. DPF) i UK Extension to the EU-U.S. DPF, kao i Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF), kako je određeno od strane U.S. Department of Commerce. Naša kompanija je potvrdila Ministarstvu trgovine SAD-a da se pridržava EU-U.S. Data Privacy Framework Principles (EU-U.S. DPF Principles) u vezi s obradom osobnih podataka koje prima iz Europske unije i Ujedinjenog Kraljevstva pozivajući se na EU-U.S. DPF i UK Extension to the EU-U.S. DPF. Naša kompanija je potvrdila Ministarstvu trgovine SAD-a da se pridržava Swiss-U.S. Data Privacy Framework Principles (Swiss-U.S. DPF Principles) u vezi s obradom osobnih podataka koje prima iz Švicarske pozivajući se na Swiss-U.S. DPF. U slučaju sukoba između odredbi naše politike privatnosti i EU-U.S. DPF Principles i/ili Swiss-U.S. DPF Principles, Principles su mjerodavne.

Za više informacija o Data Privacy Framework (DPF) programu i za pregled naše certifikacije, posjetite https://www.dataprivacyframework.gov/.


© All rights reserved by Heiko Maniero.

Ostale američke jedinice ili američke podružnice naše kompanije, koje se također pridržavaju EU-U.S. DPF Principles, uključujući UK Extension to the EU-U.S. DPF i Swiss-U.S. DPF Principles, ako postoje, navedene su u našoj politici privatnosti.

U skladu s EU-U.S. DPF i UK Extension to the EU-U.S. DPF, kao i Swiss-U.S. DPF, naša kompanija se obvezuje surađivati s tijelom koje su osnovale europske nadzorne vlasti za zaštitu podataka i britanski Information Commissioner's Office (ICO), kao i sa švicarskim Federal Data Protection and Information Commissioner (EDÖB), te slijediti njihove savjete u vezi s neriješenim pritužbama o našem rukovanju osobnim podacima koje primamo pozivajući se na EU-U.S. DPF i UK Extension to the EU-U.S. DPF i Swiss-U.S. DPF.

Obavještavamo pogođene osobe o nadležnim europskim tijelima za zaštitu podataka koja su odgovorna za rješavanje pritužbi u vezi s rukovanjem osobnim podacima naše organizacije u gornjem dijelu ovog transparentnog dokumenta te da pogođenim osobama pružamo odgovarajuće i besplatno pravno sredstvo.

Obavještavamo sve pogođene osobe da naša kompanija podliježe istražnim i izvršnim ovlastima Federal Trade Commission (FTC).

Pogođene osobe imaju pravo, pod određenim uvjetima, zatražiti obvezujuću arbitražu. Naša organizacija je obvezna riješiti zahtjeve i pridržavati se uvjeta prema Prilogu I DPF-Principles, ako je pogođena osoba zatražila obvezujuću arbitražu tako što je obavijestila našu organizaciju i pridržavala se postupaka i uvjeta prema Prilogu I Principles.

Ovdje obavještavamo sve pogođene osobe o odgovornosti naše organizacije u slučaju prijenosa osobnih podataka trećim stranama.

Za pitanja pogođenih osoba ili tijela za zaštitu podataka imenovali smo lokalne predstavnike navedene u gornjem dijelu ovog transparentnog dokumenta.

Pružamo vam mogućnost izbora (Opt-out) da li želite da vaši osobni podaci (i) budu proslijeđeni trećim stranama ili (ii) korišteni u svrhu koja se bitno razlikuje od one za koju su izvorno prikupljeni ili koju ste kasnije odobrili. Jasan, vidljiv i lako dostupan mehanizam za ostvarivanje vašeg prava izbora je kontaktiranje našeg službenika za zaštitu podataka (DSB) putem e-pošte. Nemate mogućnost izbora i nismo obvezni to učiniti ako se podaci prosljeđuju trećoj strani koja djeluje kao agent ili obrađivač podataka u naše ime i prema našim uputama. Međutim, uvijek sklapamo ugovor s takvim agentom ili obrađivačem podataka.

Za osjetljive podatke (tj. osobne podatke koji sadrže informacije o zdravstvenom stanju, rasnom ili etničkom porijeklu, političkim mišljenjima, vjerskim ili filozofskim uvjerenjima, članstvu u sindikatu ili informacije o seksualnom životu pogođene osobe) tražimo vašu izričitu suglasnost (Opt-in) kada se ti podaci (i) prosljeđuju trećim stranama ili (ii) koriste u svrhu koja se razlikuje od one za koju su izvorno prikupljeni ili za koju ste kasnije dali svoju suglasnost odabirom Opt-in. Osim toga, sve osobne podatke koje primimo od trećih strana tretiramo kao osjetljive ako ih treća strana identificira i tretira kao osjetljive.


© All rights reserved by Heiko Maniero.

Ovdje vas obavještavamo o potrebi otkrivanja osobnih podataka kao odgovor na zakonite zahtjeve vlasti, uključujući ispunjavanje zahtjeva za nacionalnu sigurnost ili provođenje zakona.

Prilikom prijenosa osobnih podataka trećoj strani koja djeluje kao voditelj obrade, pridržavamo se Principles obavještavanja i izbora. Također sklapamo ugovor s trećom stranom koja je odgovorna za obradu, koji predviđa da se ti podaci smiju obrađivati samo za ograničene i određene svrhe u skladu s vašom danom suglasnošću i da primatelj pruža istu razinu zaštite kao Principles DPF te nas obavještava ako utvrdi da više ne može ispunjavati tu obvezu. Ugovor predviđa da treća strana, koja je voditelj obrade, prekine obradu ili poduzme druge odgovarajuće i prikladne mjere kako bi se otklonio problem kada se takva situacija utvrdi.

Prilikom prijenosa osobnih podataka trećoj strani koja djeluje kao agent ili obrađivač podataka (i) prenosimo te podatke samo za ograničene i određene svrhe; (ii) uvjeravamo se da je agent ili obrađivač podataka obvezan osigurati najmanje istu razinu zaštite podataka kao što to zahtijevaju DPF-Principles; (iii) poduzimamo odgovarajuće i prikladne mjere kako bismo osigurali da agent ili obrađivač podataka stvarno obrađuje prenesene osobne podatke na način koji je u skladu s našim obvezama prema DPF-Principles; (iv) zahtijevamo od agenta ili obrađivača podataka da obavijesti našu organizaciju ako utvrdi da više ne može ispunjavati obvezu pružanja iste razine zaštite kao što to predviđaju DPF-Principles; (v) nakon obavijesti, uključujući onu pod (iv), poduzimamo odgovarajuće i prikladne korake kako bismo zaustavili neovlaštenu obradu i otklonili problem; i (vi) DPF Departmentu na zahtjev pružamo sažetak ili reprezentativni primjerak relevantnih odredbi ugovora o zaštiti podataka s tim agentom.

U skladu s EU-U.S. DPF i/ili UK Extension to the EU-U.S. DPF i/ili Swiss-U.S. DPF, naša organizacija se obvezuje surađivati s tijelom koje su osnovale europske nadzorne vlasti za zaštitu podataka i britanski Information Commissioner's Office (ICO), odnosno sa švicarskim Federal Data Protection and Information Commissioner (EDÖB), te slijediti njihove savjete u vezi s neriješenim pritužbama o našem rukovanju osobnim podacima u vezi s radnim odnosom koje primamo pozivajući se na EU-U.S. DPF i UK Extension to the EU-U.S. DPF i Swiss-U.S. DPF.

Svi subjekti podataka koji se privremeno nalaze u Europskoj uniji (EU), Europskom gospodarskom prostoru (EGP) ili Ujedinjenom Kraljevstvu, ili koji tamo imaju prebivalište ili uobičajeno boravište, imaju pravo na prava i prava ispitanika koji su objavljeni u našem Dokumenta o transparentnosti, koji također proizlaze iz članaka 15. do 22. GDPR-a, uključujući pravo na pristup osobnim podacima. Učinili smo ove informacije dostupnima na svim jezicima EU i EGP. Verzija na engleskom jeziku odnosi se na Ujedinjeno Kraljevstvo.

Svi subjekti podataka koji privremeno borave u Švicarskoj ili tamo imaju prebivalište ili uobičajeno boravište imaju pravo na prava i prava ispitanika prema švicarskom Zakonu o zaštiti podataka (DPA) i Švicarskoj uredbi o zaštiti podataka (DPR) koji su objavljeni u našoj Transparentnosti Dokument, uključujući pravo na pristup osobnim podacima. Ove smo informacije dali na tri službena jezika Švicarske (njemačkom, talijanskom i francuskom).


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

© All rights reserved by Heiko Maniero.

# SERBIAN: Информације о обради личних података (члан 13, 14 ГДПР)

Поштовани,

Лични подаци сваког појединца који је у уговорном, пред-уговорном или другом односу са нашом компанијом заслужују посебну заштиту. Наш циљ је да одржимо ниво заштите података на високом нивоу. С обзиром на то, рутински развијамо концепте заштите података и сигурности података.

Наравно, поштујемо законске одредбе о заштити података. Према члану 13 и 14 ГДПР, контролори испуњавају специфичне захтеве приликом прикупљања личних података. Овај документ испуњава те обавезе.

Терминологија правних прописа је компликована. Нажалост, употреба правних термина није се могла изоставити у припреми овог документа. Стога, желимо да истакнемо да сте увек добродошли да нас контактирате у вези са свим питањима која се тичу овог документа, коришћеним терминима или формулацијама.

## I. Усклађеност са захтевима за информације када се лични подаци прикупљају од субјекта података (члан 13 ГДПР)

### A. Идентитет и контакт подаци контролора (члан 13 (1) тачка (а) ГДПР)

Види горе

### B. Контакт подаци службеника за заштиту података (члан 13 (1) тачка (б) ГДПР)

Види горе

### C. Сврхе обраде за коју су лични подаци намењени, као и правни основ за обраду (члан 13 (1) тачка (ц) ГДПР)

Сврха обраде личних података је руковање свим операцијама које се тичу контролора, купаца, потенцијалних клијената, пословних партнера или других уговорних или предуговорних односа између наведених група (у најширем смислу) или законских обавеза контролора.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

Члан. 6 (1) тачка (а) ГДПР служи као правни основ за операције обраде за које добијамо сагласност за одређену сврху обраде. Ако је обрада личних података неопходна за извршење уговора у којем је субјекат података једна од страна, као што је случај, на пример, када су операције обраде неопходне за испоруку робе или за пружање било које друге услуге, обрада је заснована на члану 6 (1) тачка (б) ГДПР. Исто се односи и на операције обраде које су неопходне за спровођење предуговорних мера, на пример у случају захтева који се тичу наших производа или услуга. Када је наша компанија подложна законској обавези према којој је потребна обрада личних података, као што је испуњење пореских обавеза, обрада се заснива на члану 6 (1) тачка (ц) ГДПР.

У ретким случајевима, обрада личних података може бити неопходна за заштиту виталних интереса субјекта података или другог физичког лица. То би био случај, на пример, ако би се посетилац повредио у нашој компанији и његово име, године, подаци о здравственом осигурању или друге виталне информације морају бити прослеђене лекару, болници или некој трећој страни. Тада би обрада била заснована на члану 6 (1) тачка (д) ГДПР.

Када је обрада неопходна за обављање задатка који се обавља у јавном интересу или у вршењу службених овлашћења која су дата руковаоцу, правни основ је чл. 6 (1) тачка (е) ГДПР.

Коначно, операције обраде могу се заснивати на члану 6 (1) тачка (ф) ГДПР. Овај правни основ се користи за операције обраде које нису обухваћене ниједним горе наведеним правним основима, ако је обрада неопходна у сврху легитимних интереса које наша компанија или трећа страна настоје остварити, осим ако су такви интереси надјачани интересима или основним правима и слободама субјекта података који захтевају заштиту личних података. Такве операције обраде су изузетно дозвољене јер их је нарочито поменуо европски законодавац. Сматрао је да се легитимни интерес може претпоставити ако је субјект података и клијент контролора (уводна изјава 47, реченица 2 ГДПР).

## D. Када се обрада заснива на члану 6 (1) тачка (ф) ГДПР, легитимни интереси захтевани од контролора или треће стране (члан 13 (1) тачка (д) ГДПР)

Када се обрада личних података заснива на члану 6 (1) тачка (ф) ГДПР, наш легитимни интерес је да обављамо своје пословање у најбољем интересу свих наших запослених и акционара.

## E. Категорије прималаца личних података (члан 13 (1) тачка (е) ГДПР)

Орган јавне власти

Спољни орган

Додатни спољни орган


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

Орган интерне обраде

Орган унутаргрупне обраде

Остала тела

Списак наших обрађивача и прималаца података у трећим земљама и, ако је применљиво, међународним организацијама је објављен на нашој веб страници или се може затражити од нас бесплатно. Молимо контактирајте нашег службеника за заштиту података да бисте затражили ову листу.

## F. Примаоци у трећој земљи и сврсисходни или прикладни заштитни механизми и средства за прибављање њихових копија или њихово стављање на располагање (чланови 13 (1) тачка (ф), 46 (1), 46 (2) тачка (ц) ГДПР)

Све компаније и филијале које су део наше групе (у даљем тексту: Повезане компаније) које имају своје место пословања или канцеларију у трећој земљи могу припадати примаоцима личних података. Од нас се може затражити листа свих повезаних компанија или прималаца.

У складу са чланом 46 (1) ГДПР, контролор или обрађивач могу пренети личне податке трећој земљи само ако је контролор или обрађивач обезбедио одговарајуће заштитне мере и под условом да су субјекту података на располагању његова права и ефикасни правни лекови. Одговарајуће заштитне мере могу се обезбедити без потребе за било каквим посебним овлашћењем од стране надзорног органа путем стандардних уговорних клаузула, члан 46 (2) тачка (ц) ГДПР.

Стандардне уговорне клаузуле Европске уније или друге одговарајуће мере заштите договорене су са свим примаоцима из трећих земаља пре првог преноса личних података. Сходно томе, гарантују се одговарајући заштитни механизми, извршива права субјеката података и ефикасни правни лекови за субјекте података. Сваки субјект података може од нас добити копију стандардних уговорних клаузула. Стандардне уговорне клаузуле су такође доступне у Службеном листу Европске уније.

Члан 45(3) Опште уредбе о заштити података (ГДПР) даје Европској комисији овлашћење да путем имплементационог акта одлучи да земља која није чланица ЕУ обезбеди адекватан ниво заштите. То значи ниво заштите личних података који је у суштини еквивалентан нивоу заштите унутар ЕУ. Ефекат одлука о адекватности је да лични подаци могу слободно тећи из ЕУ (и Норвешке, Лихтенштајна и Исланда) у трећу земљу без даљих препрека. Слична правила постоје за Уједињено Краљевство, Швајцарску и неке друге земље.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

Када је Европска комисија или влада друге земље одлучила да трећа земља обезбеђује адекватан ниво заштите и постоји важећи Оквир (нпр. EU-U.S. Data Privacy Framework, Swiss-U.S. Data Privacy Framework, UK Extension to the EU-U.S. Data Privacy Framework), сви наши трансфери члановима таквих оквира (нпр. самосертификованим ентитетима) се искључиво заснивају на чланству тих ентитета у одговарајућем оквиру. Тамо где смо ми или један од наших групних ентитета члан таквог оквира, сви трансфери нама или нашем групном ентитету искључиво су засновани на чланству ентитета у таквом оквиру.

Сваки субјект података може добити копију оквира од нас. Поред тога, оквири су доступни и у Службеном листу Европске уније или у објављеним правним материјалима или на веб страницама надзорних органа или других надлежних органа или институција.

## G. Временски период у оквиру кога ће се чувати лични подаци, или ако то није могуће одредити, критеријуми који се користе за одређивање тог периода (члан 13 (2) тачка (а) ГДПР)

Критеријум који се користи за одређивање периода чувања личних података је одговарајући период задржавања. Након истека тог периода, одговарајући подаци се рутински бришу, све док више нису потребни за испуњење уговора или започињање уговарања.

Ако не постоји законски рок чувања, критеријум је уговорни или интерни рок задржавања.

## H. Постојање права да се од контролора затражи приступ и исправка или брисање личних података или ограничење обраде у вези са субјектом података или да се уложи приговор на обраду, као и право на преносивост података (члан 13 (2) тачка (б) ГДПР)

Сви субјекти података имају следећа права:

***Право приступа подацима***

Сваки субјекат података има право на приступ личним подацима који се односе на њега или њу. Право на приступ проширује се на све податке које обрађујемо. Право се може остварити лако и у разумним временским интервалима, како би се упознала и проверила законитост обраде (уводна изјава 63 ГДПР). Ово право произлази из чл. 15 ГДПР. Субјект података може нас контактирати да би остварио право приступа.

***Право на исправку података***

Према члану 16, реченица 1 ГДПР, субјект података има право да од контролора, без непотребног одлагања, оствари исправку нетачних личних података који се односе на њега или њу. Штавише, члан 16, реченица 2 ГДПР предвиђа да субјект података има право, узимајући у обзир сврху


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

обраде, да попуни непотпуне личне податке, укључујући и достављање допунске изјаве. Субјект података може да нас контактира да би остварио право на исправку.

***Право на брисање података (право да подаци буду заборављени)***

Додатно, субјекти података имају право на брисање и право да подаци буду заборављени на основу чл. 17 ГДПР. Ово право се такође може остварити контактирањем нас. У овом тренутку, међутим, желимо да истакнемо да се ово право не примењује у случајевима у којима је обрада неопходна да би се испунила законска обавеза која се односи на нашу компанију, члан 17 (3) тачка (б) ГДПР. То значи да можемо одобрити захтев за брисање само након истека законског рока задржавања.

***Право на ограничење обраде података***

Према члану 18 ГДПР, сваки субјект података има право на ограничење обраде података. Ограничење обраде може се тражити ако је један од услова из члана 18 (1) тачка (а) до (д) ГДПР испуњен. Субјект података може нас контактирати да би остварио право на ограничење обраде података.

***Право на приговор***

Надаље, чл. 21 ГДПР гарантује право на приговор. Субјект података може нас контактирати да би остварио право на приговор.

***Право на преносивост података***

Члан 20 ГДПР даје субјекту података право на преносивост података. Према овој одредби, субјекти података под условима из члана 20 (1) тачка (а) и (б) ГДПР имају право да примају личне податке који се односе на њега или њу, које су он или она доставили контролору, у структурираном, уобичајеном и машински читљивом формату и имају право да те податке прослеђују другом контролору без сметњи од стране контролора коме су првобитно дати лични подаци. Субјект података може нас контактирати како би остварио право на преносивост података.

## I. Постојање права да се повуче сагласност у било ком тренутку, без утицаја на законитост обраде на основу сагласности пре њеног повлачења, када се обрада заснива на члану 6 (1) тачка (а) ГДПР или члан 9 (2) тачка (а) ГДПР (члан 13 (2) тачка (ц) ГДПР)

Ако се обрада личних података заснива на чл. 6 (1) тачка (а) ГДПР, што је случај ако је субјект података дао сагласност за обраду личних података за једну или више специфичних сврха или је заснован на члану 9 (2) тачка (а) ГДПР, који регулише изричиту сагласност за обраду посебних категорија личних података, субјект података има право према члану 7 (3) реченица 1 ГДПР да повуче своју сагласност у било које време.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

Повлачење сагласности не утиче на законитост обраде на основу сагласности дате пре њеног повлачења, члан 7 (3) реченица 2 ГДПР. Повући сагласност би требало да буде једнако лако као и дати сагласност, чл. 7 (3) реченица 4 ГДПР. Према томе, повлачење сагласности увек може да се деси на исти начин као што је дат пристанак или на било који други начин, који субјект података сматра једноставнијим. У данашњем информатичком друштву, вероватно најједноставнији начин да се повуче сагласност је путем е-маила. Ако субјект података жели повући свој пристанак дат нама, довољан је да нам пошаље једноставан е-маил. Алтернативно, субјект података може изабрати било који други начин да нам саопшти своје повлачење сагласности.

## J. Право на подношење жалбе надзорном органу (члан 13 (2), тачка (д); члан 77 (1) ГДПР)

Као контролор, дужни смо да обавестимо субјекта података о праву на подношење жалбе надзорном органу, према члану 13 (2), тачка (д) ГДПР. Право на подношење жалбе надзорном органу регулисано је чланом 77 (1) ГДПР. Према овој одредби, пре улагања било којег другог административног или правног лека, сваки субјект података има право да поднесе жалбу надзорном органу, нарочито у држави чланици у којој се налази његово пребивалиште, радно место или место наводног прекршаја, ако субјект података сматра да обрада личних података који се односе на њега или њу крши одредбе ГДПР. Право на подношење жалбе надзорном органу ограничено је само правом Уније на такав начин, да се може остварити само пред једним надзорним органом (уводна изјава 141, реченица 1 ГДПР). Ово правило има за циљ да избегне двоструке жалбе истог субјекта података поводом истог случаја. Стога, ако субјект података жели да уложи жалбу против нас, тражимо да контактира само један надзорни орган.

## K. Давање личних података као законска или уговорна одредба; Услов потребан за склапање уговора; Обавеза субјекта података да достави личне податке; могуће последице непружања таквих података (чл. 13 (2) тачка (е) ГДПР)

Појаснили смо да давање личних података може бити обавезно на основу закона (нпр. Порески прописи) а такође може произаћи из уговорних одредби (нпр. Информације о другој уговорној страни).

Понекад може бити потребно закључити уговор којим нам субјект података даје личне податке, које морамо накнадно обрадити. Субјект података је, на пример, обавезан да нам достави личне податке када наша компанија потписује уговор са њим или њом. Недавање личних података би имало за последицу да се уговор са субјектом података не може закључити.

Пре него што субјект података да личне податке, мора нас контактирати. Ми ћемо објаснити субјекту података да ли је пружање личних података обавезно по закону или уговору или је


© All rights reserved by Heiko Maniero.

неопходно за закључивање уговора, да ли постоји обавеза давања личних података и последице непружања личних података.

### L. Постојање аутоматизованог одлучивања, укључујући профилисање, из члана 22 (1) и (4) ГДПР и, бар у тим случајевима, смислене информације о коришћеној логици, као и значај и предвиђене последице такве обраде за субјекта података (члан 13 (2) тачка (ф) ГДПР)

Као одговорна компанија, обично не користимо аутоматизовано доношење одлука или профилисање. Ако, у изузетним случајевима, извршимо аутоматизовано доношење одлука или профилисање, обавестићемо субјекта података или засебно или путем пододељка у нашој политици приватности (на нашој веб страници). У овом случају важи следеће:

Аутоматско доношење одлука – укључујући и профилисање – може се десити ако (1) је то неопходно за склапање или извршење уговора између субјекта података и нас, или (2) ако је то дозвољено законом Уније или државе чланице на коју ми су предмет и који такође прописује одговарајуће мере за заштиту права и слобода и легитимних интереса субјекта података; или (3) ово се заснива на изричитој сагласности субјекта података.

У случајевима наведеним у члану 22(2) (а) и (ц) ГДПР, ми ћемо применити одговарајуће мере за заштиту права и слобода и легитимних интереса субјекта података. У овим случајевима имате право да добијете људску интервенцију од стране контролора, да изразите своје гледиште и да оспорите одлуку.

Смислене информације о логици која је укључена, као и значај и предвиђене последице такве обраде за субјекта података су наведене у нашој политици приватности.

## II. Усклађеност са захтевима за информације када се лични подаци не прикупљају од субјекта података (члан 14 ГДПР)

### A. Идентитет и контакт подаци контролора (члан 14 (1) тачка (а) ГДПР)

Види горе

### B. Контакт подаци службеника за заштиту података (члан 14 (1) тачка (б) ГДПР)

Види горе


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## C. Сврха обраде за коју су лични подаци намењени, као и правни основ за обраду (члан 14 (1) тачка (ц) ГДПР)

Сврха обраде личних података је руковање свим операцијама које се тичу контролора, клијената, потенцијалних клијената, пословних партнера или других уговорних или предуговорних односа између наведених група (у најширем смислу) или законских обавеза контролора.

Ако је обрада личних података неопходна за извршење уговора у којој је субјекат података једна од уговорних страна, као што је случај, на пример, када су операције обраде неопходне за испоруку робе или за пружање било које друге услуге, обрада је заснована на основу члана 6 (1) тачка (б) ГДПР. Исто се односи и на операције обраде које су неопходне за спровођење предуговорних мера, на пример у случају питања везаних за наше производе или услуге. Када је наша компанија подложна законској обавези по којој је потребна обрада личних података, као што је испуњење пореских обавеза, обрада се заснива на члану 6 (1) тачка (ц) ГДПР.

У ретким случајевима, обрада личних података може бити неопходна за заштиту виталних интереса субјекта података или другог физичког лица. То би био случај, на пример, ако би се посетилац повредио у нашој компанији и његово име, године, подаци о здравственом осигурању или друге виталне информације би морали бити пренети лекару, болници или некој трећој страни. Тада би обрада била заснована на члану 6 (1) тачка (д) ГДПР.

Када је обрада неопходна за обављање задатка који се обавља у јавном интересу или у вршењу службених овлашћења која су дата руковаоцу, правни основ је чл. 6 (1) тачка (е) ГДПР.

Коначно, операције обраде могу се заснивати на члану 6 (1) тачка (ф) ГДПР. Овај правни основ се користи за операције обраде које нису обухваћене ниједним горе наведеним правним основима, ако је обрада неопходна у сврху легитимних интереса које наша компанија или трећа страна настоје остварити, осим ако су такви интереси надјачани интересима или основним правима и слободама субјекта података који захтевају заштиту личних података. Такве операције обраде су изричито дозвољене јер их је нарочито поменуо европски законодавац. Сматрао је да се легитимни интерес може претпоставити ако је субјект података и клијент контролора (уводна изјава 47, реченица 2 ГДПР).

## D. Категорије личних података о којима је реч (члан 14 (1) тачка (д) ГДПР)

Подаци клијената

Подаци потенцијалних клијената

Подаци запослених


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## E. Категорије прималаца личних података (члан 14 (1) тачка (е) ГДПР)

Органи јавне власти

Спољни органи

Додатни спољни органи

Орган унутрашње обраде

Орган унутаргрупне обраде

Остала тела

Списак наших обрађивача и прималаца података у трећим земљама и, ако је применљиво, међународним организацијама је објављен на нашој веб страници или се може затражити од нас бесплатно. Молимо контактирајте нашег службеника за заштиту података да бисте затражили ову листу.

## F. Примаоци у трећој земљи и сврсисходни или прикладни заштитни механизми и средства за њихово прибављање или њихово стављање на располагање (чланови 14 (1) тачка (ф), 46 (1), 46 (2) тачка (ц) ГДПР)

Све компаније и филијале које су део наше групе (у даљем тексту: Повезане компаније) које имају своје место пословања или канцеларију у трећој земљи могу припадати примаоцима личних података. Од нас се може затражити листа свих повезаних компанија или прималаца.

У складу са чланом 46 (1) ГДПР, контролор или обрађивач могу пренети личне податке трећој земљи само ако је контролор или обрађивач обезбедио одговарајуће заштитне мере и под условом да су субјекту података на располагању његова права и ефикасни правни лекови. Одговарајуће заштитне мере могу се обезбедити без потребе за било каквим посебним овлашћењем од стране надзорног органа путем стандардних уговорних клаузула, члан 46 (2) тачка (ц) ГДПР.

Стандардне уговорне клаузуле Европске уније или друге одговарајуће мере заштите договорене су са свим примаоцима из трећих земаља пре првог преноса личних података. Стога, гарантују се одговарајући заштитни механизми, извршива права субјеката података и ефикасни правни лекови за субјекте података. Сваки субјект података може од нас добити копију стандардних уговорних клаузула. Стандардне уговорне клаузуле су такође доступне у Службеном листу Европске уније.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

Члан 45(3) Опште уредбе о заштити података (ГДПР) даје Европској комисији овлашћење да путем имплементационог акта одлучи да земља која није чланица ЕУ обезбеди адекватан ниво заштите. То значи ниво заштите личних података који је у суштини еквивалентан нивоу заштите унутар ЕУ. Ефекат одлука о адекватности је да лични подаци могу слободно тећи из ЕУ (и Норвешке, Лихтенштајна и Исланда) у трећу земљу без даљих препрека. Слична правила постоје за Уједињено Краљевство, Швајцарску и неке друге земље.

Када је Европска комисија или влада друге земље одлучила да трећа земља обезбеђује адекватан ниво заштите и постоји важећи Оквир (нпр. EU-U.S. Data Privacy Framework, Swiss-U.S. Data Privacy Framework, UK Extension to the EU-U.S. Data Privacy Framework), сви наши трансфери члановима таквих оквира (нпр. самосертификованим ентитетима) се искључиво заснивају на чланству тих ентитета у одговарајућем оквиру. Тамо где смо ми или један од наших групних ентитета члан таквог оквира, сви трансфери нама или нашем групном ентитету искључиво су засновани на чланству ентитета у таквом оквиру.

Сваки субјект података може добити копију оквира од нас. Поред тога, оквири су доступни и у Службеном листу Европске уније или у објављеним правним материјалима или на веб страницама надзорних органа или других надлежних органа или институција.

## G. Временски период у оквиру кога ће се чувати лични подаци, или ако то није могуће одредити, критеријуми који се користе за одређивање тог периода (члан 14 (2) тачка (а) ГДПР)

Критеријум који се користи за одређивање периода чувања личних података је одговарајући, законом прописан период задржавања. Након истека тог периода, одговарајући подаци се рутински бришу, под условом да више нису потребни за испуњење уговора или започињање уговарања.

Ако не постоји законски рок чувања, критеријум је уговорни или интерни рок задржавања.

## H. Обавештавање о легитимним интересима које остварује контролор или трећа страна ако се обрада заснива на члану 6 (1) тачка (ф) ГДПР (Чл. 14 (2) тачка (б) ГДПР)

Према члану 6 (1) тачка (ф) ГДПР, обрада ће бити законита само ако је обрада неопходна у сврхе легитимних интереса које остварује контролор или трећа страна, осим ако су ти интереси надјачани интересима или основним правима и слободама субјекта података који захтевају заштиту личних података. Према уводној изјави 47 реченица 2 ГДПР, легитиман интерес може постојати тамо где постоји релевантан и одговарајући однос између субјекта података и контролора, нпр. у ситуацијама када је субјект података клијент контролора. У свим случајевима у


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

којима наша компанија обрађује личне податке на основу члана 6 (1) тачка (ф) ГДПР, наш легитимни интерес је да обављамо наше пословање у најбољем интересу свих наших запослених и акционара.

## I. Постојање права да се од контролора затражи приступ и исправка или брисање личних података или ограничење обраде у вези са субјектом података или да се уложи приговор на обраду, као и право на преносивост података (члан 14 (2) тачка (ц) ГДПР)

Сви субјекти података имају следећа права:

***Право приступа подацима***

Сваки субјект података има право на приступ личним подацима који се односе на њега или њу. Право на приступ проширује се на све податке које обрађујемо. Право се може остварити лако и у разумним временским интервалима, како би се упознали и проверили законитост обраде (уводна изјава 63 ГДПР). Ово право произлази из чл. 15 ГДПР. Субјект података може нас контактирати да би остварио право приступа.

***Право на исправку података***

Према члану 16, реченица 1 ГДПР, субјект података има право да од контролора, без непотребног одлагања, оствари исправку нетачних личних података који се односе на њега или њу. Штавише, члан 16, реченица 2 ГДПР предвиђа да субјект података има право, узимајући у обзир сврху обраде, да попуни непотпуне личне податке, ту укључујући и достављање допунске изјаве. Субјект података може да нас контактира да би остварио право на исправку.

***Право на брисање података (право да подаци буду заборављени)***

Поред тога, субјекти података имају право на брисање и право да подаци буду заборављени на основу чл. 17 ГДПР. Ово право се такође може остварити контактирањем нас. У овом тренутку, међутим, желимо да истакнемо да се ово право не примењује у случајевима у којима је обрада неопходна да би се испунила законска обавеза која се односи на нашу компанију, члан 17 (3) тачка (б) ГДПР. То значи да можемо одобрити захтев за брисање само након истека предвиђеног рока задржавања.

***Право на ограничење обраде података***

Према члану 18 ГДПР, сваки субјект података има право на ограничење обраде података. Ограничење обраде може се тражити ако је један од услова из члана 18 (1) тачка (а) до (д) ГДПР испуњен. Субјект података може нас контактирати да би остварио право на ограничење обраде података.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

***Право на приговор***

Надаље, чл. 21 ГДПР гарантује право на приговор. Субјект података може нас контактирати да би остварио право на приговор.

***Право на преносивост података***

Члан 20 ГДПР даје субјекту података право на преносивост података. Према овој одредби, субјекти података под условима из члана 20 (1) тачка (а) и (б) ГДПР имају право да примају личне податке који се односе на њега или њу, које су он или она доставили контролору, у структурираном, уобичајеном и машински читљивом формату и имају право да те податке прослеђују другом контролору без сметњи од стране контролора коме су већ дати лични подаци. Субјект података може да нас контактира како би остварио право на преносивост података.

## J. Постојање права да се повуче сагласност у било ком тренутку, без утицаја на законитост обраде на основу сагласности пре њеног повлачења, када се обрада заснива на члану 6 (1) тачка (а) ГДПР или члан 9 (2) тачка (а) ГДПР (члан 14 (2) тачка (д) ГДПР)

Ако се обрада личних података заснива на чл. 6 (1) тачка (а) ГДПР, што је случај ако је субјект података дао сагласност за обраду личних података за једну или више специфичних сврха или је заснован на члану 9 (2) тачка (а) ГДПР, који регулише изричиту сагласност за обраду посебних категорија личних података, субјект података има према члану 7 (3) реченица 1 ГДПР право да повуче своју сагласност у било које време.

Повлачење сагласности не утиче на законитост обраде на основу сагласности пре њеног повлачења, члан 7 (3) реченица 2 ГДПР. Требало би бити лако повући сагласност на једноставан начин као што се и даје, чл. 7 (3) реченица 4 ГДПР. Према томе, повлачење сагласности увек може да се деси на исти начин као што је дата или на било који други начин, који субјект података сматра једноставнијим. У данашњем информатичком друштву, вероватно је најједноставнији начин да се повуче сагласност путем е-маила. Ако субјект података жели повући свој пристанак, довољан је једноставан е-маил. Алтернативно, субјект података може изабрати било који други начин да нам саопшти своје повлачење сагласности.

## K. Право на подношење жалбе надзорном органу (члан 14 (2), тачка (е); члан 77 (1) ГДПР)

Као контролор, дужни смо да обавестимо субјекта података о праву на подношење жалбе надзорном органу, члан 14 (2), тачка (е) ГДПР. Право на подношење жалбе надзорном органу регулисано је чланом 77 (1) ГДПР. Према овој одредби, без претходног улагања било ког другог административног или правног лека, сваки субјект података има право да поднесе жалбу надзорном органу, посебно у држави чланици у којој се налази његово пребивалиште, радно место


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

или место наводног прекршаја, ако субјект података сматра да обрада личних података који се односе на њега или њу крши одредбе ГДПР. Право на подношење жалбе надзорном органу ограничено је само правом Уније на такав начин, да се може остварити само пред једним надзорним органом (уводна изјава 141, реченица 1 ГДПР). Ово правило има за циљ да се избегну двоструке жалбе истог субјекта података у истом предмету. Стога, ако субјект података жели да уложи жалбу против нас, тражимо да контактира само један надзорни орган.

## L. Извор личних података, и ако је примењиво, да ли долазе из јавно доступних извора (члан 14 (2) тачка (ф) ГДПР)

У принципу, лични подаци се прикупљају директно од субјекта података или у сарадњи са органом (нпр. Проналажење података из званичног регистра). Остали подаци о субјектима података су изведени из трансфера групе компанија. У контексту ове опште информације, именовање тачних извора из којих су лични подаци проистекли или је немогуће или би укључивало несразмерне напоре у смислу чл. 14 (5) тачка (б) ГДПР. У принципу, ми не прикупљамо личне податке из јавно доступних извора.

Сваки субјект података може нас контактирати у било које време како би добио детаљније информације о тачним изворима личних података који га се тичу. Када се порекло личних података не може предочити субјекту података јер су коришћени различити извори, треба дати опште информације (уводна изјава 61, реченица 4 ГДПР).

## M. Постојање аутоматизованог одлучивања, укључујући профилисање, из члана 22 (1) и (4) ГДПР и, бар у тим случајевима, смислене информације о томе о којој је логици реч, као и значај и предвиђених последица такве обраде за субјекта података (члан 14 (2) тачка (г) ГДПР)

Као одговорна компанија, обично не користимо аутоматизовано доношење одлука или профилисање. Ако, у изузетним случајевима, извршимо аутоматизовано доношење одлука или профилисање, обавестићемо субјекта података или засебно или путем пододељака у нашој политици приватности (на нашој веб страници). У овом случају важи следеће:

Аутоматско доношење одлука – укључујући и профилисање – може се десити ако (1) је то неопходно за склапање или извршење уговора између субјекта података и нас, или (2) ако је то дозвољено законом Уније или државе чланице на коју ми су предмет и који такође прописује одговарајуће мере за заштиту права и слобода и легитимних интереса субјекта података; или (3) ово се заснива на изричитој сагласности субјекта података.

У случајевима наведеним у члану 22(2) (а) и (ц) ГДПР, ми ћемо применити одговарајуће мере за заштиту права и слобода и легитимних интереса субјекта података. У овим случајевима имате


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

право да добијете људску интервенцију од стране контролора, да изразите своје гледиште и да оспорите одлуку.

Смислене информације о логици која је укључена, као и значај и предвиђене последице такве обраде за субјекта података су наведене у нашој политици приватности.

## III. EU-U.S. Data Privacy Framework (EU-U.S. DPF), UK Extension to the EU-U.S. DPF, Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF)

Ako je naša organizacija sertifikovani član EU-U.S. Data Privacy Framework (EU-U.S. DPF) i/ili UK Extension to the EU-U.S. DPF i/ili Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF), važi sledeće:

Mi se pridržavamo EU-U.S. Data Privacy Framework (EU-U.S. DPF) i UK Extension to the EU-U.S. DPF, kao i Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF), kako je određeno od strane U.S. Department of Commerce. Naša kompanija je potvrdila Ministarstvu trgovine SAD-a da se pridržava EU-U.S. Data Privacy Framework Principles (EU-U.S. DPF Principles) u vezi sa obradom ličnih podataka koje prima iz Evropske unije i Ujedinjenog Kraljevstva pozivajući se na EU-U.S. DPF i UK Extension to the EU-U.S. DPF. Naša kompanija je potvrdila Ministarstvu trgovine SAD-a da se pridržava Swiss-U.S. Data Privacy Framework Principles (Swiss-U.S. DPF Principles) u vezi sa obradom ličnih podataka koje prima iz Švajcarske pozivajući se na Swiss-U.S. DPF. U slučaju sukoba između odredbi naše politike privatnosti i EU-U.S. DPF Principles i/ili Swiss-U.S. DPF Principles, Principles su merodavne.

Za više informacija o Data Privacy Framework (DPF) programu i za pregled naše sertifikacije, posetite https://www.dataprivacyframework.gov/.

Ostale američke jedinice ili američke podružnice naše kompanije, koje se takođe pridržavaju EU-U.S. DPF Principles, uključujući UK Extension to the EU-U.S. DPF i Swiss-U.S. DPF Principles, ako postoje, navedene su u našoj politici privatnosti.

U skladu sa EU-U.S. DPF i UK Extension to the EU-U.S. DPF, kao i Swiss-U.S. DPF, naša kompanija se obavezuje da sarađuje sa telom koje su osnovale evropske nadzorne vlasti za zaštitu podataka i britanski Information Commissioner's Office (ICO), kao i sa švajcarskim Federal Data Protection and Information Commissioner (EDÖB), te da prati njihove savete u vezi sa nerešenim pritužbama o našem rukovanju ličnim podacima koje primamo pozivajući se na EU-U.S. DPF i UK Extension to the EU-U.S. DPF i Swiss-U.S. DPF.

Obaveštavamo pogođene osobe o nadležnim evropskim telima za zaštitu podataka koja su odgovorna za rešavanje pritužbi u vezi sa rukovanjem ličnim podacima naše organizacije u gornjem delu ovog transparentnog dokumenta te da pogođenim osobama pružamo odgovarajuće i besplatno pravno sredstvo.


© All rights reserved by Heiko Maniero.

Obaveštavamo sve pogođene osobe da naša kompanija podleže istražnim i izvršnim ovlašćenjima Federal Trade Commission (FTC).

Pogođene osobe imaju pravo, pod određenim uslovima, da zatraže obavezujuću arbitražu. Naša organizacija je obavezna da reši zahteve i pridržava se uslova prema Aneksu I DPF-Principles, ako je pogođena osoba zatražila obavezujuću arbitražu tako što je obavestila našu organizaciju i pridržavala se postupaka i uslova prema Aneksu I Principles.

Ovim obaveštavamo sve pogođene osobe o odgovornosti naše organizacije u slučaju prenosa ličnih podataka trećim stranama.

Za pitanja pogođenih osoba ili tela za zaštitu podataka imenovali smo lokalne predstavnike navedene u gornjem delu ovog transparentnog dokumenta.

Pružamo vam mogućnost izbora (Opt-out) da li želite da vaši lični podaci (i) budu prosleđeni trećim stranama ili (ii) korišćeni u svrhu koja se bitno razlikuje od one za koju su izvorno prikupljeni ili koju ste kasnije odobrili. Jasan, vidljiv i lako dostupan mehanizam za ostvarivanje vašeg prava izbora je kontaktiranje našeg službenika za zaštitu podataka (DSB) putem e-pošte. Nemate mogućnost izbora i nismo obavezni to učiniti ako se podaci prosleđuju trećoj strani koja deluje kao agent ili obrađivač podataka u naše ime i prema našim uputama. Međutim, uvek sklapamo ugovor sa takvim agentom ili obrađivačem podataka.

Za osetljive podatke (tj. lične podatke koji sadrže informacije o zdravstvenom stanju, rasnom ili etničkom poreklu, političkim mišljenjima, verskim ili filozofskim uverenjima, članstvu u sindikatu ili informacije o seksualnom životu pogođene osobe) tražimo vašu izričitu saglasnost (Opt-in) kada se ti podaci (i) prosleđuju trećim stranama ili (ii) koriste u svrhu koja se razlikuje od one za koju su izvorno prikupljeni ili za koju ste kasnije dali svoju saglasnost odabirom Opt-in. Osim toga, sve lične podatke koje primimo od trećih strana tretiramo kao osetljive ako ih treća strana identifikuje i tretira kao osetljive.

Ovim vas obaveštavamo o potrebi otkrivanja ličnih podataka kao odgovor na zakonite zahteve vlasti, uključujući ispunjavanje zahteva za nacionalnu bezbednost ili sprovođenje zakona.

Prilikom prenosa ličnih podataka trećoj strani koja deluje kao rukovalac obrade, pridržavamo se Principals obaveštavanja i izbora. Takođe sklapamo ugovor sa trećom stranom koja je odgovorna za obradu, koji predviđa da se ti podaci smeju obrađivati samo za ograničene i određene svrhe u skladu sa vašom danom saglasnošću i da primalac pruža isti nivo zaštite kao Principals DPF te nas obaveštava ako utvrdi da više ne može ispunjavati tu obavezu. Ugovor predviđa da treća strana, koja je rukovalac obrade, prekine obradu ili preduzme druge odgovarajuće i prikladne mere kako bi se otklonio problem kada se takva situacija utvrdi.

Prilikom prenosa ličnih podataka trećoj strani koja deluje kao agent ili obrađivač podataka (i) prenosimo te podatke samo za ograničene i određene svrhe; (ii) uveravamo se da je agent ili obrađivač podataka obavezan da obezbedi najmanje isti nivo zaštite podataka kao što to zahtevaju DPF-Principles; (iii) preduzimamo odgovarajuće i prikladne mere kako bismo osigurali da agent ili obrađivač podataka stvarno


© All rights reserved by Heiko Maniero.

обрађује пренете личне податке на начин који је у складу са нашим обавезама према DPF-Principles; (iv) захтевамо од агента или обрађивача података да обавести нашу организацију ако утврди да више не може испуњавати обавезу пружања истог нивоа заштите као што то предвиђају DPF-Principles; (v) након обавештења, укључујући оно под (iv), предузимамо одговарајуће и прикладне кораке како бисмо зауставили неовлашћену обраду и отклонили проблем; и (vi) DPF Departmentu на захтев пружамо сажетак или репрезентативни примерак релевантних одредби уговора о заштити података са тим агентом.

U skladu sa EU-U.S. DPF i/ili UK Extension to the EU-U.S. DPF i/ili Swiss-U.S. DPF, naša organizacija se obavezuje da sarađuje sa telom koje su osnovale evropske nadzorne vlasti za zaštitu podataka i britanski Information Commissioner's Office (ICO), odnosno sa švajcarskim Federal Data Protection and Information Commissioner (EDÖB), te da prati njihove savete u vezi sa nerešenim pritužbama o našem rukovanju ličnim podacima u vezi sa radnim odnosom koje primamo pozivajući se na EU-U.S. DPF i UK Extension to the EU-U.S. DPF i Swiss-U.S. DPF.

Сви субјекти података који се привремено налазе у Европској унији (ЕУ), Европском економском простору (ЕЕА) или Уједињеном Краљевству, или који тамо имају пребивалиште или уобичајено боравиште, имају право на права и права носилаца података која су објављена у нашем Транспарентност документа, који такође произилазе из чланова 15 до 22 ГДПР, укључујући право на приступ личним подацима. Ове информације смо учинили доступним на свим језицима ЕУ и ЕЕА. Верзија на енглеском језику важи за Уједињено Краљевство.

Сви субјекти података који имају привремени боравак у Швајцарској или имају пребивалиште или уобичајено боравиште тамо имају право на права и права носилаца података према Швајцарском закону о заштити података (ДПА) и Швајцарској уредби о заштити података (ДПР) који су објављени у нашој Транспарентности Документ, укључујући право на приступ личним подацима. Ову информацију смо дали на три званична језика Швајцарске (немачки, италијански и француски).


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

# SERBIAN: Информације о обради личних података за запослене и подносиоце захтева (члан 13, 14 ГДПР)

Поштовани,

Лични подаци запослених и подносиоца захтева заслужују посебну заштиту. Наш циљ је да одржимо ниво заштите података на високом нивоу. Стога рутински развијамо концепт заштите података и сигурности података.

Наравно, поштујемо законске одредбе о заштити података. Према члану 13, 14 ГДПР, контролори испуњавају специфичне захтеве приликом прикупљања личних података. Овај документ испуњава те обавезе.

Терминологија правних прописа је компликована. Нажалост, употреба правних термина није се могла изоставити у припреми овог документа. Стога, желимо да истакнемо да сте увек добродошли да нас контактирате у вези свих питања која се тичу овог документа, коришћених термина или формулација.

## I. Усклађеност са захтевима за информације када се лични подаци прикупљају од субјекта података (члан 13 ГДПР)

### A. Идентитет и контакт подаци контролора (члан 13 (1) тачка (а) ГДПР)

Види горе

### B. Контакт подаци службеника за заштиту података (члан 13 (1) тачка (б) ГДПР)

Види горе

### C. Сврха обраде за коју су лични подаци намењени, као и правни основ за обраду (члан 13 (1) тачка (ц) ГДПР)

За податке подносиоца пријаве, сврха обраде података је да се спроведе испитивање пријаве током процеса регрутације. У ту сврху обрађујемо све податке које сте нам доставили. На основу података достављених током процеса регрутације, ми ћемо проверити да ли сте позвани на интервју за посао (део процеса селекције). У случају генерално прикладних кандидата, посебно у контексту интервјуа за посао, обрађујемо неке друге личне податке које сте нам доставили, што је


Powered by ICB International Certification Body. © All rights reserved by Heiko Maniero.

од суштинске важности за нашу одлуку о одабиру. Ако вас запослимо, подаци о подносиоцима захтева ће се аутоматски променити у податке о запосленима. Као део процеса регрутације, ми ћемо обрадити друге личне податке о вама које тражимо од вас и које су потребни за склапање или испуњење вашег уговора (као што су лични идентификациони бројеви или порески бројеви). За податке о запосленима, сврха обраде података је извршење уговора о раду или поштовање других законских одредби које се односе на радни однос (нпр. Порески закон), као и коришћење ваших личних података за испуњавање уговора о раду закљученог с вама (нпр. објављивање вашег имена и контактне информације унутар компаније или клијентима).

Подаци о запосленима чувају се након престанка радног односа ради испуњења законског периода задржавања.

Правна основа за обраду података је члан 6 (1) тачка (б) ГДПР, члан 9 (2) тачке (б) и (х) ГДПР, члан 88 (1) ГДПР и национално законодавство, као што је за Немачку Одељак 26 БДСГ (Савезни закон о заштити података).

## D. Категорије примаоца личних података (члан 13 (1) тачка (е) ГДПР)

Орган јавне власти

Спољни орган

Додатни спољни орган

Орган интерне обраде

Орган међугрупне обраде

Остала тела

Списак наших обрађивача и прималаца података у трећим земљама и, ако је применљиво, међународним организацијама је објављен на нашој веб страници или се може затражити од нас бесплатно. Молимо контактирајте нашег службеника за заштиту података да бисте затражили ову листу.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## E. Примаоци у трећој земљи и сврсисходни или прикладни заштитни механизми и средства за њихово прибављање или њихово стављање на располагање (чланови 13 (1) тачка (ф), 46 (1), 46 (2) тачка (ц) ГДПР)

Све компаније и филијале које су део наше групе (у даљем тексту: Повезане компаније) које имају своје место пословања или канцеларију у трећој земљи могу припадати примаоцима личних података. Од нас се може затражити листа свих повезаних компанија или прималаца.

У складу са чланом 46 (1) ГДПР, контролор или обрађивач могу пренети личне податке трећој земљи само ако је контролор или обрађивач обезбедио одговарајуће заштитне мере и под условом да су субјекту података на располагању његова права и ефикасни правни лекови. Одговарајуће заштитне мере могу се обезбедити без потребе за било каквим посебним овлашћењем од стране надзорног органа путем стандардних уговорних клаузула, члан 46 (2) тачка (ц) ГДПР.

Стандардне уговорне клаузуле Европске уније или друге одговарајуће мере заштите договорене су са свим примаоцима из трећих земаља пре првог преноса личних података. Сходно томе, гарантују се одговарајући заштитни механизми, извршива права субјеката података и ефикасни правни лекови за субјекте података. Сваки субјект података може од нас добити копију стандардних уговорних клаузула. Стандардне уговорне клаузуле су такође доступне у Службеном листу Европске уније.

Члан 45(3) Опште уредбе о заштити података (ГДПР) даје Европској комисији овлашћење да путем имплементационог акта одлучи да земља која није чланица ЕУ обезбеди адекватан ниво заштите. То значи ниво заштите личних података који је у суштини еквивалентан нивоу заштите унутар ЕУ. Ефекат одлука о адекватности је да лични подаци могу слободно тећи из ЕУ (и Норвешке, Лихтенштајна и Исланда) у трећу земљу без даљих препрека. Слична правила постоје за Уједињено Краљевство, Швајцарску и неке друге земље.

Када је Европска комисија или влада друге земље одлучила да трећа земља обезбеђује адекватан ниво заштите и постоји важећи Оквир (нпр. EU-U.S. Data Privacy Framework, Swiss-U.S. Data Privacy Framework, UK Extension to the EU-U.S. Data Privacy Framework), сви наши трансфери чланови таквих оквира (нпр. самосертификованим ентитетима) се искључиво заснивају на чланству тих ентитета у одговарајућем оквиру. Тамо где смо ми или један од наших групних ентитета члан таквог оквира, сви трансфери нама или нашем групном ентитету искључиво су засновани на чланству ентитета у таквом оквиру.

Сваки субјект података може добити копију оквира од нас. Поред тога, оквири су доступни и у Службеном листу Европске уније или у објављеним правним материјалима или на веб страницама надзорних органа или других надлежних органа или институција.


© All rights reserved by Heiko Maniero.

## F. Период у којем ће се чувати лични подаци, или ако то није могуће, критеријуме који се користе за одређивање тог периода (члан 13(2) тачка А ГДПР)

Период чувања личних података кандидата је 6 месеци. За податке о запосленима примењује се односни период задржавања. Након истека тог периода, одговарајући подаци се рутински бришу, све док више нису потребни за испуњење уговора или покретање уговора.

## G. Постојање права да се од контролора затражи приступ и исправка или брисање личних података или ограничење обраде у вези са субјектом података или да се уложи приговор на обраду, као и право на преносивост података (члан 13 (2) тачка (б) ГДПР)

Сви субјекти података имају следећа права:

***Право приступа***

Сваки субјект података има право на приступ личним подацима који се односе на њега или њу. Право на приступ проширује се на све податке које обрађујемо. Право се може остварити лако и у разумним временским интервалима, како би се упознали и проверили законитост обраде (уводна изјава 63 ГДПР). Ово право произлази из чл. 15 ГДПР. Субјект података може нас контактирати да би остварио право приступа.

***Право на исправку***

Према члану 16, реченица 1 ГДПР, субјект података има право да од контролора, без непотребног одлагања, оствари исправку нетачних личних података који се односе на њега или њу. Штавише, члан 16, реченица 2 ГДПР предвиђа да субјект података има право, узимајући у обзир сврху обраде, да допуни непотпуне личне податке, укључујући и достављање допунске изјаве. Субјект података може да нас контактира да би остварио право на исправку.

***Право на брисање (право да подаци буду заборављени)***

Поред тога, субјекти података имају право на брисање и право да подаци буду заборављени на основу чл. 17 ГДПР. Ово право се такође може остварити контактирањем нас. У овом тренутку, међутим, желимо да истакнемо да се ово право не примењује у случајевима у којима је обрада неопходна да би се испунила законска обавеза која се односи на нашу компанију, члан 17 (3) тачка (б) ГДПР. То значи да можемо одобрити захтев за брисање само након истека законског рока задржавања.

***Право на ограничење обраде података***

Према члану 18 ГДПР, сваки субјект података има право на ограничење обраде података. Ограничење обраде може се тражити ако је један од услова из члана 18 (1) тачка (а) до (д) ГДПР


© All rights reserved by Heiko Maniero.

испуњен. Субјект података може нас контактирати да би остварио право на ограничење обраде података.

***Право на приговор***

Надаље, чл. 21 ГДПР гарантује право на приговор. Субјект података може нас контактирати да би остварио право на приговор.

***Право на преносивост података***

Члан 20 ГДПР даје субјекту података право на преносивост података. Према овој одредби, субјекти података под условима из члана 20 (1) тачка (а) и (б) ГДПР имају право да примају личне податке који се односе на њега или њу, које су он или она доставили контролору, у структурираном, уобичајеном и машински читљивом формату и имају право да те податке прослеђују другом контролору без сметњи од стране контролора коме су већ дати лични подаци. Субјект података може да нас контактира како би остварио право на преносивост података.

## H. Постојање права да се повуче сагласност у било ком тренутку, без утицаја на законитост обраде на основу сагласности пре њеног повлачења, када се обрада заснива на члану 6 (1) тачка (а) ГДПР или члан 9 (2) тачка (а) ГДПР (члан 14 (2) тачка (д) ГДПР)

Ако се обрада личних података заснива на чл. 6 (1) тачка (а) ГДПР, што је случај ако је субјект података дао сагласност за обраду личних података за једну или више специфичних сврха или је заснован на члану 9 (2) тачка (а) ГДПР, који регулише изричиту сагласност за обраду посебних категорија личних података, субјект података има према члану 7 (3) реченица 1 ГДПР право да повуче своју сагласност у било које време.

Повлачење сагласности не утиче на законитост обраде на основу сагласности дате пре њеног повлачења, члан 7 (3) реченица 2 ГДПР. Требало би бити лако повући сагласност на једноставан начин као што се и даје, чл. 7 (3) реченица 4 ГДПР. Према томе, повлачење сагласности увек може да се деси на исти начин као што је дата или на било који други начин, који субјект података сматра једноставнијим. У данашњем информатичком друштву, вероватно је најједноставнији начин да се повуче сагласност путем е-маила. Ако субјект података жели повући свој пристанак који нам је претходно дат, довољан је једноставан е-маил. Алтернативно, субјект података може изабрати било који други начин да нам саопшти своје повлачење сагласности.

## I. Право на подношење жалбе надзорном органу (члан 13 (2), тачка (д); члан 77 (1) ГДПР)

Као контролор, дужни смо да обавестимо субјекта података о праву на подношење жалбе надзорном органу, члан 13 (2), тачка (д) ГДПР. Право на подношење жалбе надзорном органу


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

регулисано је чланом 77 (1) ГДПР. Према овој одредби, пре улагања било ког другог административног или правног лека, сваки субјект података има право да поднесе жалбу надзорном органу, нарочито у држави чланици у којој се налази његово или њено пребивалиште, радно место или место наводног прекршаја, ако субјект података сматра да обрада личних података који се односе на њега или њу крши одредбе ГДПР. Право на подношење жалбе надзорном органу ограничено је само правом Уније на такав начин, да се може остварити само пред једним надзорним органом (уводна изјава 141, реченица 1 ГДПР). Ово правило има за циљ да избегне двоструке жалбе истог субјекта података у истом предмету. Стога, ако субјект података жели да уложи жалбу против нас, тражимо да контактира само један надзорни орган.

## J. Пружање личних података као законских или уговорних захтева; Потреба за склапање уговора; Обавеза субјекта података да достави личне податке; могуће последице не пружања таквих података (члан 13, тачка (е) ГДПР)

Појаснили смо да је давање личних података делимично обавезно по закону (нпр. Порески прописи) или може бити резултат уговорних одредби (нпр. Информације о уговорном партнеру).

Понекад може бити потребно закључити уговор којим нам субјект података даје личне податке, које морамо накнадно обрадити. Субјект података је, на пример, обавезан да нам достави личне податке када наша компанија потпише уговор са њим или њом. Непружање личних података имало би за последицу да се уговор са субјектом података не може закључити.

Пре него што субјект података да личне податке, субјект података мора нас контактирати. Објаснићемо субјекту података да ли је пружање личних података обавезно по закону или уговору или је неопходно за закључивање уговора, да ли постоји обавеза давања личних података и последица непружања личних података.

## K. Постојање аутоматизованог одлучивања, укључујући профилисање, из члана 22 (1) и (4) ГДПР и, бар у тим случајевима, значајне информације о томе о којој је логици реч, као и значај и предвиђених последица такве обраде за субјекта података (члан 13 (2) тачка (ф) ГДПР)

Као одговорна компанија, обично не користимо аутоматизовано доношење одлука или профилисање. Ако, у изузетним случајевима, извршимо аутоматизовано доношење одлука или профилисање, обавестићемо субјекта података или засебно или путем пододељка у нашој политици приватности (на нашој веб страници). У овом случају важи следеће:

Аутоматско доношење одлука – укључујући и профилисање – може се десити ако (1) је то неопходно за склапање или извршење уговора између субјекта података и нас, или (2) ако је то дозвољено законом Уније или државе чланице на коју ми су предмет и који такође прописује


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

одговарајуће мере за заштиту права и слобода и легитимних интереса субјекта података; или (3) ово се заснива на изричитој сагласности субјекта података.

У случајевима наведеним у члану 22(2) (а) и (ц) ГДПР, ми ћемо применити одговарајуће мере за заштиту права и слобода и легитимних интереса субјекта података. У овим случајевима имате право да добијете људску интервенцију од стране контролора, да изразите своје гледиште и да оспорите одлуку.

Смислене информације о логици која је укључена, као и значај и предвиђене последице такве обраде за субјекта података су наведене у нашој политици приватности.

## II. Усклађеност са захтевима за информације када се лични подаци не прикупљају од субјекта података (члан 14 ГДПР)

### A. Идентитет и контакт подаци контролора (члан 14 (1) тачка (а) ГДПР)

Види горе

### B. Контакт подаци службеника за заштиту података (члан 14 (1) тачка (б) ГДПР)

Види горе

### C. Сврха обраде за коју су лични подаци намењени, као и правни основ за обраду (члан 14 (1) тачка (ц) ГДПР)

За податке подносиоца захтјева који нису прикупљени од субјекта података, сврха обраде података је да се спроведе испитивање пријаве током процеса регрутације. У ту сврху можемо обрађивати податке који нису прикупљени од вас. На основу података достављених током процеса регрутације, ми ћемо проверити да ли сте позвани на интервју за посао (део процеса селекције). Ако вас запослимо, подаци о подносиоцима захтева ће се аутоматски променити у податке о запосленима. За податке о запосленима, сврха обраде података је извршење уговора о раду или поштовање других законских одредби које се односе на радни однос. Подаци о запосленима чувају се након престанка радног односа ради испуњења законског периода задржавања.

Правна основа за обраду података је члан 6 (1) тачка (б) и (ф) ГДПР, члан 9 (2) тачке (б) и (х) ГДПР, члан 88 (1) ГДПР и национално законодавство, као што је за Немачку Одељак 26 БДСГ (Савезни закон о заштити података).


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## D. Категорије личних података о којима је реч (члан 14 (1) тачка (д) ГДПР)

Подаци подносиоца захтева

Подаци о запосленима

## E. Категорије примаоца личних података (члан 14 (1) тачка (е) ГДПР)

Орган јавне власти

Спољни орган

Додатни спољни орган

Орган интерне обраде

Орган међугрупне обраде

Остала тела

Списак наших обрађивача и прималаца података у трећим земљама и, ако је применљиво, међународним организацијама је објављен на нашој веб страници или се може затражити од нас бесплатно. Молимо контактирајте нашег службеника за заштиту података да бисте затражили ову листу.

## F. Примаоци у трећој земљи и сврсисходни или прикладни заштитни механизми и средства за њихово прибављање или њихово стављање на располагање (чланови 14 (1) тачка (ф), 46 (1), 46 (2) тачка (ц) ГДПР)

Све компаније и филијале које су део наше групе (у даљем тексту: Повезане компаније) које имају своје место пословања или канцеларију у трећој земљи могу припадати примаоцима личних података. Од нас се може затражити листа свих повезаних компанија или прималаца.

У складу са чланом 46 (1) ГДПР, контролор или обрађивач могу пренети личне податке трећој земљи само ако је контролор или обрађивач обезбедио одговарајуће заштитне мере и под условом да су субјекту података на располагању његова права и ефикасни правни лекови. Одговарајуће заштитне мере могу се обезбедити без потребе за било каквим посебним овлашћењем од стране надзорног органа путем стандардних клаузула за заштиту података, члан 46 (2) тачка (ц) ГДПР.


© All rights reserved by Heiko Maniero.

Стандардне уговорне клаузуле Европске уније или друге одговарајуће мере заштите договорене су са свим примаоцима из трећих земаља пре првог преноса личних података. Сходно томе, гарантују се одговарајући заштитни механизми, извршива права субјеката података и ефикасни правни лекови за субјекте података. Сваки субјект података може од нас добити копију стандардних уговорних клаузула. Стандардне уговорне клаузуле су такође доступне у Службеном листу Европске уније.

Члан 45(3) Опште уредбе о заштити података (ГДПР) даје Европској комисији овлашћење да путем имплементационог акта одлучи да земља која није чланица ЕУ обезбеди адекватан ниво заштите. То значи ниво заштите личних података који је у суштини еквивалентан нивоу заштите унутар ЕУ. Ефекат одлука о адекватности је да лични подаци могу слободно тећи из ЕУ (и Норвешке, Лихтенштајна и Исланда) у трећу земљу без даљих препрека. Слична правила постоје за Уједињено Краљевство, Швајцарску и неке друге земље.

Када је Европска комисија или влада друге земље одлучила да трећа земља обезбеђује адекватан ниво заштите и постоји важећи Оквир (нпр. EU-U.S. Data Privacy Framework, Swiss-U.S. Data Privacy Framework, UK Extension to the EU-U.S. Data Privacy Framework), сви наши трансфери члановима таквих оквира (нпр. самосертификованим ентитетима) се искључиво заснивају на чланству тих ентитета у одговарајућем оквиру. Тамо где смо ми или један од наших групних ентитета члан таквог оквира, сви трансфери нама или нашем групном ентитету искључиво су засновани на чланству ентитета у таквом оквиру.

Сваки субјект података може добити копију оквира од нас. Поред тога, оквири су доступни и у Службеном листу Европске уније или у објављеним правним материјалима или на веб страницама надзорних органа или других надлежних органа или институција.

## G. Временски период у оквиру кога ће се чувати лични подаци, или ако то није могуће одредити, критеријуми који се користе за одређивање тог периода (члан 14 (2) тачка (а) ГДПР)

Рок чувања личних података кандидата је 6 месеци. За податке о запосленима примењује се прописани период задржавања. Након истека тог периода, одговарајући подаци се рутински бришу, под условом да више нису потребни за испуњење уговора или започињање уговарања.

## H. Обавештавање о легитимним интересима које остварује контролор или трећа страна ако се обрада заснива на члану 6 (1) тачка (ф) ГДПР (Чл. 14 (2) тачка (б) ГДПР)

Према члану 6 (1) тачка (ф) ГДПР, обрада ће бити законита само ако је обрада неопходна у сврхе легитимних интереса које остварује контролор или трећа страна, изузев ако су ти интереси


© All rights reserved by Heiko Maniero.

надјачани интересима или основним правима и слободама субјекта података који захтевају заштиту личних података. Према уводној изјави 47 реченица 2 ГДПР, легитиман интерес може постојати тамо где постоји релевантан и одговарајући однос између субјекта података и контролора, нпр. у ситуацијама када је субјект података клијент контролора. У свим случајевима у којима наша компанија обрађује податке подносиоца пријаве на основу члана 6 (1) тачка (ф) ГДПР, наш легитимни интерес је запошљавање одговарајућег особља и професионалаца.

## I. Постојање права да се од контролора затражи приступ и исправка или брисање личних података или ограничење обраде у вези са субјектом података или да се уложи приговор на обраду, као и право на преносивост података (члан 14 (2) тачка (ц) ГДПР)

Сви субјекти података имају следећа права:

***Право приступа подацима***

Сваки субјект података има право на приступ личним подацима који се односе на њега или њу. Право на приступ проширује се на све податке које обрађујемо. Право се може остварити лако и у разумним временским интервалима, како би се упознали и проверили законитост обраде (уводна изјава 63 ГДПР). Ово право произлази из чл. 15 ГДПР. Субјект података може нас контактирати да би остварио право приступа.

***Право на исправку података***

Према члану 16, реченица 1 ГДПР, субјект података има право да од контролора, без непотребног одлагања, оствари исправку нетачних личних података који се односе на њега или њу. Штавише, члан 16, реченица 2 ГДПР предвиђа да субјект података има право, узимајући у обзир сврху обраде, да попуни непотпуне личне податке, ту укључујући и достављање допунске изјаве. Субјект података може да нас контактира да би остварио право на исправку.

***Право на брисање података (право да подаци буду заборављени)***

Поред тога, субјекти података имају право на брисање и право да подаци буду заборављени на основу чл. 17 ГДПР. Ово право се такође може остварити контактирањем нас. У овом тренутку, међутим, желимо да истакнемо да се ово право не примењује у случајевима у којима је обрада неопходна да би се испунила законска обавеза која се односи на нашу компанију, члан 17 (3) тачка (б) ГДПР. То значи да можемо одобрити захтев за брисање само након истека законског рока задржавања.

***Право на ограничење обраде података***

Према члану 18 ГДПР, сваки субјект података има право на ограничење обраде података. Ограничење обраде може се тражити ако је један од услова из члана 18 (1) тачка (а) до (д) ГДПР испуњен. Субјект података може нас контактирати да би остварио право на ограничење обраде података.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

***Право на приговор***

Надаље, чл. 21 ГДПР гарантује право на приговор. Субјект података може нас контактирати да би остварио право на приговор.

***Право на преносивост података***

Члан 20 ГДПР даје субјекту података право на преносивост података. Према овој одредби, субјекти података под условима из члана 20 (1) тачка (а) и (б) ГДПР имају право да примају личне податке који се односе на њега или њу, које су он или она доставили контролору, у структурираном, уобичајеном и машински читљивом формату и имају право да те податке прослеђују другом контролору без сметњи од стране контролора коме су првобитно дати лични подаци. Субјект података може да нас контактира како би остварио право на преносивост података.

## J. Постојање права да се повуче сагласност у било ком тренутку, без утицаја на законитост обраде на основу сагласности пре њеног повлачења, када се обрада заснива на члану 6 (1) тачка (а) ГДПР или члан 9 (2) тачка (а) ГДПР (члан 14 (2) тачка (д) ГДПР)

Ако се обрада личних података заснива на чл. 6 (1) тачка (а) ГДПР, што је случај ако је субјект података дао сагласност за обраду личних података за једну или више специфичних сврха или је заснован на члану 9 (2) тачка (а) ГДПР, који регулише изричиту сагласност за обраду посебних категорија личних података, субјект података има према члану 7 (3) реченица 1 ГДПР право да повуче своју сагласност у било које време.

Повлачење сагласности не утиче на законитост обраде на основу сагласности дате пре њеног повлачења, члан 7 (3) реченица 2 ГДПР. Требало би бити лако повући сагласност на једноставан начин као што се и даје, чл. 7 (3) реченица 4 ГДПР. Према томе, повлачење сагласности увек може да се деси на исти начин као што је дат пристанак или на било који други начин, који субјект података сматра једноставнијим. У данашњем информатичком друштву, вероватно је најједноставнији начин да се повуче сагласност једноставним е-маилом. Ако субјект података жели повући свој пристанак, довољан је једноставан е-маил. Алтернативно, субјект података може изабрати било који други начин да нам саопшти своје повлачење сагласности.

## K. Право на подношење жалбе надзорном органу (члан 14 (2), тачка (е); члан 77 (1) ГДПР)

Као контролор, дужни смо да обавестимо субјекта података о праву на подношење жалбе надзорном органу, члан 14 (2), тачка (е) ГДПР. Право на подношење жалбе надзорном органу регулисано је чланом 77 (1) ГДПР. Према овој одредби, без прејудицирања било ког другог административног или правног лека, сваки субјект података има право да поднесе жалбу надзорном органу, посебно у држави чланици у којој се налази његово пребивалиште, радно место


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

или место наводног прекршаја, ако субјект података сматра да обрада личних података који се односе на њега или њу крши одредбе ГДПР. Право на подношење жалбе надзорном органу ограничено је само правом Уније на такав начин, да се може остварити само пред једним надзорним органом (уводна изјава 141, реченица 1 ГДПР). Ово правило има за циљ да избегне двоструке жалбе истог субјекта података у истом предмету. Стога, ако субјект података жели да уложи жалбу против нас, тражимо да контактира само један надзорни орган.

## L. Извор одакле лични подаци потичу, и ако је примењиво, да ли долазе из јавно доступних извора (члан 14 (2) тачка (ф) ГДПР)

У принципу, лични подаци се прикупљају директно од субјекта података или у сарадњи са органом (нпр. Проналажење података из званичног регистра). Остали подаци о субјектима података су изведени из трансфера групе компанија. У контексту ове опште информације, именовање тачних извора из којих су лични подаци проистекли или је немогуће или би укључивало несразмерне напоре у смислу чл. 14 (5) тачка (б) ГДПР. У принципу, ми не прикупљамо личне податке из јавно доступних извора.

Сваки субјект података може нас контактирати у било које време како би добио детаљније информације о тачним изворима личних података који се односе на њега. Када се порекло личних података не може предочити субјекту података јер су коришћени различити извори, треба дати опште информације (уводна изјава 61, реченица 4 ГДПР).

## M. Постојање аутоматизованог одлучивања, укључујући профилисање, из члана 22 (1) и (4) ГДПР и, бар у тим случајевима, смислене информације о томе о којој је логици реч, као и значај и предвиђених последица такве обраде за субјекта података (члан 14 (2) тачка (г) ГДПР)

Као одговорна компанија, обично не користимо аутоматизовано доношење одлука или профилисање. Ако, у изузетним случајевима, извршимо аутоматизовано доношење одлука или профилисање, обавестићемо субјекта података или засебно или путем пододељака у нашој политици приватности (на нашој веб страници). У овом случају важи следеће:

Аутоматско доношење одлука – укључујући и профилисање – може се десити ако (1) је то неопходно за склапање или извршење уговора између субјекта података и нас, или (2) ако је то дозвољено законом Уније или државе чланице на коју ми су предмет и који такође прописује одговарајуће мере за заштиту права и слобода и легитимних интереса субјекта података; или (3) ово се заснива на изричитој сагласности субјекта података.

У случајевима наведеним у члану 22(2) (а) и (ц) ГДПР, ми ћемо применити одговарајуће мере за заштиту права и слобода и легитимних интереса субјекта података. У овим случајевима имате


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

право да добијете људску интервенцију од стране контролора, да изразите своје гледиште и да оспорите одлуку.

Смислене информације о логици која је укључена, као и значај и предвиђене последице такве обраде за субјекта података су наведене у нашој политици приватности.

## III. EU-U.S. Data Privacy Framework (EU-U.S. DPF), UK Extension to the EU-U.S. DPF, Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF)

Ako je naša organizacija sertifikovani član EU-U.S. Data Privacy Framework (EU-U.S. DPF) i/ili UK Extension to the EU-U.S. DPF i/ili Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF), važi sledeće:

Mi se pridržavamo EU-U.S. Data Privacy Framework (EU-U.S. DPF) i UK Extension to the EU-U.S. DPF, kao i Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF), kako je određeno od strane U.S. Department of Commerce. Naša kompanija je potvrdila Ministarstvu trgovine SAD-a da se pridržava EU-U.S. Data Privacy Framework Principles (EU-U.S. DPF Principles) u vezi sa obradom ličnih podataka koje prima iz Evropske unije i Ujedinjenog Kraljevstva pozivajući se na EU-U.S. DPF i UK Extension to the EU-U.S. DPF. Naša kompanija je potvrdila Ministarstvu trgovine SAD-a da se pridržava Swiss-U.S. Data Privacy Framework Principles (Swiss-U.S. DPF Principles) u vezi sa obradom ličnih podataka koje prima iz Švajcarske pozivajući se na Swiss-U.S. DPF. U slučaju sukoba između odredbi naše politike privatnosti i EU-U.S. DPF Principles i/ili Swiss-U.S. DPF Principles, Principles su merodavne.

Za više informacija o Data Privacy Framework (DPF) programu i za pregled naše sertifikacije, posetite https://www.dataprivacyframework.gov/.

Ostale američke jedinice ili američke podružnice naše kompanije, koje se takođe pridržavaju EU-U.S. DPF Principles, uključujući UK Extension to the EU-U.S. DPF i Swiss-U.S. DPF Principles, ako postoje, navedene su u našoj politici privatnosti.

U skladu sa EU-U.S. DPF i UK Extension to the EU-U.S. DPF, kao i Swiss-U.S. DPF, naša kompanija se obavezuje da sarađuje sa telom koje su osnovale evropske nadzorne vlasti za zaštitu podataka i britanski Information Commissioner's Office (ICO), kao i sa švajcarskim Federal Data Protection and Information Commissioner (EDÖB), te da prati njihove savete u vezi sa nerešenim pritužbama o našem rukovanju ličnim podacima koje primamo pozivajući se na EU-U.S. DPF i UK Extension to the EU-U.S. DPF i Swiss-U.S. DPF.

Obaveštavamo pogođene osobe o nadležnim evropskim telima za zaštitu podataka koja su odgovorna za rešavanje pritužbi u vezi sa rukovanjem ličnim podacima naše organizacije u gornjem delu ovog transparentnog dokumenta te da pogođenim osobama pružamo odgovarajuće i besplatno pravno sredstvo.


© All rights reserved by Heiko Maniero.

Obaveštavamo sve pogođene osobe da naša kompanija podleže istražnim i izvršnim ovlašćenjima Federal Trade Commission (FTC).

Pogođene osobe imaju pravo, pod određenim uslovima, da zatraže obavezujuću arbitražu. Naša organizacija je obavezna da reši zahteve i pridržava se uslova prema Aneksu I DPF-Principles, ako je pogođena osoba zatražila obavezujuću arbitražu tako što je obavestila našu organizaciju i pridržavala se postupaka i uslova prema Aneksu I Principles.

Ovim obaveštavamo sve pogođene osobe o odgovornosti naše organizacije u slučaju prenosa ličnih podataka trećim stranama.

Za pitanja pogođenih osoba ili tela za zaštitu podataka imenovali smo lokalne predstavnike navedene u gornjem delu ovog transparentnog dokumenta.

Pružamo vam mogućnost izbora (Opt-out) da li želite da vaši lični podaci (i) budu prosleđeni trećim stranama ili (ii) korišćeni u svrhu koja se bitno razlikuje od one za koju su izvorno prikupljeni ili koju ste kasnije odobrili. Jasan, vidljiv i lako dostupan mehanizam za ostvarivanje vašeg prava izbora je kontaktiranje našeg službenika za zaštitu podataka (DSB) putem e-pošte. Nemate mogućnost izbora i nismo obavezni to učiniti ako se podaci prosleđuju trećoj strani koja deluje kao agent ili obrađivač podataka u naše ime i prema našim uputama. Međutim, uvek sklapamo ugovor sa takvim agentom ili obrađivačem podataka.

Za osetljive podatke (tj. lične podatke koji sadrže informacije o zdravstvenom stanju, rasnom ili etničkom poreklu, političkim mišljenjima, verskim ili filozofskim uverenjima, članstvu u sindikatu ili informacije o seksualnom životu pogođene osobe) tražimo vašu izričitu saglasnost (Opt-in) kada se ti podaci (i) prosleđuju trećim stranama ili (ii) koriste u svrhu koja se razlikuje od one za koju su izvorno prikupljeni ili za koju ste kasnije dali svoju saglasnost odabirom Opt-in. Osim toga, sve lične podatke koje primimo od trećih strana tretiramo kao osetljive ako ih treća strana identifikuje i tretira kao osetljive.

Ovim vas obaveštavamo o potrebi otkrivanja ličnih podataka kao odgovor na zakonite zahteve vlasti, uključujući ispunjavanje zahteva za nacionalnu bezbednost ili sprovođenje zakona.

Prilikom prenosa ličnih podataka trećoj strani koja deluje kao rukovalac obrade, pridržavamo se Principals obaveštavanja i izbora. Takođe sklapamo ugovor sa trećom stranom koja je odgovorna za obradu, koji predviđa da se ti podaci smeju obrađivati samo za ograničene i određene svrhe u skladu sa vašom danom saglasnošću i da primalac pruža isti nivo zaštite kao Principals DPF te nas obaveštava ako utvrdi da više ne može ispunjavati tu obavezu. Ugovor predviđa da treća strana, koja je rukovalac obrade, prekine obradu ili preduzme druge odgovarajuće i prikladne mere kako bi se otklonio problem kada se takva situacija utvrdi.

Prilikom prenosa ličnih podataka trećoj strani koja deluje kao agent ili obrađivač podataka (i) prenosimo te podatke samo za ograničene i određene svrhe; (ii) uveravamo se da je agent ili obrađivač podataka obavezan da obezbedi najmanje isti nivo zaštite podataka kao što to zahtevaju DPF-Principles; (iii) preduzimamo odgovarajuće i prikladne mere kako bismo osigurali da agent ili obrađivač podataka stvarno


© All rights reserved by Heiko Maniero.

обрађује пренете личне податке на начин који је у складу са нашим обавезама према DPF-Principles; (iv) захтевамо од агента или обрађивача података да обавести нашу организацију ако утврди да више не може испуњавати обавезу пружања истог нивоа заштите као што то предвиђају DPF-Principles; (v) након обавештења, укључујући оно под (iv), предузимамо одговарајуће и прикладне кораке како бисмо зауставили неовлашћену обраду и отклонили проблем; и (vi) DPF Departmentu на захтев пружамо сажетак или репрезентативни примерак релевантних одредби уговора о заштити података са тим агентом.

U skladu sa EU-U.S. DPF i/ili UK Extension to the EU-U.S. DPF i/ili Swiss-U.S. DPF, naša organizacija se obavezuje da sarađuje sa telom koje su osnovale evropske nadzorne vlasti za zaštitu podataka i britanski Information Commissioner's Office (ICO), odnosno sa švajcarskim Federal Data Protection and Information Commissioner (EDÖB), te da prati njihove savete u vezi sa nerešenim pritužbama o našem rukovanju ličnim podacima u vezi sa radnim odnosom koje primamo pozivajući se na EU-U.S. DPF i UK Extension to the EU-U.S. DPF i Swiss-U.S. DPF.

Сви субјекти података који се привремено налазе у Европској унији (ЕУ), Европском економском простору (ЕЕА) или Уједињеном Краљевству, или који тамо имају пребивалиште или уобичајено боравиште, имају право на права и права носилаца података која су објављена у нашем Транспарентност документа, који такође произилазе из чланова 15 до 22 ГДПР, укључујући право на приступ личним подацима. Ове информације смо учинили доступним на свим језицима ЕУ и ЕЕА. Верзија на енглеском језику важи за Уједињено Краљевство.

Сви субјекти података који имају привремени боравак у Швајцарској или имају пребивалиште или уобичајено боравиште тамо имају право на права и права носилаца података према Швајцарском закону о заштити података (ДПА) и Швајцарској уредби о заштити података (ДПР) који су објављени у нашој Транспарентности Документ, укључујући право на приступ личним подацима. Ову информацију смо дали на три званична језика Швајцарске (немачки, италијански и француски).


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

# RUSSIAN: Информация об обработке персональных данных (статья 13, 14 Общий Регламент по Защите Данных, ОРЗД (GDPR))

Уважаемые дамы или господа,

Персональные данные каждого человека, который находится в договорных, преддоговорных или иных отношениях с нашей компанией, заслуживают особой защиты. Наша цель - поддерживать высокий уровень защиты данных. Поэтому мы регулярно развиваем наши концепции защиты данных.

Разумеется, мы соблюдаем законодательные положения о защите данных. Согласно Статье 13, 14 ОРЗД, контролеры отвечают определенным информационным требованиям при сборе персональных данных. Этот документ выполняет следующие обязательства.

Терминология правовых норм сложна. К сожалению, использование юридических терминов нельзя было обойтись при подготовке этого документа. Поэтому мы хотели бы отметить, что вы всегда можете связаться с нами по всем вопросам, касающимся этого документа, используемых терминов или формулировок.

## I. Соответствие требованиям в отношении информации, когда личные данные собираются от субъекта данных (статья 13 ОРЗД)

### A. Идентификационные данные и контактные данные контролера (статья 13 (1) букв. ОРЗД)

См. Выше

### B. Контактные данные защиты данных Сотрудников (статья 13 (1) лит. B ОРЗД)

См. Выше

### C. Цели обработки, для которых предназначены личные данные, а также правовая основа для их обработки (Статья 13 (1) лит. в ОРЗД)

Цель обработки персональных данных - это обработка всех операций, которые касаются контролера, клиентов, потенциальных клиентов, деловых партнеров или других договорных или преддоговорных отношений между названными группами (в широком смысле) или юридических обязательств контролера.

Изобразительное искусство. 6 (1) лит. ОРЗД служит правовой основой для операций обработки, на которые мы получаем согласие для конкретной цели обработки. Если обработка


Powered by ICB International Certification Body. © All rights reserved by Heiko Maniero.

персональных данных необходима для выполнения договора, участником которого является субъект данных, как, например, в случае, когда операции обработки необходимы для поставки товаров или для предоставления какой-либо другой услуги, обработка является на основании статьи 6 (1) лит. б ОРЗД. То же самое относится к таким операциям обработки, которые необходимы для выполнения преддоговорных мер, например, в случае запросов относительно наших продуктов или услуг. Подлежит ли наша компания юридическому обязательству, при котором требуется обработка персональных данных, например, для выполнения налоговых обязательств, обработка основана на ст. 6 (1) в ОРЗД.

В редких случаях обработка персональных данных может быть необходима для защиты жизненно важных интересов субъекта данных или другого физического лица. Это может иметь место, например, если посетитель получил травму в нашей компании и его имя, возраст, данные медицинского страхования или другая важная информация должны были быть переданы врачу, больнице или другой третьей стороне. Тогда обработка будет основана на ст. 6 (1) лит. г ОРЗД.

Если обработка необходима для выполнения задачи, решаемой в общественных интересах или в рамках осуществления официальных полномочий, возложенных на контроллера, правовым основанием является ст. 6 (1) лит. е ОРЗД.

Наконец, обработка может быть основана на Статье 6 (1) лит. е ОРЗД. Эта правовая основа используется для операций обработки, которые не подпадают ни под одно из вышеупомянутых правовых оснований, если обработка необходима для целей законных интересов, преследуемых нашей компанией или третьей стороной, за исключением случаев, когда такие интересы перекрываются интересами или фундаментальные права и свободы субъекта данных, которые требуют защиты персональных данных. Такие операции обработки особенно допустимы, потому что они были специально упомянуты европейским законодателем. Он считал, что законный интерес может быть принят, если субъект данных является клиентом контролера (Декламация 47 Предложение 2 ОРЗД).

## D. Если обработка основана на статье 6 (1) лит. е GDPR законные интересы, преследуемые контролером или третьей стороной (Статья 13 (1) лит. г ОРЗД)

Если обработка персональных данных основана на Статье 6 (1) лит. е ОРЗД наш законный интерес состоит в том, чтобы вести наш бизнес в интересах благополучия всех наших сотрудников и акционеров.

## E. Категории получателей персональных данных (статья 13 (1) и т. д. ОРЗД)

Государственные органы

Внешние органы

Дополнительные внешние органы

Внутренняя обработка

Внутригрупповая обработка


© All rights reserved by Heiko Maniero.

Другие органы

Список наших обработчиков и получателей данных в третьих странах и, при необходимости, международных организаций публикуется на нашем сайте или может быть запрошен у нас бесплатно. Пожалуйста, свяжитесь с нашим сотрудником по защите данных, чтобы запросить этот список.

## F. Получатели в третьей стране и соответствующие или подходящие гарантии и средства, с помощью которых получить их копию или там, где они были предоставлены (статья 13 (1) лит. д, 46 (1), 46 (2) лит. в ОРЗД)

Все компании и филиалы, входящие в нашу группу (далее упоминается) к «групповым компаниям»), которые имеют свое коммерческое предприятие или офис в третьей стране, могут принадлежать получателям персональных данных. У нас можно запросить список всех компаний или получателей группы.

Согласно Статье 46 (1) ОРЗД, контроллер или процессор может передавать личные данные только в третью страну, если контроллер или процессор предоставил соответствующие гарантии, и при условии, что для субъектов данных доступны действующие права субъекта данных и эффективные средства правовой защиты. Соответствующие меры предосторожности могут быть предоставлены без какого-либо специального разрешения от надзорного органа посредством стандартных договорных положений, Статья 46 (2) лит. в ОРЗД.

Стандартные договорные положения Европейского Союза или другие соответствующие меры предосторожности согласовываются со всеми получателями из третьих стран до первой передачи персональных данных. Следовательно, гарантируется, что гарантируются надлежащие меры защиты, осуществимые права субъекта данных и эффективные средства правовой защиты для субъектов данных. Каждый субъект данных может получить у нас копию стандартных договорных положений. Стандартные договорные положения также доступны в Официальном журнале Европейского Союза.

Статья 45(3) Общего регламента по защите данных (GDPR) предоставляет Европейской комиссии право посредством имплементационного акта принимать решение о том, что страна за пределами ЕС обеспечивает адекватный уровень защиты. Это означает, что уровень защиты персональных данных в целом эквивалентен уровню защиты в ЕС. В результате принятия решения о достаточном уровне защиты персональные данные могут свободно передаваться из стран ЕС (а также Норвегии, Лихтенштейна и Исландии) в третьи страны без каких-либо препятствий. Аналогичные правила действуют в Великобритании, Швейцарии и некоторых других странах.

В случае если Европейская комиссия или правительство другой страны примет решение о том, что третья страна обеспечивает адекватный уровень защиты, а также о применимых рамках (например, EU-U.S. Data Privacy Framework, Swiss-U.S. Data Privacy Framework, UK Extension to the EU-U.S. Data Privacy Framework), все передачи нами данных членам таких рамочных программ (например, самосертифицированным организациям) будут основываться исключительно на членстве этих организаций в соответствующей рамочной программе. В случае если мы или одна из наших групп компаний является членом такой структуры, все передачи нам или нашей группе компаний основываются исключительно на членстве компании в такой структуре.

Любой субъект данных может получить у нас копию рамочных документов. Кроме того, эти рамки также доступны в Официальном журнале Европейского союза, в опубликованных правовых


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

материалах или на веб-сайтах надзорных органов или других компетентных органов или учреждений.

## G. Период, в течение которого будут храниться персональные данные, или, если это невозможно, критерии, используемые для определения этого периода (Статья 13 (2) лит. ОРЗД)

Критерии, используемые для определения периода хранения персональных данных, соответствующий установленный законом срок хранения. По истечении этого периода соответствующие данные обычно удаляются, если они больше не нужны для выполнения контракта или для инициирования контракта.

Если нет установленного законом срока хранения, критерием является договорной или внутренний срок хранения.

## H. Наличие права запрашивать у контролера доступ и исправление или удаление персональных данных или ограничение обработки, касающейся субъекта данных или объекта обработки, а также право на переносимость данных (статья 13 (2) лит. В ОРЗД)

Все субъекты данных имеют следующие права:

***Право на доступ***

Каждый субъект данных имеет право на доступ к своим персональным данным. Право на доступ распространяется на все данные, обрабатываемые нами. Право может быть реализовано легко и через разумные промежутки времени, чтобы знать и проверять законность обработки (Декламация 63 ОРЗД). Это право вытекает из ст. 15 ОРЗД. Субъект данных может связаться с нами, чтобы воспользоваться правом доступа.

***Право на исправление***

В соответствии со Статьей 16 Предложения 1 ОРЗД субъект данных имеет право без промедления получить от контролера исправление неточных личных данных, касающихся его или ее. Кроме того, Статья 16 Предложения 2 ОРЗД предусматривает, что субъект данных имеет право, с учетом целей обработки, заполнять неполные персональные данные, в том числе посредством предоставления дополнительного заявления. Субъект данных может связаться с нами для осуществления права на исправление.

***Право на удаление (право быть забытым)***

Кроме того, субъекты данных имеют право на стирание и быть забытыми в соответствии со ст. 17 ОРЗД. Это право также может быть реализовано, связавшись с нами. На этом этапе, однако, мы хотели бы указать, что это право не применяется, поскольку обработка необходима для выполнения юридического обязательства, которому подчиняется наша компания, Статья 17 (3) освещена. б ОРЗД. Это означает, что мы можем одобрить заявку на удаление только после истечения установленного законом срока хранения.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

***Право на ограничение обработки***

Согласно статье 18 ОРЗД любой субъект данных имеет право на ограничение обработки. Ограничение обработки может потребоваться, если одно из условий, изложенных в Статье 18 (1), объявление ОРЗД выполнено. Субъект данных может связаться с нами, чтобы воспользоваться правом на ограничение обработки.

***Право на возражение***

Кроме того, ст. 21 ОРЗД гарантирует право на возражение. Субъект данных может связаться с нами, чтобы воспользоваться правом на возражение.

***Право на переносимость данных***

Ст. 20 ОРЗД предоставляет субъекту данных право на переносимость данных. В соответствии с этим положением субъект данных в условиях, изложенных в Статье 20 (1), освещен. а и б ОРЗД - право на получение относящихся к нему персональных данных, которые он или она предоставил контроллеру, в структурированном, широко используемом и машиночитаемом формате и имеет право передавать эти данные другому контроллеру без помех от контроллера, которому были предоставлены персональные данные. Субъект данных может связаться с нами, чтобы воспользоваться правом на переносимость данных.

## I. Наличие права на отзыв согласия в любое время, не затрагивая законность обработки, основанной на согласии до его отзыва, если обработка основана на статье 6 (1) лит. ОРЗД или Статья 9 (2) лит. ОРЗД (Статья 13 (2) лит. в ОРЗД)

Если обработка персональных данных основана на ст. 6 (1) лит. ОРЗД, что имеет место, если субъект данных дал согласие на обработку персональных данных для одной или нескольких конкретных целей или он основан на Статье 9 (2) освещен. ОРЗД, который регулирует явное согласие на обработку специальных категорий персональных данных, субъект данных в соответствии со Статьей 7 (3) Предложения 1 ОРЗД имеет право отозвать свое согласие в любое время.

Отзыв согласия не влияет на законность обработки, основанной на согласии до его отзыва, Статья 7 (3) Предложение 2 ОРЗД. Изъять его так же легко, как и дать согласие, ст. 7 (3) Предложение 4 ОРЗД. Следовательно, отзыв согласия всегда может происходить так же, как было дано согласие, или любым другим способом, который субъект данных считает более простым. В современном информационном обществе, вероятно, самый простой способ отозвать согласие - это простое электронное письмо. Если субъект данных хочет отозвать свое согласие, нам достаточно простого электронного письма. В качестве альтернативы субъект данных может выбрать любой другой способ сообщить о своем отзыве согласия.

## J. Право подать жалобу в надзорный орган (статья 13 (2) лит. Г, 77 (1) ОРЗД)

Как контролирующий, мы обязаны уведомить субъект данных о праве подать жалобу в надзорный орган, Статья 13 (2) лит. г ОРЗД. Право на подачу жалобы в надзорный орган регулируется Статьей 77 (1) ОРЗД. Согласно этому положению, без ущерба для любого другого административного или судебного средства правовой защиты, каждый субъект данных имеет право подать жалобу в орган надзора, в частности в государстве-члене своего обычного места жительства, места работы или места работы. предполагаемое нарушение, если субъект данных считает, что обработка относящихся к нему персональных данных нарушает Общие положения о защите данных. Право на подачу жалобы в надзорный орган ограничивалось


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

законодательством Союза только таким образом, что оно может быть реализовано только в одном надзорном органе (Декламация 141 Предложение 1 ОРЗД). Это правило направлено на то, чтобы избежать двойных жалоб одного и того же субъекта данных на один и тот же вопрос. Если субъект данных хочет подать жалобу на нас, мы просим связаться только с одним надзорным органом.

## K. Предоставление персональных данных в качестве законодательного или договорного требования; Требование, необходимое для заключения договора; Обязательство субъекта данных предоставлять персональные данные; возможные последствия непредоставления таких данных (ст. 13 (2) лит. е ОРЗД)

Мы разъясняем, что предоставление персональных данных частично требуется законом (например, налоговые правила) или также может быть результатом договорных положений (например, информация о договорный партнер).

Иногда может потребоваться заключить договор о том, что субъект данных предоставляет нам персональные данные, которые впоследствии должны быть обработаны нами. Субъект данных, например, обязан предоставить нам персональные данные, когда наша компания заключает с ним договор. Непредоставление персональных данных приведет к тому, что договор с субъектом данных не может быть заключен.

Прежде чем личные данные будут предоставлены субъект данных должен связаться с нами. Мы уточняем субъекту данных, требуется ли предоставление персональных данных по закону или договору или необходимо для заключения договора, есть ли обязательство предоставлять персональные данные и последствия непредоставления персональных данных ,

## L. Наличие автоматизированного процесса принятия решений, включая профилирование, о котором говорится в статье 22 (1) и (4) ОРЗД, и, по крайней мере, в этих случаях, содержательную информацию о соответствующей логике, а также о значении и предполагаемых последствиях такая обработка для субъекта данных (Статья 13 (2), лит. д ОРЗД)

Как ответственная компания, мы обычно не используем автоматизированное принятие решений или профилирование. Если в исключительных случаях мы осуществляем автоматизированное принятие решений или профилирование, мы информируем об этом субъекта данных либо отдельно, либо через подраздел в нашей политике конфиденциальности (на нашем сайте). В этом случае действует следующее:

Автоматизированное принятие решений - включая профилирование - может иметь место, если (1) это необходимо для заключения или исполнения договора между субъектом данных и нами, или (2) это разрешено законодательством Союза или государства-члена, которому мы подчиняемся и которое также устанавливает соответствующие меры для защиты прав и свобод и законных интересов субъекта данных, или (3) это основано на явном согласии субъекта данных.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

В случаях, указанных в статье 22(2)(a) и (c) GDPR, мы должны принять соответствующие меры для защиты прав и свобод субъекта данных и его законных интересов. В этих случаях вы имеете право на вмешательство человека со стороны контроллера, на выражение своей точки зрения и на оспаривание принятого решения.

Содержательная информация о задействованной логике, а также о значении и предполагаемых последствиях такой обработки для субъекта данных изложена в нашей политике конфиденциальности.

# II. Соответствие требованиям в отношении информации, когда личные данные не собираются от субъекта данных (Статья 14 ОРЗД)

## A. Идентификационные данные и контактные данные контролера (Статья 14 (1) лит. ОРЗД)

См. Выше

## B. Контактные данные данных Сотрудник по защите (Статья 14 (1), лит. B ОРЗД)

См. Выше

## C. Цели обработки, для которых предназначены персональные данные, а также правовое основание для обработки (статья 14 (1), лит. в ОРЗД)

Цель обработка персональных данных - это обработка всех операций, которые касаются контролера, клиентов, потенциальных клиентов, деловых партнеров или других договорных или преддоговорных отношений между названными группами (в широком смысле) или юридических обязательств контролера.

Если обработка персональных данных необходима для выполнения договора, участником которого является субъект данных, как, например, в случае, когда операции обработки необходимы для поставки товаров или для предоставления какой-либо другой услуги, обработка является на основании Статьи 6 (1) лит. б ОРЗД. То же самое относится к таким операциям обработки, которые необходимы для выполнения преддоговорных мер, например, в случае запросов относительно наших продуктов или услуг. Подлежит ли наша компания юридическому обязательству, при котором требуется обработка персональных данных, например, для выполнения налоговых обязательств, обработка основана на ст. 6 (1) горит с ОРЗД.

В редких случаях обработка персональных данных может быть необходима для защиты жизненно важных интересов субъекта данных или другого физического лица. Это может иметь место, например, если посетитель получил травму в нашей компании и его имя, возраст, данные медицинского страхования или другая важная информация должны были быть переданы врачу, больнице или другой третьей стороне. Тогда обработка будет основана на ст. 6 (1) г ОРЗД.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

Если обработка необходима для выполнения задачи, решаемой в общественных интересах или в рамках осуществления официальных полномочий, возложенных на контроллера, правовым основанием является ст. 6 (1) лит. e ОРЗД.

Наконец, обработка может быть основана на Статье 6 (1) лит. д ОРЗД. Эта правовая основа используется для операций обработки, которые не подпадают ни под одно из вышеупомянутых правовых оснований, если обработка необходима для целей законных интересов, преследуемых нашей компанией или третьей стороной, за исключением случаев, когда такие интересы перекрываются интересами или фундаментальные права и свободы субъекта данных, которые требуют защиты персональных данных. Такие операции обработки особенно допустимы, потому что они были специально упомянуты европейским законодателем. Он считал, что законный интерес может быть принят, если субъект данных является клиентом контролера (Декламация 47 Предложения 2 ОРЗД).

## D. Категория персональных данныхсвязанных (Статья 14 (1) лит. г ОРЗД)

данные клиентов

Данныепотенциальных клиентов

данных работников

данных поставщиков

## E. категорий получателей персональных данных (Статья 14 (1) лит. г ОРЗД)

Государственные органы

Внешние органы

Другие внешние органы

Внутренняя обработка

Внутригрупповая обработка

Другие органы

Список наших обработчиков и получателей данных в третьих странах и, при необходимости, международных организаций публикуется на нашем сайте или может быть запрошен у нас бесплатно. Пожалуйста, свяжитесь с нашим сотрудником по защите данных, чтобы запросить этот список.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## F. Получатели в третьей стране и соответствующие или подходящие гарантии и средства, с помощью которых можно получить их копию или когда они были предоставлены (Статья 14 (1) лит. д, 46 (1), 46 (2) лит. в ОРЗД)

Все компании и филиалы, входящие в нашу группу (далее именуемые «группы компаний»), которые имеют коммерческие предприятия или офис в третьей стране. могут принадлежать получателям персональных данных. Список всех компаний группы можно запросить у нас.

Согласно Статье 46 (1) ОРЗД, контроллер или процессор может передавать личные данные только в третью страну, если контроллер или процессор предоставил соответствующие гарантии, и при условии, что для субъектов данных доступны действующие права субъекта данных и эффективные средства правовой защиты. Соответствующие меры предосторожности могут быть предоставлены без какого-либо специального разрешения от надзорного органа посредством стандартных положений о защите данных, статья 46 (2) освещена. с ОРЗД.

Стандартные договорные положения Европейского Союза или другие соответствующие меры предосторожности согласовываются со всеми получателями из третьих стран до первой передачи персональных данных. Следовательно, гарантируется, что гарантируются надлежащие меры защиты, осуществимые права субъекта данных и эффективные средства правовой защиты для субъектов данных. Каждый субъект данных может получить у нас копию стандартных договорных положений. Стандартные договорные положения также доступны в Официальном журнале Европейского Союза.

Статья 45(3) Общего регламента по защите данных (GDPR) предоставляет Европейской комиссии право посредством имплементационного акта принимать решение о том, что страна за пределами ЕС обеспечивает адекватный уровень защиты. Это означает, что уровень защиты персональных данных в целом эквивалентен уровню защиты в ЕС. В результате принятия решения о достаточном уровне защиты персональные данные могут свободно передаваться из стран ЕС (а также Норвегии, Лихтенштейна и Исландии) в третьи страны без каких-либо препятствий. Аналогичные правила действуют в Великобритании, Швейцарии и некоторых других странах.

В случае если Европейская комиссия или правительство другой страны примет решение о том, что третья страна обеспечивает адекватный уровень защиты, а также о применимых рамках (например, EU-U.S. Data Privacy Framework, Swiss-U.S. Data Privacy Framework, UK Extension to the EU-U.S. Data Privacy Framework), все передачи нами данных членам таких рамочных программ (например, самосертифицированным организациям) будут основываться исключительно на членстве этих организаций в соответствующей рамочной программе. В случае если мы или одна из наших групп компаний является членом такой структуры, все передачи нам или нашей группе компаний основываются исключительно на членстве компании в такой структуре.

Любой субъект данных может получить у нас копию рамочных документов. Кроме того, эти рамки также доступны в Официальном журнале Европейского союза, в опубликованных правовых материалах или на веб-сайтах надзорных органов или других компетентных органов или учреждений.


© All rights reserved by Heiko Maniero.

## G. Период, в течение которого будут храниться персональные данные, или, если это невозможно, критерии, используемые для определения этого периода (Статья 14 (2) лит. ОРЗД)

Критерии, используемые для определения периода хранения персональных данных: соответствующий установленный законом срок хранения. По истечении этого периода соответствующие данные обычно удаляются, если они больше не нужны для выполнения контракта или для инициирования контракта.

Если нет установленного законом срока хранения, критерием является договорной или внутренний срок хранения.

## H. Уведомление о законных интересах, преследуемых контролером или третьей стороной, если обработка основана на статье 6 (1) лит. г ОРЗД (ст. 14 (2) лит. б ОРЗД)

В соответствии со Статьей 6 (1) лит. д ОРЗД, обработка должна быть законной, только если обработка необходима для целей законных интересов, преследуемых контролером или третьей стороной, за исключением случаев, когда такие интересы перекрываются интересами или основными правами и свободами субъекта данных, которые требуют защиты. личных данных. Согласно Декламации 47 Предложения 2 ОРЗД, законный интерес может существовать в тех случаях, когда существует релевантная и надлежащая связь между субъектом данных и контроллером, например, в ситуациях, когда субъект данных является клиентом контроллера. Во всех случаях, когда наша компания обрабатывает персональные данные в соответствии со статьей 6 (1) лит. г ОРЗД, наш законный интерес заключается в том, чтобы вести наш бизнес в интересах благополучия всех наших сотрудников и акционеров.

## I. Наличие права запрашивать у контролера доступ и исправление или стирание персональных данных или ограничение обработки, касающейся субъекта данных и объекта обработки, а также право на переносимость данных (Статья 14 (2) лит. В) ОРЗД)

Все субъекты данных имеют следующие права:

***Право на доступ***

Каждый субъект данных имеет право на доступ к своим персональным данным. Право на доступ распространяется на все данные, обрабатываемые нами. Право может быть реализовано легко и через разумные промежутки времени, чтобы знать и проверять законность обработки (Декламация 63 ОРЗД). Это право вытекает из ст. 15 ОРЗД. Субъект данных может связаться с нами, чтобы воспользоваться правом доступа.

***Право на исправление***

В соответствии со Статьей 16 Предложения 1 ОРЗД субъект данных имеет право без промедления получить от контролера исправление неточных личных данных, касающихся его или ее. Кроме того, Статья 16 Предложения 2 ОРЗД предусматривает, что субъект данных имеет право, с учетом целей обработки, заполнять неполные персональные данные, в том числе


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

посредством предоставления дополнительного заявления. Субъект данных может связаться с нами для осуществления права на исправление.

***Право на удаление (право быть забытым)***

Кроме того, субъекты данных имеют право на стирание и быть забытыми в соответствии со ст. 17 ОРЗД. Это право также может быть реализовано, связавшись с нами. На этом этапе, однако, мы хотели бы указать, что это право не применяется, поскольку обработка необходима для выполнения юридического обязательства, которому подчиняется наша компания, Статья 17 (3) освещена. б ОРЗД. Это означает, что мы можем одобрить заявку на удаление только после истечения установленного законом срока хранения.

***Право на ограничение обработки***

Согласно Статье 18 ОРЗД любой субъект данных имеет право на ограничение обработки. Ограничение обработки может потребоваться, если одно из условий, изложенных в Статье 18 (1), лит. объявление ОРЗД выполнено. Субъект данных может связаться с нами, чтобы воспользоваться правом на ограничение обработки.

***Право на возражение***

Кроме того, ст. 21 ОРЗД гарантирует право на возражение. Субъект данных может связаться с нами, чтобы воспользоваться правом на возражение.

***Право на переносимость данных***

Ст. 20 ОРЗД предоставляет субъекту данных право на переносимость данных. Согласно этому положению субъект данных в условиях, изложенных в Статье 20 (1), освещен. а и б ОРЗД - право на получение относящихся к нему персональных данных, которые он или она предоставил контроллеру, в структурированном, широко используемом и машиночитаемом формате и имеет право передавать эти данные другому контроллеру без помех от контроллера, которому были предоставлены персональные данные. Субъект данных может связаться с нами, чтобы воспользоваться правом на переносимость данных.

## J. Наличие права на отзыв согласия в любое время, не затрагивая законность обработки, основанной на согласии до его отзыва, если обработка основана на статье 6 (1) лит. или Статья 9 (2) лит. ОРЗД (ст. 14 (2) лит. г ОРЗД)

Если обработка персональных данных основана на ст. 6 (1) горит ОРЗД, что имеет место, если субъект данных дал согласие на обработку персональных данных для одной или нескольких конкретных целей или он основан на Статье 9 (2) лит. ОРЗД, который регулирует явное согласие на обработку специальных категорий персональных данных, субъект данных в соответствии со Статьей 7 (3) Предложения 1 ОРЗД имеет право отозвать свое согласие в любое время.

Отзыв согласия не влияет на законность обработки, основанной на согласии до его отзыва, Статья 7 (3) Предложение 2 ОРЗД. Изъять его так же легко, как и дать согласие, ст. 7 (3) Предложение 4 ОРЗД. Следовательно, отзыв согласия всегда может происходить так же, как было дано согласие, или любым другим способом, который субъект данных считает более простым. В современном информационном обществе, вероятно, самый простой способ отозвать согласие - это простое электронное письмо. Если субъект данных хочет отозвать свое согласие, нам достаточно простого электронного письма. В качестве альтернативы субъект данных может выбрать любой другой способ сообщить о своем отзыве согласия.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## K. Право подать жалобу в надзорный орган (Статья 14 (2) и т. Д. 77 (1) ОРЗД)

Как контролирующий, мы обязаны уведомить субъект данных о праве подать жалобу в надзорный орган , Статья 14 (2) лит. е ОРЗД. Право на подачу жалобы в надзорный орган регулируется Статьей 77 (1) ОРЗД. Согласно этому положению, без ущерба для любого другого административного или судебного средства правовой защиты, каждый субъект данных имеет право подать жалобу в орган надзора, в частности в государстве-члене своего обычного места жительства, места работы или места работы. предполагаемое нарушение, если субъект данных считает, что обработка относящихся к нему персональных данных нарушает Общие положения о защите данных. Право на подачу жалобы в надзорный орган ограничивалось законодательством Союза только таким образом, что оно может быть реализовано только в одном надзорном органе (Декламация 141 Предложения 1 ОРЗД). Это правило направлено на то, чтобы избежать двойных жалоб одного и того же субъекта данных на один и тот же вопрос. Если субъект данных хочет подать жалобу на нас, мы просим связаться только с одним надзорным органом.

## L. Источник, из которого происходят персональные данные, и, если применимо, получены ли они из общедоступных источников (Статья 14 (2), лит. г ОРЗД)

В принципе, личные данные собираются непосредственно от субъекта данных или в сотрудничестве с органом (например, поиск данных из официального реестра). Другие данные по темам данных получено из передач группы компаний. В контексте этой общей информации наименование точных источников, из которых получены личные данные, либо невозможно, либо может привести к непропорциональным усилиям по смыслу ст. 14 (5) лит. б ОРЗД. В принципе, мы не собираем личные данные из общедоступных источников.

Любой субъект данных может связаться с нами в любое время, чтобы получить более подробную информацию о точных источниках персональных данных, касающихся его или ее. Если источник личных данных не может быть предоставлен субъекту данных из-за того, что использовались различные источники, должна быть предоставлена общая информация ( Декламация 61 Предложения 4 ОРЗД).

## M. Наличие автоматизированного процесса принятия решений, включая профилирование, о котором говорится в статье 22 (1) и (4) ОРЗД, и, по крайней мере, в этих случаях, содержательную информацию о соответствующей логике, а также о значении и предполагаемых последствиях такая обработка для субъекта данных (Статья 14 (2) лит. Ё ОРЗД)

Как ответственная компания, мы обычно не используем автоматизированное принятие решений или профилирование. Если в исключительных случаях мы осуществляем автоматизированное принятие решений или профилирование, мы информируем об этом субъекта данных либо отдельно, либо через подраздел в нашей политике конфиденциальности (на нашем сайте). В этом случае действует следующее:

Автоматизированное принятие решений - включая профилирование - может иметь место, если (1) это необходимо для заключения или исполнения договора между субъектом данных и нами, или (2) это разрешено законодательством Союза или государства-члена, которому мы


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

подчиняемся и которое также устанавливает соответствующие меры для защиты прав и свобод и законных интересов субъекта данных, или (3) это основано на явном согласии субъекта данных.

В случаях, указанных в статье 22(2)(a) и (c) GDPR, мы должны принять соответствующие меры для защиты прав и свобод субъекта данных и его законных интересов. В этих случаях вы имеете право на вмешательство человека со стороны контроллера, на выражение своей точки зрения и на оспаривание принятого решения.

Содержательная информация о задействованной логике, а также о значении и предполагаемых последствиях такой обработки для субъекта данных изложена в нашей политике конфиденциальности.

## III. EU-U.S. Data Privacy Framework (EU-U.S. DPF), UK Extension to the EU-U.S. DPF, Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF)

Если наша организация является сертифицированным членом EU-U.S. Data Privacy Framework (EU-U.S. DPF) и/или UK Extension to the EU-U.S. DPF и/или Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF), применяется следующее:

Мы соблюдаем EU-U.S. Data Privacy Framework (EU-U.S. DPF) и UK Extension to the EU-U.S. DPF, а также Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF), как установлено U.S. Department of Commerce. Наша компания подтвердила Министерству торговли США, что соблюдает EU-U.S. Data Privacy Framework Principles (EU-U.S. DPF Principles) в отношении обработки персональных данных, получаемых из Европейского Союза и Соединенного Королевства на основании EU-U.S. DPF и UK Extension to the EU-U.S. DPF. Наша компания подтвердила Министерству торговли США, что соблюдает Swiss-U.S. Data Privacy Framework Principles (Swiss-U.S. DPF Principles) в отношении обработки персональных данных, получаемых из Швейцарии на основании Swiss-U.S. DPF. В случае противоречия между положениями нашей политики конфиденциальности и EU-U.S. DPF Principles и/или Swiss-U.S. DPF Principles, принципы (Principles) имеют приоритет.

Для получения дополнительной информации о программе Data Privacy Framework (DPF) и для просмотра нашей сертификации, посетите https://www.dataprivacyframework.gov/.

Другие подразделения или дочерние компании нашей компании в США, которые также соблюдают EU-U.S. DPF Principles, включая UK Extension to the EU-U.S. DPF и Swiss-U.S. DPF Principles, если таковые имеются, указаны в нашей политике конфиденциальности.

В соответствии с EU-U.S. DPF и UK Extension to the EU-U.S. DPF, а также Swiss-U.S. DPF, наша компания обязуется сотрудничать с органами, созданными европейскими органами по защите данных и британским Information Commissioner's Office (ICO), а также швейцарским Federal Data Protection and Information Commissioner (EDÖB), и следовать их рекомендациям по нерешенным жалобам на наше обращение с персональными данными, которые мы получаем на основании EU-U.S. DPF и UK Extension to the EU-U.S. DPF и Swiss-U.S. DPF.

Мы информируем затронутых лиц о компетентных европейских органах по защите данных, ответственных за рассмотрение жалоб на обращение нашей организации с персональными данными, в верхней части данного документа о прозрачности, а также о том, что мы предоставляем затронутым лицам адекватные и бесплатные средства правовой защиты.

Мы информируем всех затронутых лиц о том, что наша компания подлежит расследованиям и исполнительным полномочиям Federal Trade Commission (FTC).


© All rights reserved by Heiko Maniero.

Затронутые лица имеют возможность, при определенных условиях, обратиться к обязательному арбитражу. Наша организация обязана разрешать претензии и соблюдать условия согласно Приложению I DPF-Principles, если затронутое лицо запросило обязательный арбитраж, уведомив нашу организацию и следуя процедурам и условиям согласно Приложению I Principles.

Настоящим мы информируем всех затронутых лиц об ответственности нашей организации в случае передачи персональных данных третьим лицам.

Для вопросов затронутых лиц или надзорных органов по защите данных мы назначили местных представителей, указанных в верхней части данного документа о прозрачности.

Мы предоставляем вам возможность выбора (Opt-out), хотите ли вы, чтобы ваши персональные данные (i) были переданы третьим лицам или (ii) использовались для цели, существенно отличающейся от той(их), для которой(их) они первоначально были собраны или позднее вами одобрены. Ясный, хорошо видимый и легко доступный механизм для реализации вашего права выбора заключается в том, чтобы связаться с нашим уполномоченным по защите данных (DSB) по электронной почте. У вас нет возможности выбора, и мы не обязаны это делать, если данные передаются третьей стороне, которая действует как агент или обработчик данных от нашего имени и по нашим инструкциям. Однако мы всегда заключаем договор с таким агентом или обработчиком данных.

Для чувствительных данных (то есть персональных данных, содержащих информацию о состоянии здоровья, расовом или этническом происхождении, политических взглядах, религиозных или философских убеждениях, членстве в профсоюзе или информацию о сексуальной жизни затронутого лица) мы запрашиваем ваше явное согласие (Opt-in), если эти данные (i) передаются третьим лицам или (ii) используются для иной цели, отличной от той, для которой они были первоначально собраны или для которой вы позднее дали свое согласие, сделав выбор Opt-in. Кроме того, мы рассматриваем все персональные данные, которые получаем от третьих лиц, как чувствительные, если третья сторона идентифицирует и обрабатывает их как чувствительные.

Настоящим мы информируем вас о необходимости раскрытия персональных данных в ответ на законные запросы властей, включая выполнение требований национальной безопасности или правоохранительных органов.

При передаче персональных данных третьей стороне, которая действует как контролер, мы придерживаемся Principles уведомления и выбора. Мы также заключаем договор с третьей стороной, ответственной за обработку, который предусматривает, что эти данные могут обрабатываться только для ограниченных и определенных целей в соответствии с вашим данным согласием и что получатель предоставляет такой же уровень защиты, как и Principles DPF, и уведомляет нас, если обнаружит, что больше не может выполнять это обязательство. Договор предусматривает, что третья сторона, которая является контролером, прекращает обработку или принимает другие соответствующие и адекватные меры для устранения проблемы при установлении такой ситуации.

При передаче персональных данных третьей стороне, которая действует как агент или обработчик данных (i) мы передаем эти данные только для ограниченных и определенных целей; (ii) мы убеждаемся, что агент или обработчик данных обязан обеспечить как минимум такой же уровень защиты данных, как требуют DPF-Principles; (iii) мы предпринимаем соответствующие и адекватные меры, чтобы гарантировать, что агент или обработчик данных действительно обрабатывает переданные персональные данные таким образом, который соответствует нашим обязательствам по DPF-Principles; (iv) мы требуем от агента или обработчика данных уведомить нашу организацию, если он установит, что больше не может выполнять обязательство предоставлять такой же уровень защиты, как это предусмотрено DPF-Principles; (v) после


© All rights reserved by Heiko Maniero.

уведомления, в том числе указанного в (iv), мы предпринимаем соответствующие и адекватные шаги, чтобы прекратить несанкционированную обработку и устранить проблему; и (vi) предоставляем DPF Department по запросу резюме или репрезентативный экземпляр соответствующих положений договора о защите данных с этим агентом.

В соответствии с EU-U.S. DPF и/или UK Extension to the EU-U.S. DPF и/или Swiss-U.S. DPF, наша организация обязуется сотрудничать с органами, созданными европейскими надзорными органами по защите данных и британским Information Commissioner's Office (ICO), а также швейцарским Federal Data Protection and Information Commissioner (EDÖB), и следовать их рекомендациям по нерешенным жалобам на наше обращение с персональными данными в рамках трудовых отношений, которые мы получаем на основании EU-U.S. DPF и UK Extension to the EU-U.S. DPF и Swiss-U.S. DPF.

Все субъекты данных, которые временно находятся в Европейском союзе (ЕС), Европейской экономической зоне (ЕЭЗ) или Соединенном Королевстве или имеют там постоянное место жительства, имеют право на права и права субъектов данных, опубликованные в нашем документе о прозрачности, которые также вытекают из статей 15-22 GDPR, включая право на доступ к персональным данным. Мы разместили эту информацию на всех языках ЕС и ЕЭЗ. Версия на английском языке относится к Соединенному Королевству.

Все субъекты данных, временно проживающие в Швейцарии или имеющие там постоянное место жительства, имеют права и права субъектов данных в соответствии со Швейцарским законом о защите данных (DPA) и Швейцарским положением о защите данных (DPR), которые опубликованы в нашем документе о прозрачности, включая право на доступ к персональным данным. Мы предоставили эту информацию на трех официальных языках Швейцарии (немецком, итальянском и французском).


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

# RUSSIAN: Информация об обработке персональных данных для сотрудников и заявителей (статья 13, 14 Общий Регламент по Защите Данных, ОРЗД (GDPR))

Уважаемые дамы или господа,

Персональные данные сотрудников и заявителей заслуживают особой защиты. Наша цель - поддерживать высокий уровень защиты данных. Поэтому мы регулярно развиваем наши концепции защиты и защиты данных.

Разумеется, мы соблюдаем законодательные положения о защите данных. Согласно Статье 13, 14 ОРЗД, контролеры отвечают определенным информационным требованиям при обработке персональных данных. Этот документ выполняет эти обязательства.

Терминология правового регулирования сложна. К сожалению, использование юридических терминов нельзя было обойтись при подготовке этого документа. Поэтому мы хотели бы отметить, что вы всегда можете связаться с нами по всем вопросам, касающимся этого документа, используемых терминов или формулировок.

## I. Соответствие требованиям в отношении информации, когда личные данные собираются от субъекта данных (Статья 13 ОРЗД)

### A. Идентификационные данные и контактные данные контролера (Статья 13 (1) лит. ОРЗД)

См. Выше

### B. Контактные данные защиты данных Сотрудник (Статья 13 (1), лит. B ОРЗД)

См. Выше

### C. Цели обработки, для которых предназначены персональные данные, а также правовое основание для обработки (Статья 13 (1), лит. B ОРЗД)

Для данных заявителя Целью обработки данных является проведение экспертизы заявки в процессе найма. Для этого мы обрабатываем все предоставленные вами данные. На основании данных, представленных в процессе найма, мы проверим, приглашены ли вы на собеседование (часть процесса отбора). В случае подходящих кандидатов, особенно в контексте собеседования, мы обрабатываем некоторые другие личные данные, предоставленные вами, что важно для нашего решения о выборе. Если вы наняты нами, данные заявителя автоматически изменятся на данные сотрудника. В рамках процесса набора персонала мы будем обрабатывать другие персональные данные о вас, которые мы запрашиваем у вас и которые необходимы для инициирования или выполнения вашего контракта (например, личные идентификационные


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

номера или налоговые номера). Для данных о сотрудниках целью обработки данных является выполнение трудового договора или соблюдение других правовых норм, применимых к трудовым отношениям (например, налоговое законодательство), а также использование ваших персональных данных для выполнения трудового договора, заключенного с вами. (например, публикация вашего имени и контактной информации внутри компании или для клиентов). Данные о работниках хранятся после прекращения трудовых отношений для соблюдения законных сроков хранения.

Правовой основой для обработки данных является Статья 6 (1) лит. б ОРЗД, Статья 9 (2) лит. б и ж ОРЗД, Статья 88 (1) ОРЗД и национальное законодательство, например, для Германии Раздел 26 ФЗЗД (Федеральный закон о защите данных).

## D. Категории получателей персональных данных (Статья 13 (1) и т. Д. ОРЗД)

Государственные органы

Внешние органы

Дополнительные внешние органы

Внутренняя обработка

Внутригрупповая обработка

Другие органы

Список наших обработчиков и получателей данных в третьих странах и, при необходимости, международных организаций публикуется на нашем сайте или может быть запрошен у нас бесплатно. Пожалуйста, свяжитесь с нашим сотрудником по защите данных, чтобы запросить этот список.

## E. Получатели в третьей стране и соответствующие или подходящие гарантии и средства, с помощью которых получить их копию или там, где они были предоставлены (Статья 13 (1) лит. г, 46 (1), 46 (2) лит. в ОРЗД)

Все компании и филиалы, входящие в нашу группу (далее упоминается) к «групповым компаниям»), которые имеют свое коммерческое предприятие или офис в третьей стране, могут принадлежать получателям персональных данных. У нас можно запросить список всех компаний или получателей группы.

Согласно Статье 46 (1) ОРЗД, контроллер или процессор может передавать личные данные только в третью страну, если контроллер или процессор предоставил соответствующие гарантии, и при условии, что для субъектов данных доступны действующие права субъекта данных и эффективные средства правовой защиты. Соответствующие меры предосторожности могут быть предоставлены без какого-либо специального разрешения от надзорного органа посредством стандартных договорных положений, Статья 46 (2) лит. с ОРЗД.

Стандартные договорные положения Европейского Союза или другие соответствующие меры предосторожности согласовываются со всеми получателями из третьих стран до первой передачи персональных данных. , гарантируется, что гарантируются надлежащие меры защиты,


© All rights reserved by Heiko Maniero.

осуществимые права субъекта данных и эффективные средства правовой защиты для субъектов данных. Каждый субъект данных может получить у нас копию стандартных договорных положений. Стандартные договорные положения также доступны в Официальном журнале Европейского Союза.

Статья 45(3) Общего регламента по защите данных (GDPR) предоставляет Европейской комиссии право посредством имплементационного акта принимать решение о том, что страна за пределами ЕС обеспечивает адекватный уровень защиты. Это означает, что уровень защиты персональных данных в целом эквивалентен уровню защиты в ЕС. В результате принятия решения о достаточном уровне защиты персональные данные могут свободно передаваться из стран ЕС (а также Норвегии, Лихтенштейна и Исландии) в третьи страны без каких-либо препятствий. Аналогичные правила действуют в Великобритании, Швейцарии и некоторых других странах.

В случае если Европейская комиссия или правительство другой страны примет решение о том, что третья страна обеспечивает адекватный уровень защиты, а также о применимых рамках (например, EU-U.S. Data Privacy Framework, Swiss-U.S. Data Privacy Framework, UK Extension to the EU-U.S. Data Privacy Framework), все передачи нами данных членам таких рамочных программ (например, самосертифицированным организациям) будут основываться исключительно на членстве этих организаций в соответствующей рамочной программе. В случае если мы или одна из наших групп компаний является членом такой структуры, все передачи нам или нашей группе компаний основываются исключительно на членстве компании в такой структуре.

Любой субъект данных может получить у нас копию рамочных документов. Кроме того, эти рамки также доступны в Официальном журнале Европейского союза, в опубликованных правовых материалах или на веб-сайтах надзорных органов или других компетентных органов или учреждений.

## F. Период, в течение которого будут храниться личные данные, или, если это невозможно, критерии, используемые для определения этого периода (Статья 13 (2) лит. ОРЗД)

Продолжительность хранения персональных данных заявителей составляет 6 месяцев. Для данных о сотрудниках применяется соответствующий установленный законом срок хранения. По истечении этого периода соответствующие данные обычно удаляются, если они больше не нужны для выполнения контракта или для инициирования контракта.

## G. Наличие права запрашивать у контролера доступ и исправление или удаление персональных данных или ограничение обработки в отношении субъекта данных или объекта обработки, а также право на переносимость данных (Статья 13 (2) лит. B ОРЗД)

Все субъекты данных имеют следующие права:

***Право на доступ***

Каждый субъект данных имеет право на доступ к своим персональным данным. Право на доступ распространяется на все данные, обрабатываемые нами. Право может быть реализовано легко


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

и через разумные промежутки времени, чтобы знать и проверять законность обработки (Декламация 63 ОРЗД). Это право вытекает из ст. 15 ОРЗД. Субъект данных может связаться с нами, чтобы воспользоваться правом доступа.

***Право на исправление B***

соответствии со Статьей 16 Предложения 1 ОРЗД субъект данных имеет право без промедления получить от контролера исправление неточных личных данных, касающихся его или ее. Кроме того, Статья 16 Предложения 2 ОРЗД предусматривает, что субъект данных имеет право, с учетом целей обработки, заполнять неполные персональные данные, в том числе посредством предоставления дополнительного заявления. Субъект данных может связаться с нами для осуществления права на исправление.

***Право на удаление (право быть забытым)***

Кроме того, субъекты данных имеют право на стирание и быть забытыми в соответствии со ст. 17 ОРЗД. Это право также может быть реализовано, связавшись с нами. На этом этапе, однако, мы хотели бы указать, что это право не применяется, поскольку обработка необходима для выполнения юридического обязательства, которому подчиняется наша компания, Статья 17 (3) освещена. б ОРЗД. Это означает, что мы можем одобрить заявку на удаление только после истечения установленного законом срока хранения.

***Право на ограничение обработки***

Согласно Статье 18 ОРЗД любой субъект данных имеет право на ограничение обработки. Ограничение обработки может потребоваться, если одно из условий, изложенных в Статье 18 (1), объявление ОРЗД выполнено. Субъект данных может связаться с нами, чтобы воспользоваться правом на ограничение обработки.

***Право на возражение***

Кроме того, ст. 21 GDPR гарантирует право на возражение. Субъект данных может связаться с нами, чтобы воспользоваться правом на возражение.

***Право на переносимость данных***

Ст. 20 ОРЗД предоставляет субъекту данных право на переносимость данных. В соответствии с этим положением субъект данных в условиях, изложенных в Статье 20 (1), лит. а и б ОРЗД - право на получение относящихся к нему персональных данных, которые он или она предоставил контроллеру, в структурированном, широко используемом и машиночитаемом формате и имеет право передавать эти данные другому контроллеру без помех от контроллера, которому были предоставлены персональные данные. Субъект данных может связаться с нами, чтобы воспользоваться правом на переносимость данных.

## H. Наличие права на отзыв согласия в любое время без ущерба для законности обработки, основанной на согласии до его отзыва, если обработка основана на Статье 6 (1) лит. ОРЗД или Статья 9 (2) лит. ОРЗД(Статья 13 (2) лит. в ОРЗД)

Если обработка персональных данных основана на ст. 6 (1) лит. ОРЗД, что имеет место, если субъект данных дал согласие на обработку персональных данных для одной или нескольких конкретных целей или он основан на Статье 9 (2) освещен. ОРЗД, который регулирует явное согласие на обработку специальных категорий персональных данных, субъект данных в


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

соответствии со Статьей 7 (3) Предложения 1 ОРЗД имеет право отозвать свое согласие в любое время.

Отзыв согласия не влияет на законность обработки, основанной на согласии до его отзыва, Статья 7 (3) Предложение 2 ОРЗД. Изъять его так же легко, как и дать согласие, ст. 7 (3) Предложение 4 ОРЗД. Следовательно, отзыв согласия всегда может происходить так же, как было дано согласие, или любым другим способом, который субъект данных считает более простым. В современном информационном обществе, вероятно, самый простой способ отозвать согласие - это простое электронное письмо. Если субъект данных хочет отозвать свое согласие, нам достаточно простого электронного письма. В качестве альтернативы субъект данных может выбрать любой другой способ сообщить о своем отзыве согласия.

## I. Право подать жалобу в надзорный орган (Статья 13 (2) лит. Г, 77 (1) ОРЗД)

Как контролирующий, мы обязаны уведомить субъект данных о праве подать жалобу в надзорный орган, Статья 13 (2) лит. г ОРЗД. Право на подачу жалобы в надзорный орган регулируется Статьей 77 (1) ОРЗД. Согласно этому положению, без ущерба для любого другого административного или судебного средства правовой защиты, каждый субъект данных имеет право подать жалобу в орган надзора, в частности в государстве-члене своего обычного места жительства, места работы или места работы. предполагаемое нарушение, если субъект данных считает, что обработка относящихся к нему персональных данных нарушает Общие положения о защите данных. Право на подачу жалобы в надзорный орган ограничивалось законодательством Союза только таким образом, что оно может быть реализовано только в одном надзорном органе (Декламация 141 Предложения 1 ОРЗД). Это правило направлено на то, чтобы избежать двойных жалоб одного и того же субъекта данных на один и тот же вопрос. Если субъект данных хочет подать жалобу на нас, мы просим связаться только с одним надзорным органом.

## J. Предоставление персональных данных в качестве законодательного или договорного требования; Требование, необходимое для заключения договора; Обязательство субъекта данных предоставлять персональные данные; возможные последствия непредоставления таких данных (ст. 13 (2) лит. е ОРЗД)

Мы разъясняем, что предоставление персональных данных частично требуется законом (например, налоговые правила) или также может быть результатом договорных положений (например, информация о договорный партнер).

Иногда может потребоваться заключить договор о том, что субъект данных предоставляет нам персональные данные, которые впоследствии должны быть обработаны нами. Субъект данных, например, обязан предоставить нам персональные данные, когда наша компания заключает с ним договор. Непредоставление персональных данных приведет к тому, что договор с субъектом данных не может быть заключен.

Прежде чем личные данные будут предоставлены субъектом данных, субъект данных должен связаться с нами. Мы уточняем субъекту данных, требуется ли предоставление персональных данных по закону или договору или необходимо для заключения договора, есть ли обязательство предоставлять персональные данные и последствия непредоставления персональных данных ,


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

### K. Наличие автоматизированного процесса принятия решений, включая профилирование, о котором говорится в Статье 22 (1) и (4) ОРЗД, и, по крайней мере, в этих случаях, содержательную информацию о соответствующей логике, а также о значении и предполагаемых последствиях такая обработка для субъекта данных (Статья 13 (2), лит. д ОРЗД)

Как ответственная компания, мы обычно не используем автоматизированное принятие решений или профилирование. Если в исключительных случаях мы осуществляем автоматизированное принятие решений или профилирование, мы информируем об этом субъекта данных либо отдельно, либо через подраздел в нашей политике конфиденциальности (на нашем сайте). В этом случае действует следующее:

Автоматизированное принятие решений - включая профилирование - может иметь место, если (1) это необходимо для заключения или исполнения договора между субъектом данных и нами, или (2) это разрешено законодательством Союза или государства-члена, которому мы подчиняемся и которое также устанавливает соответствующие меры для защиты прав и свобод и законных интересов субъекта данных, или (3) это основано на явном согласии субъекта данных.

В случаях, указанных в статье 22(2)(a) и (c) GDPR, мы должны принять соответствующие меры для защиты прав и свобод субъекта данных и его законных интересов. В этих случаях вы имеете право на вмешательство человека со стороны контроллера, на выражение своей точки зрения и на оспаривание принятого решения.

Содержательная информация о задействованной логике, а также о значении и предполагаемых последствиях такой обработки для субъекта данных изложена в нашей политике конфиденциальности.

## II. Соответствие требованиям в отношении информации, когда личные данные не собираются от субъекта данных (Статья 14 ОРЗД)

### A. Идентификационные данные и контактные данные контролера (Статья 14 (1) лит. ОРЗД

См. Выше

### B. Контактные данные данных Офицер по защите (Статья 14 (1), лит. б ОРЗД)

См. Выше


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## C. Цели обработки, для которых предназначены персональные данные, а также правовое основание для обработки (Статья 14 (1), лит. в ОРЗД)

Для заявителя Данные, не собранные от субъекта данных, целью обработки данных является проведение экспертизы заявки в процессе набора персонала. Для этой цели мы можем обрабатывать данные, не полученные от вас. На основе данных, обработанных в процессе найма, мы проверим, приглашены ли вы на собеседование (часть процесса отбора). Если вы наняты нами, данные заявителя автоматически преобразуются в данные о сотрудниках. Для данных о сотрудниках целью обработки данных является выполнение трудового договора или соблюдение других правовых норм, применимых к трудовым отношениям. Данные о работниках хранятся после прекращения трудовых отношений для соблюдения законных сроков хранения.

Правовой основой для обработки данных является статья 6 (1) лит. б и д ОРЗД, Статья 9 (2) лит. б и ж ОРЗД, Статья 88 (1) ОРЗД и национальное законодательство, например, для Германии, Раздел 26 ФЗЗД (Федеральный закон о защите данных).

## D. Категории соответствующих персональных данных (Статья 14 (1) лит. г ОРЗД)

Данные заявителя Данные о сотрудниках

## E. Категории получателей персональных данных (Статья 14 (1) лит. д ОРЗД)

Государственные органы

Внешние органы

Другие внешние органы

Внутренние обработка

Внутригрупповая обработка

Другие органы

Список наших обработчиков и получателей данных в третьих странах и, при необходимости, международных организаций публикуется на нашем сайте или может быть запрошен у нас бесплатно. Пожалуйста, свяжитесь с нашим сотрудником по защите данных, чтобы запросить этот список.

## F. Получатели в третьей стране и соответствующие или подходящие гарантии и средства, с помощью которых можно получить их копию или когда они были предоставлены (Статья 14 (1), лит. д, 46 (1), 46 (2) лит. в ОРЗД)

Получатели персональных данных могут принадлежать всем компаниям и филиалам, входящим в нашу группу (далее именуемым «компании группы»), которые имеют свои коммерческие


© All rights reserved by Heiko Maniero.

предприятия или офис в третьей стране. , У нас можно запросить список всех компаний или получателей группы.

Согласно Статье 46 (1) ОРЗД, контроллер или процессор может передавать личные данные только в третью страну, если контроллер или процессор предоставил соответствующие гарантии, и при условии, что для субъектов данных доступны действующие права субъекта данных и эффективные средства правовой защиты. Соответствующие меры предосторожности могут быть предоставлены без какого-либо специального разрешения от надзорного органа посредством стандартных положений о защите данных, Статья 46 (2) освещена. с ОРЗД.

Стандартные договорные положения Европейского Союза или другие соответствующие меры предосторожности согласовываются со всеми получателями из третьих стран до первой передачи персональных данных. Следовательно, гарантируется, что гарантируются надлежащие меры защиты, осуществимые права субъекта данных и эффективные средства правовой защиты для субъектов данных. Каждый субъект данных может получить у нас копию стандартных договорных положений. Стандартные договорные положения также доступны в Официальном журнале Европейского Союза.

Статья 45(3) Общего регламента по защите данных (GDPR) предоставляет Европейской комиссии право посредством имплементационного акта принимать решение о том, что страна за пределами ЕС обеспечивает адекватный уровень защиты. Это означает, что уровень защиты персональных данных в целом эквивалентен уровню защиты в ЕС. В результате принятия решения о достаточном уровне защиты персональные данные могут свободно передаваться из стран ЕС (а также Норвегии, Лихтенштейна и Исландии) в третьи страны без каких-либо препятствий. Аналогичные правила действуют в Великобритании, Швейцарии и некоторых других странах.

В случае если Европейская комиссия или правительство другой страны примет решение о том, что третья страна обеспечивает адекватный уровень защиты, а также о применимых рамках (например, EU-U.S. Data Privacy Framework, Swiss-U.S. Data Privacy Framework, UK Extension to the EU-U.S. Data Privacy Framework), все передачи нами данных членам таких рамочных программ (например, самосертифицированным организациям) будут основываться исключительно на членстве этих организаций в соответствующей рамочной программе. В случае если мы или одна из наших групп компаний является членом такой структуры, все передачи нам или нашей группе компаний основываются исключительно на членстве компании в такой структуре.

Любой субъект данных может получить у нас копию рамочных документов. Кроме того, эти рамки также доступны в Официальном журнале Европейского союза, в опубликованных правовых материалах или на веб-сайтах надзорных органов или других компетентных органов или учреждений.

## G. Период, в течение которого будут храниться персональные данные, или, если это невозможно, критерии, используемые для определения этого периода (Статья 14 (2) лит. ОРЗД).

Срок хранения персональных данных заявителей составляет 6 месяцев. Для данных о сотрудниках применяется соответствующий установленный законом срок хранения. По истечении этого периода соответствующие данные обычно удаляются, если они больше не нужны для выполнения контракта или для инициирования контракта.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## H. Уведомление о законных интересах, преследуемых контролером или третьей стороной, если обработка основана на Статье 6 (1) лит. E ОРЗД (ст. 14 (2) лит. б ОРЗД) В

соответствии со Статьей 6 (1) лит. E ОРЗД, обработка должна быть законной, только если обработка необходима для целей законных интересов, преследуемых контролером или третьей стороной, за исключением случаев, когда такие интересы перекрываются интересами или основными правами и свободами субъекта данных, которые требуют защиты. личных данных. Согласно Декламация 47 Предложения 2 ОРЗД, законный интерес может существовать в тех случаях, когда существует релевантная и надлежащая связь между субъектом данных и контроллером, например, в ситуациях, когда субъект данных является клиентом контроллера. Во всех случаях, когда наша компания обрабатывает данные заявителя на основании Статьи 6 (1), освещается. е ОРЗД, наш законный интерес - это найм подходящего персонала и специалистов.

## I. Наличие права запрашивать у контролера доступ и исправление или стирание персональных данных или ограничение обработки, касающейся субъекта данных и объекта обработки, а также право на переносимость данных (Статья 14 (2) лит. в) ОРЗД)

Все субъекты данных имеют следующие права:

***Право на доступ***

Каждый субъект данных имеет право на доступ к своим персональным данным. Право на доступ распространяется на все данные, обрабатываемые нами. Право может быть реализовано легко и через разумные промежутки времени, чтобы знать и проверять законность обработки (Декламация 63 ОРЗД). Это право вытекает из ст. 15 ОРЗД. Субъект данных может связаться с нами, чтобы воспользоваться правом доступа.

***Право на исправление***

В соответствии со Статьей 16 предложения 1 ОРЗД субъект данных имеет право без промедления получить от контролера исправление неточных личных данных, касающихся его или ее. Кроме того, Статья 16 предложения 2 ОРЗД предусматривает, что субъект данных имеет право, с учетом целей обработки, заполнять неполные персональные данные, в том числе посредством предоставления дополнительного заявления. Субъект данных может связаться с нами для осуществления права на исправление.

***Право на удаление (право быть забытым)***

Кроме того, субъекты данных имеют право на стирание и быть забытыми в соответствии со ст. 17 ОРЗД. Это право также может быть реализовано, связавшись с нами. На этом этапе, однако, мы хотели бы указать, что это право не применяется, поскольку обработка необходима для выполнения юридического обязательства, которому подчиняется наша компания, Статья 17 (3) лит. б ОРЗД. Это означает, что мы можем одобрить заявку на удаление только после истечения установленного законом срока хранения.

***Право на ограничение обработки***

Согласно Статье 18 ОРЗД любой субъект данных имеет право на ограничение обработки. Ограничение обработки может потребоваться, если одно из условий, изложенных в Статье 18 (1), объявление ОРЗД выполнено. Субъект данных может связаться с нами, чтобы воспользоваться правом на ограничение обработки.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

***Право на возражение***

Кроме того, ст. 21 ОРЗД гарантирует право на возражение. Субъект данных может связаться с нами, чтобы воспользоваться правом на возражение.

***Право на переносимость данных***

Ст. 20 ОРЗД предоставляет субъекту данных право на переносимость данных. Согласно этому положению субъект данных в условиях, изложенных в Статье 20 (1), освещен. а и б ОРЗД - право на получение относящихся к нему персональных данных, которые он или она предоставил контроллеру, в структурированном, широко используемом и машиночитаемом формате и имеет право передавать эти данные другому контроллеру без помех от контроллера, которому были предоставлены персональные данные. Субъект данных может связаться с нами, чтобы воспользоваться правом на переносимость данных.

## J. Наличие права на отзыв согласия в любое время, не затрагивая законность обработки, основанной на согласии до его отзыва, если обработка основана на Статье 6 (1) лит. или статья 9 (2) лит. ОРЗД (ст. 14 (2) лит. г ОРЗД)

Если обработка персональных данных основана на ст. 6 (1) ОРЗД, что имеет место, если субъект данных дал согласие на обработку персональных данных для одной или нескольких конкретных целей или он основан на Статье 9 (2) лит. ОРЗД, который регулирует явное согласие на обработку специальных категорий персональных данных, субъект данных в соответствии со Статьей 7 (3) Предложения 1 ОРЗД имеет право отозвать свое согласие в любое время.

Отзыв согласия не влияет на законность обработки, основанной на согласии до его отзыва, Статья 7 (3) Предложение 2 ОРЗД. Изъять его так же легко, как и дать согласие, ст. 7 (3) Предложение 4 ОРЗД. Следовательно, отзыв согласия всегда может происходить так же, как было дано согласие, или любым другим способом, который субъект данных считает более простым. В современном информационном обществе, вероятно, самый простой способ отозвать согласие - это простое электронное письмо. Если субъект данных хочет отозвать свое согласие, нам достаточно простого электронного письма. В качестве альтернативы субъект данных может выбрать любой другой способ сообщить о своем отзыве согласия.

## K. Право подать жалобу в надзорный орган (Статья 14 (2) и т. д. 77 (1) ОРЗД)

Как контролирующий, мы обязаны уведомить субъект данных о праве подать жалобу в надзорный орган, Статья 14 (2) лит. д ОРЗД. Право на подачу жалобы в надзорный орган регулируется Статьей 77 (1) ОРЗД. Согласно этому положению, без ущерба для любого другого административного или судебного средства правовой защиты, каждый субъект данных имеет право подать жалобу в орган надзора, в частности в государстве-члене своего обычного места жительства, места работы или места работы. предполагаемое нарушение, если субъект данных считает, что обработка относящихся к нему персональных данных нарушает Общие положения о защите данных. Право на подачу жалобы в надзорный орган ограничивалось только законодательством Союза таким образом, что оно может быть реализовано только перед одним надзорным органом (Декламация 141 Предложения 1 ОРЗД). Это правило направлено на то, чтобы избежать двойных жалоб одного и того же субъекта данных на один и тот же вопрос. Если субъект данных хочет подать жалобу на нас, мы просим связаться только с одним надзорным органом.


© All rights reserved by Heiko Maniero.

## L. Источник, из которого происходят персональные данные, и, если применимо, получены ли они из общедоступных источников (Статья 14 (2), лит. Д ОРЗД)

В принципе, личные данные собираются непосредственно от субъекта данных или в сотрудничестве с органом (например, поиск данных из официального реестра). Другие данные по темам данных получено из передач группы компаний. В контексте этой общей информации наименование точных источников, из которых получены личные данные, либо невозможно, либо может привести к непропорциональным усилиям по смыслу ст. 14 (5) лит. б ОРЗД. В принципе, мы не собираем личные данные из общедоступных источников.

Любой субъект данных может связаться с нами в любое время, чтобы получить более подробную информацию о точных источниках персональных данных, касающихся его или ее. Если источник личных данных не может быть предоставлен субъекту данных из-за того, что использовались различные источники, должна быть предоставлена общая информация (Декламация 61 Предложения 4 ОРЗД).

## M. Наличие автоматизированного процесса принятия решений, включая профилирование, о котором говорится в статье 22 (1) и (4) ОРЗД, и, по крайней мере, в этих случаях, содержательную информацию о соответствующей логике, а также о значении и предполагаемых последствиях такая обработка для субъекта данных (Статья 14 (2) лит. Ё ОРЗД)

Как ответственная компания, мы обычно не используем автоматизированное принятие решений или профилирование. Если в исключительных случаях мы осуществляем автоматизированное принятие решений или профилирование, мы информируем об этом субъекта данных либо отдельно, либо через подраздел в нашей политике конфиденциальности (на нашем сайте). В этом случае действует следующее:

Автоматизированное принятие решений - включая профилирование - может иметь место, если (1) это необходимо для заключения или исполнения договора между субъектом данных и нами, или (2) это разрешено законодательством Союза или государства-члена, которому мы подчиняемся и которое также устанавливает соответствующие меры для защиты прав и свобод и законных интересов субъекта данных, или (3) это основано на явном согласии субъекта данных.

В случаях, указанных в статье 22(2)(a) и (c) GDPR, мы должны принять соответствующие меры для защиты прав и свобод субъекта данных и его законных интересов. В этих случаях вы имеете право на вмешательство человека со стороны контроллера, на выражение своей точки зрения и на оспаривание принятого решения.

Содержательная информация о задействованной логике, а также о значении и предполагаемых последствиях такой обработки для субъекта данных изложена в нашей политике конфиденциальности.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## III. EU-U.S. Data Privacy Framework (EU-U.S. DPF), UK Extension to the EU-U.S. DPF, Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF)

Если наша организация является сертифицированным членом EU-U.S. Data Privacy Framework (EU-U.S. DPF) и/или UK Extension to the EU-U.S. DPF и/или Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF), применяется следующее:

Мы соблюдаем EU-U.S. Data Privacy Framework (EU-U.S. DPF) и UK Extension to the EU-U.S. DPF, а также Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF), как установлено U.S. Department of Commerce. Наша компания подтвердила Министерству торговли США, что соблюдает EU-U.S. Data Privacy Framework Principles (EU-U.S. DPF Principles) в отношении обработки персональных данных, получаемых из Европейского Союза и Соединенного Королевства на основании EU-U.S. DPF и UK Extension to the EU-U.S. DPF. Наша компания подтвердила Министерству торговли США, что соблюдает Swiss-U.S. Data Privacy Framework Principles (Swiss-U.S. DPF Principles) в отношении обработки персональных данных, получаемых из Швейцарии на основании Swiss-U.S. DPF. В случае противоречия между положениями нашей политики конфиденциальности и EU-U.S. DPF Principles и/или Swiss-U.S. DPF Principles, принципы (Principles) имеют приоритет.

Для получения дополнительной информации о программе Data Privacy Framework (DPF) и для просмотра нашей сертификации, посетите https://www.dataprivacyframework.gov/.

Другие подразделения или дочерние компании нашей компании в США, которые также соблюдают EU-U.S. DPF Principles, включая UK Extension to the EU-U.S. DPF и Swiss-U.S. DPF Principles, если таковые имеются, указаны в нашей политике конфиденциальности.

В соответствии с EU-U.S. DPF и UK Extension to the EU-U.S. DPF, а также Swiss-U.S. DPF, наша компания обязуется сотрудничать с органами, созданными европейскими органами по защите данных и британским Information Commissioner's Office (ICO), а также швейцарским Federal Data Protection and Information Commissioner (EDÖB), и следовать их рекомендациям по нерешенным жалобам на наше обращение с персональными данными, которые мы получаем на основании EU-U.S. DPF и UK Extension to the EU-U.S. DPF и Swiss-U.S. DPF.

Мы информируем затронутых лиц о компетентных европейских органах по защите данных, ответственных за рассмотрение жалоб на обращение нашей организации с персональными данными, в верхней части данного документа о прозрачности, а также о том, что мы предоставляем затронутым лицам адекватные и бесплатные средства правовой защиты.

Мы информируем всех затронутых лиц о том, что наша компания подлежит расследованиям и исполнительным полномочиям Federal Trade Commission (FTC).

Затронутые лица имеют возможность, при определенных условиях, обратиться к обязательному арбитражу. Наша организация обязана разрешать претензии и соблюдать условия согласно Приложению I DPF-Principles, если затронутое лицо запросило обязательный арбитраж, уведомив нашу организацию и следуя процедурам и условиям согласно Приложению I Principles.

Настоящим мы информируем всех затронутых лиц об ответственности нашей организации в случае передачи персональных данных третьим лицам.

Для вопросов затронутых лиц или надзорных органов по защите данных мы назначили местных представителей, указанных в верхней части данного документа о прозрачности.

Мы предоставляем вам возможность выбора (Opt-out), хотите ли вы, чтобы ваши персональные данные (i) были переданы третьим лицам или (ii) использовались для цели, существенно


© All rights reserved by Heiko Maniero.

отличающейся от той(их), для которой(их) они первоначально были собраны или позднее вами одобрены. Ясный, хорошо видимый и легко доступный механизм для реализации вашего права выбора заключается в том, чтобы связаться с нашим уполномоченным по защите данных (DSB) по электронной почте. У вас нет возможности выбора, и мы не обязаны это делать, если данные передаются третьей стороне, которая действует как агент или обработчик данных от нашего имени и по нашим инструкциям. Однако мы всегда заключаем договор с таким агентом или обработчиком данных.

Для чувствительных данных (то есть персональных данных, содержащих информацию о состоянии здоровья, расовом или этническом происхождении, политических взглядах, религиозных или философских убеждениях, членстве в профсоюзе или информацию о сексуальной жизни затронутого лица) мы запрашиваем ваше явное согласие (Opt-in), если эти данные (i) передаются третьим лицам или (ii) используются для иной цели, отличной от той, для которой они были первоначально собраны или для которой вы позднее дали свое согласие, сделав выбор Opt-in. Кроме того, мы рассматриваем все персональные данные, которые получаем от третьих лиц, как чувствительные, если третья сторона идентифицирует и обрабатывает их как чувствительные.

Настоящим мы информируем вас о необходимости раскрытия персональных данных в ответ на законные запросы властей, включая выполнение требований национальной безопасности или правоохранительных органов.

При передаче персональных данных третьей стороне, которая действует как контролер, мы придерживаемся Principles уведомления и выбора. Мы также заключаем договор с третьей стороной, ответственной за обработку, который предусматривает, что эти данные могут обрабатываться только для ограниченных и определенных целей в соответствии с вашим данным согласием и что получатель предоставляет такой же уровень защиты, как и Principles DPF, и уведомляет нас, если обнаружит, что больше не может выполнять это обязательство. Договор предусматривает, что третья сторона, которая является контролером, прекращает обработку или принимает другие соответствующие и адекватные меры для устранения проблемы при установлении такой ситуации.

При передаче персональных данных третьей стороне, которая действует как агент или обработчик данных (i) мы передаем эти данные только для ограниченных и определенных целей; (ii) мы убеждаемся, что агент или обработчик данных обязан обеспечить как минимум такой же уровень защиты данных, как требуют DPF-Principles; (iii) мы предпринимаем соответствующие и адекватные меры, чтобы гарантировать, что агент или обработчик данных действительно обрабатывает переданные персональные данные таким образом, который соответствует нашим обязательствам по DPF-Principles; (iv) мы требуем от агента или обработчика данных уведомить нашу организацию, если он установит, что больше не может выполнять обязательство предоставлять такой же уровень защиты, как это предусмотрено DPF-Principles; (v) после уведомления, в том числе указанного в (iv), мы предпринимаем соответствующие и адекватные шаги, чтобы прекратить несанкционированную обработку и устранить проблему; и (vi) предоставляем DPF Department по запросу резюме или репрезентативный экземпляр соответствующих положений договора о защите данных с этим агентом.

В соответствии с EU-U.S. DPF и/или UK Extension to the EU-U.S. DPF и/или Swiss-U.S. DPF, наша организация обязуется сотрудничать с органами, созданными европейскими надзорными органами по защите данных и британским Information Commissioner's Office (ICO), а также швейцарским Federal Data Protection and Information Commissioner (EDÖB), и следовать их рекомендациям по нерешенным жалобам на наше обращение с персональными данными в рамках трудовых отношений, которые мы получаем на основании EU-U.S. DPF и UK Extension to the EU-U.S. DPF и Swiss-U.S. DPF.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

Все субъекты данных, которые временно находятся в Европейском союзе (ЕС), Европейской экономической зоне (ЕЭЗ) или Соединенном Королевстве или имеют там постоянное место жительства, имеют право на права и права субъектов данных, опубликованные в нашем документе о прозрачности, которые также вытекают из статей 15-22 GDPR, включая право на доступ к персональным данным. Мы разместили эту информацию на всех языках ЕС и ЕЭЗ. Версия на английском языке относится к Соединенному Королевству.

Все субъекты данных, временно проживающие в Швейцарии или имеющие там постоянное место жительства, имеют права и права субъектов данных в соответствии со Швейцарским законом о защите данных (DPA) и Швейцарским положением о защите данных (DPR), которые опубликованы в нашем документе о прозрачности, включая право на доступ к персональным данным. Мы предоставили эту информацию на трех официальных языках Швейцарии (немецком, итальянском и французском).


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

# INDONESIAN: Informasi tentang Pemrosesan Data Pribadi (Pasal 13, 14 GDPR)

Bapak atau Ibu yang terhormat,

Data pribadi setiap individu yang berada dalam hubungan kontraktual, prakontraktual, atau hubungan lainnya dengan perusahaan kami layak mendapatkan perlindungan khusus. Tujuan kami adalah untuk menjaga tingkat perlindungan data kami ke standar yang tinggi. Oleh karena itu, kami secara rutin mengembangkan konsep perlindungan data dan keamanan data kami.

Tentu saja, kami mematuhi ketentuan hukum tentang perlindungan data. Menurut Pasal 13, 14 GDPR, pengontrol memenuhi persyaratan informasi spesifik saat mengumpulkan data pribadi. Dokumen ini memenuhi kewajiban tersebut.

Terminologi peraturan hukum memang rumit. Sayangnya, penggunaan istilah-istilah hukum tidak dapat ditiadakan dalam penyusunan dokumen ini. Oleh karena itu, kami ingin menunjukkan bahwa Anda selalu dipersilakan untuk menghubungi kami untuk semua pertanyaan mengenai dokumen ini, istilah atau formulasi yang digunakan.

## I. Kepatuhan terhadap persyaratan informasi ketika data pribadi dikumpulkan dari subjek data (Pasal 13 GDPR)

### A. Identitas dan detail kontak pengontrol (Pasal 13(1) lit. a GDPR)

Lihat di atas

### B. Rincian kontak Petugas Perlindungan Data (Pasal 13(1) lit. b GDPR)

Lihat di atas

### C. Tujuan pemrosesan yang menjadi tujuan data pribadi serta dasar hukum pemrosesan (Pasal 13(1) lit. c GDPR)

Tujuan pemrosesan data pribadi adalah penanganan semua operasi yang menyangkut pengontrol, pelanggan, calon pelanggan, mitra bisnis atau hubungan kontraktual atau pra-kontraktual lainnya antara kelompok-kelompok yang disebutkan (dalam arti luas) atau kewajiban hukum pengontrol.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

Pasal 6(1) lit. a GDPR berfungsi sebagai dasar hukum untuk operasi pemrosesan yang untuknya kami memperoleh persetujuan untuk tujuan pemrosesan tertentu. 6(1) lit. a GDPR berfungsi sebagai dasar hukum untuk operasi pemrosesan yang kami peroleh persetujuannya untuk tujuan pemrosesan tertentu. Jika pemrosesan data pribadi diperlukan untuk pelaksanaan kontrak di mana subjek data adalah pihak, seperti halnya, misalnya, ketika operasi pemrosesan diperlukan untuk penyediaan barang atau untuk menyediakan layanan lain, pemrosesan didasarkan pada Pasal 6 (1) lit. b GDPR. Hal yang sama berlaku untuk operasi pemrosesan yang diperlukan untuk melakukan tindakan pra-kontrak, misalnya dalam hal pertanyaan tentang produk atau layanan kami. Apakah perusahaan kami tunduk pada kewajiban hukum yang mengharuskan pemrosesan data pribadi, seperti untuk pemenuhan kewajiban pajak, pemrosesan didasarkan pada Art. 6(1) lit. c GDPR.

Dalam kasus yang jarang terjadi, pemrosesan data pribadi mungkin diperlukan untuk melindungi kepentingan vital subjek data atau orang lain. Ini akan menjadi kasusnya, misalnya, jika seorang pengunjung terluka di perusahaan kami dan nama, usia, data asuransi kesehatan, atau informasi penting lainnya harus diteruskan ke dokter, rumah sakit, atau pihak ketiga lainnya. Maka pemrosesan akan didasarkan pada Art. 6(1) lit. d GDPR.

Jika pemrosesan diperlukan untuk pelaksanaan tugas yang dilakukan demi kepentingan umum atau dalam pelaksanaan wewenang resmi yang diberikan kepada pengendali, dasar hukumnya adalah Art. 6(1) lit. e GDPR.

Terakhir, operasi pemrosesan dapat didasarkan pada Pasal 6 (1) lit. f GDPR. Dasar hukum ini digunakan untuk operasi pemrosesan yang tidak tercakup oleh salah satu dasar hukum yang disebutkan di atas, jika pemrosesan diperlukan untuk tujuan kepentingan sah yang dikejar oleh perusahaan kami atau oleh pihak ketiga, kecuali jika kepentingan tersebut dikesampingkan oleh kepentingan atau hak-hak dasar dan kebebasan subjek data yang memerlukan perlindungan data pribadi. Operasi pemrosesan semacam itu secara khusus diizinkan karena telah disebutkan secara khusus oleh legislator Eropa. Dia menganggap bahwa kepentingan yang sah dapat diasumsikan jika subjek data adalah klien pengontrol (Recital 47 Kalimat 2 GDPR).

## D. Apabila pemrosesan didasarkan pada Pasal 6(1) lit. f GDPR, kepentingan sah yang dikejar oleh pengontrol atau oleh pihak ketiga (Pasal 13(1) lit. d GDPR)

Jika pemrosesan data pribadi didasarkan pada Pasal 6 (1) lit. f GDPR, kepentingan sah kami adalah untuk menjalankan bisnis kami demi kesejahteraan semua karyawan dan pemegang saham kami.

## E. Kategori penerima data pribadi (Pasal 13 (1) lit. e GDPR)

Otoritas publik


© All rights reserved by Heiko Maniero.

Badan eksternal

Badan eksternal lebih lanjut

Pemrosesan internal

Pemrosesan intrakelompok

Badan-badan lain

Daftar pemroses dan penerima data kami di negara ketiga dan, jika berlaku, organisasi internasional dipublikasikan di situs web kami atau dapat diminta dari kami secara gratis. Silakan hubungi petugas perlindungan data kami untuk meminta daftar ini.

## F. Penerima di negara ketiga dan perlindungan yang sesuai atau cocok serta cara untuk mendapatkan salinannya atau di mana salinan tersebut telah tersedia (Pasal 13(1) lit. f, 46(1), 46 (2) lit. c GDPR)

Semua perusahaan dan cabang yang merupakan bagian dari grup kami (selanjutnya disebut sebagai "perusahaan grup") yang memiliki tempat usaha atau kantor di negara ketiga dapat menjadi bagian dari penerima data pribadi. Daftar semua perusahaan grup atau penerima dapat diminta dari kami.

Menurut Pasal 46(1) GDPR, pengontrol atau pemroses dapat mentransfer data pribadi hanya ke negara ketiga jika pengontrol atau pemroses telah memberikan perlindungan yang sesuai, dan dengan syarat bahwa hak subjek data yang dapat ditegakkan dan upaya hukum yang efektif untuk subjek data tersedia. Perlindungan yang sesuai dapat diberikan tanpa memerlukan otorisasi khusus dari otoritas pengawas melalui klausul kontrak standar, Pasal 46 (2) lit. c GDPR.

Klausul kontrak standar Uni Eropa atau perlindungan lain yang sesuai disepakati dengan semua penerima dari negara ketiga sebelum transmisi pertama data pribadi. Akibatnya, dipastikan bahwa perlindungan yang sesuai, hak subjek data yang dapat ditegakkan, dan upaya hukum yang efektif untuk subjek data dijamin. Setiap subjek data dapat memperoleh salinan klausul kontrak standar dari kami. Klausul kontrak standar juga tersedia dalam Jurnal Resmi Uni Eropa.

Pasal 45 (3) Peraturan Perlindungan Data Umum (GDPR) memberikan hak kepada Komisi Eropa untuk memutuskan, melalui sebuah undang-undang pelaksanaan, bahwa negara di luar UE memberikan tingkat perlindungan yang memadai. Ini berarti tingkat perlindungan untuk data pribadi yang secara luas setara dengan yang ada di UE. Efek dari keputusan yang menemukan tingkat perlindungan yang memadai adalah bahwa data pribadi dapat mengalir dengan bebas dari UE (dan Norwegia, Liechtenstein, dan Islandia) ke negara ketiga tanpa hambatan lebih lanjut. Aturan serupa berlaku di Inggris, Swiss, dan beberapa negara lain.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

Apabila Komisi Eropa atau pemerintah negara lain memutuskan bahwa negara ketiga memberikan tingkat perlindungan yang memadai, dan kerangka kerja yang berlaku (misalnya EU-U.S. Data Privacy Framework, Swiss-U.S. Data Privacy Framework, UK Extension to the EU-U.S. Data Privacy Framework), maka semua pemindahan yang kami lakukan kepada anggota kerangka kerja tersebut (misalnya, entitas yang bersertifikasi mandiri) hanya didasarkan pada keanggotaan entitas tersebut dalam kerangka kerja yang relevan. Apabila kami atau salah satu entitas grup kami adalah anggota kerangka kerja tersebut, semua transfer kepada kami atau entitas grup kami hanya didasarkan pada keanggotaan entitas dalam kerangka kerja tersebut.

Setiap subjek data dapat memperoleh salinan kerangka kerja dari kami. Selain itu, kerangka kerja ini juga tersedia di Jurnal Resmi Uni Eropa atau dalam materi hukum yang diterbitkan atau di situs web otoritas pengawas atau otoritas atau lembaga yang berwenang lainnya.

## G. Jangka waktu penyimpanan data pribadi, atau jika tidak memungkinkan, kriteria yang digunakan untuk menentukan jangka waktu tersebut (Pasal 13(2) lit. a GDPR)

Kriteria yang digunakan untuk menentukan periode penyimpanan data pribadi adalah periode retensi hukum masing-masing. Setelah berakhirnya periode tersebut, data terkait secara rutin dihapus, selama tidak lagi diperlukan untuk pemenuhan kontrak atau inisiasi kontrak.

Jika tidak ada periode retensi menurut undang-undang, kriterianya adalah periode retensi kontraktual atau internal.

## H. Adanya hak untuk meminta dari pengontrol akses ke dan perbaikan atau penghapusan data pribadi atau pembatasan pemrosesan mengenai subjek data atau untuk menolak pemrosesan serta hak atas portabilitas data (Pasal 13 (2) lit. b GDPR)

Semua subjek data memiliki hak-hak berikut ini:

***Hak untuk mengakses***

Setiap subjek data memiliki hak untuk mengakses data pribadi mengenai dirinya. Hak untuk mengakses meluas ke semua data yang diproses oleh kami. Hak ini dapat dilakukan dengan mudah dan pada interval yang wajar, untuk mengetahui, dan memverifikasi, keabsahan pemrosesan (Resital 63 GDPR). Hak ini dihasilkan dari Art. 15 GDPR. Subjek data dapat menghubungi kami untuk menggunakan hak untuk mengakses.

***Hak untuk perbaikan***

Menurut Pasal 16 Kalimat 1 GDPR, subjek data berhak untuk memperoleh dari pengendali tanpa penundaan yang tidak semestinya, perbaikan data pribadi yang tidak akurat mengenai dirinya. Selain itu, Pasal 16 Kalimat 2 GDPR menetapkan bahwa subjek data berhak, dengan mempertimbangkan tujuan


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

pemrosesan, untuk melengkapi data pribadi yang tidak lengkap, termasuk dengan cara memberikan pernyataan tambahan. Subjek data dapat menghubungi kami untuk menggunakan hak perbaikan.

***Hak untuk menghapus (hak untuk dilupakan)***

Selain itu, subjek data berhak atas hak untuk dihapus dan dilupakan berdasarkan Art. 17 GDPR. Hak ini juga dapat dilakukan dengan menghubungi kami. Namun, pada titik ini, kami ingin menunjukkan bahwa hak ini tidak berlaku sejauh pemrosesan diperlukan untuk memenuhi kewajiban hukum yang menjadi subjek perusahaan kami, Pasal 17 (3) lit. b GDPR. Ini berarti bahwa kami dapat menyetujui permohonan untuk menghapus hanya setelah berakhirnya periode penyimpanan menurut undang-undang.

***Hak atas pembatasan pemrosesan***

Menurut Pasal 18 GDPR, setiap subjek data berhak atas pembatasan pemrosesan. Pembatasan pemrosesan dapat diminta jika salah satu syarat yang ditetapkan dalam Pasal 18 (1) lit. a-d GDPR terpenuhi. Subjek data dapat menghubungi kami untuk menggunakan hak pembatasan pemrosesan.

***Hak untuk menolak***

Selanjutnya, Art. 21 GDPR menjamin hak untuk mengajukan keberatan. Subjek data dapat menghubungi kami untuk menggunakan hak untuk menolak.

***Hak atas portabilitas data***

Pasal 20 GDPR memberikan hak portabilitas data kepada subjek data. 20 GDPR memberikan hak portabilitas data kepada subjek data. Berdasarkan ketentuan ini, subjek data memiliki hak untuk menerima data pribadi mengenai dirinya, yang telah diberikannya kepada pengontrol, dalam format terstruktur, umum digunakan, dan dapat dibaca mesin, dan memiliki hak untuk mengirimkan data tersebut ke pengontrol lain tanpa hambatan dari pengontrol tempat data pribadi telah diberikan. Subjek data dapat menghubungi kami untuk menggunakan hak portabilitas data.

## I. Adanya hak untuk menarik persetujuan kapan saja, tanpa memengaruhi keabsahan pemrosesan berdasarkan persetujuan sebelum penarikannya, di mana pemrosesan didasarkan pada Pasal 6(1) lit. a GDPR atau Pasal 9(2) lit. a GDPR (Pasal 13(2) lit. c GDPR)

Jika pemrosesan data pribadi didasarkan pada Art. 6(1) lit. a GDPR, yang merupakan kasusnya, jika subjek data telah memberikan persetujuan untuk pemrosesan data pribadi untuk satu atau lebih tujuan tertentu atau berdasarkan Pasal 9(2) lit. a GDPR, yang mengatur persetujuan eksplisit untuk pemrosesan kategori khusus data pribadi, subjek data memiliki hak untuk menarik persetujuannya kapan saja sesuai dengan Pasal 7(3) Kalimat 1 GDPR.

Penarikan persetujuan tidak akan memengaruhi keabsahan pemrosesan berdasarkan persetujuan sebelum penarikannya, Pasal 7(3) Kalimat 2 GDPR. Penarikan persetujuan harus semudah memberikan persetujuan, Art. 7(3) Kalimat 4 GDPR. Oleh karena itu, penarikan persetujuan selalu dapat dilakukan


© All rights reserved by Heiko Maniero.

dengan cara yang sama seperti persetujuan yang telah diberikan atau dengan cara lain, yang dianggap oleh subjek data lebih sederhana. Dalam masyarakat informasi saat ini, mungkin cara paling sederhana untuk menarik persetujuan adalah email sederhana. Jika subjek data ingin menarik persetujuannya yang diberikan kepada kami, email sederhana kepada kami sudah cukup. Atau, subjek data dapat memilih cara lain untuk mengomunikasikan penarikan persetujuannya kepada kami.

## J. Hak untuk mengajukan keluhan kepada otoritas pengawas (Pasal 13(2) lit. d, 77(1) GDPR)

Sebagai pengendali, kami berkewajiban untuk memberi tahu subjek data tentang hak untuk mengajukan keluhan kepada otoritas pengawas, Pasal 13(2) lit. d GDPR. Hak untuk mengajukan keluhan kepada otoritas pengawas diatur oleh Pasal 77(1) GDPR. Menurut ketentuan ini, tanpa mengesampingkan upaya administratif atau yudisial lainnya, setiap subjek data berhak untuk mengajukan keluhan kepada otoritas pengawas, khususnya di Negara Anggota tempat tinggal, tempat kerja, atau tempat dugaan pelanggaran jika subjek data menganggap bahwa pemrosesan data pribadi yang berkaitan dengannya melanggar Peraturan Perlindungan Data Umum. Hak untuk mengajukan keluhan kepada otoritas pengawas hanya dibatasi oleh hukum Uni sedemikian rupa, sehingga hanya dapat dilakukan di hadapan satu otoritas pengawas (Recital 141 Kalimat 1 GDPR). Aturan ini dimaksudkan untuk menghindari keluhan ganda dari subjek data yang sama dalam masalah yang sama. Jika subjek data ingin mengajukan keluhan tentang kami, oleh karena itu kami diminta untuk hanya menghubungi satu otoritas pengawas.

## K. Penyediaan data pribadi sebagai persyaratan hukum atau kontrak; Persyaratan yang diperlukan untuk masuk ke dalam kontrak; Kewajiban subjek data untuk memberikan data pribadi; kemungkinan konsekuensi dari kegagalan untuk memberikan data tersebut (Art. 13 (2) lit. e GDPR)

Kami mengklarifikasi bahwa penyediaan data pribadi sebagian diwajibkan oleh hukum (misalnya peraturan pajak) atau juga dapat dihasilkan dari ketentuan kontrak (misalnya informasi tentang mitra kontrak).

Terkadang mungkin diperlukan untuk menyelesaikan kontrak bahwa subjek data memberi kami data pribadi, yang selanjutnya harus diproses oleh kami. Subjek data, misalnya, diwajibkan untuk memberikan data pribadi kepada kami ketika perusahaan kami menandatangani kontrak dengannya. Tidak disediakannya data pribadi akan memiliki konsekuensi bahwa kontrak dengan subjek data tidak dapat diselesaikan.

Sebelum data pribadi diberikan oleh subjek data, subjek data harus menghubungi kami. Kami mengklarifikasi kepada subjek data apakah penyediaan data pribadi diperlukan oleh hukum atau kontrak atau diperlukan untuk kesimpulan kontrak, apakah ada kewajiban untuk memberikan data pribadi dan konsekuensi dari tidak disediakannya data pribadi.


© All rights reserved by Heiko Maniero.

### L. Keberadaan pengambilan keputusan otomatis, termasuk pembuatan profil, sebagaimana dimaksud dalam Pasal 22(1) dan (4) GDPR dan, setidaknya dalam kasus-kasus tersebut, informasi yang berarti tentang logika yang terlibat, serta signifikansi dan konsekuensi yang diperkirakan dari pemrosesan tersebut untuk subjek data (Pasal 13 (2) lit. f GDPR)

Sebagai perusahaan yang bertanggung jawab, biasanya kami tidak menggunakan pengambilan keputusan atau pembuatan profil secara otomatis. Jika, dalam kasus luar biasa, kami melakukan pengambilan keputusan atau pembuatan profil secara otomatis, kami akan memberi tahu subjek data secara terpisah atau melalui subbagian dalam kebijakan privasi kami (di situs web kami). Dalam hal ini, hal berikut ini berlaku:

Pengambilan keputusan otomatis - termasuk pembuatan profil - dapat terjadi jika (1) hal ini diperlukan untuk mengadakan, atau melaksanakan, kontrak antara subjek data dan kami, atau (2) hal ini disahkan oleh hukum Uni atau Negara Anggota tempat kami berada dan yang juga menetapkan langkah-langkah yang sesuai untuk melindungi hak-hak dan kebebasan subjek data dan kepentingan yang sah; atau (3) hal ini didasarkan pada persetujuan eksplisit dari subjek data.

Dalam kasus yang disebutkan dalam Pasal 22 (2) (a) dan (c) GDPR, kami akan menerapkan langkah-langkah yang sesuai untuk melindungi hak dan kebebasan serta kepentingan sah subjek data. Dalam kasus ini, Anda memiliki hak untuk mendapatkan campur tangan manusia dari pihak pengendali, untuk mengekspresikan sudut pandang Anda, dan menentang keputusan tersebut.

Informasi yang berarti tentang logika yang terlibat, serta signifikansi dan konsekuensi yang diperkirakan dari pemrosesan tersebut untuk subjek data diatur dalam kebijakan privasi kami.

## II. Kepatuhan terhadap persyaratan informasi ketika data pribadi tidak dikumpulkan dari subjek data (Pasal 14 GDPR)

### A. Identitas dan detail kontak pengontrol (Pasal 14(1) lit. a GDPR)

Lihat di atas

### B. Perincian kontak Petugas Perlindungan Data (Pasal 14(1) lit. b GDPR)

Lihat di atas


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## C. Tujuan pemrosesan yang menjadi tujuan data pribadi serta dasar hukum pemrosesan (Pasal 14(1) lit. c GDPR)

Tujuan pemrosesan data pribadi adalah penanganan semua operasi yang menyangkut pengontrol, pelanggan, calon pelanggan, mitra bisnis atau hubungan kontraktual atau pra-kontraktual lainnya antara kelompok-kelompok yang disebutkan (dalam arti luas) atau kewajiban hukum pengontrol.

Jika pemrosesan data pribadi diperlukan untuk pelaksanaan kontrak di mana subjek data adalah pihak, seperti halnya, misalnya, ketika operasi pemrosesan diperlukan untuk penyediaan barang atau untuk menyediakan layanan lain, pemrosesan didasarkan pada Pasal 6 (1) lit. b GDPR. Hal yang sama berlaku untuk operasi pemrosesan yang diperlukan untuk melakukan tindakan pra-kontrak, misalnya dalam hal pertanyaan tentang produk atau layanan kami. Apakah perusahaan kami tunduk pada kewajiban hukum yang mengharuskan pemrosesan data pribadi, seperti untuk pemenuhan kewajiban pajak, pemrosesan didasarkan pada Art. 6(1) lit. c GDPR.

Dalam kasus yang jarang terjadi, pemrosesan data pribadi mungkin diperlukan untuk melindungi kepentingan vital subjek data atau orang lain. Ini akan menjadi kasusnya, misalnya, jika seorang pengunjung terluka di perusahaan kami dan nama, usia, data asuransi kesehatan, atau informasi penting lainnya harus diteruskan ke dokter, rumah sakit, atau pihak ketiga lainnya. Maka pemrosesan akan didasarkan pada Art. 6(1) lit. d GDPR.

Jika pemrosesan diperlukan untuk pelaksanaan tugas yang dilakukan demi kepentingan umum atau dalam pelaksanaan wewenang resmi yang diberikan kepada pengendali, dasar hukumnya adalah Art. 6(1) lit. e GDPR.

Terakhir, operasi pemrosesan dapat didasarkan pada Pasal 6 (1) lit. f GDPR. Dasar hukum ini digunakan untuk operasi pemrosesan yang tidak tercakup oleh salah satu dasar hukum yang disebutkan di atas, jika pemrosesan diperlukan untuk tujuan kepentingan sah yang dikejar oleh perusahaan kami atau oleh pihak ketiga, kecuali jika kepentingan tersebut dikesampingkan oleh kepentingan atau hak-hak dasar dan kebebasan subjek data yang memerlukan perlindungan data pribadi. Operasi pemrosesan semacam itu secara khusus diizinkan karena telah disebutkan secara khusus oleh legislator Eropa. Dia menganggap bahwa kepentingan yang sah dapat diasumsikan jika subjek data adalah klien pengontrol (Recital 47 Kalimat 2 GDPR).

## D. Kategori data pribadi yang bersangkutan (Pasal 14(1) lit. d GDPR)

Data pelanggan

Data pelanggan potensial

Data karyawan


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

Data pemasok

## E. Kategori penerima data pribadi (Pasal 14 (1) lit. e GDPR)

Otoritas publik

Badan eksternal

Badan eksternal lebih lanjut

Pemrosesan internal

Pemrosesan intrakelompok

Badan-badan lain

Daftar pemroses dan penerima data kami di negara ketiga dan, jika berlaku, organisasi internasional dipublikasikan di situs web kami atau dapat diminta dari kami secara gratis. Silakan hubungi petugas perlindungan data kami untuk meminta daftar ini.

## F. Penerima di negara ketiga dan perlindungan yang sesuai atau cocok serta cara untuk mendapatkan salinannya atau di mana salinan tersebut telah tersedia (Pasal 14(1) lit. f, 46(1), 46(2) lit. c GDPR)

Semua perusahaan dan cabang yang merupakan bagian dari grup kami (selanjutnya disebut sebagai "perusahaan grup") yang memiliki tempat usaha atau kantor di negara ketiga dapat menjadi bagian dari penerima data pribadi. Daftar semua perusahaan grup dapat diminta dari kami.

Menurut Pasal 46(1) GDPR, pengontrol atau pemroses dapat mentransfer data pribadi hanya ke negara ketiga jika pengontrol atau pemroses telah memberikan perlindungan yang sesuai, dan dengan syarat bahwa hak subjek data yang dapat ditegakkan dan upaya hukum yang efektif untuk subjek data tersedia. Perlindungan yang sesuai dapat diberikan tanpa memerlukan otorisasi khusus dari otoritas pengawas melalui klausul perlindungan data standar, Pasal 46 (2) lit. c GDPR.

Klausul kontrak standar Uni Eropa atau perlindungan lain yang sesuai disepakati dengan semua penerima dari negara ketiga sebelum transmisi pertama data pribadi. Akibatnya, dipastikan bahwa perlindungan yang sesuai, hak subjek data yang dapat ditegakkan, dan upaya hukum yang efektif untuk subjek data dijamin. Setiap subjek data dapat memperoleh salinan klausul kontrak standar dari kami. Klausul kontrak standar juga tersedia dalam Jurnal Resmi Uni Eropa.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

Pasal 45 (3) Peraturan Perlindungan Data Umum (GDPR) memberikan hak kepada Komisi Eropa untuk memutuskan, melalui sebuah undang-undang pelaksanaan, bahwa negara di luar UE memberikan tingkat perlindungan yang memadai. Ini berarti tingkat perlindungan untuk data pribadi yang secara luas setara dengan yang ada di UE. Efek dari keputusan yang menemukan tingkat perlindungan yang memadai adalah bahwa data pribadi dapat mengalir dengan bebas dari UE (dan Norwegia, Liechtenstein, dan Islandia) ke negara ketiga tanpa hambatan lebih lanjut. Aturan serupa berlaku di Inggris, Swiss, dan beberapa negara lain.

Apabila Komisi Eropa atau pemerintah negara lain memutuskan bahwa negara ketiga memberikan tingkat perlindungan yang memadai, dan kerangka kerja yang berlaku (misalnya EU-U.S. Data Privacy Framework, Swiss-U.S. Data Privacy Framework, UK Extension to the EU-U.S. Data Privacy Framework), maka semua pemindahan yang kami lakukan kepada anggota kerangka kerja tersebut (misalnya, entitas yang bersertifikasi mandiri) hanya didasarkan pada keanggotaan entitas tersebut dalam kerangka kerja yang relevan. Apabila kami atau salah satu entitas grup kami adalah anggota kerangka kerja tersebut, semua transfer kepada kami atau entitas grup kami hanya didasarkan pada keanggotaan entitas dalam kerangka kerja tersebut.

Setiap subjek data dapat memperoleh salinan kerangka kerja dari kami. Selain itu, kerangka kerja ini juga tersedia di Jurnal Resmi Uni Eropa atau dalam materi hukum yang diterbitkan atau di situs web otoritas pengawas atau otoritas atau lembaga yang berwenang lainnya.

## G. Jangka waktu penyimpanan data pribadi, atau jika tidak memungkinkan, kriteria yang digunakan untuk menentukan jangka waktu tersebut (Pasal 14 (2) lit. a GDPR)

Kriteria yang digunakan untuk menentukan periode penyimpanan data pribadi adalah periode retensi hukum masing-masing. Setelah berakhirnya periode tersebut, data terkait secara rutin dihapus, selama tidak lagi diperlukan untuk pemenuhan kontrak atau inisiasi kontrak.

Jika tidak ada periode retensi menurut undang-undang, kriterianya adalah periode retensi kontraktual atau internal.

## H. Pemberitahuan kepentingan sah yang dikejar oleh pengontrol atau oleh pihak ketiga jika pemrosesan didasarkan pada Pasal 6(1) lit. f GDPR (Pasal 14(2) lit. b GDPR)

Menurut Pasal 6(1) lit. f GDPR, pemrosesan akan sah hanya jika pemrosesan diperlukan untuk tujuan kepentingan sah yang dikejar oleh pengontrol atau oleh pihak ketiga, kecuali jika kepentingan tersebut dikesampingkan oleh kepentingan atau hak-hak dasar dan kebebasan subjek data yang memerlukan perlindungan data pribadi. Menurut Resital 47 Kalimat 2 GDPR, kepentingan yang sah dapat ada jika terdapat hubungan yang relevan dan sesuai antara subjek data dan pengendali, misalnya dalam situasi di mana subjek data adalah klien pengendali. Dalam semua kasus di mana perusahaan kami memproses


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

data pribadi berdasarkan Pasal 6(1) lit. f GDPR, kepentingan sah kami adalah dalam menjalankan bisnis kami demi kesejahteraan semua karyawan dan pemegang saham kami.

## I. Adanya hak untuk meminta dari pengontrol akses ke dan perbaikan atau penghapusan data pribadi atau pembatasan pemrosesan mengenai subjek data dan untuk menolak pemrosesan serta hak atas portabilitas data (Pasal 14 (2) lit. c GDPR)

Semua subjek data memiliki hak-hak berikut ini:

***Hak untuk mengakses***

Setiap subjek data memiliki hak untuk mengakses data pribadi mengenai dirinya. Hak untuk mengakses meluas ke semua data yang diproses oleh kami. Hak ini dapat dilakukan dengan mudah dan pada interval yang wajar, untuk mengetahui, dan memverifikasi, keabsahan pemrosesan (Resital 63 GDPR). Hak ini dihasilkan dari Art. 15 GDPR. Subjek data dapat menghubungi kami untuk menggunakan hak untuk mengakses.

***Hak untuk perbaikan***

Menurut Pasal 16 Kalimat 1 GDPR, subjek data berhak untuk memperoleh dari pengendali tanpa penundaan yang tidak semestinya, perbaikan data pribadi yang tidak akurat mengenai dirinya. Selain itu, Pasal 16 Kalimat 2 GDPR menetapkan bahwa subjek data berhak, dengan mempertimbangkan tujuan pemrosesan, untuk melengkapi data pribadi yang tidak lengkap, termasuk dengan cara memberikan pernyataan tambahan. Subjek data dapat menghubungi kami untuk menggunakan hak perbaikan.

***Hak untuk menghapus (hak untuk dilupakan)***

Selain itu, subjek data berhak atas hak untuk dihapus dan dilupakan berdasarkan Art. 17 GDPR. Hak ini juga dapat dilakukan dengan menghubungi kami. Namun, pada titik ini, kami ingin menunjukkan bahwa hak ini tidak berlaku sejauh pemrosesan diperlukan untuk memenuhi kewajiban hukum yang menjadi subjek perusahaan kami, Pasal 17 (3) lit. b GDPR. Ini berarti bahwa kami dapat menyetujui permohonan untuk menghapus hanya setelah berakhirnya periode penyimpanan menurut undang-undang.

***Hak atas pembatasan pemrosesan***

Menurut Pasal 18 GDPR, setiap subjek data berhak atas pembatasan pemrosesan. Pembatasan pemrosesan dapat diminta jika salah satu syarat yang ditetapkan dalam Pasal 18 (1) lit. a-d GDPR terpenuhi. Subjek data dapat menghubungi kami untuk menggunakan hak pembatasan pemrosesan.

***Hak untuk menolak***

Selanjutnya, Art. 21 GDPR menjamin hak untuk mengajukan keberatan. Subjek data dapat menghubungi kami untuk menggunakan hak untuk menolak.

***Hak atas portabilitas data***

Pasal 20 GDPR memberikan hak portabilitas data kepada subjek data. 20 GDPR memberikan hak portabilitas data kepada subjek data. Menurut ketentuan ini, subjek data memiliki hak untuk menerima


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

data pribadi mengenai dirinya, yang telah diberikannya kepada pengontrol, dalam format terstruktur, umum digunakan, dan dapat dibaca mesin, dan memiliki hak untuk mengirimkan data tersebut ke pengontrol lain tanpa hambatan dari pengontrol tempat data pribadi telah diberikan. Subjek data dapat menghubungi kami untuk menggunakan hak portabilitas data.

## J. Adanya hak untuk menarik persetujuan kapan saja, tanpa memengaruhi keabsahan pemrosesan berdasarkan persetujuan sebelum penarikannya, di mana pemrosesan didasarkan pada Pasal 6(1) lit. a atau Pasal 9(2) lit. a GDPR (Pasal 14(2) lit. d GDPR)

Jika pemrosesan data pribadi didasarkan pada Art. 6(1) lit. a GDPR, yang merupakan kasusnya, jika subjek data telah memberikan persetujuan untuk pemrosesan data pribadi untuk satu atau lebih tujuan tertentu atau berdasarkan Pasal 9(2) lit. a GDPR, yang mengatur persetujuan eksplisit untuk pemrosesan kategori khusus data pribadi, subjek data memiliki hak untuk menarik persetujuannya kapan saja sesuai dengan Pasal 7(3) Kalimat 1 GDPR.

Penarikan persetujuan tidak akan memengaruhi keabsahan pemrosesan berdasarkan persetujuan sebelum penarikannya, Pasal 7(3) Kalimat 2 GDPR. Penarikan persetujuan harus semudah memberikan persetujuan, Art. 7(3) Kalimat 4 GDPR. Oleh karena itu, penarikan persetujuan selalu dapat dilakukan dengan cara yang sama seperti persetujuan yang telah diberikan atau dengan cara lain, yang dianggap oleh subjek data lebih sederhana. Dalam masyarakat informasi saat ini, mungkin cara paling sederhana untuk menarik persetujuan adalah email sederhana. Jika subjek data ingin menarik persetujuannya yang diberikan kepada kami, email sederhana kepada kami sudah cukup. Atau, subjek data dapat memilih cara lain untuk mengomunikasikan penarikan persetujuannya kepada kami.

## K. Hak untuk mengajukan keluhan kepada otoritas pengawas (Pasal 14(2) lit. e, 77(1) GDPR)

Sebagai pengendali, kami berkewajiban untuk memberi tahu subjek data tentang hak untuk mengajukan keluhan kepada otoritas pengawas, Pasal 14(2) lit. e GDPR. Hak untuk mengajukan keluhan kepada otoritas pengawas diatur oleh Pasal 77(1) GDPR. Menurut ketentuan ini, tanpa mengesampingkan upaya administratif atau yudisial lainnya, setiap subjek data berhak untuk mengajukan keluhan kepada otoritas pengawas, khususnya di Negara Anggota tempat tinggal, tempat kerja, atau tempat dugaan pelanggaran jika subjek data menganggap bahwa pemrosesan data pribadi yang berkaitan dengannya melanggar Peraturan Perlindungan Data Umum. Hak untuk mengajukan keluhan kepada otoritas pengawas hanya dibatasi oleh hukum Uni sedemikian rupa, sehingga hanya dapat dilakukan di hadapan satu otoritas pengawas (Recital 141 Kalimat 1 GDPR). Aturan ini dimaksudkan untuk menghindari pengaduan ganda dari subjek data yang sama dalam masalah yang sama. Jika subjek data ingin mengajukan keluhan tentang kami, oleh karena itu kami diminta untuk hanya menghubungi satu otoritas pengawas.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## L. Sumber data pribadi berasal, dan jika berlaku, apakah berasal dari sumber yang dapat diakses publik (Pasal 14(2) lit. f GDPR)

Pada prinsipnya, data pribadi dikumpulkan langsung dari subjek data atau bekerja sama dengan otoritas (misalnya, pengambilan data dari daftar resmi). Data lain tentang subjek data berasal dari transfer grup perusahaan. Dalam konteks informasi umum ini, penamaan sumber yang tepat dari mana data pribadi berasal tidak mungkin atau akan melibatkan upaya yang tidak proporsional dalam arti Art. 14(5) lit. b GDPR. Pada prinsipnya, kami tidak mengumpulkan data pribadi dari sumber yang dapat diakses publik.

Setiap subjek data dapat menghubungi kami kapan saja untuk mendapatkan informasi yang lebih terperinci tentang sumber pasti dari data pribadi mengenai dirinya. Apabila asal data pribadi tidak dapat diberikan kepada subjek data karena berbagai sumber telah digunakan, informasi umum harus diberikan (Resital 61 Kalimat 4 GDPR).

## M. Keberadaan pengambilan keputusan otomatis, termasuk pembuatan profil, sebagaimana dimaksud dalam Pasal 22(1) dan (4) GDPR dan, setidaknya dalam kasus-kasus tersebut, informasi yang berarti tentang logika yang terlibat, serta signifikansi dan konsekuensi yang diperkirakan dari pemrosesan tersebut untuk subjek data (Pasal 14(2) lit. g GDPR)

Sebagai perusahaan yang bertanggung jawab, biasanya kami tidak menggunakan pengambilan keputusan atau pembuatan profil secara otomatis. Jika, dalam kasus luar biasa, kami melakukan pengambilan keputusan atau pembuatan profil secara otomatis, kami akan memberi tahu subjek data secara terpisah atau melalui subbagian dalam kebijakan privasi kami (di situs web kami). Dalam hal ini, hal berikut ini berlaku:

Pengambilan keputusan otomatis - termasuk pembuatan profil - dapat terjadi jika (1) hal ini diperlukan untuk mengadakan, atau melaksanakan, kontrak antara subjek data dan kami, atau (2) hal ini disahkan oleh hukum Uni atau Negara Anggota tempat kami berada dan yang juga menetapkan langkah-langkah yang sesuai untuk melindungi hak-hak dan kebebasan subjek data dan kepentingan yang sah; atau (3) hal ini didasarkan pada persetujuan eksplisit dari subjek data.

Dalam kasus yang disebutkan dalam Pasal 22 (2) (a) dan (c) GDPR, kami akan menerapkan langkah-langkah yang sesuai untuk melindungi hak dan kebebasan serta kepentingan sah subjek data. Dalam kasus ini, Anda memiliki hak untuk mendapatkan campur tangan manusia dari pihak pengendali, untuk mengekspresikan sudut pandang Anda, dan menentang keputusan tersebut.

Informasi yang berarti tentang logika yang terlibat, serta signifikansi dan konsekuensi yang diperkirakan dari pemrosesan tersebut untuk subjek data diatur dalam kebijakan privasi kami.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## III. EU-U.S. Data Privacy Framework (EU-U.S. DPF), UK Extension to the EU-U.S. DPF, Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF)

Jika organisasi kami adalah anggota bersertifikat dari EU-U.S. Data Privacy Framework (EU-U.S. DPF) dan/atau UK Extension to the EU-U.S. DPF dan/atau Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF), maka berlaku hal-hal berikut:

Kami mematuhi EU-U.S. Data Privacy Framework (EU-U.S. DPF) dan UK Extension to the EU-U.S. DPF serta Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF), seperti yang ditetapkan oleh U.S. Department of Commerce. Perusahaan kami telah mengonfirmasi kepada Departemen Perdagangan AS bahwa kami mematuhi EU-U.S. Data Privacy Framework Principles (EU-U.S. DPF Principles) terkait dengan pemrosesan data pribadi yang diterima dari Uni Eropa dan Britania Raya berdasarkan EU-U.S. DPF dan UK Extension to the EU-U.S. DPF. Perusahaan kami telah mengonfirmasi kepada Departemen Perdagangan AS bahwa kami mematuhi Swiss-U.S. Data Privacy Framework Principles (Swiss-U.S. DPF Principles) terkait dengan pemrosesan data pribadi yang diterima dari Swiss berdasarkan Swiss-U.S. DPF. Jika terjadi pertentangan antara ketentuan kebijakan privasi kami dan EU-U.S. DPF Principles dan/atau Swiss-U.S. DPF Principles, maka Principles yang akan berlaku.

Untuk mengetahui lebih lanjut tentang program Data Privacy Framework (DPF) dan untuk melihat sertifikasi kami, silakan kunjungi https://www.dataprivacyframework.gov/.

Unit-unit atau anak perusahaan AS lainnya dari perusahaan kami yang juga mematuhi EU-U.S. DPF Principles, termasuk UK Extension to the EU-U.S. DPF dan Swiss-U.S. DPF Principles, jika ada, disebutkan dalam kebijakan privasi kami.

Sesuai dengan EU-U.S. DPF dan UK Extension to the EU-U.S. DPF serta Swiss-U.S. DPF, perusahaan kami berkomitmen untuk bekerja sama dengan otoritas perlindungan data Eropa dan Information Commissioner's Office (ICO) Inggris serta Federal Data Protection and Information Commissioner (EDÖB) Swiss dan mengikuti nasihat mereka terkait dengan keluhan yang belum terselesaikan tentang cara kami menangani data pribadi yang kami terima berdasarkan EU-U.S. DPF dan UK Extension to the EU-U.S. DPF dan Swiss-U.S. DPF.

Kami memberi tahu individu yang terpengaruh tentang otoritas perlindungan data Eropa yang bertanggung jawab untuk menangani keluhan tentang cara organisasi kami menangani data pribadi di bagian atas dokumen transparansi ini dan bahwa kami memberikan remedi hukum yang memadai dan gratis kepada individu yang terpengaruh.

Kami memberi tahu semua individu yang terpengaruh bahwa perusahaan kami tunduk pada wewenang investigasi dan penegakan Federal Trade Commission (FTC).


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

Individu yang terpengaruh memiliki kemungkinan untuk mengajukan arbitrase yang mengikat dalam kondisi tertentu. Organisasi kami wajib menyelesaikan klaim dan mematuhi ketentuan sesuai Lampiran I dari DPF-Principles, jika individu yang terpengaruh mengajukan arbitrase yang mengikat dengan memberi tahu organisasi kami dan mengikuti prosedur dan ketentuan sesuai Lampiran I dari Principles.

Kami dengan ini memberi tahu semua individu yang terpengaruh tentang tanggung jawab organisasi kami dalam hal pengungkapan data pribadi kepada pihak ketiga.

Untuk pertanyaan dari individu yang terpengaruh atau otoritas perlindungan data, kami telah menunjuk perwakilan lokal yang disebutkan di atas dalam dokumen transparansi ini.

Kami memberi Anda pilihan (Opt-out), apakah data pribadi Anda (i) dibagikan kepada pihak ketiga atau (ii) digunakan untuk tujuan yang berbeda secara signifikan dari tujuan awal dikumpulkan atau yang Anda setujui kemudian. Mekanisme yang jelas, terlihat, dan mudah diakses untuk melaksanakan hak pilihan Anda adalah dengan menghubungi petugas perlindungan data (DSB) kami melalui email. Anda tidak memiliki pilihan dan kami tidak berkewajiban untuk melakukannya jika data tersebut dibagikan kepada pihak ketiga yang bertindak sebagai agen atau pemroses data atas nama kami dan sesuai instruksi kami. Namun, kami selalu membuat kontrak dengan agen atau pemroses data semacam itu.

Untuk data sensitif (yaitu data pribadi yang mencakup informasi tentang kondisi kesehatan, asal ras atau etnis, pendapat politik, keyakinan agama atau filosofi, keanggotaan serikat pekerja, atau informasi tentang kehidupan seksual individu yang bersangkutan) kami meminta persetujuan eksplisit Anda (Opt-in) jika data tersebut (i) dibagikan kepada pihak ketiga atau (ii) digunakan untuk tujuan selain dari tujuan awal dikumpulkan atau yang kemudian Anda setujui dengan membuat pilihan Opt-in. Selain itu, kami memperlakukan semua data pribadi yang kami terima dari pihak ketiga sebagai data sensitif jika pihak ketiga tersebut mengidentifikasi dan memperlakukannya sebagai data sensitif.

Kami dengan ini memberi tahu Anda tentang keharusan untuk mengungkapkan data pribadi sebagai tanggapan atas permintaan yang sah dari otoritas, termasuk pemenuhan persyaratan keamanan nasional atau penegakan hukum.

Dalam hal pengalihan data pribadi kepada pihak ketiga yang bertindak sebagai pengendali, kami mematuhi Principles pemberitahuan dan pilihan. Kami juga membuat kontrak dengan pihak ketiga yang bertanggung jawab atas pemrosesan, yang menetapkan bahwa data tersebut hanya boleh diproses untuk tujuan terbatas dan ditentukan sesuai dengan persetujuan yang Anda berikan dan bahwa penerima memberikan tingkat perlindungan yang sama seperti Principles DPF dan memberi tahu kami jika mereka menemukan bahwa mereka tidak lagi dapat memenuhi kewajiban tersebut. Kontrak menetapkan bahwa pihak ketiga yang bertindak sebagai pengendali, menghentikan pemrosesan atau mengambil langkah-langkah yang sesuai dan memadai untuk memperbaiki masalah jika situasi tersebut ditemukan.

Dalam hal pengalihan data pribadi kepada pihak ketiga yang bertindak sebagai agen atau pemroses data, (i) kami mengalihkan data tersebut hanya untuk tujuan terbatas dan ditentukan; (ii) kami memastikan bahwa agen atau pemroses data tersebut diwajibkan untuk menyediakan tingkat


© All rights reserved by Heiko Maniero.

perlindungan data yang setidaknya setara dengan yang diwajibkan oleh DPF-Principles; (iii) kami mengambil langkah-langkah yang sesuai dan memadai untuk memastikan bahwa agen atau pemroses data tersebut benar-benar memproses data pribadi yang dialihkan dengan cara yang sesuai dengan kewajiban kami sesuai dengan DPF-Principles; (iv) kami meminta agen atau pemroses data untuk memberi tahu organisasi kami jika mereka menemukan bahwa mereka tidak lagi dapat memenuhi kewajiban untuk menyediakan tingkat perlindungan yang sama seperti yang diwajibkan oleh DPF-Principles; (v) setelah pemberitahuan, termasuk yang ada di (iv), kami mengambil langkah-langkah yang sesuai dan memadai untuk menghentikan pemrosesan yang tidak sah dan memperbaiki masalah; dan (vi) kami menyediakan kepada DPF Department atas permintaan, ringkasan atau salinan representatif dari ketentuan perlindungan data yang relevan dalam kontrak dengan agen tersebut.

Sesuai dengan EU-U.S. DPF dan/atau UK Extension to the EU-U.S. DPF dan/atau Swiss-U.S. DPF, organisasi kami berkomitmen untuk bekerja sama dengan badan yang didirikan oleh otoritas perlindungan data Eropa dan Information Commissioner's Office (ICO) Inggris, serta Federal Data Protection and Information Commissioner (EDÖB) Swiss, dan mengikuti nasihat mereka terkait dengan keluhan yang belum terselesaikan tentang cara kami menangani data pribadi dalam konteks hubungan kerja yang kami terima berdasarkan EU-U.S. DPF dan UK Extension to the EU-U.S. DPF dan Swiss-U.S. DPF.

Semua subjek data yang untuk sementara waktu berada di Uni Eropa (UE), Wilayah Ekonomi Eropa (EEA), atau Inggris Raya, atau yang berdomisili atau memiliki tempat tinggal di sana, berhak atas hak-hak dan hak-hak subjek data yang dipublikasikan dalam Dokumen Transparansi kami, yang juga muncul dari Pasal 15 hingga 22 GDPR, termasuk hak untuk mengakses data pribadi. Kami telah menyediakan informasi ini dalam semua bahasa Uni Eropa dan EEA. Versi bahasa Inggris berlaku untuk Inggris Raya.

Semua subjek data yang tinggal sementara di Swiss atau berdomisili atau memiliki tempat tinggal biasa di sana berhak atas hak-hak dan hak-hak subjek data di bawah Undang-Undang Perlindungan Data Swiss (DPA) dan Regulasi Perlindungan Data Swiss (DPR) yang dipublikasikan dalam Dokumen Transparansi kami, termasuk hak untuk mengakses data pribadi. Kami telah menyediakan informasi ini dalam tiga bahasa resmi Swiss (Jerman, Italia, dan Prancis).


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

# INDONESIAN: Informasi tentang Pemrosesan Data Pribadi untuk Karyawan dan Pelamar (Pasal 13, 14 GDPR)

Bapak atau Ibu yang terhormat,

Data pribadi karyawan dan pelamar layak mendapatkan perlindungan khusus. Tujuan kami adalah untuk menjaga tingkat perlindungan data kami ke standar yang tinggi. Oleh karena itu, kami secara rutin mengembangkan konsep perlindungan data dan keamanan data kami.

Tentu saja, kami mematuhi ketentuan hukum tentang perlindungan data. Menurut Pasal 13, 14 GDPR, pengontrol memenuhi persyaratan informasi spesifik saat memproses data pribadi. Dokumen ini memenuhi kewajiban tersebut.

Terminologi peraturan hukum itu rumit. Sayangnya, penggunaan istilah-istilah hukum tidak dapat ditiadakan dalam penyusunan dokumen ini. Oleh karena itu, kami ingin menunjukkan bahwa Anda selalu dipersilakan untuk menghubungi kami untuk semua pertanyaan mengenai dokumen ini, istilah yang digunakan atau formulasi.

## I. Kepatuhan terhadap persyaratan informasi ketika data pribadi dikumpulkan dari subjek data (Pasal 13 GDPR)

### A. Identitas dan detail kontak pengontrol (Pasal 13(1) lit. a GDPR)

Lihat di atas

### B. Rincian kontak Petugas Perlindungan Data (Pasal 13(1) lit. b GDPR)

Lihat di atas

### C. Tujuan pemrosesan yang menjadi tujuan data pribadi serta dasar hukum pemrosesan (Pasal 13(1) lit. c GDPR)

Untuk data pelamar, tujuan pemrosesan data adalah untuk melakukan pemeriksaan aplikasi selama proses rekrutmen. Untuk tujuan ini, kami memproses semua data yang Anda berikan. Berdasarkan data yang diserahkan selama proses rekrutmen, kami akan memeriksa apakah Anda diundang untuk wawancara kerja (bagian dari proses seleksi). Dalam hal kandidat yang secara umum cocok, khususnya dalam konteks wawancara kerja, kami memproses data pribadi tertentu lainnya yang Anda berikan, yang penting untuk keputusan seleksi kami. Jika Anda dipekerjakan oleh kami, data pelamar akan secara


© All rights reserved by Heiko Maniero.

otomatis berubah menjadi data karyawan. Sebagai bagian dari proses perekrutan, kami akan memproses data pribadi lainnya tentang Anda yang kami minta dari Anda dan yang diperlukan untuk memulai atau memenuhi kontrak Anda (seperti nomor identifikasi pribadi atau nomor pajak). Untuk data karyawan, tujuan pemrosesan data adalah pelaksanaan kontrak kerja atau kepatuhan terhadap ketentuan hukum lainnya yang berlaku untuk hubungan kerja (misalnya, undang-undang perpajakan) serta penggunaan data pribadi Anda untuk melaksanakan kontrak kerja yang disepakati dengan Anda (misalnya, publikasi nama Anda dan informasi kontak di dalam perusahaan atau kepada pelanggan). Data karyawan disimpan setelah pemutusan hubungan kerja untuk memenuhi periode retensi hukum.

Dasar hukum untuk pemrosesan data adalah Pasal 6 (1) lit. b GDPR, Pasal 9 (2) lit. b dan h GDPR, Pasal 88 (1) GDPR dan undang-undang nasional, seperti untuk Jerman Bagian 26 BDSG (Undang-Undang Perlindungan Data Federal).

## D. Kategori penerima data pribadi (Pasal 13(1) lit. e GDPR)

Otoritas publik

Badan eksternal

Badan eksternal lebih lanjut

Pemrosesan internal

Pemrosesan intrakelompok

Badan-badan lain

Daftar pemroses dan penerima data kami di negara ketiga dan, jika berlaku, organisasi internasional dipublikasikan di situs web kami atau dapat diminta dari kami secara gratis. Silakan hubungi petugas perlindungan data kami untuk meminta daftar ini.

## E. Penerima di negara ketiga dan perlindungan yang sesuai atau cocok serta cara untuk mendapatkan salinannya atau di mana salinan tersebut telah tersedia (Pasal 13(1) lit. f, 46(1), 46 (2) lit. c GDPR)

Semua perusahaan dan cabang yang merupakan bagian dari grup kami (selanjutnya disebut sebagai "perusahaan grup") yang memiliki tempat usaha atau kantor di negara ketiga dapat menjadi bagian dari penerima data pribadi. Daftar semua perusahaan grup atau penerima dapat diminta dari kami.

Menurut Pasal 46(1) GDPR, pengontrol atau pemroses dapat mentransfer data pribadi hanya ke negara ketiga jika pengontrol atau pemroses telah memberikan perlindungan yang sesuai, dan dengan syarat


© All rights reserved by Heiko Maniero.

bahwa hak subjek data yang dapat ditegakkan dan upaya hukum yang efektif untuk subjek data tersedia. Perlindungan yang sesuai dapat diberikan tanpa memerlukan otorisasi khusus dari otoritas pengawas melalui klausul kontrak standar, Pasal 46 (2) lit. c GDPR.

Klausul kontrak standar Uni Eropa atau perlindungan lain yang sesuai disepakati dengan semua penerima dari negara ketiga sebelum transmisi pertama data pribadi. Akibatnya, dipastikan bahwa perlindungan yang sesuai, hak subjek data yang dapat ditegakkan, dan upaya hukum yang efektif untuk subjek data dijamin. Setiap subjek data dapat memperoleh salinan klausul kontrak standar dari kami. Klausul kontrak standar juga tersedia dalam Jurnal Resmi Uni Eropa.

Pasal 45 (3) Peraturan Perlindungan Data Umum (GDPR) memberikan hak kepada Komisi Eropa untuk memutuskan, melalui sebuah undang-undang pelaksanaan, bahwa negara di luar UE memberikan tingkat perlindungan yang memadai. Ini berarti tingkat perlindungan untuk data pribadi yang secara luas setara dengan yang ada di UE. Efek dari keputusan yang menemukan tingkat perlindungan yang memadai adalah bahwa data pribadi dapat mengalir dengan bebas dari UE (dan Norwegia, Liechtenstein, dan Islandia) ke negara ketiga tanpa hambatan lebih lanjut. Aturan serupa berlaku di Inggris, Swiss, dan beberapa negara lain.

Apabila Komisi Eropa atau pemerintah negara lain memutuskan bahwa negara ketiga memberikan tingkat perlindungan yang memadai, dan kerangka kerja yang berlaku (misalnya EU-U.S. Data Privacy Framework, Swiss-U.S. Data Privacy Framework, UK Extension to the EU-U.S. Data Privacy Framework), maka semua pemindahan yang kami lakukan kepada anggota kerangka kerja tersebut (misalnya, entitas yang bersertifikasi mandiri) hanya didasarkan pada keanggotaan entitas tersebut dalam kerangka kerja yang relevan. Apabila kami atau salah satu entitas grup kami adalah anggota kerangka kerja tersebut, semua transfer kepada kami atau entitas grup kami hanya didasarkan pada keanggotaan entitas dalam kerangka kerja tersebut.

Setiap subjek data dapat memperoleh salinan kerangka kerja dari kami. Selain itu, kerangka kerja ini juga tersedia di Jurnal Resmi Uni Eropa atau dalam materi hukum yang diterbitkan atau di situs web otoritas pengawas atau otoritas atau lembaga yang berwenang lainnya.

## F. Periode penyimpanan data pribadi, atau jika tidak memungkinkan, kriteria yang digunakan untuk menentukan periode tersebut (Pasal 13(2) lit. a GDPR)

Durasi penyimpanan data pribadi pelamar adalah 6 bulan. Untuk data karyawan, periode penyimpanan menurut undang-undang masing-masing berlaku. Setelah berakhirnya periode tersebut, data terkait secara rutin dihapus, selama tidak lagi diperlukan untuk pemenuhan kontrak atau inisiasi kontrak.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## G. Keberadaan hak untuk meminta dari pengontrol akses ke dan perbaikan atau penghapusan data pribadi atau pembatasan pemrosesan mengenai subjek data atau untuk menolak pemrosesan serta hak atas portabilitas data (Pasal 13 (2) lit. b GDPR)

Semua subjek data memiliki hak-hak berikut ini:

***Hak untuk mengakses***

Setiap subjek data memiliki hak untuk mengakses data pribadi mengenai dirinya. Hak untuk mengakses meluas ke semua data yang diproses oleh kami. Hak ini dapat dilakukan dengan mudah dan pada interval yang wajar, untuk mengetahui, dan memverifikasi, keabsahan pemrosesan (Resital 63 GDPR). Hak ini dihasilkan dari Art. 15 GDPR. Subjek data dapat menghubungi kami untuk menggunakan hak untuk mengakses.

***Hak untuk perbaikan***

Menurut Pasal 16 Kalimat 1 GDPR, subjek data berhak untuk memperoleh dari pengendali tanpa penundaan yang tidak semestinya, perbaikan data pribadi yang tidak akurat mengenai dirinya. Selain itu, Pasal 16 Kalimat 2 GDPR menetapkan bahwa subjek data berhak, dengan mempertimbangkan tujuan pemrosesan, untuk melengkapi data pribadi yang tidak lengkap, termasuk dengan cara memberikan pernyataan tambahan. Subjek data dapat menghubungi kami untuk menggunakan hak perbaikan.

***Hak untuk menghapus (hak untuk dilupakan)***

Selain itu, subjek data berhak atas hak untuk dihapus dan dilupakan berdasarkan Art. 17 GDPR. Hak ini juga dapat dilakukan dengan menghubungi kami. Namun, pada titik ini, kami ingin menunjukkan bahwa hak ini tidak berlaku sejauh pemrosesan diperlukan untuk memenuhi kewajiban hukum yang menjadi subjek perusahaan kami, Pasal 17 (3) lit. b GDPR. Ini berarti bahwa kami dapat menyetujui permohonan untuk menghapus hanya setelah berakhirnya periode penyimpanan menurut undang-undang.

***Hak atas pembatasan pemrosesan***

Menurut Pasal 18 GDPR, setiap subjek data berhak atas pembatasan pemrosesan. Pembatasan pemrosesan dapat diminta jika salah satu syarat yang ditetapkan dalam Pasal 18 (1) lit. a-d GDPR terpenuhi. Subjek data dapat menghubungi kami untuk menggunakan hak pembatasan pemrosesan.

***Hak untuk menolak***

Selanjutnya, Art. 21 GDPR menjamin hak untuk mengajukan keberatan. Subjek data dapat menghubungi kami untuk menggunakan hak untuk menolak.

***Hak atas portabilitas data***

Pasal 20 GDPR memberikan hak portabilitas data kepada subjek data. 20 GDPR memberikan hak portabilitas data kepada subjek data. Berdasarkan ketentuan ini, subjek data memiliki hak untuk menerima data pribadi mengenai dirinya, yang telah diberikannya kepada pengontrol, dalam format terstruktur, umum digunakan, dan dapat dibaca mesin, dan memiliki hak untuk mengirimkan data tersebut ke pengontrol lain tanpa hambatan dari pengontrol tempat data pribadi telah diberikan. Subjek data dapat menghubungi kami untuk menggunakan hak portabilitas data.


© All rights reserved by Heiko Maniero.

## H. Adanya hak untuk menarik persetujuan kapan saja, tanpa memengaruhi keabsahan pemrosesan berdasarkan persetujuan sebelum penarikannya, di mana pemrosesan didasarkan pada Pasal 6(1) lit. a GDPR atau Pasal 9(2) lit. a GDPR (Pasal 13(2) lit. c GDPR)

Jika pemrosesan data pribadi didasarkan pada Art. 6(1) lit. a GDPR, yang merupakan kasusnya, jika subjek data telah memberikan persetujuan untuk pemrosesan data pribadi untuk satu atau lebih tujuan tertentu atau berdasarkan Pasal 9(2) lit. a GDPR, yang mengatur persetujuan eksplisit untuk pemrosesan kategori khusus data pribadi, subjek data memiliki hak untuk menarik persetujuannya kapan saja sesuai dengan Pasal 7(3) Kalimat 1 GDPR.

Penarikan persetujuan tidak akan memengaruhi keabsahan pemrosesan berdasarkan persetujuan sebelum penarikannya, Pasal 7(3) Kalimat 2 GDPR. Penarikan persetujuan harus semudah memberikan persetujuan, Art. 7(3) Kalimat 4 GDPR. Oleh karena itu, penarikan persetujuan selalu dapat dilakukan dengan cara yang sama seperti persetujuan yang telah diberikan atau dengan cara lain, yang dianggap oleh subjek data lebih sederhana. Dalam masyarakat informasi saat ini, mungkin cara paling sederhana untuk menarik persetujuan adalah email sederhana. Jika subjek data ingin menarik persetujuannya yang telah diberikan kepada kami, email sederhana kepada kami sudah cukup. Atau, subjek data dapat memilih cara lain untuk mengomunikasikan penarikan persetujuannya kepada kami.

## I. Hak untuk mengajukan keluhan kepada otoritas pengawas (Pasal 13(2) lit. d, 77(1) GDPR)

Sebagai pengendali, kami berkewajiban untuk memberi tahu subjek data tentang hak untuk mengajukan keluhan kepada otoritas pengawas, Pasal 13(2) lit. d GDPR. Hak untuk mengajukan keluhan kepada otoritas pengawas diatur oleh Pasal 77(1) GDPR. Menurut ketentuan ini, tanpa mengesampingkan upaya administratif atau yudisial lainnya, setiap subjek data berhak untuk mengajukan keluhan kepada otoritas pengawas, khususnya di Negara Anggota tempat tinggal, tempat kerja, atau tempat dugaan pelanggaran jika subjek data menganggap bahwa pemrosesan data pribadi yang berkaitan dengannya melanggar Peraturan Perlindungan Data Umum. Hak untuk mengajukan keluhan kepada otoritas pengawas hanya dibatasi oleh hukum Uni sedemikian rupa, sehingga hanya dapat dilakukan di hadapan satu otoritas pengawas (Recital 141 Kalimat 1 GDPR). Aturan ini dimaksudkan untuk menghindari keluhan ganda dari subjek data yang sama dalam masalah yang sama. Jika subjek data ingin mengajukan keluhan tentang kami, oleh karena itu kami diminta untuk hanya menghubungi satu otoritas pengawas.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## J. Penyediaan data pribadi sebagai persyaratan hukum atau kontrak; Persyaratan yang diperlukan untuk mengadakan kontrak; Kewajiban subjek data untuk memberikan data pribadi; kemungkinan konsekuensi dari kegagalan untuk memberikan data tersebut (Pasal 13 (2) lit. e GDPR)

Kami mengklarifikasi bahwa penyediaan data pribadi sebagian diwajibkan oleh hukum (misalnya peraturan pajak) atau juga dapat dihasilkan dari ketentuan kontrak (misalnya informasi tentang mitra kontrak).

Terkadang mungkin diperlukan untuk menyelesaikan kontrak bahwa subjek data memberi kami data pribadi, yang selanjutnya harus diproses oleh kami. Subjek data, misalnya, diwajibkan untuk memberikan data pribadi kepada kami ketika perusahaan kami menandatangani kontrak dengannya. Tidak disediakannya data pribadi akan memiliki konsekuensi bahwa kontrak dengan subjek data tidak dapat diselesaikan.

Sebelum data pribadi diberikan oleh subjek data, subjek data harus menghubungi kami. Kami mengklarifikasi kepada subjek data apakah penyediaan data pribadi diperlukan oleh hukum atau kontrak atau diperlukan untuk kesimpulan kontrak, apakah ada kewajiban untuk memberikan data pribadi dan konsekuensi dari tidak disediakannya data pribadi.

## K. Keberadaan pengambilan keputusan otomatis, termasuk pembuatan profil, sebagaimana dimaksud dalam Pasal 22(1) dan (4) GDPR dan, setidaknya dalam kasus tersebut, informasi yang berarti tentang logika yang terlibat, serta signifikansi dan konsekuensi yang diperkirakan dari pemrosesan tersebut untuk subjek data (Pasal 13 (2) lit. f GDPR)

Sebagai perusahaan yang bertanggung jawab, biasanya kami tidak menggunakan pengambilan keputusan atau pembuatan profil secara otomatis. Jika, dalam kasus luar biasa, kami melakukan pengambilan keputusan atau pembuatan profil secara otomatis, kami akan memberi tahu subjek data secara terpisah atau melalui subbagian dalam kebijakan privasi kami (di situs web kami). Dalam hal ini, hal berikut ini berlaku:

Pengambilan keputusan otomatis - termasuk pembuatan profil - dapat terjadi jika (1) hal ini diperlukan untuk mengadakan, atau melaksanakan, kontrak antara subjek data dan kami, atau (2) hal ini disahkan oleh hukum Uni atau Negara Anggota tempat kami berada dan yang juga menetapkan langkah-langkah yang sesuai untuk melindungi hak-hak dan kebebasan subjek data dan kepentingan yang sah; atau (3) hal ini didasarkan pada persetujuan eksplisit dari subjek data.

Dalam kasus yang disebutkan dalam Pasal 22 (2) (a) dan (c) GDPR, kami akan menerapkan langkah-langkah yang sesuai untuk melindungi hak dan kebebasan serta kepentingan sah subjek data. Dalam


© All rights reserved by Heiko Maniero.

kasus ini, Anda memiliki hak untuk mendapatkan campur tangan manusia dari pihak pengendali, untuk mengekspresikan sudut pandang Anda, dan menentang keputusan tersebut.

Informasi yang berarti tentang logika yang terlibat, serta signifikansi dan konsekuensi yang diperkirakan dari pemrosesan tersebut untuk subjek data diatur dalam kebijakan privasi kami.

## II. Kepatuhan terhadap persyaratan informasi ketika data pribadi tidak dikumpulkan dari subjek data (Pasal 14 GDPR)

### A. Identitas dan detail kontak pengontrol (Pasal 14(1) lit. a GDPR)

Lihat di atas

### B. Perincian kontak Petugas Perlindungan Data (Pasal 14(1) lit. b GDPR)

Lihat di atas

### C. Tujuan pemrosesan yang menjadi tujuan data pribadi serta dasar hukum pemrosesan (Pasal 14(1) lit. c GDPR)

Untuk data pelamar yang tidak dikumpulkan dari subjek data, tujuan pemrosesan data adalah untuk melakukan pemeriksaan aplikasi selama proses rekrutmen. Untuk tujuan ini, kami dapat memproses data yang tidak dikumpulkan dari Anda. Berdasarkan data yang diproses selama proses perekrutan, kami akan memeriksa apakah Anda diundang untuk wawancara kerja (bagian dari proses seleksi). Jika Anda dipekerjakan oleh kami, data pelamar akan secara otomatis berubah menjadi data karyawan. Untuk data karyawan, tujuan pemrosesan data adalah pelaksanaan kontrak kerja atau kepatuhan terhadap ketentuan hukum lainnya yang berlaku untuk hubungan kerja. Data karyawan disimpan setelah pemutusan hubungan kerja untuk memenuhi periode retensi hukum.

Dasar hukum untuk pemrosesan data adalah Pasal 6 (1) lit. b dan f GDPR, Pasal 9 (2) lit. b dan h GDPR, Pasal 88 (1) GDPR dan undang-undang nasional, seperti untuk Jerman Bagian 26 BDSG (Undang-Undang Perlindungan Data Federal).

### D. Kategori data pribadi yang bersangkutan (Pasal 14(1) lit. d GDPR)

Data pemohon


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## E. Kategori penerima data pribadi (Pasal 14 (1) lit. e GDPR)

Otoritas publik

Badan eksternal

Badan eksternal lebih lanjut

Pemrosesan internal

Pemrosesan intrakelompok

Badan-badan lain

Daftar pemroses dan penerima data kami di negara ketiga dan, jika berlaku, organisasi internasional dipublikasikan di situs web kami atau dapat diminta dari kami secara gratis. Silakan hubungi petugas perlindungan data kami untuk meminta daftar ini.

## F. Penerima di negara ketiga dan perlindungan yang sesuai atau cocok serta cara untuk mendapatkan salinannya atau di mana salinan tersebut telah tersedia (Pasal 14(1) lit. f, 46(1), 46(2) lit. c GDPR)

Semua perusahaan dan cabang yang merupakan bagian dari grup kami (selanjutnya disebut sebagai "perusahaan grup") yang memiliki tempat usaha atau kantor di negara ketiga dapat menjadi bagian dari penerima data pribadi. Daftar semua perusahaan grup atau penerima dapat diminta dari kami.

Menurut Pasal 46(1) GDPR, pengontrol atau pemroses dapat mentransfer data pribadi hanya ke negara ketiga jika pengontrol atau pemroses telah memberikan perlindungan yang sesuai, dan dengan syarat bahwa hak subjek data yang dapat ditegakkan dan upaya hukum yang efektif untuk subjek data tersedia. Perlindungan yang sesuai dapat diberikan tanpa memerlukan otorisasi khusus dari otoritas pengawas melalui klausul perlindungan data standar, Pasal 46 (2) lit. c GDPR.

Klausul kontrak standar Uni Eropa atau perlindungan lain yang sesuai disepakati dengan semua penerima dari negara ketiga sebelum transmisi pertama data pribadi. Akibatnya, dipastikan bahwa perlindungan yang sesuai, hak subjek data yang dapat ditegakkan, dan upaya hukum yang efektif untuk subjek data dijamin. Setiap subjek data dapat memperoleh salinan klausul kontrak standar dari kami. Klausul kontrak standar juga tersedia dalam Jurnal Resmi Uni Eropa.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

Pasal 45 (3) Peraturan Perlindungan Data Umum (GDPR) memberikan hak kepada Komisi Eropa untuk memutuskan, melalui sebuah undang-undang pelaksanaan, bahwa negara di luar UE memberikan tingkat perlindungan yang memadai. Ini berarti tingkat perlindungan untuk data pribadi yang secara luas setara dengan yang ada di UE. Efek dari keputusan yang menemukan tingkat perlindungan yang memadai adalah bahwa data pribadi dapat mengalir dengan bebas dari UE (dan Norwegia, Liechtenstein, dan Islandia) ke negara ketiga tanpa hambatan lebih lanjut. Aturan serupa berlaku di Inggris, Swiss, dan beberapa negara lain.

Apabila Komisi Eropa atau pemerintah negara lain memutuskan bahwa negara ketiga memberikan tingkat perlindungan yang memadai, dan kerangka kerja yang berlaku (misalnya EU-U.S. Data Privacy Framework, Swiss-U.S. Data Privacy Framework, UK Extension to the EU-U.S. Data Privacy Framework), maka semua pemindahan yang kami lakukan kepada anggota kerangka kerja tersebut (misalnya, entitas yang bersertifikasi mandiri) hanya didasarkan pada keanggotaan entitas tersebut dalam kerangka kerja yang relevan. Apabila kami atau salah satu entitas grup kami adalah anggota kerangka kerja tersebut, semua transfer kepada kami atau entitas grup kami hanya didasarkan pada keanggotaan entitas dalam kerangka kerja tersebut.

Setiap subjek data dapat memperoleh salinan kerangka kerja dari kami. Selain itu, kerangka kerja ini juga tersedia di Jurnal Resmi Uni Eropa atau dalam materi hukum yang diterbitkan atau di situs web otoritas pengawas atau otoritas atau lembaga yang berwenang lainnya.

## G. Jangka waktu penyimpanan data pribadi, atau jika tidak memungkinkan, kriteria yang digunakan untuk menentukan jangka waktu tersebut (Pasal 14 (2) lit. a GDPR)

Durasi penyimpanan data pribadi pelamar adalah 6 bulan. Untuk data karyawan, periode penyimpanan menurut undang-undang masing-masing berlaku. Setelah berakhirnya periode tersebut, data terkait secara rutin dihapus, selama tidak lagi diperlukan untuk pemenuhan kontrak atau inisiasi kontrak.

## H. Pemberitahuan kepentingan sah yang dikejar oleh pengontrol atau oleh pihak ketiga jika pemrosesan didasarkan pada Pasal 6(1) lit. f GDPR (Pasal 14(2) lit. b GDPR)

Menurut Pasal 6(1) lit. f GDPR, pemrosesan akan sah hanya jika pemrosesan diperlukan untuk tujuan kepentingan sah yang dikejar oleh pengontrol atau oleh pihak ketiga, kecuali jika kepentingan tersebut dikesampingkan oleh kepentingan atau hak-hak dasar dan kebebasan subjek data yang memerlukan perlindungan data pribadi. Menurut Resital 47 Kalimat 2 GDPR, kepentingan yang sah dapat ada jika terdapat hubungan yang relevan dan sesuai antara subjek data dan pengendali, misalnya dalam situasi di mana subjek data adalah klien pengendali. Dalam semua kasus di mana perusahaan kami memproses data pelamar berdasarkan Pasal 6(1) lit. f GDPR, kepentingan sah kami adalah mempekerjakan personel dan profesional yang sesuai.


© All rights reserved by Heiko Maniero.

## I. Adanya hak untuk meminta dari pengontrol akses ke dan perbaikan atau penghapusan data pribadi atau pembatasan pemrosesan mengenai subjek data dan untuk menolak pemrosesan serta hak atas portabilitas data (Pasal 14 (2) lit. c GDPR)

Semua subjek data memiliki hak-hak berikut ini:

***Hak untuk mengakses***

Setiap subjek data memiliki hak untuk mengakses data pribadi mengenai dirinya. Hak untuk mengakses meluas ke semua data yang diproses oleh kami. Hak ini dapat dilakukan dengan mudah dan pada interval yang wajar, untuk mengetahui, dan memverifikasi, keabsahan pemrosesan (Resital 63 GDPR). Hak ini dihasilkan dari Art. 15 GDPR. Subjek data dapat menghubungi kami untuk menggunakan hak untuk mengakses.

***Hak untuk perbaikan***

Menurut Pasal 16 Kalimat 1 GDPR, subjek data berhak untuk memperoleh dari pengendali tanpa penundaan yang tidak semestinya, perbaikan data pribadi yang tidak akurat mengenai dirinya. Selain itu, Pasal 16 Kalimat 2 GDPR menetapkan bahwa subjek data berhak, dengan mempertimbangkan tujuan pemrosesan, untuk melengkapi data pribadi yang tidak lengkap, termasuk dengan cara memberikan pernyataan tambahan. Subjek data dapat menghubungi kami untuk menggunakan hak perbaikan.

***Hak untuk menghapus (hak untuk dilupakan)***

Selain itu, subjek data berhak atas hak untuk dihapus dan dilupakan berdasarkan Art. 17 GDPR. Hak ini juga dapat dilakukan dengan menghubungi kami. Namun, pada titik ini, kami ingin menunjukkan bahwa hak ini tidak berlaku sejauh pemrosesan diperlukan untuk memenuhi kewajiban hukum yang menjadi subjek perusahaan kami, Pasal 17 (3) lit. b GDPR. Ini berarti bahwa kami dapat menyetujui permohonan untuk menghapus hanya setelah berakhirnya periode penyimpanan menurut undang-undang.

***Hak atas pembatasan pemrosesan***

Menurut Pasal 18 GDPR, setiap subjek data berhak atas pembatasan pemrosesan. Pembatasan pemrosesan dapat diminta jika salah satu syarat yang ditetapkan dalam Pasal 18 (1) lit. a-d GDPR terpenuhi. Subjek data dapat menghubungi kami untuk menggunakan hak pembatasan pemrosesan.

***Hak untuk menolak***

Selanjutnya, Art. 21 GDPR menjamin hak untuk mengajukan keberatan. Subjek data dapat menghubungi kami untuk menggunakan hak untuk menolak.

***Hak atas portabilitas data***

Pasal 20 GDPR memberikan hak portabilitas data kepada subjek data. 20 GDPR memberikan hak portabilitas data kepada subjek data. Menurut ketentuan ini, subjek data memiliki hak untuk menerima data pribadi mengenai dirinya, yang telah diberikannya kepada pengontrol, dalam format terstruktur, umum digunakan, dan dapat dibaca mesin, dan memiliki hak untuk mengirimkan data tersebut ke


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

pengontrol lain tanpa hambatan dari pengontrol tempat data pribadi telah diberikan. Subjek data dapat menghubungi kami untuk menggunakan hak portabilitas data.

## J. Adanya hak untuk menarik persetujuan kapan saja, tanpa memengaruhi keabsahan pemrosesan berdasarkan persetujuan sebelum penarikannya, di mana pemrosesan didasarkan pada Pasal 6(1) lit. a atau Pasal 9(2) lit. a GDPR (Pasal 14(2) lit. d GDPR)

Jika pemrosesan data pribadi didasarkan pada Art. 6(1) lit. a GDPR, yang merupakan kasusnya, jika subjek data telah memberikan persetujuan untuk pemrosesan data pribadi untuk satu atau lebih tujuan tertentu atau berdasarkan Pasal 9(2) lit. a GDPR, yang mengatur persetujuan eksplisit untuk pemrosesan kategori khusus data pribadi, subjek data memiliki hak untuk menarik persetujuannya kapan saja sesuai dengan Pasal 7(3) Kalimat 1 GDPR.

Penarikan persetujuan tidak akan memengaruhi keabsahan pemrosesan berdasarkan persetujuan sebelum penarikannya, Pasal 7(3) Kalimat 2 GDPR. Penarikan persetujuan harus semudah memberikan persetujuan, Art. 7(3) Kalimat 4 GDPR. Oleh karena itu, penarikan persetujuan selalu dapat dilakukan dengan cara yang sama seperti persetujuan yang telah diberikan atau dengan cara lain, yang dianggap oleh subjek data lebih sederhana. Dalam masyarakat informasi saat ini, mungkin cara paling sederhana untuk menarik persetujuan adalah email sederhana. Jika subjek data ingin menarik persetujuannya yang telah diberikan kepada kami, email sederhana kepada kami sudah cukup. Atau, subjek data dapat memilih cara lain untuk mengomunikasikan penarikan persetujuannya kepada kami.

## K. Hak untuk mengajukan keluhan kepada otoritas pengawas (Pasal 14(2) lit. e, 77(1) GDPR)

Sebagai pengendali, kami berkewajiban untuk memberi tahu subjek data tentang hak untuk mengajukan keluhan kepada otoritas pengawas, Pasal 14(2) lit. e GDPR. Hak untuk mengajukan keluhan kepada otoritas pengawas diatur oleh Pasal 77(1) GDPR. Menurut ketentuan ini, tanpa mengesampingkan upaya administratif atau yudisial lainnya, setiap subjek data berhak untuk mengajukan keluhan kepada otoritas pengawas, khususnya di Negara Anggota tempat tinggal, tempat kerja, atau tempat dugaan pelanggaran jika subjek data menganggap bahwa pemrosesan data pribadi yang berkaitan dengannya melanggar Peraturan Perlindungan Data Umum. Hak untuk mengajukan keluhan kepada otoritas pengawas hanya dibatasi oleh hukum Uni sedemikian rupa, sehingga hanya dapat dilakukan di hadapan satu otoritas pengawas (Recital 141 Kalimat 1 GDPR). Aturan ini dimaksudkan untuk menghindari keluhan ganda dari subjek data yang sama dalam masalah yang sama. Jika subjek data ingin mengajukan keluhan tentang kami, oleh karena itu kami diminta untuk hanya menghubungi satu otoritas pengawas.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## L. Sumber data pribadi berasal, dan jika berlaku, apakah berasal dari sumber yang dapat diakses publik (Pasal 14(2) lit. f GDPR)

Pada prinsipnya, data pribadi dikumpulkan langsung dari subjek data atau bekerja sama dengan otoritas (misalnya, pengambilan data dari daftar resmi). Data lain tentang subjek data berasal dari transfer grup perusahaan. Dalam konteks informasi umum ini, penamaan sumber yang tepat dari mana data pribadi berasal tidak mungkin atau akan melibatkan upaya yang tidak proporsional dalam arti Art. 14(5) lit. b GDPR. Pada prinsipnya, kami tidak mengumpulkan data pribadi dari sumber yang dapat diakses publik.

Setiap subjek data dapat menghubungi kami kapan saja untuk mendapatkan informasi yang lebih terperinci tentang sumber pasti dari data pribadi mengenai dirinya. Apabila asal data pribadi tidak dapat diberikan kepada subjek data karena berbagai sumber telah digunakan, informasi umum harus diberikan (Resital 61 Kalimat 4 GDPR).

## M. Keberadaan pengambilan keputusan otomatis, termasuk pembuatan profil, sebagaimana dimaksud dalam Pasal 22(1) dan (4) GDPR dan, setidaknya dalam kasus-kasus tersebut, informasi yang berarti tentang logika yang terlibat, serta signifikansi dan konsekuensi yang diperkirakan dari pemrosesan tersebut untuk subjek data (Pasal 14(2) lit. g GDPR)

Sebagai perusahaan yang bertanggung jawab, biasanya kami tidak menggunakan pengambilan keputusan atau pembuatan profil secara otomatis. Jika, dalam kasus luar biasa, kami melakukan pengambilan keputusan atau pembuatan profil secara otomatis, kami akan memberi tahu subjek data secara terpisah atau melalui subbagian dalam kebijakan privasi kami (di situs web kami). Dalam hal ini, hal berikut ini berlaku:

Pengambilan keputusan otomatis - termasuk pembuatan profil - dapat terjadi jika (1) hal ini diperlukan untuk mengadakan, atau melaksanakan, kontrak antara subjek data dan kami, atau (2) hal ini disahkan oleh hukum Uni atau Negara Anggota tempat kami berada dan yang juga menetapkan langkah-langkah yang sesuai untuk melindungi hak-hak dan kebebasan subjek data dan kepentingan yang sah; atau (3) hal ini didasarkan pada persetujuan eksplisit dari subjek data.

Dalam kasus yang disebutkan dalam Pasal 22 (2) (a) dan (c) GDPR, kami akan menerapkan langkah-langkah yang sesuai untuk melindungi hak dan kebebasan serta kepentingan sah subjek data. Dalam kasus ini, Anda memiliki hak untuk mendapatkan campur tangan manusia dari pihak pengendali, untuk mengekspresikan sudut pandang Anda, dan menentang keputusan tersebut.

Informasi yang berarti tentang logika yang terlibat, serta signifikansi dan konsekuensi yang diperkirakan dari pemrosesan tersebut untuk subjek data diatur dalam kebijakan privasi kami.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## III. EU-U.S. Data Privacy Framework (EU-U.S. DPF), UK Extension to the EU-U.S. DPF, Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF)

Jika organisasi kami adalah anggota bersertifikat dari EU-U.S. Data Privacy Framework (EU-U.S. DPF) dan/atau UK Extension to the EU-U.S. DPF dan/atau Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF), maka berlaku hal-hal berikut:

Kami mematuhi EU-U.S. Data Privacy Framework (EU-U.S. DPF) dan UK Extension to the EU-U.S. DPF serta Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF), seperti yang ditetapkan oleh U.S. Department of Commerce. Perusahaan kami telah mengonfirmasi kepada Departemen Perdagangan AS bahwa kami mematuhi EU-U.S. Data Privacy Framework Principles (EU-U.S. DPF Principles) terkait dengan pemrosesan data pribadi yang diterima dari Uni Eropa dan Britania Raya berdasarkan EU-U.S. DPF dan UK Extension to the EU-U.S. DPF. Perusahaan kami telah mengonfirmasi kepada Departemen Perdagangan AS bahwa kami mematuhi Swiss-U.S. Data Privacy Framework Principles (Swiss-U.S. DPF Principles) terkait dengan pemrosesan data pribadi yang diterima dari Swiss berdasarkan Swiss-U.S. DPF. Jika terjadi pertentangan antara ketentuan kebijakan privasi kami dan EU-U.S. DPF Principles dan/atau Swiss-U.S. DPF Principles, maka Principles yang akan berlaku.

Untuk mengetahui lebih lanjut tentang program Data Privacy Framework (DPF) dan untuk melihat sertifikasi kami, silakan kunjungi https://www.dataprivacyframework.gov/.

Unit-unit atau anak perusahaan AS lainnya dari perusahaan kami yang juga mematuhi EU-U.S. DPF Principles, termasuk UK Extension to the EU-U.S. DPF dan Swiss-U.S. DPF Principles, jika ada, disebutkan dalam kebijakan privasi kami.

Sesuai dengan EU-U.S. DPF dan UK Extension to the EU-U.S. DPF serta Swiss-U.S. DPF, perusahaan kami berkomitmen untuk bekerja sama dengan otoritas perlindungan data Eropa dan Information Commissioner's Office (ICO) Inggris serta Federal Data Protection and Information Commissioner (EDÖB) Swiss dan mengikuti nasihat mereka terkait dengan keluhan yang belum terselesaikan tentang cara kami menangani data pribadi yang kami terima berdasarkan EU-U.S. DPF dan UK Extension to the EU-U.S. DPF dan Swiss-U.S. DPF.

Kami memberi tahu individu yang terpengaruh tentang otoritas perlindungan data Eropa yang bertanggung jawab untuk menangani keluhan tentang cara organisasi kami menangani data pribadi di bagian atas dokumen transparansi ini dan bahwa kami memberikan remedi hukum yang memadai dan gratis kepada individu yang terpengaruh.

Kami memberi tahu semua individu yang terpengaruh bahwa perusahaan kami tunduk pada wewenang investigasi dan penegakan Federal Trade Commission (FTC).

Individu yang terpengaruh memiliki kemungkinan untuk mengajukan arbitrase yang mengikat dalam kondisi tertentu. Organisasi kami wajib menyelesaikan klaim dan mematuhi ketentuan sesuai Lampiran


© All rights reserved by Heiko Maniero.

I dari DPF-Principles, jika individu yang terpengaruh mengajukan arbitrase yang mengikat dengan memberi tahu organisasi kami dan mengikuti prosedur dan ketentuan sesuai Lampiran I dari Principles.

Kami dengan ini memberi tahu semua individu yang terpengaruh tentang tanggung jawab organisasi kami dalam hal pengungkapan data pribadi kepada pihak ketiga.

Untuk pertanyaan dari individu yang terpengaruh atau otoritas perlindungan data, kami telah menunjuk perwakilan lokal yang disebutkan di atas dalam dokumen transparansi ini.

Kami memberi Anda pilihan (Opt-out), apakah data pribadi Anda (i) dibagikan kepada pihak ketiga atau (ii) digunakan untuk tujuan yang berbeda secara signifikan dari tujuan awal dikumpulkan atau yang Anda setujui kemudian. Mekanisme yang jelas, terlihat, dan mudah diakses untuk melaksanakan hak pilihan Anda adalah dengan menghubungi petugas perlindungan data (DSB) kami melalui email. Anda tidak memiliki pilihan dan kami tidak berkewajiban untuk melakukannya jika data tersebut dibagikan kepada pihak ketiga yang bertindak sebagai agen atau pemroses data atas nama kami dan sesuai instruksi kami. Namun, kami selalu membuat kontrak dengan agen atau pemroses data semacam itu.

Untuk data sensitif (yaitu data pribadi yang mencakup informasi tentang kondisi kesehatan, asal ras atau etnis, pendapat politik, keyakinan agama atau filosofi, keanggotaan serikat pekerja, atau informasi tentang kehidupan seksual individu yang bersangkutan) kami meminta persetujuan eksplisit Anda (Opt-in) jika data tersebut (i) dibagikan kepada pihak ketiga atau (ii) digunakan untuk tujuan selain dari tujuan awal dikumpulkan atau yang kemudian Anda setujui dengan membuat pilihan Opt-in. Selain itu, kami memperlakukan semua data pribadi yang kami terima dari pihak ketiga sebagai data sensitif jika pihak ketiga tersebut mengidentifikasi dan memperlakukannya sebagai data sensitif.

Kami dengan ini memberi tahu Anda tentang keharusan untuk mengungkapkan data pribadi sebagai tanggapan atas permintaan yang sah dari otoritas, termasuk pemenuhan persyaratan keamanan nasional atau penegakan hukum.

Dalam hal pengalihan data pribadi kepada pihak ketiga yang bertindak sebagai pengendali, kami mematuhi Principles pemberitahuan dan pilihan. Kami juga membuat kontrak dengan pihak ketiga yang bertanggung jawab atas pemrosesan, yang menetapkan bahwa data tersebut hanya boleh diproses untuk tujuan terbatas dan ditentukan sesuai dengan persetujuan yang Anda berikan dan bahwa penerima memberikan tingkat perlindungan yang sama seperti Principles DPF dan memberi tahu kami jika mereka menemukan bahwa mereka tidak lagi dapat memenuhi kewajiban tersebut. Kontrak menetapkan bahwa pihak ketiga yang bertindak sebagai pengendali, menghentikan pemrosesan atau mengambil langkah-langkah yang sesuai dan memadai untuk memperbaiki masalah jika situasi tersebut ditemukan.

Dalam hal pengalihan data pribadi kepada pihak ketiga yang bertindak sebagai agen atau pemroses data, (i) kami mengalihkan data tersebut hanya untuk tujuan terbatas dan ditentukan; (ii) kami memastikan bahwa agen atau pemroses data tersebut diwajibkan untuk menyediakan tingkat perlindungan data yang setidaknya setara dengan yang diwajibkan oleh DPF-Principles; (iii) kami mengambil langkah-langkah yang sesuai dan memadai untuk memastikan bahwa agen atau pemroses


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

data tersebut benar-benar memproses data pribadi yang dialihkan dengan cara yang sesuai dengan kewajiban kami sesuai dengan DPF-Principles; (iv) kami meminta agen atau pemroses data untuk memberi tahu organisasi kami jika mereka menemukan bahwa mereka tidak lagi dapat memenuhi kewajiban untuk menyediakan tingkat perlindungan yang sama seperti yang diwajibkan oleh DPF-Principles; (v) setelah pemberitahuan, termasuk yang ada di (iv), kami mengambil langkah-langkah yang sesuai dan memadai untuk menghentikan pemrosesan yang tidak sah dan memperbaiki masalah; dan (vi) kami menyediakan kepada DPF Department atas permintaan, ringkasan atau salinan representatif dari ketentuan perlindungan data yang relevan dalam kontrak dengan agen tersebut.

Sesuai dengan EU-U.S. DPF dan/atau UK Extension to the EU-U.S. DPF dan/atau Swiss-U.S. DPF, organisasi kami berkomitmen untuk bekerja sama dengan badan yang didirikan oleh otoritas perlindungan data Eropa dan Information Commissioner's Office (ICO) Inggris, serta Federal Data Protection and Information Commissioner (EDÖB) Swiss, dan mengikuti nasihat mereka terkait dengan keluhan yang belum terselesaikan tentang cara kami menangani data pribadi dalam konteks hubungan kerja yang kami terima berdasarkan EU-U.S. DPF dan UK Extension to the EU-U.S. DPF dan Swiss-U.S. DPF.

Semua subjek data yang untuk sementara waktu berada di Uni Eropa (UE), Wilayah Ekonomi Eropa (EEA), atau Inggris Raya, atau yang berdomisili atau memiliki tempat tinggal di sana, berhak atas hak-hak dan hak-hak subjek data yang dipublikasikan dalam Dokumen Transparansi kami, yang juga muncul dari Pasal 15 hingga 22 GDPR, termasuk hak untuk mengakses data pribadi. Kami telah menyediakan informasi ini dalam semua bahasa Uni Eropa dan EEA. Versi bahasa Inggris berlaku untuk Inggris Raya.

Semua subjek data yang tinggal sementara di Swiss atau berdomisili atau memiliki tempat tinggal biasa di sana berhak atas hak-hak dan hak-hak subjek data di bawah Undang-Undang Perlindungan Data Swiss (DPA) dan Regulasi Perlindungan Data Swiss (DPR) yang dipublikasikan dalam Dokumen Transparansi kami, termasuk hak untuk mengakses data pribadi. Kami telah menyediakan informasi ini dalam tiga bahasa resmi Swiss (Jerman, Italia, dan Prancis).


© All rights reserved by Heiko Maniero.

# JAPANESE: 個人情報の取り扱いに関するご案内 (GDPR第13条、第14条)

拝啓

当社と契約上、契約前、またはその他の関係にあるすべての個人の個人情報は、特別な保護に値します。当社の目標は、データ保護レベルを高い水準に維持することです。そのため、私たちはデータ保護とデータセキュリティの概念を**日常的に**発展させています。

もちろん、データ保護に関する法定規定を遵守しています。GDPRの第13条、第14条によると、管理者は個人データを収集する際に特定の情報要件を満たしています。この文書は、これらの義務を果たすものです。

法的規制の用語は複雑です。残念ながら、本書の作成にあたり、法律用語の使用を省くことはできませんでした。従って，本書や使用されている用語，製剤に関するご質問は，いつでも弊社にご連絡ください。

## I. データ主体から個人データを収集する際の情報要件の遵守（GDPR第13条）

### A.管理者の身元および連絡先（GDPR第13条1項a号）

上記参照

### B. データ保護責任者の連絡先（GDPR第13条1項b）

上記参照

### C. 個人データが意図される処理の目的および処理の法的根拠（GDPR13条1項c号）

個人情報の処理目的は、管理者、顧客、見込み顧客、ビジネスパートナー、または指定されたグループ（広義の）間のその他の契約上または契約前の関係、または管理者の法的義務に関わるすべての業務を処理することです。


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

Art.6(1) lit. a GDPRは、特定の処理目的について同意を得た処理業務の法的根拠となります。データ対象者が当事者となっている契約の履行に個人データの処理が必要な場合、例えば、商品の供給やその他のサービスの提供に処理業務が必要な場合、処理はGDPR第6条第1項第2号に基づくものとします。例えば、当社の製品またはサービスに関する問い合わせの場合など、契約前の措置を実行するために必要な処理作業についても同様です。当社が、納税義務の履行など、個人データの処理が必要とされる法的義務の対象である場合、その処理はGDPR6(1)cに基づいて行われます。6(1) lit. c GDPRに基づくものです。

まれに、データ対象者または他の自然人の重大な利益を保護するために、個人データの処理が必要となる場合があります。例えば、お客様が当社で負傷され、その方の氏名、年齢、健康保険のデータまたはその他の重要な情報を医師、病院またはその他の第三者に提供しなければならない場合などがこれにあたります。この場合、処理はGDPR第6条1項d号に基づいて行われます。6(1) lit. d GDPRに基づくことになります。

**処理が公共の利益のために、または管理者に与えられた公的権限の行使のために実施される業務の遂行に必要である場合、法的根拠はArt. 6(1) lit. e GDPRです。**

最後に、処理操作は、GDPR第6条1項f号に基づくことができます。この法的根拠は、当社または第三者が追求する正当な利益のために処理が必要な場合、上記のいずれの法的根拠にも該当しない処理業務に使用されます。ただし、かかる利益が、個人データの保護を必要とするデータ主体の利益または基本的権利および自由によって打ち消される場合は、その限りではありません。このような処理操作は、欧州の立法者によって特に言及されているため、特に許容されるものです。同氏は、データ対象者が管理者の顧客である場合、正当な利益が想定されると考えています（Recital 47 Sentence 2 GDPR）。

## D. 処理がGDPR第6条1項f号に基づいている場合、管理者または第三者が追求する正当な利益（GDPR第13条1項d号）。

個人データの処理がGDPR第6条1項f号に基づく場合、当社の正当な利益は、当社の全従業員と株主の幸福のために事業を遂行することです。

## E. 個人データの受領者のカテゴリー（GDPR第13条1項e号）

公的機関

外部団体


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

その他の外部機関

内部処理

グループ内処理

その他の団体

**第三国における当社のデータ処理者およびデータ受領者のリスト、および該当する場合は国際機関のリストは、当社のウェブサイトに掲載されているか、当社から無料で請求することができます。このリストをご希望の場合は、当社のデータ保護担当者までご連絡ください。**

## F. 第三国の受信者と適切なまたは適切な保護措置とそのコピーを取得する手段またはそれらが利用可能になった場所（GDPR13条1項f号、46条1項、46条2項c号）

。

当社のグループ会社（以下、「グループ会社」といいます）のうち、第三国に事業所または事務所を有するすべての会社および支店が、個人データの受領者に属することがあります。すべてのグループ会社または受領者のリストは、弊社に請求することができます。

GDPR第46条1項によると、管理者または処理者が適切なセーフガードを提供し、データ主体の権利およびデータ主体のための効果的な法的救済が利用可能であることを条件として、管理者または処理者は個人データを第三国にのみ移転することができます。適切な保護措置は、標準的な契約条項（GDPR第46条2項c）により、監督当局の特別な許可を必要とせずに提供することができます。

欧州連合の標準契約条項またはその他の適切な保護措置は、個人データを最初に送信する前に、第三国からのすべての受信者と合意されます。その結果、データ対象者のための適切な保護措置、強制力のあるデータ対象者の権利、効果的な法的救済措置が保証されることが保証されます。すべてのデータ対象者は、当社から標準契約条項のコピーを入手することができます。標準契約条項は、欧州連合官報 にも掲載されています。

**一般データ保護規則（GDPR）第45条3項は、欧州委員会に対し、EU域外の国が適切な保護レベルを提供していると実施法によって決定する権利を認めている。これは、EU域内とほぼ同等の個人データ保護レベルを意味する。適切な保護レベルを認める決定の効果として、個人データはEU（およびノルウェー、リヒテンシュタイン、アイスランド）から第三国へ、さらなる障害なく自由に流れることができる。同様の規則は、英国、スイス、その他いくつかの国にも適用される。**

**欧州委員会または他の国の政府が、第三国が適切なレベルの保護を提供すると決定し、適用される枠組み（EU-U.S. Data Privacy Framework, Swiss-U.S. Data Privacy Framework, UK Extension to the EU-**


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

U.S. Data Privacy Framework）が適用される場合、当社による当該枠組みのメンバー（自己認証事業体など）へのすべての移転は、当該事業体が関連枠組みに加盟していることのみに基づきます。当社または当社のグループ事業体の1つが当該フレームワークのメンバーである場合、当社または当社のグループ事業体へのすべての移転は、当該事業体が当該フレームワークのメンバーであることのみに基づきます。

データ対象者は誰でも当社から枠組みを入手することができます。また、欧州連合官報、公表された法的資料、または監督当局やその他の管轄当局・機関のウェブサイトからも入手することができます。

## G. 個人データが保存される期間、またはそれが不可能な場合は、その期間を決定するために使用される基準（GDPR第13条2項a）。

個人データの保存期間を決定するために使用される基準は、それぞれの法定保存期間です。その期間の経過後、契約の履行または契約の開始に必要でなくなった時点で、対応するデータは定期的に削除されます。

法定保存期間がない場合は、契約上の保存期間または内部保存期間が基準となる。

## H. 情報主体に関する個人情報へのアクセスおよび修正、消去、処理の制限を管理者に要求する権利、または処理に異議を唱える権利、ならびにデータのポータビリティに対する権利の存在（GDPR13条2項b号）

すべてのデータ対象者は、以下の権利を有する。

***アクセス権***

各データ対象者は、自分に関する個人データにアクセスする権利を有します。アクセスする権利は、当社が処理するすべてのデータに及びます。この権利は、処理の合法性を認識し、検証するために、合理的な間隔で容易に行使することができます（GDPR説明書63）。この権利は、GDPR第15条に起因するものです。15 GDPRに起因するものです。データ対象者は、アクセス権を行使するために当社に連絡することができます。

***修正する権利***

GDPR第16条第1項により、データ対象者は自分に関する不正確な個人データの修正を管理者から不当に遅れることなく取得する権利を有します。さらに、GDPR第16条第2項では、データ対象者は、処理の目的を考慮し、補足説明の提供を含め、不完全な個人データを補完してもらう権利を有すると定めています。データ対象者は、修正する権利を行使するために当社に連絡することができます。


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

*消去する権利（忘れられる権利）*

さらに、データ対象者は、GDPR第17条に基づき、消去および忘れられる権利を有します。17 GDPRに基づき、データ対象者は消去および忘却の権利を有します。この権利は、当社に連絡することによっても行使することができます。ただし、この時点で、当社が従うべき法的義務を果たすために処理が必要である限り、この権利は適用されないことを指摘したいと思います（GDPR17条3項b号）。つまり、法的な保存期間の終了後にのみ、消去の申請を承認することができます。

*処理の制限に関する権利*

GDPR第18条によると、データ対象者は処理の制限を受ける権利を有します。処理の制限は、GDPR第18条1項a～dに規定された条件のいずれかが満たされた場合に要求することができます。データ対象者は、処理制限の権利を行使するために当社に連絡することができます。

*異議申し立ての権利*

さらに、Art.21 GDPRは異議を唱える権利を保証しています。データ対象者は、異議を唱える権利を行使するために当社に連絡することができます。

*データポータビリティの権利*

Art.20 GDPR はデータ対象者にデータポータビリティの権利を付与しています。この規定に基づき、データ対象者はGDPR第20条1項aおよびbに定める条件の下で、管理者に提供した自分に関する個人データを、構造化された、一般的に使用され機械で読み取り可能な形式で受け取り、個人データが提供された管理者から支障なくそれらのデータを他の管理者に転送する権利を有します。データ対象者は、データポータビリティの権利を行使するために、当社に連絡することができます。

## I. 処理がGDPR第6条1項a号またはGDPR第9条2項a号に基づく場合、撤回前の同意に基づく処理の合法性に影響を与えることなく、いつでも同意を撤回する権利の存在（GDPR第13条2項c号）。

個人データの処理が GDPR 第 6 条第 1 項に基づいている場合。6(1) lit. a GDPR、つまりデータ対象者が一つまたは複数の特定の目的のために個人データの処理に同意した場合、または特殊な個人データの処理に対する明示的な同意を規定する第9条(2) lit. a GDPRに基づいている場合、データ対象者はGDPR第7条(3) 文章1に従っていつでもその同意を撤回する権利を有しているものとします。

同意の撤回が撤回前の同意に基づく処理の合法性に影響を与えることはない、GDPR7条3項2文。同意を撤回することは、同意を与えることと同じくらい容易でなければならない。7(3) センテンス4 GDPR。したがって、同意の取り消しは、同意が与えられたときと同じ方法か、データ対象者がより簡単だと考える他の方法で常に行うことができます。今日の情報社会では、同意を撤回する最も簡単な方法は、おそらく単純な電子メールでしょう。データ対象者が当社に与えた同意を撤回したい場合


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

は、当社宛の簡単な電子メールで十分です。また、データ対象者は、同意の撤回を当社に伝えるために、他の方法を選択することもできます。

## J.監督機関に苦情を申し立てる権利（GDPR13条2項d号、77条1項）

管理者として、当社はデータ対象者に、監督機関に苦情を申し立てる権利（GDPR13条2項d号）を通知する義務があります。監督機関に苦情を申し立てる権利は、GDPR第77条1項により規定されています。この規定によると、データ対象者が自分に関する個人データの処理が一般データ保護規則に違反していると考える場合、他の行政上または司法上の救済手段を損なうことなく、すべてのデータ対象者は、特に自分の居住地、勤務地または違反の疑いがある場所の加盟国の監督当局に苦情を申し立てる権利を有するものとします。監督機関に苦情を申し立てる権利は、EUの法律により、単一の監督機関にのみ行使できるよう制限されています（Recital 141 Sentence 1 GDPR）。この規則は、同じデータ対象者が同じ問題で二重に苦情を申し立てることを避けるためのものです。したがって、データ対象者が当社に対して苦情を申し立てたい場合、当社は単一の監督機関にのみ連絡するよう要請します。

## K.　法的または契約上の要件としての個人データの提供；契約締結に必要な要件；データ主体の個人データ提供義務；当該データを提供しなかった場合に起こりうる結果（GDPR13条2項e号）

個人情報の提供は、法律（例：税法）により要求される場合もあれば、契約上の規定（例：契約相手に関する情報）によりもたらされる場合もあることを明確にします。

データ対象者が当社に個人データを提供し、その後当社がそのデータを処理することが、 契約締結のために必要な場合があります。例えば、当社がデータ対象者と契約を締結する際に、データ対象者は当社に個人データを提 供する義務があります。個人データが提供されない場合、データ対象者との契約は締結されないことになります。

データ対象者が個人データを提供する前に、データ対象者は当社に連絡しなければなりま せん。当社は、データ対象者に対し、個人データの提供が法律または契約によって要求されているか、または契約の締結に必要であるか、個人データを提供する義務があるか、個人データを提供しなかった場合にどのような結果になるかについて明らかにします。


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

### L. GDPR第22条（1）及び（4）に言及されるプロファイリングを含む自動的意思決定の存在、及び少なくともその場合、データ主体に対する当該処理の意義及び想定される結果と同様に、関連する論理に関する意味のある情報（GDPR第13条（2）項f）。

責任ある企業として、通常、当社は自動化された意思決定またはプロファイリングを使用しません。例外的に自動化された意思決定またはプロファイリングを行う場合は、別途、または当社のプライバシー・ポリシー（当社ウェブサイト）の小項目を通じて、データ対象者に通知します。この場合、以下が適用されます：

自動化された意思決定（プロファイリングを含む）は、(1)データ対象者と当社との間で契約を締結または履行するために必要である場合、(2)当社が準拠する連邦法または加盟国の法律により許可され、データ対象者の権利および自由、正当な利益を保護するための適切な措置が定められている場合、または(3)データ対象者の明示的な同意に基づく場合に行われることがあります。

GDPR第22条第2項(a)および(c)に規定されている場合、当社はデータ主体の権利および自由、正当な利益を保護するための適切な措置を講じるものとします。このような場合、お客様は、管理者側からの人的介入を受け、ご自身の見解を表明し、決定に異議を唱える権利を有します。

このような処理がデータ主体にとってどのような意味を持ち、どのような結果をもたらすかについては、当社のプライバシー・ポリシーに記載されています。

## II. データ主体から個人データを収集しない場合の情報要件の遵守（GDPR第14条）

### A.管理者の身元および連絡先（GDPR第14条1項a号

上記参照

### B. データ保護責任者の連絡先（GDPR第14条1項b）

上記参照


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## C. 個人データが意図される処理の目的および処理の法的根拠（GDPR 14条1項c号）

個人情報の処理目的は、管理者、顧客、見込み顧客、ビジネスパートナー、または指定されたグループ（広義の）間のその他の契約上または契約前の関係、または管理者の法的義務に関係するすべての業務の処理です。

データ対象者が当事者となっている契約の履行に個人データの処理が必要な場合、例えば、商品の供給やその他のサービスの提供に処理業務が必要な場合、処理はGDPR第6条1項bに基づきます。例えば、当社の製品またはサービスに関する問い合わせの場合など、契約前の措置を実行するために必要な処理作業についても同様です。当社が、納税義務の履行など、個人データの処理が必要とされる法的義務の対象である場合、その処理はGDPR6(1)cに基づいて行われます。6(1) lit. c GDPRに基づくものです。

まれに、データ対象者または他の自然人の重大な利益を保護するために、個人データの処理が必要となる場合があります。例えば、お客様が当社で負傷され、その方の氏名、年齢、健康保険のデータまたはその他の重要な情報を医師、病院またはその他の第三者に提供しなければならない場合などがこれにあたります。この場合、処理はGDPR第6条1項d号に基づいて行われます。6(1) lit. d GDPRに基づくことになります。

**処理が公共の利益のために、または管理者に与えられた公的権限の行使のために実施される業務の遂行に必要である場合、法的根拠はArt. 6(1) lit. e GDPRです。**

最後に、処理操作は、GDPR第6条1項f号に基づくことができます。この法的根拠は、当社または第三者が追求する正当な利益のために処理が必要な場合、上記のいずれの法的根拠にも該当しない処理業務に使用されます。ただし、かかる利益が、個人データの保護を必要とするデータ主体の利益または基本的権利および自由によって打ち消される場合は、その限りではありません。このような処理操作は、ヨーロッパの立法者によって特に言及されているため、特に許容されるものです。同氏は、データ対象者が管理者の顧客である場合、正当な利益が想定されると考えています（Recital 47 Sentence 2 GDPR）。

## D. 当該個人データのカテゴリー（GDPR第14条1項d）

顧客データ

潜在顧客データ

社員データ


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

仕入先データ

## E. 個人データの受領者のカテゴリー（GDPR14条1項e号）

公的機関

外部団体

その他の外部機関

内部処理

グループ内処理

その他の団体

**第三国における当社のデータ処理者およびデータ受領者のリスト、および該当する場合は国際機関のリストは、当社のウェブサイトに掲載されているか、当社から無料で請求することができます。このリストをご希望の場合は、当社のデータ保護担当者までご連絡ください。**

## F. 第三国の受信者と適切なまたは適切な保護措置とそのコピーを取得する手段またはそれらが利用可能になった場所（GDPR第14条1項f、46条1項、46条2項c）。

当社のグループ会社（以下、「グループ会社」といいます）のうち、第三国に事業所または事務所を有するすべての会社および支店が、個人データの受領者に属する場合があります。すべてのグループ会社のリストは、弊社に請求することができます。

GDPR 第 46(1) 条によると、管理者または処理者は、管理者または処理者が適切なセーフガードを提供し、データ主体の権利およびデータ主体のための有効な法的救済が利用可能であることを条件として、個人データを第三国にのみ移転することができます。適切な保護措置は、標準的なデータ保護条項（GDPR第46条2項c）により、監督官庁の特別な許可を必要とせずに提供することができます。

欧州連合の標準契約条項またはその他の適切な保護措置は、個人データを最初に送信する前に、第三国からのすべての受信者と合意されます。その結果、データ対象者のための適切な保護措置、強制力のあるデータ対象者の権利、効果的な法的救済措置が保証されることが保証されます。すべてのデータ対象者は、当社から標準契約条項のコピーを入手することができます。標準契約条項は、欧州連合官報 にも掲載されています。


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

一般データ保護規則（GDPR）第45条3項は、欧州委員会に対し、EU域外の国が適切な保護レベルを提供していると実施法によって決定する権利を認めている。これは、EU域内とほぼ同等の個人データ保護レベルを意味する。適切な保護レベルを認める決定の効果として、個人データはEU（およびノルウェー、リヒテンシュタイン、アイスランド）から第三国へ、さらなる障害なく自由に流れることができる。同様の規則は、英国、スイス、その他いくつかの国にも適用される。

欧州委員会または他の国の政府が、第三国が適切なレベルの保護を提供すると決定し、適用される枠組み（EU-U.S. Data Privacy Framework, Swiss-U.S. Data Privacy Framework, UK Extension to the EU-U.S. Data Privacy Framework）が適用される場合、当社による当該枠組みのメンバー（自己認証事業体など）へのすべての移転は、当該事業体が関連枠組みに加盟していることのみに基づきます。当社または当社のグループ事業体の1つが当該フレームワークのメンバーである場合、当社または当社のグループ事業体へのすべての移転は、当該事業体が当該フレームワークのメンバーであることのみに基づきます。

データ対象者は誰でも当社から枠組みを入手することができます。また、欧州連合官報、公表された法的資料、または監督当局やその他の管轄当局・機関のウェブサイトからも入手することができます。

## G. 個人データが保存される期間、またはそれが不可能な場合は、その期間を決定するために使用される基準（GDPR第14条2項a）。

個人データの保存期間を決定するために使用される基準は、それぞれの法定保存期間です。その期間の経過後、契約の履行または契約の開始に必要でなくなった時点で、対応するデータは定期的に削除されます。

法定保存期間がない場合は、契約上の保存期間または内部保存期間が基準となる。

## H. 処理がGDPR第6条1項f号（GDPR第14条2項b号）に基づく場合、管理者または第三者が追求する正当な利益についての通知

GDPR第6条1項f号によると、管理者または第三者が追求する正当な利益のために処理が必要な場合に限り、処理は合法であるものとします。GDPRの説明47条2項によれば、データ対象者が管理者の顧客である場合など、データ対象者と管理者の間に適切な関係がある場合、正当な利益が存在する可能性があります。当社がGDPR第6条1項f号に基づいて個人情報を処理するすべての場合において、当社の正当な利益は、当社の全従業員および株主の幸福のために事業を遂行することです。


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## I. 情報主体に関する個人情報へのアクセスおよび修正、消去、処理の制限を管理者に要求する権利、およびデータのポータビリティに対する権利（GDPR第14条2項c号）の存在

すべてのデータ対象者は、以下の権利を有する。

***アクセス権***

各データ対象者は、自分に関する個人データにアクセスする権利を有します。アクセスする権利は、当社が処理するすべてのデータに及びます。この権利は、処理の合法性を認識し、検証するために、合理的な間隔で容易に行使することができます（GDPR説明書63）。この権利は、GDPR第15条に起因するものです。15 GDPRに起因するものです。データ対象者は、アクセス権を行使するために当社に連絡することができます。

***修正する権利***

GDPR第16条第1項により、データ対象者は自分に関する不正確な個人データの修正を管理者から不当に遅れることなく取得する権利を有します。さらに、GDPR第16条第2項では、データ対象者は、処理の目的を考慮し、補足説明の提供を含め、不完全な個人データを補完してもらう権利を有すると定めています。データ対象者は、修正する権利を行使するために当社に連絡することができます。

***消去する権利（忘れられる権利）***

さらに、データ対象者は、GDPR第17条に基づき、消去および忘れられる権利を有します。17 GDPRに基づき、データ対象者は消去および忘却の権利を有します。この権利は、当社に連絡することによっても行使することができます。ただし、この時点で、当社が従うべき法的義務を果たすために処理が必要である限り、この権利は適用されないことを指摘したいと思います（GDPR17条3項b号）。つまり、法的な保存期間の終了後にのみ、消去の申請を承認することができます。

***処理の制限に関する権利***

GDPR第18条によると、データ対象者は処理の制限を受ける権利を有します。処理の制限は、GDPR第18条1項a～dに規定された条件のいずれかが満たされる場合に要求することができます。データ対象者は、処理制限の権利を行使するために当社に連絡することができます。

***異議申し立ての権利***

さらに、Art.21 GDPRは異議を唱える権利を保証しています。データ対象者は、異議を唱える権利を行使するために当社に連絡することができます。

***データポータビリティの権利***

Art.20 GDPR はデータ対象者にデータポータビリティの権利を付与しています。この規定によると、データ対象者は、GDPR第20条1項aおよびbに規定された条件下で、管理者に提供した自分に関する個人データを、構造化された、一般的に使用され機械で読み取り可能な形式で受け取り、個人データ


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

が提供された管理者から支障なくそれらのデータを他の管理者に転送する権利を有します。データ対象者は、データポータビリティの権利を行使するために、当社に連絡することができます。

## J. 処理が6条1項a号または9条2項a号GDPRに基づく場合、撤回前の同意に基づく処理の合法性に影響を与えることなく、いつでも同意を撤回する権利の存在（14条2項d号GDPR）。

個人データの処理が GDPR 第 6 条第 1 項に基づいている場合。6(1) lit. a GDPR、つまりデータ対象者が一つまたは複数の特定の目的のために個人データの処理に同意した場合、または特殊な個人データの処理に対する明示的な同意を規定する第9条(2) lit. a GDPRに基づいている場合、データ対象者はGDPR第7条(3) 文章1に従っていつでもその同意を撤回する権利を有しているものとします。

同意の撤回が、撤回前の同意に基づく処理の合法性に影響を及ぼすことはない、GDPR第7条（3）文2。同意を撤回することは、同意を与えることと同じくらい容易でなければならない。7(3) センテンス4 GDPR。したがって、同意の取り消しは、同意が与えられたときと同じ方法か、データ対象者がより簡単だと考える他の方法で常に行うことができます。今日の情報社会では、同意を撤回する最も簡単な方法は、おそらく単純な電子メールでしょう。データ対象者が当社に与えた同意を撤回したい場合は、当社宛の簡単な電子メールで十分です。また、データ対象者は、同意の撤回を当社に伝えるために、他の方法を選択することもできます。

## K. 監督官庁に苦情を申し立てる権利（GDPR14条2項e号、77条1項）

管理者として、当社はデータ対象者に、監督機関に苦情を申し立てる権利（GDPR第14条2項e号）を通知する義務を負います。監督機関に苦情を申し立てる権利は、GDPR第77条（1）項によって規定されています。この規定によると、データ対象者が自分に関する個人データの処理が一般データ保護規則に違反していると考える場合、他の行政上または司法上の救済手段を損なうことなく、すべてのデータ対象者は、特に自分の居住地、勤務地または違反の疑いがある場所の加盟国の監督機関に苦情を申し立てる権利を有するものとします。監督機関に苦情を申し立てる権利は、EUの法律により、単一の監督機関にのみ行使できるよう制限されています（Recital 141 Sentence 1 GDPR）。この規則は、同じデータ対象者が同じ問題で二重に苦情を申し立てることを避けるためのものです。したがって、データ対象者が当社に対して苦情を申し立てたい場合、当社は単一の監督機関にのみ連絡するよう要請します。


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## L. 個人データの出所、および該当する場合、公にアクセス可能な出所からのものかどうか（GDPR 14条2項f号）

原則として、個人データはデータ対象者から直接、または当局の協力のもとに収集されます（例：公的登録簿からのデータ検索）。データ対象者に関するその他のデータは、グループ会社からの移転により入手されます。この一般的な情報において、個人データの正確な出所を示すことは不可能であり、またGDP第14条5項b号の意味において不相応な労力を要すると思われます。14(5) lit. b GDPRの意味において、個人データの正確な出所を示すことは不可能であるか、または不相応な労力を要すると考えられます。原則として、当社は一般にアクセス可能な情報源から個人データを収集することはありません。

データ対象者はいつでも当社に連絡し、自分に関する個人データの正確な出所について のより詳細な情報を入手することができます。様々な情報源が使用されているため、個人データの出所をデータ対象者に提供できない場合は、一般的な情報を提供する必要があります（Recital 61 Sentence 4 GDPR）。

## M. GDPR第22条1項及び4項に言及されるプロファイリングを含む自動的意思決定の存在、及び少なくともその場合、データ主体にとっての当該処理の意義及び想定される結果とともに、関連する論理に関する意味のある情報（GDPR第14条2項g号）。

**責任ある企業として、通常、当社は自動化された意思決定またはプロファイリングを使用しません。例外的に自動化された意思決定またはプロファイリングを行う場合は、別途、または当社のプライバシー・ポリシー（当社ウェブサイト）の小項目を通じて、データ対象者に通知します。この場合、以下が適用されます：**

**自動化された意思決定（プロファイリングを含む）は、(1)データ対象者と当社との間で契約を締結または履行するために必要である場合、(2)当社が準拠する連邦法または加盟国の法律により許可され、データ対象者の権利および自由、正当な利益を保護するための適切な措置が定められている場合、または(3)データ対象者の明示的な同意に基づく場合に行われることがあります。**

**GDPR第22条第2項(a)および(c)に規定されている場合、当社はデータ主体の権利および自由、正当な利益を保護するための適切な措置を講じるものとします。このような場合、お客様は、管理者側からの人的介入を受け、ご自身の見解を表明し、決定に異議を唱える権利を有します。**

**このような処理がデータ主体にとってどのような意味を持ち、どのような結果をもたらすかについては、当社のプライバシー・ポリシーに記載されています。**


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## III. EU-U.S. Data Privacy Framework (EU-U.S. DPF), UK Extension to the EU-U.S. DPF, Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF)

当組織が EU-U.S. Data Privacy Framework (EU-U.S. DPF) および/または UK Extension to the EU-U.S. DPF および/または Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF) の認定メンバーである場合、以下のことが適用されます：

当社は EU-U.S. Data Privacy Framework (EU-U.S. DPF) および UK Extension to the EU-U.S. DPF 並びに Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF) を、U.S. Department of Commerce が定めたとおりに遵守します。当社は米国商務省に対し、EU-U.S. Data Privacy Framework Principles (EU-U.S. DPF Principles) に従って、EU および UK から EU-U.S. DPF および UK Extension to the EU-U.S. DPF に基づいて受領する個人データの処理に関して遵守していることを確認しました。当社は米国商務省に対し、Swiss-U.S. Data Privacy Framework Principles (Swiss-U.S. DPF Principles) に従って、スイスから Swiss-U.S. DPF に基づいて受領する個人データの処理に関して遵守していることを確認しました。当社のプライバシーポリシーの規定と EU-U.S. DPF Principles および/または Swiss-U.S. DPF Principles の間に矛盾がある場合、Principles が優先されます。

Data Privacy Framework (DPF) プログラムの詳細および当社の認証をご覧になるには、https://www.dataprivacyframework.gov/ にアクセスしてください。

当社の他の米国の部門または子会社も EU-U.S. DPF Principles を遵守しており、UK Extension to the EU-U.S. DPF および Swiss-U.S. DPF Principles を含む場合は、当社のプライバシーポリシーに記載されています。

EU-U.S. DPF および UK Extension to the EU-U.S. DPF 並びに Swiss-U.S. DPF に従い、当社は EU のデータ保護当局および英国の Information Commissioner's Office (ICO) ならびにスイスの Federal Data Protection and Information Commissioner (EDÖB) によって設立された機関と協力し、EU-U.S. DPF および UK Extension to the EU-U.S. DPF および Swiss-U.S. DPF に基づいて当社が受領する個人データの取り扱いに関する未解決の苦情について、その助言に従うことを約束します。

当社は、当社組織の個人データの取り扱いに関する苦情を処理する責任のある欧州のデータ保護当局について、影響を受ける個人にこの透明性ドキュメントの上部で通知し、影響を受ける個人に適切かつ無料の救済措置を提供します。

当社は、影響を受けるすべての個人に対し、当社が Federal Trade Commission (FTC) の調査および執行権限の対象であることを通知します。


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

影響を受ける個人は、特定の条件下で拘束力のある仲裁を求める権利があります。当社は、影響を受ける個人が当社に通知し、Principles の附属書 I に従って手続きおよび条件を遵守することで、拘束力のある仲裁を申請した場合、要求を解決し、DPF-Principles の附属書 I に基づく条件を遵守することを約束します。

当社は、個人データを第三者に提供する場合の当社の責任について、影響を受けるすべての個人に通知します。

影響を受ける個人またはデータ保護監督当局の質問については、この透明性ドキュメントの上部に記載された地域の担当者を指定しました。

当社は、個人データを第三者に提供するかどうか (i) または収集時の目的と実質的に異なる目的で使用するかどうか (ii) について、選択する機会 (Opt-out) を提供します。選択権を行使するための明確で目立ち、簡単にアクセスできるメカニズムは、当社のデータ保護担当者 (DSB) に電子メールで連絡することです。個人データが第三者に提供される場合、当社の指示に従って当社の代理人または処理者として行動する場合には、選択の機会はありませんし、当社もその義務はありません。しかし、当社は常にそのような代理人または処理者と契約を結びます。

敏感なデータ (すなわち、健康状態、人種または民族的出自、政治的見解、宗教的または哲学的信念、労働組合への加入、または対象者の性生活に関する情報を含む個人データ) については、これらのデータを第三者に提供する場合 (i) または収集時の目的と異なる目的で使用する場合 (ii) には、明示的な同意 (Opt-in) を取得します。さらに、第三者から受け取ったすべての個人データを、第三者がそれを敏感なデータとして識別し取り扱う場合、敏感なデータとして扱います。

当社は、当局からの合法的な要求に応じて個人データを開示する必要があることを、ここに通知します。これには、国家安全保障または法執行機関の要件の遵守が含まれます。

個人データを管理者として行動する第三者に転送する場合、当社は通知と選択の原則 (Principles) を遵守します。また、処理を担当する第三者と契約を締結し、これらのデータは限定された特定の目的のためにのみ処理されること、受信者が DPF の原則 (Principles) と同じレベルの保護を提供し、これ以上この義務を履行できないことを確認した場合には当社に通知することを規定します。契約には、管理者としての第三者がそのような状況が確認された場合、処理を停止するか、適切な是正措置を講じることが求められます。

個人データを代理人または処理者として行動する第三者に転送する場合、(i) 当社はこれらのデータを限定された特定の目的のためにのみ転送します。(ii) 代理人または処理者が DPF-Principles で求められるのと同等のデータ保護レベルを提供することを確認します。 (iii) 当社の義務に基づいて代理人または処理者が実際に転送された個人データを処理していることを確認するために適切な措置を講じます。 (iv) 代理人または処理者がこの義務を履行できなくなったことを確認した場合、当社に通知するこ


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

とを要求します。 (v) 通知後 (iv を含む)、不正な処理を停止し是正措置を講じるために適切な措置を講じます。 (vi) DPF Department の要求に応じて、その代理人との契約の関連するデータ保護規定の要約または代表的な例を提供します。

EU-U.S. DPF および/または UK Extension to the EU-U.S. DPF および/または Swiss-U.S. DPF に従い、当社は EU のデータ保護当局および英国の Information Commissioner's Office (ICO) ならびにスイスの Federal Data Protection and Information Commissioner (EDÖB) によって設立された機関と協力し、EU-U.S. DPF および UK Extension to the EU-U.S. DPF および Swiss-U.S. DPF に基づいて当社が受領する個人データの取り扱いに関する未解決の苦情について、その助言に従うことを約束します。

欧州連合（EU）、欧州経済地域（EEA）または英国に一時的に滞在している、あるいはそこに住所または常居所を有するすべてのデータ主体は、個人データにアクセスする権利を含むGDPR第15条から第22条からも生じる、当社の透明性文書で公表されている権利およびデータ主体の権利を有します。当社は、この情報をすべてのEUおよびEEA言語で利用できるようにしています。英語版は英国に適用されます。

スイスに一時的に居住している、またはスイスに住所もしくは常居所を有するすべてのデータ対象者は、個人データにアクセスする権利を含め、当社の透明性文書で公表されているスイスデータ保護法（DPA）およびスイスデータ保護規則（DPR）に基づく権利およびデータ対象者の権利を有します。当社はこの情報をスイスの3つの公用語（ドイツ語、イタリア語、フランス語）で提供しています。


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

# JAPANESE: 従業員および応募者の個人データ処理に関する情報（GDPR第13条、第14条）

拝啓

従業員および応募者の個人情報は、特別に保護されるべきものです。私たちの目標は、データ保護レベルを高い水準に維持することです。そのため、私たちはデータ保護とデータセキュリティの概念を**日常的に**発展させています。

もちろん、データ保護に関する法定規定を遵守しています。GDPRの第13条、第14条によると、管理者は個人データを処理する際に特定の情報要件を満たしています。この文書は、これらの義務を果たすものです。

法的規制の専門用語は複雑です。残念ながら、本書の作成にあたり、法律用語の使用を省くことはできませんでした。従って、この文書、使用されている用語、またはフォーミュレーションに関するすべての質問については、いつでも弊社にご連絡ください。

## I. データ主体から個人データを収集する際の情報要件の遵守（GDPR第13条）

### A.管理者の身元および連絡先（GDPR第13条1項a号）

上記参照

### B.データ保護責任者の連絡先（GDPR第13条1項b）

上記参照

### C. 個人データが意図される処理の目的および処理の法的根拠（GDPR13条1項c号）

応募者のデータについては、データ処理の目的は、採用プロセスにおいて応募者の審査を行うことです。この目的のために、当社は、お客様から提供されたすべてのデータを処理します。採用プロセスで提出されたデータに基づいて、当社は、あなたが面接（選考プロセスの一部）に招待されているか


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

どうかを確認します。一般的に適切な候補者の場合、特に面接の際に、当社は、当社の選考の判断に不可欠な、お客様から提供されたその他の特定の個人データを処理します。あなたが当社に採用された場合、応募者のデータは自動的に従業員データに変更されます。採用プロセスの一環として、当社は、お客様から要求され、お客様の契約を開始または履行するために必要なお客様に関するその他の個人データ（個人識別番号や納税者番号など）を処理することになります。従業員データについては、データ処理の目的は、雇用契約の履行、または雇用関係に適用されるその他の法的規定（税法など）の遵守、およびお客様と締結した雇用契約を履行するためのお客様の個人データの使用（社内または顧客へのお客様の氏名および連絡先の公表など）です。従業員データは、法的な保存期間を満たすために、雇用関係の終了後も保存されます。

データ処理の法的根拠は、GDPR第6条1項b号、GDPR第9条2項b号およびh号、GDPR第88条1項および国内法（ドイツの場合はBDSG第26条（連邦データ保護法）など）です。

## D. 個人データの受領者のカテゴリー（GDPR第13条1項e号）

公的機関

外部団体

その他の外部機関

内部処理

グループ内処理

その他の団体

**第三国における当社のデータ処理者およびデータ受領者のリスト、および該当する場合は国際機関のリストは、当社のウェブサイトに掲載されているか、当社から無料で請求することができます。このリストをご希望の場合は、当社のデータ保護担当者までご連絡ください。**


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## E. 第三国の受信者と適切なまたは適切な保護措置とそのコピーを取得する手段またはそれらが利用可能になった場所（GDPR13条1項f号、46条1項、46条2項c号）

。

当社のグループ会社（以下、「グループ会社」といいます）のうち、第三国に事業所または事務所を有するすべての会社および支店が、個人データの受領者に属することがあります。すべてのグループ会社または受領者のリストは、弊社に請求することができます。

GDPR第46条1項によると、管理者または処理者が適切なセーフガードを提供し、データ主体の権利およびデータ主体のための効果的な法的救済が利用可能であることを条件として、管理者または処理者は個人データを第三国にのみ移転することができます。適切な保護措置は、標準的な契約条項（GDPR第46条2項c）により、監督当局の特別な許可を必要とせずに提供することができます。

欧州連合の標準契約条項またはその他の適切な保護措置は、個人データを最初に送信する前に、第三国からのすべての受信者と合意されます。その結果、データ対象者のための適切な保護措置、強制力のあるデータ対象者の権利、効果的な法的救済措置が保証されることが保証されます。すべてのデータ対象者は、当社から標準契約条項のコピーを入手することができます。標準契約条項は、欧州連合官報 にも掲載されています。

一般データ保護規則（GDPR）第45条3項は、欧州委員会に対し、EU域外の国が適切な保護レベルを提供していると実施法によって決定する権利を認めている。これは、EU域内とほぼ同等の個人データ保護レベルを意味する。適切な保護レベルを認める決定の効果として、個人データはEU（およびノルウェー、リヒテンシュタイン、アイスランド）から第三国へ、さらなる障害なく自由に流れることができる。同様の規則は、英国、スイス、その他いくつかの国にも適用される。

欧州委員会または他の国の政府が、第三国が適切なレベルの保護を提供すると決定し、適用される枠組み（EU-U.S. Data Privacy Framework, Swiss-U.S. Data Privacy Framework, UK Extension to the EU-U.S. Data Privacy Framework）が適用される場合、当社による当該枠組みのメンバー（自己認証事業体など）へのすべての移転は、当該事業体が関連枠組みに加盟していることのみに基づきます。当社または当社のグループ事業体の1つが当該フレームワークのメンバーである場合、当社または当社のグループ事業体へのすべての移転は、当該事業体が当該フレームワークのメンバーであることのみに基づきます。

データ対象者は誰でも当社から枠組みを入手することができます。また、欧州連合官報、公表された法的資料、または監督当局やその他の管轄当局・機関のウェブサイトからも入手することができます。


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## F. 個人データを保管する期間、またはそれが不可能な場合は、その期間を決定するために使用した基準（GDPR第13条2項a）

応募者の個人情報の保存期間は6ヶ月です。従業員のデータについては、それぞれの法定保存期間が適用されます。この期間の終了後、契約の履行または契約の開始に必要でなくなった時点で、対応するデータは定期的に削除されます。

## G. 情報主体に関する個人情報へのアクセス、修正、消去、処理の制限を管理者に要求する権利、または処理に異議を唱える権利、およびデータのポータビリティに対する権利の存在（GDPR13条2項b号）

すべてのデータ対象者は、以下の権利を有する。

***アクセス権***

各データ対象者は、自分に関する個人データにアクセスする権利を有します。アクセスする権利は、当社が処理するすべてのデータに及びます。この権利は、処理の合法性を認識し、検証するために、合理的な間隔で容易に行使することができます（GDPR説明書63）。この権利は、GDPR第15条に起因するものです。15 GDPRに起因するものです。データ対象者は、アクセス権を行使するために当社に連絡することができます。

***修正する権利***

GDPR第16条第1項により、データ対象者は自分に関する不正確な個人データの修正を管理者から不当に遅れることなく取得する権利を有します。さらに、GDPR第16条第2項では、データ対象者は、処理の目的を考慮し、補足説明の提供を含め、不完全な個人データを補完してもらう権利を有すると定めています。データ対象者は、修正する権利を行使するために当社に連絡することができます。

***消去する権利（忘れられる権利）***

さらに、データ対象者は、GDPR第17条に基づき、消去および忘れられる権利を有します。17 GDPRに基づき、データ対象者は消去および忘却の権利を有します。この権利は、当社に連絡することによっても行使することができます。ただし、この時点で、当社が従うべき法的義務を果たすために処理が必要である限り、この権利は適用されないことを指摘したいと思います（GDPR17条3項b号）。つまり、法的な保存期間の終了後にのみ、消去の申請を承認することができます。

***処理の制限に関する権利***

GDPR第18条によると、データ対象者は処理の制限を受ける権利を有します。処理の制限は、GDPR第18条1項a～dに規定された条件のいずれかが満たされた場合に要求することができます。データ対象者は、処理制限の権利を行使するために当社に連絡することができます。


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

*異議申し立ての権利*

さらに、Art.21　GDPRは異議を唱える権利を保証しています。データ対象者は、異議を唱える権利を行使するために当社に連絡することができます。

*データポータビリティの権利*

Art.20 GDPR はデータ対象者にデータポータビリティの権利を付与しています。この規定に基づき、データ対象者はGDPR第20条1項aおよびbに定める条件の下で、管理者に提供した自分に関する個人データを、構造化された、一般的に使用され機械で読み取り可能な形式で受け取り、個人データが提供された管理者から支障なくそれらのデータを他の管理者に転送する権利を有します。データ対象者は、データポータビリティの権利を行使するために、当社に連絡することができます。

## H.　処理がGDPR第6条1項a号またはGDPR第9条2項a号に基づく場合、撤回前の同意に基づく処理の合法性に影響を与えることなく、いつでも同意を撤回する権利の存在（GDPR第13条2項c号）。

個人データの処理が GDPR 第 6 条第 1 項に基づいている場合。6(1) lit. a GDPR、つまりデータ対象者が一つまたは複数の特定の目的のために個人データの処理に同意した場合、または特殊な個人データの処理に対する明示的な同意を規定する第9条(2)　lit.　a　GDPRに基づいている場合、データ対象者はGDPR第7条(3) 文章1に従っていつでもその同意を撤回する権利を有しているものとします。

同意の撤回が、撤回前の同意に基づく処理の合法性に影響を及ぼすことはない、GDPR第7条(3)文2。同意を撤回することは、同意を与えることと同じくらい容易でなければならない。7(3)　センテンス4 GDPR。したがって、同意の撤回は常に、同意が与えられたときと同じ方法、またはデータ対象者がより簡単だと考える他の方法で行うことができます。今日の情報社会では、同意を撤回する最も簡単な方法は、おそらく単純な電子メールでしょう。データ対象者が当社に与えた同意を撤回したい場合は、当社宛の簡単な電子メールだけで十分です。また、データ対象者は、同意の撤回を当社に伝えるために、他の方法を選択することもできます。

## I.監督機関に苦情を申し立てる権利（GDPR13条2項d号、77条1項）

管理者として、当社はデータ対象者に、監督機関に苦情を申し立てる権利（GDPR第13条2項d号）を通知する義務があります。監督機関に苦情を申し立てる権利は、GDPR第77条1項により規定されています。この規定によると、データ対象者が自分に関する個人データの処理が一般データ保護規則に違反していると考える場合、他の行政上または司法上の救済手段を損なうことなく、すべてのデータ対象者は、特に自分の居住地、勤務地または違反の疑いがある場所の加盟国の監督当局に苦情を申し立てる権利を有するものとします。監督機関に苦情を申し立てる権利は、EUの法律により、単一の監督


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

機関にのみ行使できるよう制限されています（Recital 141 Sentence 1 GDPR）。この規則は、同じデータ対象者が同じ問題で二重に苦情を申し立てることを避けるためのものです。したがって、データ対象者が当社に対して苦情を申し立てたい場合、当社は単一の監督機関にのみ連絡するよう要請します。

## J. 法的または契約上の要件としての個人データの提供；契約締結に必要な要件；データ主体の個人データ提供の義務；当該データを提供しない場合に起こりうる結果（GDPR13条2項e号）。

個人情報の提供は、法律（例：税法）により要求される場合もあれば、契約上の規定（例：契約相手に関する情報）によりもたらされる場合もあることを明確にします。

データ対象者が当社に個人データを提供し、その後当社がそのデータを処理することが、 契約締結のために必要な場合があります。例えば、当社がデータ対象者と契約を締結する際に、データ対象者は当社に個人データを提 供する義務があります。個人データが提供されない場合、データ対象者との契約は締結されないことになります。

データ対象者が個人データを提供する前に、データ対象者は当社に連絡しなければなりま せん。当社は、データ対象者に対し、個人データの提供が法律または契約によって要求されているか、または契約の締結に必要であるか、個人データを提供する義務があるか、個人データを提供しなかった場合にどのような結果になるかについて明らかにします。

## K. GDPR第22条（1）及び（4）に言及されるプロファイリングを含む自動的意思決定の存在、及び少なくともその場合、データ主体に対する当該処理の意義及び想定される結果と同様に、関連する論理に関する意味のある情報（GDPR第13条（2）項f）。

**責任ある企業として、通常、当社は自動化された意思決定またはプロファイリングを使用しません。例外的に自動化された意思決定またはプロファイリングを行う場合は、別途、または当社のプライバシー・ポリシー（当社ウェブサイト）の小項目を通じて、データ対象者に通知します。この場合、以下が適用されます：**

**自動化された意思決定（プロファイリングを含む）は、(1)データ対象者と当社との間で契約を締結または履行するために必要である場合、(2)当社が準拠する連邦法または加盟国の法律により許可され、データ対象者の権利および自由、正当な利益を保護するための適切な措置が定められている場合、または(3)データ対象者の明示的な同意に基づく場合に行われることがあります。**


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

GDPR第22条第2項(a)および(c)に規定されている場合、当社はデータ主体の権利および自由、正当な利益を保護するための適切な措置を講じるものとします。このような場合、お客様は、管理者側からの人的介入を受け、ご自身の見解を表明し、決定に異議を唱える権利を有します。

このような処理がデータ主体にとってどのような意味を持ち、どのような結果をもたらすかについては、当社のプライバシー・ポリシーに記載されています。

## II. データ主体から個人データを収集しない場合の情報要件の遵守（GDPR14条）

### A.管理者の身元および連絡先（GDPR第14条1項a号

上記参照

### B. データ保護責任者の連絡先（GDPR第14条1項b）

上記参照

### C. 個人データが意図される処理の目的および処理の法的根拠（GDPR 14条1項c号）

データ対象者から収集されなかった応募者のデータについては、データ処理の目的 は、採用プロセスにおける応募者の審査にあります。この目的のために、当社はお客様から収集したのではないデータを処理することがあります。採用プロセスで処理されたデータに基づいて、当社は、お客様が面接（選考プロセスの一部）に招待されるかどうかを確認します。あなたが当社で採用された場合、応募者のデータは自動的に従業員データに変換されます。従業員データについては、データ処理の目的は、雇用契約の履行、または雇用関係に適用されるその他の法的規定の遵守です。従業員データは、法的な保存期間を満たすために、雇用関係が終了した後も保存されます。

データ処理の法的根拠は、GDPR第6条1項bおよびf、GDPR第9条2項bおよびh、GDPR第88条1項および国内法（ドイツの場合はBDSG第26条（連邦データ保護法）など）です。

### D. 当該個人データのカテゴリー（GDPR第14条1項d）


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

応募者データ

社員データ

## E. 個人データの受領者のカテゴリー（GDPR14条1項e号）

公的機関

外部団体

その他の外部機関

内部処理

グループ内処理

その他の団体

**第三国における当社のデータ処理者およびデータ受領者のリスト、および該当する場合は国際機関のリストは、当社のウェブサイトに掲載されているか、当社から無料で請求することができます。このリストをご希望の場合は、当社のデータ保護担当者までご連絡ください。**

## F. 第三国の受信者と適切なまたは適切な保護措置とそのコピーを取得する手段またはそれらが利用可能になった場所（GDPR第14条1項f、46条1項、46条2項c）。

当社のグループ会社（以下、「グループ会社」といいます）のうち、第三国に事業所または事務所を有するすべての会社および支店が、個人データの受領者に属する場合があります。すべてのグループ会社または受領者のリストは、弊社に請求することができます。

GDPR 第 46(1) 条によると、管理者または処理者は、管理者または処理者が適切なセーフガードを提供し、データ主体の権利およびデータ主体のための有効な法的救済が利用可能であることを条件として、個人データを第三国にのみ移転することができます。適切な保護措置は、標準的なデータ保護条項（GDPR第46条2項c）により、監督官庁の特別な許可を必要とせずに提供することができます。

欧州連合の標準契約条項またはその他の適切な保護措置は、個人データを最初に送信する前に、第三国からのすべての受信者と合意されます。その結果、データ対象者のための適切な保護措置、強制力のあるデータ対象者の権利、効果的な法的救済措置が保証されることが保証されます。すべてのデー


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

タ対象者は、当社から標準契約条項のコピーを入手することができます。標準契約条項は、欧州連合官報 にも掲載されています。

一般データ保護規則（GDPR）第45条3項は、欧州委員会に対し、EU域外の国が適切な保護レベルを提供していると実施法によって決定する権利を認めている。これは、EU域内とほぼ同等の個人データ保護レベルを意味する。適切な保護レベルを認める決定の効果として、個人データはEU（およびノルウェー、リヒテンシュタイン、アイスランド）から第三国へ、さらなる障害なく自由に流れることができる。同様の規則は、英国、スイス、その他いくつかの国にも適用される。

欧州委員会または他の国の政府が、第三国が適切なレベルの保護を提供すると決定し、適用される枠組み（EU-U.S. Data Privacy Framework, Swiss-U.S. Data Privacy Framework, UK Extension to the EU-U.S. Data Privacy Framework）が適用される場合、当社による当該枠組みのメンバー（自己認証事業体など）へのすべての移転は、当該事業体が関連枠組みに加盟していることのみに基づきます。当社または当社のグループ事業体の1つが当該フレームワークのメンバーである場合、当社または当社のグループ事業体へのすべての移転は、当該事業体が当該フレームワークのメンバーであることのみに基づきます。

データ対象者は誰でも当社から枠組みを入手することができます。また、欧州連合官報、公表された法的資料、または監督当局やその他の管轄当局・機関のウェブサイトからも入手することができます。

## G. 個人データが保存される期間、またはそれが不可能な場合は、その期間を決定するために使用される基準（GDPR第14条2項a）。

応募者の個人情報の保存期間は6ヶ月です。従業員のデータについては、それぞれの法定保存期間が適用されます。この期間の終了後、契約の履行または契約の開始に必要でなくなった時点で、対応するデータは定期的に削除されます。

## H. 処理がGDPR第6条1項f号（GDPR第14条2項b号）に基づく場合、管理者または第三者が追求する正当な利益についての通知

GDPR第6条1項f号によると、管理者または第三者が追求する正当な利益のために処理が必要な場合に限り、処理は合法であるものとします。GDPRの説明47条2項によれば、データ対象者が管理者の顧客である場合など、データ対象者と管理者の間に適切な関係がある場合、正当な利益が存在する可能性があります。当社がGDPR第6条1項f号に基づいて応募者のデータを処理するすべてのケースにおいて、当社の正当な利益は、適切な人材および専門家の雇用にあります。


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## I. 情報主体に関する個人情報へのアクセスおよび修正、消去、処理の制限を管理者に要求する権利、およびデータのポータビリティに対する権利（GDPR第14条2項c号）の存在

すべてのデータ対象者は、以下の権利を有する。

***アクセス権***

各データ対象者は、自分に関する個人データにアクセスする権利を有します。アクセスする権利は、当社が処理するすべてのデータに及びます。この権利は、処理の合法性を認識し、検証するために、合理的な間隔で容易に行使することができます（GDPR説明書63）。この権利は、GDPR第15条に起因するものです。15 GDPRに起因するものです。データ対象者は、アクセス権を行使するために当社に連絡することができます。

***修正する権利***

GDPR第16条第1項により、データ対象者は自分に関する不正確な個人データの修正を管理者から不当に遅れることなく取得する権利を有します。さらに、GDPR第16条第2項では、データ対象者は、処理の目的を考慮し、補足説明の提供を含め、不完全な個人データを補完してもらう権利を有すると定めています。データ対象者は、修正する権利を行使するために当社に連絡することができます。

***消去する権利（忘れられる権利）***

さらに、データ対象者は、GDPR第17条に基づき、消去および忘れられる権利を有します。17 GDPRに基づき、データ対象者は消去および忘却の権利を有します。この権利は、当社に連絡することによっても行使することができます。ただし、この時点で、当社が従うべき法的義務を果たすために処理が必要である限り、この権利は適用されないことを指摘したいと思います（GDPR17条3項b号）。つまり、法的な保存期間の終了後にのみ、消去の申請を承認することができます。

***処理の制限に関する権利***

GDPR第18条によると、データ対象者は処理の制限を受ける権利を有します。処理の制限は、GDPR第18条1項a～dに規定された条件のいずれかが満たされる場合に要求することができます。データ対象者は、処理制限の権利を行使するために当社に連絡することができます。

***異議申し立ての権利***

さらに、Art.21 GDPRは異議を唱える権利を保証しています。データ対象者は、異議を唱える権利を行使するために当社に連絡することができます。

***データポータビリティの権利***

Art.20 GDPR はデータ対象者にデータポータビリティの権利を付与しています。この規定によると、データ対象者は、GDPR第20条1項aおよびbに規定された条件下で、管理者に提供した自分に関する


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

個人データを、構造化された、一般的に使用され機械で読み取り可能な形式で受け取り、個人データが提供された管理者から支障なくそれらのデータを他の管理者に転送する権利を有します。データ対象者は、データポータビリティの権利を行使するために、当社に連絡することができます。

## J. 処理が6条1項a号または9条2項a号GDPRに基づく場合、撤回前の同意に基づく処理の合法性に影響を与えることなく、いつでも同意を撤回する権利の存在（14条2項d号GDPR）。

個人データの処理が GDPR 第 6 条第 1 項に基づいている場合。6(1) lit. a GDPR、つまりデータ対象者が一つまたは複数の特定の目的のために個人データの処理に同意した場合、または特殊な個人データの処理に対する明示的な同意を規定する第9条(2) lit. a GDPRに基づいている場合、データ対象者はGDPR第7条(3) 文章1に従っていつでもその同意を撤回する権利を有しているものとします。

同意の撤回が、撤回前の同意に基づく処理の合法性に影響を及ぼすことはない、GDPR第7条（3）文2。同意を撤回することは、同意を与えることと同じくらい容易でなければならない。7(3) センテンス4 GDPR。したがって、同意の撤回は常に、同意が与えられたときと同じ方法、またはデータ対象者がより簡単だと考える他の方法で行うことができます。今日の情報社会では、同意を撤回する最も簡単な方法は、おそらく単純な電子メールでしょう。データ対象者が当社に与えた同意を撤回したい場合は、当社宛の簡単な電子メールだけで十分です。また、データ対象者は、同意の撤回を当社に伝えるために、他の方法を選択することもできます。

## K. 監督官庁に苦情を申し立てる権利（GDPR14条2項e号、77条1項

管理者として、当社はデータ対象者に、監督機関に苦情を申し立てる権利（GDPR第14条2項e号）を通知する義務を負います。監督機関に苦情を申し立てる権利は、GDPR第77条（1）項によって規定されています。この規定によると、データ対象者が自分に関する個人データの処理が一般データ保護規則に違反していると考える場合、他の行政上または司法上の救済手段を損なうことなく、すべてのデータ対象者は、特に自分の居住地、勤務地または違反の疑いがある場所の加盟国の監督機関に苦情を申し立てる権利を有するものとします。監督機関に苦情を申し立てる権利は、EUの法律により、単一の監督機関にのみ行使できるよう制限されています（Recital 141 Sentence 1 GDPR）。この規則は、同じデータ対象者が同じ問題で二重に苦情を申し立てることを避けるためのものです。したがって、データ対象者が当社に対して苦情を申し立てたい場合、当社は単一の監督機関にのみ連絡するよう要請します。


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## L. 個人データの出所、および該当する場合、公にアクセス可能な出所からのものかどうか（GDPR 14条2項f号）

原則として、個人データはデータ対象者から直接、または当局の協力のもとに収集されます（例：公的登録簿からのデータ検索）。データ対象者に関するその他のデータは、グループ会社からの移転により入手されます。この一般的な情報において、個人データの正確な出所を示すことは不可能であり、またGDP第14条5項b号の意味において不相応な労力を要すると思われます。14(5) lit. b GDPRの意味において、個人データの正確な出所を示すことは不可能であるか、または不相応な労力を要すると考えられます。原則として、当社は一般にアクセス可能な情報源から個人データを収集することはありません。

データ対象者はいつでも当社に連絡し、自分に関する個人データの正確な出所について のより詳細な情報を入手することができます。様々な情報源が使用されているため、個人データの出所をデータ対象者に提供できない場合は、一般的な情報を提供する必要があります（Recital 61 Sentence 4 GDPR）。

## M. GDPR第22条1項及び4項に言及されるプロファイリングを含む自動的意思決定の存在、及び少なくともその場合、データ主体にとっての当該処理の意義及び想定される結果とともに、関連する論理に関する意味のある情報（GDPR第14条2項g号）。

**責任ある企業として、通常、当社は自動化された意思決定またはプロファイリングを使用しません。例外的に自動化された意思決定またはプロファイリングを行う場合は、別途、または当社のプライバシー・ポリシー（当社ウェブサイト）の小項目を通じて、データ対象者に通知します。この場合、以下が適用されます：**

**自動化された意思決定（プロファイリングを含む）は、(1)データ対象者と当社との間で契約を締結または履行するために必要である場合、(2)当社が準拠する連邦法または加盟国の法律により許可され、データ対象者の権利および自由、正当な利益を保護するための適切な措置が定められている場合、または(3)データ対象者の明示的な同意に基づく場合に行われることがあります。**

**GDPR第22条第2項(a)および(c)に規定されている場合、当社はデータ主体の権利および自由、正当な利益を保護するための適切な措置を講じるものとします。このような場合、お客様は、管理者側からの人的介入を受け、ご自身の見解を表明し、決定に異議を唱える権利を有します。**

**このような処理がデータ主体にとってどのような意味を持ち、どのような結果をもたらすかについては、当社のプライバシー・ポリシーに記載されています。**


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

© All rights reserved by Heiko Maniero.

## III. EU-U.S. Data Privacy Framework (EU-U.S. DPF), UK Extension to the EU-U.S. DPF, Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF)

当組織が EU-U.S. Data Privacy Framework (EU-U.S. DPF) および/または UK Extension to the EU-U.S. DPF および/または Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF) の認定メンバーである場合、以下のことが適用されます：

当社は EU-U.S. Data Privacy Framework (EU-U.S. DPF) および UK Extension to the EU-U.S. DPF 並びに Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF) を、U.S. Department of Commerce が定めたとおりに遵守します。当社は米国商務省に対し、EU-U.S. Data Privacy Framework Principles (EU-U.S. DPF Principles) に従って、EU および UK から EU-U.S. DPF および UK Extension to the EU-U.S. DPF に基づいて受領する個人データの処理に関して遵守していることを確認しました。当社は米国商務省に対し、Swiss-U.S. Data Privacy Framework Principles (Swiss-U.S. DPF Principles) に従って、スイスから Swiss-U.S. DPF に基づいて受領する個人データの処理に関して遵守していることを確認しました。当社のプライバシーポリシーの規定と EU-U.S. DPF Principles および/または Swiss-U.S. DPF Principles の間に矛盾がある場合、Principles が優先されます。

Data Privacy Framework (DPF) プログラムの詳細および当社の認証をご覧になるには、https://www.dataprivacyframework.gov/ にアクセスしてください。

当社の他の米国の部門または子会社も EU-U.S. DPF Principles を遵守しており、UK Extension to the EU-U.S. DPF および Swiss-U.S. DPF Principles を含む場合は、当社のプライバシーポリシーに記載されています。

EU-U.S. DPF および UK Extension to the EU-U.S. DPF 並びに Swiss-U.S. DPF に従い、当社は EU のデータ保護当局および英国の Information Commissioner's Office (ICO) ならびにスイスの Federal Data Protection and Information Commissioner (EDÖB) によって設立された機関と協力し、EU-U.S. DPF および UK Extension to the EU-U.S. DPF および Swiss-U.S. DPF に基づいて当社が受領する個人データの取り扱いに関する未解決の苦情について、その助言に従うことを約束します。

当社は、当社組織の個人データの取り扱いに関する苦情を処理する責任のある欧州のデータ保護当局について、影響を受ける個人にこの透明性ドキュメントの上部で通知し、影響を受ける個人に適切かつ無料の救済措置を提供します。

当社は、影響を受けるすべての個人に対し、当社が Federal Trade Commission (FTC) の調査および執行権限の対象であることを通知します。


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

影響を受ける個人は、特定の条件下で拘束力のある仲裁を求める権利があります。当社は、影響を受ける個人が当社に通知し、Principles の附属書 I に従って手続きおよび条件を遵守することで、拘束力のある仲裁を申請した場合、要求を解決し、DPF-Principles の附属書 I に基づく条件を遵守することを約束します。

当社は、個人データを第三者に提供する場合の当社の責任について、影響を受けるすべての個人に通知します。

影響を受ける個人またはデータ保護監督当局の質問については、この透明性ドキュメントの上部に記載された地域の担当者を指定しました。

当社は、個人データを第三者に提供するかどうか (i) または収集時の目的と実質的に異なる目的で使用するかどうか (ii) について、選択する機会 (Opt-out) を提供します。選択権を行使するための明確で目立ち、簡単にアクセスできるメカニズムは、当社のデータ保護担当者 (DSB) に電子メールで連絡することです。個人データが第三者に提供される場合、当社の指示に従って当社の代理人または処理者として行動する場合には、選択の機会はありませんし、当社もその義務はありません。しかし、当社は常にそのような代理人または処理者と契約を結びます。

敏感なデータ (すなわち、健康状態、人種または民族的出自、政治的見解、宗教的または哲学的信念、労働組合への加入、または対象者の性生活に関する情報を含む個人データ) については、これらのデータを第三者に提供する場合 (i) または収集時の目的と異なる目的で使用する場合 (ii) には、明示的な同意 (Opt-in) を取得します。さらに、第三者から受け取ったすべての個人データを、第三者がそれを敏感なデータとして識別し取り扱う場合、敏感なデータとして扱います。

当社は、当局からの合法的な要求に応じて個人データを開示する必要があることを、ここに通知します。これには、国家安全保障または法執行機関の要件の遵守が含まれます。

個人データを管理者として行動する第三者に転送する場合、当社は通知と選択の原則 (Principles) を遵守します。また、処理を担当する第三者と契約を締結し、これらのデータは限定された特定の目的のためにのみ処理されること、受信者が DPF の原則 (Principles) と同じレベルの保護を提供し、これ以上この義務を履行できないことを確認した場合には当社に通知することを規定します。契約には、管理者としての第三者がそのような状況が確認された場合、処理を停止するか、適切な是正措置を講じることが求められます。

個人データを代理人または処理者として行動する第三者に転送する場合、(i) 当社はこれらのデータを限定された特定の目的のためにのみ転送します。(ii) 代理人または処理者が DPF-Principles で求められるのと同等のデータ保護レベルを提供することを確認します。 (iii) 当社の義務に基づいて代理人または処理者が実際に転送された個人データを処理していることを確認するために適切な措置を講じます。 (iv) 代理人または処理者がこの義務を履行できなくなったことを確認した場合、当社に通知するこ


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

とを要求します。 (v) 通知後 (iv を含む)、不正な処理を停止し是正措置を講じるために適切な措置を講じます。 (vi) DPF Department の要求に応じて、その代理人との契約の関連するデータ保護規定の要約または代表的な例を提供します。

EU-U.S. DPF および/または UK Extension to the EU-U.S. DPF および/または Swiss-U.S. DPF に従い、当社は EU のデータ保護当局および英国の Information Commissioner's Office (ICO) ならびにスイスの Federal Data Protection and Information Commissioner (EDÖB) によって設立された機関と協力し、EU-U.S. DPF および UK Extension to the EU-U.S. DPF および Swiss-U.S. DPF に基づいて当社が受領する個人データの取り扱いに関する未解決の苦情について、その助言に従うことを約束します。

欧州連合（EU）、欧州経済地域（EEA）または英国に一時的に滞在している、あるいはそこに住所または常居所を有するすべてのデータ主体は、個人データにアクセスする権利を含むGDPR第15条から第22条からも生じる、当社の透明性文書で公表されている権利およびデータ主体の権利を有します。当社は、この情報をすべてのEUおよびEEA言語で利用できるようにしています。英語版は英国に適用されます。

スイスに一時的に居住している、またはスイスに住所もしくは常居所を有するすべてのデータ対象者は、個人データにアクセスする権利を含め、当社の透明性文書で公表されているスイスデータ保護法（DPA）およびスイスデータ保護規則（DPR）に基づく権利およびデータ対象者の権利を有します。当社はこの情報をスイスの3つの公用語（ドイツ語、イタリア語、フランス語）で提供しています。


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

# TURKISH: Kişisel Verilerin İşlenmesi Hakkında Bilgilendirme (GDPR Madde 13, 14)

Sayın Bay veya Bayan,

Şirketimizle sözleşmeye dayalı, sözleşme öncesi veya başka bir ilişki içinde olan her bireyin kişisel verileri özel korumayı hak eder. Hedefimiz, veri koruma düzeyimizi yüksek bir standartta tutmaktır. Bu nedenle, veri koruma ve veri güvenliği konseptlerimizi rutin olarak geliştiriyoruz.

Elbette, veri korumaya ilişkin yasal hükümlere uyuyoruz. GDPR Madde 13, 14'e göre, kontrolörler kişisel verileri toplarken belirli bilgi gereksinimlerini karşılar. Bu belge bu yükümlülükleri yerine getirmektedir.

Yasal düzenlemelerin terminolojisi karmaşıktır. Ne yazık ki, bu belgenin hazırlanmasında yasal terimlerin kullanılmasından vazgeçilememiştir. Bu nedenle, bu belge, kullanılan terimler veya formülasyonlarla ilgili tüm sorularınız için her zaman bizimle iletişime geçebileceğinizi belirtmek isteriz.

## I. Veri sahibinden kişisel veriler toplandığında bilgi gerekliliklerine uygunluk (GDPR Madde 13)

### A. Kontrolörün kimliği ve iletişim bilgileri (GDPR Madde 13(1) lit. a)

Yukarıya bakın

### B. Veri Koruma Görevlisinin iletişim bilgileri (GDPR Madde 13(1) lit. b)

Yukarıya bakın

### C. Kişisel verilerin işlenme amaçları ve işlemenin yasal dayanağı (GDPR Madde 13(1) lit. c)

Kişisel verilerin işlenmesinin amacı, denetleyiciyi, müşterileri, potansiyel müşterileri, iş ortaklarını veya adı geçen gruplar arasındaki diğer sözleşmeye dayalı veya sözleşme öncesi ilişkileri (en geniş anlamda) veya denetleyicinin yasal yükümlülüklerini ilgilendiren tüm işlemlerin gerçekleştirilmesidir.

Madde 6(1) lit. 6(1) lit. a GDPR, belirli bir işleme amacı için onay aldığımız işleme operasyonları için yasal dayanak olarak hizmet eder. Kişisel verilerin işlenmesi, veri sahibinin taraf olduğu bir sözleşmenin ifası için gerekliyse, örneğin işleme operasyonları malların tedariki veya başka bir hizmetin sağlanması için gerekli olduğunda olduğu gibi, işleme GDPR Madde 6 (1) lit. b'ye dayanır. Aynı durum, örneğin


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

ürünlerimiz veya hizmetlerimizle ilgili sorularda olduğu gibi, sözleşme öncesi önlemlerin alınması için gerekli olan işleme faaliyetleri için de geçerlidir. Şirketimiz, vergi yükümlülüklerinin yerine getirilmesi gibi kişisel verilerin işlenmesinin gerekli olduğu yasal bir yükümlülüğe tabi ise, işleme GDPR Madde 6(1) c bendine dayanır. 6(1) lit. c GDPR.

Nadir durumlarda, kişisel verilerin işlenmesi, veri sahibinin veya başka bir gerçek kişinin hayati çıkarlarını korumak için gerekli olabilir. Örneğin, bir ziyaretçinin şirketimizde yaralanması ve adının, yaşının, sağlık sigortası verilerinin veya diğer hayati bilgilerin bir doktora, hastaneye veya başka bir üçüncü tarafa iletilmesi gerektiğinde durum böyle olacaktır. Bu durumda işleme, GDPR Madde 6(1) lit. d GDPR.

İşlemenin kamu yararına yürütülen bir görevin yerine getirilmesi veya kontrolöre verilen resmi yetkinin kullanılması için gerekli olduğu durumlarda, yasal dayanak GDPR Madde 6(1) lit. e GDPR.

Son olarak, işleme operasyonları GDPR Madde 6(1) lit. f'ye dayandırılabilir. Bu yasal dayanak, yukarıda belirtilen yasal dayanaklardan herhangi birinin kapsamına girmeyen işleme operasyonları için, şirketimiz veya üçüncü bir tarafça izlenen meşru menfaatlerin amaçları için işlemenin gerekli olması durumunda, bu menfaatlerin kişisel verilerin korunmasını gerektiren veri sahibinin menfaatleri veya temel hak ve özgürlükleri tarafından geçersiz kılınması haricinde kullanılır. Bu tür işleme faaliyetlerine özellikle izin verilmektedir çünkü bunlar Avrupa yasa koyucusu tarafından özellikle belirtilmiştir. Veri sahibinin kontrolörün müşterisi olması halinde meşru bir menfaatin varsayılabileceğini düşünmüştür (GDPR 47. Madde 2. Cümle).

## D. İşlemenin GDPR Madde 6(1) lit. f'ye dayandığı durumlarda, kontrolör veya üçüncü bir tarafça gözetilen meşru menfaatler (GDPR Madde 13(1) lit. d)

Kişisel verilerin işlenmesinin GDPR Madde 6(1) f bendine dayandığı durumlarda meşru menfaatimiz, işimizi tüm çalışanlarımızın ve hissedarlarımızın refahı lehine yürütmektir.

## E. Kişisel verilerin alıcılarının kategorileri (GDPR Madde 13(1) lit. e)

Kamu yetkilileri

Dış organlar

Diğer dış kuruluşlar

Dahili işleme

Grup içi işleme

Diğer kurumlar


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

Üçüncü ülkelerdeki ve varsa uluslararası kuruluşlardaki işleyicilerimizin ve veri alıcılarımızın bir listesi ya web sitemizde yayınlanır ya da bizden ücretsiz olarak talep edilebilir. Bu listeyi talep etmek için lütfen veri koruma görevlimizle iletişime geçin.

## F. Üçüncü bir ülkedeki alıcılar ve uygun veya uygun koruma önlemleri ve bunların bir kopyasının elde edilebileceği veya kullanıma sunulduğu araçlar (GDPR Madde 13 (1) f, 46 (1), 46 (2) c bendi)

Grubumuzun bir parçası olan ve üçüncü bir ülkede iş yeri veya ofisi bulunan tüm şirketler ve şubeler (bundan böyle "grup şirketleri" olarak anılacaktır) kişisel verilerin alıcılarına ait olabilir. Tüm grup şirketlerinin veya alıcıların bir listesi bizden talep edilebilir.

GDPR madde 46(1) uyarınca, bir kontrolör veya işleyici kişisel verileri üçüncü bir ülkeye yalnızca kontrolör veya işleyicinin uygun güvenceleri sağlaması ve veri sahipleri için uygulanabilir veri sahibi hakları ve etkili yasal çözüm yollarının mevcut olması koşuluyla aktarabilir. Uygun güvenceler, standart sözleşme maddeleri vasıtasıyla bir denetim makamından herhangi bir özel izin alınmasını gerektirmeksizin sağlanabilir, GDPR madde 46(2) lit. c.

Avrupa Birliği'nin standart sözleşme maddeleri veya diğer uygun güvenceler, kişisel verilerin ilk iletiminden önce üçüncü ülkelerden gelen tüm alıcılarla kararlaştırılır. Sonuç olarak, uygun güvencelerin, uygulanabilir veri sahibi haklarının ve veri sahipleri için etkili yasal çözüm yollarının garanti edilmesi sağlanır. Her veri sahibi, standart sözleşme maddelerinin bir kopyasını bizden temin edebilir. Standart sözleşme maddeleri Avrupa Birliği Resmi Gazetesinde de mevcuttur.

Genel Veri Koruma Tüzüğü'nün (GDPR) 45(3) maddesi, Avrupa Komisyonu'na, bir uygulama yasası aracılığıyla, AB dışındaki bir ülkenin yeterli düzeyde koruma sağladığına karar verme hakkı vermektedir. Bu, kişisel veriler için AB'dekine genel olarak eşdeğer bir koruma düzeyi anlamına gelir. Yeterli düzeyde koruma sağlandığına dair kararların etkisi, kişisel verilerin AB'den (ve Norveç, Lihtenştayn ve İzlanda'dan) üçüncü bir ülkeye başka engeller olmaksızın serbestçe akabilmesidir. Benzer kurallar Birleşik Krallık, İsviçre ve diğer bazı ülkelerde de uygulanmaktadır.

Avrupa Komisyonu veya başka bir ülkenin hükümetinin üçüncü bir ülkenin yeterli düzeyde koruma sağladığına karar vermesi ve geçerli çerçevenin (örneğin, EU-U.S. Data Privacy Framework, Swiss-U.S. Data Privacy Framework, UK-Extension to the EU-U.S. Data Privacy Framework) belirlenmesi durumunda, tarafımızdan bu tür çerçevelerin üyelerine (örneğin, kendi kendini onaylayan kuruluşlar) yapılan tüm aktarımlar yalnızca bu kuruluşların ilgili çerçeveye üyeliğine dayanmaktadır. Bizim veya grup kuruluşlarımızdan birinin bu tür bir çerçevenin üyesi olması durumunda, bize veya grup kuruluşumuza yapılan tüm aktarımlar yalnızca kuruluşun bu çerçeveye üyeliğine dayanır.

Herhangi bir veri sahibi çerçevelerin bir kopyasını bizden temin edebilir. Ayrıca, çerçeveler Avrupa Birliği Resmi Gazetesi'nde veya yayınlanan yasal materyallerde veya denetim makamlarının veya diğer yetkili makamların veya kurumların web sitelerinde de mevcuttur.


© All rights reserved by Heiko Maniero.

## G. Kişisel verilerin saklanacağı süre veya bu mümkün değilse, bu süreyi belirlemek için kullanılan kriterler (GDPR Madde 13(2) lit. a)

Kişisel verilerin saklanma süresini belirlemek için kullanılan kriter, ilgili yasal saklama süresidir. Bu sürenin sona ermesinden sonra, ilgili veriler, sözleşmenin yerine getirilmesi veya bir sözleşmenin başlatılması için artık gerekli olmadığı sürece rutin olarak silinir.

Yasal bir saklama süresi yoksa, kriter sözleşmeye dayalı veya dahili saklama süresidir.

## H. Veri sorumlusundan kişisel verilere erişim ve bunların düzeltilmesini veya silinmesini ya da veri sahibiyle ilgili işlemenin kısıtlanmasını talep etme veya işlemeye itiraz etme hakkının yanı sıra veri taşınabilirliği hakkının varlığı (GDPR Madde 13(2) lit. b)

Tüm veri sahipleri aşağıdaki haklara sahiptir:

***Erişim hakkı***

Her veri sahibi, kendisiyle ilgili kişisel verilere erişme hakkına sahiptir. Erişim hakkı tarafımızca işlenen tüm verileri kapsamaktadır. Bu hak, işlemenin yasallığından haberdar olmak ve bunu doğrulamak için kolaylıkla ve makul aralıklarla kullanılabilir (GDPR 63. Madde). Bu hak GDPR Madde 15'ten kaynaklanmaktadır. 15 GDPR'DEN KAYNAKLANMAKTADIR. Veri sahibi, erişim hakkını kullanmak için bizimle iletişime geçebilir.

***Düzeltme hakkı***

GDPR Madde 16 Cümle 1 uyarınca veri sahibi, kendisiyle ilgili yanlış kişisel verilerin düzeltilmesini gecikmeksizin kontrolörden talep etme hakkına sahiptir. Ayrıca, GDPR Madde 16 Cümle 2, veri sahibinin, işleme amaçlarını dikkate alarak, ek bir beyan sağlamak da dahil olmak üzere, eksik kişisel verilerin tamamlanmasını isteme hakkına sahip olduğunu öngörmektedir. Veri sahibi, düzeltme hakkını kullanmak için bizimle iletişime geçebilir.

***Silme hakkı (unutulma hakkı)***

Buna ek olarak, veri sahipleri Madde 17 uyarınca silme ve unutulma hakkına sahiptir. 17 GDPR. Bu hak bizimle iletişime geçilerek de kullanılabilir. Ancak bu noktada, bu hakkın, işlemenin şirketimizin tabi olduğu yasal bir yükümlülüğü yerine getirmek için gerekli olduğu sürece geçerli olmadığını belirtmek isteriz, Madde 17 (3) lit. b GDPR. Bu, bir silme başvurusunu ancak yasal saklama süresinin sona ermesinden sonra onaylayabileceğimiz anlamına gelir.

***İşlemenin kısıtlanması hakkı***

GDPR Madde 18 uyarınca, herhangi bir veri sahibi işlemenin kısıtlanmasını talep etme hakkına sahiptir. İşlemenin kısıtlanması, GDPR Madde 18(1) lit. a-d'de belirtilen koşullardan birinin yerine getirilmesi


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

halinde talep edilebilir. Veri sahibi, işlemenin kısıtlanması hakkını kullanmak için bizimle iletişime geçebilir.

***İtiraz hakkı***

Ayrıca, Madde 21 GDPR itiraz hakkını garanti eder. İlgili kişi itiraz hakkını kullanmak için bizimle iletişime geçebilir.

***Veri taşınabilirliği hakkı***

Madde 20 20 GDPR, veri sahibine veri taşınabilirliği hakkı tanır. Bu hüküm uyarınca, veri sahibi, GDPR Madde 20(1) lit. a ve b'de belirtilen koşullar altında, bir denetleyiciye sağladığı kendisiyle ilgili kişisel verileri yapılandırılmış, yaygın olarak kullanılan ve makine tarafından okunabilir bir formatta alma ve bu verileri kişisel verilerin sağlandığı denetleyiciden herhangi bir engel olmaksızın başka bir denetleyiciye iletme hakkına sahiptir. Veri sahibi, veri taşınabilirliği hakkını kullanmak için bizimle iletişime geçebilir.

## I. İşlemenin GDPR Madde 6(1) a bendine veya GDPR Madde 9(2) a bendine (GDPR Madde 13(2) c bendine) dayandığı durumlarda, geri çekilmeden önce rızaya dayalı işlemenin yasallığını etkilemeksizin rızayı herhangi bir zamanda geri çekme hakkının varlığı

Kişisel verilerin işlenmesi GDPR Madde 6(1) a bendine dayanıyorsa 6(1) lit. a GDPR, veri sahibi kişisel verilerin bir veya daha fazla özel amaç için işlenmesine rıza göstermişse veya özel kategorilerdeki kişisel verilerin işlenmesine açık rızayı düzenleyen Madde 9(2) lit. a GDPR'ye dayanıyorsa, veri sahibi Madde 7(3) Cümle 1 GDPR'ye göre rızasını istediği zaman geri çekme hakkına sahiptir.

Rızanın geri çekilmesi, geri çekilmeden önce rızaya dayalı olarak gerçekleştirilen işleme faaliyetinin hukuka uygunluğunu etkilemez, GDPR Madde 7(3) Cümle 2. Rızanın geri çekilmesi rıza vermek kadar kolay olmalıdır, GDPR Madde GDPR Madde 7(3) Cümle 4. Bu nedenle, rızanın geri çekilmesi her zaman rızanın verildiği şekilde veya veri sahibi tarafından daha basit olduğu düşünülen başka bir şekilde gerçekleşebilir. Günümüz bilgi toplumunda, muhtemelen rızayı geri çekmenin en basit yolu basit bir e-postadır. Veri sahibi bize verdiği rızayı geri çekmek isterse, bize basit bir e-posta göndermesi yeterlidir. Alternatif olarak, veri sahibi rızasını geri çektiğini bize iletmek için başka bir yol seçebilir.

## J. Bir denetim makamına şikayette bulunma hakkı (GDPR Madde 13(2) lit. d, 77(1))

Veri sorumlusu olarak, veri sahibini bir denetim makamına şikayette bulunma hakkı konusunda bilgilendirmekle yükümlüyüz, GDPR Madde 13(2) lit. d. Bir denetim makamına şikayette bulunma hakkı, GDPR Madde 77(1) ile düzenlenmektedir. Bu hüküm uyarınca, diğer idari veya adli çözüm yollarına halel gelmeksizin, her veri sahibinin, kendisiyle ilgili kişisel verilerin işlenmesinin Genel Veri Koruma Tüzüğü'nü ihlal ettiğini düşünmesi halinde, özellikle mutat meskeninin, iş yerinin veya iddia edilen ihlalin gerçekleştiği yerin bulunduğu Üye Devlet'teki bir denetim makamına şikayette bulunma hakkı vardır. Bir denetim


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

makamına şikayette bulunma hakkı Birlik hukuku tarafından yalnızca tek bir denetim makamı nezdinde kullanılabilecek şekilde sınırlandırılmıştır (Resital 141 Cümle 1 GDPR). Bu kural, aynı veri sahibinin aynı konuda çifte şikayette bulunmasını önlemeyi amaçlamaktadır. Bu nedenle, bir veri sahibi hakkımızda şikayette bulunmak isterse, yalnızca tek bir denetim makamıyla iletişime geçmesi istenir.

## K. Yasal veya sözleşmesel gereklilik olarak kişisel verilerin sağlanması; Bir sözleşme yapmak için gerekli gereklilik; Veri sahibinin kişisel verileri sağlama yükümlülüğü; Bu tür verilerin sağlanmamasının olası sonuçları (GDPR Madde 13 (2) lit. e)

Kişisel verilerin sağlanmasının kısmen kanunen gerekli olduğunu (örneğin vergi düzenlemeleri) veya sözleşme hükümlerinden de kaynaklanabileceğini (örneğin sözleşme ortağı hakkında bilgi) açıklığa kavuşturuyoruz.

Bazen, veri sahibinin bize kişisel verilerini sağladığı ve daha sonra tarafımızdan işlenmesi gereken bir sözleşme yapılması gerekebilir. Örneğin, şirketimiz kendisiyle bir sözleşme imzaladığında veri sahibi bize kişisel verilerini sağlamakla yükümlüdür. Kişisel verilerin sağlanmaması, veri sahibi ile sözleşmenin akdedilememesi sonucunu doğuracaktır.

Kişisel veriler veri sahibi tarafından sağlanmadan önce, veri sahibi bizimle iletişime geçmelidir. Veri sahibine, kişisel verilerin sağlanmasının yasa veya sözleşme gereği olup olmadığını veya sözleşmenin imzalanması için gerekli olup olmadığını, kişisel verileri sağlama yükümlülüğü olup olmadığını ve kişisel verilerin sağlanmamasının sonuçlarını açıklıyoruz.

## L. GDPR Madde 22(1) ve (4)'te atıfta bulunulan profil oluşturma da dahil olmak üzere otomatik karar vermenin varlığı ve en azından bu durumlarda, ilgili mantık hakkında anlamlı bilgilerin yanı sıra veri sahibi için bu tür işlemenin önemi ve öngörülen sonuçları (GDPR Madde 13 (2) f bendi)

Sorumlu bir şirket olarak genellikle otomatik karar verme veya profil oluşturmayı kullanmıyoruz. İstisnai durumlarda, otomatik karar verme veya profil oluşturma işlemi gerçekleştirirsek, veri sahibini ayrı olarak veya gizlilik politikamızın (web sitemizde) bir alt bölümü aracılığıyla bilgilendireceğiz. Bu durumda aşağıdakiler geçerlidir:

Profil oluşturma da dahil olmak üzere otomatik karar alma, (1) veri sahibi ile aramızda bir sözleşmenin yapılması veya bu sözleşmenin ifası için gerekli olması veya (2) buna, bağlı olduğumuz Birlik veya Üye Devlet kanunları tarafından yetki verilmesi durumunda gerçekleşebilir. konu olan ve aynı zamanda veri sahibinin hak ve özgürlükleri ile meşru çıkarlarının korunmasına yönelik uygun önlemleri belirleyen; veya (3) bunun veri sahibinin açık rızasına dayanması.


© All rights reserved by Heiko Maniero.

GDPR Madde 22(2) (a) ve (c)'de atıfta bulunulan durumlarda, veri sahibinin hak ve özgürlükleri ile meşru çıkarlarını korumak için uygun önlemleri uygulayacağız. Bu durumlarda, kontrolörden insan müdahalesi alma, görüşünüzü ifade etme ve karara itiraz etme hakkına sahipsiniz.

İlgili mantığa ilişkin anlamlı bilgilerin yanı sıra söz konusu işlemenin veri sahibi açısından önemi ve öngörülen sonuçları gizlilik politikamızda belirtilmiştir.

## II. Kişisel verilerin veri sahibinden toplanmadığı durumlarda bilgi gerekliliklerine uygunluk (GDPR Madde 14)

### A. Kontrolörün kimliği ve iletişim bilgileri (GDPR Madde 14(1) lit. a)

Yukarıya bakın

### B. Veri Koruma Görevlisinin iletişim bilgileri (GDPR Madde 14(1) lit. b)

Yukarıya bakın

### C. Kişisel verilerin işlenme amaçları ve işlemenin yasal dayanağı (GDPR Madde 14(1) lit. c)

Kişisel verilerin işlenmesinin amacı, denetleyiciyi, müşterileri, potansiyel müşterileri, iş ortaklarını veya adı geçen gruplar arasındaki diğer sözleşmeye dayalı veya sözleşme öncesi ilişkileri (en geniş anlamda) veya denetleyicinin yasal yükümlülüklerini ilgilendiren tüm işlemlerin gerçekleştirilmesidir.

Kişisel verilerin işlenmesi, veri sahibinin taraf olduğu bir sözleşmenin ifası için gerekliyse, örneğin işleme operasyonları malların tedariki veya başka bir hizmetin sağlanması için gerekli olduğunda olduğu gibi, işleme GDPR Madde 6 (1) lit. b'ye dayanmaktadır. Aynı durum, örneğin ürünlerimiz veya hizmetlerimizle ilgili sorular söz konusu olduğunda, sözleşme öncesi önlemlerin alınması için gerekli olan işleme faaliyetleri için de geçerlidir. Şirketimiz, vergi yükümlülüklerinin yerine getirilmesi gibi kişisel verilerin işlenmesinin gerekli olduğu yasal bir yükümlülüğe tabi ise, işleme GDPR Madde 6(1) fıkra c'ye dayanır. 6(1) lit. c GDPR.

Nadir durumlarda, kişisel verilerin işlenmesi, veri sahibinin veya başka bir gerçek kişinin hayati çıkarlarını korumak için gerekli olabilir. Örneğin, bir ziyaretçinin şirketimizde yaralanması ve adının, yaşının, sağlık sigortası verilerinin veya diğer hayati bilgilerin bir doktora, hastaneye veya başka bir üçüncü tarafa iletilmesi gerektiğinde durum böyle olacaktır. Bu durumda işleme, GD Madde 6(1) d bendine dayanacaktır. 6(1) lit. d GDPR.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

İşlemenin kamu yararına yürütülen bir görevin yerine getirilmesi veya kontrolöre verilen resmi yetkinin kullanılması için gerekli olduğu durumlarda, yasal dayanak GDPR Madde 6(1) lit. e GDPR.

Son olarak, işleme operasyonları GDPR Madde 6(1) lit. f'ye dayandırılabilir. Bu yasal dayanak, yukarıda belirtilen yasal dayanaklardan herhangi birinin kapsamına girmeyen işleme operasyonları için, şirketimiz veya üçüncü bir tarafça izlenen meşru menfaatlerin amaçları için işlemenin gerekli olması durumunda, bu menfaatlerin kişisel verilerin korunmasını gerektiren veri sahibinin menfaatleri veya temel hak ve özgürlükleri tarafından geçersiz kılınması haricinde kullanılır. Bu tür işleme faaliyetlerine özellikle izin verilmektedir çünkü bunlar Avrupa yasa koyucusu tarafından özellikle belirtilmiştir. Veri sahibinin kontrolörün müşterisi olması halinde meşru bir menfaatin varsayılabileceğini düşünmüştür (GDPR 47. Madde 2. Cümle).

## D. İlgili kişisel veri kategorileri (GDPR Madde 14(1) lit. d)

Müşteri verileri

Potansiyel müşterilerin verileri

Çalışan verileri

Tedarikçilerin verileri

## E. Kişisel verilerin alıcılarının kategorileri (GDPR Madde 14(1) lit. e)

Kamu yetkilileri

Dış organlar

Diğer dış kuruluşlar

Dahili işleme

Grup içi işleme

Diğer kurumlar

Üçüncü ülkelerdeki ve varsa uluslararası kuruluşlardaki işleyicilerimizin ve veri alıcılarımızın bir listesi ya web sitemizde yayınlanır ya da bizden ücretsiz olarak talep edilebilir. Bu listeyi talep etmek için lütfen veri koruma görevlimizle iletişime geçin.


© All rights reserved by Heiko Maniero.

## F. Üçüncü bir ülkedeki alıcılar ve uygun veya uygun koruma önlemleri ve bunların bir kopyasının elde edilebileceği veya kullanıma sunulduğu araçlar (GDPR Madde 14(1) f, 46(1), 46(2) c bendi)

Grubumuzun bir parçası olan ve üçüncü bir ülkede iş yeri veya ofisi bulunan tüm şirketler ve şubeler (bundan böyle "grup şirketleri" olarak anılacaktır) kişisel verilerin alıcılarına ait olabilir. Tüm grup şirketlerinin bir listesi bizden talep edilebilir.

GDPR madde 46(1) uyarınca, bir kontrolör veya işleyici kişisel verileri üçüncü bir ülkeye ancak kontrolör veya işleyicinin uygun güvenceleri sağlaması ve veri sahipleri için uygulanabilir veri sahibi hakları ve etkili yasal çözüm yollarının mevcut olması koşuluyla aktarabilir. Uygun güvenceler, GDPR madde 46(2) bent c uyarınca standart veri koruma hükümleri vasıtasıyla bir denetim makamından herhangi bir özel izin alınmasını gerektirmeksizin sağlanabilir.

Avrupa Birliği'nin standart sözleşme maddeleri veya diğer uygun güvenceler, kişisel verilerin ilk iletiminden önce üçüncü ülkelerden gelen tüm alıcılarla kararlaştırılır. Sonuç olarak, uygun güvencelerin, uygulanabilir veri sahibi haklarının ve veri sahipleri için etkili yasal çözüm yollarının garanti edilmesi sağlanır. Her veri sahibi, standart sözleşme maddelerinin bir kopyasını bizden temin edebilir. Standart sözleşme maddeleri Avrupa Birliği Resmi Gazetesinde de mevcuttur.

Genel Veri Koruma Tüzüğü'nün (GDPR) 45(3) maddesi, Avrupa Komisyonu'na, bir uygulama yasası aracılığıyla, AB dışındaki bir ülkenin yeterli düzeyde koruma sağladığına karar verme hakkı vermektedir. Bu, kişisel veriler için AB'dekine genel olarak eşdeğer bir koruma düzeyi anlamına gelir. Yeterli düzeyde koruma sağlandığına dair kararların etkisi, kişisel verilerin AB'den (ve Norveç, Lihtenştayn ve İzlanda'dan) üçüncü bir ülkeye başka engeller olmaksızın serbestçe akabilmesidir. Benzer kurallar Birleşik Krallık, İsviçre ve diğer bazı ülkelerde de uygulanmaktadır.

Avrupa Komisyonu veya başka bir ülkenin hükümetinin üçüncü bir ülkenin yeterli düzeyde koruma sağladığına karar vermesi ve geçerli çerçevenin (örneğin, EU-U.S. Data Privacy Framework, Swiss-U.S. Data Privacy Framework, UK-Extension to the EU-U.S. Data Privacy Framework) belirlenmesi durumunda, tarafımızdan bu tür çerçevelerin üyelerine (örneğin, kendi kendini onaylayan kuruluşlar) yapılan tüm aktarımlar yalnızca bu kuruluşların ilgili çerçeveye üyeliğine dayanmaktadır. Bizim veya grup kuruluşlarımızdan birinin bu tür bir çerçevenin üyesi olması durumunda, bize veya grup kuruluşumuza yapılan tüm aktarımlar yalnızca kuruluşun bu çerçeveye üyeliğine dayanır.

Herhangi bir veri sahibi çerçevelerin bir kopyasını bizden temin edebilir. Ayrıca, çerçeveler Avrupa Birliği Resmi Gazetesi'nde veya yayınlanan yasal materyallerde veya denetim makamlarının veya diğer yetkili makamların veya kurumların web sitelerinde de mevcuttur.


© All rights reserved by Heiko Maniero.

## G. Kişisel verilerin saklanacağı süre veya bu mümkün değilse, bu süreyi belirlemek için kullanılan kriterler (GDPR Madde 14(2) lit. a)

Kişisel verilerin saklanma süresini belirlemek için kullanılan kriter, ilgili yasal saklama süresidir. Bu sürenin sona ermesinden sonra, ilgili veriler, sözleşmenin yerine getirilmesi veya bir sözleşmenin başlatılması için artık gerekli olmadığı sürece rutin olarak silinir.

Yasal bir saklama süresi yoksa, kriter sözleşmeye dayalı veya dahili saklama süresidir.

## H. İşlemenin GDPR Madde 6(1) f bendine dayanması halinde kontrolör veya üçüncü bir tarafça gözetilen meşru menfaatlerin bildirilmesi (GDPR Madde 14(2) b bendi)

GDPR Madde 6(1) f bendi uyarınca, işleme faaliyeti ancak veri sahibinin kişisel verilerinin korunmasını gerektiren menfaatleri veya temel hak ve özgürlükleri tarafından bu menfaatlerin geçersiz kılındığı durumlar haricinde, kontrolör veya üçüncü bir tarafça gözetilen meşru menfaatler için gerekli olması halinde hukuka uygun olacaktır. GDPR'nin 47. Maddesinin 2. Fıkrasına göre, veri sahibi ile kontrolör arasında ilgili ve uygun bir ilişki olduğunda, örneğin veri sahibinin kontrolörün müşterisi olduğu durumlarda meşru bir menfaat mevcut olabilir. Şirketimizin GDPR Madde 6(1) f bendine dayanarak kişisel verileri işlediği tüm durumlarda, meşru menfaatimiz işimizi tüm çalışanlarımızın ve hissedarlarımızın refahı lehine yürütmektir.

## I. Veri sorumlusundan kişisel verilere erişim ve bunların düzeltilmesini veya silinmesini ya da veri sahibi ile ilgili işlemenin kısıtlanmasını talep etme ve veri işlemeye itiraz etme hakkının yanı sıra veri taşınabilirliği hakkının varlığı (GDPR Madde 14(2) c bendi)

Tüm veri sahipleri aşağıdaki haklara sahiptir:

***Erişim hakkı***

Her veri sahibi, kendisiyle ilgili kişisel verilere erişme hakkına sahiptir. Erişim hakkı tarafımızca işlenen tüm verileri kapsamaktadır. Bu hak, işlemenin yasallığından haberdar olmak ve bunu doğrulamak için kolaylıkla ve makul aralıklarla kullanılabilir (GDPR 63. Madde). Bu hak GDPR Madde 15'ten kaynaklanmaktadır. 15 GDPR'DEN KAYNAKLANMAKTADIR. Veri sahibi, erişim hakkını kullanmak için bizimle iletişime geçebilir.

***Düzeltme hakkı***

GDPR Madde 16 Cümle 1 uyarınca veri sahibi, kendisiyle ilgili yanlış kişisel verilerin düzeltilmesini gecikmeksizin kontrolörden talep etme hakkına sahiptir. Ayrıca, GDPR Madde 16 Cümle 2, veri sahibinin, işleme amaçlarını dikkate alarak, ek bir beyan sağlamak da dahil olmak üzere, eksik kişisel verilerin


© All rights reserved by Heiko Maniero.

tamamlanmasını isteme hakkına sahip olduğunu öngörmektedir. Veri sahibi, düzeltme hakkını kullanmak için bizimle iletişime geçebilir.

***Silme hakkı (unutulma hakkı)***

Buna ek olarak, veri sahipleri Madde 17 uyarınca silme ve unutulma hakkına sahiptir. 17 GDPR. Bu hak bizimle iletişime geçilerek de kullanılabilir. Ancak bu noktada, bu hakkın, işlemenin şirketimizin tabi olduğu yasal bir yükümlülüğü yerine getirmek için gerekli olduğu sürece geçerli olmadığını belirtmek isteriz, Madde 17 (3) lit. b GDPR. Bu, bir silme başvurusunu ancak yasal saklama süresinin sona ermesinden sonra onaylayabileceğimiz anlamına gelir.

***İşlemenin kısıtlanması hakkı***

GDPR Madde 18'e göre, herhangi bir veri sahibi işlemenin kısıtlanması hakkına sahiptir. İşlemenin kısıtlanması, GDPR Madde 18(1) lit. a-d'de belirtilen koşullardan birinin yerine getirilmesi halinde talep edilebilir. Veri sahibi, işlemenin kısıtlanması hakkını kullanmak için bizimle iletişime geçebilir.

***İtiraz hakkı***

Ayrıca, Madde 21 GDPR itiraz hakkını garanti eder. İlgili kişi itiraz hakkını kullanmak için bizimle iletişime geçebilir.

***Veri taşınabilirliği hakkı***

Madde 20 GDPR Madde 20, veri sahibine veri taşınabilirliği hakkı vermektedir. Bu hükme göre veri sahibi, GDPR Madde 20(1) lit. a ve b'de belirtilen koşullar altında, bir kontrolöre sağladığı kendisiyle ilgili kişisel verileri yapılandırılmış, yaygın olarak kullanılan ve makine tarafından okunabilir bir formatta alma ve bu verileri kişisel verilerin sağlandığı kontrolör tarafından engellenmeden başka bir kontrolöre iletme hakkına sahiptir. Veri sahibi, veri taşınabilirliği hakkını kullanmak için bizimle iletişime geçebilir.

## J. İşlemenin GDPR Madde 6(1) lit. a veya Madde 9(2) lit. a'ya dayandığı durumlarda, geri çekilmeden önce rızaya dayalı işlemenin yasallığını etkilemeksizin rızayı herhangi bir zamanda geri çekme hakkının varlığı (GDPR Madde 14(2) lit. d)

Kişisel verilerin işlenmesi GDPR Madde 6(1) a bendine dayanıyorsa 6(1) lit. a GDPR, veri sahibi kişisel verilerin bir veya daha fazla özel amaç için işlenmesine rıza göstermişse veya özel kategorilerdeki kişisel verilerin işlenmesine açık rızayı düzenleyen Madde 9(2) lit. a GDPR'ye dayanıyorsa, veri sahibi Madde 7(3) Cümle 1 GDPR'ye göre rızasını istediği zaman geri çekme hakkına sahiptir.

Rızanın geri çekilmesi, geri çekilmeden önce rızaya dayalı olarak gerçekleştirilen işleme faaliyetinin hukuka uygunluğunu etkilemez, GDPR Madde 7(3) Cümle 2. Rızanın geri çekilmesi rıza vermek kadar kolay olmalıdır, GDPR Madde GDPR Madde 7(3) Cümle 4. Bu nedenle, rızanın geri çekilmesi her zaman rızanın verildiği şekilde veya veri sahibi tarafından daha basit olduğu düşünülen başka bir şekilde gerçekleşebilir. Günümüz bilgi toplumunda, muhtemelen rızayı geri çekmenin en basit yolu basit bir e-postadır. Veri sahibi bize verdiği rızayı geri çekmek isterse, bize basit bir e-posta göndermesi yeterlidir. Alternatif olarak, veri sahibi rızasını geri çektiğini bize iletmek için başka bir yol seçebilir.


© All rights reserved by Heiko Maniero.

## K. Bir denetim makamına şikayette bulunma hakkı (GDPR Madde 14(2) lit. e, 77(1))

Veri sorumlusu olarak, GDPR Madde 14(2) lit. e uyarınca veri sahibini bir denetim makamına şikayette bulunma hakkı konusunda bilgilendirmekle yükümlüyüz. Bir denetim makamına şikayette bulunma hakkı, GDPR Madde 77(1) ile düzenlenmektedir. Bu hükme göre, diğer idari veya adli çözüm yollarına halel gelmeksizin, her veri sahibi, kendisiyle ilgili kişisel verilerin işlenmesinin Genel Veri Koruma Tüzüğü'nü ihlal ettiğini düşünmesi halinde, özellikle mutat meskeninin, iş yerinin veya iddia edilen ihlalin gerçekleştiği yerin bulunduğu Üye Devlet'teki bir denetim makamına şikayette bulunma hakkına sahiptir. Bir denetim makamına şikayette bulunma hakkı Birlik hukuku tarafından yalnızca tek bir denetim makamı nezdinde kullanılabilecek şekilde sınırlandırılmıştır (Resital 141 Cümle 1 GDPR). Bu kural, aynı veri sahibinin aynı konuda çifte şikayette bulunmasını önlemeyi amaçlamaktadır. Bu nedenle, bir veri sahibi hakkımızda şikayette bulunmak isterse, yalnızca tek bir denetim makamıyla iletişime geçmesi istenir.

## L. Kişisel verilerin kaynağı ve varsa kamuya açık kaynaklardan gelip gelmediği (GDPR Madde 14(2) f bendi)

Prensip olarak, kişisel veriler doğrudan veri sahibinden veya bir yetkili ile işbirliği içinde toplanır (örneğin, resmi bir kayıttan verilerin alınması). Veri sahiplerine ilişkin diğer veriler grup şirketlerinin transferlerinden elde edilir. Bu genel bilgi bağlamında, kişisel verilerin kaynaklandığı kesin kaynakların isimlendirilmesi ya imkansızdır ya da GD Madde 14(5) bendi anlamında orantısız bir çaba gerektirecektir. 14(5) lit. b GDPR. Prensip olarak, kamuya açık kaynaklardan kişisel veri toplamıyoruz.

Herhangi bir veri sahibi, kendisiyle ilgili kişisel verilerin tam kaynakları hakkında daha ayrıntılı bilgi almak için istediği zaman bizimle iletişime geçebilir. Çeşitli kaynakların kullanılmış olması nedeniyle kişisel verilerin kaynağının veri sahibine sağlanamadığı durumlarda, genel bilgiler sağlanmalıdır (Resital 61 Cümle 4 GDPR).

## M. GDPR Madde 22(1) ve (4)'te atıfta bulunulan profil oluşturma da dahil olmak üzere otomatik karar vermenin varlığı ve en azından bu durumlarda, ilgili mantık hakkında anlamlı bilgilerin yanı sıra veri sahibi için bu tür işlemenin önemi ve öngörülen sonuçları (GDPR Madde 14(2) lit. g)

Sorumlu bir şirket olarak genellikle otomatik karar verme veya profil oluşturmayı kullanmıyoruz. İstisnai durumlarda, otomatik karar verme veya profil oluşturma işlemi gerçekleştirirsek, veri sahibini ayrı olarak veya gizlilik politikamızın (web sitemizde) bir alt bölümü aracılığıyla bilgilendireceğiz. Bu durumda aşağıdakiler geçerlidir:

Profil oluşturma da dahil olmak üzere otomatik karar alma, (1) veri sahibi ile aramızda bir sözleşmenin yapılması veya bu sözleşmenin ifası için gerekli olması veya (2) buna, bağlı olduğumuz Birlik veya Üye


© All rights reserved by Heiko Maniero.

Devlet kanunları tarafından yetki verilmesi durumunda gerçekleşebilir. konu olan ve aynı zamanda veri sahibinin hak ve özgürlükleri ile meşru çıkarlarının korunmasına yönelik uygun önlemleri belirleyen; veya (3) bunun veri sahibinin açık rızasına dayanması.

GDPR Madde 22(2) (a) ve (c)'de atıfta bulunulan durumlarda, veri sahibinin hak ve özgürlükleri ile meşru çıkarlarını korumak için uygun önlemleri uygulayacağız. Bu durumlarda, kontrolörden insan müdahalesi alma, görüşünüzü ifade etme ve karara itiraz etme hakkına sahipsiniz.

İlgili mantığa ilişkin anlamlı bilgilerin yanı sıra söz konusu işlemenin veri sahibi açısından önemi ve öngörülen sonuçları gizlilik politikamızda belirtilmiştir.

## III. EU-U.S. Data Privacy Framework (EU-U.S. DPF), UK Extension to the EU-U.S. DPF, Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF)

Eğer organizasyonumuz EU-U.S. Data Privacy Framework (EU-U.S. DPF) ve/veya UK Extension to the EU-U.S. DPF ve/veya Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF) sertifikalı bir üye ise, aşağıdaki hususlar geçerlidir:

Biz, U.S. Department of Commerce tarafından belirlenen şekilde EU-U.S. Data Privacy Framework (EU-U.S. DPF) ve UK Extension to the EU-U.S. DPF ile Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF) kurallarına uyarız. Şirketimiz, Avrupa Birliği ve Birleşik Krallık'tan EU-U.S. DPF ve UK Extension to the EU-U.S. DPF kapsamında aldığı kişisel verilerin işlenmesiyle ilgili olarak EU-U.S. Data Privacy Framework Principles (EU-U.S. DPF Principles) ilkesine uyduğunu U.S. Department of Commerce'e teyit etmiştir. Şirketimiz, İsviçre'den Swiss-U.S. DPF kapsamında aldığı kişisel verilerin işlenmesiyle ilgili olarak Swiss-U.S. Data Privacy Framework Principles (Swiss-U.S. DPF Principles) ilkesine uyduğunu U.S. Department of Commerce'e teyit etmiştir. Gizlilik politikamızın hükümleri ile EU-U.S. DPF Principles ve/veya Swiss-U.S. DPF Principles arasında bir çelişki olması durumunda, Principles esas alınacaktır.

Data Privacy Framework (DPF) programı hakkında daha fazla bilgi edinmek ve sertifikamızı görmek için lütfen https://www.dataprivacyframework.gov/ adresini ziyaret edin.

Şirketimizin diğer ABD birimleri veya bağlı ortaklıkları, varsa, UK Extension to the EU-U.S. DPF ve Swiss-U.S. DPF Principals dahil olmak üzere, EU-U.S. DPF Principals'a da uymaktadır ve gizlilik politikamızda belirtilmiştir.

EU-U.S. DPF ve UK Extension to the EU-U.S. DPF ile Swiss-U.S. DPF ile uyum içinde, şirketimiz, Avrupa veri koruma yetkilileri ve Birleşik Krallık Information Commissioner's Office (ICO) ile İsviçre Federal Data Protection and Information Commissioner (EDÖB) tarafından kurulan organlarla işbirliği yapmayı ve EU-U.S. DPF ve UK Extension to the EU-U.S. DPF ile Swiss-U.S. DPF kapsamında aldığımız kişisel verilerin işlenmesiyle ilgili olarak çözümsüz şikayetler hakkında bu organların tavsiyelerine uymayı taahhüt eder.


© All rights reserved by Heiko Maniero.

İlgili kişilere, kişisel verilerin işlenmesiyle ilgili şikayetleri ele almakla sorumlu Avrupa veri koruma yetkilileri hakkında bu şeffaflık belgesinin üst kısmında bilgi veririz ve ilgili kişilere uygun ve ücretsiz bir hukuk yolu sağlarız.

Tüm ilgili kişilere, şirketimizin Federal Trade Commission (FTC) soruşturma ve icra yetkilerine tabi olduğunu bildiririz.

İlgili kişiler belirli koşullar altında bağlayıcı bir tahkim talep etme hakkına sahiptir. Organizasyonumuz, ilgili kişinin tahkim talebinde bulunması ve Principals'ın Ek I'ine uygun olarak prosedür ve şartlara uyması durumunda, talepleri çözmeyi ve DPF-Principles'ın Ek I'ine göre şartlara uymayı taahhüt eder.

Burada, kişisel verilerin üçüncü taraflara aktarılması durumunda organizasyonumuzun sorumluluğu hakkında tüm ilgili kişilere bilgi veriyoruz.

İlgili kişilerin veya veri koruma denetleme makamlarının soruları için, bu şeffaflık belgesinin üst kısmında belirtilen yerel temsilcileri atadık.

Kişisel verilerinizin (i) üçüncü taraflara aktarılıp aktarılmayacağı veya (ii) başlangıçta toplandıkları amaçtan veya daha sonra tarafınızdan onaylanan amaçlardan önemli ölçüde farklı bir amaç için kullanılıp kullanılmayacağı konusunda size seçim yapma imkanı sunuyoruz (Opt-out). Seçim hakkınızı kullanmak için açık, görünür ve kolayca erişilebilir bir mekanizma, veri koruma sorumlumuz (DSB) ile e-posta yoluyla iletişime geçmektir. Üçüncü bir tarafa aktarılan veriler, bizim adımıza ve talimatlarımız doğrultusunda görev yapan bir temsilci veya veri işleyici tarafından işleniyorsa, seçim hakkınız yoktur ve biz de bunu yapmakla yükümlü değiliz. Ancak, her zaman bu tür temsilci veya veri işleyici ile bir sözleşme yaparız.

Hassas veriler için (örneğin, sağlık durumu, ırk veya etnik köken, siyasi görüşler, dini veya felsefi inançlar, sendika üyeliği veya ilgili kişinin cinsel yaşamı hakkında bilgiler içeren kişisel veriler), bu verilerin (i) üçüncü taraflara aktarılması veya (ii) başlangıçta toplandıkları veya daha sonra onayladığınız amaçtan farklı bir amaç için kullanılması durumunda açık rızanızı (Opt-in) alırız. Ayrıca, üçüncü taraflardan aldığımız tüm kişisel verileri, üçüncü taraf bunları hassas olarak tanımlayıp işliyorsa hassas olarak ele alırız.

Yasal otoritelerden gelen meşru taleplere yanıt olarak kişisel verilerin ifşa edilmesi gerekliliği konusunda sizi burada bilgilendiriyoruz. Bu, ulusal güvenlik veya kolluk kuvvetleri gerekliliklerinin karşılanmasını içerir.

Kişisel verilerin sorumlu olarak hareket eden üçüncü bir tarafa aktarılması durumunda, bildirim ve seçim ilkesine (Principals) uyarız. Ayrıca, bu verilerin yalnızca sınırlı ve belirli amaçlar için, sizin verdiğiniz onay doğrultusunda işlenmesini ve alıcının DPF'nin ilkelerine (Principals) eşdeğer koruma seviyesini sağladığını ve bu yükümlülüğü daha fazla yerine getiremeyeceğini tespit ettiğinde bize bildirmesini şart koşan bir sözleşme yaparız. Sözleşme, sorumlu olarak hareket eden üçüncü tarafın bu tür bir durum tespit edildiğinde işleme faaliyetlerini durdurmasını veya diğer uygun ve yeterli tedbirleri almasını gerektirir.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

Kişisel verilerin bir temsilci veya veri işleyici olarak hareket eden üçüncü bir tarafa aktarılması durumunda, (i) bu verileri yalnızca sınırlı ve belirli amaçlar için aktarırız; (ii) temsilci veya veri işleyicinin DPF-Principles'ın gerektirdiği şekilde en az aynı düzeyde veri koruması sağlamasını taahhüt ederiz; (iii) temsilci veya veri işleyicinin aktarılan kişisel verileri, DPF-Principles'a uygun olarak işlemelerini sağlamak için uygun ve yeterli önlemleri alırız; (iv) temsilci veya veri işleyiciden, bu yükümlülüğü daha fazla yerine getiremeyeceğini tespit ettiğinde organizasyonumuzu bilgilendirmesini talep ederiz; (v) bildirimden sonra (iv dahil), yetkisiz işlemi durdurmak ve sorunu düzeltmek için uygun ve yeterli adımları atarız; ve (vi) talep üzerine DPF Department'a bu temsilci ile yapılan ilgili veri koruma hükümlerinin bir özetini veya temsil niteliğinde bir örneğini sağlarız.

EU-U.S. DPF ve/veya UK Extension to the EU-U.S. DPF ve/veya Swiss-U.S. DPF ile uyumlu olarak, organizasyonumuz, EU veri koruma yetkilileri ve Birleşik Krallık Information Commissioner's Office (ICO) ile İsviçre Federal Data Protection and Information Commissioner (EDÖB) tarafından kurulan organlarla işbirliği yapmayı ve EU-U.S. DPF ve UK Extension to the EU-U.S. DPF ile Swiss-U.S. DPF kapsamında aldığımız iş ilişkileriyle ilgili kişisel verilerin işlenmesiyle ilgili olarak çözümsüz şikayetler hakkında bu organların tavsiyelerine uymayı taahhüt eder.

Geçici olarak Avrupa Birliği'nde (AB), Avrupa Ekonomik Alanı'nda (AEA) veya Birleşik Krallık'ta bulunan ya da ikametgahı veya mutat meskeni buralarda olan tüm veri sahipleri, Şeffaflık Belgemizde yayınlanan ve kişisel verilere erişim hakkı da dahil olmak üzere GDPR'nin 15 ila 22. maddelerinden kaynaklanan haklara ve veri sahibi haklarına sahiptir. Bu bilgileri tüm AB ve AEA dillerinde kullanıma sunduk. İngilizce versiyon Birleşik Krallık için geçerlidir.

İsviçre'de geçici olarak ikamet eden veya ikametgahı veya mutat meskeni orada bulunan tüm veri sahipleri, kişisel verilere erişim hakkı da dahil olmak üzere Şeffaflık Belgemizde yayınlanan İsviçre Veri Koruma Yasası (DPA) ve İsviçre Veri Koruma Yönetmeliği (DPR) kapsamındaki haklara ve veri sahibi haklarına sahiptir. Bu bilgileri İsviçre'nin üç resmi dilinde (Almanca, İtalyanca ve Fransızca) sağladık.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

# TURKISH: Çalışanlar ve Başvuru Sahipleri için Kişisel Verilerin İşlenmesi Hakkında Bilgilendirme (GDPR Madde 13, 14)

Sayın Bay veya Bayan,

Çalışanların ve başvuru sahiplerinin kişisel verileri özel korumayı hak etmektedir. Hedefimiz, veri koruma düzeyimizi yüksek bir standartta tutmaktır. Bu nedenle, veri koruma ve veri güvenliği konseptlerimizi rutin olarak geliştiriyoruz.

Elbette, veri korumaya ilişkin yasal hükümlere uyuyoruz. GDPR Madde 13, 14'e göre, kontrolörler kişisel verileri işlerken belirli bilgi gereksinimlerini karşılar. Bu belge bu yükümlülükleri yerine getirmektedir.

Yasal düzenleme terminolojisi karmaşıktır. Ne yazık ki, bu belgenin hazırlanmasında yasal terimlerin kullanılmasından vazgeçilememiştir. Bu nedenle, bu belge, kullanılan terimler veya formülasyonlarla ilgili tüm sorularınız için her zaman bizimle iletişime geçebileceğinizi belirtmek isteriz.

## I. Veri sahibinden kişisel veriler toplandığında bilgi gerekliliklerine uygunluk (GDPR Madde 13)

### A. Kontrolörün kimliği ve iletişim bilgileri (GDPR Madde 13(1) lit. a)

Yukarıya bakın

### B. Veri Koruma Görevlisinin iletişim bilgileri (GDPR Madde 13(1) lit. b)

Yukarıya bakın

### C. Kişisel verilerin işlenme amaçları ve işlemenin yasal dayanağı (GDPR Madde 13(1) lit. c)

Başvuru sahibinin verileri için, veri işlemenin amacı işe alım sürecinde başvurunun incelenmesidir. Bu amaçla, tarafınızdan sağlanan tüm verileri işlemekteyiz. İşe alım sürecinde sunulan verilere dayanarak, bir iş görüşmesine davet edilip edilmediğinizi kontrol edeceğiz (seçim sürecinin bir parçası). Genel olarak uygun adaylar söz konusu olduğunda, özellikle iş görüşmesi bağlamında, seçim kararımız için gerekli olan ve tarafınızdan sağlanan diğer bazı kişisel verileri işleriz. Tarafımızca işe alınmanız halinde, başvuru sahibinin verileri otomatik olarak çalışan verilerine dönüşecektir. İşe alım sürecinin bir parçası olarak,


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

sizden talep ettiğimiz ve sözleşmenizi başlatmak veya yerine getirmek için gerekli olan diğer kişisel verilerinizi işleyeceğiz (kişisel kimlik numaraları veya vergi numaraları gibi). Çalışan verileri için veri işlemenin amacı, iş sözleşmesinin yerine getirilmesi veya iş ilişkisine uygulanabilir diğer yasal hükümlere (örneğin vergi kanunu) uyulması ve kişisel verilerinizin sizinle yapılan iş sözleşmesini yerine getirmek için kullanılmasıdır (örneğin adınızın ve iletişim bilgilerinizin şirket içinde veya müşterilere yayınlanması). Çalışan verileri, yasal saklama sürelerini yerine getirmek için iş ilişkisinin sona ermesinden sonra saklanır.

Veri işlemenin yasal dayanağı GDPR Madde 6(1) lit. b, GDPR Madde 9(2) lit. b ve h, GDPR Madde 88(1) ve Almanya için Madde 26 BDSG (Federal Veri Koruma Yasası) gibi ulusal mevzuattır.

## D. Kişisel verilerin alıcılarının kategorileri (GDPR Madde 13(1) lit. e)

Kamu yetkilileri

Dış organlar

Diğer dış kuruluşlar

Dahili işleme

Grup içi işleme

Diğer kurumlar

Üçüncü ülkelerdeki ve varsa uluslararası kuruluşlardaki işleyicilerimizin ve veri alıcılarımızın bir listesi ya web sitemizde yayınlanır ya da bizden ücretsiz olarak talep edilebilir. Bu listeyi talep etmek için lütfen veri koruma görevlimizle iletişime geçin.

## E. Üçüncü bir ülkedeki alıcılar ve uygun veya uygun koruma önlemleri ve bunların bir kopyasının elde edilebileceği veya kullanıma sunulduğu araçlar (GDPR Madde 13 (1) f, 46 (1), 46 (2) c bendi)

Grubumuzun bir parçası olan ve üçüncü bir ülkede iş yeri veya ofisi bulunan tüm şirketler ve şubeler (bundan böyle "grup şirketleri" olarak anılacaktır) kişisel verilerin alıcılarına ait olabilir. Tüm grup şirketlerinin veya alıcıların bir listesi bizden talep edilebilir.

GDPR madde 46(1) uyarınca, bir kontrolör veya işleyici kişisel verileri üçüncü bir ülkeye yalnızca kontrolör veya işleyicinin uygun güvenceleri sağlaması ve veri sahipleri için uygulanabilir veri sahibi hakları ve etkili yasal çözüm yollarının mevcut olması koşuluyla aktarabilir. Uygun güvenceler, standart sözleşme maddeleri vasıtasıyla bir denetim makamından herhangi bir özel izin alınmasını gerektirmeksizin sağlanabilir, GDPR madde 46(2) lit. c.


© All rights reserved by Heiko Maniero.

Avrupa Birliği'nin standart sözleşme maddeleri veya diğer uygun güvenceler, kişisel verilerin ilk iletiminden önce üçüncü ülkelerden gelen tüm alıcılarla kararlaştırılır. Sonuç olarak, uygun güvencelerin, uygulanabilir veri sahibi haklarının ve veri sahipleri için etkili yasal çözüm yollarının garanti edilmesi sağlanır. Her veri sahibi, standart sözleşme maddelerinin bir kopyasını bizden temin edebilir. Standart sözleşme maddeleri Avrupa Birliği Resmi Gazetesinde de mevcuttur.

Genel Veri Koruma Tüzüğü'nün (GDPR) 45(3) maddesi, Avrupa Komisyonu'na, bir uygulama yasası aracılığıyla, AB dışındaki bir ülkenin yeterli düzeyde koruma sağladığına karar verme hakkı vermektedir. Bu, kişisel veriler için AB'dekine genel olarak eşdeğer bir koruma düzeyi anlamına gelir. Yeterli düzeyde koruma sağlandığına dair kararların etkisi, kişisel verilerin AB'den (ve Norveç, Lihtenştayn ve İzlanda'dan) üçüncü bir ülkeye başka engeller olmaksızın serbestçe akabilmesidir. Benzer kurallar Birleşik Krallık, İsviçre ve diğer bazı ülkelerde de uygulanmaktadır.

Avrupa Komisyonu veya başka bir ülkenin hükümetinin üçüncü bir ülkenin yeterli düzeyde koruma sağladığına karar vermesi ve geçerli çerçevenin (örneğin, EU-U.S. Data Privacy Framework, Swiss-U.S. Data Privacy Framework, UK-Extension to the EU-U.S. Data Privacy Framework) belirlenmesi durumunda, tarafımızdan bu tür çerçevelerin üyelerine (örneğin, kendi kendini onaylayan kuruluşlar) yapılan tüm aktarımlar yalnızca bu kuruluşların ilgili çerçeveye üyeliğine dayanmaktadır. Bizim veya grup kuruluşlarımızdan birinin bu tür bir çerçevenin üyesi olması durumunda, bize veya grup kuruluşumuza yapılan tüm aktarımlar yalnızca kuruluşun bu çerçeveye üyeliğine dayanır.

Herhangi bir veri sahibi çerçevelerin bir kopyasını bizden temin edebilir. Ayrıca, çerçeveler Avrupa Birliği Resmi Gazetesi'nde veya yayınlanan yasal materyallerde veya denetim makamlarının veya diğer yetkili makamların veya kurumların web sitelerinde de mevcuttur.

## F. Kişisel verilerin saklanacağı süre veya bu mümkün değilse, bu süreyi belirlemek için kullanılan kriterler (GDPR Madde 13(2) lit. a)

Başvuru sahiplerinin kişisel verilerinin saklanma süresi 6 aydır. Çalışan verileri için ilgili yasal saklama süresi geçerlidir. Bu sürenin sona ermesinden sonra, ilgili veriler, sözleşmenin yerine getirilmesi veya bir sözleşmenin başlatılması için artık gerekli olmadığı sürece rutin olarak silinir.

## G. Veri sorumlusundan kişisel verilere erişim ve bunların düzeltilmesini veya silinmesini ya da veri sahibi ile ilgili işlemenin kısıtlanmasını talep etme veya işlemeye itiraz etme hakkının yanı sıra veri taşınabilirliği hakkının varlığı (GDPR Madde 13(2) lit. b)

Tüm veri sahipleri aşağıdaki haklara sahiptir:


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

***Erişim hakkı***

Her veri sahibi, kendisiyle ilgili kişisel verilere erişme hakkına sahiptir. Erişim hakkı tarafımızca işlenen tüm verileri kapsamaktadır. Bu hak, işlemenin yasallığından haberdar olmak ve bunu doğrulamak için kolaylıkla ve makul aralıklarla kullanılabilir (GDPR 63. Madde). Bu hak GDPR Madde 15'ten kaynaklanmaktadır. 15 GDPR'DEN KAYNAKLANMAKTADIR. Veri sahibi, erişim hakkını kullanmak için bizimle iletişime geçebilir.

***Düzeltme hakkı***

GDPR Madde 16 Cümle 1 uyarınca veri sahibi, kendisiyle ilgili yanlış kişisel verilerin düzeltilmesini gecikmeksizin kontrolörden talep etme hakkına sahiptir. Ayrıca, GDPR Madde 16 Cümle 2, veri sahibinin, işleme amaçlarını dikkate alarak, ek bir beyan sağlamak da dahil olmak üzere, eksik kişisel verilerin tamamlanmasını isteme hakkına sahip olduğunu öngörmektedir. Veri sahibi, düzeltme hakkını kullanmak için bizimle iletişime geçebilir.

***Silme hakkı (unutulma hakkı)***

Buna ek olarak, veri sahipleri Madde 17 uyarınca silme ve unutulma hakkına sahiptir. 17 GDPR. Bu hak bizimle iletişime geçilerek de kullanılabilir. Ancak bu noktada, işlemenin şirketimizin tabi olduğu yasal bir yükümlülüğü yerine getirmek için gerekli olduğu durumlarda bu hakkın geçerli olmadığını belirtmek isteriz, GDPR Madde 17(3) lit. b. Bu, bir silme başvurusunu ancak yasal saklama süresinin sona ermesinden sonra onaylayabileceğimiz anlamına gelir.

***İşlemenin kısıtlanması hakkı***

GDPR Madde 18 uyarınca, herhangi bir veri sahibi işlemenin kısıtlanmasını talep etme hakkına sahiptir. İşlemenin kısıtlanması, GDPR Madde 18(1) lit. a-d'de belirtilen koşullardan birinin yerine getirilmesi halinde talep edilebilir. Veri sahibi, işlemenin kısıtlanması hakkını kullanmak için bizimle iletişime geçebilir.

***İtiraz hakkı***

Ayrıca, Madde 21 GDPR itiraz hakkını garanti eder. İlgili kişi itiraz hakkını kullanmak için bizimle iletişime geçebilir.

***Veri taşınabilirliği hakkı***

Madde 20 20 GDPR, veri sahibine veri taşınabilirliği hakkı tanır. Bu hüküm uyarınca, veri sahibi, GDPR Madde 20(1) lit. a ve b'de belirtilen koşullar altında, bir denetleyiciye sağladığı kendisiyle ilgili kişisel verileri yapılandırılmış, yaygın olarak kullanılan ve makine tarafından okunabilir bir formatta alma ve bu verileri kişisel verilerin sağlandığı denetleyiciden herhangi bir engel olmaksızın başka bir denetleyiciye iletme hakkına sahiptir. Veri sahibi, veri taşınabilirliği hakkını kullanmak için bizimle iletişime geçebilir.


© All rights reserved by Heiko Maniero.

## H. İşlemenin GDPR Madde 6(1) a bendine veya GDPR Madde 9(2) a bendine (GDPR Madde 13(2) c bendine) dayandığı durumlarda, geri çekilmeden önce rızaya dayalı işlemenin yasallığını etkilemeksizin rızayı herhangi bir zamanda geri çekme hakkının varlığı

Kişisel verilerin işlenmesi GDPR Madde 6(1) a bendine dayanıyorsa 6(1) lit. a GDPR, veri sahibi kişisel verilerin bir veya daha fazla spesifik amaç için işlenmesine rıza göstermişse veya özel kategorilerdeki kişisel verilerin işlenmesine açık rızayı düzenleyen Madde 9(2) lit. a GDPR'ye dayanıyorsa, veri sahibi Madde 7(3) Cümle 1 GDPR uyarınca rızasını istediği zaman geri çekme hakkına sahiptir.

Rızanın geri çekilmesi, geri çekilmeden önce rızaya dayalı olarak gerçekleştirilen işleme faaliyetinin hukuka uygunluğunu etkilemez, GDPR Madde 7(3) Cümle 2. Rızanın geri çekilmesi rıza vermek kadar kolay olmalıdır, GDPR Madde GDPR Madde 7(3) Cümle 4. Bu nedenle, rızanın geri çekilmesi her zaman rızanın verildiği şekilde veya veri sahibi tarafından daha basit olduğu düşünülen başka bir şekilde gerçekleşebilir. Günümüz bilgi toplumunda, muhtemelen rızayı geri çekmenin en basit yolu basit bir e-postadır. Veri sahibi bize verdiği rızayı geri çekmek isterse, bize basit bir e-posta göndermesi yeterlidir. Alternatif olarak, veri sahibi rızasını geri çektiğini bize iletmek için başka bir yol seçebilir.

## I. Bir denetim makamına şikayette bulunma hakkı (GDPR Madde 13(2) lit. d, 77(1))

Veri sorumlusu olarak, veri sahibini bir denetim makamına şikayette bulunma hakkı konusunda bilgilendirmekle yükümlüyüz, GDPR Madde 13(2) lit. d. Bir denetim makamına şikayette bulunma hakkı, GDPR Madde 77(1) ile düzenlenmektedir. Bu hükme göre, diğer idari veya adli çözüm yollarına halel gelmeksizin, her veri sahibi, kendisiyle ilgili kişisel verilerin işlenmesinin Genel Veri Koruma Tüzüğü'nü ihlal ettiğini düşünmesi halinde, özellikle mutat meskeninin, iş yerinin veya iddia edilen ihlalin gerçekleştiği yerin bulunduğu Üye Devlet'teki bir denetim makamına şikayette bulunma hakkına sahiptir. Bir denetim makamına şikayette bulunma hakkı Birlik hukuku tarafından yalnızca tek bir denetim makamı nezdinde kullanılabilecek şekilde sınırlandırılmıştır (Resital 141 Cümle 1 GDPR). Bu kural, aynı veri sahibinin aynı konuda çifte şikayette bulunmasını önlemeyi amaçlamaktadır. Bu nedenle, bir veri sahibi hakkımızda şikayette bulunmak isterse, yalnızca tek bir denetim makamıyla iletişime geçmesi istenir.

## J. Yasal veya sözleşmesel gereklilik olarak kişisel verilerin sağlanması; Bir sözleşme yapmak için gerekli gereklilik; Veri sahibinin kişisel verileri sağlama yükümlülüğü; Bu tür verilerin sağlanmamasının olası sonuçları (GDPR Madde 13(2) lit. e)

Kişisel verilerin sağlanmasının kısmen kanunen gerekli olduğunu (örn. vergi düzenlemeleri) veya sözleşme hükümlerinden de kaynaklanabileceğini (örn. sözleşme ortağı hakkında bilgi) açıklığa kavuşturuyoruz.


© All rights reserved by Heiko Maniero.

Bazen, veri sahibinin bize kişisel verilerini sağladığı ve daha sonra tarafımızdan işlenmesi gereken bir sözleşme yapılması gerekebilir. Örneğin, şirketimiz kendisiyle bir sözleşme imzaladığında veri sahibi bize kişisel verilerini sağlamakla yükümlüdür. Kişisel verilerin sağlanmaması, veri sahibi ile sözleşmenin akdedilememesi sonucunu doğuracaktır.

Kişisel veriler veri sahibi tarafından sağlanmadan önce, veri sahibi bizimle iletişime geçmelidir. Veri sahibine, kişisel verilerin sağlanmasının yasa veya sözleşme gereği olup olmadığını veya sözleşmenin imzalanması için gerekli olup olmadığını, kişisel verileri sağlama yükümlülüğü olup olmadığını ve kişisel verilerin sağlanmamasının sonuçlarını açıklıyoruz.

### K. GDPR Madde 22(1) ve (4)'te atıfta bulunulan profil oluşturma da dahil olmak üzere otomatik karar vermenin varlığı ve en azından bu durumlarda, ilgili mantık hakkında anlamlı bilgilerin yanı sıra veri sahibi için bu tür işlemenin önemi ve öngörülen sonuçları (GDPR Madde 13 (2) lit. f)

Sorumlu bir şirket olarak genellikle otomatik karar verme veya profil oluşturmayı kullanmıyoruz. İstisnai durumlarda, otomatik karar verme veya profil oluşturma işlemi gerçekleştirirsek, veri sahibini ayrı olarak veya gizlilik politikamızın (web sitemizde) bir alt bölümü aracılığıyla bilgilendireceğiz. Bu durumda aşağıdakiler geçerlidir:

Profil oluşturma da dahil olmak üzere otomatik karar alma, (1) veri sahibi ile aramızda bir sözleşmenin yapılması veya bu sözleşmenin ifası için gerekli olması veya (2) buna, bağlı olduğumuz Birlik veya Üye Devlet kanunları tarafından yetki verilmesi durumunda gerçekleşebilir. konu olan ve aynı zamanda veri sahibinin hak ve özgürlükleri ile meşru çıkarlarının korunmasına yönelik uygun önlemleri belirleyen; veya (3) bunun veri sahibinin açık rızasına dayanması.

GDPR Madde 22(2) (a) ve (c)'de atıfta bulunulan durumlarda, veri sahibinin hak ve özgürlükleri ile meşru çıkarlarını korumak için uygun önlemleri uygulayacağız. Bu durumlarda, kontrolörden insan müdahalesi alma, görüşünüzü ifade etme ve karara itiraz etme hakkına sahipsiniz.

İlgili mantığa ilişkin anlamlı bilgilerin yanı sıra söz konusu işlemenin veri sahibi açısından önemi ve öngörülen sonuçları gizlilik politikamızda belirtilmiştir.

## II. Kişisel verilerin veri sahibinden toplanmadığı durumlarda bilgi gerekliliklerine uygunluk (GDPR Madde 14)

### A. Kontrolörün kimliği ve iletişim bilgileri (GDPR Madde 14(1) lit. a)

Yukarıya bakın


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## B. Veri Koruma Görevlisinin iletişim bilgileri (GDPR Madde 14(1) lit. b)

Yukarıya bakın

## C. Kişisel verilerin işlenme amaçları ve işlemenin yasal dayanağı (GDPR Madde 14(1) lit. c)

Başvuru sahibinin veri sahibinden toplanmayan verileri için, veri işlemenin amacı işe alım sürecinde başvurunun incelenmesidir. Bu amaçla, sizden toplanmayan verileri işleyebiliriz. İşe alım sürecinde işlenen verilere dayanarak, bir iş görüşmesine davet edilip edilmediğinizi kontrol edeceğiz (seçim sürecinin bir parçası). Tarafımızdan işe alınırsanız, başvuru sahibinin verileri otomatik olarak çalışan verilerine dönüşecektir. Çalışan verileri için, veri işlemenin amacı iş sözleşmesinin yerine getirilmesi veya iş ilişkisi için geçerli olan diğer yasal hükümlere uyulmasıdır. Çalışan verileri, yasal saklama sürelerini yerine getirmek için iş ilişkisinin sona ermesinden sonra saklanır.

Veri işlemenin yasal dayanağı GDPR Madde 6(1) b ve f bentleri, GDPR Madde 9(2) b ve h bentleri, GDPR Madde 88(1) ve Almanya için BDSG (Federal Veri Koruma Yasası) Madde 26 gibi ulusal mevzuattır.

## D. İlgili kişisel veri kategorileri (GDPR Madde 14(1) lit. d)

Başvuru sahibinin verileri

Çalışan verileri

## E. Kişisel verilerin alıcılarının kategorileri (GDPR Madde 14(1) lit. e)

Kamu yetkilileri

Dış organlar

Diğer dış kuruluşlar

Dahili işleme

Grup içi işleme

Diğer kurumlar


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

Üçüncü ülkelerdeki ve varsa uluslararası kuruluşlardaki işleyicilerimizin ve veri alıcılarımızın bir listesi ya web sitemizde yayınlanır ya da bizden ücretsiz olarak talep edilebilir. Bu listeyi talep etmek için lütfen veri koruma görevlimizle iletişime geçin.

## F. Üçüncü bir ülkedeki alıcılar ve uygun veya uygun koruma önlemleri ve bunların bir kopyasının elde edilebileceği veya kullanıma sunulduğu araçlar (GDPR Madde 14(1) f, 46(1), 46(2) c bendi)

Grubumuzun bir parçası olan ve üçüncü bir ülkede iş yeri veya ofisi bulunan tüm şirketler ve şubeler (bundan böyle "grup şirketleri" olarak anılacaktır) kişisel verilerin alıcılarına ait olabilir. Tüm grup şirketlerinin veya alıcıların bir listesi bizden talep edilebilir.

GDPR madde 46(1) uyarınca, bir kontrolör veya işleyici kişisel verileri üçüncü bir ülkeye ancak kontrolör veya işleyicinin uygun güvenceleri sağlaması ve veri sahipleri için uygulanabilir veri sahibi hakları ve etkili yasal çözüm yollarının mevcut olması koşuluyla aktarabilir. Uygun güvenceler, GDPR madde 46(2) bent c uyarınca standart veri koruma hükümleri vasıtasıyla bir denetim makamından herhangi bir özel izin alınmasını gerektirmeksizin sağlanabilir.

Avrupa Birliği'nin standart sözleşme maddeleri veya diğer uygun güvenceler, kişisel verilerin ilk iletiminden önce üçüncü ülkelerden gelen tüm alıcılarla kararlaştırılır. Sonuç olarak, uygun güvencelerin, uygulanabilir veri sahibi haklarının ve veri sahipleri için etkili yasal çözüm yollarının garanti edilmesi sağlanır. Her veri sahibi, standart sözleşme maddelerinin bir kopyasını bizden temin edebilir. Standart sözleşme maddeleri Avrupa Birliği Resmi Gazetesinde de mevcuttur.

Genel Veri Koruma Tüzüğü'nün (GDPR) 45(3) maddesi, Avrupa Komisyonu'na, bir uygulama yasası aracılığıyla, AB dışındaki bir ülkenin yeterli düzeyde koruma sağladığına karar verme hakkı vermektedir. Bu, kişisel veriler için AB'dekine genel olarak eşdeğer bir koruma düzeyi anlamına gelir. Yeterli düzeyde koruma sağlandığına dair kararların etkisi, kişisel verilerin AB'den (ve Norveç, Lihtenştayn ve İzlanda'dan) üçüncü bir ülkeye başka engeller olmaksızın serbestçe akabilmesidir. Benzer kurallar Birleşik Krallık, İsviçre ve diğer bazı ülkelerde de uygulanmaktadır.

Avrupa Komisyonu veya başka bir ülkenin hükümetinin üçüncü bir ülkenin yeterli düzeyde koruma sağladığına karar vermesi ve geçerli çerçevenin (örneğin, EU-U.S. Data Privacy Framework, Swiss-U.S. Data Privacy Framework, UK-Extension to the EU-U.S. Data Privacy Framework) belirlenmesi durumunda, tarafımızdan bu tür çerçevelerin üyelerine (örneğin, kendi kendini onaylayan kuruluşlar) yapılan tüm aktarımlar yalnızca bu kuruluşların ilgili çerçeveye üyeliğine dayanmaktadır. Bizim veya grup kuruluşlarımızdan birinin bu tür bir çerçevenin üyesi olması durumunda, bize veya grup kuruluşumuza yapılan tüm aktarımlar yalnızca kuruluşun bu çerçeveye üyeliğine dayanır.

Herhangi bir veri sahibi çerçevelerin bir kopyasını bizden temin edebilir. Ayrıca, çerçeveler Avrupa Birliği Resmi Gazetesi'nde veya yayınlanan yasal materyallerde veya denetim makamlarının veya diğer yetkili makamların veya kurumların web sitelerinde de mevcuttur.


© All rights reserved by Heiko Maniero.

## G. Kişisel verilerin saklanacağı süre veya bu mümkün değilse, bu süreyi belirlemek için kullanılan kriterler (GDPR Madde 14(2) lit. a)

Başvuru sahiplerinin kişisel verilerinin saklanma süresi 6 aydır. Çalışan verileri için ilgili yasal saklama süresi geçerlidir. Bu sürenin sona ermesinden sonra, ilgili veriler, sözleşmenin yerine getirilmesi veya bir sözleşmenin başlatılması için artık gerekli olmadığı sürece rutin olarak silinir.

## H. İşlemenin GDPR Madde 6(1) f bendine dayanması halinde kontrolör veya üçüncü bir tarafça gözetilen meşru menfaatlerin bildirilmesi (GDPR Madde 14(2) b bendi)

GDPR Madde 6(1) f bendi uyarınca, işleme faaliyeti ancak veri sahibinin kişisel verilerinin korunmasını gerektiren menfaatleri veya temel hak ve özgürlükleri tarafından bu menfaatlerin geçersiz kılındığı durumlar haricinde, kontrolör veya üçüncü bir tarafça gözetilen meşru menfaatler için gerekli olması halinde hukuka uygun olacaktır. GDPR'nin 47. Maddesinin 2. Fıkrasına göre, veri sahibi ile kontrolör arasında ilgili ve uygun bir ilişki olduğunda, örneğin veri sahibinin kontrolörün müşterisi olduğu durumlarda meşru bir menfaat mevcut olabilir. Şirketimizin başvuru sahibinin verilerini GDPR Madde 6(1) f bendine dayanarak işlediği tüm durumlarda, meşru menfaatimiz uygun personel ve profesyonellerin istihdam edilmesidir.

## I. Veri sorumlusundan kişisel verilere erişim ve bunların düzeltilmesini veya silinmesini ya da veri sahibi ile ilgili işlemenin kısıtlanmasını talep etme ve veri işlemeye itiraz etme hakkının yanı sıra veri taşınabilirliği hakkının varlığı (GDPR Madde 14(2) c bendi)

Tüm veri sahipleri aşağıdaki haklara sahiptir:

***Erişim hakkı***

Her veri sahibi, kendisiyle ilgili kişisel verilere erişme hakkına sahiptir. Erişim hakkı tarafımızca işlenen tüm verileri kapsamaktadır. Bu hak, işlemenin yasallığından haberdar olmak ve bunu doğrulamak için kolaylıkla ve makul aralıklarla kullanılabilir (GDPR 63. Madde). Bu hak GDPR Madde 15'ten kaynaklanmaktadır. 15 GDPR'DEN KAYNAKLANMAKTADIR. Veri sahibi, erişim hakkını kullanmak için bizimle iletişime geçebilir.

***Düzeltme hakkı***

GDPR Madde 16 Cümle 1 uyarınca veri sahibi, kendisiyle ilgili yanlış kişisel verilerin düzeltilmesini gecikmeksizin kontrolörden talep etme hakkına sahiptir. Ayrıca, GDPR Madde 16 Cümle 2, veri sahibinin, işleme amaçlarını dikkate alarak, ek bir beyan sağlamak da dahil olmak üzere, eksik kişisel verilerin


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

tamamlanmasını isteme hakkına sahip olduğunu öngörmektedir. Veri sahibi, düzeltme hakkını kullanmak için bizimle iletişime geçebilir.

***Silme hakkı (unutulma hakkı)***

Buna ek olarak, veri sahipleri Madde 17 uyarınca silme ve unutulma hakkına sahiptir. 17 GDPR. Bu hak bizimle iletişime geçilerek de kullanılabilir. Ancak bu noktada, bu hakkın, işlemenin şirketimizin tabi olduğu yasal bir yükümlülüğü yerine getirmek için gerekli olduğu sürece geçerli olmadığını belirtmek isteriz, Madde 17 (3) lit. b GDPR. Bu, bir silme başvurusunu ancak yasal saklama süresinin sona ermesinden sonra onaylayabileceğimiz anlamına gelir.

***İşlemenin kısıtlanması hakkı***

GDPR Madde 18'e göre, herhangi bir veri sahibi işlemenin kısıtlanması hakkına sahiptir. İşlemenin kısıtlanması, GDPR Madde 18(1) lit. a-d'de belirtilen koşullardan birinin yerine getirilmesi halinde talep edilebilir. Veri sahibi, işlemenin kısıtlanması hakkını kullanmak için bizimle iletişime geçebilir.

***İtiraz hakkı***

Ayrıca, Madde 21 GDPR itiraz hakkını garanti eder. İlgili kişi itiraz hakkını kullanmak için bizimle iletişime geçebilir.

***Veri taşınabilirliği hakkı***

Madde 20 GDPR Madde 20, veri sahibine veri taşınabilirliği hakkı vermektedir. Bu hükme göre veri sahibi, GDPR Madde 20(1) lit. a ve b'de belirtilen koşullar altında, bir denetleyiciye sağladığı kendisiyle ilgili kişisel verileri yapılandırılmış, yaygın olarak kullanılan ve makine tarafından okunabilir bir formatta alma ve bu verileri kişisel verilerin sağlandığı denetleyiciden herhangi bir engel olmaksızın başka bir denetleyiciye iletme hakkına sahiptir. Veri sahibi, veri taşınabilirliği hakkını kullanmak için bizimle iletişime geçebilir.

## J. İşlemenin GDPR Madde 6(1) lit. a veya Madde 9(2) lit. a'ya dayandığı durumlarda, geri çekilmeden önce rızaya dayalı işlemenin yasallığını etkilemeksizin rızayı herhangi bir zamanda geri çekme hakkının varlığı (GDPR Madde 14(2) lit. d)

Kişisel verilerin işlenmesi GDPR Madde 6(1) a bendine dayanıyorsa 6(1) lit. a GDPR, veri sahibi kişisel verilerin bir veya daha fazla spesifik amaç için işlenmesine rıza göstermişse veya özel kategorilerdeki kişisel verilerin işlenmesine açık rızayı düzenleyen Madde 9(2) lit. a GDPR'ye dayanıyorsa, veri sahibi Madde 7(3) Cümle 1 GDPR uyarınca rızasını istediği zaman geri çekme hakkına sahiptir.

Rızanın geri çekilmesi, geri çekilmeden önce rızaya dayalı olarak gerçekleştirilen işleme faaliyetinin hukuka uygunluğunu etkilemez, GDPR Madde 7(3) Cümle 2. Rızanın geri çekilmesi rıza vermek kadar kolay olmalıdır, GDPR Madde GDPR Madde 7(3) Cümle 4. Bu nedenle, rızanın geri çekilmesi her zaman rızanın verildiği şekilde veya veri sahibi tarafından daha basit olduğu düşünülen başka bir şekilde gerçekleşebilir. Günümüz bilgi toplumunda, muhtemelen rızayı geri çekmenin en basit yolu basit bir e-


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

postadır. Veri sahibi bize verdiği rızayı geri çekmek isterse, bize basit bir e-posta göndermesi yeterlidir. Alternatif olarak, veri sahibi rızasını geri çektiğini bize iletmek için başka bir yol seçebilir.

## K. Bir denetim makamına şikayette bulunma hakkı (GDPR Madde 14(2) lit. e, 77(1))

Veri sorumlusu olarak, veri sahibini bir denetim makamına şikayette bulunma hakkı konusunda bilgilendirmekle yükümlüyüz, GDPR Madde 14(2) lit. e. Bir denetim makamına şikayette bulunma hakkı, GDPR Madde 77(1) ile düzenlenmektedir. Bu hükme göre, diğer idari veya adli çözüm yollarına halel gelmeksizin, her veri sahibi, kendisiyle ilgili kişisel verilerin işlenmesinin Genel Veri Koruma Tüzüğü'nü ihlal ettiğini düşünmesi halinde, özellikle mutat meskeninin, iş yerinin veya iddia edilen ihlalin gerçekleştiği yerin bulunduğu Üye Devlet'teki bir denetim makamına şikayette bulunma hakkına sahiptir. Bir denetim makamına şikayette bulunma hakkı Birlik hukuku tarafından yalnızca tek bir denetim makamı nezdinde kullanılabilecek şekilde sınırlandırılmıştır (Resital 141 Cümle 1 GDPR). Bu kural, aynı veri sahibinin aynı konuda çifte şikayette bulunmasını önlemeyi amaçlamaktadır. Bu nedenle, bir veri sahibi hakkımızda şikayette bulunmak isterse, yalnızca tek bir denetim makamıyla iletişime geçmesi istenir.

## L. Kişisel verilerin kaynağı ve varsa kamuya açık kaynaklardan gelip gelmediği (GDPR Madde 14(2) f bendi)

Prensip olarak, kişisel veriler doğrudan veri sahibinden veya bir yetkili ile işbirliği içinde toplanır (örneğin, verilerin resmi bir kayıttan alınması). Veri sahiplerine ilişkin diğer veriler grup şirketlerinin transferlerinden elde edilir. Bu genel bilgiler bağlamında, kişisel verilerin kaynaklandığı kesin kaynakların isimlendirilmesi ya imkansızdır ya da GD Madde 14(5) bendi anlamında orantısız bir çaba gerektirecektir. 14(5) lit. b GDPR. Prensip olarak, kamuya açık kaynaklardan kişisel veri toplamıyoruz.

Herhangi bir veri sahibi, kendisiyle ilgili kişisel verilerin tam kaynakları hakkında daha ayrıntılı bilgi almak için istediği zaman bizimle iletişime geçebilir. Çeşitli kaynakların kullanılmış olması nedeniyle kişisel verilerin kaynağının veri sahibine sağlanamadığı durumlarda, genel bilgiler sağlanmalıdır (Resital 61 Cümle 4 GDPR).

## M. GDPR Madde 22(1) ve (4)'te atıfta bulunulan profil oluşturma da dahil olmak üzere otomatik karar vermenin varlığı ve en azından bu durumlarda, ilgili mantık hakkında anlamlı bilgilerin yanı sıra veri sahibi için bu tür işlemenin önemi ve öngörülen sonuçları (GDPR Madde 14(2) lit. g)

Sorumlu bir şirket olarak genellikle otomatik karar verme veya profil oluşturmayı kullanmıyoruz. İstisnai durumlarda, otomatik karar verme veya profil oluşturma işlemi gerçekleştirirsek, veri sahibini ayrı olarak veya gizlilik politikamızın (web sitemizde) bir alt bölümü aracılığıyla bilgilendireceğiz. Bu durumda aşağıdakiler geçerlidir:


© All rights reserved by Heiko Maniero.

Profil oluşturma da dahil olmak üzere otomatik karar alma, (1) veri sahibi ile aramızda bir sözleşmenin yapılması veya bu sözleşmenin ifası için gerekli olması veya (2) buna, bağlı olduğumuz Birlik veya Üye Devlet kanunları tarafından yetki verilmesi durumunda gerçekleşebilir. konu olan ve aynı zamanda veri sahibinin hak ve özgürlükleri ile meşru çıkarlarının korunmasına yönelik uygun önlemleri belirleyen; veya (3) bunun veri sahibinin açık rızasına dayanması.

GDPR Madde 22(2) (a) ve (c)'de atıfta bulunulan durumlarda, veri sahibinin hak ve özgürlükleri ile meşru çıkarlarını korumak için uygun önlemleri uygulayacağız. Bu durumlarda, kontrolörden insan müdahalesi alma, görüşünüzü ifade etme ve karara itiraz etme hakkına sahipsiniz.

İlgili mantığa ilişkin anlamlı bilgilerin yanı sıra söz konusu işlemenin veri sahibi açısından önemi ve öngörülen sonuçları gizlilik politikamızda belirtilmiştir.

## III. EU-U.S. Data Privacy Framework (EU-U.S. DPF), UK Extension to the EU-U.S. DPF, Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF)

Eğer organizasyonumuz EU-U.S. Data Privacy Framework (EU-U.S. DPF) ve/veya UK Extension to the EU-U.S. DPF ve/veya Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF) sertifikalı bir üye ise, aşağıdaki hususlar geçerlidir:

Biz, U.S. Department of Commerce tarafından belirlenen şekilde EU-U.S. Data Privacy Framework (EU-U.S. DPF) ve UK Extension to the EU-U.S. DPF ile Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF) kurallarına uyarız. Şirketimiz, Avrupa Birliği ve Birleşik Krallık'tan EU-U.S. DPF ve UK Extension to the EU-U.S. DPF kapsamında aldığı kişisel verilerin işlenmesiyle ilgili olarak EU-U.S. Data Privacy Framework Principles (EU-U.S. DPF Principles) ilkesine uyduğunu U.S. Department of Commerce'e teyit etmiştir. Şirketimiz, İsviçre'den Swiss-U.S. DPF kapsamında aldığı kişisel verilerin işlenmesiyle ilgili olarak Swiss-U.S. Data Privacy Framework Principles (Swiss-U.S. DPF Principles) ilkesine uyduğunu U.S. Department of Commerce'e teyit etmiştir. Gizlilik politikamızın hükümleri ile EU-U.S. DPF Principles ve/veya Swiss-U.S. DPF Principles arasında bir çelişki olması durumunda, Principles esas alınacaktır.

Data Privacy Framework (DPF) programı hakkında daha fazla bilgi edinmek ve sertifikamızı görmek için lütfen https://www.dataprivacyframework.gov/ adresini ziyaret edin.

Şirketimizin diğer ABD birimleri veya bağlı ortaklıkları, varsa, UK Extension to the EU-U.S. DPF ve Swiss-U.S. DPF Principals dahil olmak üzere, EU-U.S. DPF Principals'a da uymaktadır ve gizlilik politikamızda belirtilmiştir.

EU-U.S. DPF ve UK Extension to the EU-U.S. DPF ile Swiss-U.S. DPF ile uyum içinde, şirketimiz, Avrupa veri koruma yetkilileri ve Birleşik Krallık Information Commissioner's Office (ICO) ile İsviçre Federal Data Protection and Information Commissioner (EDÖB) tarafından kurulan organlarla işbirliği yapmayı ve EU-


© All rights reserved by Heiko Maniero.

U.S. DPF ve UK Extension to the EU-U.S. DPF ile Swiss-U.S. DPF kapsamında aldığımız kişisel verilerin işlenmesiyle ilgili olarak çözümsüz şikayetler hakkında bu organların tavsiyelerine uymayı taahhüt eder.

İlgili kişilere, kişisel verilerin işlenmesiyle ilgili şikayetleri ele almakla sorumlu Avrupa veri koruma yetkilileri hakkında bu şeffaflık belgesinin üst kısmında bilgi veririz ve ilgili kişilere uygun ve ücretsiz bir hukuk yolu sağlarız.

Tüm ilgili kişilere, şirketimizin Federal Trade Commission (FTC) soruşturma ve icra yetkilerine tabi olduğunu bildiririz.

İlgili kişiler belirli koşullar altında bağlayıcı bir tahkim talep etme hakkına sahiptir. Organizasyonumuz, ilgili kişinin tahkim talebinde bulunması ve Principals'ın Ek I'ine uygun olarak prosedür ve şartlara uyması durumunda, talepleri çözmeyi ve DPF-Principles'ın Ek I'ine göre şartlara uymayı taahhüt eder.

Burada, kişisel verilerin üçüncü taraflara aktarılması durumunda organizasyonumuzun sorumluluğu hakkında tüm ilgili kişilere bilgi veriyoruz.

İlgili kişilerin veya veri koruma denetleme makamlarının soruları için, bu şeffaflık belgesinin üst kısmında belirtilen yerel temsilcileri atadık.

Kişisel verilerinizin (i) üçüncü taraflara aktarılıp aktarılmayacağı veya (ii) başlangıçta toplandıkları amaçtan veya daha sonra tarafınızdan onaylanan amaçlardan önemli ölçüde farklı bir amaç için kullanılıp kullanılmayacağı konusunda size seçim yapma imkanı sunuyoruz (Opt-out). Seçim hakkınızı kullanmak için açık, görünür ve kolayca erişilebilir bir mekanizma, veri koruma sorumlumuz (DSB) ile e-posta yoluyla iletişime geçmektir. Üçüncü bir tarafa aktarılan veriler, bizim adımıza ve talimatlarımız doğrultusunda görev yapan bir temsilci veya veri işleyici tarafından işleniyorsa, seçim hakkınız yoktur ve biz de bunu yapmakla yükümlü değiliz. Ancak, her zaman bu tür temsilci veya veri işleyici ile bir sözleşme yaparız.

Hassas veriler için (örneğin, sağlık durumu, ırk veya etnik köken, siyasi görüşler, dini veya felsefi inançlar, sendika üyeliği veya ilgili kişinin cinsel yaşamı hakkında bilgiler içeren kişisel veriler), bu verilerin (i) üçüncü taraflara aktarılması veya (ii) başlangıçta toplandıkları veya daha sonra onayladığınız amaçtan farklı bir amaç için kullanılması durumunda açık rızanızı (Opt-in) alırız. Ayrıca, üçüncü taraflardan aldığımız tüm kişisel verileri, üçüncü taraf bunları hassas olarak tanımlayıp işliyorsa hassas olarak ele alırız.

Yasal otoritelerden gelen meşru taleplere yanıt olarak kişisel verilerin ifşa edilmesi gerekliliği konusunda sizi burada bilgilendiriyoruz. Bu, ulusal güvenlik veya kolluk kuvvetleri gerekliliklerinin karşılanmasını içerir.

Kişisel verilerin sorumlu olarak hareket eden üçüncü bir tarafa aktarılması durumunda, bildirim ve seçim ilkesine (Principals) uyarız. Ayrıca, bu verilerin yalnızca sınırlı ve belirli amaçlar için, sizin verdiğiniz onay doğrultusunda işlenmesini ve alıcının DPF'nin ilkelerine (Principals) eşdeğer koruma seviyesini sağladığını ve bu yükümlülüğü daha fazla yerine getiremeyeceğini tespit ettiğinde bize bildirmesini şart koşan bir sözleşme yaparız. Sözleşme, sorumlu olarak hareket eden üçüncü tarafın bu tür bir durum


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

tespit edildiğinde işleme faaliyetlerini durdurmasını veya diğer uygun ve yeterli tedbirleri almasını gerektirir.

Kişisel verilerin bir temsilci veya veri işleyici olarak hareket eden üçüncü bir tarafa aktarılması durumunda, (i) bu verileri yalnızca sınırlı ve belirli amaçlar için aktarırız; (ii) temsilci veya veri işleyicinin DPF-Principles'ın gerektirdiği şekilde en az aynı düzeyde veri koruması sağlamasını taahhüt ederiz; (iii) temsilci veya veri işleyicinin aktarılan kişisel verileri, DPF-Principles'a uygun olarak işlemelerini sağlamak için uygun ve yeterli önlemleri alırız; (iv) temsilci veya veri işleyiciden, bu yükümlülüğü daha fazla yerine getiremeyeceğini tespit ettiğinde organizasyonumuzu bilgilendirmesini talep ederiz; (v) bildirimden sonra (iv dahil), yetkisiz işlemi durdurmak ve sorunu düzeltmek için uygun ve yeterli adımları atarız; ve (vi) talep üzerine DPF Department'a bu temsilci ile yapılan ilgili veri koruma hükümlerinin bir özetini veya temsil niteliğinde bir örneğini sağlarız.

EU-U.S. DPF ve/veya UK Extension to the EU-U.S. DPF ve/veya Swiss-U.S. DPF ile uyumlu olarak, organizasyonumuz, EU veri koruma yetkilileri ve Birleşik Krallık Information Commissioner's Office (ICO) ile İsviçre Federal Data Protection and Information Commissioner (EDÖB) tarafından kurulan organlarla işbirliği yapmayı ve EU-U.S. DPF ve UK Extension to the EU-U.S. DPF ile Swiss-U.S. DPF kapsamında aldığımız iş ilişkileriyle ilgili kişisel verilerin işlenmesiyle ilgili olarak çözümsüz şikayetler hakkında bu organların tavsiyelerine uymayı taahhüt eder.

Geçici olarak Avrupa Birliği'nde (AB), Avrupa Ekonomik Alanı'nda (AEA) veya Birleşik Krallık'ta bulunan ya da ikametgahı veya mutat meskeni buralarda olan tüm veri sahipleri, Şeffaflık Belgemizde yayınlanan ve kişisel verilere erişim hakkı da dahil olmak üzere GDPR'nin 15 ila 22. maddelerinden kaynaklanan haklara ve veri sahibi haklarına sahiptir. Bu bilgileri tüm AB ve AEA dillerinde kullanıma sunduk. İngilizce versiyon Birleşik Krallık için geçerlidir.

İsviçre'de geçici olarak ikamet eden veya ikametgahı veya mutat meskeni orada bulunan tüm veri sahipleri, kişisel verilere erişim hakkı da dahil olmak üzere Şeffaflık Belgemizde yayınlanan İsviçre Veri Koruma Yasası (DPA) ve İsviçre Veri Koruma Yönetmeliği (DPR) kapsamındaki haklara ve veri sahibi haklarına sahiptir. Bu bilgileri İsviçre'nin üç resmi dilinde (Almanca, İtalyanca ve Fransızca) sağladık.


© All rights reserved by Heiko Maniero.

# UKRAINIAN: Інформація про обробку персональних даних (стаття 13, 14 GDPR)

Шановний пане або пані,

Персональні дані кожної особи, яка перебуває в договірних, переддоговірних або інших відносинах з нашою компанією, заслуговують на особливий захист. Наша мета - підтримувати рівень захисту даних на високому рівні. Тому ми регулярно розвиваємо наші концепції захисту та безпеки даних.

Безумовно, ми дотримуємося законодавчих положень щодо захисту даних. Відповідно до ст. 13, 14 GDPR, контролери виконують конкретні інформаційні вимоги при зборі персональних даних. Цей документ виконує ці зобов'язання.

Термінологія нормативно-правових актів є складною. На жаль, при підготовці цього документу не вдалося уникнути використання юридичних термінів. У зв'язку з цим зазначаємо, що Ви завжди можете звернутися до нас з усіх питань, що стосуються цього документа, використаних термінів чи формулювань.

## I. Дотримання вимог щодо інформування при зборі персональних даних у суб'єкта персональних даних (ст. 13 GDPR)

### A. Ідентифікація та контактні дані контролера (стаття 13(1) літ. "a" GDPR)

Див. вище

### B. Контактні дані Уповноваженого із захисту даних (стаття 13(1) літ. b GDPR)

Див. вище

### C. Цілі обробки, для яких призначені персональні дані, а також правові підстави для обробки (ст. 13(1) п. "c" GDPR)

Метою обробки персональних даних є здійснення всіх операцій, які стосуються контролера, клієнтів, потенційних клієнтів, ділових партнерів або інших договірних чи переддоговірних відносин між названими групами (у найширшому розумінні) або юридичних зобов'язань контролера.

Ст. 6 (1) літ. a GDPR служить правовою основою для операцій обробки, на які ми отримуємо згоду для конкретної мети обробки. Якщо обробка персональних даних необхідна для виконання


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

договору, стороною якого є суб'єкт даних, як, наприклад, у випадку, коли операції з обробки необхідні для поставки товарів або надання будь-якої іншої послуги, обробка здійснюється на підставі ст. 6 ч. 1 п. b GDPR. Те ж саме стосується таких операцій обробки, які необхідні для проведення переддоговірних заходів, наприклад, у випадку запитів щодо наших продуктів або послуг. Чи є наша компанія суб'єктом правового зобов'язання, за яким необхідна обробка персональних даних, наприклад, для виконання податкових зобов'язань, обробка здійснюється на підставі ст. 6 ч. 1 п. "c" GDPR. 6 (1) літ. c GDPR.

У рідкісних випадках обробка персональних даних може бути необхідною для захисту життєво важливих інтересів суб'єкта даних або іншої фізичної особи. Це може статися, наприклад, якщо відвідувач отримав травму в нашій компанії і його ім'я, вік, дані медичного страхування або інша життєво важлива інформація повинна бути передана лікарю, лікарні або іншій третій стороні. Тоді обробка буде здійснюватися на підставі ст. 6 (1) літ. d GDPR.

Якщо обробка необхідна для виконання завдання, що здійснюється в інтересах суспільства або при здійсненні офіційних повноважень, покладених на контролера, правовою основою є ст. 6(1) літ. e GDPR.

Нарешті, операції з обробки можуть здійснюватися на підставі статті 6(1) літ. f GDPR. Ця правова підстава використовується для операцій обробки, які не охоплюються жодною з вищезазначених правових підстав, якщо обробка необхідна для цілей законних інтересів, переслідуваних нашою компанією або третьою стороною, за винятком випадків, коли такі інтереси переважають над інтересами або основними правами і свободами суб'єкта даних, які вимагають захисту персональних даних. Такі операції з обробки є особливо допустимими, оскільки вони були спеціально зазначені європейським законодавцем. Він вважає, що законний інтерес можна припустити, якщо суб'єкт даних є клієнтом контролера (ст. 47, речення 2 GDPR).

## D. Якщо обробка ґрунтується на статті 6(1) літ. f GDPR, законні інтереси, що переслідуються контролером або третьою стороною (стаття 13(1) літ. d GDPR)

Якщо обробка персональних даних ґрунтується на статті 6(1) літ. f GDPR, наш законний інтерес полягає у здійсненні нашої діяльності на користь добробуту всіх наших працівників та акціонерів.

## E. Категорії отримувачів персональних даних (ст. 13(1) п. "e" GDPR)

Органи державної влади

Зовнішні органи

Інші зовнішні органи


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

Внутрішня переробка

Внутрішньогрупова обробка

Інші органи

Список наших обробників і одержувачів даних у третіх країнах і, за необхідності, міжнародних організаціях опублікований на нашому веб-сайті або може бути безкоштовно наданий за запитом. Будь ласка, зв'яжіться з нашим співробітником із захисту даних, щоб запросити цей список.

## F. Одержувачі в третій країні та відповідні або придатні гарантії, а також засоби, за допомогою яких можна отримати їхню копію або де вони були надані (ст. 13(1) літ. f, 46(1), 46(2) літ. c GDPR)

До одержувачів персональних даних можуть належати всі компанії та філії, що входять до складу нашої групи (далі - "компанії групи"), які мають місцезнаходження або офіс у третій країні. Перелік всіх компаній групи або одержувачів можна запросити у нас.

Відповідно до статті 46(1) GDPR контролер або процесор може передавати персональні дані до третьої країни лише за умови, що контролер або процесор забезпечив відповідні гарантії, а також за умови, що права суб'єктів даних, які підлягають захисту, та ефективні засоби правового захисту для суб'єктів даних є доступними. Відповідні гарантії можуть бути надані без необхідності отримання будь-якого спеціального дозволу від наглядового органу за допомогою стандартних договірних положень, стаття 46(2) літ. "c" GDPR.

Стандартні договірні положення Європейського Союзу або інші відповідні гарантії узгоджуються з усіма одержувачами з третіх країн перед першою передачею персональних даних. Таким чином, забезпечуються відповідні гарантії, права суб'єктів даних, що підлягають виконанню, та ефективні засоби правового захисту для суб'єктів даних. Кожен суб'єкт даних може отримати від нас копію стандартних договірних положень. Стандартні договірні положення також доступні в Офіційному віснику Європейського Союзу.

Стаття 45(3) Загального регламенту про захист даних (GDPR) надає Європейській Комісії право за допомогою імплементаційного акту прийняти рішення про те, що країна за межами ЄС забезпечує належний рівень захисту. Це означає, що рівень захисту персональних даних в цілому еквівалентний рівню захисту в ЄС. Наслідком рішень, які визнають адекватний рівень захисту, є те, що персональні дані можуть вільно передаватися з ЄС (а також Норвегії, Ліхтенштейну та Ісландії) до третьої країни без подальших перешкод. Подібні правила діють у Великобританії, Швейцарії та деяких інших країнах.

Якщо Європейська Комісія або уряд іншої країни вирішить, що третя країна забезпечує належний рівень захисту, а також відповідну структуру (наприклад, EU-U.S. Data Privacy Framework, Swiss-


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

U.S. Data Privacy Framework, UK Extension to the EU-U.S. Data Privacy Framework), всі передачі, які ми здійснюємо членам таких структур (наприклад, самосертифікованим суб'єктам), ґрунтуються виключно на членстві цих суб'єктів у відповідній структурі. У випадку, якщо ми або одна з компаній нашої групи є членом такої структури, всі передачі нам або компанії нашої групи ґрунтуються виключно на членстві компанії в такій структурі.

Будь-який суб'єкт даних може отримати копію цих рамок у нас. Крім того, рамки також доступні в Офіційному віснику Європейського Союзу, в опублікованих юридичних матеріалах або на веб-сайтах наглядових органів чи інших компетентних органів або установ.

## G. Період, протягом якого персональні дані будуть зберігатися, або, якщо це неможливо, критерії, використані для визначення цього періоду (ст. 13(2) п. "a" GDPR)

Критерієм, який використовується для визначення періоду зберігання персональних даних, є відповідний встановлений законом термін зберігання. Після закінчення цього терміну відповідні дані видаляються в звичайному порядку, якщо вони більше не є необхідними для виконання договору або ініціювання договору.

Якщо немає законодавчо встановленого терміну зберігання, критерієм є договірний або внутрішній термін зберігання.

## H. Існування права вимагати від контролера доступу до персональних даних та їх виправлення чи видалення або обмеження обробки, що стосується суб'єкта даних, або заперечувати проти обробки, а також права на перенесення даних (ст. 13(2) п. "b" GDPR)

Всі суб'єкти персональних даних мають наступні права:

***Право на доступ***

Кожен суб'єкт персональних даних має право на доступ до персональних даних, які його стосуються. Право на доступ поширюється на всі дані, які ми обробляємо. Це право може бути реалізовано легко і з розумними інтервалами, щоб бути в курсі і перевіряти законність обробки (ст. 63 GDPR). Це право випливає зі ст. 15 GDPR. Суб'єкт даних може зв'язатися з нами для здійснення права на доступ.

***Право на виправлення***

Відповідно до частини 1 статті 16 GDPR суб'єкт даних має право вимагати від контролера без невиправданої затримки виправлення неточних персональних даних, які його стосуються. Крім того, ч. 2 ст. 16 GDPR передбачає, що суб'єкт даних має право, з урахуванням цілей обробки, на


© All rights reserved by Heiko Maniero.

доповнення неповних персональних даних, у тому числі шляхом надання додаткової заяви. Суб'єкт даних може звернутися до нас для реалізації права на виправлення.

***Право на видалення (право на забуття)***

Крім того, суб'єкти даних мають право на видалення та право на забуття відповідно до ст. 17 GDPR. Цим правом також можна скористатися, звернувшись до нас. Однак на цьому етапі ми хотіли б зазначити, що це право не застосовується, якщо обробка необхідна для виконання юридичного зобов'язання, яке є предметом нашої компанії, ст. 17 (3) літ. b GDPR. Це означає, що ми можемо затвердити заявку на видалення тільки після закінчення встановленого законом терміну зберігання.

***Право на обмеження обробки даних***

Відповідно до статті 18 GDPR будь-який суб'єкт даних має право на обмеження обробки. Обмеження обробки може вимагатися, якщо виконується одна з умов, викладених у статті 18 (1) літ. a-d GDPR. Суб'єкт даних може зв'язатися з нами, щоб скористатися правом на обмеження обробки.

***Право на заперечення***

Крім того, ст. 21 GDPR гарантує право на заперечення. Суб'єкт даних може зв'язатися з нами, щоб скористатися правом на заперечення.

***Право на перенесення даних***

Ст. 20 GDPR надає суб'єкту даних право на перенесення даних. Відповідно до цього положення, суб'єкт даних має право за умов, викладених у ст. 20(1) пп. a та b GDPR, отримувати персональні дані, що стосуються його або її, які він або вона надали контролеру, у структурованому, загальноприйнятому та машинозчитуваному форматі, а також має право передавати ці дані іншому контролеру без перешкод з боку контролера, якому були надані персональні дані. Суб'єкт даних може зв'язатися з нами, щоб скористатися правом на перенесення даних.

## I. Існування права відкликати згоду в будь-який час, не впливаючи на законність обробки на підставі згоди до її відкликання, якщо обробка здійснюється на підставі ст. 6(1) п. "a" GDPR або ст. 9(2) п. "a" GDPR (ст. 13(2) п. "c" GDPR)

Якщо обробка персональних даних здійснюється на підставі ст. 6 ч. 1 п. "a" GDPR, тобто якщо суб'єкт даних надав згоду на обробку персональних даних для однієї або декількох конкретних цілей, або на підставі ст. 9 ч. 2 п. "a" GDPR, яка регулює пряму згоду на обробку спеціальних категорій персональних даних, суб'єкт даних має право відповідно до ст. 7 ч. 3 речення 1 GDPR відкликати свою згоду в будь-який час.

Відкликання згоди не впливає на законність обробки, яка здійснювалася на підставі згоди до її відкликання, ст. 7(3), речення 2 GDPR. Відкликати згоду має бути так само легко, як і надати згоду, ст. 7(3) речення 4 GDPR. Таким чином, відкликання згоди завжди може відбуватися у той самий


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

спосіб, у який вона була надана, або у будь-який інший спосіб, який суб'єкт даних вважає більш простим. У сучасному інформаційному суспільстві, ймовірно, найпростішим способом відкликання згоди є простий електронний лист. Якщо суб'єкт даних бажає відкликати свою згоду, надану нам, достатньо надіслати нам простий електронний лист. Крім того, суб'єкт даних може обрати будь-який інший спосіб повідомити нам про відкликання своєї згоди.

## J. Право на подання скарги до наглядового органу (ст. 13(2) літ. d, 77(1) GDPR)

Як контролер, ми зобов'язані повідомити суб'єкта даних про право подати скаргу до наглядового органу, стаття 13(2) літ. d GDPR. Право на подання скарги до наглядового органу регулюється статтею 77(1) GDPR. Відповідно до цього положення, без шкоди для будь-якого іншого адміністративного або судового засобу правового захисту, кожен суб'єкт даних має право подати скаргу до наглядового органу, зокрема, в державі-члені за місцем його постійного проживання, місцем роботи або місцем передбачуваного порушення, якщо суб'єкт даних вважає, що обробка персональних даних, які його стосуються, порушує Загальний регламент про захист даних. Право на подання скарги до наглядового органу було обмежено правом Союзу лише таким чином, що воно може бути реалізоване лише в одному наглядовому органі (ст. 141, речення 1 GDPR). Це правило спрямоване на уникнення подвійних скарг одного і того ж суб'єкта даних з одного і того ж питання. Тому, якщо суб'єкт даних хоче подати скаргу на нас, ми просимо звертатися лише до одного наглядового органу.

## K. Надання персональних даних як законодавча або договірна вимога; вимога, необхідна для укладення договору; обов'язок суб'єкта даних надати персональні дані; можливі наслідки ненадання таких даних (ст. 13(2) літ. e GDPR)

Ми роз'яснюємо, що надання персональних даних частково вимагається законом (наприклад, податкове законодавство) або може також випливати з договірних положень (наприклад, інформація про договірного партнера).

Іноді може виникнути необхідність в укладенні договору про те, що суб'єкт даних надає нам персональні дані, які в подальшому повинні бути оброблені нами. Суб'єкт даних, наприклад, зобов'язаний надати нам персональні дані, коли наша компанія підписує з ним договір. Ненадання персональних даних матиме наслідком те, що договір з суб'єктом даних не може бути укладений.

Перед наданням персональних даних суб'єктом персональних даних суб'єкт персональних даних повинен зв'язатися з нами. Ми роз'яснюємо суб'єкту персональних даних, чи вимагається надання персональних даних законом або договором або є необхідним для укладення договору, чи існує обов'язок надання персональних даних та наслідки ненадання персональних даних.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

### L. Існування автоматизованого прийняття рішень, включаючи профілювання, про яке йдеться в ст. 22 (1) і (4) GDPR, і, принаймні, в цих випадках, змістовна інформація про логіку, а також про значення і передбачувані наслідки такої обробки для суб'єкта даних (ст. 13 (2) lit. f GDPR).

Як відповідальна компанія, ми зазвичай не використовуємо автоматизоване прийняття рішень або профілювання. Якщо у виняткових випадках ми здійснюємо автоматизоване прийняття рішень або профілювання, ми інформуємо суб'єкта даних або окремо, або через підрозділ у нашій політиці конфіденційності (на нашому веб-сайті). У цьому випадку застосовується наступне:

Автоматизоване прийняття рішень, включаючи профілювання, може відбуватися, якщо (1) це необхідно для укладення або виконання договору між суб'єктом даних і нами, або (2) це дозволено законодавством Союзу або держави-члена, якому ми підпорядковуємося, і яке також встановлює відповідні заходи для захисту прав, свобод і законних інтересів суб'єкта даних; або (3) це ґрунтується на явній згоді суб'єкта даних.

У випадках, зазначених у статті 22(2)(a) і (c) GDPR, ми повинні вжити належних заходів для захисту прав, свобод і законних інтересів суб'єкта даних. У цих випадках ви маєте право на людське втручання з боку контролера, висловлення своєї точки зору та оскарження рішення.

Змістовна інформація про задіяну логіку, а також про значення і передбачувані наслідки такої обробки для суб'єкта даних викладена в нашій політиці конфіденційності.

## II. Дотримання вимог щодо інформування, коли персональні дані не збираються у суб'єкта персональних даних (ст. 14 GDPR)

### A. Ідентифікація та контактні дані контролера (стаття 14(1), підпункт "a" GDPR)

Див. вище

### B. Контактні дані Уповноваженого із захисту даних (стаття 14(1) літ. b GDPR)

Див. вище


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## C. Цілі обробки, для яких призначені персональні дані, а також правові підстави для обробки (ст. 14(1) п. "c" GDPR)

Метою обробки персональних даних є здійснення всіх операцій, які стосуються контролера, клієнтів, потенційних клієнтів, ділових партнерів або інших договірних чи переддоговірних відносин між названими групами (у найширшому розумінні) або юридичних зобов'язань контролера.

Якщо обробка персональних даних необхідна для виконання договору, стороною якого є суб'єкт даних, як, наприклад, у випадку, коли операції з обробки необхідні для поставки товарів або надання будь-якої іншої послуги, обробка здійснюється на підставі статті 6 (1) літ. b GDPR. Те ж саме стосується таких операцій обробки, які необхідні для здійснення переддоговірних заходів, наприклад, у випадку запитів щодо наших продуктів або послуг. Чи є наша компанія суб'єктом правового зобов'язання, за яким необхідна обробка персональних даних, наприклад, для виконання податкових зобов'язань, обробка здійснюється на підставі ст. 6 ч. 1 п. "c" GDPR. 6 (1) літ. c GDPR.

У рідкісних випадках обробка персональних даних може бути необхідною для захисту життєво важливих інтересів суб'єкта даних або іншої фізичної особи. Це може статися, наприклад, якщо відвідувач отримав травму в нашій компанії і його ім'я, вік, дані медичного страхування або інша життєво важлива інформація повинна бути передана лікарю, лікарні або іншій третій стороні. Тоді обробка буде здійснюватися на підставі ст. 6 (1) літ. d GDPR.

Якщо обробка необхідна для виконання завдання, що здійснюється в інтересах суспільства або при здійсненні офіційних повноважень, покладених на контролера, правовою основою є ст. 6(1) літ. e GDPR.

Нарешті, операції з обробки можуть здійснюватися на підставі статті 6(1) літ. f GDPR. Ця правова підстава використовується для операцій обробки, які не охоплюються жодною з вищезазначених правових підстав, якщо обробка необхідна для цілей законних інтересів, переслідуваних нашою компанією або третьою стороною, за винятком випадків, коли такі інтереси переважають над інтересами або основними правами і свободами суб'єкта даних, які вимагають захисту персональних даних. Такі операції з обробки є особливо допустимими, оскільки вони були спеціально зазначені європейським законодавцем. Він вважає, що законний інтерес можна припустити, якщо суб'єкт даних є клієнтом контролера (ст. 47, речення 2 GDPR).

## D. Категорії відповідних персональних даних (ст. 14(1) п. "d" GDPR)

Дані клієнта

Дані потенційних клієнтів


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

Дані працівників

Дані постачальників

## E. Категорії отримувачів персональних даних (ст. 14(1) п. "e" GDPR)

Органи державної влади

Зовнішні органи

Інші зовнішні органи

Внутрішня переробка

Внутрішньогрупова обробка

Інші органи

Список наших обробників і одержувачів даних у третіх країнах і, за необхідності, міжнародних організаціях опублікований на нашому веб-сайті або може бути безкоштовно наданий за запитом. Будь ласка, зв'яжіться з нашим співробітником із захисту даних, щоб запросити цей список.

## F. Одержувачі в третій країні та відповідні або придатні гарантії, а також засоби, за допомогою яких можна отримати їхню копію або де вони були надані (ст. 14(1) літ. f, 46(1), 46(2) літ. c GDPR)

До одержувачів персональних даних можуть належати всі компанії та філії, що входять до складу нашої групи (далі - "компанії групи"), які мають місцезнаходження або офіс у третій країні. Перелік всіх компаній групи можна запросити у нас.

Відповідно до статті 46(1) GDPR контролер або процесор може передавати персональні дані до третьої країни лише за умови, що контролер або процесор забезпечив відповідні гарантії, а також за умови, що права суб'єктів даних, які підлягають захисту, та ефективні засоби правового захисту для суб'єктів даних є доступними. Відповідні гарантії можуть бути надані без необхідності отримання спеціального дозволу від наглядового органу за допомогою стандартних положень про захист даних, стаття 46(2), підпункт "c" GDPR.

Стандартні договірні положення Європейського Союзу або інші відповідні гарантії узгоджуються з усіма одержувачами з третіх країн перед першою передачею персональних даних. Таким чином, забезпечуються відповідні гарантії, права суб'єктів даних, що підлягають виконанню, та ефективні засоби правового захисту для суб'єктів даних. Кожен суб'єкт даних може отримати від нас копію


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

стандартних договірних положень. Стандартні договірні положення також доступні в Офіційному віснику Європейського Союзу.

Стаття 45(3) Загального регламенту про захист даних (GDPR) надає Європейській Комісії право за допомогою імплементаційного акту прийняти рішення про те, що країна за межами ЄС забезпечує належний рівень захисту. Це означає, що рівень захисту персональних даних в цілому еквівалентний рівню захисту в ЄС. Наслідком рішень, які визнають адекватний рівень захисту, є те, що персональні дані можуть вільно передаватися з ЄС (а також Норвегії, Ліхтенштейну та Ісландії) до третьої країни без подальших перешкод. Подібні правила діють у Великобританії, Швейцарії та деяких інших країнах.

Якщо Європейська Комісія або уряд іншої країни вирішить, що третя країна забезпечує належний рівень захисту, а також відповідну структуру (наприклад, EU-U.S. Data Privacy Framework, Swiss-U.S. Data Privacy Framework, UK Extension to the EU-U.S. Data Privacy Framework), всі передачі, які ми здійснюємо членам таких структур (наприклад, самосертифікованим суб'єктам), ґрунтуються виключно на членстві цих суб'єктів у відповідній структурі. У випадку, якщо ми або одна з компаній нашої групи є членом такої структури, всі передачі нам або компанії нашої групи ґрунтуються виключно на членстві компанії в такій структурі.

Будь-який суб'єкт даних може отримати копію цих рамок у нас. Крім того, рамки також доступні в Офіційному віснику Європейського Союзу, в опублікованих юридичних матеріалах або на веб-сайтах наглядових органів чи інших компетентних органів або установ.

## G. Період, протягом якого персональні дані будуть зберігатися, або, якщо це неможливо, критерії, використані для визначення цього періоду (ст. 14(2) п. "a" GDPR)

Критерієм, який використовується для визначення періоду зберігання персональних даних, є відповідний встановлений законом термін зберігання. Після закінчення цього терміну відповідні дані видаляються в звичайному порядку, якщо вони більше не є необхідними для виконання договору або ініціювання договору.

Якщо немає законодавчо встановленого терміну зберігання, критерієм є договірний або внутрішній термін зберігання.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## H. Повідомлення про законні інтереси, переслідувані контролером або третьою стороною, якщо обробка ґрунтується на статті 6(1) літ. f GDPR (ст. 14(2) літ. b GDPR)

Відповідно до статті 6(1) літ. f GDPR, обробка повинна бути законною, тільки якщо обробка необхідна для цілей законних інтересів, переслідуваних контролером або третьою стороною, за винятком випадків, коли такі інтереси переважають інтереси або основоположні права і свободи суб'єкта даних, які вимагають захисту персональних даних. Відповідно до п. 47 речення 2 GDPR законний інтерес може існувати, якщо між суб'єктом даних та контролером існують відповідні та належні відносини, наприклад, у ситуаціях, коли суб'єкт даних є клієнтом контролера. У всіх випадках, коли наша компанія обробляє персональні дані на підставі статті 6(1) літ. f GDPR, наш законний інтерес полягає у здійсненні нашої діяльності на користь добробуту всіх наших співробітників та акціонерів.

## I. Існування права вимагати від контролера доступу до персональних даних, їх виправлення чи видалення або обмеження обробки, що стосується суб'єкта даних, та заперечувати проти обробки, а також права на перенесення даних (ст. 14(2) п. "c" GDPR)

Всі суб'єкти персональних даних мають наступні права:

***Право на доступ***

Кожен суб'єкт персональних даних має право на доступ до персональних даних, які його стосуються. Право на доступ поширюється на всі дані, які ми обробляємо. Це право може бути реалізовано легко і з розумними інтервалами, щоб бути в курсі і перевіряти законність обробки (ст. 63 GDPR). Це право випливає зі ст. 15 GDPR. Суб'єкт даних може зв'язатися з нами для здійснення права на доступ.

***Право на виправлення***

Відповідно до частини 1 статті 16 GDPR суб'єкт даних має право вимагати від контролера без невиправданої затримки виправлення неточних персональних даних, що стосуються його або її, без невиправданої затримки. Крім того, ч. 2 ст. 16 GDPR передбачає, що суб'єкт даних має право, з урахуванням цілей обробки, на доповнення неповних персональних даних, у тому числі шляхом надання додаткової заяви. Суб'єкт даних може звернутися до нас для реалізації права на виправлення.

***Право на видалення (право на забуття)***

Крім того, суб'єкти даних мають право на видалення та право на забуття відповідно до ст. 17 GDPR. Цим правом також можна скористатися, звернувшись до нас. Однак на цьому етапі ми хотіли б зазначити, що це право не застосовується, якщо обробка необхідна для виконання юридичного зобов'язання, яке є предметом нашої компанії, ст. 17 (3) літ. b GDPR. Це означає, що


© All rights reserved by Heiko Maniero.

ми можемо затвердити заявку на видалення тільки після закінчення встановленого законом терміну зберігання.

***Право на обмеження обробки даних***

Відповідно до статті 18 GDPR будь-який суб'єкт даних має право на обмеження обробки. Обмеження обробки може вимагатися, якщо виконується одна з умов, викладених у статті 18 (1) літ. a-d GDPR. Суб'єкт даних може зв'язатися з нами, щоб скористатися правом на обмеження обробки.

***Право на заперечення***

Крім того, ст. 21 GDPR гарантує право на заперечення. Суб'єкт даних може зв'язатися з нами, щоб скористатися правом на заперечення.

***Право на перенесення даних***

Ст. 20 GDPR надає суб'єкту даних право на перенесення даних. Відповідно до цього положення суб'єкт даних має право за умов, викладених у ст. 20(1) пп. a та b GDPR, отримувати персональні дані, що стосуються його або її, які він або вона надали контролеру, у структурованому, загальноприйнятому та машинозчитуваному форматі, а також має право передавати ці дані іншому контролеру без перешкод з боку контролера, якому були надані персональні дані. Суб'єкт даних може звернутися до нас, щоб скористатися правом на перенесення даних.

## J. Існування права відкликати згоду в будь-який час, не впливаючи на законність обробки на підставі згоди до її відкликання, якщо обробка здійснюється на підставі ст. 6(1) п. "a" або ст. 9(2) п. "a" GDPR (ст. 14(2) п. "d" GDPR)

Якщо обробка персональних даних здійснюється на підставі ст. 6 ч. 1 п. "a" GDPR, тобто якщо суб'єкт даних надав згоду на обробку персональних даних для однієї або декількох конкретних цілей, або на підставі ст. 9 ч. 2 п. "a" GDPR, яка регулює пряму згоду на обробку спеціальних категорій персональних даних, суб'єкт даних має право відповідно до ст. 7 ч. 3 речення 1 GDPR відкликати свою згоду в будь-який час.

Відкликання згоди не впливає на законність обробки, яка здійснювалася на підставі згоди до її відкликання, ст. 7(3), речення 2 GDPR. Відкликати згоду має бути так само легко, як і надати згоду, ст. 7(3) речення 4 GDPR. Таким чином, відкликання згоди завжди може відбуватися у той самий спосіб, у який вона була надана, або у будь-який інший спосіб, який суб'єкт даних вважає більш простим. У сучасному інформаційному суспільстві, ймовірно, найпростішим способом відкликання згоди є простий електронний лист. Якщо суб'єкт даних бажає відкликати свою згоду, надану нам, достатньо надіслати нам простий електронний лист. Крім того, суб'єкт даних може обрати будь-який інший спосіб повідомити нам про відкликання своєї згоди.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## K. Право на подання скарги до наглядового органу (ст. 14(2) п. "e", 77(1) GDPR)

Як контролер, ми зобов'язані повідомити суб'єкта даних про право подати скаргу до наглядового органу, стаття 14(2) літ. e GDPR. Право на подання скарги до наглядового органу регулюється статтею 77(1) GDPR. Відповідно до цього положення, без шкоди для будь-якого іншого адміністративного або судового засобу правового захисту, кожен суб'єкт даних має право подати скаргу до наглядового органу, зокрема, в державі-члені за місцем свого постійного проживання, місцем роботи або місцем передбачуваного порушення, якщо суб'єкт даних вважає, що обробка персональних даних, які його стосуються, порушує Загальний регламент про захист даних. Право на подання скарги до наглядового органу було обмежено правом Союзу лише таким чином, що воно може бути реалізоване лише в одному наглядовому органі (ст. 141, речення 1 GDPR). Це правило спрямоване на уникнення подвійних скарг одного і того ж суб'єкта даних з одного і того ж питання. Тому, якщо суб'єкт даних хоче подати скаргу на нас, ми просимо звертатися лише до одного наглядового органу.

## L. Джерело походження персональних даних, і, якщо застосовно, чи були вони отримані з загальнодоступних джерел (ст. 14(2) п. f GDPR)

В принципі, персональні дані збираються безпосередньо від суб'єкта даних або у співпраці з органом влади (наприклад, отримання даних з офіційного реєстру). Інші дані про суб'єктів даних отримуються з передач компаній групи. У контексті цієї загальної інформації точне визначення джерел, з яких походять персональні дані, є або неможливим, або вимагатиме непропорційних зусиль у розумінні ст. 14(5)(b) ЗРЗД. 14 (5) літ. b GDPR. В принципі, ми не збираємо персональні дані з загальнодоступних джерел.

Будь-який суб'єкт даних може звернутися до нас у будь-який час для отримання більш детальної інформації про точні джерела персональних даних, що стосуються його або її. Якщо походження персональних даних не може бути надано суб'єкту даних, оскільки використовувалися різні джерела, повинна бути надана загальна інформація (ст. 61, речення 4 GDPR).

## M. Існування автоматизованого прийняття рішень, включаючи профілювання, про яке йдеться в ст. 22(1) і (4) GDPR, і, принаймні, в цих випадках, змістовна інформація про логіку, а також про значення і передбачувані наслідки такої обробки для суб'єкта даних (ст. 14(2) lit. g GDPR).

Як відповідальна компанія, ми зазвичай не використовуємо автоматизоване прийняття рішень або профілювання. Якщо у виняткових випадках ми здійснюємо автоматизоване прийняття рішень або профілювання, ми інформуємо суб'єкта даних або окремо, або через підрозділ у нашій політиці конфіденційності (на нашому веб-сайті). У цьому випадку застосовується наступне:


© All rights reserved by Heiko Maniero.

Автоматизоване прийняття рішень, включаючи профілювання, може відбуватися, якщо (1) це необхідно для укладення або виконання договору між суб'єктом даних і нами, або (2) це дозволено законодавством Союзу або держави-члена, якому ми підпорядковуємося, і яке також встановлює відповідні заходи для захисту прав, свобод і законних інтересів суб'єкта даних; або (3) це ґрунтується на явній згоді суб'єкта даних.

У випадках, зазначених у статті 22(2)(a) і (c) GDPR, ми повинні вжити належних заходів для захисту прав, свобод і законних інтересів суб'єкта даних. У цих випадках ви маєте право на людське втручання з боку контролера, висловлення своєї точки зору та оскарження рішення.

Змістовна інформація про задіяну логіку, а також про значення і передбачувані наслідки такої обробки для суб'єкта даних викладена в нашій політиці конфіденційності.

## III. EU-U.S. Data Privacy Framework (EU-U.S. DPF), UK Extension to the EU-U.S. DPF, Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF)

Якщо наша організація є сертифікованим членом EU-U.S. Data Privacy Framework (EU-U.S. DPF) та/або UK Extension to the EU-U.S. DPF та/або Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF), то діють наступні положення:

Ми дотримуємось EU-U.S. Data Privacy Framework (EU-U.S. DPF) та UK Extension to the EU-U.S. DPF, а також Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF), як це встановлено U.S. Department of Commerce. Наша компанія підтвердила Міністерству торгівлі США, що дотримується EU-U.S. Data Privacy Framework Principles (EU-U.S. DPF Principles) щодо обробки персональних даних, отриманих з Європейського Союзу та Сполученого Королівства на підставі EU-U.S. DPF та UK Extension to the EU-U.S. DPF. Наша компанія підтвердила Міністерству торгівлі США, що дотримується Swiss-U.S. Data Privacy Framework Principles (Swiss-U.S. DPF Principles) щодо обробки персональних даних, отриманих зі Швейцарії на підставі Swiss-U.S. DPF. У випадку суперечності між положеннями нашої політики конфіденційності та EU-U.S. DPF Principles та/або Swiss-U.S. DPF Principles, головними є Principles.

Щоб дізнатися більше про програму Data Privacy Framework (DPF) та переглянути нашу сертифікацію, відвідайте, будь ласка, https://www.dataprivacyframework.gov/.

Інші підрозділи або дочірні компанії нашої компанії у США, які також дотримуються EU-U.S. DPF Principles, включаючи UK Extension to the EU-U.S. DPF та Swiss-U.S. DPF Principles, якщо такі є, зазначені у нашій політиці конфіденційності.

Відповідно до EU-U.S. DPF та UK Extension to the EU-U.S. DPF, а також Swiss-U.S. DPF, наша компанія зобов'язується співпрацювати з органами, створеними європейськими органами захисту


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

даних та британським Information Commissioner's Office (ICO), а також швейцарським Federal Data Protection and Information Commissioner (EDÖB), та дотримуватись їхніх порад щодо невирішених скарг на наше поводження з персональними даними, які ми отримали на підставі EU-U.S. DPF, UK Extension to the EU-U.S. DPF та Swiss-U.S. DPF.

Ми інформуємо постраждалих осіб про компетентні європейські органи захисту даних, відповідальні за розгляд скарг на поводження нашої організації з персональними даними у верхній частині цього документа прозорості та про те, що ми надаємо постраждалим особам адекватні та безкоштовні засоби правового захисту.

Ми інформуємо всіх постраждалих осіб про те, що наша компанія підлягає розслідувальним та виконавчим повноваженням Federal Trade Commission (FTC).

Постраждалі особи мають можливість за певних умов скористатися обов'язковим арбітражем. Наша організація зобов'язується врегульовувати вимоги та дотримуватися умов відповідно до Додатка I до DPF-Principals, якщо постраждала особа подала запит на обов'язковий арбітраж, повідомивши нашу організацію та дотримуючись процедур і умов, викладених у Додатку I до Principals.

Ми цим інформуємо всіх постраждалих осіб про відповідальність нашої організації у випадку передачі персональних даних третім особам.

Для запитань постраждалих осіб або органів нагляду за захистом даних ми призначили місцевих представників, зазначених у верхній частині цього документа прозорості.

Ми надаємо вам можливість вибору (Opt-out), чи будуть ваші персональні дані (i) передані третім особам або (ii) використані з метою, яка суттєво відрізняється від тієї (тих), для якої (яких) вони були спочатку зібрані або пізніше вами схвалені. Чіткий, добре видимий і легкодоступний механізм для реалізації вашого права вибору полягає у зв'язку з нашим відповідальним за захист даних (DSB) електронною поштою. У вас немає можливості вибору, і ми не зобов'язані це робити, якщо дані передаються третій стороні, яка діє як агент або обробник даних від нашого імені та за нашими вказівками. Однак ми завжди укладаємо договір з таким агентом або обробником даних.

Щодо чутливих даних (тобто персональних даних, які містять інформацію про стан здоров'я, расову або етнічну приналежність, політичні погляди, релігійні або філософські переконання, членство у профспілці або інформацію про сексуальне життя постраждалої особи), ми отримуємо вашу явну згоду (Opt-in), якщо ці дані (i) передаються третім особам або (ii) використовуються з іншою метою, ніж та, для якої вони були спочатку зібрані або для якої ви згодом надали свою згоду, зробивши вибір Opt-in. Крім того, ми розглядаємо всі персональні дані, які ми отримуємо від третіх осіб, як чутливі, якщо третя сторона їх ідентифікує та обробляє як чутливі.

Ми цим інформуємо вас про необхідність розкриття персональних даних у відповідь на законні запити органів влади, включаючи виконання вимог національної безпеки або правоохоронних органів.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

Під час передачі персональних даних третій стороні, яка діє як контролер, ми дотримуємося принципів повідомлення та вибору (Principals). Ми також укладаємо договір з третьою стороною, відповідальною за обробку, який передбачає, що ці дані можуть оброблятися лише для обмежених та визначених цілей відповідно до наданої вами згоди та що отримувач забезпечує такий самий рівень захисту, як Principals DPF, і повідомляє нас, якщо виявить, що більше не може виконувати це зобов'язання. Договір передбачає, що третя сторона, яка діє як контролер, припиняє обробку або вживає інших відповідних і адекватних заходів для усунення проблеми у разі виявлення такої ситуації.

Під час передачі персональних даних третій стороні, яка діє як агент або обробник даних, (i) ми передаємо ці дані лише для обмежених і визначених цілей; (ii) ми переконуємося, що агент або обробник даних зобов'язується забезпечити рівень захисту даних, принаймні такий самий, як вимагають DPF-Principals; (iii) ми вживаємо відповідних і адекватних заходів, щоб забезпечити, що агент або обробник даних фактично обробляє передані персональні дані таким чином, який відповідає нашим зобов'язанням відповідно до DPF-Principals; (iv) ми вимагаємо від агента або обробника даних повідомити нашу організацію, якщо він виявить, що більше не може виконувати зобов'язання щодо забезпечення такого ж рівня захисту, як це передбачено DPF-Principals; (v) після повідомлення, включаючи повідомлення за пунктом (iv), ми вживаємо відповідних і адекватних заходів, щоб припинити несанкціоновану обробку та усунути проблему; та (vi) ми надаємо DPF Department на запит резюме або представницький екземпляр відповідних положень договору про захист даних із цим агентом.

Відповідно до EU-U.S. DPF та/або UK Extension to the EU-U.S. DPF та/або Swiss-U.S. DPF, наша організація зобов’язується співпрацювати з органами, створеними європейськими органами захисту даних та британським Information Commissioner’s Office (ICO), а також швейцарським Federal Data Protection and Information Commissioner (EDÖB), та дотримуватись їхніх порад щодо невирішених скарг на наше поводження з персональними даними у зв'язку з трудовими відносинами, які ми отримали на підставі EU-U.S. DPF, UK Extension to the EU-U.S. DPF та Swiss-U.S. DPF.

Усі суб'єкти даних, які тимчасово перебувають у Європейському Союзі (ЄС), Європейській економічній зоні (ЄЕЗ) або Сполученому Королівстві, або мають там місце проживання чи звичайне місцеперебування, мають право на права та обов'язки суб'єктів даних, які опубліковані в нашому Документі про прозорість, а також випливають зі статей 15-22 GDPR, включаючи право на доступ до персональних даних. Ми зробили цю інформацію доступною всіма мовами ЄС та ЄЕЗ. Версія англійською мовою застосовується до Сполученого Королівства.

Усі суб'єкти даних, які тимчасово проживають у Швейцарії або мають там постійне місце проживання, користуються правами та обов'язками суб'єктів даних відповідно до Швейцарського закону про захист даних (DPA) та Швейцарського регламенту про захист даних (DPR), які опубліковані в нашому Документі про прозорість, включаючи право на доступ до персональних


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

даних. Ми надали цю інформацію трьома офіційними мовами Швейцарії (німецькою, італійською та французькою).


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

# UKRAINIAN: Інформація про обробку персональних даних для працівників та заявників (стаття 13, 14 GDPR)

Шановний пане або пані,

Персональні дані працівників та абітурієнтів заслуговують на особливий захист. Наша мета - підтримувати рівень захисту даних на високому рівні. Тому ми регулярно розвиваємо наші концепції захисту та безпеки даних.

Безумовно, ми дотримуємося законодавчих положень щодо захисту даних. Відповідно до ст. 13, 14 GDPR, контролери відповідають певним інформаційним вимогам при обробці персональних даних. Цей документ виконує ці зобов'язання.

Термінологія правового регулювання є складною. На жаль, при підготовці цього документу не вдалося уникнути використання юридичних термінів. У зв'язку з цим зазначаємо, що Ви завжди можете звернутися до нас з усіх питань, що стосуються цього документу, використаних термінів або формулювань.

## I. Дотримання вимог щодо інформування при зборі персональних даних у суб'єкта персональних даних (ст. 13 GDPR)

### A. Ідентифікація та контактні дані контролера (стаття 13(1) літ. "a" GDPR)

Див. вище

### B. Контактні дані відповідального за захист даних (стаття 13(1) літ. b GDPR)

Див. вище

### C. Цілі обробки, для яких призначені персональні дані, а також правові підстави для обробки (ст. 13(1) п. "c" GDPR)

Що стосується даних заявника, то метою обробки даних є проведення експертизи заявки в процесі прийому на роботу. Для цього ми обробляємо всі надані Вами дані. На підставі даних, наданих в процесі підбору персоналу, ми перевіримо, чи запрошуємо Вас на співбесіду (частина процесу відбору). У випадку, якщо кандидати в цілому підходять, зокрема, в контексті співбесіди, ми обробляємо деякі інші надані Вами персональні дані, які є важливими для прийняття рішення про відбір. Якщо Ви будете прийняті нами на роботу, дані кандидата автоматично перетворюються на


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

дані працівника. В рамках процесу найму ми будемо обробляти інші персональні дані про Вас, які ми запитуємо у Вас і які необхідні для ініціювання або виконання Вашого контракту (наприклад, персональні ідентифікаційні номери або податкові номери). Для даних працівників метою обробки даних є виконання трудового договору або дотримання інших правових норм, що застосовуються до трудових відносин (наприклад, податкового законодавства), а також використання Ваших персональних даних для виконання укладеного з Вами трудового договору (наприклад, публікація Вашого імені та контактної інформації всередині компанії або клієнтам). Дані працівника зберігаються після припинення трудових відносин для виконання встановлених законом строків зберігання.

Правовою основою для обробки даних є стаття 6(1) літ. b GDPR, стаття 9(2) літ. b та h GDPR, стаття 88(1) GDPR та національне законодавство, наприклад, для Німеччини стаття 26 BDSG (Федеральний закон про захист даних).

## D. Категорії отримувачів персональних даних (ст. 13(1) п. "e" GDPR)

Органи державної влади

Зовнішні органи

Інші зовнішні органи

Внутрішня переробка

Внутрішньогрупова обробка

Інші органи

Список наших обробників і одержувачів даних у третіх країнах і, за необхідності, міжнародних організаціях опублікований на нашому веб-сайті або може бути безкоштовно наданий за запитом. Будь ласка, зв'яжіться з нашим співробітником із захисту даних, щоб запросити цей список.

## E. Одержувачі в третій країні та відповідні або придатні гарантії, а також засоби, за допомогою яких можна отримати їхню копію або де вони були надані (ст. 13(1) літ. f, 46(1), 46(2) літ. c GDPR)

До одержувачів персональних даних можуть належати всі компанії та філії, що входять до складу нашої групи (далі - "компанії групи"), які мають місцезнаходження або офіс у третій країні. Перелік всіх компаній групи або одержувачів можна запросити у нас.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

Відповідно до статті 46(1) GDPR контролер або процесор може передавати персональні дані до третьої країни лише за умови, що контролер або процесор забезпечив відповідні гарантії, а також за умови, що права суб'єктів даних, які підлягають захисту, та ефективні засоби правового захисту для суб'єктів даних є доступними. Відповідні гарантії можуть бути надані без необхідності отримання будь-якого спеціального дозволу від наглядового органу за допомогою стандартних договірних положень, стаття 46(2) літ. "c" GDPR.

Стандартні договірні положення Європейського Союзу або інші відповідні гарантії узгоджуються з усіма одержувачами з третіх країн перед першою передачею персональних даних. Таким чином, забезпечуються відповідні гарантії, права суб'єктів даних, що підлягають виконанню, та ефективні засоби правового захисту для суб'єктів даних. Кожен суб'єкт даних може отримати від нас копію стандартних договірних положень. Стандартні договірні положення також доступні в Офіційному віснику Європейського Союзу.

Стаття 45(3) Загального регламенту про захист даних (GDPR) надає Європейській Комісії право за допомогою імплементаційного акту прийняти рішення про те, що країна за межами ЄС забезпечує належний рівень захисту. Це означає, що рівень захисту персональних даних в цілому еквівалентний рівню захисту в ЄС. Наслідком рішень, які визнають адекватний рівень захисту, є те, що персональні дані можуть вільно передаватися з ЄС (а також Норвегії, Ліхтенштейну та Ісландії) до третьої країни без подальших перешкод. Подібні правила діють у Великобританії, Швейцарії та деяких інших країнах.

Якщо Європейська Комісія або уряд іншої країни вирішить, що третя країна забезпечує належний рівень захисту, а також відповідну структуру (наприклад, EU-U.S. Data Privacy Framework, Swiss-U.S. Data Privacy Framework, UK Extension to the EU-U.S. Data Privacy Framework), всі передачі, які ми здійснюємо членам таких структур (наприклад, самосертифікованим суб'єктам), ґрунтуються виключно на членстві цих суб'єктів у відповідній структурі. У випадку, якщо ми або одна з компаній нашої групи є членом такої структури, всі передачі нам або компанії нашої групи ґрунтуються виключно на членстві компанії в такій структурі.

Будь-який суб'єкт даних може отримати копію цих рамок у нас. Крім того, рамки також доступні в Офіційному віснику Європейського Союзу, в опублікованих юридичних матеріалах або на веб-сайтах наглядових органів чи інших компетентних органів або установ.

## F. Період, протягом якого персональні дані будуть зберігатися, або, якщо це неможливо, критерії, використані для визначення цього періоду (ст. 13(2) п. "a" GDPR)

Термін зберігання персональних даних заявників становить 6 місяців. Для даних працівників застосовується відповідний законодавчо встановлений термін зберігання. Після закінчення цього


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

терміну відповідні дані видаляються в робочому порядку, якщо вони більше не є необхідними для виконання договору або ініціювання договору.

## G. Наявність права вимагати від контролера доступу до персональних даних, їх виправлення чи видалення або обмеження обробки, що стосується суб'єкта даних, або заперечувати проти обробки, а також права на перенесення даних (ст. 13(2) п. "b" GDPR)

Всі суб'єкти персональних даних мають наступні права:

***Право на доступ***

Кожен суб'єкт персональних даних має право на доступ до персональних даних, які його стосуються. Право на доступ поширюється на всі дані, які ми обробляємо. Це право може бути реалізовано легко і з розумними інтервалами, щоб бути в курсі і перевіряти законність обробки (ст. 63 GDPR). Це право випливає зі ст. 15 GDPR. Суб'єкт даних може зв'язатися з нами для здійснення права на доступ.

***Право на виправлення***

Відповідно до частини 1 статті 16 GDPR суб'єкт даних має право вимагати від контролера без невиправданої затримки виправлення неточних персональних даних, які його стосуються. Крім того, частина 2 статті 16 GDPR передбачає, що суб'єкт даних має право, з урахуванням цілей обробки, на доповнення неповних персональних даних, у тому числі шляхом надання додаткової заяви. Суб'єкт даних може звернутися до нас для реалізації права на виправлення.

***Право на видалення (право на забуття)***

Крім того, суб'єкти даних мають право на видалення та право на забуття відповідно до ст. 17 GDPR. Цим правом також можна скористатися, звернувшись до нас. Однак на цьому етапі ми хотіли б зазначити, що це право не застосовується, якщо обробка необхідна для виконання юридичного зобов'язання, яке є предметом нашої компанії, стаття 17 (3), підпункт b GDPR. Це означає, що ми можемо затвердити заявку на видалення тільки після закінчення встановленого законом терміну зберігання.

***Право на обмеження обробки даних***

Відповідно до статті 18 GDPR будь-який суб'єкт даних має право на обмеження обробки. Обмеження обробки може вимагатися, якщо виконується одна з умов, викладених у статті 18 (1) літ. a-d GDPR. Суб'єкт даних може зв'язатися з нами, щоб скористатися правом на обмеження обробки.

***Право на заперечення***

Крім того, ст. 21 GDPR гарантує право на заперечення. Суб'єкт даних може зв'язатися з нами, щоб скористатися правом на заперечення.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

***Право на перенесення даних***

Ст. 20 GDPR надає суб'єкту даних право на перенесення даних. Відповідно до цього положення, суб'єкт даних має право за умов, викладених у ст. 20(1) пп. a та b GDPR, отримувати персональні дані, що стосуються його або її, які він або вона надали контролеру, у структурованому, загальноприйнятому та машинозчитуваному форматі, а також має право передавати ці дані іншому контролеру без перешкод з боку контролера, якому ці персональні дані були надані. Суб'єкт даних може звернутися до нас, щоб скористатися правом на перенесення даних.

## H. Існування права відкликати згоду в будь-який час, не впливаючи на законність обробки на підставі згоди до її відкликання, якщо обробка здійснюється на підставі статті 6(1) літ. a GDPR або статті 9(2) літ. a GDPR (стаття 13(2) літ. c GDPR)

Якщо обробка персональних даних здійснюється на підставі ст. 6 ч. 1 п. "a" GDPR, тобто якщо суб'єкт даних надав згоду на обробку персональних даних для однієї або декількох конкретних цілей, або на підставі ст. 9 ч. 2 п. "a" GDPR, яка регулює пряму згоду на обробку спеціальних категорій персональних даних, суб'єкт даних має право відповідно до ст. 7 ч. 3 речення 1 GDPR відкликати свою згоду в будь-який час.

Відкликання згоди не впливає на законність обробки, яка здійснювалася на підставі згоди до її відкликання, ст. 7(3), речення 2 GDPR. Відкликати згоду має бути так само просто, як і надати згоду, ст. 7(3) речення 4 GDPR. Таким чином, відкликання згоди завжди може відбуватися у той самий спосіб, у який вона була надана, або у будь-який інший спосіб, який суб'єкт даних вважає більш простим. У сучасному інформаційному суспільстві, напевно, найпростішим способом відкликання згоди є простий електронний лист. Якщо суб'єкт даних бажає відкликати свою згоду, надану нам, достатньо надіслати нам простий електронний лист. Крім того, суб'єкт даних може обрати будь-який інший спосіб повідомити нам про відкликання своєї згоди.

## I. Право на подання скарги до наглядового органу (ст. 13(2) п. "d", 77(1) GDPR)

Як контролер, ми зобов'язані повідомити суб'єкта даних про право подати скаргу до наглядового органу, стаття 13(2) літ. d GDPR. Право на подання скарги до наглядового органу регулюється статтею 77(1) GDPR. Відповідно до цього положення, без шкоди для будь-якого іншого адміністративного або судового засобу правового захисту, кожен суб'єкт даних має право подати скаргу до наглядового органу, зокрема, в державі-члені за місцем його постійного проживання, місцем роботи або місцем передбачуваного порушення, якщо суб'єкт даних вважає, що обробка персональних даних, які його стосуються, порушує Загальний регламент про захист даних. Право на подання скарги до наглядового органу було обмежено правом Союзу лише таким чином, що воно може бути реалізоване лише в одному наглядовому органі (ст. 141, речення 1 GDPR). Це


© All rights reserved by Heiko Maniero.

правило спрямоване на уникнення подвійних скарг одного і того ж суб'єкта даних з одного і того ж питання. Тому, якщо суб'єкт даних хоче подати скаргу на нас, ми просимо звертатися лише до одного наглядового органу.

## J. Надання персональних даних як законодавча або договірна вимога; вимога, необхідна для укладення договору; обов'язок суб'єкта даних надати персональні дані; можливі наслідки ненадання таких даних (ст. 13(2) літ. e GDPR)

Ми роз'яснюємо, що надання персональних даних частково вимагається законом (наприклад, податкове законодавство) або може також випливати з договірних положень (наприклад, інформація про договірного партнера).

Іноді може виникнути необхідність в укладенні договору про те, що суб'єкт даних надає нам персональні дані, які в подальшому повинні бути оброблені нами. Суб'єкт даних, наприклад, зобов'язаний надати нам персональні дані, коли наша компанія підписує з ним договір. Ненадання персональних даних матиме наслідком те, що договір з суб'єктом даних не може бути укладений.

Перед наданням персональних даних суб'єктом персональних даних суб'єкт персональних даних повинен зв'язатися з нами. Ми роз'яснюємо суб'єкту персональних даних, чи вимагається надання персональних даних законом або договором або є необхідним для укладення договору, чи існує обов'язок надання персональних даних та наслідки ненадання персональних даних.

## K. Існування автоматизованого прийняття рішень, включаючи профілювання, про яке йдеться в ст. 22 (1) і (4) GDPR, і, принаймні, в цих випадках, змістовна інформація про логіку, а також про значення і передбачувані наслідки такої обробки для суб'єкта даних (ст. 13 (2) lit. f GDPR).

Як відповідальна компанія, ми зазвичай не використовуємо автоматизоване прийняття рішень або профілювання. Якщо у виняткових випадках ми здійснюємо автоматизоване прийняття рішень або профілювання, ми інформуємо суб'єкта даних або окремо, або через підрозділ у нашій політиці конфіденційності (на нашому веб-сайті). У цьому випадку застосовується наступне:

Автоматизоване прийняття рішень, включаючи профілювання, може відбуватися, якщо (1) це необхідно для укладення або виконання договору між суб'єктом даних і нами, або (2) це дозволено законодавством Союзу або держави-члена, якому ми підпорядковуємося, і яке також встановлює відповідні заходи для захисту прав, свобод і законних інтересів суб'єкта даних; або (3) це ґрунтується на явній згоді суб'єкта даних.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

У випадках, зазначених у статті 22(2)(a) і (c) GDPR, ми повинні вжити належних заходів для захисту прав, свобод і законних інтересів суб'єкта даних. У цих випадках ви маєте право на людське втручання з боку контролера, висловлення своєї точки зору та оскарження рішення.

Змістовна інформація про задіяну логіку, а також про значення і передбачувані наслідки такої обробки для суб'єкта даних викладена в нашій політиці конфіденційності.

## II. Дотримання вимог щодо інформування, коли персональні дані не збираються у суб'єкта персональних даних (ст. 14 GDPR)

### A. Ідентифікація та контактні дані контролера (стаття 14(1), підпункт "a" GDPR)

Див. вище

### B. Контактні дані Уповноваженого із захисту даних (стаття 14(1) літ. b GDPR)

Див. вище

### C. Цілі обробки, для яких призначені персональні дані, а також правові підстави для обробки (ст. 14(1) п. "c" GDPR)

Для даних заявника, які не були отримані від суб'єкта даних, метою обробки даних є проведення експертизи заявки в процесі прийому на роботу. З цією метою ми можемо обробляти дані, які не були отримані від Вас. На підставі даних, оброблених в процесі прийому на роботу, ми перевіримо, чи запрошені Ви на співбесіду (частина процесу відбору). Якщо ви будете прийняті нами на роботу, дані претендента будуть автоматично перетворені в дані працівника. Для даних працівників метою обробки даних є виконання трудового договору або дотримання інших правових норм, що застосовуються до трудових відносин. Дані працівника зберігаються після припинення трудових відносин з метою дотримання встановлених законодавством строків зберігання.

Правовою основою для обробки даних є стаття 6(1) пп. b і f GDPR, стаття 9(2) пп. b і h GDPR, стаття 88(1) GDPR та національне законодавство, наприклад, для Німеччини - розділ 26 BDSG (Федеральний закон про захист даних).

### D. Категорії відповідних персональних даних (ст. 14(1) п. "d" GDPR)

Дані заявника


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## E. Категорії отримувачів персональних даних (ст. 14(1) п. "e" GDPR)

Органи державної влади

Зовнішні органи

Інші зовнішні органи

Внутрішня переробка

Внутрішньогрупова обробка

Інші органи

Список наших обробників і одержувачів даних у третіх країнах і, за необхідності, міжнародних організаціях опублікований на нашому веб-сайті або може бути безкоштовно наданий за запитом. Будь ласка, зв'яжіться з нашим співробітником із захисту даних, щоб запросити цей список.

## F. Одержувачі в третій країні та відповідні або придатні гарантії, а також засоби, за допомогою яких можна отримати їхню копію або де вони були надані (ст. 14(1) літ. f, 46(1), 46(2) літ. c GDPR)

До одержувачів персональних даних можуть належати всі компанії та філії, що входять до складу нашої групи (далі - "компанії групи"), які мають місцезнаходження або офіс у третій країні. Перелік всіх компаній групи або одержувачів можна запросити у нас.

Відповідно до статті 46(1) GDPR контролер або процесор може передавати персональні дані до третьої країни лише за умови, що контролер або процесор забезпечив відповідні гарантії, а також за умови, що права суб'єктів даних, які підлягають захисту, та ефективні засоби правового захисту для суб'єктів даних є доступними. Відповідні гарантії можуть бути надані без необхідності отримання спеціального дозволу від наглядового органу за допомогою стандартних положень про захист даних, стаття 46(2), підпункт "c" GDPR.

Стандартні договірні положення Європейського Союзу або інші відповідні гарантії узгоджуються з усіма одержувачами з третіх країн перед першою передачею персональних даних. Таким чином, забезпечуються відповідні гарантії, права суб'єктів даних, що підлягають виконанню, та ефективні засоби правового захисту для суб'єктів даних. Кожен суб'єкт даних може отримати від нас копію стандартних договірних положень. Стандартні договірні положення також доступні в Офіційному віснику Європейського Союзу.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

Стаття 45(3) Загального регламенту про захист даних (GDPR) надає Європейській Комісії право за допомогою імплементаційного акту прийняти рішення про те, що країна за межами ЄС забезпечує належний рівень захисту. Це означає, що рівень захисту персональних даних в цілому еквівалентний рівню захисту в ЄС. Наслідком рішень, які визнають адекватний рівень захисту, є те, що персональні дані можуть вільно передаватися з ЄС (а також Норвегії, Ліхтенштейну та Ісландії) до третьої країни без подальших перешкод. Подібні правила діють у Великобританії, Швейцарії та деяких інших країнах.

Якщо Європейська Комісія або уряд іншої країни вирішить, що третя країна забезпечує належний рівень захисту, а також відповідну структуру (наприклад, EU-U.S. Data Privacy Framework, Swiss-U.S. Data Privacy Framework, UK Extension to the EU-U.S. Data Privacy Framework), всі передачі, які ми здійснюємо членам таких структур (наприклад, самосертифікованим суб'єктам), ґрунтуються виключно на членстві цих суб'єктів у відповідній структурі. У випадку, якщо ми або одна з компаній нашої групи є членом такої структури, всі передачі нам або компанії нашої групи ґрунтуються виключно на членстві компанії в такій структурі.

Будь-який суб'єкт даних може отримати копію цих рамок у нас. Крім того, рамки також доступні в Офіційному віснику Європейського Союзу, в опублікованих юридичних матеріалах або на веб-сайтах наглядових органів чи інших компетентних органів або установ.

## G. Період, протягом якого персональні дані будуть зберігатися, або, якщо це неможливо, критерії, використані для визначення цього періоду (ст. 14(2) п. "a" GDPR)

Термін зберігання персональних даних заявників становить 6 місяців. Для даних працівників застосовується відповідний законодавчо встановлений термін зберігання. Після закінчення цього терміну відповідні дані видаляються в робочому порядку, якщо вони більше не є необхідними для виконання трудового договору або укладення трудового договору.

## H. Повідомлення про законні інтереси, переслідувані контролером або третьою стороною, якщо обробка ґрунтується на статті 6(1) літ. f GDPR (ст. 14(2) літ. b GDPR)

Відповідно до статті 6(1) літ. f GDPR, обробка повинна бути законною, тільки якщо обробка необхідна для цілей законних інтересів, переслідуваних контролером або третьою стороною, за винятком випадків, коли такі інтереси переважають інтереси або основоположні права і свободи суб'єкта даних, які вимагають захисту персональних даних. Відповідно до п. 47 речення 2 GDPR законний інтерес може існувати, якщо між суб'єктом даних і контролером існують відповідні та належні відносини, наприклад, у ситуаціях, коли суб'єкт даних є клієнтом контролера. У всіх


© All rights reserved by Heiko Maniero.

випадках, коли наша компанія обробляє дані заявника на підставі статті 6(1) літ. f GDPR, наш законний інтерес полягає у залученні відповідного персоналу та професіоналів.

## I. Існування права вимагати від контролера доступу до персональних даних, їх виправлення чи видалення або обмеження обробки, що стосується суб'єкта даних, та заперечувати проти обробки, а також права на перенесення даних (ст. 14(2) п. "c" GDPR)

Всі суб'єкти персональних даних мають наступні права:

***Право на доступ***

Кожен суб'єкт персональних даних має право на доступ до персональних даних, які його стосуються. Право на доступ поширюється на всі дані, які ми обробляємо. Це право може бути реалізовано легко і з розумними інтервалами, щоб бути в курсі і перевіряти законність обробки (ст. 63 GDPR). Це право випливає зі ст. 15 GDPR. Суб'єкт даних може зв'язатися з нами для здійснення права на доступ.

***Право на виправлення***

Відповідно до частини 1 статті 16 GDPR суб'єкт даних має право вимагати від контролера без невиправданої затримки виправлення неточних персональних даних, що стосуються його або її, без невиправданої затримки. Крім того, ч. 2 ст. 16 GDPR передбачає, що суб'єкт даних має право, з урахуванням цілей обробки, на доповнення неповних персональних даних, у тому числі шляхом надання додаткової заяви. Суб'єкт даних може звернутися до нас для реалізації права на виправлення.

***Право на видалення (право на забуття)***

Крім того, суб'єкти даних мають право на видалення та право на забуття відповідно до ст. 17 GDPR. Цим правом також можна скористатися, звернувшись до нас. Однак на цьому етапі ми хотіли б зазначити, що це право не застосовується, якщо обробка необхідна для виконання юридичного зобов'язання, яке є предметом нашої компанії, ст. 17 (3) літ. b GDPR. Це означає, що ми можемо затвердити заявку на видалення тільки після закінчення встановленого законом терміну зберігання.

***Право на обмеження обробки даних***

Відповідно до статті 18 GDPR будь-який суб'єкт даних має право на обмеження обробки. Обмеження обробки може вимагатися, якщо виконується одна з умов, викладених у статті 18 (1) літ. a-d GDPR. Суб'єкт даних може зв'язатися з нами, щоб скористатися правом на обмеження обробки.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

***Право на заперечення***

Крім того, ст. 21 GDPR гарантує право на заперечення. Суб'єкт даних може зв'язатися з нами, щоб скористатися правом на заперечення.

***Право на перенесення даних***

Ст. 20 GDPR надає суб'єкту даних право на перенесення даних. Відповідно до цього положення суб'єкт даних має право за умов, викладених у ст. 20(1) пп. a і b GDPR, отримувати персональні дані, що стосуються його або її, які він або вона надали контролеру, у структурованому, загальноприйнятому та машинозчитуваному форматі, а також має право передавати ці дані іншому контролеру без перешкод з боку контролера, якому були надані персональні дані. Суб'єкт даних може зв'язатися з нами, щоб скористатися правом на перенесення даних.

## J. Існування права відкликати згоду в будь-який час, не впливаючи на законність обробки на підставі згоди до її відкликання, якщо обробка здійснюється на підставі ст. 6(1) п. "a" або ст. 9(2) п. "a" GDPR (ст. 14(2) п. "d" GDPR)

Якщо обробка персональних даних здійснюється на підставі ст. 6 ч. 1 п. "a" GDPR, тобто якщо суб'єкт даних надав згоду на обробку персональних даних для однієї або декількох конкретних цілей, або на підставі ст. 9 ч. 2 п. "a" GDPR, яка регулює пряму згоду на обробку спеціальних категорій персональних даних, суб'єкт даних має право відповідно до ст. 7 ч. 3 речення 1 GDPR відкликати свою згоду в будь-який час.

Відкликання згоди не впливає на законність обробки, яка здійснювалася на підставі згоди до її відкликання, ст. 7(3), речення 2 GDPR. Відкликати згоду має бути так само просто, як і надати згоду, ст. 7(3) речення 4 GDPR. Таким чином, відкликання згоди завжди може відбуватися у той самий спосіб, у який вона була надана, або у будь-який інший спосіб, який суб'єкт даних вважає більш простим. У сучасному інформаційному суспільстві, напевно, найпростішим способом відкликання згоди є простий електронний лист. Якщо суб'єкт даних бажає відкликати свою згоду, надану нам, достатньо надіслати нам простий електронний лист. Крім того, суб'єкт даних може обрати будь-який інший спосіб повідомити нам про відкликання своєї згоди.

## K. Право подати скаргу до наглядового органу (ст. 14(2) п. "e", 77(1) GDPR)

Як контролер, ми зобов'язані повідомити суб'єкта даних про право подати скаргу до наглядового органу, стаття 14(2) літ. e GDPR. Право на подання скарги до наглядового органу регулюється статтею 77(1) GDPR. Відповідно до цього положення, без шкоди для будь-якого іншого адміністративного або судового засобу правового захисту, кожен суб'єкт даних має право подати скаргу до наглядового органу, зокрема, в державі-члені за місцем свого постійного проживання, місцем роботи або місцем передбачуваного порушення, якщо суб'єкт даних вважає, що обробка персональних даних, які його стосуються, порушує Загальний регламент про захист даних. Право


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

на подання скарги до наглядового органу було обмежено правом Союзу лише таким чином, що воно може бути реалізоване лише в одному наглядовому органі (ст. 141, речення 1 GDPR). Це правило спрямоване на уникнення подвійних скарг одного і того ж суб'єкта даних з одного і того ж питання. Тому, якщо суб'єкт даних хоче подати скаргу на нас, ми просимо звертатися лише до одного наглядового органу.

## L. Джерело походження персональних даних, і, якщо застосовно, чи були вони отримані з загальнодоступних джерел (ст. 14(2) п. f GDPR)

В принципі, персональні дані збираються безпосередньо від суб'єкта даних або у співпраці з органом влади (наприклад, отримання даних з офіційного реєстру). Інші дані про суб'єктів даних отримуються з передач компаній групи. У контексті цієї загальної інформації точне визначення джерел, з яких походять персональні дані, є або неможливим, або вимагатиме непропорційних зусиль у розумінні ст. 14(5)(b) ЗРЗД. 14 (5) літ. b GDPR. В принципі, ми не збираємо персональні дані з загальнодоступних джерел.

Будь-який суб'єкт даних може звернутися до нас у будь-який час для отримання більш детальної інформації про точні джерела персональних даних, що стосуються його або її. Якщо походження персональних даних не може бути надано суб'єкту даних, оскільки використовувалися різні джерела, повинна бути надана загальна інформація (ст. 61, речення 4 GDPR).

## M. Існування автоматизованого прийняття рішень, включаючи профілювання, про яке йдеться в ст. 22(1) і (4) GDPR, і, принаймні, в цих випадках, змістовна інформація про логіку, а також про значення і передбачувані наслідки такої обробки для суб'єкта даних (ст. 14(2) lit. g GDPR).

Як відповідальна компанія, ми зазвичай не використовуємо автоматизоване прийняття рішень або профілювання. Якщо у виняткових випадках ми здійснюємо автоматизоване прийняття рішень або профілювання, ми інформуємо суб'єкта даних або окремо, або через підрозділ у нашій політиці конфіденційності (на нашому веб-сайті). У цьому випадку застосовується наступне:

Автоматизоване прийняття рішень, включаючи профілювання, може відбуватися, якщо (1) це необхідно для укладення або виконання договору між суб'єктом даних і нами, або (2) це дозволено законодавством Союзу або держави-члена, якому ми підпорядковуємося, і яке також встановлює відповідні заходи для захисту прав, свобод і законних інтересів суб'єкта даних; або (3) це ґрунтується на явній згоді суб'єкта даних.

У випадках, зазначених у статті 22(2)(a) і (c) GDPR, ми повинні вжити належних заходів для захисту прав, свобод і законних інтересів суб'єкта даних. У цих випадках ви маєте право на людське втручання з боку контролера, висловлення своєї точки зору та оскарження рішення.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

Змістовна інформація про задіяну логіку, а також про значення і передбачувані наслідки такої обробки для суб'єкта даних викладена в нашій політиці конфіденційності.

## III. EU-U.S. Data Privacy Framework (EU-U.S. DPF), UK Extension to the EU-U.S. DPF, Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF)

Якщо наша організація є сертифікованим членом EU-U.S. Data Privacy Framework (EU-U.S. DPF) та/або UK Extension to the EU-U.S. DPF та/або Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF), то діють наступні положення:

Ми дотримуємось EU-U.S. Data Privacy Framework (EU-U.S. DPF) та UK Extension to the EU-U.S. DPF, а також Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF), як це встановлено U.S. Department of Commerce. Наша компанія підтвердила Міністерству торгівлі США, що дотримується EU-U.S. Data Privacy Framework Principles (EU-U.S. DPF Principles) щодо обробки персональних даних, отриманих з Європейського Союзу та Сполученого Королівства на підставі EU-U.S. DPF та UK Extension to the EU-U.S. DPF. Наша компанія підтвердила Міністерству торгівлі США, що дотримується Swiss-U.S. Data Privacy Framework Principles (Swiss-U.S. DPF Principles) щодо обробки персональних даних, отриманих зі Швейцарії на підставі Swiss-U.S. DPF. У випадку суперечності між положеннями нашої політики конфіденційності та EU-U.S. DPF Principles та/або Swiss-U.S. DPF Principles, головними є Principles.

Щоб дізнатися більше про програму Data Privacy Framework (DPF) та переглянути нашу сертифікацію, відвідайте, будь ласка, https://www.dataprivacyframework.gov/.

Інші підрозділи або дочірні компанії нашої компанії у США, які також дотримуються EU-U.S. DPF Principles, включаючи UK Extension to the EU-U.S. DPF та Swiss-U.S. DPF Principles, якщо такі є, зазначені у нашій політиці конфіденційності.

Відповідно до EU-U.S. DPF та UK Extension to the EU-U.S. DPF, а також Swiss-U.S. DPF, наша компанія зобов'язується співпрацювати з органами, створеними європейськими органами захисту даних та британським Information Commissioner’s Office (ICO), а також швейцарським Federal Data Protection and Information Commissioner (EDÖB), та дотримуватись їхніх порад щодо невирішених скарг на наше поводження з персональними даними, які ми отримали на підставі EU-U.S. DPF, UK Extension to the EU-U.S. DPF та Swiss-U.S. DPF.

Ми інформуємо постраждалих осіб про компетентні європейські органи захисту даних, відповідальні за розгляд скарг на поводження нашої організації з персональними даними у верхній частині цього документа прозорості та про те, що ми надаємо постраждалим особам адекватні та безкоштовні засоби правового захисту.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

Ми інформуємо всіх постраждалих осіб про те, що наша компанія підлягає розслідувальним та виконавчим повноваженням Federal Trade Commission (FTC).

Постраждалі особи мають можливість за певних умов скористатися обов'язковим арбітражем. Наша організація зобов'язується врегульовувати вимоги та дотримуватися умов відповідно до Додатка I до DPF-Principals, якщо постраждала особа подала запит на обов'язковий арбітраж, повідомивши нашу організацію та дотримуючись процедур і умов, викладених у Додатку I до Principals.

Ми цим інформуємо всіх постраждалих осіб про відповідальність нашої організації у випадку передачі персональних даних третім особам.

Для запитань постраждалих осіб або органів нагляду за захистом даних ми призначили місцевих представників, зазначених у верхній частині цього документа прозорості.

Ми надаємо вам можливість вибору (Opt-out), чи будуть ваші персональні дані (i) передані третім особам або (ii) використані з метою, яка суттєво відрізняється від тієї (тих), для якої (яких) вони були спочатку зібрані або пізніше вами схвалені. Чіткий, добре видимий і легкодоступний механізм для реалізації вашого права вибору полягає у зв'язку з нашим відповідальним за захист даних (DSB) електронною поштою. У вас немає можливості вибору, і ми не зобов'язані це робити, якщо дані передаються третій стороні, яка діє як агент або обробник даних від нашого імені та за нашими вказівками. Однак ми завжди укладаємо договір з таким агентом або обробником даних.

Щодо чутливих даних (тобто персональних даних, які містять інформацію про стан здоров'я, расову або етнічну приналежність, політичні погляди, релігійні або філософські переконання, членство у профспілці або інформацію про сексуальне життя постраждалої особи), ми отримуємо вашу явну згоду (Opt-in), якщо ці дані (i) передаються третім особам або (ii) використовуються з іншою метою, ніж та, для якої вони були спочатку зібрані або для якої ви згодом надали свою згоду, зробивши вибір Opt-in. Крім того, ми розглядаємо всі персональні дані, які ми отримуємо від третіх осіб, як чутливі, якщо третя сторона їх ідентифікує та обробляє як чутливі.

Ми цим інформуємо вас про необхідність розкриття персональних даних у відповідь на законні запити органів влади, включаючи виконання вимог національної безпеки або правоохоронних органів.

Під час передачі персональних даних третій стороні, яка діє як контролер, ми дотримуємося принципів повідомлення та вибору (Principals). Ми також укладаємо договір з третьою стороною, відповідальною за обробку, який передбачає, що ці дані можуть оброблятися лише для обмежених та визначених цілей відповідно до наданої вами згоди та що отримувач забезпечує такий самий рівень захисту, як Principals DPF, і повідомляє нас, якщо виявить, що більше не може виконувати це зобов'язання. Договір передбачає, що третя сторона, яка діє як контролер, припиняє обробку або вживає інших відповідних і адекватних заходів для усунення проблеми у разі виявлення такої ситуації.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

Під час передачі персональних даних третій стороні, яка діє як агент або обробник даних, (i) ми передаємо ці дані лише для обмежених і визначених цілей; (ii) ми переконуємося, що агент або обробник даних зобов'язується забезпечити рівень захисту даних, принаймні такий самий, як вимагають DPF-Principals; (iii) ми вживаємо відповідних і адекватних заходів, щоб забезпечити, що агент або обробник даних фактично обробляє передані персональні дані таким чином, який відповідає нашим зобов'язанням відповідно до DPF-Principals; (iv) ми вимагаємо від агента або обробника даних повідомити нашу організацію, якщо він виявить, що більше не може виконувати зобов'язання щодо забезпечення такого ж рівня захисту, як це передбачено DPF-Principals; (v) після повідомлення, включаючи повідомлення за пунктом (iv), ми вживаємо відповідних і адекватних заходів, щоб припинити несанкціоновану обробку та усунути проблему; та (vi) ми надаємо DPF Department на запит резюме або представницький екземпляр відповідних положень договору про захист даних із цим агентом.

Відповідно до EU-U.S. DPF та/або UK Extension to the EU-U.S. DPF та/або Swiss-U.S. DPF, наша організація зобов’язується співпрацювати з органами, створеними європейськими органами захисту даних та британським Information Commissioner’s Office (ICO), а також швейцарським Federal Data Protection and Information Commissioner (EDÖB), та дотримуватись їхніх порад щодо невирішених скарг на наше поводження з персональними даними у зв'язку з трудовими відносинами, які ми отримали на підставі EU-U.S. DPF, UK Extension to the EU-U.S. DPF та Swiss-U.S. DPF.

Усі суб'єкти даних, які тимчасово перебувають у Європейському Союзі (ЄС), Європейській економічній зоні (ЄЕЗ) або Сполученому Королівстві, або мають там місце проживання чи звичайне місцеперебування, мають право на права та обов'язки суб'єктів даних, які опубліковані в нашому Документі про прозорість, а також випливають зі статей 15-22 GDPR, включаючи право на доступ до персональних даних. Ми зробили цю інформацію доступною всіма мовами ЄС та ЄЕЗ. Версія англійською мовою застосовується до Сполученого Королівства.

Усі суб'єкти даних, які тимчасово проживають у Швейцарії або мають там постійне місце проживання, користуються правами та обов'язками суб'єктів даних відповідно до Швейцарського закону про захист даних (DPA) та Швейцарського регламенту про захист даних (DPR), які опубліковані в нашому Документі про прозорість, включаючи право на доступ до персональних даних. Ми надали цю інформацію трьома офіційними мовами Швейцарії (німецькою, італійською та французькою).


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

# CHINESE：有关个人数据处理的信息（GDPR第13、14条）。

亲爱的先生或女士。

与我们公司有合同关系、合同前关系或其他关系的每个人的个人数据都应受到特别保护。我们的目标是将我们的数据保护水平保持在一个高标准。因此，我们例行展我们的数据保护和数据安全概念。

当然，我们遵守关于数据保护的法定条款。根据GDPR第13、14条，控制者在收集个人数据时满足特定的信息要求。本文件履行了这些义务。

法律规章的术语很复杂。不幸的是，在编写本文件的过程中，不能省略法律术语的使用。因此，我们想指出，如果您对本文件、所使用的术语或配方有任何疑问，随时欢迎与我们联系。

## I. 从数据主体收集个人数据时遵守信息要求（GDPR第13条）

### A.控制器的身份和联系方式（GDPR第13(1)条a款）

见上文

### B. 数据保护官的联系方式（GDPR 第13(1) 条b项）

见上文

### C. 个人数据的处理目的以及处理的法律依据（GDPR第13(1)条c项）

处理个人数据的目的是处理所有涉及控制器、客户、潜在客户、商业伙伴或其他命名群体之间的合同或合同前关系（最广泛的意义）或控制器的法律义务的业务。

艺术。6(1) lit. a GDPR作为处理业务的法律依据，我们为特定的处理目的获得同意。如果个人数据的处理对于履行数据主体为一方的合同是必要的，例如，当处理操作对于供应货物或提供任何其他服务是必要的，则处理是基于GDPR第6(1)条b项。这同样适用于为执行合同前措施而必须进行的处理操作，例如


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

，在有关我们的产品或服务的查询中。如果我们的公司受到法律义务的约束，需要对个人数据进行处理，例如为了履行税收义务，处理过程是基于GDPR第6（1）条。6(1) lit. c GDPR。

**在极少数情况下**，为了保护数据主体或其他自然人的重要利益，对个人数据的处理可能是必要的。例如，如果一个访客在我们公司受伤，他的姓名、年龄、健康保险数据或其他重要信息必须被传递给医生、医院或其他第三方，就会出现这种情况。那么，处理将基于第6(1)条。6(1) lit. d GDPR。

**如果**处理是出于公共利益或在行使赋予控制者的官方权力时执行任务所必需，则法律依据为《欧洲人权公约》第 6(1)e(e)条。6(1) lit. e GDPR。

**最后**，处理操作可以基于GDPR第6（1）条f项。这一法律依据用于不属于上述任何法律依据的处理操作，如果处理是我们公司**或第三方追求的合法利益所必需的**，**除非**这些利益被需要保护个人数据的数据主体的利益或基本权利和自由所压倒。这种处理操作是特别允许的，因为欧洲立法者已经特别提到了。他认为，如果数据主体是控制者的客户，就可以假定有合法的利益（Recital 47 Sentence 2 GDPR）。

## D. 如果处理是基于GDPR第6(1)条f项，控制人或第三方追求的合法利益（GDPR第13(1)条d项）

**如果个人数据的**处理是基于GDPR第6(1)条f款，**我**们的合法利益是为了有利于我们所有员工和股东的福祉而开展业务。

## E. 个人资料接收者的类别（GDPR第13(1)条e款）

**公共当局**

**外部机构**

**其他外部机构**

**内部**处理

**集**团内部处理


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

**其他机构**

**我**们在网站上公布或免费向我们索取我们在第三国的处理者和数据接收者（如适用）以及国际组织的名单。如需索取，请联系我们的数据保护专员。

## F. 第三国的接受者和**适当或合适的保障措施，以及**获得其副本的方式或已经提供的地方（GDPR第13(1)条f款，46(1)条，46(2)条c款）。

**所有属于我**们集团的公司和分支机构（以下简称 **"集**团公司"），**如果其**营业地或办公室在第三国，则可能属于个人数据的接收者。可以向我们索取所有集团公司或接收者的名单。

**根据**GDPR**第46(1)条，控制者或**处理者只能在控制者或处理者提供适当保障的情况下将个人数据转移到第三国，而且条件是可以为数据主体提供可执行的数据主体权利和有效的法律补救措施。适当的保障措施可以通过标准合同条款提供，而不需要监管机构的任何具体授权，GDPR**第46(2)条c款。**

**欧盟的**标准合同条款或其他适当的保障措施是在第一次传输个人数据之前与所有来**自第三国的接收者达成的。因此，可以确保适当的保障措施、可**执行的数据主体权利和对数据主体的有效法律补救措施得到保证。每个数据主体都可以从我们这里获得一份标准合同条款的副本。标准合同条款也可在《欧盟官方公报》上查阅。

**一般数据保**护条例》（GDPR）**第 45(3)条**规定，欧盟委员会有权通过实施法案，决定欧盟以外的国家是否能提供足够水平的保护。这意味着对个人数据的保护水平大致相当于欧盟的保护水平。认定具有适当保护水平的决定的效果是，个人数据可以从欧盟（以及挪威、列支敦士登和冰岛）自由流向第三国，而不会遇到进一步的障碍。英国、瑞士和其他一些国家也有类似的规定。

**如果欧盟委**员会或其他国家的政府决定第三国提供足够水平的保护，以及适用的框架（EU-U.S. Data Privacy Framework, Swiss-U.S. Data Privacy Framework, UK Extension to the EU-U.S. Data Privacy Framework），**我**们向此类框架成员（例如，自我认证实体）进行的所有传输仅基于这些实体在相关框架中的成员身份。如果我们或我们集团的某个实体是此类框架的成员，则向我们或我们集团的实体进行的所有转让完全基于该实体在此类框架中的成员身份。


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

任何数据当事人都可以从我们这里获得这些框架的副本。此外，这些框架也可在《欧盟官方公报》、已出版的法律资料或监管当局或其他主管当局或机构的网站上查阅。

## G. 个人数据的存储期限，或者如果不可能的话，用于确定该期限的标准（GDPR第13条第2款a项）

**用于确定个人数据存**储期限的标准是相应的法定保留期。该期限届满后，只要不再需要履行合同或启动合同，相应的数据将被例行删除。

**如果没有法定保留期限**，则以合同或内部保留期限为标准。

## H.向 控制人要求访问和纠正或删除个人数据或限制有关数据主体的处理或反对处理的权利的存在，以及数据移植的权利（GDPR第13(2)条b项）。

**所有数据主体都有以下**权利。

***获取的权利***

**每个数据主体都有**权利访问有关他或她的个人数据。访问的权利延伸到我们处理的所有数据。该权利可以在合理的时间间隔内轻松行使，以便**了解和核**实处理的合法性（GDPR**第63条**）。这项权利来自于第**15条。**15 GDPR。**数据主体可以**联系我们以行使访问权。

***纠正的权利***

**根据**GDPR**第16条第1款**，**数据主体有**权从控制者那里获得关于他或她的不准确的个人数据的纠正，而不会有不当的延迟。此外，GDPR**第16条第2款**规定，考虑到处理的目的，数据主体有权要求完成不完整的个人数据，包括通过提供补充说明的方式。数据主体可以与我们联系，行使纠正的权利。

***删除权(被遗忘权)***

**此外，根据第17条，数据主体有**权删除和被遗忘的权利。17GDPR。这一权利也可以通过联**系我**们来行使。然而，在这一点上，我们想指出的是，如果处理是为了履行我们公司必须遵守的法律义务，即GDPR**第17(3)条b款，那么**这项权利并不适用。这意味着，我们只能在法定保留期结束后批准删除申请。


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

*限制处理的权利*

根据GDPR第18条，任何数据主体都有权要求限制处理。如果符合GDPR第18(1)条a-d款规定的条件之一，就可以要求限制处理。数据主体可以联系我们以行使限制处理的权利。

*反对的权利*

此外，Art.21条GDPR保证了反对权。数据主体可以联系我们，行使反对权。

*数据可移植的权利*

第20条GDPR授予数据主体数据可移植性的权利。GDPR第20条授予数据主体数据可移植性的权利。根据这项规定，数据主体在GDPR第20(1)条a和b款规定的条件下，有权以结构化的、常用的和机器可读的格式接收他或她提供给控制者的关于他或她的个人数据，并有权将这些数据传送给另一个控制者，而不受提供个人数据的控制者的阻挠。数据主体可以联系我们，行使数据可移植性的权利。

## I. 如果处理是基于GDPR第6(1)条a项或GDPR第9(2)条a项，则存在随时撤销同意的权利，但不影响撤销前基于同意的处理的合法性(GDPR第13(2)条c项)

6(1) lit. a GDPR，也就是在这种情况下，如果数据主体已经同意为一个或多个特定目的处理个人数据，或者是基于第9(2)lit. a GDPR，其中规定了对特殊类别个人数据处理的明确同意，根据第7(3)句GDPR，数据主体有权在任何时候撤回他或她的同意。

撤销同意不应影响在撤销前基于同意的处理的合法性，GDPR第7(3)句话2。撤回同意应与给予同意一样容易，第7(3)条第4句GDPR。7(3) Sentence 4 GDPR。因此，撤销同意总是可以以与给予同意相同的方式或以数据主体认为更简单的任何其他方式进行。在当今的信息社会，撤销同意的最简单方式可能是一封简单的电子邮件。如果数据主体希望撤销他或她给予我们的同意，只需向我们发送一封简单的电子邮件即可。或者，数据主体可以选择任何其他方式向我们传达他或她对同意的撤销。

## J.向监管机构提出投诉的权利（GDPR第13(2)条d项、第77(1)条）

作为控制者，我们有义务通知数据主体向监督机构提出投诉的权利，GDPR第13（2）条d款。向监督机构提出投诉的权利由GDPR第77(1)条规定。根据该条款，在不影响任何其他行政或司法补救措施的情况下，如果数据主体认为与他或她有关的个人数据的处理违反了《一般数据保护条例》，每个数据主体应


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

有权向监督机构提出投诉，特别是在其惯常居住地、工作地点或被指控的侵权行为发生地所在的成员国。向监管机构提出投诉的权利只受到欧盟法律的限制，即只能在单一监管机构行使（GDPR第141句）。这一规则旨在避免同一数据主体在同一事项上的双重投诉。如果数据主体想对我们提出投诉，我们因此要求只联系一个监督机构。

## K. 作为法定或合同要求提供个人数据；签订合同的必要要求；数据主体提供个人数据的义务；未能提供此类数据的可能后果（GDPR第13(2)条e款）

我们澄清，个人数据的提供部分是由法律要求的（如税收规定），或者也可能是合同规定的结果（如关于合同伙伴的信息）。

有时，为了签订合同，数据主体可能需要向我们提供个人数据，而这些数据随后必须由我们处理。例如，当我们的公司与他或她签署合同时，数据主体有义务向我们提供个人数据。不提供个人数据的后果是，与数据主体的合同无法签订。

在数据主体提供个人数据之前，数据主体必须联系我们。我们向数据主体说明，提供个人数据是否是法律或合同要求的，或者是缔结合同所必需的，是否有义务提供个人数据以及不提供个人数据的后果。

## L. 存在GDPR第22(1)和(4)条中提到的自动决策，包括剖析，至少在这些情况下，提供有关所涉及的逻辑的有意义的信息，以及这种处理对数据主体的重要性和设想的后果（GDPR第13(2)条f项）。

作为一家负责任的公司，我们通常不会使用自动决策或特征分析。如果在特殊情况下，我们进行自动决策或特征分析，我们会单独或通过隐私政策的一个子部分（在我们的网站上）通知数据当事人。在这种情况下，适用以下规定：

在以下情况下，可进行自动决策（包括特征分析）：(1) 这是数据主体与我们之间签订或履行合同所必需的；或 (2) 这是我们所遵守的欧盟或成员国法律所授权的，并且该法律还规定了适当的措施来保障数据主体的权利和自由以及合法利益；或 (3) 这是基于数据主体的明确同意。


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

在 GDPR 第 22(2)(a)和(c)条提及的情况下，我们将采取适当措施保障数据当事人的权利、自由和合法利益。在这些情况下，您有权获得控制方的人工干预，表达您的观点并对决定提出异议。

在我们的隐私政策中，我们会为数据当事人提供有关逻辑以及此类处理的意义和预期后果的有意义的信息。

## II. 当不从数据主体收集个人数据时，遵守信息要求（GDPR第14条）

### A.控制器的身份和联系方式（GDPR第14(1)条a款）。

见上文

### B. 数据保护官的联系方式（GDPR第14(1)条b项）

见上文

### C. 个人数据的处理目的以及处理的法律依据（GDPR第14(1)条c项）

处理个人数据的目的是处理所有涉及控制器、客户、潜在客户、商业伙伴或其他命名群体之间的合同或合同前关系（最广泛的意义）或控制器的法律义务的业务。

如果个人数据的处理对于履行数据主体为一方的合同是必要的，例如，当处理操作对于供应货物或提供任何其他服务是必要的，则处理是基于GDPR第6(1)条b项。这同样适用于为执行合同前措施而必须进行的处理操作，例如，在有关我们的产品或服务的查询中。如果我们的公司受到法律义务的约束，需要对个人数据进行处理，例如为了履行税收义务，处理过程是基于GDPR第6（1）条。6(1) lit. c GDPR。

在极少数情况下，为了保护数据主体或其他自然人的重要利益，对个人数据的处理可能是必要的。例如，如果一个访客在我们公司受伤，他的姓名、年龄、健康保险数据或其他重要信息必须被传递给医生、医院或其他第三方，就会出现这种情况。那么，处理将基于第6(1)条。6(1) lit. d GDPR。


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

**如果**处理是出于公共利益或在行使赋予控制者的官方权力时执行任务所必需，则法律依据为《欧洲人权公约》第 6(1)e(e)**条**。6(1) lit. e GDPR。

**最后**，处理操作可以基于GDPR**第**6（1）**条**f项。这一法律依据用于不属于上述任何法律依据的处理操作，如果处理是我们公司或第三方追求的合法利益**所必需的**，**除非**这些利益被需要保护个人数据的数据主体的利益或基本权利和自由所压倒。这种处理操作是特别允许的，因为欧洲立法者已经特别提到了。他认为，如果数据主体是控制者的客户，就可以假定有合法的利益（Recital 47 Sentence 2 GDPR）。

## D. 有**关个人数据的**类别（GDPR第14(1)条d项）

**客**户数据

**潜在客**户的数据

**雇**员的数据

**供**应商的数据

## E. 个人资料接收者的类别（GDPR第14(1)条e款）

**公共当局**

**外部机构**

**其他外部机构**

**内部**处理

**集**团内部处理

**其他机构**


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

我们在网站上公布或免费向我们索取我们在第三国的处理者和数据接收者（如适用）以及国际组织的名单。如需索取，请联系我们的数据保护专员。

## F. 第三国的接受者和适当或合适的保障措施，以及获得其副本的方式或已经提供的地方（GDPR第14(1)条f款，46(1)条，46(2)条c款）。

所有属于我们集团的公司和分支机构（以下简称 "集团公司"），如果其营业场所或办公室在第三国，则可能属于个人数据的接收者。可以向我们索取所有集团公司的名单。

根据GDPR第46(1)条，控制者或处理者只能在控制者或处理者提供适当保障的情况下将个人数据转移到第三国，而且条件是可以为数据主体提供可执行的数据主体权利和有效的法律补救措施。适当的保障措施可以通过标准数据保护条款提供，而不需要监管机构的任何具体授权，GDPR第46（2）条c款。

欧盟的标准合同条款或其他适当的保障措施是在第一次传输个人数据之前与所有来自第三国的接收者达成的。因此，可以确保适当的保障措施、可执行的数据主体权利和对数据主体的有效法律补救措施得到保证。每个数据主体都可以从我们这里获得一份标准合同条款的副本。标准合同条款也可在《欧盟官方公报》上查阅。

一般数据保护条例》（GDPR）第 45(3)条规定，欧盟委员会有权通过实施法案，决定欧盟以外的国家是否能提供足够水平的保护。这意味着对个人数据的保护水平大致相当于欧盟的保护水平。认定具有适当保护水平的决定的效果是，个人数据可以从欧盟（以及挪威、列支敦士登和冰岛）自由流向第三国，而不会遇到进一步的障碍。英国、瑞士和其他一些国家也有类似的规定。

如果欧盟委员会或其他国家的政府决定第三国提供足够水平的保护，以及适用的框架（EU-U.S. Data Privacy Framework, Swiss-U.S. Data Privacy Framework, UK Extension to the EU-U.S. Data Privacy Framework），我们向此类框架成员（例如，自我认证实体）进行的所有传输仅基于这些实体在相关框架中的成员身份。如果我们或我们集团的某个实体是此类框架的成员，则向我们或我们集团的实体进行的所有转让完全基于该实体在此类框架中的成员身份。

任何数据当事人都可以从我们这里获得这些框架的副本。此外，这些框架也可在《欧盟官方公报》、已出版的法律资料或监管当局或其他主管当局或机构的网站上查阅。


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## G. 个人数据的存储期限，或者如果不可能的话，用于确定该期限的标准（GDPR第14(2)条a款）

**用来确定个人数据存**储期限的标准是各自的法定保留期。该期限届满后，只要不再需要履行合同或启动合同，相应的数据将被例行删除。

**如果没有法定保留期限**，则以合同或内部保留期限为标准。

## H. 如果处理是基于GDPR第6(1)条f项，则通知控制器或第三方所追求的合法利益（GDPR第14(2)条b项）。

**根据GDPR第6(1)条f**项，只有当处理是为了控制者或第三方所追求的合法利益所必需的，处理才是合法的，除非这些利益被需要保护个人数据的数据主体的利益或基本权利和自由所压倒。根据**GDPR第47句**话，如果数据主体和控制者之间存在相关和适当的关系，例如数据主体是控制者的客户的情况下，可能存在合法利益。在我们公司根据**GDPR第6(1)条f款**处理个人数据的所有情况下，我们的合法利益是为了有利于我们所有员工和股东的福祉而开展业务。

## I.向 控制人要求访问和纠正或删除个人数据或限制有关数据主体的处理以及反对处理的权利的存在，以及数据移植的权利（GDPR第14(2)条c项）。

**所有数据主体都有以下**权利。

***获取的权利***

**每个数据主体都有**权利访问有关他或她的个人数据。访问的权利延伸到我们处理的所有数据。该权利可以在合理的时间间隔内轻松行使，以便了解和核实处理的合法性（**GDPR第63条**）。这项权利来自于第**15条。15 GDPR。数据主体可以**联系我们以行使访问权。

***纠正的权利***

**根据GDPR第16条第1款，数据主体有**权从控制者那里获得关于他或她的不准确的个人数据的纠正，而不会有不当的延误。此外，**GDPR第16条第2句**规定，考虑到处**理的目的，数据主体有**权要求补全不完整的个人数据，包括通过提供补充说明。数据主体可以与我们联系，行使纠正的权利。


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

*删除权(被遗忘权)*

此外，根据第17条，数据主体有权删除和被遗忘的权利。17GDPR。这项权利也可以通过联系我们来行使。然而，在这一点上，我们想指出的是，如果处理是为了履行我们公司必须遵守的法律义务，即GDPR第17(3)条b款，那么这项权利并不适用。这意味着，我们只能在法定保留期结束后批准删除申请。

*限制处理的权利*

根据GDPR第18条，任何数据主体都有权要求限制处理。如果符合GDPR第18(1)条a-d款规定的条件之一，就可以要求限制处理。数据主体可以联系我们以行使限制处理的权利。

*反对的权利*

此外，Art.21条GDPR保证了反对权。数据主体可以联系我们，行使反对权。

*数据可移植的权利*

第20条GDPR授予数据主体数据可移植性的权利。GDPR第20条赋予数据主体以数据可移植性的权利。根据这项规定，数据主体在GDPR第20(1)条a和b款规定的条件下，有权以结构化的、常用的和机器可读的格式接收他或她提供给控制者的关于他或她的个人数据，并有权将这些数据传送给另一个控制者，而不受提供个人数据的控制者的阻挠。数据主体可以联系我们，行使数据可移植性的权利。

## J. 如果处理是基于GDPR第6(1)条a款或第9(2)条a款，则存在随时撤销同意的权利，但不影响撤销前基于同意的处理的合法性（GDPR第14(2)条d款）。

6(1) lit. a GDPR，也就是在这种情况下，如果数据主体已经同意为一个或多个特定目的处理个人数据，或者是基于第9(2)lit. a GDPR，其中规定了对特殊类别个人数据处理的明确同意，根据第7(3)句GDPR，数据主体有权在任何时候撤回他或她的同意。

撤销同意不应影响在撤销前基于同意的处理的合法性，GDPR第7(3)句话2。撤回同意应与给予同意一样容易，第7(3)条第4款。7(3) Sentence 4 GDPR。因此，撤销同意总是可以以与给予同意相同的方式或以数据主体认为更简单的任何其他方式进行。在当今的信息社会，撤销同意的最简单方式可能是一封简单的电子邮件。如果数据主体希望撤销他或她给予我们的同意，只需向我们发送一封简单的电子邮件即可。或者，数据主体可以选择任何其他方式向我们传达他或她的撤销同意。


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## K. 向监管机构提出投诉的权利（GDPR第14(2)条e款、第77(1)条）

作为控制者，我们有义务通知数据主体向监督机构提出投诉的权利，GDPR第14(2)条e款。向监督机构提出投诉的权利由GDPR第77(1)条规定。根据该条款，在不影响任何其他行政或司法补救措施的情况下，如果数据主体认为与他或她有关的个人数据的处理违反了《一般数据保护条例》，每个数据主体应有权向监督机构提出投诉，特别是在其惯常居住地、工作地点或被指控的侵权行为发生地所在的成员国。向监管机构提出投诉的权利只受到欧盟法律的限制，即只能在单一监管机构行使（GDPR第141句）。这一规则旨在避免同一数据主体在同一事项上的双重投诉。如果数据主体想对我们提出投诉，我们因此要求只与单一监管机构联系。

## L. 个人数据的来源，如果适用，是否来自可公开获取的来源（GDPR第14(2)条f项）

原则上，个人数据是直接从数据主体那里收集的，或者与权威机构合作（例如从官方登记册中检索数据）。其他关于数据主体的数据来自于集团公司的转让。在此一般信息的背景下，命名个人数据的确切来源是不可能的，或者会涉及到第14(5)条意义上的不相称的努力。14(5) lit. b GDPR。原则上，我们不会从公开渠道收集个人数据。

任何数据主体都可以在任何时候联系我们，以获得有关他或她的个人数据的确切来源的更详细的信息。如果因为使用了各种来源而无法向数据主体提供个人数据的来源，则应提供一般信息（Recital 61 Sentence 4 GDPR）。

## M. 存在GDPR第22(1)和(4)条中提到的自动决策，包括剖析，至少在这些情况下，提供有关所涉及的逻辑的有意义的信息，以及这种处理对数据主体的重要性和设想的后果（GDPR第14(2)条g项）。

作为一家负责任的公司，我们通常不会使用自动决策或特征分析。如果在特殊情况下，我们进行自动决策或特征分析，我们会单独或通过隐私政策的一个子部分（在我们的网站上）通知数据当事人。在这种情况下，适用以下规定：


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

在以下情况下，可进行自动决策（包括特征分析）：(1) 这是数据主体与我们之间签订或履行合同所必需的；或 (2) 这是我们所遵守的欧盟或成员国法律所授权的，并且该法律还规定了适当的措施来保障数据主体的权利和自由以及合法利益；或 (3) 这是基于数据主体的明确同意。

在 GDPR 第 22(2)(a)和(c)条提及的情况下，我们将采取适当措施保障数据当事人的权利、自由和合法利益。在这些情况下，您有权获得控制方的人工干预，表达您的观点并对决定提出异议。

在我们的隐私政策中，我们会为数据当事人提供有关逻辑以及此类处理的意义和预期后果的有意义的信息。

## III. EU-U.S. Data Privacy Framework (EU-U.S. DPF), UK Extension to the EU-U.S. DPF, Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF)

如果我们的组织是 EU-U.S. Data Privacy Framework (EU-U.S. DPF) 和/或 UK Extension to the EU-U.S. DPF 和/或 Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF) 的认证成员，则适用以下规定:

我们遵守 U.S. Department of Commerce 规定的 EU-U.S. Data Privacy Framework (EU-U.S. DPF)、UK Extension to the EU-U.S. DPF 以及 Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF)。本公司已向美国商务部确认，其遵守 EU-U.S. Data Privacy Framework Principles (EU-U.S. DPF Principles)，以处理从欧盟和英国根据 EU-U.S. DPF 和 UK Extension to the EU-U.S. DPF 接收的个人数据。本公司已向美国商务部确认，其遵守 Swiss-U.S. Data Privacy Framework Principles (Swiss-U.S. DPF Principles)，以处理从瑞士根据 Swiss-U.S. DPF 接收的个人数据。如果我们的隐私政策条款与 EU-U.S. DPF Principles 和/或 Swiss-U.S. DPF Principles 之间存在冲突，以 Principles 为准。

要了解更多有关 Data Privacy Framework (DPF) 计划的信息并查看我们的认证，请访问 https://www.dataprivacyframework.gov/。

本公司的其他美国单位或子公司也遵守 EU-U.S. DPF Principles，包括 UK Extension to the EU-U.S. DPF 和 Swiss-U.S. DPF Principles（如有），这些内容已在我们的隐私政策中列出。


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

根据 EU-U.S. DPF 和 UK Extension to the EU-U.S. DPF 以及 Swiss-U.S. DPF，本公司承诺与欧盟数据保护机构和英国 Information Commissioner's Office (ICO) 以及瑞士 Federal Data Protection and Information Commissioner (EDÖB) 设立的机构合作，并遵循其对我们根据 EU-U.S. DPF 和 UK Extension to the EU-U.S. DPF 以及 Swiss-U.S. DPF 接收的个人数据处理的未解决投诉的建议。

我们会在本透明度文件的顶部部分告知相关个人负责处理有关我们组织如何处理个人数据的投诉的相关欧洲数据保护机构，并告知我们向相关个人提供适当且免费的补救措施。

我们会告知所有相关个人，我们的公司受 Federal Trade Commission (FTC) 的调查和执行权限的管辖。

在特定条件下，相关个人有权申请具有约束力的仲裁程序。如果相关个人通知我们的组织并遵守附录 I 中规定的程序和条件申请具有约束力的仲裁程序，我们的组织有义务解决索赔并遵守 DPF-Principals 附录 I 中的条件。

我们在此告知所有相关个人，如果将个人数据传输给第三方，我们的组织将承担责任。

对于相关个人或数据保护监督机构的询问，我们已指定在本透明度文件顶部部分列出的当地代表。

我们为您提供选择（Opt-out）的机会，您可以选择您的个人数据（i）是否传输给第三方，或（ii）是否用于与最初收集或您后来授权的目的有实质性不同的目的。行使您选择权的明确、显眼且易于访问的机制是通过电子邮件联系我们的数据保护官 (DSB)。如果数据传输给在我们的指示下代表我们行事的代理人或数据处理者，您没有选择权，我们也没有义务这样做。然而，我们始终与此类代理人或数据处理者签订合同。

对于敏感数据（即包含健康状况、种族或民族出身、政治观点、宗教或哲学信仰、工会会员资格或相关个人的性生活信息的个人数据），如果这些数据（i）传输给第三方，或（ii）用于与最初收集或您后来授权的目的不同的其他目的，我们会征得您的明确同意（Opt-in）。此外，如果第三方将其识别和处理为敏感数据，我们将所有从第三方收到的个人数据视为敏感数据。

我们在此通知您，根据合法的政府请求披露个人数据的要求，包括履行国家安全或执法要求。


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

在将个人数据传输给作为数据控制者的第三方时，我们遵守通知和选择的原则（Principals）。我们还与负责处理的第三方签订合同，规定这些数据只能按照您提供的同意用于有限且特定的目的，并且接收方提供与 DPF 的 Principles 同等的保护水平，并在其发现无法继续履行该义务时通知我们。合同规定，当发现这种情况时，作为数据控制者的第三方应停止处理或采取其他适当和适当的措施以补救。

在将个人数据传输给作为代理人或数据处理者的第三方时，（i）我们仅将这些数据用于有限且特定的目的；（ii）我们确保代理人或数据处理者承诺提供至少与 DPF-Principals 要求相同的保护水平；（iii）我们采取适当和适当的措施，以确保代理人或数据处理者实际上按照与我们根据 DPF-Principals 的义务一致的方式处理传输的个人数据；（iv）我们要求代理人或数据处理者在发现无法继续履行与 DPF-Principals 所要求的相同保护水平的义务时通知我们的组织；（v）在通知（包括 (iv) 的通知）后，我们采取适当和适当的步骤以停止未经授权的处理并补救；（vi）我们应 DPF Department 的要求，提供与该代理人相关的数据保护条款的摘要或代表性副本。

根据 EU-U.S. DPF 和/或 UK Extension to the EU-U.S. DPF 和/或 Swiss-U.S. DPF，我们的组织承诺与欧盟数据保护机构和英国 Information Commissioner's Office (ICO) 以及瑞士 Federal Data Protection and Information Commissioner (EDÖB) 设立的机构合作，并遵循其对我们根据 EU-U.S. DPF 和 UK Extension to the EU-U.S. DPF 以及 Swiss-U.S. DPF 接收的与雇佣关系相关的个人数据处理的未解决投诉的建议。

所有临时居住在欧盟 (EU)、欧洲经济区 (EEA) 或英国的数据主体，或在欧盟、欧洲经济区或英国有住所或惯常居所的数据主体，均有权享有我们的透明度文件中公布的权利和数据主体权利，这些权利和权利也源于 GDPR 第 15 至 22 条，包括访问个人数据的权利。我们以所有欧盟和欧洲经济区语言提供此信息。英语版本适用于英国。

所有临时居住在瑞士或在瑞士有住所或惯常居所的数据主体均有权享有我们的透明度文件中公布的《瑞士数据保护法》（DPA）和《瑞士数据保护条例》（DPR）规定的权利和数据主体权利，包括访问个人数据的权利。我们以瑞士的三种官方语言（德语、意大利语和法语）提供这些信息。


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

# CHINESE：雇员和申请人的个人数据处理信息（GDPR第13、14条）。

亲爱的先生或女士。

**雇**员和申请人的个人数据应得到特别保护。我们的目标是将我们的数据保护水平保持在一个高标准。因此，我们例行展我们的数据保护和数据安全概念。

**当然，我**们遵守关于数据保护的法定条款。根据GDPR**第13、14条，控制者在**处理个人数据时满足特定的信息要求。本文件履行了这些义务。

**法律**规章的术语很复杂。不幸的是，在编写本文件的过程中，无法省去法律术语的使用。因此，我们想指出，如果您对本文件、所使用的术语或配方有任何疑问，随时欢迎与我们联系。

## I. 从数据主体收集个人数据时遵守信息要求（GDPR第13条）

### A.控制器的身**份和**联系方式（GDPR第13(1)条a款）

见上文

### B.数据保护官的联系方式（GDPR第13(1)条b项）

见上文

### C. 个人数据的处理目的以及处理的法律依据（GDPR第13(1)条c项）

对于申请人的数据，数据处理的目的是为了在招聘过程中对申请进行审查。为此，我们会处理您提供的所有数据。根据招聘过程中提交的数据，我们将检查您是否被邀请参加工作面试（选拔过程的一部分）。如果是一般合适的候选人，特别是在工作面试的情况下，我们会处理您提供的某些其他个人数据，这些数据对我们的选择决定至关重要。如果您被我们聘用，申请人的数据将自动转变为雇员数据。作为招


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

聘过程的一部分，我们将处理我们要求您提供的、为启动或履行您的合同所需的其他个人数据（如个人身份证号码或税号）。对于员工数据，数据处理的目的是履行雇佣合同**或遵守适用于雇佣关系的其他法律**规定（如税法），以及使用您的个人数据来执行与您缔结的雇佣合同（如在公司内部或向客户公布您的姓名和联系信息）。雇员数据在雇佣关系终止后被保存，以履行法律规定的保留期限。

**数据**处理的法律依据是GDPR第6条第1款b项、GDPR第9条第2款b项和h项、GDPR第88条第1款和国家**立法，例如德国的**BDSG第26条（联邦数据保护法）。

## D. 个人资料接收者的类别（GDPR第13(1)条e款）

**公共当局**

**外部机构**

**其他外部机构**

**内部**处理

**集**团内部处理

**其他机构**

**我**们在网站上公布或免费向我们索取我们在第三国的处理者和数据接收者（如适用）以及国际组织的名单。如需索取，请联系我们的数据保护专员。

## E. 第三国的收件人和**适当或合适的保障措施，以及**获得其副本的方式或已经提供的地方（GDPR第13(1)条f款，46(1)条，46(2)条c款）。

**所有属于我**们集团的公司和分支机构（以下简称 **"集**团公司"），**如果其**营业地或办公室在第三国，则可能属于个人数据的接收者。可以向我们索取所有集团公司或接收者的名单。


© All rights reserved by Heiko Maniero.

根据GDPR第46(1)条，控制者或处理者只能在控制者或处理者提供适当保障的情况下将个人数据转移到第三国，而且条件是可以为数据主体提供可执行的数据主体权利和有效的法律补救措施。适当的保障措施可以通过标准合同条款提供，而不需要监管机构的任何具体授权，GDPR第46(2)条c项。

欧盟的标准合同条款或其他适当的保障措施是在第一次传输个人数据之前与所有来自第三国的接收者达成的。因此，可以确保适当的保障措施、可执行的数据主体权利和对数据主体的有效法律补救措施得到保证。每个数据主体都可以从我们这里获得一份标准合同条款的副本。标准合同条款也可在《欧盟官方公报》上查阅。

一般数据保护条例》（GDPR）第 45(3)条规定，欧盟委员会有权通过实施法案，决定欧盟以外的国家是否能提供足够水平的保护。这意味着对个人数据的保护水平大致相当于欧盟的保护水平。认定具有适当保护水平的决定的效果是，个人数据可以从欧盟（以及挪威、列支敦士登和冰岛）自由流向第三国，而不会遇到进一步的障碍。英国、瑞士和其他一些国家也有类似的规定。

如果欧盟委员会或其他国家的政府决定第三国提供足够水平的保护，以及适用的框架（EU-U.S. Data Privacy Framework, Swiss-U.S. Data Privacy Framework, UK Extension to the EU-U.S. Data Privacy Framework），我们向此类框架成员（例如，自我认证实体）进行的所有传输仅基于这些实体在相关框架中的成员身份。如果我们或我们集团的某个实体是此类框架的成员，则向我们或我们集团的实体进行的所有转让完全基于该实体在此类框架中的成员身份。

任何数据当事人都可以从我们这里获得这些框架的副本。此外，这些框架也可在《欧盟官方公报》、已出版的法律资料或监管当局或其他主管当局或机构的网站上查阅。

## F. 个人数据的存储期限，或者如果不可能，用于确定该期限的标准（GDPR第13(2)条a项）

申请人的个人数据的保存期限为6个月。对于雇员的数据，适用相应的法定保存期。该期限结束后，只要不再需要履行合同或启动合同，相应的数据将被例行删除。


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## G. 有权要求控制人访问和纠正或删除个人数据或限制对数据主体的处理，或反对处理以及数据可移植性的权利（GDPR第13(2)条b项）。

**所有数据主体都有以下**权利。

***获取的权利***

**每个数据主体都有**权利访问有关他或她的个人数据。访问的权利延伸到我们处理的所有数据。该权利可以在合理的时间间隔内轻松行使，以便了解和核实处理的合法性（**GDPR第63条**）。这项权利来自于第15条。15 GDPR。**数据主体可以**联系我们以行使访问权。

***纠正的权利***

**根据GDPR第16条第1款，数据主体有**权从控制者那里获得关于他或她的不准确的个人数据的纠正，而不会有不当的延迟。此外，**GDPR第16条第2款**规定，考虑到处理的目的，数据主体有权要求完成不完整的个人数据，包括通过提供补充说明的方式。数据主体可以与我们联系，行使纠正的权利。

***删除权(被遗忘权)***

**此外，根据第17条，数据主体有**权删除和被遗忘的权利。17GDPR。这项权利也可以通过联系我们来行使。然而，在这一点上，我们想指出的是，如果处理是为了履行我们公司必须遵守的法律义务，即**GDPR第17(3)条b款，那么**这项权利并不适用。这意味着，我们只能在法定保留期结束后批准删除申请。

***限制处理的权利***

**根据GDPR第18条，任何数据主体都有**权要求限制处理。如果符合**GDPR第18(1)条a-d款**规定的条件之一，就可以要求限制处理。数据主体可以联系我们以行使限制处理的权利。

***反对的权利***

**此外，Art.21条GDPR保**证了反对权。数据主体可以联系我们，行使反对权。

***数据可移植的权利***

**第20条GDPR授予数据主体数据可移植性的**权利。**GDPR第20条授予数据主体数据可移植性的**权利。根据这项规定，数据主体在**GDPR第20(1)条a和b款**规定的条件下，有权以结构化的、常用的和机器可读的格式接收他或她提供给控制者的关于他或她的个人数据，并有权将这些数据传输给另一个控制者，而不受提供个人数据的控制者的阻碍。数据主体可以联系我们，行使数据可移植性的权利。


© All rights reserved by Heiko Maniero.

## H. 在处理基于GDPR第6条第1款a项或GDPR第9条第2款a项的情况下，存在随时撤销同意的权利，但不影响撤销前基于同意的处理的合法性（GDPR第13条第2款c项）。

6(1) lit. a GDPR，**也就是在**这种情况下，如果数据主体已经同意为一个或多个特定目的处理个人数据，或者是基于第9(2)lit. a GDPR，**其中**规定了对特殊类别个人数据处理的明确同意，根据第7(3)**句**GDPR，**数据主体有**权在任何时候撤回他或她的同意。

**撤**销同意不应影响在撤销前基于同意的处理的合法性，GDPR**第**7(3)**句**话2。**撤回同意**应与给予同意一样容易，第7(3)**条第**4**款**。GDPR**第**7(3)**条第**4**句**。**因此**，**撤**销同意总是可以以与给予同意相同的方式或以数据主体认为更简单的任何其他方式进行。在今天的信息社会，撤销同意的最简单方式可能是一封简单的电子邮件。如果数据主体希望撤销他或她给予我们的同意，向我们发送一封简单的电子邮件就足够了。或者，数据主体可以选择任何其他方式向我们传达他或她的撤销同意。

## I.向监管机构提出投诉的权利（GDPR第13(2)条d项、第77(1)条）

**作**为控制者，我们有义务通知数据主体向监督机构提出投诉的权利，GDPR**第**13(2)**条**d**款**。**向**监督机构提出投诉的权利**由**GDPR第77(1)条**规定。根据该条款，在不影响任何其他行政或司法补救措施的情况下，如果数据主体认为与他或她有关的个人数据的处理违反了《一般数据保护条例》，每个数据主体应有权向监督机构提出投诉，特别是在其惯常居住地、工作地点或被指控的侵权行为发生地所在的成员国。向监管机构提出投诉的权利只受到欧盟法律的限制，即只能在单一监管机构行使（GDPR**第**141**句**）。这一规则旨在避免同一数据主体在同一事项上的双重投诉。如果数据主体想对我们提出投诉，我们因此要求只联系一个监督机构。

## J. 作为法定或合同要求提供个人数据；签订合同的必要要求；数据主体提供个人数据的义务；未能提供此类数据的可能后果（GDPR第13(2)条e款）

**我**们澄清，个人数据的提供部分是由法律要求的（如税收规定），或者也可能是合同规定的结果（如关于合同伙伴的信息）。


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

有时，为了签订合同，数据主体可能需要向我们提供个人数据，而这些数据随后必须由我们处理。例如，当我们的公司与他或她签署合同时，数据主体有义务向我们提供个人数据。不提供个人数据的后果是，与数据主体的合同无法签订。

在数据主体提供个人数据之前，数据主体必须联系我们。我们向数据主体说明，提供个人数据是否是法律或合同要求的，或者是缔结合同所必需的，是否有义务提供个人数据以及不提供个人数据的后果。

### K. 存在GDPR第22(1)和(4)条中提到的自动决策，包括剖析，至少在这些情况下，要有关于所涉及的逻辑的有意义的信息，以及这种处理对数据主体的重要性和预期的后果（GDPR第13(2)条f项）。

作为一家负责任的公司，我们通常不会使用自动决策或特征分析。如果在特殊情况下，我们进行自动决策或特征分析，我们会单独或通过隐私政策的一个子部分（在我们的网站上）通知数据当事人。在这种情况下，适用以下规定：

在以下情况下，可进行自动决策（包括特征分析）：(1) 这是数据主体与我们之间签订或履行合同所必需的；或 (2) 这是我们所遵守的欧盟或成员国法律所授权的，并且该法律还规定了适当的措施来保障数据主体的权利和自由以及合法利益；或 (3) 这是基于数据主体的明确同意。

在 GDPR 第 22(2)(a)和(c)条提及的情况下，我们将采取适当措施保障数据当事人的权利、自由和合法利益。在这些情况下，您有权获得控制方的人工干预，表达您的观点并对决定提出异议。

在我们的隐私政策中，我们会为数据当事人提供有关逻辑以及此类处理的意义和预期后果的有意义的信息。

## II. 当不从数据主体收集个人数据时，遵守信息要求（GDPR第14条）

### A.控制器的身份和联系方式（GDPR第14(1)条a款）。

见上文


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## B. 数据保护官的联系方式（GDPR第14(1)条b项）

见上文

## C. 个人数据的处理目的以及处理的法律依据（GDPR第14(1)条c项）

对于不是从数据主体收集的申请人的数据，数据处理的目的是为了在招聘过程中对申请进行审查。为此，我们可能会处理不是从您那里收集的数据。根据招聘过程中处理的数据，我们将检查您是否被邀请参加工作面试（选拔过程的一部分）。如果您被我们录用，申请人的数据将自动转换为雇员数据。对于雇员数据，数据处理的目的是为了履行雇佣合同或遵守适用于雇佣关系的其他法律规定。雇员数据在雇佣关系终止后被**保存，以履行法律**规定的保留期限。

**数据**处理的法律依据是GDPR第6条第1款b和f项、GDPR第9条第2款b和h项、GDPR第88条第1款和国家**立法，如德国**BDSG第26条（联邦数据保护法）。

## D. 有**关个人数据的**类别（GDPR第14（1）条d项）

**申**请人的数据

**雇**员数据

## E. 个人资料接收者的类别（GDPR第14(1)条e款）

**公共当局**

**外部机构**

**其他外部机构**

**内部**处理

**集**团内部处理


© All rights reserved by Heiko Maniero.

**其他机构**

**我**们在网站上公布或免费向我们索取我们在第三国的处理者和数据接收者（如适用）以及国际组织的名单。如需索取，请联系我们的数据保护专员。

## F. 第三国的接受者和**适当或合适的保障措施，以及**获得其副本的方式或已经提供的地方（GDPR第14(1)条f款，46(1)条，46(2)条c款）。

**作**为我们集团一部分的所有公司和分支机构（以下简称 **"集**团公司"），**如果其**营业场所或办公室在第三国，则可能属于个人数据的接收者。可以向我们索取所有集团公司或接收者的名单。

**根据**GDPR第46(1)条，**控制者或**处理者只能在控制者或处理者提供适当保障的情况下将个人数据转移到第三国，而且条件是可以为数据主体提供可执行的数据主体权利和有效的法律补救措施。适当的保障措施可以通过标**准数据保**护条款提供，而不需要监管机构的任何具体授权，GDPR第46（2）条c款。

**欧盟的**标准合同条款**或其他适当的保障措施是在第一次**传输个人数据之前与所有来自第三国的接收者**达成的。因此，可以确保适当的保障措施、可**执行的数据主体权利和对数据主体的有效法律补救措施得到保证。每个数据主体都可以从我们这里获得一份标准合同条款的副本。标准合同条款也可在《欧盟官方公报》上查阅。

**一般数据保**护条例》（GDPR）第 45(3)条规定，欧盟委员会有权通过实施法案，决定欧盟以外的国家是否能提供足够水平的保护。这意味着对个人数据的保护水平大致相当于欧盟的保护水平。认定具有适当保护水平的决定的效果是，个人数据可以从欧盟（以及挪威、列支敦士登和冰岛）自由流向第三国，而不会遇到进一步的障碍。英国、瑞士和其他一些国家也有类似的规定。

**如果欧盟委**员会或其他国家的政府决定第三国提供足够水平的保护，以及适用的框架（EU-U.S. Data Privacy Framework, Swiss-U.S. Data Privacy Framework, UK Extension to the EU-U.S. Data Privacy Framework），**我**们向此类框架成员（例如，自我认证实体）进行的所有传输仅基于这些实体在相关框架中的成员身份。如果我们或我们集团的某个实体是此类框架的成员，则向我们或我们集团的实体进行的所有转让完全基于该实体在此类框架中的成员身份。


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

**任何数据当事人都可以从我**们这里获得这些框架的副本。此外，这些框架也可在《欧盟官方公报》、已出版的法律资料或监管当局或其他主管当局或机构的网站上查阅。

## G. 个人数据的存储期限，或者如果不可能的话，用于确定该期限的标准（GDPR第14(2)条a款）

**申**请人的个人数据的保存期限为**6个月**。对于雇员的数据，适用相应的法定保存期。该期限结束后，只要不再需要履行合同或启动合同，相应的数据将被例行删除。

## H. 如果处理是基于GDPR第6(1)条f项，则通知控制器或第三方所追求的合法利益（GDPR第14(2)条b项）。

**根据GDPR第6(1)条f**项，只有当处理是为了控制者或第三方所追求的合法利益的目的所必需时，处理才是合法的，除非这些利益被需要保护个人数据的数据主体的利益**或基本**权利和自由所压倒。根据GDPR**第47句**话，如果数据主体和控制者之间存在相关和适当的关系，例如数据主体是控制者的客户的情况下，可能存在合法利益。在我们公司根据**GDPR第6(1)条f款**处理申请人数据的所有情况下，我们的合法利益是雇用合适的人员和专业人士。

## I.向 控制人要求访问和纠正或删除个人数据或限制有关数据主体的处理以及反对处理的权利的存在，以及数据移植的权利（GDPR第14(2)条c项）。

**所有数据主体都有以下**权利。

***获取的权利***

**每个数据主体都有**权利访问有关他或她的个人数据。访问的权利延伸到我们处理的所有数据。该权利可以在合理的时间间隔内轻松行使，以便了解和核实处理的合法性（**GDPR第63条**）。这项权利来自于第**15条。15 GDPR。数据主体可以**联系我们以行使访问权。


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

*纠正的权利*

**根据GDPR第16条第1款，数据主体有**权从控制者那里获得关于他或她的不准确的个人数据的纠正，而不会有不当的延误。此外，GDPR**第16条第2句**规定，考虑到处理的目的，数据主体有权要求补全不完整的个人数据，包括通过提供补充说明。数据主体可以与我们联系，行使纠正的权利。

*删除权(被遗忘权)*

**此外，根据第17条，数据主体有**权删除和被遗忘的权利。17GDPR。这项权利也可以通过联系我们来行使。然而，在这一点上，我们想指出的是，如果处理是为了履行我们公司必须遵守的法律义务，即GDPR**第17(3)条b款，那么**这项权利并不适用。这意味着，我们只能在法定保留期结束后批准删除的申请。

*限制处理的权利*

**根据GDPR第18条，任何数据主体都有**权要求限制处理。如果符合GDPR**第18(1)条a-d款**规定的条件之一，就可以要求限制处理。数据主体可以联系我们以行使限制处理的权利。

*反对的权利*

**此外，**Art.21**条GDPR保**证了反对权。数据主体可以联**系我**们，行使反对权。

*数据可移植的权利*

**第20条GDPR授予数据主体数据可移植性的**权利。GDPR**第20条**赋予数据主体以数据可移植性的权利。根据这项规定，数据主体在GDPR**第20(1)条a和b款**规定的条件下，有权以结构化的、常用的和机器可读的格式接收他或她提供给控制器的关于他或她的个人数据，并有权将这些数据传送给另一个控制器，而不受提供个人数据的控制器的阻挠。数据主体可以联系我们，行使数据可移植性的权利。

## J. 如果处理是基于GDPR第6(1)条a款或第9(2)条a款，则存在随时撤销同意的权利，但不影响撤销前基于同意的处理的合法性（GDPR第14(2)条d款）。

6(1) lit. a GDPR，**即如果数据主体已**经同意为一个或多个特定目的处理个人数据，或者是基于第9(2)lit. a GDPR，**其中**规定了对特殊类别个人数据处理的明确同意，根据第7(3)**句**GDPR，**数据主体有**权在任何时候撤回他或她的同意。


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

撤销同意不应影响在撤销前基于同意的处理的合法性，GDPR第7(3)句话2。撤回同意应与给予同意一样容易，第7(3)条第4款。GDPR第7(3)条第4句。因此，撤销同意总是可以以与给予同意相同的方式或以数据主体认为更简单的任何其他方式进行。在今天的信息社会，撤销同意的最简单方式可能是一封简单的电子邮件。如果数据主体希望撤销他或她给予我们的同意，向我们发送一封简单的电子邮件就足够了。或者，数据主体可以选择任何其他方式向我们传达他或她的撤销同意。

## K. 向监管机构提出投诉的权利（GDPR第14(2)条e款，第77(1)条）。

作为控制者，我们有义务通知数据主体向监督机构提出投诉的权利，GDPR第14(2)条e款。向监督机构提出投诉的权利由GDPR第77(1)条规定。根据该条款，在不影响任何其他行政或司法补救措施的情况下，如果数据主体认为与他或她有关的个人数据的处理违反了《一般数据保护条例》，每个数据主体应有权向监督机构提出投诉，特别是在其惯常居住地、工作地点或被指控的侵权行为发生地所在的成员国。向监管机构提出投诉的权利只受到欧盟法律的限制，即只能在单一监管机构行使（GDPR第141句）。这一规则旨在避免同一数据主体在同一事项上的双重投诉。如果数据主体想对我们提出投诉，我们因此要求只与单一的监管机构联系。

## L. 个人数据的来源，如果适用，是否来自可公开获取的来源（GDPR第14(2)条f项）

原则上，个人数据是直接从数据主体那里收集的，或者与权威机构合作（例如从官方登记册中检索数据）。其他关于数据主体的数据来自于集团公司的转让。在此一般信息的背景下，命名个人数据的确切来源是不可能的，或者会涉及到第14(5)条意义上的不相称的努力。14(5) lit. b GDPR。原则上，我们不会从公开渠道收集个人数据。

任何数据主体都可以在任何时候联系我们，以获得有关他或她的个人数据的确切来源的更详细的信息。如果因为使用了不同的来源而无法向数据主体提供个人数据的来源，则应提供一般信息（Recital 61 Sentence 4 GDPR）。


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

M. 存在GDPR第22(1)和(4)条中提到的自动决策，包括剖析，至少在这些情况下，提供有关所涉及的逻辑的有意义的信息，以及这种处理对数据主体的重要性和设想的后果（GDPR第14(2)条g项）。

作为一家负责任的公司，我们通常不会使用自动决策或特征分析。如果在特殊情况下，我们进行自动决策或特征分析，我们会单独或通过隐私政策的一个子部分（在我们的网站上）通知数据当事人。在这种情况下，适用以下规定：

在以下情况下，可进行自动决策（包括特征分析）：(1) 这是数据主体与我们之间签订或履行合同所必需的；或 (2) 这是我们所遵守的欧盟或成员国法律所授权的，并且该法律还规定了适当的措施来保障数据主体的权利和自由以及合法利益；或 (3) 这是基于数据主体的明确同意。

在 GDPR 第 22(2)(a)和(c)条提及的情况下，我们将采取适当措施保障数据当事人的权利、自由和合法利益。在这些情况下，您有权获得控制方的人工干预，表达您的观点并对决定提出异议。

在我们的隐私政策中，我们会为数据当事人提供有关逻辑以及此类处理的意义和预期后果的有意义的信息。

## III. EU-U.S. Data Privacy Framework (EU-U.S. DPF), UK Extension to the EU-U.S. DPF, Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF)

如果我们的组织是 EU-U.S. Data Privacy Framework (EU-U.S. DPF) 和/或 UK Extension to the EU-U.S. DPF 和/或 Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF) 的认证成员，则适用以下规定:

我们遵守 U.S. Department of Commerce 规定的 EU-U.S. Data Privacy Framework (EU-U.S. DPF)、UK Extension to the EU-U.S. DPF 以及 Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF)。本公司已向美国商务部确认，其遵守 EU-U.S. Data Privacy Framework Principles (EU-U.S. DPF Principles)，以处理从欧盟和英国根据 EU-U.S. DPF 和 UK Extension to the EU-U.S. DPF 接收的个人数据。本公司已向美国商务部确认，其遵守 Swiss-U.S. Data Privacy Framework Principles (Swiss-U.S. DPF Principles)，以处理从瑞士根据 Swiss-U.S. DPF 接收的个人数据。如果我们的隐私政策条款与 EU-U.S. DPF Principles 和/或 Swiss-U.S. DPF Principles 之间存在冲突，以 Principles 为准。


© All rights reserved by Heiko Maniero.

要了解更多有关 Data Privacy Framework (DPF) 计划的信息并查看我们的认证，请访问 https://www.dataprivacyframework.gov/。

本公司的其他美国单位或子公司也遵守 EU-U.S. DPF Principles，包括 UK Extension to the EU-U.S. DPF 和 Swiss-U.S. DPF Principles（如有），这些内容已在我们的隐私政策中列出。

根据 EU-U.S. DPF 和 UK Extension to the EU-U.S. DPF 以及 Swiss-U.S. DPF，本公司承诺与欧盟数据保护机构和英国 Information Commissioner's Office (ICO) 以及瑞士 Federal Data Protection and Information Commissioner (EDÖB) 设立的机构合作，并遵循其对我们根据 EU-U.S. DPF 和 UK Extension to the EU-U.S. DPF 以及 Swiss-U.S. DPF 接收的个人数据处理的未解决投诉的建议。

我们会在本透明度文件的顶部部分告知相关个人负责处理有关我们组织如何处理个人数据的投诉的相关欧洲数据保护机构，并告知我们向相关个人提供适当且免费的补救措施。

我们会告知所有相关个人，我们的公司受 Federal Trade Commission (FTC) 的调查和执行权限的管辖。

在特定条件下，相关个人有权申请具有约束力的仲裁程序。如果相关个人通知我们的组织并遵守附录 I 中规定的程序和条件申请具有约束力的仲裁程序，我们的组织有义务解决索赔并遵守 DPF-Principals 附录 I 中的条件。

我们在此告知所有相关个人，如果将个人数据传输给第三方，我们的组织将承担责任。

对于相关个人或数据保护监督机构的询问，我们已指定在本透明度文件顶部部分列出的当地代表。

我们为您提供选择（Opt-out）的机会，您可以选择您的个人数据（i）是否传输给第三方，或（ii）是否用于与最初收集或您后来授权的目的有实质性不同的目的。行使您选择权的明确、显眼且易于访问的机制是通过电子邮件联系我们的数据保护官 (DSB)。如果数据传输给在我们的指示下代表我们行事的代理人或数据处理者，您没有选择权，我们也没有义务这样做。然而，我们始终与此类代理人或数据处理者签订合同。

对于敏感数据（即包含健康状况、种族或民族出身、政治观点、宗教或哲学信仰、工会会员资格或相关个人的性生活信息的个人数据），如果这些数据（i）传输给第三方，或（ii）用于与最初收集或您后来


© All rights reserved by Heiko Maniero.

授权的目的不同的其他目的，我们会征得您的明确同意（Opt-in）。此外，如果第三方将其识别和处理为敏感数据，我们将所有从第三方收到的个人数据视为敏感数据。

我们在此通知您，根据合法的政府请求披露个人数据的要求，包括履行国家安全或执法要求。

在将个人数据传输给作为数据控制者的第三方时，我们遵守通知和选择的原则（Principals）。我们还与负责处理的第三方签订合同，规定这些数据只能按照您提供的同意用于有限且特定的目的，并且接收方提供与 DPF 的 Principles 同等的保护水平，并在其发现无法继续履行该义务时通知我们。合同规定，当发现这种情况时，作为数据控制者的第三方应停止处理或采取其他适当和适当的措施以补救。

在将个人数据传输给作为代理人或数据处理者的第三方时，（i）我们仅将这些数据用于有限且特定的目的；（ii）我们确保代理人或数据处理者承诺提供至少与 DPF-Principals 要求相同的保护水平；（iii）我们采取适当和适当的措施，以确保代理人或数据处理者实际上按照与我们根据 DPF-Principals 的义务一致的方式处理传输的个人数据；（iv）我们要求代理人或数据处理者在发现无法继续履行与 DPF-Principals 所要求的相同保护水平的义务时通知我们的组织；（v）在通知（包括 (iv) 的通知）后，我们采取适当和适当的步骤以停止未经授权的处理并补救；（vi）我们应 DPF Department 的要求，提供与该代理人相关的数据保护条款的摘要或代表性副本。

根据 EU-U.S. DPF 和/或 UK Extension to the EU-U.S. DPF 和/或 Swiss-U.S. DPF，我们的组织承诺与欧盟数据保护机构和英国 Information Commissioner's Office (ICO) 以及瑞士 Federal Data Protection and Information Commissioner (EDÖB) 设立的机构合作，并遵循其对我们根据 EU-U.S. DPF 和 UK Extension to the EU-U.S. DPF 以及 Swiss-U.S. DPF 接收的与雇佣关系相关的个人数据处理的未解决投诉的建议。

所有临时居住在欧盟 (EU)、欧洲经济区 (EEA) 或英国的数据主体，或在欧盟、欧洲经济区或英国有住所或惯常居所的数据主体，均有权享有我们的透明度文件中公布的权利和数据主体权利，这些权利和权利也源于 GDPR 第 15 至 22 条，包括访问个人数据的权利。我们以所有欧盟和欧洲经济区语言提供此信息。英语版本适用于英国。


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

所有临时居住在瑞士或在瑞士有住所或惯常居所的数据主体均有权享有我们的透明度文件中公布的《瑞士数据保护法》（DPA）和《瑞士数据保护条例》（DPR）规定的权利和数据主体权利，包括访问个人数据的权利。我们以瑞士的三种官方语言（德语、意大利语和法语）提供这些信息。


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

# CZECH: Informace o zpracování osobních údajů (článek 13, 14 GDPR)

Vážený pane nebo paní,

Osobní údaje každé osoby, která je s naší společností ve smluvním, předsmluvním nebo jiném vztahu, si zaslouží zvláštní ochranu. Naším cílem je udržovat úroveň ochrany osobních údajů na vysoké úrovni. Proto běžně rozvíjíme naše koncepce ochrany a zabezpečení údajů.

Samozřejmě dodržujeme zákonná ustanovení o ochraně osobních údajů. Podle článků 13, 14 GDPR splňují správci při shromažďování osobních údajů zvláštní informační požadavky. Tento dokument tyto povinnosti splňuje.

Terminologie právních předpisů je složitá. Při přípravě tohoto dokumentu se bohužel nebylo možné obejít bez používání právních termínů. Proto bychom vás rádi upozornili, že se na nás můžete kdykoli obrátit se všemi dotazy týkajícími se tohoto dokumentu, použitých pojmů nebo formulací.

## I. Informace poskytované v případě, že osobní údaje jsou získány od subjektu údajů (článek 13 GDPR).

### A. Totožnost a kontaktní údaje správce a jeho případného zástupce (čl. 13 odst. 1 písm. a) GDPR)

Viz výše

### B. Případně kontaktní údaje případného pověřence pro ochranu osobních údajů (čl. 13 odst. 1 písm. b) GDPR)

Viz výše

### C. účely zpracování, pro které jsou osobní údaje určeny, a právní základ pro zpracování (čl. 13 odst. 1 písm. c) GDPR)

Účelem zpracování osobních údajů je vyřízení všech operací, které se týkají správce, zákazníků, potenciálních zákazníků, obchodních partnerů nebo jiných smluvních či předsmluvních vztahů mezi jmenovanými skupinami (v nejširším slova smyslu) nebo právních povinností správce.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

Čl. 6 odst. 1 písm. a) GDPR slouží jako právní základ pro operace zpracování, k nimž získáváme souhlas pro konkrétní účel zpracování. Pokud je zpracování osobních údajů nezbytné pro plnění smlouvy, jejíž smluvní stranou je subjekt údajů, jako je tomu například v případě, kdy jsou operace zpracování nezbytné pro dodání zboží nebo poskytnutí jiné služby, je zpracování založeno na čl. 6 odst. 1 písm. b GDPR. Totéž platí pro takové operace zpracování, které jsou nezbytné pro provedení opatření před uzavřením smlouvy, například v případě dotazů týkajících se našich produktů nebo služeb. Podléhá-li naše společnost právní povinnosti, kterou je vyžadováno zpracování osobních údajů, například pro plnění daňových povinností, je zpracování založeno na čl. 6 odst. 1 písm. c GDPR.

Ve výjimečných případech může být zpracování osobních údajů nezbytné pro ochranu životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby. Tak by tomu bylo například v případě, že by se návštěvník v naší společnosti zranil a jeho jméno, věk, údaje o zdravotním pojištění nebo jiné životně důležité informace by musely být předány lékaři, nemocnici nebo jiné třetí straně. Pak by se zpracování zakládalo na čl. 6 odst. 1 písm. d GDPR.

Pokud je zpracování nezbytné pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci svěřené správci, je právním základem čl. 6 odst. 1 písm. e) GDPR.

Nakonec mohou být operace zpracování založeny na čl. 6 odst. 1 písm. f) GDPR. Tento právní základ se používá pro operace zpracování, na které se nevztahuje žádný z výše uvedených právních základů, pokud je zpracování nezbytné pro účely oprávněných zájmů naší společnosti nebo třetí strany, s výjimkou případů, kdy před těmito zájmy mají přednost zájmy nebo základní práva a svobody subjektu údajů, které vyžadují ochranu osobních údajů. Takové operace zpracování jsou zvláště přípustné, protože byly výslovně zmíněny evropským zákonodárcem. Domníval se, že oprávněný zájem lze předpokládat, pokud je subjekt údajů klientem správce (47. bod odůvodnění, věta 2 GDPR).

## D. Oprávněné zájmy správce nebo třetí strany v případě, že je zpracování založeno na čl. 6 odst. 1 písm. f) (čl. 13 odst. 1 písm. d) GDPR).

Pokud je zpracování osobních údajů založeno na čl. 6 odst. 1 písm. f GDPR, je naším oprávněným zájmem vykonávat naši činnost ve prospěch blaha všech našich zaměstnanců a akcionářů.

## E. Případné příjemce nebo kategorie příjemců osobních údajů (čl. 13 odst. 1 písm. e) GDPR)

Orgány veřejné správy

Externí subjekty

Další externí subjekty


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

Interní zpracování

Zpracování v rámci skupiny

Ostatní subjekty

Seznam našich zpracovatelů a příjemců údajů ve třetích zemích a případně mezinárodních organizací je zveřejněn na našich webových stránkách nebo si jej můžete u nás bezplatně vyžádat. Pro vyžádání tohoto seznamu se prosím obraťte na našeho pověřence pro ochranu osobních údajů.

## F. Případný úmysl správce předat osobní údaje do třetí země nebo mezinárodní organizaci a existenci či neexistenci rozhodnutí Komise o odpovídající ochraně nebo, v případech předání uvedených v článcích 46 nebo 47 nebo čl. 49 odst. 1 druhém pododstavci, odkaz na vhodné záruky a prostředky k získání kopie těchto údajů nebo informace o tom, kde byly tyto údaje zpřístupněny.

Mezi příjemce osobních údajů mohou patřit všechny společnosti a pobočky, které jsou součástí naší skupiny (dále jen "společnosti skupiny") a které mají místo podnikání nebo kancelář ve třetí zemi. Seznam všech společností skupiny nebo příjemců si můžete vyžádat u nás.

Podle čl. 46 odst. 1 GDPR může správce nebo zpracovatel předat osobní údaje do třetí země pouze tehdy, pokud správce nebo zpracovatel poskytl vhodné záruky a pokud jsou k dispozici vymahatelná práva subjektu údajů a účinné právní prostředky nápravy pro subjekty údajů. Vhodné záruky lze poskytnout, aniž by bylo vyžadováno zvláštní povolení dozorového úřadu, prostřednictvím standardních smluvních doložek, čl. 46 odst. 2 písm. c) GDPR.

Se všemi příjemci ze třetích zemí jsou před prvním předáním osobních údajů dohodnuty standardní smluvní doložky Evropské unie nebo jiné vhodné záruky. V důsledku toho je zajištěno, že jsou zaručeny vhodné záruky, vymahatelná práva subjektů údajů a účinné právní prostředky nápravy pro subjekty údajů. Každý subjekt údajů u nás může získat kopii standardních smluvních doložek. Standardní smluvní doložky jsou rovněž k dispozici v Úředním věstníku Evropské unie.

Podle čl. 45 odst. 3 obecného nařízení o ochraně osobních údajů (GDPR) má Evropská komise právo rozhodnout prostřednictvím prováděcího aktu, že země mimo EU poskytuje odpovídající úroveň ochrany. To znamená úroveň ochrany osobních údajů, která je v zásadě rovnocenná úrovni ochrany v EU. Důsledkem rozhodnutí o odpovídající úrovni ochrany je, že osobní údaje mohou volně proudit z EU (a Norska, Lichtenštejnska a Islandu) do třetí země bez dalších překážek. Podobná pravidla platí ve Spojeném království, Švýcarsku a některých dalších zemích.

V případě, že Evropská komise nebo vláda jiné země rozhodne, že třetí země poskytuje odpovídající úroveň ochrany, a příslušný rámec (např. EU-U.S. Data Privacy Framework, Swiss-U.S. Data Privacy Framework, UK Extension to the EU-U.S. Data Privacy Framework), veškerá naše předávání údajů


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

členům těchto rámců (např. samostatně certifikovaným subjektům) jsou založena výhradně na členství těchto subjektů v příslušném rámci. V případě, že jsme my nebo některý ze subjektů naší skupiny členem takového rámce, jsou veškerá předání nám nebo subjektu naší skupiny založena výhradně na členství tohoto subjektu v takovém rámci.

Každý subjekt údajů u nás může získat kopii rámců. Kromě toho jsou rámce k dispozici také v Úředním věstníku Evropské unie nebo ve zveřejněných právních materiálech či na internetových stránkách dozorových úřadů nebo jiných příslušných orgánů či institucí.

## G. Doba, po kterou budou osobní údaje uloženy, nebo není-li ji možné určit, kritéria použitá pro stanovení této doby (čl. 13 odst. 2 písm. a) GDPR)

Kritériem pro určení doby uchovávání osobních údajů je příslušná zákonná doba uchovávání. Po uplynutí této doby jsou příslušné údaje běžně vymazávány, pokud již nejsou nezbytné pro plnění smlouvy nebo zahájení smlouvy.

Pokud neexistuje zákonná doba uchovávání, je kritériem smluvní nebo interní doba uchovávání.

## H. Existence práva požadovat od správce přístup k osobním údajům týkajícím se subjektu údajů, jejich opravu nebo výmaz, popřípadě omezení zpracování, a vznést námitku proti zpracování, jakož i práva na přenositelnost údajů (čl. 13 odst. 2 písm. b) GDPR)

Všechny subjekty údajů mají následující práva:

***Právo na přístup***

Každý subjekt údajů má právo na přístup k osobním údajům, které se ho týkají. Právo na přístup se vztahuje na všechny údaje, které zpracováváme. Toto právo lze uplatnit snadno a v přiměřených intervalech, aby bylo možné se seznámit se zákonností zpracování a ověřit si ji (63. bod odůvodnění GDPR). Toto právo vyplývá z čl. 15 GDPR. Subjekt údajů nás může kontaktovat za účelem uplatnění práva na přístup.

***Právo na opravu***

Podle článku 16 věty 1 GDPR má subjekt údajů právo na to, aby správce bez zbytečného odkladu opravil nepřesné osobní údaje, které se ho týkají. Článek 16 věta 2 GDPR dále stanoví, že subjekt údajů má s ohledem na účely zpracování právo na doplnění neúplných osobních údajů, a to i prostřednictvím poskytnutí doplňujícího prohlášení. Subjekt údajů se na nás může obrátit, aby uplatnil právo na opravu.

***Právo na výmaz (právo být zapomenut)***

Kromě toho mají subjekty údajů právo na výmaz a právo být zapomenut podle čl. 17 GDPR. Toto právo lze rovněž uplatnit tak, že nás kontaktujete. Na tomto místě bychom však rádi upozornili, že toto právo


© All rights reserved by Heiko Maniero.

neplatí, pokud je zpracování nezbytné pro splnění právní povinnosti, která se na naši společnost vztahuje, čl. 17 odst. 3 písm. b GDPR. To znamená, že žádost o výmaz můžeme schválit až po uplynutí zákonné doby uchovávání.

***Právo na omezení zpracování***

Podle článku 18 GDPR má každý subjekt údajů právo na omezení zpracování. Omezení zpracování lze požadovat, pokud je splněna jedna z podmínek uvedených v čl. 18 odst. 1 písm. a-d GDPR. Subjekt údajů nás může kontaktovat, aby uplatnil právo na omezení zpracování.

***Právo vznést námitku***

Kromě toho čl. 21 GDPR zaručuje právo vznést námitku. Subjekt údajů nás může kontaktovat, aby uplatnil právo na námitku.

***Právo na přenositelnost údajů***

Čl. 20 GDPR přiznává subjektu údajů právo na přenositelnost údajů. Podle tohoto ustanovení má subjekt údajů za podmínek stanovených v čl. 20 odst. 1 písm. a) a b) GDPR právo získat osobní údaje, které se ho týkají a které poskytl správci, ve strukturovaném, běžně používaném a strojově čitelném formátu a má právo předat tyto údaje jinému správci, aniž by tomu správce, kterému byly osobní údaje poskytnuty, bránil. Subjekt údajů nás může kontaktovat za účelem uplatnění práva na přenositelnost údajů.

## I. Pokud je zpracování založeno na čl. 6 odst. 1 písm. a) nebo čl. 9 odst. 2 písm. a), existence práva odvolat kdykoli souhlas, aniž je tím dotčena zákonnost zpracování založená na souhlasu uděleném před jeho odvoláním (čl. 13 odst. 2 písm. c) GDPR).

Pokud je zpracování osobních údajů založeno na čl. 6 odst. 1 písm. a) GDPR, což je případ, kdy subjekt údajů udělil souhlas se zpracováním osobních údajů pro jeden nebo více konkrétních účelů, nebo je založeno na čl. 9 odst. 2 písm. a) GDPR, který upravuje výslovný souhlas se zpracováním zvláštních kategorií osobních údajů, má subjekt údajů podle čl. 7 odst. 3 věty první GDPR právo svůj souhlas kdykoli odvolat.

Odvolání souhlasu nemá vliv na zákonnost zpracování založeného na souhlasu před jeho odvoláním, čl. 7 odst. 3 věta druhá GDPR. Odvolání souhlasu musí být stejně snadné jako jeho udělení, čl. 7 odst. 3 věta 4 GDPR. K odvolání souhlasu proto může dojít vždy stejným způsobem, jakým byl souhlas udělen, nebo jakýmkoli jiným způsobem, který subjekt údajů považuje za jednodušší. V dnešní informační společnosti je pravděpodobně nejjednodušším způsobem odvolání souhlasu prostý e-mail. Pokud si subjekt údajů přeje odvolat svůj souhlas, který nám udělil, stačí nám zaslat jednoduchý e-mail. Případně si subjekt údajů může zvolit jakýkoli jiný způsob, jak nám svůj souhlas odvolat.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## J. Existence práva podat stížnost u dozorového úřadu (čl. 13 odst. 2 písm. d), čl. 77 odst. 1 GDPR)

Jako správce jsme povinni informovat subjekt údajů o právu podat stížnost u dozorového úřadu, čl. 13 odst. 2 písm. d) GDPR. Právo podat stížnost u dozorového úřadu upravuje čl. 77 odst. 1 GDPR. Podle tohoto ustanovení, aniž jsou dotčeny jakékoli jiné správní nebo soudní prostředky nápravy, má každý subjekt údajů právo podat stížnost u dozorového úřadu, zejména v členském státě svého obvyklého bydliště, pracoviště nebo místa údajného porušení, pokud se subjekt údajů domnívá, že zpracování osobních údajů, které se ho týkají, porušuje obecné nařízení o ochraně osobních údajů. Právo podat stížnost u dozorového úřadu bylo právem Unie omezeno pouze tak, že jej lze uplatnit pouze u jediného dozorového úřadu (141. bod odůvodnění věta první obecného nařízení o ochraně osobních údajů). Toto pravidlo má zabránit dvojím stížnostem téhož subjektu údajů v téže věci. Pokud na nás chce subjekt údajů podat stížnost, požádali jsme ho proto, aby se obrátil pouze na jediný dozorový úřad.

## K. Skutečnost, zda poskytování osobních údajů je zákonným či smluvním požadavkem, nebo požadavkem, který je nutné uvést do smlouvy, a zda má subjekt údajů povinnost osobní údaje poskytnout, a ohledně možných důsledků neposkytnutí těchto údajů (čl. 13 odst. 2 písm. e) GDPR)

Upřesňujeme, že poskytnutí osobních údajů je částečně vyžadováno zákonem (např. daňovými předpisy) nebo může vyplývat také ze smluvních ustanovení (např. informace o smluvním partnerovi).

Někdy může být pro uzavření smlouvy nezbytné, aby nám subjekt údajů poskytl osobní údaje, které musíme následně zpracovat. Subjekt údajů je například povinen poskytnout nám osobní údaje, když s ním naše společnost uzavře smlouvu. Neposkytnutí osobních údajů by mělo za následek, že by smlouva se subjektem údajů nemohla být uzavřena.

Před poskytnutím osobních údajů subjektem údajů nás musí subjekt údajů kontaktovat. Subjektu údajů objasníme, zda je poskytnutí osobních údajů vyžadováno zákonem nebo smlouvou nebo zda je nezbytné pro uzavření smlouvy, zda existuje povinnost osobní údaje poskytnout a jaké jsou důsledky neposkytnutí osobních údajů.

## L. Skutečnost, že dochází k automatizovanému rozhodování, včetně profilování, uvedenému v čl. 22 odst. 1 a 4, a přinejmenším v těchto případech smysluplné informace týkající se použitého postupu, jakož i významu a předpokládaných důsledků takového zpracování pro subjekt údajů (čl. 13 odst. 2 písm. f) GDPR).

Jako odpovědná společnost obvykle nepoužíváme automatizované rozhodování ani profilování. Pokud ve výjimečných případech automatizované rozhodování nebo profilování provádíme, informujeme o tom


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

subjekt údajů buď samostatně, nebo prostřednictvím pododdílu v našich zásadách ochrany osobních údajů (na našich webových stránkách). V takovém případě platí následující:

K automatizovanému rozhodování - včetně profilování - může dojít, pokud (1) je to nezbytné pro uzavření nebo plnění smlouvy mezi subjektem údajů a námi, nebo (2) je to povoleno právem Unie nebo členského státu, které se na nás vztahuje a které rovněž stanoví vhodná opatření na ochranu práv a svobod a oprávněných zájmů subjektu údajů, nebo (3) je to založeno na výslovném souhlasu subjektu údajů.

V případech uvedených v čl. 22 odst. 2 písm. a) a c) GDPR provedeme vhodná opatření na ochranu práv a svobod a oprávněných zájmů subjektu údajů. V těchto případech máte právo na lidský zásah ze strany správce, na vyjádření svého názoru a na napadení rozhodnutí.

Smysluplné informace o příslušné logice, jakož i o významu a předpokládaných důsledcích takového zpracování pro subjekt údajů jsou uvedeny v našich zásadách ochrany osobních údajů.

## II. Informace poskytované v případě, že osobní údaje nebyly získány od subjektu údajů (článek 14 GDPR)

### A. Totožnost a kontaktní údaje správce a případně jeho zástupce (čl. 14 odst. 1 písm. a) GDPR)

Viz výše

### B. Případně kontaktní údaje případného pověřence pro ochranu osobních údajů (čl. 14 odst. 1 písm. b) GDPR)

Viz výše

### C. účely zpracování, pro které jsou osobní údaje určeny, a právní základ pro zpracování (čl. 14 odst. 1 písm. c) GDPR)

Účelem zpracování osobních údajů je vyřízení všech operací, které se týkají správce, zákazníků, potenciálních zákazníků, obchodních partnerů nebo jiných smluvních či předsmluvních vztahů mezi jmenovanými skupinami (v nejširším slova smyslu) nebo právních povinností správce.

Pokud je zpracování osobních údajů nezbytné pro plnění smlouvy, jejíž smluvní stranou je subjekt údajů, jako je tomu například v případě, kdy jsou operace zpracování nezbytné pro dodání zboží nebo poskytnutí jiné služby, je zpracování založeno na čl.6 odst.1 písm. b) GDPR. Totéž platí pro takové operace zpracování, které jsou nezbytné pro provedení opatření před uzavřením smlouvy, například v


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

případě dotazů týkajících se našich produktů nebo služeb. Podléhá-li naše společnost právní povinnosti, kterou je vyžadováno zpracování osobních údajů, například pro plnění daňových povinností, je zpracování založeno na čl. 6 odst. 1 písm. c GDPR.

Ve výjimečných případech může být zpracování osobních údajů nezbytné pro ochranu životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby. Tak by tomu bylo například v případě, že by se návštěvník v naší společnosti zranil a jeho jméno, věk, údaje o zdravotním pojištění nebo jiné životně důležité informace by musely být předány lékaři, nemocnici nebo jiné třetí straně. Pak by se zpracování zakládalo na čl. 6 odst. 1 písm. d GDPR.

Pokud je zpracování nezbytné pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci svěřené správci, je právním základem čl. 6 odst. 1 písm. e) GDPR.

Nakonec mohou být operace zpracování založeny na čl. 6 odst. 1 písm. f) GDPR. Tento právní základ se používá pro operace zpracování, na které se nevztahuje žádný z výše uvedených právních základů, pokud je zpracování nezbytné pro účely oprávněných zájmů naší společnosti nebo třetí strany, s výjimkou případů, kdy před těmito zájmy mají přednost zájmy nebo základní práva a svobody subjektu údajů, které vyžadují ochranu osobních údajů. Takové operace zpracování jsou zvláště přípustné, protože byly výslovně zmíněny evropským zákonodárcem. Domníval se, že oprávněný zájem lze předpokládat, pokud je subjekt údajů klientem správce (47. bod odůvodnění, věta 2 GDPR).

## D. Kategorie dotčených osobních údajů (čl. 14 odst. 1 písm. d) GDPR)

Údaje o zákaznících

Údaje o potenciálních zákaznících

Údaje o zaměstnancích

Údaje o dodavatelích

## E. Případné příjemce nebo kategorie příjemců osobních údajů (čl. 14 odst. 1 písm. e) GDPR)

Orgány veřejné správy

Externí subjekty

Další externí subjekty


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

Interní zpracování

Zpracování v rámci skupiny

Ostatní subjekty

Seznam našich zpracovatelů a příjemců údajů ve třetích zemích a případně mezinárodních organizací je zveřejněn na našich webových stránkách nebo si jej můžete u nás bezplatně vyžádat. Pro vyžádání tohoto seznamu se prosím obraťte na našeho pověřence pro ochranu osobních údajů.

## F. Případný záměr správce předat osobní údaje příjemci ve třetí zemi nebo mezinárodní organizaci a existence či neexistence rozhodnutí Komise o odpovídající ochraně nebo, v případech předání uvedených v článcích 46 nebo 47 nebo v čl. 49 odst. 1 druhém pododstavci, odkaz na vhodné záruky a prostředky k získání kopie těchto údajů nebo informace o tom, kde byly tyto údaje zpřístupněny (čl. 14 odst. 1 písm. F GDPR).

Mezi příjemce osobních údajů mohou patřit všechny společnosti a pobočky, které jsou součástí naší skupiny (dále jen "společnosti skupiny") a které mají místo podnikání nebo kancelář ve třetí zemi. Seznam všech společností skupiny si můžete vyžádat u nás.

Podle čl. 46 odst. 1 GDPR může správce nebo zpracovatel předat osobní údaje do třetí země pouze tehdy, pokud správce nebo zpracovatel poskytl vhodné záruky a pokud jsou k dispozici vymahatelná práva subjektu údajů a účinné právní prostředky nápravy pro subjekty údajů. Vhodné záruky lze poskytnout, aniž by bylo vyžadováno zvláštní povolení dozorového úřadu, prostřednictvím standardních doložek o ochraně údajů, čl. 46 odst. 2 písm. c) GDPR.

Se všemi příjemci ze třetích zemí jsou před prvním předáním osobních údajů dohodnuty standardní smluvní doložky Evropské unie nebo jiné vhodné záruky. V důsledku toho je zajištěno, že jsou zaručeny vhodné záruky, vymahatelná práva subjektů údajů a účinné právní prostředky nápravy pro subjekty údajů. Každý subjekt údajů u nás může získat kopii standardních smluvních doložek. Standardní smluvní doložky jsou rovněž k dispozici v Úředním věstníku Evropské unie.

Podle čl. 45 odst. 3 obecného nařízení o ochraně osobních údajů (GDPR) má Evropská komise právo rozhodnout prostřednictvím prováděcího aktu, že země mimo EU poskytuje odpovídající úroveň ochrany. To znamená úroveň ochrany osobních údajů, která je v zásadě rovnocenná úrovni ochrany v EU. Důsledkem rozhodnutí o odpovídající úrovni ochrany je, že osobní údaje mohou volně proudit z EU (a Norska, Lichtenštejnska a Islandu) do třetí země bez dalších překážek. Podobná pravidla platí ve Spojeném království, Švýcarsku a některých dalších zemích.

V případě, že Evropská komise nebo vláda jiné země rozhodne, že třetí země poskytuje odpovídající úroveň ochrany, a příslušný rámec (např. EU-U.S. Data Privacy Framework, Swiss-U.S. Data Privacy


© All rights reserved by Heiko Maniero.

Framework, UK Extension to the EU-U.S. Data Privacy Framework), veškerá naše předávání údajů členům těchto rámců (např. samostatně certifikovaným subjektům) jsou založena výhradně na členství těchto subjektů v příslušném rámci. V případě, že jsme my nebo některý ze subjektů naší skupiny členem takového rámce, jsou veškerá předání nám nebo subjektu naší skupiny založena výhradně na členství tohoto subjektu v takovém rámci.

Každý subjekt údajů u nás může získat kopii rámců. Kromě toho jsou rámce k dispozici také v Úředním věstníku Evropské unie nebo ve zveřejněných právních materiálech či na internetových stránkách dozorových úřadů nebo jiných příslušných orgánů či institucí.

## G. Doba, po kterou budou osobní údaje uloženy, nebo není-li ji možné určit, kritéria použitá pro stanovení této doby (čl. 14 odst. 2 písm. a) GDPR)

Kritériem pro určení doby uchovávání osobních údajů je příslušná zákonná doba uchovávání. Po uplynutí této doby jsou příslušné údaje běžně vymazávány, pokud již nejsou nezbytné pro plnění smlouvy nebo zahájení smlouvy.

Pokud neexistuje zákonná doba uchovávání, je kritériem smluvní nebo interní doba uchovávání.

## H. Oprávněné zájmy správce nebo třetí strany v případě, že je zpracování založeno na čl. 6 odst. 1 písm. f) (čl. 14 odst. 2 písm. b GDPR).

Podle čl. 6 odst. 1 písm. f) GDPR je zpracování zákonné pouze tehdy, pokud je zpracování nezbytné pro účely oprávněných zájmů správce nebo třetí strany, s výjimkou případů, kdy před těmito zájmy mají přednost zájmy nebo základní práva a svobody subjektu údajů, které vyžadují ochranu osobních údajů. Podle 47. bodu odůvodnění věty druhé obecného nařízení o ochraně osobních údajů by oprávněný zájem mohl existovat, pokud existuje relevantní a přiměřený vztah mezi subjektem údajů a správcem, např. v situacích, kdy je subjekt údajů klientem správce. Ve všech případech, kdy naše společnost zpracovává osobní údaje na základě čl. 6 odst. 1 písm. f) GDPR, je naším oprávněným zájmem vykonávání naší činnosti ve prospěch blaha všech našich zaměstnanců a akcionářů.

## I. Existence práva požadovat od správce přístup k osobním údajům týkajícím se subjektu údajů, jejich opravu nebo výmaz anebo omezení zpracování a práva vznést námitku proti zpracování, jakož i práva na přenositelnost údajů (čl. 14 odst. 2 písm. c) GDPR)

Všechny subjekty údajů mají následující práva:


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

***Právo na přístup***

Každý subjekt údajů má právo na přístup k osobním údajům, které se ho týkají. Právo na přístup se vztahuje na všechny údaje, které zpracováváme. Toto právo lze uplatnit snadno a v přiměřených intervalech, aby bylo možné se seznámit se zákonností zpracování a ověřit si ji (63. bod odůvodnění GDPR). Toto právo vyplývá z čl. 15 GDPR. Subjekt údajů nás může kontaktovat za účelem uplatnění práva na přístup.

***Právo na opravu***

Podle článku 16 věty 1 GDPR má subjekt údajů právo na to, aby správce bez zbytečného odkladu opravil nepřesné osobní údaje, které se ho týkají. Článek 16 věta 2 GDPR dále stanoví, že subjekt údajů má s ohledem na účely zpracování právo na doplnění neúplných osobních údajů, a to i prostřednictvím poskytnutí doplňujícího prohlášení. Subjekt údajů se na nás může obrátit, aby uplatnil právo na opravu.

***Právo na výmaz (právo být zapomenut)***

Kromě toho mají subjekty údajů právo na výmaz a právo být zapomenut podle čl. 17 GDPR. Toto právo lze rovněž uplatnit tak, že nás kontaktujete. Na tomto místě bychom však rádi upozornili, že toto právo neplatí, pokud je zpracování nezbytné pro splnění právní povinnosti, která se na naši společnost vztahuje, čl. 17 odst. 3 písm. b GDPR. To znamená, že žádost o výmaz můžeme schválit až po uplynutí zákonné doby uchovávání.

***Právo na omezení zpracování***

Podle článku 18 GDPR má každý subjekt údajů právo na omezení zpracování. Omezení zpracování lze požadovat, pokud je splněna jedna z podmínek uvedených v čl. 18 odst. 1 písm. a-d GDPR. Subjekt údajů nás může kontaktovat, aby uplatnil právo na omezení zpracování.

***Právo vznést námitku***

Kromě toho čl. 21 GDPR zaručuje právo vznést námitku. Subjekt údajů nás může kontaktovat, aby uplatnil právo na námitku.

***Právo na přenositelnost údajů***

Čl. 20 GDPR přiznává subjektu údajů právo na přenositelnost údajů. Podle tohoto ustanovení má subjekt údajů za podmínek stanovených v čl. 20 odst. 1 písm. a) a b) GDPR právo získat osobní údaje, které se ho týkají a které poskytl správci, ve strukturovaném, běžně používaném a strojově čitelném formátu a má právo předat tyto údaje jinému správci, aniž by tomu správce, kterému byly osobní údaje poskytnuty, bránil. Subjekt údajů nás může kontaktovat za účelem uplatnění práva na přenositelnost údajů.

## J. Pokud je zpracování založeno na čl. 6 odst. 1 písm. a) nebo čl. 9 odst. 2 písm. a), existence práva odvolat kdykoli souhlas, aniž je tím dotčena zákonnost zpracování založená na souhlasu uděleném před jeho odvoláním; (čl. 14 odst. 2 písm. d) GDPR).

Pokud je zpracování osobních údajů založeno na čl. 6 odst. 1 písm. a) GDPR, což je případ, kdy subjekt údajů udělil souhlas se zpracováním osobních údajů pro jeden nebo více konkrétních účelů, nebo je


© All rights reserved by Heiko Maniero.

založeno na čl. 9 odst. 2 písm. a) GDPR, který upravuje výslovný souhlas se zpracováním zvláštních kategorií osobních údajů, má subjekt údajů podle čl. 7 odst. 3 věty první GDPR právo svůj souhlas kdykoli odvolat.

Odvolání souhlasu nemá vliv na zákonnost zpracování založeného na souhlasu před jeho odvoláním, čl. 7 odst. 3 věta druhá GDPR. Odvolání souhlasu musí být stejně snadné jako jeho udělení, čl. 7 odst. 3 věta 4 GDPR. K odvolání souhlasu proto může dojít vždy stejným způsobem, jakým byl souhlas udělen, nebo jakýmkoli jiným způsobem, který subjekt údajů považuje za jednodušší. V dnešní informační společnosti je pravděpodobně nejjednodušším způsobem odvolání souhlasu prostý e-mail. Pokud si subjekt údajů přeje odvolat svůj souhlas, který nám udělil, stačí nám zaslat jednoduchý e-mail. Případně si subjekt údajů může zvolit jakýkoli jiný způsob, jak nám svůj souhlas odvolat.

## K. Existence práva podat stížnost u dozorového úřadu (čl. 14 odst. 2 písm. e), čl. 77 odst. 1 GDPR)

Jako správce jsme povinni informovat subjekt údajů o právu podat stížnost u dozorového úřadu, čl. 14 odst. 2 písm. e) GDPR. Právo podat stížnost u dozorového úřadu upravuje čl. 77 odst. 1 GDPR. Podle tohoto ustanovení, aniž jsou dotčeny jakékoli jiné správní nebo soudní prostředky nápravy, má každý subjekt údajů právo podat stížnost u dozorového úřadu, zejména v členském státě svého obvyklého bydliště, pracoviště nebo místa údajného porušení, pokud se subjekt údajů domnívá, že zpracování osobních údajů, které se ho týkají, porušuje obecné nařízení o ochraně osobních údajů. Právo podat stížnost u dozorového úřadu bylo právem Unie omezeno pouze tak, že jej lze uplatnit pouze u jediného dozorového úřadu (141. bod odůvodnění věta první obecného nařízení o ochraně osobních údajů). Toto pravidlo má zabránit dvojím stížnostem téhož subjektu údajů v téže věci. Pokud na nás chce subjekt údajů podat stížnost, požádali jsme ho proto, aby se obrátil pouze na jediný dozorový úřad.

## L. Zdroj, ze kterého osobní údaje pocházejí, a případně informace o tom, zda údaje pocházejí z veřejně dostupných zdrojů (čl. 14 odst. 2 písm. f) GDPR)

Osobní údaje se v zásadě shromažďují přímo od subjektu údajů nebo ve spolupráci s orgánem (např. vyhledáním údajů v úředním registru). Ostatní údaje o subjektech údajů jsou získávány z předávání údajů společností skupiny. V souvislosti s těmito obecnými informacemi je pojmenování přesných zdrojů, z nichž osobní údaje pocházejí, buď nemožné, nebo by vyžadovalo nepřiměřené úsilí ve smyslu čl. 14 odst. 5 písm. b) GDPR. Osobní údaje z veřejně přístupných zdrojů zásadně neshromažďujeme.

Každý subjekt údajů nás může kdykoli kontaktovat a získat podrobnější informace o přesných zdrojích osobních údajů, které se ho týkají. Pokud nelze subjektu údajů poskytnout informace o původu osobních údajů, protože byly použity různé zdroje, měly by být poskytnuty obecné informace (61. bod odůvodnění, 4. věta obecného nařízení o ochraně osobních údajů).


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

### M. Skutečnost, že dochází k automatizovanému rozhodování, včetně profilování, uvedenému v čl. 22 odst. 1 a 4, a přinejmenším v těchto případech smysluplné informace týkající se použitého postupu, jakož i významu a předpokládaných důsledků takového zpracování pro subjekt údajů. (čl. 14 odst. 2 písm. g) GDPR).

Jako odpovědná společnost obvykle nepoužíváme automatizované rozhodování ani profilování. Pokud ve výjimečných případech automatizované rozhodování nebo profilování provádíme, informujeme o tom subjekt údajů buď samostatně, nebo prostřednictvím pododdílu v našich zásadách ochrany osobních údajů (na našich webových stránkách). V takovém případě platí následující:

K automatizovanému rozhodování - včetně profilování - může dojít, pokud (1) je to nezbytné pro uzavření nebo plnění smlouvy mezi subjektem údajů a námi, nebo (2) je to povoleno právem Unie nebo členského státu, které se na nás vztahuje a které rovněž stanoví vhodná opatření na ochranu práv a svobod a oprávněných zájmů subjektu údajů, nebo (3) je to založeno na výslovném souhlasu subjektu údajů.

V případech uvedených v čl. 22 odst. 2 písm. a) a c) GDPR provedeme vhodná opatření na ochranu práv a svobod a oprávněných zájmů subjektu údajů. V těchto případech máte právo na lidský zásah ze strany správce, na vyjádření svého názoru a na napadení rozhodnutí.

Smysluplné informace o příslušné logice, jakož i o významu a předpokládaných důsledcích takového zpracování pro subjekt údajů jsou uvedeny v našich zásadách ochrany osobních údajů.

## III. EU-U.S. Data Privacy Framework (EU-U.S. DPF), UK Extension to the EU-U.S. DPF, Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF)

Pokud je naše organizace certifikovaným členem EU-U.S. Data Privacy Framework (EU-U.S. DPF) a/nebo UK Extension to the EU-U.S. DPF a/nebo Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF), platí následující:

Dodržujeme EU-U.S. Data Privacy Framework (EU-U.S. DPF) a UK Extension to the EU-U.S. DPF i Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF), jak bylo stanoveno U.S. Department of Commerce. Naše společnost potvrdila Ministerstvu obchodu USA, že dodržuje EU-U.S. Data Privacy Framework Principles (EU-U.S. DPF Principles) týkající se zpracování osobních údajů, které obdrží z Evropské unie a Spojeného království na základě EU-U.S. DPF a UK Extension to the EU-U.S. DPF. Naše společnost potvrdila Ministerstvu obchodu USA, že dodržuje Swiss-U.S. Data Privacy Framework Principles (Swiss-U.S. DPF Principles) týkající se zpracování osobních údajů, které obdrží ze Švýcarska na základě Swiss-U.S. DPF. V případě rozporu mezi ustanoveními našeho prohlášení o ochraně osobních údajů a EU-U.S. DPF Principles a/nebo Swiss-U.S. DPF Principles, jsou závazné Principles.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

Pro více informací o programu Data Privacy Framework (DPF) a pro zobrazení našeho certifikátu navštivte prosím https://www.dataprivacyframework.gov/.

Ostatní americké jednotky nebo dceřiné společnosti naší společnosti, které také dodržují EU-U.S. DPF Principles, včetně UK Extension to the EU-U.S. DPF a Swiss-U.S. DPF Principles, jsou uvedeny v našem prohlášení o ochraně osobních údajů.

V souladu s EU-U.S. DPF a UK Extension to the EU-U.S. DPF a Swiss-U.S. DPF se naše společnost zavazuje spolupracovat s orgány zřízenými evropskými orgány na ochranu údajů a britským Information Commissioner's Office (ICO) a švýcarským Federal Data Protection and Information Commissioner (EDÖB) a dodržovat jejich rady týkající se nevyřešených stížností na naše zacházení s osobními údaji, které jsme obdrželi na základě EU-U.S. DPF, UK Extension to the EU-U.S. DPF a Swiss-U.S. DPF.

Informujeme dotčené osoby o příslušných evropských orgánech na ochranu osobních údajů, které jsou odpovědné za vyřizování stížností na zacházení naší organizace s osobními údaji, v horní části tohoto dokumentu transparentnosti a také o tom, že dotčeným osobám poskytujeme přiměřené a bezplatné právní prostředky.

Informujeme všechny dotčené osoby, že naše společnost podléhá vyšetřovacím a výkonným pravomocím Federal Trade Commission (FTC).

Dotčené osoby mají za určitých podmínek možnost požádat o závazné rozhodčí řízení. Naše organizace je povinna řešit nároky a dodržovat podmínky podle přílohy I DPF-Principals, pokud dotčená osoba požádala o závazné rozhodčí řízení tím, že o tom informovala naši organizaci a dodržela postupy a podmínky podle přílohy I Principles.

Tímto informujeme všechny dotčené osoby o odpovědnosti naší organizace v případě předání osobních údajů třetím stranám.

Pro dotazy dotčených osob nebo orgánů na ochranu osobních údajů jsme jmenovali místní zástupce uvedené výše v tomto dokumentu transparentnosti.

Nabízíme vám možnost volby (Opt-out), zda vaše osobní údaje (i) budou předány třetím stranám, nebo (ii) budou použity pro účel, který se podstatně liší od účelu (účelů), pro který (které) byly původně shromážděny nebo později vámi schváleny. Jednoznačný, dobře viditelný a snadno dostupný mechanismus pro uplatnění vašeho práva volby spočívá v kontaktování našeho pověřence pro ochranu osobních údajů (DSB) prostřednictvím e-mailu. Nemáte žádnou volbu a my také nejsme povinni to dělat, pokud jsou údaje předány třetí straně, která jedná jako náš zástupce nebo zpracovatel údajů naším jménem a podle našich pokynů. Nicméně, s takovým zástupcem nebo zpracovatelem údajů vždy uzavíráme smlouvu.

Pro citlivé údaje (tj. osobní údaje, které obsahují informace o zdravotním stavu, rasovém nebo etnickém původu, politických názorech, náboženských nebo filozofických přesvědčeních, členství v odborech nebo informace o sexuálním životě dotyčné osoby) získáváme váš výslovný souhlas (Opt-in), pokud tyto údaje


© All rights reserved by Heiko Maniero.

(i) budou předány třetím stranám, nebo (ii) budou použity pro jiný účel, než pro který byly původně shromážděny nebo pro který jste později udělili svůj souhlas, tím, že jste učinili svou volbu Opt-in. Kromě toho, všechny osobní údaje, které obdržíme od třetích stran, považujeme za citlivé, pokud je třetí strana identifikuje a zpracovává jako citlivé.

Tímto vás informujeme o nutnosti zveřejnění osobních údajů v reakci na zákonné požadavky orgánů, včetně splnění požadavků národní bezpečnosti nebo prosazování práva.

Při předávání osobních údajů třetí straně, která jedná jako správce, dodržujeme Principy oznámení a volby. Rovněž uzavíráme smlouvu s třetí stranou odpovědnou za zpracování, která stanoví, že tyto údaje mohou být zpracovány pouze pro omezené a určené účely v souladu s vaším poskytnutým souhlasem a že příjemce poskytuje stejnou úroveň ochrany jako Principy DPF a nás informuje, pokud zjistí, že již nemůže tuto povinnost plnit. Smlouva stanoví, že třetí strana, která jedná jako správce, zastaví zpracování nebo přijme jiné vhodné a přiměřené opatření k nápravě, pokud je taková situace zjištěna.

Při předávání osobních údajů třetí straně, která jedná jako agent nebo zpracovatel údajů, (i) předáváme tyto údaje pouze pro omezené a určené účely; (ii) ujistíme se, že agent nebo zpracovatel údajů se zavázal zajistit alespoň stejnou úroveň ochrany údajů, jakou požadují DPF-Principals; (iii) přijmeme vhodná a přiměřená opatření k zajištění toho, že agent nebo zpracovatel údajů skutečně zpracovává předané osobní údaje způsobem, který je v souladu s našimi závazky podle DPF-Principals; (iv) požadujeme od agenta nebo zpracovatele údajů, aby informoval naši organizaci, pokud zjistí, že již nemůže plnit svou povinnost zajistit stejnou úroveň ochrany, jakou požadují DPF-Principals; (v) po oznámení, včetně oznámení podle bodu (iv), přijmeme vhodná a přiměřená opatření k zastavení neoprávněného zpracování a k nápravě; a (vi) na žádost poskytneme DPF Department shrnutí nebo reprezentativní kopii příslušných ustanovení o ochraně údajů ve smlouvě s tímto agentem.

V souladu s EU-U.S. DPF a/nebo UK Extension to the EU-U.S. DPF a/nebo Swiss-U.S. DPF se naše organizace zavazuje spolupracovat s orgány zřízenými evropskými orgány na ochranu údajů a britským Information Commissioner's Office (ICO) a švýcarským Federal Data Protection and Information Commissioner (EDÖB) a dodržovat jejich rady týkající se nevyřešených stížností na naše zacházení s osobními údaji v souvislosti s pracovním vztahem, které jsme obdrželi na základě EU-U.S. DPF, UK Extension to the EU-U.S. DPF a Swiss-U.S. DPF.

Všechny subjekty údajů, které se dočasně nacházejí v Evropské unii (EU), Evropském hospodářském prostoru (EHP) nebo ve Spojeném království, nebo které tam mají bydliště či obvyklý pobyt, mají nárok na práva a práva subjektu údajů, která jsou zveřejněna v našem dokumentu o transparentnosti a která rovněž vyplývají z článků 15 až 22 GDPR, včetně práva na přístup k osobním údajům. Tyto informace jsme zpřístupnili ve všech jazycích EU a EHP. Anglická verze platí pro Spojené království.

Všechny subjekty údajů, které mají ve Švýcarsku dočasný pobyt nebo tam mají bydliště či obvyklý pobyt, mají podle švýcarského zákona o ochraně osobních údajů (DPA) a švýcarského nařízení o ochraně osobních údajů (DPR) práva a nároky subjektu údajů, které jsou zveřejněny v našem dokumentu o


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

transparentnosti, včetně práva na přístup k osobním údajům. Tyto informace jsme poskytli ve třech úředních jazycích Švýcarska (němčině, italštině a francouzštině).


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

# CZECH: Informace o zpracování osobních údajů zaměstnanců a uchazečů (článek 13, 14 GDPR)

Vážený pane nebo paní,

Osobní údaje zaměstnanců a uchazečů si zaslouží zvláštní ochranu. Naším cílem je udržovat úroveň ochrany osobních údajů na vysoké úrovni. Proto běžně rozvíjíme naše koncepce ochrany a zabezpečení údajů.

Samozřejmě dodržujeme zákonná ustanovení o ochraně osobních údajů. Podle článků 13, 14 GDPR splňují správci při zpracování osobních údajů zvláštní informační požadavky. Tento dokument tyto povinnosti splňuje.

Terminologie právní úpravy je složitá. Při přípravě tohoto dokumentu se bohužel nebylo možné obejít bez používání právních termínů. Proto bychom vás rádi upozornili, že se na nás můžete kdykoli obrátit se všemi dotazy týkajícími se tohoto dokumentu, použitých pojmů nebo formulací.

## I. Informace poskytované v případě, že osobní údaje jsou získány od subjektu údajů (článek 13 GDPR).

### A. Totožnost a kontaktní údaje správce a jeho případného zástupce (čl. 13 odst. 1 písm. a) GDPR)

Viz výše

### B. Případně kontaktní údaje případného pověřence pro ochranu osobních údajů (čl. 13 odst. 1 písm. b) GDPR)

Viz výše

### C. účely zpracování, pro které jsou osobní údaje určeny, a právní základ pro zpracování (čl. 13 odst. 1 písm. c) GDPR)

V případě údajů uchazeče je účelem zpracování údajů posouzení žádosti během náborového procesu. Za tímto účelem zpracováváme všechny vámi poskytnuté údaje. Na základě údajů poskytnutých v průběhu náborového řízení ověříme, zda jste pozváni na pracovní pohovor (součást výběrového řízení). V případě obecně vhodných uchazečů, zejména v rámci pracovního pohovoru, zpracováváme některé


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

další vámi poskytnuté osobní údaje, které jsou nezbytné pro naše rozhodnutí o výběru. Pokud vás přijmeme, údaje uchazeče se automaticky změní na údaje zaměstnance. V rámci výběrového řízení budeme zpracovávat i další vaše osobní údaje, které si od vás vyžádáme a které jsou nezbytné pro zahájení nebo plnění smlouvy (např. osobní identifikační čísla nebo daňová čísla). V případě údajů o zaměstnancích je účelem zpracování údajů plnění pracovní smlouvy nebo dodržování jiných právních předpisů vztahujících se na pracovní poměr (např. daňových předpisů), jakož i využití vašich osobních údajů k plnění pracovní smlouvy uzavřené s vámi (např. zveřejnění vašeho jména a kontaktních údajů v rámci společnosti nebo zákazníkům). Údaje zaměstnanců jsou uchovávány i po skončení pracovního poměru, aby byly splněny zákonné lhůty pro jejich uchovávání.

Právním základem pro zpracování údajů je čl.6 odst.1 písm.b GDPR, čl.9 odst.2 písm.b a h GDPR, čl.88 odst.1 GDPR a vnitrostátní právní předpisy, např. v Německu § 26 BDSG (Spolkový zákon o ochraně osobních údajů).

## D. Případné příjemce nebo kategorie příjemců osobních údajů (čl. 13 odst. 1 písm. e) GDPR)

Orgány veřejné správy

Externí subjekty

Další externí subjekty

Interní zpracování

Zpracování v rámci skupiny

Ostatní subjekty

Seznam našich zpracovatelů a příjemců údajů ve třetích zemích a případně mezinárodních organizací je zveřejněn na našich webových stránkách nebo si jej můžete u nás bezplatně vyžádat. Pro vyžádání tohoto seznamu se prosím obraťte na našeho pověřence pro ochranu osobních údajů.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## E. Případný úmysl správce předat osobní údaje do třetí země nebo mezinárodní organizaci a existenci či neexistenci rozhodnutí Komise o odpovídající ochraně nebo, v případech předání uvedených v článcích 46 nebo 47 nebo čl. 49 odst. 1 druhém pododstavci, odkaz na vhodné záruky a prostředky k získání kopie těchto údajů nebo informace o tom, kde byly tyto údaje zpřístupněny (čl. 13 odst. 1 písm. f, čl. 46 odst. 1, čl. 46 odst. 2 písm. c GDPR).

Mezi příjemce osobních údajů mohou patřit všechny společnosti a pobočky, které jsou součástí naší skupiny (dále jen "společnosti skupiny") a které mají místo podnikání nebo kancelář ve třetí zemi. Seznam všech společností skupiny nebo příjemců si můžete vyžádat u nás.

Podle čl. 46 odst. 1 GDPR může správce nebo zpracovatel předat osobní údaje do třetí země pouze tehdy, pokud správce nebo zpracovatel poskytl vhodné záruky a pokud jsou k dispozici vymahatelná práva subjektu údajů a účinné právní prostředky nápravy pro subjekty údajů. Vhodné záruky lze poskytnout, aniž by bylo vyžadováno zvláštní povolení dozorového úřadu, prostřednictvím standardních smluvních doložek, čl. 46 odst. 2 písm. c) GDPR.

Se všemi příjemci ze třetích zemí jsou před prvním předáním osobních údajů dohodnuty standardní smluvní doložky Evropské unie nebo jiné vhodné záruky. V důsledku toho je zajištěno, že jsou zaručeny vhodné záruky, vymahatelná práva subjektů údajů a účinné právní prostředky nápravy pro subjekty údajů. Každý subjekt údajů u nás může získat kopii standardních smluvních doložek. Standardní smluvní doložky jsou rovněž k dispozici v Úředním věstníku Evropské unie.

Podle čl. 45 odst. 3 obecného nařízení o ochraně osobních údajů (GDPR) má Evropská komise právo rozhodnout prostřednictvím prováděcího aktu, že země mimo EU poskytuje odpovídající úroveň ochrany. To znamená úroveň ochrany osobních údajů, která je v zásadě rovnocenná úrovni ochrany v EU. Důsledkem rozhodnutí o odpovídající úrovni ochrany je, že osobní údaje mohou volně proudit z EU (a Norska, Lichtenštejnska a Islandu) do třetí země bez dalších překážek. Podobná pravidla platí ve Spojeném království, Švýcarsku a některých dalších zemích.

V případě, že Evropská komise nebo vláda jiné země rozhodne, že třetí země poskytuje odpovídající úroveň ochrany, a příslušný rámec (např. EU-U.S. Data Privacy Framework, Swiss-U.S. Data Privacy Framework, UK Extension to the EU-U.S. Data Privacy Framework), veškerá naše předávání údajů členům těchto rámců (např. samostatně certifikovaným subjektům) jsou založena výhradně na členství těchto subjektů v příslušném rámci. V případě, že jsme my nebo některý ze subjektů naší skupiny členem takového rámce, jsou veškerá předání nám nebo subjektu naší skupiny založena výhradně na členství tohoto subjektu v takovém rámci.

Každý subjekt údajů u nás může získat kopii rámců. Kromě toho jsou rámce k dispozici také v Úředním věstníku Evropské unie nebo ve zveřejněných právních materiálech či na internetových stránkách dozorových úřadů nebo jiných příslušných orgánů či institucí.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## F. Doba, po kterou budou osobní údaje uloženy, nebo není-li ji možné určit, kritéria použitá pro stanovení této doby (čl. 13 odst. 2 písm. a) GDPR)

Doba uchovávání osobních údajů žadatelů je 6 měsíců. Pro údaje zaměstnanců platí příslušná zákonná doba uchovávání. Po uplynutí této doby jsou příslušné údaje běžně vymazávány, pokud již nejsou nezbytné pro plnění smlouvy nebo zahájení smlouvy.

## G. Existence práva požadovat od správce přístup k osobním údajům týkajícím se subjektu údajů, jejich opravu nebo výmaz, popřípadě omezení zpracování, a vznést námitku proti zpracování, jakož i práva na přenositelnost údajů (čl. 13 odst. 2 písm. b) GDPR).

Všechny subjekty údajů mají následující práva:

***Právo na přístup***

Každý subjekt údajů má právo na přístup k osobním údajům, které se ho týkají. Právo na přístup se vztahuje na všechny údaje, které zpracováváme. Toto právo lze uplatnit snadno a v přiměřených intervalech, aby bylo možné se seznámit se zákonností zpracování a ověřit si ji (63. bod odůvodnění GDPR). Toto právo vyplývá z čl. 15 GDPR. Subjekt údajů nás může kontaktovat za účelem uplatnění práva na přístup.

***Právo na opravu***

Podle článku 16 věty 1 GDPR má subjekt údajů právo na to, aby správce bez zbytečného odkladu opravil nepřesné osobní údaje, které se ho týkají. Článek 16 věta 2 GDPR dále stanoví, že subjekt údajů má s ohledem na účely zpracování právo na doplnění neúplných osobních údajů, a to i prostřednictvím poskytnutí doplňujícího prohlášení. Subjekt údajů se na nás může obrátit, aby uplatnil právo na opravu.

***Právo na výmaz (právo být zapomenut)***

Kromě toho mají subjekty údajů právo na výmaz a právo být zapomenut podle čl. 17 GDPR. Toto právo lze rovněž uplatnit tak, že nás kontaktujete. Na tomto místě bychom však rádi upozornili, že toto právo neplatí, pokud je zpracování nezbytné pro splnění právní povinnosti, která se na naši společnost vztahuje, čl. 17 odst. 3 písm. b GDPR. To znamená, že žádost o výmaz můžeme schválit až po uplynutí zákonné doby uchovávání.

***Právo na omezení zpracování***

Podle článku 18 GDPR má každý subjekt údajů právo na omezení zpracování. Omezení zpracování lze požadovat, pokud je splněna jedna z podmínek uvedených v čl. 18 odst. 1 písm. a-d GDPR. Subjekt údajů nás může kontaktovat, aby uplatnil právo na omezení zpracování.

***Právo vznést námitku***

Kromě toho čl. 21 GDPR zaručuje právo vznést námitku. Subjekt údajů nás může kontaktovat, aby uplatnil právo na námitku.


© All rights reserved by Heiko Maniero.

***Právo na přenositelnost údajů***

Čl. 20 GDPR přiznává subjektu údajů právo na přenositelnost údajů. Podle tohoto ustanovení má subjekt údajů za podmínek stanovených v čl. 20 odst. 1 písm. a) a b) GDPR právo získat osobní údaje, které se ho týkají a které poskytl správci, ve strukturovaném, běžně používaném a strojově čitelném formátu a má právo předat tyto údaje jinému správci, aniž by tomu správce, kterému byly osobní údaje poskytnuty, bránil. Subjekt údajů nás může kontaktovat za účelem uplatnění práva na přenositelnost údajů.

## H. Pokud je zpracování založeno na čl. 6 odst. 1 písm. a) nebo čl. 9 odst. 2 písm. a), existence práva odvolat kdykoli souhlas, aniž je tím dotčena zákonnost zpracování založená na souhlasu uděleném před jeho odvoláním (čl. 13 odst. 2 písm. c) GDPR).

Pokud je zpracování osobních údajů založeno na čl. 6 odst. 1 písm. a) GDPR, což je případ, kdy subjekt údajů udělil souhlas se zpracováním osobních údajů pro jeden nebo více konkrétních účelů, nebo je založeno na čl. 9 odst. 2 písm. a) GDPR, který upravuje výslovný souhlas se zpracováním zvláštních kategorií osobních údajů, má subjekt údajů podle čl. 7 odst. 3 věty první GDPR právo svůj souhlas kdykoli odvolat.

Odvolání souhlasu nemá vliv na zákonnost zpracování založeného na souhlasu před jeho odvoláním, čl. 7 odst. 3 věta druhá GDPR. Odvolání souhlasu musí být stejně snadné jako jeho udělení, čl. 7 odst. 3 věta 4 GDPR. K odvolání souhlasu proto může dojít vždy stejným způsobem, jakým byl souhlas udělen, nebo jakýmkoli jiným způsobem, který subjekt údajů považuje za jednodušší. V dnešní informační společnosti je pravděpodobně nejjednodušším způsobem odvolání souhlasu prostý e-mail. Pokud si subjekt údajů přeje odvolat svůj souhlas, který nám udělil, stačí nám zaslat jednoduchý e-mail. Případně si subjekt údajů může zvolit jakýkoli jiný způsob, jak nám svůj souhlas odvolat.

## I. Existence práva podat stížnost u dozorového úřadu (čl. 13 odst. 2 písm. d), čl. 77 odst. 1 GDPR)

Jako správce jsme povinni informovat subjekt údajů o právu podat stížnost u dozorového úřadu, čl. 13 odst. 2 písm. d) GDPR. Právo podat stížnost u dozorového úřadu upravuje čl. 77 odst. 1 GDPR. Podle tohoto ustanovení, aniž jsou dotčeny jakékoli jiné správní nebo soudní prostředky nápravy, má každý subjekt údajů právo podat stížnost u dozorového úřadu, zejména v členském státě svého obvyklého bydliště, pracoviště nebo místa údajného porušení, pokud se subjekt údajů domnívá, že zpracování osobních údajů, které se ho týkají, porušuje obecné nařízení o ochraně osobních údajů. Právo podat stížnost u dozorového úřadu bylo právem Unie omezeno pouze tak, že jej lze uplatnit pouze u jediného dozorového úřadu (141. bod odůvodnění věta první obecného nařízení o ochraně osobních údajů). Toto pravidlo má zabránit dvojím stížnostem téhož subjektu údajů v téže věci. Pokud na nás chce subjekt údajů podat stížnost, požádali jsme ho proto, aby se obrátil pouze na jediný dozorový úřad.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## J. Skutečnost, zda poskytování osobních údajů je zákonným či smluvním požadavkem, nebo požadavkem, který je nutné uvést do smlouvy, a zda má subjekt údajů povinnost osobní údaje poskytnout, a ohledně možných důsledků neposkytnutí těchto údajů (čl. 13 odst. 2 písm. e) GDPR)

Upřesňujeme, že poskytnutí osobních údajů je částečně vyžadováno zákonem (např. daňovými předpisy) nebo může vyplývat také ze smluvních ustanovení (např. informace o smluvním partnerovi).

Někdy může být pro uzavření smlouvy nezbytné, aby nám subjekt údajů poskytl osobní údaje, které musíme následně zpracovat. Subjekt údajů je například povinen poskytnout nám osobní údaje, když s ním naše společnost uzavře smlouvu. Neposkytnutí osobních údajů by mělo za následek, že by smlouva se subjektem údajů nemohla být uzavřena.

Před poskytnutím osobních údajů subjektem údajů nás musí subjekt údajů kontaktovat. Subjektu údajů objasníme, zda je poskytnutí osobních údajů vyžadováno zákonem nebo smlouvou nebo zda je nezbytné pro uzavření smlouvy, zda existuje povinnost osobní údaje poskytnout a jaké jsou důsledky neposkytnutí osobních údajů.

## K. Skutečnost, že dochází k automatizovanému rozhodování, včetně profilování, uvedenému v čl. 22 odst. 1 a 4, a přinejmenším v těchto případech smysluplné informace týkající se použitého postupu, jakož i významu a předpokládaných důsledků takového zpracování pro subjekt údajů (čl. 13 odst. 2 písm. f) GDPR).

Jako odpovědná společnost obvykle nepoužíváme automatizované rozhodování ani profilování. Pokud ve výjimečných případech automatizované rozhodování nebo profilování provádíme, informujeme o tom subjekt údajů buď samostatně, nebo prostřednictvím pododdílu v našich zásadách ochrany osobních údajů (na našich webových stránkách). V takovém případě platí následující:

K automatizovanému rozhodování - včetně profilování - může dojít, pokud (1) je to nezbytné pro uzavření nebo plnění smlouvy mezi subjektem údajů a námi, nebo (2) je to povoleno právem Unie nebo členského státu, které se na nás vztahuje a které rovněž stanoví vhodná opatření na ochranu práv a svobod a oprávněných zájmů subjektu údajů, nebo (3) je to založeno na výslovném souhlasu subjektu údajů.

V případech uvedených v čl. 22 odst. 2 písm. a) a c) GDPR provedeme vhodná opatření na ochranu práv a svobod a oprávněných zájmů subjektu údajů. V těchto případech máte právo na lidský zásah ze strany správce, na vyjádření svého názoru a na napadení rozhodnutí.

Smysluplné informace o příslušné logice, jakož i o významu a předpokládaných důsledcích takového zpracování pro subjekt údajů jsou uvedeny v našich zásadách ochrany osobních údajů.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## II. Informace poskytované v případě, že osobní údaje nebyly získány od subjektu údajů (článek 14 GDPR)

### A. Totožnost a kontaktní údaje správce a případně jeho zástupce (čl. 14 odst. 1 písm. a) GDPR)

Viz výše

### B. Případně kontaktní údaje případného pověřence pro ochranu osobních údajů (čl. 14 odst. 1 písm. b) GDPR)

Viz výše

### C. účely zpracování, pro které jsou osobní údaje určeny, a právní základ pro zpracování (čl. 14 odst. 1 písm. c) GDPR)

V případě údajů uchazeče, které nebyly získány od subjektu údajů, je účelem zpracování údajů posouzení žádosti během náborového procesu. Za tímto účelem můžeme zpracovávat údaje, které nebyly shromážděny od vás. Na základě údajů zpracovávaných v průběhu náborového procesu ověříme, zda jste pozváni na pracovní pohovor (součást výběrového řízení). Pokud vás přijmeme, údaje uchazeče se automaticky převedou na údaje zaměstnance. V případě údajů zaměstnanců je účelem zpracování údajů plnění pracovní smlouvy nebo dodržování jiných právních předpisů vztahujících se na pracovní poměr. Údaje zaměstnanců jsou uchovávány i po skončení pracovního poměru, aby byly splněny zákonné lhůty pro uchovávání údajů.

Právním základem pro zpracování údajů je čl.6 odst.1 písm.b) a f) GDPR, čl.9 odst.2 písm.b) a h) GDPR, čl.88 odst.1 GDPR a vnitrostátní právní předpisy, např. v Německu § 26 BDSG (Spolkový zákon o ochraně osobních údajů).

### D. Kategorie dotčených osobních údajů (čl. 14 odst. 1 písm. d) GDPR)

Údaje žadatele

Údaje o zaměstnancích


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## E. Případné příjemce nebo kategorie příjemců osobních údajů (čl. 14 odst. 1 písm. e) GDPR)

Orgány veřejné správy

Externí subjekty

Další externí subjekty

Interní zpracování

Zpracování v rámci skupiny

Ostatní subjekty

Seznam našich zpracovatelů a příjemců údajů ve třetích zemích a případně mezinárodních organizací je zveřejněn na našich webových stránkách nebo si jej můžete u nás bezplatně vyžádat. Pro vyžádání tohoto seznamu se prosím obraťte na našeho pověřence pro ochranu osobních údajů.

## F. Případný záměr správce předat osobní údaje příjemci ve třetí zemi nebo mezinárodní organizaci a existence či neexistence rozhodnutí Komise o odpovídající ochraně nebo, v případech předání uvedených v článcích 46 nebo 47 nebo v čl. 49 odst. 1 druhém pododstavci, odkaz na vhodné záruky a prostředky k získání kopie těchto údajů nebo informace o tom, kde byly tyto údaje zpřístupněny (čl. 14 odst. 1 písm. F GDPR).

Mezi příjemce osobních údajů mohou patřit všechny společnosti a pobočky, které jsou součástí naší skupiny (dále jen "společnosti skupiny") a které mají místo podnikání nebo kancelář ve třetí zemi. Seznam všech společností skupiny nebo příjemců si můžete vyžádat u nás.

Podle čl. 46 odst. 1 GDPR může správce nebo zpracovatel předat osobní údaje do třetí země pouze tehdy, pokud správce nebo zpracovatel poskytl vhodné záruky a pokud jsou k dispozici vymahatelná práva subjektu údajů a účinné právní prostředky nápravy pro subjekty údajů. Vhodné záruky lze poskytnout, aniž by bylo vyžadováno zvláštní povolení dozorového úřadu, prostřednictvím standardních doložek o ochraně údajů, čl. 46 odst. 2 písm. c) GDPR.

Se všemi příjemci ze třetích zemí jsou před prvním předáním osobních údajů dohodnuty standardní smluvní doložky Evropské unie nebo jiné vhodné záruky. V důsledku toho je zajištěno, že jsou zaručeny vhodné záruky, vymahatelná práva subjektů údajů a účinné právní prostředky nápravy pro subjekty údajů. Každý subjekt údajů u nás může získat kopii standardních smluvních doložek. Standardní smluvní doložky jsou rovněž k dispozici v Úředním věstníku Evropské unie.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

Podle čl. 45 odst. 3 obecného nařízení o ochraně osobních údajů (GDPR) má Evropská komise právo rozhodnout prostřednictvím prováděcího aktu, že země mimo EU poskytuje odpovídající úroveň ochrany. To znamená úroveň ochrany osobních údajů, která je v zásadě rovnocenná úrovni ochrany v EU. Důsledkem rozhodnutí o odpovídající úrovni ochrany je, že osobní údaje mohou volně proudit z EU (a Norska, Lichtenštejnska a Islandu) do třetí země bez dalších překážek. Podobná pravidla platí ve Spojeném království, Švýcarsku a některých dalších zemích.

V případě, že Evropská komise nebo vláda jiné země rozhodne, že třetí země poskytuje odpovídající úroveň ochrany, a příslušný rámec (např. EU-U.S. Data Privacy Framework, Swiss-U.S. Data Privacy Framework, UK Extension to the EU-U.S. Data Privacy Framework), veškerá naše předávání údajů členům těchto rámců (např. samostatně certifikovaným subjektům) jsou založena výhradně na členství těchto subjektů v příslušném rámci. V případě, že jsme my nebo některý ze subjektů naší skupiny členem takového rámce, jsou veškerá předání nám nebo subjektu naší skupiny založena výhradně na členství tohoto subjektu v takovém rámci.

Každý subjekt údajů u nás může získat kopii rámců. Kromě toho jsou rámce k dispozici také v Úředním věstníku Evropské unie nebo ve zveřejněných právních materiálech či na internetových stránkách dozorových úřadů nebo jiných příslušných orgánů či institucí.

## G. Doba, po kterou budou osobní údaje uloženy, nebo není-li ji možné určit, kritéria použitá pro stanovení této doby (čl. 14 odst. 2 písm. a) GDPR)

Doba uchovávání osobních údajů žadatelů je 6 měsíců. Pro údaje zaměstnanců platí příslušná zákonná doba uchovávání. Po uplynutí této doby jsou příslušné údaje běžně vymazávány, pokud již nejsou nezbytné pro plnění smlouvy nebo zahájení smlouvy.

## H. Oprávněné zájmy správce nebo třetí strany v případě, že je zpracování založeno na čl. 6 odst. 1 písm. f) (čl. 14 odst. 2 písm. b GDPR).

Podle čl. 6 odst. 1 písm. f) GDPR je zpracování zákonné pouze tehdy, pokud je zpracování nezbytné pro účely oprávněných zájmů správce nebo třetí strany, s výjimkou případů, kdy před těmito zájmy mají přednost zájmy nebo základní práva a svobody subjektu údajů, které vyžadují ochranu osobních údajů. Podle 47. bodu odůvodnění věty druhé obecného nařízení o ochraně osobních údajů by oprávněný zájem mohl existovat, pokud existuje relevantní a přiměřený vztah mezi subjektem údajů a správcem, např. v situacích, kdy je subjekt údajů klientem správce. Ve všech případech, kdy naše společnost zpracovává údaje uchazečů na základě čl. 6 odst. 1 písm. f GDPR, je naším oprávněným zájmem zaměstnávání vhodných pracovníků a odborníků.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## I. Existence práva požadovat od správce přístup k osobním údajům týkajícím se subjektu údajů, jejich opravu nebo výmaz anebo omezení zpracování a práva vznést námitku proti zpracování, jakož i práva na přenositelnost údajů (čl. 14 odst. 2 písm. c) GDPR)

Všechny subjekty údajů mají následující práva:

***Právo na přístup***

Každý subjekt údajů má právo na přístup k osobním údajům, které se ho týkají. Právo na přístup se vztahuje na všechny údaje, které zpracováváme. Toto právo lze uplatnit snadno a v přiměřených intervalech, aby bylo možné se seznámit se zákonností zpracování a ověřit si ji (63. bod odůvodnění GDPR). Toto právo vyplývá z čl. 15 GDPR. Subjekt údajů nás může kontaktovat za účelem uplatnění práva na přístup.

***Právo na opravu***

Podle článku 16 věty 1 GDPR má subjekt údajů právo na to, aby správce bez zbytečného odkladu opravil nepřesné osobní údaje, které se ho týkají. Článek 16 věta 2 GDPR dále stanoví, že subjekt údajů má s ohledem na účely zpracování právo na doplnění neúplných osobních údajů, a to i prostřednictvím poskytnutí doplňujícího prohlášení. Subjekt údajů se na nás může obrátit, aby uplatnil právo na opravu.

***Právo na výmaz (právo být zapomenut)***

Kromě toho mají subjekty údajů právo na výmaz a právo být zapomenut podle čl. 17 GDPR. Toto právo lze rovněž uplatnit tak, že nás kontaktujete. Na tomto místě bychom však rádi upozornili, že toto právo neplatí, pokud je zpracování nezbytné pro splnění právní povinnosti, která se na naši společnost vztahuje, čl. 17 odst. 3 písm. b GDPR. To znamená, že žádost o výmaz můžeme schválit až po uplynutí zákonné doby uchovávání.

***Právo na omezení zpracování***

Podle článku 18 GDPR má každý subjekt údajů právo na omezení zpracování. Omezení zpracování lze požadovat, pokud je splněna jedna z podmínek uvedených v čl. 18 odst. 1 písm. a-d GDPR. Subjekt údajů nás může kontaktovat, aby uplatnil právo na omezení zpracování.

***Právo vznést námitku***

Kromě toho čl. 21 GDPR zaručuje právo vznést námitku. Subjekt údajů nás může kontaktovat, aby uplatnil právo na námitku.

***Právo na přenositelnost údajů***

Čl. 20 GDPR přiznává subjektu údajů právo na přenositelnost údajů. Podle tohoto ustanovení má subjekt údajů za podmínek stanovených v čl. 20 odst. 1 písm. a) a b) GDPR právo získat osobní údaje, které se ho týkají a které poskytl správci, ve strukturovaném, běžně používaném a strojově čitelném formátu a má právo předat tyto údaje jinému správci, aniž by tomu správce, kterému byly osobní údaje poskytnuty, bránil. Subjekt údajů nás může kontaktovat za účelem uplatnění práva na přenositelnost údajů.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## J. Pokud je zpracování založeno na čl. 6 odst. 1 písm. a) nebo čl. 9 odst. 2 písm. a), existence práva odvolat kdykoli souhlas, aniž je tím dotčena zákonnost zpracování založená na souhlasu uděleném před jeho odvoláním (čl. 14 odst. 2 písm. d) GDPR).

Pokud je zpracování osobních údajů založeno na čl. 6 odst. 1 písm. a) GDPR, což je případ, kdy subjekt údajů udělil souhlas se zpracováním osobních údajů pro jeden nebo více konkrétních účelů, nebo je založeno na čl. 9 odst. 2 písm. a) GDPR, který upravuje výslovný souhlas se zpracováním zvláštních kategorií osobních údajů, má subjekt údajů podle čl. 7 odst. 3 věty první GDPR právo svůj souhlas kdykoli odvolat.

Odvolání souhlasu nemá vliv na zákonnost zpracování založeného na souhlasu před jeho odvoláním, čl. 7 odst. 3 věta druhá GDPR. Odvolání souhlasu musí být stejně snadné jako jeho udělení, čl. 7 odst. 3 věta 4 GDPR. K odvolání souhlasu proto může dojít vždy stejným způsobem, jakým byl souhlas udělen, nebo jakýmkoli jiným způsobem, který subjekt údajů považuje za jednodušší. V dnešní informační společnosti je pravděpodobně nejjednodušším způsobem odvolání souhlasu prostý e-mail. Pokud si subjekt údajů přeje odvolat svůj souhlas, který nám udělil, stačí nám zaslat jednoduchý e-mail. Případně si subjekt údajů může zvolit jakýkoli jiný způsob, jak nám svůj souhlas odvolat.

## K. Existence práva podat stížnost u dozorového úřadu (čl. 14 odst. 2 písm. e), čl. 77 odst. 1 GDPR)

Jako správce jsme povinni informovat subjekt údajů o právu podat stížnost u dozorového úřadu, čl. 14 odst. 2 písm. e) GDPR. Právo podat stížnost u dozorového úřadu upravuje čl. 77 odst. 1 GDPR. Podle tohoto ustanovení, aniž jsou dotčeny jakékoli jiné správní nebo soudní prostředky nápravy, má každý subjekt údajů právo podat stížnost u dozorového úřadu, zejména v členském státě svého obvyklého bydliště, pracoviště nebo místa údajného porušení, pokud se subjekt údajů domnívá, že zpracování osobních údajů, které se ho týkají, porušuje obecné nařízení o ochraně osobních údajů. Právo podat stížnost u dozorového úřadu bylo právem Unie omezeno pouze tak, že jej lze uplatnit pouze u jediného dozorového úřadu (141. bod odůvodnění věta první obecného nařízení o ochraně osobních údajů). Toto pravidlo má zabránit dvojím stížnostem téhož subjektu údajů v téže věci. Pokud na nás chce subjekt údajů podat stížnost, požádali jsme ho proto, aby se obrátil pouze na jediný dozorový úřad.

## L. Zdroj, ze kterého osobní údaje pocházejí, a případně informace o tom, zda údaje pocházejí z veřejně dostupných zdrojů (čl. 14 odst. 2 písm. f) GDPR)

Osobní údaje se v zásadě shromažďují přímo od subjektu údajů nebo ve spolupráci s orgánem (např. vyhledáním údajů v úředním registru). Ostatní údaje o subjektech údajů jsou získávány z předávání údajů společností skupiny. V souvislosti s těmito obecnými informacemi je pojmenování přesných zdrojů, z


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

nichž osobní údaje pocházejí, buď nemožné, nebo by vyžadovalo nepřiměřené úsilí ve smyslu čl. 14 odst. 5 písm. b) GDPR. Osobní údaje z veřejně přístupných zdrojů zásadně neshromažďujeme.

Každý subjekt údajů nás může kdykoli kontaktovat a získat podrobnější informace o přesných zdrojích osobních údajů, které se ho týkají. Pokud nelze subjektu údajů poskytnout informace o původu osobních údajů, protože byly použity různé zdroje, měly by být poskytnuty obecné informace (61. bod odůvodnění, 4. věta obecného nařízení o ochraně osobních údajů).

### M. Skutečnost, že dochází k automatizovanému rozhodování, včetně profilování, uvedenému v čl. 22 odst. 1 a 4, a přinejmenším v těchto případech smysluplné informace týkající se použitého postupu, jakož i významu a předpokládaných důsledků takového zpracování pro subjekt údajů (čl. 14 odst. 2 písm. g) GDPR).

Jako odpovědná společnost obvykle nepoužíváme automatizované rozhodování ani profilování. Pokud ve výjimečných případech automatizované rozhodování nebo profilování provádíme, informujeme o tom subjekt údajů buď samostatně, nebo prostřednictvím pododdílu v našich zásadách ochrany osobních údajů (na našich webových stránkách). V takovém případě platí následující:

K automatizovanému rozhodování - včetně profilování - může dojít, pokud (1) je to nezbytné pro uzavření nebo plnění smlouvy mezi subjektem údajů a námi, nebo (2) je to povoleno právem Unie nebo členského státu, které se na nás vztahuje a které rovněž stanoví vhodná opatření na ochranu práv a svobod a oprávněných zájmů subjektu údajů, nebo (3) je to založeno na výslovném souhlasu subjektu údajů.

V případech uvedených v čl. 22 odst. 2 písm. a) a c) GDPR provedeme vhodná opatření na ochranu práv a svobod a oprávněných zájmů subjektu údajů. V těchto případech máte právo na lidský zásah ze strany správce, na vyjádření svého názoru a na napadení rozhodnutí.

Smysluplné informace o příslušné logice, jakož i o významu a předpokládaných důsledcích takového zpracování pro subjekt údajů jsou uvedeny v našich zásadách ochrany osobních údajů.

## III. EU-U.S. Data Privacy Framework (EU-U.S. DPF), UK Extension to the EU-U.S. DPF, Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF)

Pokud je naše organizace certifikovaným členem EU-U.S. Data Privacy Framework (EU-U.S. DPF) a/nebo UK Extension to the EU-U.S. DPF a/nebo Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF), platí následující:

Dodržujeme EU-U.S. Data Privacy Framework (EU-U.S. DPF) a UK Extension to the EU-U.S. DPF i Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF), jak bylo stanoveno U.S. Department of


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

Commerce. Naše společnost potvrdila Ministerstvu obchodu USA, že dodržuje EU-U.S. Data Privacy Framework Principles (EU-U.S. DPF Principles) týkající se zpracování osobních údajů, které obdrží z Evropské unie a Spojeného království na základě EU-U.S. DPF a UK Extension to the EU-U.S. DPF. Naše společnost potvrdila Ministerstvu obchodu USA, že dodržuje Swiss-U.S. Data Privacy Framework Principles (Swiss-U.S. DPF Principles) týkající se zpracování osobních údajů, které obdrží ze Švýcarska na základě Swiss-U.S. DPF. V případě rozporu mezi ustanoveními našeho prohlášení o ochraně osobních údajů a EU-U.S. DPF Principles a/nebo Swiss-U.S. DPF Principles, jsou závazné Principles.

Pro více informací o programu Data Privacy Framework (DPF) a pro zobrazení našeho certifikátu navštivte prosím https://www.dataprivacyframework.gov/.

Ostatní americké jednotky nebo dceřiné společnosti naší společnosti, které také dodržují EU-U.S. DPF Principles, včetně UK Extension to the EU-U.S. DPF a Swiss-U.S. DPF Principles, jsou uvedeny v našem prohlášení o ochraně osobních údajů.

V souladu s EU-U.S. DPF a UK Extension to the EU-U.S. DPF a Swiss-U.S. DPF se naše společnost zavazuje spolupracovat s orgány zřízenými evropskými orgány na ochranu údajů a britským Information Commissioner's Office (ICO) a švýcarským Federal Data Protection and Information Commissioner (EDÖB) a dodržovat jejich rady týkající se nevyřešených stížností na naše zacházení s osobními údaji, které jsme obdrželi na základě EU-U.S. DPF, UK Extension to the EU-U.S. DPF a Swiss-U.S. DPF.

Informujeme dotčené osoby o příslušných evropských orgánech na ochranu osobních údajů, které jsou odpovědné za vyřizování stížností na zacházení naší organizace s osobními údaji, v horní části tohoto dokumentu transparentnosti a také o tom, že dotčeným osobám poskytujeme přiměřené a bezplatné právní prostředky.

Informujeme všechny dotčené osoby, že naše společnost podléhá vyšetřovacím a výkonným pravomocím Federal Trade Commission (FTC).

Dotčené osoby mají za určitých podmínek možnost požádat o závazné rozhodčí řízení. Naše organizace je povinna řešit nároky a dodržovat podmínky podle přílohy I DPF-Principals, pokud dotčená osoba požádala o závazné rozhodčí řízení tím, že o tom informovala naši organizaci a dodržela postupy a podmínky podle přílohy I Principles.

Tímto informujeme všechny dotčené osoby o odpovědnosti naší organizace v případě předání osobních údajů třetím stranám.

Pro dotazy dotčených osob nebo orgánů na ochranu osobních údajů jsme jmenovali místní zástupce uvedené výše v tomto dokumentu transparentnosti.

Nabízíme vám možnost volby (Opt-out), zda vaše osobní údaje (i) budou předány třetím stranám, nebo (ii) budou použity pro účel, který se podstatně liší od účelu (účelů), pro který (které) byly původně shromážděny nebo později vámi schváleny. Jednoznačný, dobře viditelný a snadno dostupný mechanismus pro uplatnění vašeho práva volby spočívá v kontaktování našeho pověřence pro ochranu


© All rights reserved by Heiko Maniero.

osobních údajů (DSB) prostřednictvím e-mailu. Nemáte žádnou volbu a my také nejsme povinni to dělat, pokud jsou údaje předány třetí straně, která jedná jako náš zástupce nebo zpracovatel údajů naším jménem a podle našich pokynů. Nicméně, s takovým zástupcem nebo zpracovatelem údajů vždy uzavíráme smlouvu.

Pro citlivé údaje (tj. osobní údaje, které obsahují informace o zdravotním stavu, rasovém nebo etnickém původu, politických názorech, náboženských nebo filozofických přesvědčeních, členství v odborech nebo informace o sexuálním životě dotyčné osoby) získáváme váš výslovný souhlas (Opt-in), pokud tyto údaje (i) budou předány třetím stranám, nebo (ii) budou použity pro jiný účel, než pro který byly původně shromážděny nebo pro který jste později udělili svůj souhlas, tím, že jste učinili svou volbu Opt-in. Kromě toho, všechny osobní údaje, které obdržíme od třetích stran, považujeme za citlivé, pokud je třetí strana identifikuje a zpracovává jako citlivé.

Tímto vás informujeme o nutnosti zveřejnění osobních údajů v reakci na zákonné požadavky orgánů, včetně splnění požadavků národní bezpečnosti nebo prosazování práva.

Při předávání osobních údajů třetí straně, která jedná jako správce, dodržujeme Principy oznámení a volby. Rovněž uzavíráme smlouvu s třetí stranou odpovědnou za zpracování, která stanoví, že tyto údaje mohou být zpracovány pouze pro omezené a určené účely v souladu s vaším poskytnutým souhlasem a že příjemce poskytuje stejnou úroveň ochrany jako Principy DPF a nás informuje, pokud zjistí, že již nemůže tuto povinnost plnit. Smlouva stanoví, že třetí strana, která jedná jako správce, zastaví zpracování nebo přijme jiné vhodné a přiměřené opatření k nápravě, pokud je taková situace zjištěna.

Při předávání osobních údajů třetí straně, která jedná jako agent nebo zpracovatel údajů, (i) předáváme tyto údaje pouze pro omezené a určené účely; (ii) ujistíme se, že agent nebo zpracovatel údajů se zavázal zajistit alespoň stejnou úroveň ochrany údajů, jakou požadují DPF-Principals; (iii) přijmeme vhodná a přiměřená opatření k zajištění toho, že agent nebo zpracovatel údajů skutečně zpracovává předané osobní údaje způsobem, který je v souladu s našimi závazky podle DPF-Principals; (iv) požadujeme od agenta nebo zpracovatele údajů, aby informoval naši organizaci, pokud zjistí, že již nemůže plnit svou povinnost zajistit stejnou úroveň ochrany, jakou požadují DPF-Principals; (v) po oznámení, včetně oznámení podle bodu (iv), přijmeme vhodná a přiměřená opatření k zastavení neoprávněného zpracování a k nápravě; a (vi) na žádost poskytneme DPF Department shrnutí nebo reprezentativní kopii příslušných ustanovení o ochraně údajů ve smlouvě s tímto agentem.

V souladu s EU-U.S. DPF a/nebo UK Extension to the EU-U.S. DPF a/nebo Swiss-U.S. DPF se naše organizace zavazuje spolupracovat s orgány zřízenými evropskými orgány na ochranu údajů a britským Information Commissioner's Office (ICO) a švýcarským Federal Data Protection and Information Commissioner (EDÖB) a dodržovat jejich rady týkající se nevyřešených stížností na naše zacházení s osobními údaji v souvislosti s pracovním vztahem, které jsme obdrželi na základě EU-U.S. DPF, UK Extension to the EU-U.S. DPF a Swiss-U.S. DPF.

Všechny subjekty údajů, které se dočasně nacházejí v Evropské unii (EU), Evropském hospodářském prostoru (EHP) nebo ve Spojeném království, nebo které tam mají bydliště či obvyklý pobyt, mají nárok


© All rights reserved by Heiko Maniero.

na práva a práva subjektu údajů, která jsou zveřejněna v našem dokumentu o transparentnosti a která rovněž vyplývají z článků 15 až 22 GDPR, včetně práva na přístup k osobním údajům. Tyto informace jsme zpřístupnili ve všech jazycích EU a EHP. Anglická verze platí pro Spojené království.

Všechny subjekty údajů, které mají ve Švýcarsku dočasný pobyt nebo tam mají bydliště či obvyklý pobyt, mají podle švýcarského zákona o ochraně osobních údajů (DPA) a švýcarského nařízení o ochraně osobních údajů (DPR) práva a nároky subjektu údajů, které jsou zveřejněny v našem dokumentu o transparentnosti, včetně práva na přístup k osobním údajům. Tyto informace jsme poskytli ve třech úředních jazycích Švýcarska (němčině, italštině a francouzštině).


© All rights reserved by Heiko Maniero.

# BULGARIAN: Информация за обработката на лични данни (член 13, 14 от ОРЗД)

Уважаеми господине или госпожо,

Личните данни на всяко лице, което е в договорни, преддоговорни или други отношения с нашата компания, заслужават специална защита. Нашата цел е да поддържаме високо ниво на защита на данните. Поради това рутинно развиваме нашите концепции за защита и сигурност на данните.

Разбира се, ние спазваме законовите разпоредби за защита на данните. Съгласно членове 13, 14 от ОРЗД администраторите изпълняват конкретни изисквания за информация при събирането на лични данни. С настоящия документ се изпълняват тези задължения.

Терминологията на правните разпоредби е сложна. За съжаление, при изготвянето на този документ не можеше да се избегне използването на правни термини. Ето защо бихме искали да отбележим, че винаги можете да се свържете с нас по всички въпроси, свързани с този документ, използваните термини или формулировки.

## I. Информация, предоставяна при събиране на лични данни от субекта на данните (член 13 от ОРЗД)

### A. данните, които идентифицират администратора и координатите за връзка с него и, когато е приложимо, тези на представителя на администратора (член 13, параграф 1, буква а) от ОРЗД)

Вижте по-горе

### B. координатите за връзка с длъжностното лице по защита на данните, когато е приложимо (член 13, параграф 1, буква б) от ОРЗД)

Вижте по-горе

### C. целите на обработването, за което личните данни са предназначени, както и правното основание за обработването (член 13, параграф 1, буква в) от ОРЗД)

Целта на обработката на лични данни е извършването на всички операции, които се отнасят до администратора, клиентите, потенциалните клиенти, бизнес партньорите или други договорни или


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

преддоговорни отношения между посочените групи (в най-широк смисъл) или до правните задължения на администратора.

Чл. 6, параграф 1, буква а) от ОРЗД служи като правно основание за операции по обработване, за които получаваме съгласие за конкретна цел на обработване. Ако обработката на лични данни е необходима за изпълнението на договор, по който субектът на данните е страна, какъвто е случаят например, когато операциите по обработка са необходими за доставката на стоки или за предоставянето на друга услуга, обработката се основава на член 6, параграф 1, буква б) от ОРЗД. Същото важи и за такива операции по обработване, които са необходими за извършване на преддоговорни мерки, например в случай на запитвания относно нашите продукти или услуги. Подчинено ли е нашето дружество на правно задължение, по силата на което се изисква обработване на лични данни, например за изпълнение на данъчни задължения, обработването се основава на чл. 6, параграф 1, буква в) от ОРЗД.

В редки случаи обработката на лични данни може да е необходима за защита на жизненоважните интереси на субекта на данните или на друго физическо лице. Такъв би бил случаят, например, ако посетител се нарани в нашата компания и неговото име, възраст, данни за здравното осигуряване или друга жизненоважна информация трябва да бъдат предадени на лекар, болница или друга трета страна. Тогава обработката ще се основава на чл. 6, параграф 1, буква г) от ОРЗД.

Когато обработването е необходимо за изпълнението на задача, извършвана в обществен интерес или при упражняването на официални правомощия, предоставени на администратора, правното основание е чл. 6, параграф 1, буква д) от ОРЗД.

И накрая, операциите по обработване могат да се основават на член 6, параграф 1, буква е) от ОРЗД. Това правно основание се използва за операции по обработване, които не са обхванати от нито едно от горепосочените правни основания, ако обработването е необходимо за целите на законните интереси, преследвани от нашето дружество или от трета страна, освен когато пред тези интереси преимущество имат интересите или основните права и свободи на субекта на данните, които изискват защита на личните данни. Такива операции по обработване са особено допустими, тъй като са изрично упоменати от европейския законодател. Той счита, че легитимен интерес може да се приеме, ако субектът на данните е клиент на администратора (съображение 47, изречение 2 от ОРЗД).

## D. когато обработването се извършва въз основа на член 6, параграф 1, буква е), законните интереси, преследвани от администратора или от трета страна (член 13, параграф 1, буква г) от ОРЗД)

Когато обработката на лични данни се основава на член 6, параграф 1, буква е) от ОРЗД, нашият легитимен интерес е да извършваме дейността си в полза на благосъстоянието на всички наши служители и акционери.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## E. получателите или категориите получатели на личните данни, ако има такива (член 13, параграф 1, буква д) от ОРЗД)

Публични органи

Външни органи

Други външни органи

Вътрешна обработка

Вътрешногрупова обработка

Други органи

Списък на нашите обработващи и получатели на данни в трети държави и, ако е приложимо, на международни организации е публикуван на нашия уебсайт или може да бъде поискан от нас безплатно. Моля, свържете се с нашето длъжностно лице по защита на данните, за да поискате този списък.

## F. когато е приложимо, намерението на администратора да предаде личните данни на трета държава или на международна организация, както и наличието или отсъствието на решение на Комисията относно адекватното ниво на защита или в случай на предаване на данни съгласно посоченото в членове 46 или 47, или член 49, параграф 1, втора алинея позоваване на подходящите или приложимите гаранции и средствата за получаване на копие от тях или на информация къде са налични (член 13, параграф 1, буква е).

Всички дружества и клонове, които са част от нашата група (наричани по-долу "дружества от групата"), които имат място на стопанска дейност или офис в трета държава, могат да бъдат получатели на лични данни. Списък на всички дружества от групата или получатели може да бъде поискан от нас.

Съгласно член 46, параграф 1 от ОРЗД администратор или обработващ лични данни може да предава лични данни на трета държава само ако е осигурил подходящи гаранции и при условие че са налице изпълними права на субекта на данни и ефективни правни средства за защита на субектите на данни. Подходящи гаранции могат да бъдат предоставени, без да се изисква специално разрешение от надзорния орган, посредством стандартни договорни клаузи, член 46, параграф 2, буква в) от ОРЗД.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

Стандартните договорни клаузи на Европейския съюз или други подходящи предпазни мерки се договарят с всички получатели от трети държави преди първото предаване на лични данни. В резултат на това се гарантира, че са осигурени подходящи гаранции, изпълними права на субектите на данни и ефективни правни средства за защита на субектите на данни. Всеки субект на данни може да получи от нас копие от стандартните договорни клаузи. Стандартните договорни клаузи са на разположение и в Официален вестник на Европейския съюз.

Член 45, параграф 3 от Общия регламент относно защитата на данните (ОРЗД) предоставя на Европейската комисия правото да реши чрез акт за изпълнение, че държава извън ЕС осигурява адекватно ниво на защита. Това означава ниво на защита на личните данни, което в общи линии е еквивалентно на това в ЕС. Резултатът от решенията, с които се установява адекватно ниво на защита, е, че личните данни могат да се пренасят свободно от ЕС (и Норвегия, Лихтенщайн и Исландия) в трета държава без допълнителни пречки. Подобни правила се прилагат в Обединеното кралство, Швейцария и някои други държави.

В случай че Европейската комисия или правителството на друга държава реши, че трета държава осигурява адекватно ниво на защита, и приложимата рамка (например EU-U.S. Data Privacy Framework, Swiss-U.S. Data Privacy Framework, UK Extension to the EU-U.S. Data Privacy Framework), всички трансфери от нас към членове на такива рамки (например самосертифицирани субекти) се основават единствено на членството на тези субекти в съответната рамка. В случай че ние или някое от нашите образувания от групата е член на такава рамка, всички прехвърляния към нас или към образувание от нашата група се основават единствено на членството на образуването в такава рамка.

Всеки субект на данни може да получи от нас копие от рамката. Освен това рамките са достъпни и в Официален вестник на Европейския съюз или в публикуваните правни материали, или на уебсайтовете на надзорните органи или други компетентни органи или институции.

## G. срока, за който ще се съхраняват личните данни, а ако това е невъзможно, критериите, използвани за определяне на този срок (член 13, параграф 2, буква а) от ОРЗД)

Критериите, използвани за определяне на периода на съхранение на личните данни, са съответният законоустановен период на съхранение. След изтичането на този период съответните данни се изтриват рутинно, ако вече не са необходими за изпълнението на договора или за започването на договор.

Ако няма законоустановен период на съхранение, критерият е договорният или вътрешният период на съхранение.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## H. съществуването на право да се изиска от администратора достъп до, коригиране или изтриване на лични данни или ограничаване на обработването на лични данни, свързани със субекта на данните, или право да се направи възражение срещу обработването, както и правото на преносимост на данните (член 13, параграф 2, буква б) от ОРЗД)

Всички субекти на данни имат следните права:

***Право на достъп***

Всеки субект на данни има право на достъп до личните данни, които го засягат. Правото на достъп се отнася за всички данни, обработвани от нас. Правото може да се упражнява лесно и на разумни интервали от време, за да се запознаете и да проверите законосъобразността на обработката (съображение 63 от ОРЗД). Това право произтича от чл. 15 ОТ ОРЗД. Субектът на данните може да се свърже с нас, за да упражни правото си на достъп.

***Право на коригиране***

Съгласно член 16, изречение 1 от ОРЗД субектът на данните има право да получи от администратора без ненужно забавяне коригирането на неточни лични данни, които го засягат. Освен това член 16, изречение 2 от ОРЗД предвижда, че субектът на данните има право, като се вземат предвид целите на обработването, да поиска непълните лични данни да бъдат попълнени, включително чрез предоставяне на допълнителна декларация. Субектът на данните може да се свърже с нас, за да упражни правото си на коригиране.

***Право на изтриване (право да бъдеш забравен)***

Освен това субектите на данни имат право на право на изтриване и забравяне съгласно чл. 17 ОТ ОРЗД. Това право също може да бъде упражнено, като се свържете с нас. На това място обаче бихме искали да посочим, че това право не се прилага, доколкото обработването е необходимо за изпълнение на правно задължение, на което нашето дружество е подчинено, член 17, параграф 3, буква б) от ОРЗД. Това означава, че можем да одобрим заявлението за изтриване само след изтичане на законоустановения период на съхранение.

***Право на ограничаване на обработката***

Съгласно член 18 от ОРЗД всеки субект на данни има право на ограничаване на обработката. Ограничаване на обработването може да се поиска, ако е изпълнено едно от условията, посочени в член 18, параграф 1, буква а-г от ОРЗД. Субектът на данни може да се свърже с нас, за да упражни правото си на ограничаване на обработката.

***Право на възражение***

Освен това чл. 21 от ОРЗД се гарантира правото на възражение. Субектът на данните може да се свърже с нас, за да упражни правото си на възражение.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

***Право на преносимост на данните***

Чл. 20 от ОРЗД предоставя на субекта на данните правото на преносимост на данните. Съгласно тази разпоредба субектът на данните има право при условията, предвидени в член 20, параграф 1, букви а) и б) от ОРЗД, да получи личните данни, които го засягат и които той е предоставил на администратор, в структуриран, широко използван и пригоден за машинно четене формат, както и да предаде тези данни на друг администратор, без да бъде възпрепятстван от администратора, на когото са предоставени личните данни. Субектът на данните може да се свърже с нас, за да упражни правото си на преносимост на данните.

## I. когато обработването се основава на член 6, параграф 1, буква а) или член 9, параграф 2, буква а), съществуването на право на оттегляне на съгласието по всяко време, без да се засяга законосъобразността на обработването въз основа на съгласие, преди то да бъде оттеглено (член 13, параграф 2, буква в) от ОРЗД)

Ако обработката на лични данни се основава на чл. 6, параграф 1, буква а) от ОРЗД, какъвто е случаят, ако субектът на данните е дал съгласие за обработване на лични данни за една или повече конкретни цели, или се основава на член 9, параграф 2, буква а) от ОРЗД, който урежда изричното съгласие за обработване на специални категории лични данни, субектът на данните има право съгласно член 7, параграф 3, изречение 1 от ОРЗД да оттегли съгласието си по всяко време.

Оттеглянето на съгласието не засяга законосъобразността на обработването, основано на съгласието преди неговото оттегляне, член 7, параграф 3, изречение 2 от ОРЗД. Оттеглянето на съгласието трябва да бъде толкова лесно, колкото и даването му, чл. 7, параграф 3, изречение 4 от ОРЗД. Следователно оттеглянето на съгласието винаги може да се извърши по същия начин, по който е дадено съгласието, или по друг начин, който субектът на данните счита за по-лесен. В днешното информационно общество вероятно най-простият начин за оттегляне на съгласието е обикновено електронно писмо. Ако субектът на данните желае да оттегли съгласието си, което ни е дал, е достатъчно да ни изпрати просто имейл. Като алтернатива субектът на данните може да избере друг начин да ни съобщи за оттеглянето на съгласието си.

## J. правото на жалба до надзорен орган (член 13, параграф 2, буква г) и член 77, параграф 1 от ОРЗД)

В качеството си на администратор сме длъжни да уведомим субекта на данните за правото му да подаде жалба до надзорен орган, член 13, параграф 2, буква г) от ОРЗД. Правото на подаване на жалба до надзорен орган е уредено в член 77, параграф 1 от ОРЗД. Съгласно тази разпоредба, без да се засягат други административни или съдебни средства за защита, всеки субект на данни


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

има право да подаде жалба до надзорен орган, по-специално в държавата членка на обичайното си местопребиваване, място на работа или място на предполагаемото нарушение, ако субектът на данни счита, че обработването на лични данни, свързани с него, нарушава Общия регламент относно защитата на данните. Правото на подаване на жалба до надзорен орган беше ограничено от правото на Съюза по такъв начин, че то може да бъде упражнено само пред един надзорен орган (съображение 141, изречение 1 от Общия регламент относно защитата на данните). Това правило има за цел да се избегне двойното подаване на жалби от един и същ субект на данни по един и същи въпрос. Ето защо, ако субект на данни иска да подаде жалба срещу нас, ние го молим да се обърне само към един-единствен надзорен орган.

## K. дали предоставянето на лични данни е задължително или договорно изискване, или изискване, необходимо за сключването на договор, както и дали субектът на данните е длъжен да предостави личните данни и евентуалните последствия, ако тези данни не бъдат предоставени (член 13, параграф 2, буква д) от ОРЗД)

Поясняваме, че предоставянето на лични данни се изисква отчасти по закон (напр. данъчни разпоредби) или може да произтича от договорни разпоредби (напр. информация за договорния партньор).

Понякога може да е необходимо за сключването на договор субектът на данни да ни предостави лични данни, които впоследствие трябва да бъдат обработени от нас. Субектът на данни например е длъжен да ни предостави лични данни, когато нашето дружество сключва договор с него. Непредоставянето на личните данни би имало за последица невъзможността да се сключи договор със субекта на данните.

Преди субектът на данните да предостави личните си данни, той трябва да се свърже с нас. Ние разясняваме на субекта на данните дали предоставянето на личните данни се изисква по закон или договор или е необходимо за сключването на договора, дали съществува задължение за предоставяне на личните данни и какви са последиците от непредоставянето на личните данни.

## L. съществуването на автоматизирано вземане на решения, включително профилирането, посочено в член 22, параграфи 1 и 4, и поне в тези случаи съществена информация относно използваната логика, както и значението и предвидените последствия от това обработване за субекта на данните (член 13, параграф 2, буква е) от ОРЗД)

Като отговорна компания обикновено не използваме автоматизирано вземане на решения или профилиране. Ако в изключителни случаи извършваме автоматизирано вземане на решения или


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

профилиране, ще информираме субекта на данните отделно или чрез подраздел в нашата политика за поверителност (на нашия уебсайт). В този случай се прилага следното:

Автоматизирано вземане на решения - включително профилиране - може да се извърши, ако (1) това е необходимо за сключването или изпълнението на договор между субекта на данните и нас, или (2) това е разрешено от правото на Съюза или на държава членка, което се прилага спрямо нас и в което също така са предвидени подходящи мерки за защита на правата и свободите и законните интереси на субекта на данните; или (3) това се основава на изричното съгласие на субекта на данните.

В случаите, посочени в член 22, параграф 2, букви а) и в) от ОРЗД, ние прилагаме подходящи мерки за защита на правата и свободите и законните интереси на субекта на данните. В тези случаи имате право да получите човешка намеса от страна на администратора, да изразите своята гледна точка и да оспорите решението.

Съществена информация за използваната логика, както и за значението и предвидените последици от това обработване за субекта на данните, е изложена в нашата политика за поверителност.

## II. Информация, предоставяна, когато личните данни идват от субекта на данните (член 14 от ОРЗД)

### A. данните, които идентифицират администратора и координатите за връзка с него и, когато е приложимо, тези на представителя на администратора (член 14, параграф 1, буква а) от ОРЗД)

Вижте по-горе

### B. координатите за връзка с длъжностното лице по защита на данните, когато е приложимо (член 14, параграф 1, буква б) от ОРЗД)

Вижте по-горе

### C. целите на обработването, за което личните данни са предназначени, както и правното основание за обработването (член 14, параграф 1, буква в) от ОРЗД)

Целта на обработката на лични данни е извършването на всички операции, които се отнасят до администратора, клиентите, потенциалните клиенти, бизнес партньорите или други договорни или


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

преддоговорни отношения между посочените групи (в най-широк смисъл) или до правните задължения на администратора.

Ако обработката на лични данни е необходима за изпълнението на договор, по който субектът на данните е страна, както е например в случаите, когато операциите по обработката са необходими за доставката на стоки или за предоставянето на друга услуга, обработката се основава на член 6, параграф 1, буква б) от ОРЗД. Същото важи и за такива операции по обработване, които са необходими за извършване на преддоговорни мерки, например в случай на запитвания относно нашите продукти или услуги. Подчинено ли е нашето дружество на правно задължение, по силата на което се изисква обработване на лични данни, например за изпълнение на данъчни задължения, обработването се основава на чл. 6, параграф 1, буква в) от ОРЗД.

В редки случаи обработката на лични данни може да е необходима за защита на жизненоважните интереси на субекта на данните или на друго физическо лице. Такъв би бил случаят, например, ако посетител се нарани в нашата компания и неговото име, възраст, данни за здравното осигуряване или друга жизненоважна информация трябва да бъдат предадени на лекар, болница или друга трета страна. Тогава обработката ще се основава на чл. 6, параграф 1, буква г) от ОРЗД.

Когато обработването е необходимо за изпълнението на задача, извършвана в обществен интерес или при упражняването на официални правомощия, предоставени на администратора, правното основание е чл. 6, параграф 1, буква д) от ОРЗД.

И накрая, операциите по обработване могат да се основават на член 6, параграф 1, буква е) от ОРЗД. Това правно основание се използва за операции по обработване, които не са обхванати от нито едно от горепосочените правни основания, ако обработването е необходимо за целите на законните интереси, преследвани от нашето дружество или от трета страна, освен когато пред тези интереси преимущество имат интересите или основните права и свободи на субекта на данните, които изискват защита на личните данни. Такива операции по обработване са особено допустими, тъй като са изрично посочени от европейския законодател. Той счита, че легитимен интерес може да се приеме, ако субектът на данните е клиент на администратора (съображение 47, изречение 2 от ОРЗД).

## D. съответните категории лични данни (член 14, параграф 1, буква г) от ОРЗД)

Данни за клиентите

Данни за потенциални клиенти

Данни за служителите

Данни за доставчиците


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## E. получателите или категориите получатели на личните данни, ако има такива (член 14, параграф 1, буква д) от ОРЗД)

Публични органи

Външни органи

Други външни органи

Вътрешна обработка

Вътрешногрупова обработка

Други органи

Списък на нашите обработващи и получатели на данни в трети държави и, ако е приложимо, на международни организации е публикуван на нашия уебсайт или може да бъде поискан от нас безплатно. Моля, свържете се с нашето длъжностно лице по защита на данните, за да поискате този списък.

## F. когато е приложимо, намерението на администратора да предаде данните на трета държава или на международна организация, и наличието или отсъствието на решение на Комисията относно адекватното ниво на защита или в случай на предаване на данни съгласно член 46 или 47, или член 49, параграф 1, втора алинея с позоваване на подходящите или приложимите гаранции и средствата за получаване на копие от тях или на информация къде са налични (член 14, параграф 1, буква е).

Всички дружества и клонове, които са част от нашата група (наричани по-долу "дружества от групата"), които имат място на стопанска дейност или офис в трета държава, могат да бъдат получатели на лични данни. Списък на всички дружества от групата може да бъде поискан от нас.

Съгласно член 46, параграф 1 от ОРЗД администратор или обработващ лични данни може да предава лични данни на трета държава само ако е осигурил подходящи гаранции и при условие че са налице изпълними права на субекта на данни и ефективни правни средства за защита на субектите на данни. Подходящи гаранции могат да бъдат предоставени, без да се изисква специално разрешение от надзорния орган, посредством стандартни клаузи за защита на данните, член 46, параграф 2, буква в) от ОРЗД.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

Стандартните договорни клаузи на Европейския съюз или други подходящи предпазни мерки се договарят с всички получатели от трети държави преди първото предаване на лични данни. В резултат на това се гарантира, че са осигурени подходящи гаранции, изпълними права на субектите на данни и ефективни правни средства за защита на субектите на данни. Всеки субект на данни може да получи от нас копие от стандартните договорни клаузи. Стандартните договорни клаузи са на разположение и в Официален вестник на Европейския съюз.

Член 45, параграф 3 от Общия регламент относно защитата на данните (ОРЗД) предоставя на Европейската комисия правото да реши чрез акт за изпълнение, че държава извън ЕС осигурява адекватно ниво на защита. Това означава ниво на защита на личните данни, което в общи линии е еквивалентно на това в ЕС. Резултатът от решенията, с които се установява адекватно ниво на защита, е, че личните данни могат да се пренасят свободно от ЕС (и Норвегия, Лихтенщайн и Исландия) в трета държава без допълнителни пречки. Подобни правила се прилагат в Обединеното кралство, Швейцария и някои други държави.

В случай че Европейската комисия или правителството на друга държава реши, че трета държава осигурява адекватно ниво на защита, и приложимата рамка (например EU-U.S. Data Privacy Framework, Swiss-U.S. Data Privacy Framework, UK Extension to the EU-U.S. Data Privacy Framework), всички трансфери от нас към членове на такива рамки (например самосертифицирани субекти) се основават единствено на членството на тези субекти в съответната рамка. В случай че ние или някое от нашите образувания от групата е член на такава рамка, всички прехвърляния към нас или към образувание от нашата група се основават единствено на членството на образуването в такава рамка.

Всеки субект на данни може да получи от нас копие от рамката. Освен това рамките са достъпни и в Официален вестник на Европейския съюз или в публикуваните правни материали, или на уебсайтовете на надзорните органи или други компетентни органи или институции.

## G. срока, за който ще се съхраняват личните данни, а ако това е невъзможно, критериите, използвани за определяне на този срок (член 14, параграф 2, буква а) от ОРЗД)

Критериите, използвани за определяне на периода на съхранение на личните данни, са съответният законоустановен период на съхранение. След изтичането на този период съответните данни се изтриват рутинно, ако вече не са необходими за изпълнението на договора или за започването на договор.

Ако няма законоустановен период на съхранение, критерият е договорният или вътрешният период на съхранение.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## H. когато обработването се извършва въз основа на член 6, параграф 1, буква е), законните интереси, преследвани от администратора или от трета страна (член 14, параграф 2, буква б) от ОРЗД)

В съответствие с член 6, параграф 1, буква е) от ОРЗД обработването е законосъобразно само ако е необходимо за целите на законните интереси на администратора или на трета страна, освен когато пред тези интереси преимущество имат интересите или основните права и свободи на субекта на данните, които изискват защита на личните данни. Съгласно съображение 47, изречение 2 от ОРЗД легитимен интерес би могъл да съществува, когато между субекта на данните и администратора съществува съответна и подходяща връзка, например в ситуации, в които субектът на данните е клиент на администратора. Във всички случаи, в които нашето дружество обработва лични данни въз основа на член 6, параграф 1, буква е) от ОРЗД, нашият легитимен интерес е да осъществяваме дейността си в полза на благосъстоянието на всички наши служители и акционери.

## I. съществуването на право да се изиска от администратора достъп до, коригиране или изтриване на лични данни, свързани със субекта на данните, или ограничаване на обработването, и правото да се направи възражение срещу обработването, както и правото на преносимост на данните (член 14, параграф 2, буква в) от ОРЗД)

Всички субекти на данни имат следните права:

***Право на достъп***

Всеки субект на данни има право на достъп до личните данни, които го засягат. Правото на достъп се отнася за всички данни, обработвани от нас. Правото може да се упражнява лесно и на разумни интервали от време, за да се запознаете и да проверите законосъобразността на обработката (съображение 63 от ОРЗД). Това право произтича от чл. 15 ОТ ОРЗД. Субектът на данните може да се свърже с нас, за да упражни правото си на достъп.

***Право на коригиране***

Съгласно член 16, изречение 1 от ОРЗД субектът на данните има право да получи от администратора без ненужно забавяне коригирането на неточни лични данни, които го засягат. Освен това член 16, изречение 2 от ОРЗД предвижда, че субектът на данните има право, като се вземат предвид целите на обработването, да поиска непълните лични данни да бъдат попълнени, включително чрез предоставяне на допълнителна декларация. Субектът на данните може да се свърже с нас, за да упражни правото си на коригиране.

***Право на изтриване (право да бъдеш забравен)***

Освен това субектите на данни имат право на право на изтриване и забравяне съгласно чл. 17 ОТ ОРЗД. Това право също може да бъде упражнено, като се свържете с нас. На това място обаче


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

бихме искали да посочим, че това право не се прилага, доколкото обработването е необходимо за изпълнение на правно задължение, на което нашето дружество е подчинено, член 17, параграф 3, буква б) от ОРЗД. Това означава, че можем да одобрим заявлението за изтриване само след изтичане на законоустановения период на съхранение.

***Право на ограничаване на обработката***

Съгласно член 18 от ОРЗД всеки субект на данни има право на ограничаване на обработката. Ограничаване на обработването може да се поиска, ако е изпълнено едно от условията, посочени в член 18, параграф 1, буква а-г от ОРЗД. Субектът на данни може да се свърже с нас, за да упражни правото си на ограничаване на обработката.

***Право на възражение***

Освен това чл. 21 от ОРЗД се гарантира правото на възражение. Субектът на данните може да се свърже с нас, за да упражни правото си на възражение.

***Право на преносимост на данните***

Чл. 20 от ОРЗД предоставя на субекта на данните правото на преносимост на данните. Съгласно тази разпоредба субектът на данни има право при условията, предвидени в член 20, параграф 1, букви а) и б) от ОРЗД, да получи личните данни, които го засягат и които той е предоставил на администратор, в структуриран, широко използван и пригоден за машинно четене формат, както и да предаде тези данни на друг администратор, без да бъде възпрепятстван от администратора, на когото са предоставени личните данни. Субектът на данните може да се свърже с нас, за да упражни правото си на преносимост на данните.

## J. когато обработването се основава на член 6, параграф 1, буква а) или член 9, параграф 2, буква а), съществуването на право на оттегляне на съгласието по всяко време, без да се засяга законосъобразността на обработването въз основа на съгласие, преди то да бъде оттеглено (член 14, параграф 2, буква г) от ОРЗД)

Ако обработката на лични данни се основава на чл. 6, параграф 1, буква а) от ОРЗД, какъвто е случаят, ако субектът на данните е дал съгласие за обработване на лични данни за една или повече конкретни цели, или се основава на член 9, параграф 2, буква а) от ОРЗД, който урежда изричното съгласие за обработване на специални категории лични данни, субектът на данните има право съгласно член 7, параграф 3, изречение 1 от ОРЗД да оттегли съгласието си по всяко време.

Оттеглянето на съгласието не засяга законосъобразността на обработването, основано на съгласието преди неговото оттегляне, член 7, параграф 3, изречение 2 от ОРЗД. Оттеглянето на съгласието трябва да бъде толкова лесно, колкото и даването му, чл. 7, параграф 3, изречение 4 от ОРЗД. Следователно оттеглянето на съгласието винаги може да се извърши по същия начин,


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

по който е дадено съгласието, или по друг начин, който субектът на данните счита за по-лесен. В днешното информационно общество вероятно най-простият начин за оттегляне на съгласието е обикновено електронно писмо. Ако субектът на данните желае да оттегли съгласието си, което ни е дал, е достатъчно да ни изпрати просто имейл. Като алтернатива субектът на данните може да избере друг начин да ни съобщи за оттеглянето на съгласието си.

## K. правото на жалба до надзорен орган (член 14, параграф 2, буква д) и член 77, параграф 1 от ОРЗД)

В качеството си на администратор сме длъжни да уведомим субекта на данните за правото му да подаде жалба до надзорен орган, член 14, параграф 2, буква д) от ОРЗД. Правото на подаване на жалба до надзорен орган е уредено в член 77, параграф 1 от ОРЗД. Съгласно тази разпоредба, без да се засягат други административни или съдебни средства за защита, всеки субект на данни има право да подаде жалба до надзорен орган, по-специално в държавата членка на обичайното си местопребиваване, място на работа или място на предполагаемото нарушение, ако субектът на данни счита, че обработването на лични данни, свързани с него, нарушава Общия регламент относно защитата на данните. Правото на подаване на жалба до надзорен орган беше ограничено от правото на Съюза по такъв начин, че то може да бъде упражнено само пред един надзорен орган (съображение 141, изречение 1 от Общия регламент относно защитата на данните). Това правило има за цел да се избегнат двойни жалби на един и същ субект на данни по един и същ въпрос. Ето защо, ако субект на данни иска да подаде жалба срещу нас, ние го молим да се обърне само към един-единствен надзорен орган.

## L. източника на личните данни и, ако е приложимо, дали данните са от публично достъпен източник (член 14, параграф 2, буква е) от ОРЗД)

По принцип личните данни се събират директно от субекта на данните или в сътрудничество с орган (напр. извличане на данни от официален регистър). Други данни за субектите на данни се извличат от трансфери на дружества от групата. В контекста на тази обща информация посочването на точните източници, от които произхождат личните данни, е или невъзможно, или би изисквало непропорционални усилия по смисъла на чл. 14, параграф 5, буква б) от ОРЗД. По принцип ние не събираме лични данни от публично достъпни източници.

Всеки субект на данни може да се свърже с нас по всяко време, за да получи по-подробна информация за точните източници на личните данни, които го засягат. Когато произходът на личните данни не може да бъде предоставен на субекта на данните, тъй като са използвани различни източници, следва да се предостави обща информация (съображение 61, изречение 4 от ОРЗД).


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

### M. съществуването на автоматизирано вземане на решения, включително профилирането, посочено в член 22, параграфи 1 и 4, и поне в тези случаи съществена информация относно използваната логика, както и значението и предвидените последствия от това обработване за субекта на данните (член 14, параграф 2, буква ж от ОРЗД)

Като отговорна компания обикновено не използваме автоматизирано вземане на решения или профилиране. Ако в изключителни случаи извършваме автоматизирано вземане на решения или профилиране, ще информираме субекта на данните отделно или чрез подраздел в нашата политика за поверителност (на нашия уебсайт). В този случай се прилага следното:

Автоматизирано вземане на решения - включително профилиране - може да се извърши, ако (1) това е необходимо за сключването или изпълнението на договор между субекта на данните и нас, или (2) това е разрешено от правото на Съюза или на държава членка, което се прилага спрямо нас и в което също така са предвидени подходящи мерки за защита на правата и свободите и законните интереси на субекта на данните; или (3) това се основава на изричното съгласие на субекта на данните.

В случаите, посочени в член 22, параграф 2, букви а) и в) от ОРЗД, ние прилагаме подходящи мерки за защита на правата и свободите и законните интереси на субекта на данните. В тези случаи имате право да получите човешка намеса от страна на администратора, да изразите своята гледна точка и да оспорите решението.

Съществена информация за използваната логика, както и за значението и предвидените последици от това обработване за субекта на данните, е изложена в нашата политика за поверителност.

## III. EU-U.S. Data Privacy Framework (EU-U.S. DPF), UK Extension to the EU-U.S. DPF, Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF)

Ако нашата организация е сертифициран член на EU-U.S. Data Privacy Framework (EU-U.S. DPF) и/или на UK Extension to the EU-U.S. DPF и/или на Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF), се прилага следното:

Ние спазваме EU-U.S. Data Privacy Framework (EU-U.S. DPF) и UK Extension to the EU-U.S. DPF, както и Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF), както е установено от U.S. Department of Commerce. Нашата компания е потвърдила пред Министерството на търговията на САЩ, че спазва EU-U.S. Data Privacy Framework Principles (EU-U.S. DPF Principles) по отношение на обработката на лични данни, които получава от Европейския съюз и Обединеното кралство на основание EU-U.S. DPF и UK Extension to the EU-U.S. DPF. Нашата компания е потвърдила пред


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

Министерството на търговията на САЩ, че спазва Swiss-U.S. Data Privacy Framework Principles (Swiss-U.S. DPF Principles) по отношение на обработката на лични данни, които получава от Швейцария на основание Swiss-U.S. DPF. В случай на противоречие между разпоредбите на нашата политика за поверителност и EU-U.S. DPF Principles и/или Swiss-U.S. DPF Principles, основните са Principles.

За да научите повече за програмата Data Privacy Framework (DPF) и за да видите нашата сертификация, моля, посетете https://www.dataprivacyframework.gov/.

Другите американски единици или дъщерни дружества на нашата компания, които също спазват EU-U.S. DPF Principles, включително UK Extension to the EU-U.S. DPF и Swiss-U.S. DPF Principles, ако има такива, са посочени в нашата политика за поверителност.

В съответствие с EU-U.S. DPF и UK Extension to the EU-U.S. DPF, както и Swiss-U.S. DPF, нашата компания се ангажира да сътрудничи с органите, създадени от европейските органи за защита на данните и британския Information Commissioner's Office (ICO), както и с швейцарския Federal Data Protection and Information Commissioner (EDÖB), и да спазва техните препоръки относно неразрешени жалби за нашето отношение към личните данни, които получаваме на основание EU-U.S. DPF и UK Extension to the EU-U.S. DPF и Swiss-U.S. DPF.

Информираме засегнатите лица за компетентните европейски органи за защита на данните, които отговарят за разглеждане на жалби относно отношението на нашата организация към лични данни в горната част на този документ за прозрачност и също така, че предоставяме на засегнатите лица адекватни и безплатни средства за правна защита.

Информираме всички засегнати лица, че нашата компания подлежи на разследващите и изпълнителните правомощия на Federal Trade Commission (FTC).

Засегнатите лица имат при определени условия възможността да поискат обвързващ арбитраж. Нашата организация е задължена да разрешава претенции и да спазва условията съгласно Приложение I на DPF-Principals, ако засегнатото лице е поискало обвързващ арбитраж, като е уведомило нашата организация и е спазило процедурите и условията съгласно Приложение I на Principles.

С настоящото информираме всички засегнати лица за отговорността на нашата организация в случай на предаване на лични данни на трети страни.

За въпроси на засегнатите лица или органите за надзор на защита на данните сме назначили местни представители, посочени в горната част на този документ за прозрачност.

Ние ви предлагаме възможността да изберете (Opt-out) дали вашите лични данни (i) да бъдат предадени на трети страни или (ii) да бъдат използвани за цел, която съществено се различава от целта (целите), за която (които) те първоначално са били събрани или по-късно одобрени от вас. Ясният, добре видим и леснодостъпен механизъм за упражняване на вашето право на избор


© All rights reserved by Heiko Maniero.

е да се свържете с нашия служител по защита на данните (DSB) по електронна поща. Нямате право на избор и ние също не сме задължени да го правим, ако данните се предават на трета страна, която действа като наш агент или обработващ данни от наше име и според нашите указания. Въпреки това, ние винаги сключваме договор с такъв агент или обработващ данни.

За чувствителни данни (т.е. лични данни, които съдържат информация за здравословното състояние, расовия или етническия произход, политическите възгледи, религиозните или философските убеждения, членството в профсъюз или информация за сексуалния живот на засегнатото лице), ние получаваме вашето изрично съгласие (Opt-in), ако тези данни (i) се предават на трети страни или (ii) се използват за друга цел, различна от първоначално събраната или от целта, за която сте дали своето съгласие, като сте направили избора си Opt-in. Освен това, ние третираме всички лични данни, които получаваме от трети страни, като чувствителни, ако третата страна ги идентифицира и обработва като чувствителни.

С настоящото ви информираме за изискването за разкриване на лични данни в отговор на законни искания от органите, включително изпълнение на изискванията за национална сигурност или правоприлагане.

При предаване на лични данни на трета страна, която действа като администратор на данни, спазваме Принципите за уведомление и избор (Principals). Също така сключваме договор с третата страна, отговорна за обработката, който предвижда тези данни да се обработват само за ограничени и определени цели в съответствие с вашето предоставено съгласие и че получателят осигурява същото ниво на защита като Принципите на DPF и ни уведомява, ако установи, че вече не може да изпълнява това задължение. Договорът предвижда, че третата страна, която действа като администратор, спира обработката или предприема други подходящи и адекватни мерки за отстраняване на проблема, ако се установи такава ситуация.

При предаване на лични данни на трета страна, която действа като агент или обработващ данни, (i) предаваме тези данни само за ограничени и определени цели; (ii) уверяваме се, че агентът или обработващият данни е задължен да осигури най-малко същото ниво на защита на данните, каквото изискват DPF-Principals; (iii) предприемаме подходящи и адекватни мерки, за да гарантираме, че агентът или обработващият данни действително обработва предадените лични данни по начин, който е в съответствие с нашите задължения съгласно DPF-Principals; (iv) изискваме от агента или обработващия данни да уведоми нашата организация, ако установи, че вече не може да изпълнява задължението си да осигури същото ниво на защита, каквото изискват DPF-Principals; (v) след уведомление, включително уведомление по точка (iv), предприемаме подходящи и адекватни мерки за спиране на неразрешената обработка и за отстраняване на проблема; и (vi) на искане предоставяме на DPF Department резюме или представителен екземпляр на съответните разпоредби за защита на данните в договора с този агент.

В съответствие с EU-U.S. DPF и/или UK Extension to the EU-U.S. DPF и/или Swiss-U.S. DPF, нашата организация се ангажира да сътрудничи с органите, създадени от европейските органи за защита


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

на данните и британския Information Commissioner's Office (ICO), както и с швейцарския Federal Data Protection and Information Commissioner (EDÖB), и да спазва техните препоръки относно неразрешени жалби за нашето отношение към лични данни във връзка с трудовите отношения, които получаваме на основание EU-U.S. DPF, UK Extension to the EU-U.S. DPF и Swiss-U.S. DPF.

Всички субекти на данни, които временно се намират в Европейския съюз (ЕС), Европейското икономическо пространство (ЕИП) или Обединеното кралство, или които имат местоживеене или обичайно пребиваване там, имат право на правата и правата на субектите на данни, които са публикувани в нашия Документ за прозрачност и които също така произтичат от членове 15-22 от ОРЗД, включително правото на достъп до лични данни. Предоставили сме тази информация на всички езици на ЕС и ЕИП. Версията на английски език се отнася за Обединеното кралство.

Всички субекти на данни, които временно пребивават в Швейцария или имат местоживеене или обичайно пребиваване там, имат право на права и права на субекта на данни съгласно швейцарския Закон за защита на данните (ЗЗД) и швейцарския Регламент за защита на данните (РЗД), които са публикувани в нашия Документ за прозрачност, включително правото на достъп до лични данни. Предоставили сме тази информация на трите официални езика на Швейцария (немски, италиански и френски).


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

# BULGARIAN: Информация за обработката на лични данни за служители и кандидати (член 13, 14 от ОРЗД)

Уважаеми господине или госпожо,

Личните данни на служителите и кандидатите заслужават специална защита. Нашата цел е да поддържаме високо ниво на защита на данните. Ето защо рутинно развиваме нашите концепции за защита и сигурност на данните.

Разбира се, ние спазваме законовите разпоредби за защита на данните. Съгласно членове 13, 14 от ОРЗД администраторите изпълняват конкретни изисквания за информация при обработката на лични данни. С настоящия документ се изпълняват тези задължения.

Терминологията на правното регулиране е сложна. За съжаление, при изготвянето на този документ не можеше да се избегне използването на правни термини. Ето защо бихме искали да отбележим, че винаги можете да се свържете с нас по всички въпроси, свързани с този документ, използваните термини или формулировки.

## I. Информация, предоставяна при събиране на лични данни от субекта на данните (член 13 от ОРЗД)

### A. данните, които идентифицират администратора и координатите за връзка с него и, когато е приложимо, тези на представителя на администратора (член 13, параграф 1, буква а) от ОРЗД)

Вижте по-горе

### B. координатите за връзка с длъжностното лице по защита на данните, когато е приложимо (член 13, параграф 1, буква б) от ОРЗД)

Вижте по-горе

### C. целите на обработването, за което личните данни са предназначени, както и правното основание за обработването (член 13, параграф 1, буква в) от ОРЗД)

Целта на обработката на данните на кандидатите е да се извърши проверка на кандидатурата по време на процеса на набиране на персонал. За тази цел обработваме всички предоставени от вас


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

данни. Въз основа на данните, предоставени по време на процеса на набиране на персонал, ще проверим дали сте поканени на интервю за работа (част от процеса на подбор). В случай на общо взето подходящи кандидати, по-специално в контекста на интервюто за работа, ние обработваме някои други лични данни, предоставени от вас, които са от съществено значение за нашето решение за подбор. Ако бъдете наети от нас, данните на кандидата автоматично се променят в данни на служителя. Като част от процеса на набиране на персонал ще обработваме други Ваши лични данни, които изискваме от Вас и които са необходими за започване или изпълнение на договора (като например лични идентификационни номера или данъчни номера). За данните на служителите целта на обработката на данните е изпълнението на трудовия договор или спазването на други законови разпоредби, приложими към трудовото правоотношение (напр. данъчното законодателство), както и използването на Вашите лични данни за изпълнение на сключения с Вас трудов договор (напр. публикуване на Вашето име и информация за контакт в рамките на компанията или пред клиенти). Данните на служителите се съхраняват след прекратяване на трудовото правоотношение, за да се спазят законовите срокове за съхранение.

Правното основание за обработката на данни е член 6, параграф 1, буква б) от ОРЗД, член 9, параграф 2, букви б) и з) от ОРЗД, член 88, параграф 1 от ОРЗД и националното законодателство, като например в Германия член 26 от BDSG (Федерален закон за защита на данните).

## D. получателите или категориите получатели на личните данни, ако има такива (член 13, параграф 1, буква д) от ОРЗД)

Публични органи

Външни органи

Други външни органи

Вътрешна обработка

Вътрешногрупова обработка

Други органи

Списък на нашите обработващи и получатели на данни в трети държави и, ако е приложимо, на международни организации е публикуван на нашия уебсайт или може да бъде поискан от нас безплатно. Моля, свържете се с нашето длъжностно лице по защита на данните, за да поискате този списък.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## E. когато е приложимо, намерението на администратора да предаде личните данни на трета държава или на международна организация, както и наличието или отсъствието на решение на Комисията относно адекватното ниво на защита или в случай на предаване на данни съгласно посоченото в членове 46 или 47, или член 49, параграф 1, втора алинея позоваване на подходящите или приложимите гаранции и средствата за получаване на копие от тях или на информация къде са налични (член 13, параграф 1, буква е).

Всички дружества и клонове, които са част от нашата група (наричани по-долу "дружества от групата"), които имат място на стопанска дейност или офис в трета държава, могат да бъдат получатели на лични данни. Списък на всички дружества от групата или получатели може да бъде поискан от нас.

Съгласно член 46, параграф 1 от ОРЗД администратор или обработващ лични данни може да предава лични данни на трета държава само ако е осигурил подходящи гаранции и при условие че са налице изпълними права на субекта на данни и ефективни правни средства за защита на субектите на данни. Подходящи гаранции могат да бъдат предоставени, без да се изисква специално разрешение от надзорния орган, посредством стандартни договорни клаузи, член 46, параграф 2, буква в) от ОРЗД.

Стандартните договорни клаузи на Европейския съюз или други подходящи предпазни мерки се договарят с всички получатели от трети държави преди първото предаване на лични данни. В резултат на това се гарантира, че са осигурени подходящи гаранции, изпълними права на субектите на данни и ефективни правни средства за защита на субектите на данни. Всеки субект на данни може да получи от нас копие от стандартните договорни клаузи. Стандартните договорни клаузи са на разположение и в Официален вестник на Европейския съюз.

Член 45, параграф 3 от Общия регламент относно защитата на данните (ОРЗД) предоставя на Европейската комисия правото да реши чрез акт за изпълнение, че държава извън ЕС осигурява адекватно ниво на защита. Това означава ниво на защита на личните данни, което в общи линии е еквивалентно на това в ЕС. Резултатът от решенията, с които се установява адекватно ниво на защита, е, че личните данни могат да се пренасят свободно от ЕС (и Норвегия, Лихтенщайн и Исландия) в трета държава без допълнителни пречки. Подобни правила се прилагат в Обединеното кралство, Швейцария и някои други държави.

В случай че Европейската комисия или правителството на друга държава реши, че трета държава осигурява адекватно ниво на защита, и приложимата рамка (например EU-U.S. Data Privacy Framework, Swiss-U.S. Data Privacy Framework, UK Extension to the EU-U.S. Data Privacy Framework), всички трансфери от нас към членове на такива рамки (например самосертифицирани субекти) се основават единствено на членството на тези субекти в съответната рамка. В случай че ние или някое от нашите образувания от групата е член на такава


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

рамка, всички прехвърляния към нас или към образувание от нашата група се основават единствено на членството на образуването в такава рамка.

Всеки субект на данни може да получи от нас копие от рамката. Освен това рамките са достъпни и в Официален вестник на Европейския съюз или в публикуваните правни материали, или на уебсайтовете на надзорните органи или други компетентни органи или институции.

## F. срока, за който ще се съхраняват личните данни, а ако това е невъзможно, критериите, използвани за определяне на този срок (член 13, параграф 2, буква а) от ОРЗД)

Срокът за съхранение на личните данни на кандидатите е 6 месеца. За данните на служителите се прилага съответният законоустановен период на съхранение. След изтичането на този период съответните данни се изтриват рутинно, ако вече не са необходими за изпълнението на договора или за започването на договор.

## G. съществуването на право да се изиска от администратора достъп до, коригиране или изтриване на лични данни или ограничаване на обработването на лични данни, свързани със субекта на данните, или право да се направи възражение срещу обработването, както и правото на преносимост на данните (член 13, параграф 2, буква б) от ОРЗД)

Всички субекти на данни имат следните права:

***Право на достъп***

Всеки субект на данни има право на достъп до личните данни, които го засягат. Правото на достъп се отнася за всички данни, обработвани от нас. Правото може да се упражнява лесно и на разумни интервали от време, за да се запознаете и да проверите законосъобразността на обработката (съображение 63 от ОРЗД). Това право произтича от чл. 15 ОТ ОРЗД. Субектът на данните може да се свърже с нас, за да упражни правото си на достъп.

***Право на коригиране***

Съгласно член 16, изречение 1 от ОРЗД субектът на данните има право да получи от администратора без ненужно забавяне коригирането на неточни лични данни, които го засягат. Освен това член 16, изречение 2 от ОРЗД предвижда, че субектът на данните има право, като се вземат предвид целите на обработването, да поиска непълните лични данни да бъдат попълнени, включително чрез предоставяне на допълнителна декларация. Субектът на данните може да се свърже с нас, за да упражни правото си на коригиране.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

***Право на изтриване (право да бъдеш забравен)***

Освен това субектите на данни имат право на право на изтриване и забравяне съгласно чл. 17 ОТ ОРЗД. Това право също може да бъде упражнено, като се свържете с нас. На това място обаче бихме искали да посочим, че това право не се прилага, доколкото обработването е необходимо за изпълнение на правно задължение, на което нашето дружество е подчинено, член 17, параграф 3, буква б) от ОРЗД. Това означава, че можем да одобрим заявлението за изтриване само след изтичане на законоустановения период на съхранение.

***Право на ограничаване на обработката***

Съгласно член 18 от ОРЗД всеки субект на данни има право на ограничаване на обработката. Ограничаване на обработването може да се поиска, ако е изпълнено едно от условията, посочени в член 18, параграф 1, буква а-г от ОРЗД. Субектът на данни може да се свърже с нас, за да упражни правото си на ограничаване на обработката.

***Право на възражение***

Освен това чл. 21 от ОРЗД се гарантира правото на възражение. Субектът на данните може да се свърже с нас, за да упражни правото си на възражение.

***Право на преносимост на данните***

Чл. 20 от ОРЗД предоставя на субекта на данните правото на преносимост на данните. Съгласно тази разпоредба субектът на данните има право при условията, предвидени в член 20, параграф 1, букви а) и б) от ОРЗД, да получи личните данни, които го засягат и които той е предоставил на администратор, в структуриран, широко използван и пригоден за машинно четене формат, както и да предаде тези данни на друг администратор, без да бъде възпрепятстван от администратора, на когото са предоставени личните данни. Субектът на данните може да се свърже с нас, за да упражни правото си на преносимост на данните.

## Н. когато обработването се основава на член 6, параграф 1, буква а) или член 9, параграф 2, буква а), съществуването на право на оттегляне на съгласието по всяко време, без да се засяга законосъобразността на обработването въз основа на съгласие, преди то да бъде оттеглено (член 13, параграф 2, буква в) от ОРЗД)

Ако обработката на лични данни се основава на чл. 6, параграф 1, буква а) от ОРЗД, какъвто е случаят, ако субектът на данните е дал съгласие за обработване на лични данни за една или повече конкретни цели, или се основава на член 9, параграф 2, буква а) от ОРЗД, който урежда изричното съгласие за обработване на специални категории лични данни, субектът на данните има право съгласно член 7, параграф 3, изречение 1 от ОРЗД да оттегли съгласието си по всяко време.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

Оттеглянето на съгласието не засяга законосъобразността на обработването, основано на съгласието преди неговото оттегляне, член 7, параграф 3, изречение 2 от ОРЗД. Оттеглянето на съгласието трябва да бъде толкова лесно, колкото и даването му, чл. 7, параграф 3, изречение 4 от ОРЗД. Следователно оттеглянето на съгласието винаги може да се извърши по същия начин, по който е дадено съгласието, или по друг начин, който субектът на данните счита за по-лесен. В днешното информационно общество вероятно най-простият начин за оттегляне на съгласието е обикновено електронно писмо. Ако субектът на данните желае да оттегли съгласието, което ни е дал, е достатъчно да ни изпрати просто имейл. Като алтернатива субектът на данните може да избере друг начин да ни съобщи за оттеглянето на съгласието си.

## I. правото на жалба до надзорен орган (член 13, параграф 2, буква г) и член 77, параграф 1 от ОРЗД)

В качеството си на администратор сме длъжни да уведомим субекта на данните за правото му да подаде жалба до надзорен орган, член 13, параграф 2, буква г) от ОРЗД. Правото на подаване на жалба до надзорен орган е уредено в член 77, параграф 1 от ОРЗД. Съгласно тази разпоредба, без да се засягат други административни или съдебни средства за защита, всеки субект на данни има право да подаде жалба до надзорен орган, по-специално в държавата членка на обичайното си местопребиваване, място на работа или място на предполагаемото нарушение, ако субектът на данни счита, че обработването на лични данни, свързани с него, нарушава Общия регламент относно защитата на данните. Правото на подаване на жалба до надзорен орган беше ограничено от правото на Съюза по такъв начин, че то може да бъде упражнено само пред един надзорен орган (съображение 141, изречение 1 от Общия регламент относно защитата на данните). Това правило има за цел да се избегнат двойни жалби на един и същ субект на данни по един и същ въпрос. Ето защо, ако субект на данни иска да подаде жалба срещу нас, ние го молим да се обърне само към един-единствен надзорен орган.

## J. дали предоставянето на лични данни е задължително или договорно изискване, или изискване, необходимо за сключването на договор, както и дали субектът на данните е длъжен да предостави личните данни и евентуалните последствия, ако тези данни не бъдат предоставени (член 13, параграф 2, буква д) от ОРЗД)

Поясняваме, че предоставянето на лични данни се изисква отчасти по закон (напр. данъчни разпоредби) или може да произтича от договорни разпоредби (напр. информация за договорния партньор).

Понякога може да е необходимо за сключването на договор субектът на данните да ни предостави лични данни, които впоследствие трябва да бъдат обработени от нас. Субектът на данни


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

например е длъжен да ни предостави лични данни, когато нашето дружество сключва договор с него. Непредоставянето на личните данни би имало за последица невъзможността да се сключи договор със субекта на данните.

Преди субектът на данните да предостави личните си данни, той трябва да се свърже с нас. Ние разясняваме на субекта на данните дали предоставянето на личните данни се изисква по закон или договор или е необходимо за сключването на договора, дали съществува задължение за предоставяне на личните данни и какви са последиците от непредоставянето на личните данни.

### K. съществуването на автоматизирано вземане на решения, включително профилирането, посочено в член 22, параграфи 1 и 4, и поне в тези случаи съществена информация относно използваната логика, както и значението и предвидените последствия от това обработване за субекта на данните (член 13, параграф 2, буква е) от ОРЗД)

Като отговорна компания обикновено не използваме автоматизирано вземане на решения или профилиране. Ако в изключителни случаи извършваме автоматизирано вземане на решения или профилиране, ще информираме субекта на данните отделно или чрез подраздел в нашата политика за поверителност (на нашия уебсайт). В този случай се прилага следното:

Автоматизирано вземане на решения - включително профилиране - може да се извърши, ако (1) това е необходимо за сключването или изпълнението на договор между субекта на данните и нас, или (2) това е разрешено от правото на Съюза или на държава членка, което се прилага спрямо нас и в което също така са предвидени подходящи мерки за защита на правата и свободите и законните интереси на субекта на данните; или (3) това се основава на изричното съгласие на субекта на данните.

В случаите, посочени в член 22, параграф 2, букви а) и в) от ОРЗД, ние прилагаме подходящи мерки за защита на правата и свободите и законните интереси на субекта на данните. В тези случаи имате право да получите човешка намеса от страна на администратора, да изразите своята гледна точка и да оспорите решението.

Съществена информация за използваната логика, както и за значението и предвидените последици от това обработване за субекта на данните, е изложена в нашата политика за поверителност.

## II. Информация, предоставяна, когато личните данни идват от субекта на данните (член 14 от ОРЗД)


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## A. данните, които идентифицират администратора и координатите за връзка с него и, когато е приложимо, тези на представителя на администратора (член 14, параграф 1, буква а) от ОРЗД)

Вижте по-горе

## B. координатите за връзка с длъжностното лице по защита на данните, когато е приложимо (член 14, параграф 1, буква б) от ОРЗД)

Вижте по-горе

## C. целите на обработването, за което личните данни са предназначени, както и правното основание за обработването (член 14, параграф 1, буква в) от ОРЗД)

За данните на кандидата, които не са събрани от субекта на данните, целта на обработката на данните е да се извърши проверка на кандидатурата по време на процеса на набиране на персонал. За тази цел може да обработваме данни, които не са събрани от вас. Въз основа на данните, обработени по време на процеса на набиране на персонал, ще проверим дали сте поканени на интервю за работа (част от процеса на подбор). Ако бъдете наети от нас, данните на кандидата автоматично ще се превърнат в данни на служителя. За данните на служителите целта на обработката на данни е изпълнението на трудовия договор или спазването на други законови разпоредби, приложими към трудовото правоотношение. Данните на служителите се съхраняват след прекратяване на трудовото правоотношение, за да се спазят законовите срокове за съхранение.

Правното основание за обработката на данни е член 6, параграф 1, букви б и е от ОРЗД, член 9, параграф 2, букви б и з от ОРЗД, член 88, параграф 1 от ОРЗД и националното законодателство, като например в Германия член 26 от BDSG (Федерален закон за защита на данните).

## D. съответните категории лични данни (член 14, параграф 1, буква г) от ОРЗД)

Данни на заявителя

Данни за служителите


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## E. получателите или категориите получатели на личните данни, ако има такива (член 14, параграф 1, буква д) от ОРЗД)

Публични органи

Външни органи

Други външни органи

Вътрешна обработка

Вътрешногрупова обработка

Други органи

Списък на нашите обработващи и получатели на данни в трети държави и, ако е приложимо, на международни организации е публикуван на нашия уебсайт или може да бъде поискан от нас безплатно. Моля, свържете се с нашето длъжностно лице по защита на данните, за да поискате този списък.

## F. когато е приложимо, намерението на администратора да предаде данните на трета държава или на международна организация, и наличието или отсъствието на решение на Комисията относно адекватното ниво на защита или в случай на предаване на данни съгласно член 46 или 47, или член 49, параграф 1, втора алинея с позоваване на подходящите или приложимите гаранции и средствата за получаване на копие от тях или на информация къде са налични (член 14, параграф 1, буква е).

Всички дружества и клонове, които са част от нашата група (наричани по-долу "дружества от групата"), които имат място на стопанска дейност или офис в трета държава, могат да бъдат получатели на лични данни. Списък на всички дружества от групата или получатели може да бъде поискан от нас.

Съгласно член 46, параграф 1 от ОРЗД администратор или обработващ лични данни може да предава лични данни на трета държава само ако е осигурил подходящи гаранции и при условие че са налице изпълними права на субекта на данни и ефективни правни средства за защита на субектите на данни. Подходящи гаранции могат да бъдат предоставени, без да се изисква специално разрешение от надзорния орган, посредством стандартни клаузи за защита на данните, член 46, параграф 2, буква в) от ОРЗД.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

Стандартните договорни клаузи на Европейския съюз или други подходящи предпазни мерки се договарят с всички получатели от трети държави преди първото предаване на лични данни. В резултат на това се гарантира, че са осигурени подходящи гаранции, изпълними права на субектите на данни и ефективни правни средства за защита на субектите на данни. Всеки субект на данни може да получи от нас копие от стандартните договорни клаузи. Стандартните договорни клаузи са достъпни и в Официален вестник на Европейския съюз.

Член 45, параграф 3 от Общия регламент относно защитата на данните (ОРЗД) предоставя на Европейската комисия правото да реши чрез акт за изпълнение, че държава извън ЕС осигурява адекватно ниво на защита. Това означава ниво на защита на личните данни, което в общи линии е еквивалентно на това в ЕС. Резултатът от решенията, с които се установява адекватно ниво на защита, е, че личните данни могат да се пренасят свободно от ЕС (и Норвегия, Лихтенщайн и Исландия) в трета държава без допълнителни пречки. Подобни правила се прилагат в Обединеното кралство, Швейцария и някои други държави.

В случай че Европейската комисия или правителството на друга държава реши, че трета държава осигурява адекватно ниво на защита, и приложимата рамка (например EU-U.S. Data Privacy Framework, Swiss-U.S. Data Privacy Framework, UK Extension to the EU-U.S. Data Privacy Framework), всички трансфери от нас към членове на такива рамки (например самосертифицирани субекти) се основават единствено на членството на тези субекти в съответната рамка. В случай че ние или някое от нашите образувания от групата е член на такава рамка, всички прехвърляния към нас или към образувание от нашата група се основават единствено на членството на образуването в такава рамка.

Всеки субект на данни може да получи от нас копие от рамката. Освен това рамките са достъпни и в Официален вестник на Европейския съюз или в публикуваните правни материали, или на уебсайтовете на надзорните органи или други компетентни органи или институции.

## G. срока, за който ще се съхраняват личните данни, а ако това е невъзможно, критериите, използвани за определяне на този срок (член 14, параграф 2, буква а) от ОРЗД)

Срокът за съхранение на личните данни на кандидатите е 6 месеца. За данните на служителите се прилага съответният законоустановен период на съхранение. След изтичането на този период съответните данни се изтриват рутинно, ако вече не са необходими за изпълнението на договора или за започването на договор.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## H. когато обработването се извършва въз основа на член 6, параграф 1, буква е), законните интереси, преследвани от администратора или от трета страна (член 14, параграф 2, буква б) от ОРЗД)

В съответствие с член 6, параграф 1, буква е) от ОРЗД обработването е законосъобразно само ако е необходимо за целите на законните интереси на администратора или на трета страна, освен когато пред тези интереси преимущество имат интересите или основните права и свободи на субекта на данните, които изискват защита на личните данни. Съгласно съображение 47, изречение 2 от ОРЗД легитимен интерес би могъл да съществува, когато между субекта на данните и администратора съществува съответна и подходяща връзка, например в ситуации, в които субектът на данните е клиент на администратора. Във всички случаи, в които нашето дружество обработва данни на кандидати въз основа на член 6, параграф 1, буква е) от ОРЗД, нашият легитимен интерес е наемането на работа на подходящ персонал и специалисти.

## I. съществуването на право да се изиска от администратора достъп до, коригиране или изтриване на лични данни, свързани със субекта на данните, или ограничаване на обработването, и правото да се направи възражение срещу обработването, както и правото на преносимост на данните (член 14, параграф 2, буква в) от ОРЗД)

Всички субекти на данни имат следните права:

***Право на достъп***

Всеки субект на данни има право на достъп до личните данни, които го засягат. Правото на достъп се отнася за всички данни, обработвани от нас. Правото може да бъде упражнено лесно и на разумни интервали от време, за да се запознаете и да проверите законосъобразността на обработката (съображение 63 от ОРЗД). Това право произтича от чл. 15 ОТ ОРЗД. Субектът на данните може да се свърже с нас, за да упражни правото си на достъп.

***Право на коригиране***

Съгласно член 16, изречение 1 от ОРЗД субектът на данните има право да получи от администратора без ненужно забавяне коригирането на неточни лични данни, отнасящи се до него. Освен това член 16, изречение 2 от ОРЗД предвижда, че субектът на данните има право, като се вземат предвид целите на обработването, да поиска непълните лични данни да бъдат попълнени, включително чрез предоставяне на допълнителна декларация. Субектът на данните може да се свърже с нас, за да упражни правото си на коригиране.

***Право на изтриване (право да бъдеш забравен)***

Освен това субектите на данни имат право на право на изтриване и забравяне съгласно чл. 17 ОТ ОРЗД. Това право също може да бъде упражнено, като се свържете с нас. На това място обаче бихме искали да посочим, че това право не се прилага, доколкото обработването е необходимо


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

за изпълнение на правно задължение, на което нашето дружество е подчинено, член 17, параграф 3, буква б) от ОРЗД. Това означава, че можем да одобрим заявлението за изтриване само след изтичане на законоустановения период на съхранение.

***Право на ограничаване на обработката***

Съгласно член 18 от ОРЗД всеки субект на данни има право на ограничаване на обработката. Ограничаване на обработването може да се поиска, ако е изпълнено едно от условията, посочени в член 18, параграф 1, буква а-г от ОРЗД. Субектът на данни може да се свърже с нас, за да упражни правото си на ограничаване на обработката.

***Право на възражение***

Освен това чл. 21 от ОРЗД се гарантира правото на възражение. Субектът на данните може да се свърже с нас, за да упражни правото си на възражение.

***Право на преносимост на данните***

Чл. 20 от ОРЗД предоставя на субекта на данните правото на преносимост на данните. Съгласно тази разпоредба субектът на данни има право при условията, предвидени в член 20, параграф 1, букви а) и б) от ОРЗД, да получи личните данни, които го засягат и които той е предоставил на администратор, в структуриран, широко използван и пригоден за машинно четене формат, както и да предаде тези данни на друг администратор, без да бъде възпрепятстван от администратора, на когото са предоставени личните данни. Субектът на данните може да се свърже с нас, за да упражни правото си на преносимост на данните.

## J. когато обработването се основава на член 6, параграф 1, буква а) или член 9, параграф 2, буква а), съществуването на право на оттегляне на съгласието по всяко време, без да се засяга законосъобразността на обработването въз основа на съгласие, преди то да бъде оттеглено (член 14, параграф 2, буква г) от ОРЗД)

Ако обработката на лични данни се основава на чл. 6, параграф 1, буква а) от ОРЗД, какъвто е случаят, ако субектът на данните е дал съгласие за обработване на лични данни за една или повече конкретни цели, или се основава на член 9, параграф 2, буква а) от ОРЗД, който урежда изричното съгласие за обработване на специални категории лични данни, субектът на данните има право съгласно член 7, параграф 3, изречение 1 от ОРЗД да оттегли съгласието си по всяко време.

Оттеглянето на съгласието не засяга законосъобразността на обработването, основано на съгласието преди неговото оттегляне, член 7, параграф 3, изречение 2 от ОРЗД. Оттеглянето на съгласието трябва да бъде толкова лесно, колкото и даването му, чл. 7, параграф 3, изречение 4 от ОРЗД. Следователно оттеглянето на съгласието винаги може да се извърши по същия начин, по който е дадено съгласието, или по друг начин, който субектът на данните счита за по-лесен. В


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

днешното информационно общество вероятно най-простият начин за оттегляне на съгласието е обикновено електронно писмо. Ако субектът на данните желае да оттегли съгласието си, което ни е дал, е достатъчно да ни изпрати обикновен имейл. Като алтернатива субектът на данните може да избере друг начин да ни съобщи за оттеглянето на съгласието си.

## K. правото на жалба до надзорен орган (член 14, параграф 2, буква д) и член 77, параграф 1 от ОРЗД)

В качеството си на администратор сме длъжни да уведомим субекта на данните за правото му да подаде жалба до надзорен орган, член 14, параграф 2, буква д) от ОРЗД. Правото на подаване на жалба до надзорен орган е уредено в член 77, параграф 1 от ОРЗД. Съгласно тази разпоредба, без да се засягат други административни или съдебни средства за защита, всеки субект на данни има право да подаде жалба до надзорен орган, по-специално в държавата членка на обичайното си местопребиваване, място на работа или място на предполагаемото нарушение, ако субектът на данни счита, че обработването на лични данни, свързани с него, нарушава Общия регламент относно защитата на данните. Правото на подаване на жалба до надзорен орган беше ограничено от правото на Съюза по такъв начин, че то може да бъде упражнено само пред един надзорен орган (съображение 141, изречение 1 от Общия регламент относно защитата на данните). Това правило има за цел да се избегнат двойни жалби на един и същ субект на данни по един и същ въпрос. Ето защо, ако субект на данни иска да подаде жалба срещу нас, ние го молим да се обърне само към един-единствен надзорен орган.

## L. източника на личните данни и, ако е приложимо, дали данните са от публично достъпен източник (член 14, параграф 2, буква е) от ОРЗД)

По принцип личните данни се събират директно от субекта на данните или в сътрудничество с орган (напр. извличане на данни от официален регистър). Други данни за субектите на данни се извличат от трансфери на дружества от групата. В контекста на тази обща информация посочването на точните източници, от които произхождат личните данни, е или невъзможно, или би изисквало непропорционални усилия по смисъла на чл. 14, параграф 5, буква б) от ОРЗД. По принцип ние не събираме лични данни от публично достъпни източници.

Всеки субект на данни може да се свърже с нас по всяко време, за да получи по-подробна информация за точните източници на личните данни, които го засягат. Когато произходът на личните данни не може да бъде предоставен на субекта на данните, тъй като са използвани различни източници, следва да се предостави обща информация (съображение 61, изречение 4 от ОРЗД).


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

### M. съществуването на автоматизирано вземане на решения, включително профилирането, посочено в член 22, параграфи 1 и 4, и поне в тези случаи съществена информация относно използваната логика, както и значението и предвидените последствия от това обработване за субекта на данните (член 14, параграф 2, буква ж от ОРЗД)

Като отговорна компания обикновено не използваме автоматизирано вземане на решения или профилиране. Ако в изключителни случаи извършваме автоматизирано вземане на решения или профилиране, ще информираме субекта на данните отделно или чрез подраздел в нашата политика за поверителност (на нашия уебсайт). В този случай се прилага следното:

Автоматизирано вземане на решения - включително профилиране - може да се извърши, ако (1) това е необходимо за сключването или изпълнението на договор между субекта на данните и нас, или (2) това е разрешено от правото на Съюза или на държава членка, което се прилага спрямо нас и в което също така са предвидени подходящи мерки за защита на правата и свободите и законните интереси на субекта на данните; или (3) това се основава на изричното съгласие на субекта на данните.

В случаите, посочени в член 22, параграф 2, букви а) и в) от ОРЗД, ние прилагаме подходящи мерки за защита на правата и свободите и законните интереси на субекта на данните. В тези случаи имате право да получите човешка намеса от страна на администратора, да изразите своята гледна точка и да оспорите решението.

Съществена информация за използваната логика, както и за значението и предвидените последици от това обработване за субекта на данните, е изложена в нашата политика за поверителност.

## III. EU-U.S. Data Privacy Framework (EU-U.S. DPF), UK Extension to the EU-U.S. DPF, Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF)

Ако нашата организация е сертифициран член на EU-U.S. Data Privacy Framework (EU-U.S. DPF) и/или на UK Extension to the EU-U.S. DPF и/или на Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF), се прилага следното:

Ние спазваме EU-U.S. Data Privacy Framework (EU-U.S. DPF) и UK Extension to the EU-U.S. DPF, както и Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF), както е установено от U.S. Department of Commerce. Нашата компания е потвърдила пред Министерството на търговията на САЩ, че спазва EU-U.S. Data Privacy Framework Principles (EU-U.S. DPF Principles) по отношение на обработката на лични данни, които получава от Европейския съюз и Обединеното кралство на основание EU-U.S. DPF и UK Extension to the EU-U.S. DPF. Нашата компания е потвърдила пред


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

Министерството на търговията на САЩ, че спазва Swiss-U.S. Data Privacy Framework Principles (Swiss-U.S. DPF Principles) по отношение на обработката на лични данни, които получава от Швейцария на основание Swiss-U.S. DPF. В случай на противоречие между разпоредбите на нашата политика за поверителност и EU-U.S. DPF Principles и/или Swiss-U.S. DPF Principles, основните са Principles.

За да научите повече за програмата Data Privacy Framework (DPF) и за да видите нашата сертификация, моля, посетете https://www.dataprivacyframework.gov/.

Другите американски единици или дъщерни дружества на нашата компания, които също спазват EU-U.S. DPF Principles, включително UK Extension to the EU-U.S. DPF и Swiss-U.S. DPF Principles, ако има такива, са посочени в нашата политика за поверителност.

В съответствие с EU-U.S. DPF и UK Extension to the EU-U.S. DPF, както и Swiss-U.S. DPF, нашата компания се ангажира да сътрудничи с органите, създадени от европейските органи за защита на данните и британския Information Commissioner's Office (ICO), както и с швейцарския Federal Data Protection and Information Commissioner (EDÖB), и да спазва техните препоръки относно неразрешени жалби за нашето отношение към личните данни, които получаваме на основание EU-U.S. DPF и UK Extension to the EU-U.S. DPF и Swiss-U.S. DPF.

Информираме засегнатите лица за компетентните европейски органи за защита на данните, които отговарят за разглеждане на жалби относно отношението на нашата организация към лични данни в горната част на този документ за прозрачност и също така, че предоставяме на засегнатите лица адекватни и безплатни средства за правна защита.

Информираме всички засегнати лица, че нашата компания подлежи на разследващите и изпълнителните правомощия на Federal Trade Commission (FTC).

Засегнатите лица имат при определени условия възможността да поискат обвързващ арбитраж. Нашата организация е задължена да разрешава претенции и да спазва условията съгласно Приложение I на DPF-Principals, ако засегнатото лице е поискало обвързващ арбитраж, като е уведомило нашата организация и е спазило процедурите и условията съгласно Приложение I на Principles.

С настоящото информираме всички засегнати лица за отговорността на нашата организация в случай на предаване на лични данни на трети страни.

За въпроси на засегнатите лица или органите за надзор на защита на данните сме назначили местни представители, посочени в горната част на този документ за прозрачност.

Ние ви предлагаме възможността да изберете (Opt-out) дали вашите лични данни (i) да бъдат предадени на трети страни или (ii) да бъдат използвани за цел, която съществено се различава от целта (целите), за която (които) те първоначално са били събрани или по-късно одобрени от вас. Ясният, добре видим и леснодостъпен механизъм за упражняване на вашето право на избор


© All rights reserved by Heiko Maniero.

е да се свържете с нашия служител по защита на данните (DSB) по електронна поща. Нямате право на избор и ние също не сме задължени да го правим, ако данните се предават на трета страна, която действа като наш агент или обработващ данни от наше име и според нашите указания. Въпреки това, ние винаги сключваме договор с такъв агент или обработващ данни.

За чувствителни данни (т.е. лични данни, които съдържат информация за здравословното състояние, расовия или етническия произход, политическите възгледи, религиозните или философските убеждения, членството в профсъюз или информация за сексуалния живот на засегнатото лице), ние получаваме вашето изрично съгласие (Opt-in), ако тези данни (i) се предават на трети страни или (ii) се използват за друга цел, различна от първоначално събраната или от целта, за която сте дали своето съгласие, като сте направили избора си Opt-in. Освен това, ние третираме всички лични данни, които получаваме от трети страни, като чувствителни, ако третата страна ги идентифицира и обработва като чувствителни.

С настоящото ви информираме за изискването за разкриване на лични данни в отговор на законни искания от органите, включително изпълнение на изискванията за национална сигурност или правоприлагане.

При предаване на лични данни на трета страна, която действа като администратор на данни, спазваме Принципите за уведомление и избор (Principals). Също така сключваме договор с третата страна, отговорна за обработката, който предвижда тези данни да се обработват само за ограничени и определени цели в съответствие с вашето предоставено съгласие и че получателят осигурява същото ниво на защита като Принципите на DPF и ни уведомява, ако установи, че вече не може да изпълнява това задължение. Договорът предвижда, че третата страна, която действа като администратор, спира обработката или предприема други подходящи и адекватни мерки за отстраняване на проблема, ако се установи такава ситуация.

При предаване на лични данни на трета страна, която действа като агент или обработващ данни, (i) предаваме тези данни само за ограничени и определени цели; (ii) уверяваме се, че агентът или обработващият данни е задължен да осигури най-малко същото ниво на защита на данните, каквото изискват DPF-Principals; (iii) предприемаме подходящи и адекватни мерки, за да гарантираме, че агентът или обработващият данни действително обработва предадените лични данни по начин, който е в съответствие с нашите задължения съгласно DPF-Principals; (iv) изискваме от агента или обработващия данни да уведоми нашата организация, ако установи, че вече не може да изпълнява задължението си да осигури същото ниво на защита, каквото изискват DPF-Principals; (v) след уведомление, включително уведомление по точка (iv), предприемаме подходящи и адекватни мерки за спиране на неразрешената обработка и за отстраняване на проблема; и (vi) на искане предоставяме на DPF Department резюме или представителен екземпляр на съответните разпоредби за защита на данните в договора с този агент.

В съответствие с EU-U.S. DPF и/или UK Extension to the EU-U.S. DPF и/или Swiss-U.S. DPF, нашата организация се ангажира да сътрудничи с органите, създадени от европейските органи за защита


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

на данните и британския Information Commissioner's Office (ICO), както и с швейцарския Federal Data Protection and Information Commissioner (EDÖB), и да спазва техните препоръки относно неразрешени жалби за нашето отношение към лични данни във връзка с трудовите отношения, които получаваме на основание EU-U.S. DPF, UK Extension to the EU-U.S. DPF и Swiss-U.S. DPF.

Всички субекти на данни, които временно се намират в Европейския съюз (ЕС), Европейското икономическо пространство (ЕИП) или Обединеното кралство, или които имат местоживеене или обичайно пребиваване там, имат право на правата и правата на субектите на данни, които са публикувани в нашия Документ за прозрачност и които също така произтичат от членове 15-22 от ОРЗД, включително правото на достъп до лични данни. Предоставили сме тази информация на всички езици на ЕС и ЕИП. Версията на английски език се отнася за Обединеното кралство.

Всички субекти на данни, които временно пребивават в Швейцария или имат местоживеене или обичайно пребиваване там, имат право на права и права на субекта на данни съгласно швейцарския Закон за защита на данните (ЗЗД) и швейцарския Регламент за защита на данните (РЗД), които са публикувани в нашия Документ за прозрачност, включително правото на достъп до лични данни. Предоставили сме тази информация на трите официални езика на Швейцария (немски, италиански и френски).


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

# ESTONIAN: Teave isikuandmete töötlemise kohta (GDPR artiklid 13, 14)

Lugupeetud härra või proua,

Iga isiku, kes on meie ettevõttega lepingulises, lepingueelses või muus suhtes, isikuandmed väärivad erilist kaitset. Meie eesmärk on hoida meie andmekaitse tase kõrgel tasemel. Seetõttu arendame rutiinselt oma andmekaitse- ja andmeturbe kontseptsioone.

Loomulikult järgime me seaduslikke sätteid andmekaitse kohta. Vastavalt GDPR artiklitele 13, 14 peavad vastutavad töötlejad isikuandmete kogumisel vastama konkreetsetele teavitamisnõuetele. Käesolev dokument täidab neid kohustusi.

Õigusaktide terminoloogia on keeruline. Kahjuks ei saanud käesoleva dokumendi koostamisel loobuda juriidiliste terminite kasutamisest. Seetõttu soovime juhtida tähelepanu sellele, et olete alati oodatud meiega ühendust võtma kõigi küsimuste korral, mis puudutavad käesolevat dokumenti, kasutatud termineid või sõnastusi.

## I. Teave, mis tuleb anda juhul, kui isikuandmed on kogutud andmesubjektilt (GDPR artikkel 13)

### A. Vastutava töötleja ning kui kohaldatav, siis vastutava töötleja esindaja nimi ja kontaktandmed (GDPR artikli 13 lõike 1 punkt a)

Vt eespool

### B. Asjakohasel juhul andmekaitseametniku kontaktandmed (isikuandmete kaitse üldmääruse artikli 13 lõike 1 punkt b).

Vt eespool

### C. Isikuandmete töötlemise eesmärk ja õiguslik alus (isikuandmete kaitse üldmääruse artikli 13 lõike 1 punkt c).

Isikuandmete töötlemise eesmärk on kõikide toimingute tegemine, mis on seotud vastutava töötleja, klientide, potentsiaalsete klientide, äripartnerite või muude lepinguliste või lepingueelsete suhetega nimetatud rühmade vahel (kõige laiemas tähenduses) või vastutava töötleja juriidiliste kohustustega.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

Art. 6(1) lit. a GDPR on õiguslikuks aluseks töötlemistoimingutele, mille jaoks me saame nõusoleku konkreetsel töötlemisotstarbel. Kui isikuandmete töötlemine on vajalik sellise lepingu täitmiseks, milles andmesubjekt on osaline, nagu näiteks juhul, kui töötlemistoimingud on vajalikud kaupade tarnimiseks või muude teenuste osutamiseks, põhineb töötlemine GDPR artikli 6 lõike 1 punkti b alusel. Sama kehtib ka selliste töötlemistoimingute kohta, mis on vajalikud lepingueelsete meetmete võtmiseks, näiteks meie tooteid või teenuseid puudutavate päringute puhul. Kui meie ettevõtte suhtes kehtib õiguslik kohustus, mille kohaselt on isikuandmete töötlemine vajalik, näiteks maksukohustuste täitmiseks, põhineb töötlemine art. 6(1) lit. c GDPR.

Harvadel juhtudel võib isikuandmete töötlemine olla vajalik andmesubjekti või muu füüsilise isiku eluliste huvide kaitsmiseks. See oleks näiteks siis, kui külastaja saaks meie ettevõttes vigastada ja tema nimi, vanus, ravikindlustuse andmed või muud elutähtsad andmed tuleks edastada arstile, haiglale või muule kolmandale isikule. Sellisel juhul põhineks töötlemine art. 6(1) lit. d GDPR.

Kui töötlemine on vajalik avalikes huvides või vastutava töötleja avaliku võimu teostamiseks, on õiguslikuks aluseks art. 6(1) lit. e GDPR.

Lõpuks võivad töötlemistoimingud põhineda isikuandmete kaitse üldmääruse artikli 6 lõike 1 punktil f. Seda õiguslikku alust kasutatakse töötlemistoimingute puhul, mis ei ole hõlmatud ühegi eespool nimetatud õigusliku alusega, kui töötlemine on vajalik meie ettevõtte või kolmanda isiku õigustatud huvide tõttu, välja arvatud juhul, kui need huvid on ülimuslikud seoses andmesubjekti huvide või põhiõiguste ja -vabadustega, mis nõuavad isikuandmete kaitset. Sellised töötlemistoimingud on eriti lubatud, sest Euroopa seadusandja on neid eraldi maininud. Ta leidis, et õigustatud huvi võib eeldada, kui andmesubjekt on vastutava töötleja klient (isikuandmete kaitse üldmääruse põhjenduse 47 lause 2).

## D. Kui isikuandmete töötlemine põhineb artikli 6 lõike 1 punktil f, siis teave vastutava töötleja või kolmanda isiku õigustatud huvide kohta (GDPR artikli 13 lõike 1 punkt d).

Kui isikuandmete töötlemine põhineb isikuandmete kaitse üldmääruse artikli 6 lõike 1 punkti f alusel, on meie õigustatud huvi teostada oma äritegevust kõigi meie töötajate ja aktsionäride heaolu huvides.

## E. Asjakohasel juhul teave isikuandmete vastuvõtjate või vastuvõtjate kategooriate kohta (isikuandmete kaitse üldmääruse artikli 13 lõike 1 punkt e).

Riigiasutused

Välised asutused

Täiendavad välised asutused


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

Sisemine töötlemine

Kontsernisisene töötlemine

Muud asutused

Meie volitatud töötlejate ja andmete saajate nimekiri kolmandates riikides ja vajaduse korral rahvusvaheliste organisatsioonide nimekiri on avaldatud meie veebilehel või seda saab meilt tasuta küsida. Selle nimekirja taotlemiseks võtke palun ühendust meie andmekaitseametnikuga.

## F. Asjakohasel juhul teave selle kohta, et vastutav töötleja kavatseb edastada isikuandmed kolmandale riigile või rahvusvahelisele organisatsioonile, ning teave kaitse piisavust käsitleva komisjoni otsuse olemasolu või puudumise kohta või artiklis 46 või 47 või artikli 49 lõike 1 teises lõigus osutatud edastamise korral viide asjakohastele või sobivatele kaitsemeetmetele ja nende koopia saamise viisile või kohale, kus need on tehtud kättesaadavaks (isikuandmete kaitse üldmääruse artikli 13 lõike 1 punkt f, artikli 46 lõige 1, artikli 46 lõike 2 punkt c).

Kõik meie kontserni kuuluvad ettevõtted ja filiaalid (edaspidi "kontserni ettevõtted"), mille tegevuskoht või kontor asub kolmandas riigis, võivad kuuluda isikuandmete vastuvõtjate hulka. Kõigi kontserni ettevõtete või vastuvõtjate nimekirja saab meilt küsida.

Vastavalt isikuandmete kaitse üldmääruse artikli 46 lõikele 1 võib vastutav töötleja või volitatud töötleja edastada isikuandmeid kolmandale riigile üksnes juhul, kui vastutav töötleja või volitatud töötleja on näinud ette asjakohased kaitsemeetmed ja tingimusel, et andmesubjektidele on kättesaadavad jõustatavad andmesubjekti õigused ja tõhusad õiguskaitsevahendid. Asjakohased kaitsemeetmed võib sätestada ilma järelevalveasutuse eriluba nõudmata, kasutades selleks standardseid lepingutingimusi, isikuandmete kaitse üldmääruse artikli 46 lõike 2 punkt c.

Kõigi kolmandatest riikidest pärit vastuvõtjatega lepitakse enne isikuandmete esmakordset edastamist kokku Euroopa Liidu standardsetes lepingutingimustes või muudes asjakohastes kaitsemeetmetes. Seega on tagatud asjakohased kaitsemeetmed, jõustatavad andmesubjekti õigused ja tõhusad õiguskaitsevahendid andmesubjektidele. Iga andmesubjekt võib meilt saada koopia tüüplepinguklauslitest. Lepingute tüüptingimused on kättesaadavad ka Euroopa Liidu Teatajas.

Andmekaitse üldmääruse artikli 45 lõige 3 annab Euroopa Komisjonile õiguse otsustada rakendusaktiga, et väljaspool ELi asuv riik tagab piisava kaitsetaseme. See tähendab isikuandmete kaitse taset, mis on üldjoontes samaväärne ELi tasemega. Piisava kaitsetaseme tuvastamise otsuste tagajärjeks on see, et isikuandmed võivad vabalt liikuda EList (ja Norrast, Liechtensteinist ja Islandist) kolmandasse riiki ilma täiendavate takistusteta. Sarnaseid eeskirju kohaldatakse Ühendkuningriigis, Šveitsis ja mõnes teises riigis.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

Juhul kui Euroopa Komisjon või mõne muu riigi valitsus otsustab, et kolmas riik pakub piisavat kaitsetaset, ja kohaldatava raamistiku (nt EU-U.S. Data Privacy Framework, Swiss-U.S. Data Privacy Framework, UK Extension to the EU-U.S. Data Privacy Framework) puhul põhinevad kõik meie poolt selliste raamistike liikmetele (nt isesertifitseeritud üksused) tehtavad edastused üksnes nende üksuste liikmelisusel asjaomases raamistikus. Juhul kui meie või üks meie kontserni kuuluvatest üksustest on sellise raamistiku liige, põhinevad kõik edastused meile või meie kontserni kuuluvale üksusele üksnes selle üksuse liikmelisusel sellises raamistikus.

Iga andmesubjekt võib meilt saada raamistiku koopia. Lisaks on raamistikud kättesaadavad ka Euroopa Liidu Teatajas või avaldatud õigusmaterjalides või järelevalveasutuste või muude pädevate asutuste või institutsioonide veebisaitidel.

## G. Isikuandmete säilitamise ajavahemik või, kui see ei ole võimalik, sellise ajavahemiku määramise kriteeriumid (isikuandmete kaitse üldmääruse artikli 13 lõike 2 punkt a).

Isikuandmete säilitamisperioodi kindlaksmääramise kriteeriumiks on vastav seadusjärgne säilitamisperiood. Pärast selle tähtaja möödumist kustutatakse vastavad andmed rutiinselt, kui need ei ole enam vajalikud lepingu täitmiseks või lepingu algatamiseks.

Kui seadusjärgset säilitamisperioodi ei ole, on kriteeriumiks lepinguline või sisemine säilitamisperiood.

## H. Teave õiguse kohta taotleda vastutavalt töötlejalt juurdepääsu andmesubjekti puudutavatele isikuandmetele ning nende parandamist või kustutamist või isikuandmete töötlemise piiramist või esitada vastuväide selliste isikuandmete töötlemisele, samuti teave isikuandmete ülekandmise õiguse kohta (isikuandmete kaitse üldmääruse artikli 13 lõike 2 punkt b).

Kõigil andmesubjektidel on järgmised õigused:

***Juurdepääsuõigus***

Igal andmesubjektil on õigus tutvuda teda puudutavate isikuandmetega. Juurdepääsuõigus laieneb kõigile meie poolt töödeldavatele andmetele. Seda õigust saab kasutada lihtsalt ja mõistlike ajavahemike järel, et olla teadlik töötlemise seaduslikkusest ja seda kontrollida (isikuandmete kaitse üldmääruse põhjendus 63). See õigus tuleneb art. 15 GDPR. Andmesubjekt võib meiega ühendust võtta, et kasutada juurdepääsuõigust.

***Õigus andmete parandamisele***

GDPR artikli 16 lause 1 kohaselt on andmesubjektil õigus saada vastutavalt töötlejalt põhjendamatu viivituseta teda puudutavate ebatäpsete isikuandmete parandamine. Lisaks on GDPRi artikli 16 lause 2


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

kohaselt andmesubjektil õigus, võttes arvesse töötlemise eesmärke, saada puudulikud isikuandmed täiendatud, sealhulgas täiendava avalduse esitamise teel. Andmesubjekt võib meiega ühendust võtta, et kasutada õigust andmete parandamisele.

***Õigus andmete kustutamisele (õigus olla unustatud)***

Lisaks on andmesubjektidel õigus andmete kustutamisele ja unustamisele vastavalt art. 17 GDPR. Seda õigust saab samuti kasutada, võttes meiega ühendust. Siinkohal soovime siiski rõhutada, et see õigus ei kehti, kui töötlemine on vajalik meie ettevõtte suhtes kehtiva juriidilise kohustuse täitmiseks, GDPR artikli 17 lõike 3 punkt b. See tähendab, et me saame kustutamise taotluse heaks kiita alles pärast seadusest tuleneva säilitamisperioodi lõppu.

***Õigus töötlemise piiramisele***

Vastavalt GDPR artiklile 18 on igal andmesubjektil õigus töötlemise piiramisele. Töötlemise piiramist võib nõuda, kui on täidetud üks GDPRi artikli 18 lõike 1 punktides a-d sätestatud tingimustest. Andmesubjekt võib meiega ühendust võtta, et kasutada õigust töötlemise piiramisele.

***Õigus esitada vastuväiteid***

Lisaks sellele on artikkel. 21 GDPR tagab õiguse esitada vastuväiteid. Andmesubjekt võib meiega ühendust võtta, et kasutada vastuväite esitamise õigust.

***Õigus andmete ülekantavusele***

Art. 20 GDPR annab andmesubjektile õiguse andmete ülekantavusele. Selle sätte kohaselt on andmesubjektil üldmääruse artikli 20 lõike 1 punktides a ja b sätestatud tingimustel õigus saada teda puudutavad isikuandmed, mille ta on vastutavale töötlejale esitanud, struktureeritud, üldkasutatavas ja masinloetavas vormingus ning õigus edastada need andmed teisele vastutavale töötlejale, ilma et vastutav töötleja, kellele isikuandmed esitati, neid takistaks. Andmesubjekt võib meiega ühendust võtta, et kasutada õigust andmete ülekandmisele.

## I. Kui isikuandmete töötlemine põhineb artikli 6 lõike 1 punktil a või artikli 9 lõike 2 punktil a, siis teave õiguse kohta nõusolek igal ajal tagasi võtta, ilma et see mõjutaks enne tagasivõtmist nõusoleku alusel toimunud töötlemise seaduslikkust (GDPRi artikli 13 lõike 2 punkt c).

Kui isikuandmete töötlemise aluseks on art. 6 lõike 1 punkti a GDPR, mis on nii, kui andmesubjekt on andnud nõusoleku isikuandmete töötlemiseks ühel või mitmel konkreetsel eesmärgil, või põhineb see GDPR artikli 9 lõike 2 punkti a alusel, mis reguleerib selgesõnalist nõusolekut isikuandmete eriliikide töötlemiseks, on andmesubjektil vastavalt GDPR artikli 7 lõike 3 esimesele lausele 1 õigus oma nõusolek igal ajal tagasi võtta.

Nõusoleku tagasivõtmine ei mõjuta enne selle tagasivõtmist nõusolekul põhineva töötlemise õiguspärasust, GDPR artikli 7 lõike 3 lause 2. Nõusoleku tagasivõtmine peab olema sama lihtne kui selle


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

andmine, art. 7 lõike 3 lause 4 GDPR. Seega võib nõusoleku tagasivõtmine alati toimuda samal viisil, nagu nõusolek on antud, või muul viisil, mida andmesubjekt peab lihtsamaks. Tänapäeva infoühiskonnas on tõenäoliselt kõige lihtsam viis nõusoleku tagasivõtmiseks lihtne e-kiri. Kui andmesubjekt soovib oma meile antud nõusolekut tagasi võtta, piisab lihtsast e-kirjast meile. Alternatiivina võib andmesubjekt valida mis tahes muu viisi oma nõusoleku tagasivõtmisest teatamiseks.

## J. Teave õiguse kohta esitada kaebus järelevalveasutusele (isikuandmete kaitse üldmääruse artikli 13 lõike 2 punkt d, artikli 77 lõige 1).

Vastutava töötlejana oleme kohustatud teavitama andmesubjekti õigusest esitada kaebus järelevalveasutusele, GDPR artikli 13 lõike 2 punkt d. Õigus esitada kaebus järelevalveasutusele on reguleeritud GDPRi artikli 77 lõikega 1. Selle sätte kohaselt on igal andmesubjektil õigus esitada kaebus järelevalveasutusele, eelkõige oma alalise elukoha, töökoha või väidetava rikkumise koha liikmesriigis, kui andmesubjekt leiab, et teda puudutavate isikuandmete töötlemine on vastuolus isikuandmete kaitse üldmäärusega, ilma et see piiraks muude haldus- või õiguskaitsevahendite kasutamist. Õigus esitada kaebus järelevalveasutusele on liidu õigusega piiratud ainult selliselt, et seda saab kasutada ainult ühe järelevalveasutuse ees (isikuandmete kaitse üldmääruse põhjenduse 141 lause 1). Selle reegli eesmärk on vältida sama andmesubjekti topeltkaebusi samas küsimuses. Kui andmesubjekt soovib esitada meie kohta kaebuse, palume seetõttu pöörduda ainult ühe järelevalveasutuse poole.

## K. Teave selle kohta, kas isikuandmete esitamine on õigusaktist või lepingust tulenev kohustus või lepingu sõlmimiseks vajalik nõue, samuti selle kohta, kas andmesubjekt on kohustatud kõnealuseid isikuandmeid esitama, ning selliste andmete esitamata jätmise võimalike tagajärgede kohta, ning (GDPR artikli 13 lõike 2 punkt e).

Selgitame, et isikuandmete esitamist nõuab osaliselt seadus (nt maksueeskirjad) või see võib tuleneda ka lepingulistest sätetest (nt teave lepingupartneri kohta).

Mõnikord võib lepingu sõlmimiseks olla vajalik, et andmesubjekt edastab meile isikuandmeid, mida peame seejärel töötlema. Andmesubjekt on näiteks kohustatud esitama meile isikuandmeid, kui meie ettevõte sõlmib temaga lepingu. Isikuandmete esitamata jätmine tooks kaasa selle, et lepingut andmesubjektiga ei saa sõlmida.

Enne kui andmesubjekt esitab isikuandmed, peab ta meiega ühendust võtma. Selgitame andmesubjektile, kas isikuandmete esitamine on seadusest või lepingust tulenevalt nõutav või lepingu sõlmimiseks vajalik, kas isikuandmete esitamine on kohustuslik ja millised on isikuandmete esitamata jätmise tagajärjed.


© All rights reserved by Heiko Maniero.

### L. Teave artikli 22 lõigetes 1 ja 4 osutatud automatiseeritud otsuste, sealhulgas profiilianalüüsi tegemise kohta ning vähemalt nendel juhtudel sisuline teave kasutatava loogika ja selle kohta, millised on sellise isikuandmete töötlemise tähtsus ja prognoositavad tagajärjed andmesubjekti jaoks (GDPR artikli 13 lõike 2 punkt f).

Vastutustundliku ettevõttena ei kasuta me tavaliselt automatiseeritud otsuste tegemist ega profiilide koostamist. Kui erandjuhtudel kasutame automatiseeritud otsuste tegemist või profiilianalüüsi, teavitame sellest andmesubjekti kas eraldi või meie privaatsuspoliitika alajaotuse kaudu (meie veebisaidil). Sellisel juhul kohaldatakse järgmist:

Automatiseeritud otsuste tegemine - sealhulgas profiilianalüüs - võib toimuda, kui 1) see on vajalik andmesubjekti ja meie vahelise lepingu sõlmimiseks või täitmiseks või 2) see on lubatud liidu või liikmesriigi õigusega, mida me kohaldame ja mis sätestab ka sobivad meetmed andmesubjekti õiguste ja vabaduste ning õigustatud huvide kaitsmiseks, või 3) see põhineb andmesubjekti selgesõnalisel nõusolekul.

GDPR artikli 22 lõike 2 punktides a ja c osutatud juhtudel rakendame sobivaid meetmeid andmesubjekti õiguste ja vabaduste ning õigustatud huvide kaitsmiseks. Sellistel juhtudel on teil õigus saada vastutava töötleja poolset inimlikku sekkumist, väljendada oma seisukohta ja vaidlustada otsus.

Meie privaatsuspoliitikas on esitatud sisuline teave asjaomase loogika kohta, samuti sellise töötlemise tähtsus ja kavandatud tagajärjed andmesubjektile.

## II. Teave, mis tuleb esitada juhul, kui isikuandmed ei ole saadud andmesubjektilt (GDPR artikkel 14)

### A. Vastutava töötleja ning asjakohasel juhul vastutava töötleja esindaja nimi ja kontaktandmed (GDPR artikli 14 lõike 1 punkt a)

Vt eespool

### B. Asjakohasel juhul andmekaitseametniku kontaktandmed (isikuandmete kaitse üldmääruse artikli 14 lõike 1 punkt b).

Vt eespool


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## C. Isikuandmete töötlemise eesmärk ja õiguslik alus (isikuandmete kaitse üldmääruse artikli 14 lõike 1 punkt c).

Isikuandmete töötlemise eesmärk on kõikide toimingute tegemine, mis on seotud vastutava töötleja, klientide, potentsiaalsete klientide, äripartnerite või muude lepinguliste või lepingueelsete suhetega nimetatud rühmade vahel (kõige laiemas tähenduses) või vastutava töötleja juriidiliste kohustustega.

Kui isikuandmete töötlemine on vajalik sellise lepingu täitmiseks, milles andmesubjekt on osaline, nagu näiteks juhul, kui töötlemistoimingud on vajalikud kaupade tarnimiseks või muude teenuste osutamiseks, põhineb töötlemine GDPR artikli 6 lõike 1 punkti b alusel. Sama kehtib ka selliste töötlemistoimingute kohta, mis on vajalikud lepingueelsete meetmete võtmiseks, näiteks meie tooteid või teenuseid puudutavate päringute puhul. Kui meie ettevõtte suhtes kehtib õiguslik kohustus, mille kohaselt on isikuandmete töötlemine vajalik, näiteks maksukohustuste täitmiseks, põhineb töötlemine art. 6(1) lit. c GDPR.

Harvadel juhtudel võib isikuandmete töötlemine olla vajalik andmesubjekti või muu füüsilise isiku eluliste huvide kaitsmiseks. See oleks näiteks siis, kui külastaja saaks meie ettevõttes vigastada ja tema nimi, vanus, ravikindlustuse andmed või muud elutähtsad andmed tuleks edastada arstile, haiglale või muule kolmandale isikule. Sellisel juhul põhineks töötlemine art. 6(1) lit. d GDPR.

Kui töötlemine on vajalik avalikes huvides või vastutava töötleja avaliku võimu teostamiseks, on õiguslikuks aluseks art. 6(1) lit. e GDPR.

Lõpuks võivad töötlemistoimingud põhineda isikuandmete kaitse üldmääruse artikli 6 lõike 1 punktil f. Seda õiguslikku alust kasutatakse töötlemistoimingute puhul, mis ei ole hõlmatud ühegi eespool nimetatud õigusliku alusega, kui töötlemine on vajalik meie ettevõtte või kolmanda isiku õigustatud huvide tõttu, välja arvatud juhul, kui need huvid on ülimuslikud seoses andmesubjekti huvide või põhiõiguste ja -vabadustega, mis nõuavad isikuandmete kaitset. Sellised töötlemistoimingud on eriti lubatud, sest Euroopa seadusandja on neid eraldi maininud. Ta leidis, et õigustatud huvi võib eeldada, kui andmesubjekt on vastutava töötleja klient (isikuandmete kaitse üldmääruse põhjenduse 47 lause 2).

## D. Asjaomaste isikuandmete liigid (GDPR artikli 14 lõike 1 punkt d)

Kliendi andmed

Potentsiaalsete klientide andmed

Töötajate andmed

Tarnijate andmed


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## E. Asjakohasel juhul teave isikuandmete vastuvõtjate või vastuvõtjate kategooriate kohta (isikuandmete kaitse üldmääruse artikli 14 lõike 1 punkt e).

Riigiasutused

Välised asutused

Täiendavad välised asutused

Sisemine töötlemine

Kontsernisisene töötlemine

Muud asutused

Meie volitatud töötlejate ja andmete saajate nimekiri kolmandates riikides ja vajaduse korral rahvusvaheliste organisatsioonide nimekiri on avaldatud meie veebilehel või seda saab meilt tasuta küsida. Selle nimekirja taotlemiseks võtke palun ühendust meie andmekaitseametnikuga.

## F. Asjakohasel juhul teave selle kohta, et vastutav töötleja kavatseb edastada isikuandmed kolmandas riigis asuvale vastuvõtjale või rahvusvahelisele organisatsioonile, ning teave kaitse piisavust käsitleva komisjoni otsuse olemasolu või puudumise kohta või artiklis 46 või 47 või artikli 49 lõike 1 teises lõigus osutatud edastamise korral viide asjakohastele või sobivatele kaitsemeetmetele ja nende koopia saamise viisile või kohale, kus need on tehtud kättesaadavaks (isikuandmete kaitse üldmääruse artikli 14 lõike 1 punkt f, artikli 46 lõige 1, artikli 46 lõike 2 punkt c).

Kõik meie kontserni kuuluvad ettevõtted ja filiaalid (edaspidi "kontserni ettevõtted"), mille tegevuskoht või kontor asub kolmandas riigis, võivad kuuluda isikuandmete vastuvõtjate hulka. Kõigi kontserni kuuluvate ettevõtete nimekirja saab meilt küsida.

Vastavalt isikuandmete kaitse üldmääruse artikli 46 lõikele 1 võib vastutav töötleja või volitatud töötleja edastada isikuandmeid kolmandale riigile üksnes juhul, kui vastutav töötleja või volitatud töötleja on näinud ette asjakohased kaitsemeetmed ja tingimusel, et andmesubjektidele on kättesaadavad jõustatavad andmesubjekti õigused ja tõhusad õiguskaitsevahendid. Asjakohased kaitsemeetmed võib sätestada ilma järelevalveasutuse eriluba nõudmata, kasutades standardseid andmekaitseklausleid, GDPR artikli 46 lõike 2 punkt c.

Kõigi kolmandatest riikidest pärit vastuvõtjatega lepitakse enne isikuandmete esmakordset edastamist kokku Euroopa Liidu standardsetes lepingutingimustes või muudes asjakohastes kaitsemeetmetes. Seega on tagatud asjakohased kaitsemeetmed, jõustatavad andmesubjekti õigused ja tõhusad


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

õiguskaitsevahendid andmesubjektidele. Iga andmesubjekt võib meilt saada koopia tüüplepinguklauslitest. Lepingustandardklauslid on kättesaadavad ka Euroopa Liidu Teatajas.

Andmekaitse üldmääruse artikli 45 lõige 3 annab Euroopa Komisjonile õiguse otsustada rakendusaktiga, et väljaspool ELi asuv riik tagab piisava kaitsetaseme. See tähendab isikuandmete kaitse taset, mis on üldjoontes samaväärne ELi tasemega. Piisava kaitsetaseme tuvastamise otsuste tagajärjeks on see, et isikuandmed võivad vabalt liikuda EList (ja Norrast, Liechtensteinist ja Islandist) kolmandasse riiki ilma täiendavate takistusteta. Sarnaseid eeskirju kohaldatakse Ühendkuningriigis, Šveitsis ja mõnes teises riigis.

Juhul kui Euroopa Komisjon või mõne muu riigi valitsus otsustab, et kolmas riik pakub piisavat kaitsetaset, ja kohaldatava raamistiku (nt EU-U.S. Data Privacy Framework, Swiss-U.S. Data Privacy Framework, UK Extension to the EU-U.S. Data Privacy Framework) puhul põhinevad kõik meie poolt selliste raamistike liikmetele (nt isesertifitseeritud üksused) tehtavad edastused üksnes nende üksuste liikmelisusel asjaomases raamistikus. Juhul kui meie või üks meie kontserni kuuluvatest üksustest on sellise raamistiku liige, põhinevad kõik edastused meile või meie kontserni kuuluvale üksusele üksnes selle üksuse liikmelisusel sellises raamistikus.

Iga andmesubjekt võib meilt saada raamistiku koopia. Lisaks on raamistikud kättesaadavad ka Euroopa Liidu Teatajas või avaldatud õigusmaterjalides või järelevalveasutuste või muude pädevate asutuste või institutsioonide veebisaitidel.

## G. Isikuandmete säilitamise ajavahemik või, kui see ei ole võimalik, sellise ajavahemiku määramise kriteeriumid (isikuandmete kaitse üldmääruse artikli 14 lõike 2 punkt a).

Isikuandmete säilitamisperioodi kindlaksmääramise kriteeriumiks on vastav seadusjärgne säilitamisperiood. Pärast selle tähtaja möödumist kustutatakse vastavad andmed rutiinselt, kui need ei ole enam vajalikud lepingu täitmiseks või lepingu algatamiseks.

Kui seadusjärgset säilitamisperioodi ei ole, on kriteeriumiks lepinguline või sisemine säilitamisperiood.

## H. Kui isikuandmete töötlemine põhineb artikli 6 lõike 1 punktil f, siis teave vastutava töötleja või kolmanda isiku õigustatud huvide kohta (isikuandmete kaitse üldmääruse artikli 14 lõike 2 punkt b).

Vastavalt isikuandmete kaitse üldmääruse artikli 6 lõike 1 punktile f on töötlemine seaduslik ainult siis, kui töötlemine on vajalik vastutava töötleja või kolmanda isiku õigustatud huvide kaitseks, välja arvatud juhul, kui need huvid on ülimuslikud seoses andmesubjekti huvide või põhiõiguste ja -vabadustega, mis nõuavad isikuandmete kaitset. Vastavalt isikuandmete kaitse üldmääruse põhjenduse 47 teisele lausele


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

võib õigustatud huvi olla olemas, kui andmesubjekti ja vastutava töötleja vahel on asjakohane ja asjakohane suhe, näiteks olukorras, kus andmesubjekt on vastutava töötleja klient. Kõigil juhtudel, mil meie ettevõte töötleb isikuandmeid GDPR artikli 6 lõike 1 punkti f alusel, on meie õigustatud huvi meie äritegevuse teostamine kõigi meie töötajate ja aktsionäride heaolu huvides.

## I. Teave õiguse kohta taotleda vastutavalt töötlejalt juurdepääsu andmesubjekti puudutavatele isikuandmetele ning nende parandamist või kustutamist või isikuandmete töötlemise piiramist ning esitada vastuväide selliste isikuandmete töötlemisele, samuti teave isikuandmete ülekandmise õiguse kohta (isikuandmete kaitse üldmääruse artikli 14 lõike 2 punkt c).

Kõigil andmesubjektidel on järgmised õigused:

***Juurdepääsuõigus***

Igal andmesubjektil on õigus tutvuda teda puudutavate isikuandmetega. Juurdepääsuõigus laieneb kõigile meie poolt töödeldavatele andmetele. Seda õigust saab kasutada lihtsalt ja mõistlike ajavahemike järel, et olla teadlik töötlemise seaduslikkusest ja seda kontrollida (isikuandmete kaitse üldmääruse põhjendus 63). See õigus tuleneb art. 15 GDPR. Andmesubjekt võib meiega ühendust võtta, et kasutada juurdepääsuõigust.

***Õigus andmete parandamisele***

GDPR artikli 16 lause 1 kohaselt on andmesubjektil õigus saada vastutavalt töötlejalt põhjendamatu viivituseta teda puudutavate ebatäpsete isikuandmete parandamine. Lisaks on GDPRi artikli 16 lause 2 kohaselt andmesubjektil õigus, võttes arvesse töötlemise eesmärke, saada puudulikud isikuandmed täiendatud, sealhulgas täiendava avalduse esitamise teel. Andmesubjekt võib meiega ühendust võtta, et kasutada õigust andmete parandamisele.

***Õigus andmete kustutamisele (õigus olla unustatud)***

Lisaks on andmesubjektidel õigus andmete kustutamisele ja unustamisele vastavalt art. 17 GDPR. Seda õigust saab samuti kasutada, võttes meiega ühendust. Siinkohal soovime siiski rõhutada, et see õigus ei kehti, kui töötlemine on vajalik meie ettevõtte suhtes kehtiva juriidilise kohustuse täitmiseks, GDPR artikli 17 lõike 3 punkt b. See tähendab, et me saame kustutamise taotluse heaks kiita alles pärast seadusest tuleneva säilitamisperioodi lõppu.

***Õigus töötlemise piiramisele***

Vastavalt GDPR artiklile 18 on igal andmesubjektil õigus töötlemise piiramisele. Töötlemise piiramist võib nõuda, kui on täidetud üks GDPRi artikli 18 lõike 1 punktides a-d sätestatud tingimustest. Andmesubjekt võib meiega ühendust võtta, et kasutada õigust töötlemise piiramisele.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

***Õigus esitada vastuväiteid***

Lisaks sellele on artikkel. 21 GDPR tagab õiguse esitada vastuväiteid. Andmesubjekt võib meiega ühendust võtta, et kasutada vastuväite esitamise õigust.

***Õigus andmete ülekantavusele***

Art. 20 GDPR annab andmesubjektile õiguse andmete ülekantavusele. Selle sätte kohaselt on andmesubjektil üldmääruse artikli 20 lõike 1 punktides a ja b sätestatud tingimustel õigus saada teda puudutavad isikuandmed, mille ta on vastutavale töötlejale esitanud, struktureeritud, üldkasutatavas ja masinloetavas vormingus ning õigus edastada need andmed teisele vastutavale töötlejale, ilma et vastutav töötleja, kellele isikuandmed esitati, neid takistaks. Andmesubjekt võib meiega ühendust võtta, et kasutada õigust andmete ülekandmisele.

## J. Kui isikuandmete töötlemine põhineb artikli 6 lõike 1 punktil a või artikli 9 lõike 2 punktil a, siis teave õiguse kohta nõusolek igal ajal tagasi võtta, ilma et see mõjutaks enne tagasivõtmist nõusoleku alusel toimunud isikuandmete töötlemise seaduslikkust (GDPRi artikli 14 lõike 2 punkt d).

Kui isikuandmete töötlemise aluseks on art. 6 lõike 1 punkti a GDPR, mis on nii, kui andmesubjekt on andnud nõusoleku isikuandmete töötlemiseks ühel või mitmel konkreetsel eesmärgil, või põhineb see GDPR artikli 9 lõike 2 punkti a alusel, mis reguleerib selgesõnalist nõusolekut isikuandmete eriliikide töötlemiseks, on andmesubjektil vastavalt GDPR artikli 7 lõike 3 esimesele lausele 1 õigus oma nõusolek igal ajal tagasi võtta.

Nõusoleku tagasivõtmine ei mõjuta nõusolekul põhineva töötlemise seaduslikkust enne selle tagasivõtmist, isikuandmete kaitse üldmääruse artikli 7 lõike 3 lause 2. Nõusoleku tagasivõtmine peab olema sama lihtne kui selle andmine, art. 7 lõike 3 lause 4 GDPR. Seega võib nõusoleku tagasivõtmine alati toimuda samal viisil, nagu nõusolek on antud, või muul viisil, mida andmesubjekt peab lihtsamaks. Tänapäeva infoühiskonnas on tõenäoliselt kõige lihtsam viis nõusoleku tagasivõtmiseks lihtne e-kiri. Kui andmesubjekt soovib oma meile antud nõusolekut tagasi võtta, piisab lihtsast e-kirjast meile. Alternatiivina võib andmesubjekt valida mis tahes muu viisi oma nõusoleku tagasivõtmisest teatamiseks.

## K. Teave õiguse kohta esitada kaebus järelevalveasutusele (isikuandmete kaitse üldmääruse artikli 14 lõike 2 punkt e, artikli 77 lõige 1)

Vastutava töötlejana oleme kohustatud teavitama andmesubjekti õigusest esitada kaebus järelevalveasutusele, GDPR artikli 14 lõike 2 punkt e. Õigus esitada kaebus järelevalveasutusele on reguleeritud GDPRi artikli 77 lõikega 1. Selle sätte kohaselt on igal andmesubjektil õigus esitada kaebus järelevalveasutusele, eelkõige oma alalise elukoha, töökoha või väidetava rikkumise koha liikmesriigis, kui andmesubjekt leiab, et teda puudutavate isikuandmete töötlemine on vastuolus isikuandmete kaitse üldmäärusega, ilma et see piiraks muude haldus- või õiguskaitsevahendite kasutamist. Õigus esitada


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

kaebus järelevalveasutusele on liidu õigusega piiratud ainult selliselt, et seda saab kasutada ainult ühe järelevalveasutuse ees (isikuandmete kaitse üldmääruse põhjenduse 141 lause 1). Selle reegli eesmärk on vältida sama andmesubjekti topeltkaebusi samas küsimuses. Kui andmesubjekt soovib esitada meie kohta kaebuse, palume seetõttu pöörduda ainult ühe järelevalveasutuse poole.

## L. Teave isikuandmete päritoluallika ning asjakohasel juhul selle kohta, kas need pärinevad avalikult kättesaadavatest allikatest (isikuandmete kaitse üldmääruse artikli 14 lõike 2 punkt f).

Põhimõtteliselt kogutakse isikuandmeid otse andmesubjektilt või koostöös asutusega (nt andmete hankimine ametlikust registrist). Muud andmed andmesubjektide kohta saadakse kontserni äriühingute andmete edastamisest. Selle üldise teabe kontekstis on isikuandmete päritolu täpsete allikate nimetamine kas võimatu või tähendaks ebaproportsionaalselt suurt pingutust art. 14 lõike 5 punkti b tähenduses. Põhimõtteliselt ei kogu me isikuandmeid avalikult kättesaadavatest allikatest.

Iga andmesubjekt võib meiega igal ajal ühendust võtta, et saada täpsemat teavet teda puudutavate isikuandmete täpsete allikate kohta. Kui andmesubjektile ei ole võimalik esitada isikuandmete päritolu, sest on kasutatud erinevaid allikaid, tuleks esitada üldine teave (isikuandmete kaitse üldmääruse põhjendus 61, 4. lause).

## M. Teave artikli 22 lõigetes 1 ja 4 osutatud automatiseeritud otsuste, sealhulgas profiilianalüüsi tegemise kohta ning vähemalt nendel juhtudel sisuline teave kasutatava loogika ja selle kohta, millised on sellise töötlemise tähtsus ja prognoositavad tagajärjed andmesubjekti jaoks (GDPR artikli 14 lõike 2 punkt g).

Vastutustundliku ettevõttena ei kasuta me tavaliselt automatiseeritud otsuste tegemist ega profiilide koostamist. Kui erandjuhtudel kasutame automatiseeritud otsuste tegemist või profiilianalüüsi, teavitame sellest andmesubjekti kas eraldi või meie privaatsuspoliitika alajaotuse kaudu (meie veebisaidil). Sellisel juhul kohaldatakse järgmist:

Automatiseeritud otsuste tegemine - sealhulgas profiilianalüüs - võib toimuda, kui 1) see on vajalik andmesubjekti ja meie vahelise lepingu sõlmimiseks või täitmiseks või 2) see on lubatud liidu või liikmesriigi õigusega, mida me kohaldame ja mis sätestab ka sobivad meetmed andmesubjekti õiguste ja vabaduste ning õigustatud huvide kaitsmiseks, või 3) see põhineb andmesubjekti selgesõnalisel nõusolekul.

GDPR artikli 22 lõike 2 punktides a ja c osutatud juhtudel rakendame sobivaid meetmeid andmesubjekti õiguste ja vabaduste ning õigustatud huvide kaitsmiseks. Sellistel juhtudel on teil õigus saada vastutava töötleja poolset inimlikku sekkumist, väljendada oma seisukohta ja vaidlustada otsus.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

Meie privaatsuspoliitikas on esitatud sisuline teave asjaomase loogika kohta, samuti sellise töötlemise tähtsus ja kavandatud tagajärjed andmesubjektile.

## III. EU-U.S. Data Privacy Framework (EU-U.S. DPF), UK Extension to the EU-U.S. DPF, Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF)

Kui meie organisatsioon on EU-U.S. Data Privacy Framework (EU-U.S. DPF) ja/või UK Extension to the EU-U.S. DPF ja/või Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF) sertifitseeritud liige, kehtib järgmine:

Me järgime EU-U.S. Data Privacy Framework (EU-U.S. DPF), UK Extension to the EU-U.S. DPF ja Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF) vastavalt U.S. Department of Commerce kehtestatud nõuetele. Meie ettevõte on USA Kaubandusministeeriumile kinnitanud, et see järgib EU-U.S. Data Privacy Framework Principles (EU-U.S. DPF Principles) isikuandmete töötlemisel, mida ta saab Euroopa Liidust ja Ühendkuningriigist, tuginedes EU-U.S. DPF ja UK Extension to the EU-U.S. DPF-le. Meie ettevõte on USA Kaubandusministeeriumile kinnitanud, et see järgib Swiss-U.S. Data Privacy Framework Principles (Swiss-U.S. DPF Principles) isikuandmete töötlemisel, mida ta saab Šveitsist, tuginedes Swiss-U.S. DPF-le. Kui meie privaatsuspoliitika sätted on vastuolus EU-U.S. DPF Principles ja/või Swiss-U.S. DPF Principles-ga, on määravad Principles.

Et rohkem teada saada Data Privacy Framework (DPF) programmi kohta ja meie sertifikaati vaadata, külastage palun https://www.dataprivacyframework.gov/.

Meie ettevõtte teised USA üksused või tütarettevõtted, mis samuti järgivad EU-U.S. DPF Principles, sealhulgas UK Extension to the EU-U.S. DPF ja Swiss-U.S. DPF Principles, kui neid on, on meie privaatsuspoliitikas nimetatud.

Kooskõlas EU-U.S. DPF, UK Extension to the EU-U.S. DPF ja Swiss-U.S. DPF-ga kohustub meie ettevõte tegema koostööd Euroopa andmekaitseasutuste ja Briti Information Commissioner's Office (ICO) ning Šveitsi Federal Data Protection and Information Commissioner (EDÖB) poolt loodud organitega ja järgima nende nõuandeid seoses lahendamata kaebustega meie isikuandmete töötlemise kohta, mida me saame tuginedes EU-U.S. DPF-le, UK Extension to the EU-U.S. DPF-le ja Swiss-U.S. DPF-le.

Me teavitame asjaosalisi isikuid pädevatest Euroopa andmekaitseasutustest, mis vastutavad meie organisatsiooni isikuandmete töötlemise kaebuste lahendamise eest, selle läbipaistvusdokumendi ülaosas ja sellest, et me pakume asjaosalistele isikutele asjakohaseid ja tasuta õiguskaitsevahendeid.

Me teavitame kõiki asjaosalisi isikuid, et meie ettevõte allub Federal Trade Commission (FTC) uurimis- ja täitevvõimudele.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

Asjaosalised isikud saavad teatud tingimustel taotleda siduvat vahekohtu menetlust. Meie organisatsioon on kohustatud lahendama nõudeid ja järgima DPF-Principals lisa I tingimusi, kui asjaosaline isik on taotlenud siduvat vahekohtu menetlust, teavitades sellest meie organisatsiooni ja järgides lisa I Principles tingimusi ja protseduure.

Me teavitame kõiki asjaosalisi isikuid meie organisatsiooni vastutusest isikuandmete edastamisel kolmandatele isikutele.

Asjaosaliste isikute või andmekaitseasutuste küsimuste puhul oleme määranud kohalikke esindajaid, kes on nimetatud selle läbipaistvusdokumendi ülaosas.

Pakume teile võimalust valida (Opt-out), kas teie isikuandmeid (i) edastatakse kolmandatele isikutele või (ii) kasutatakse eesmärgil, mis erineb oluliselt sellest, milleks need algselt koguti või mille jaoks te hiljem oma nõusoleku andsite. Teie valikuvõimaluse kasutamiseks selge, hästi nähtav ja kergesti ligipääsetav mehhanism on meie andmekaitseametnikuga (DSB) e-posti teel ühendust võtmine. Teil ei ole valikuvõimalust ja me ei ole kohustatud seda tegema, kui andmed edastatakse kolmandale isikule, kes tegutseb meie nimel ja meie juhiste järgi. Siiski sõlmime alati sellise esindaja või andmetöötlejaga lepingu.

Tundlike andmete (s.t. isikuandmed, mis sisaldavad teavet tervisliku seisundi, rassilise või etnilise päritolu, poliitiliste vaadete, usuliste või filosoofiliste veendumuste, ametiühingu liikmelisuse või asjaosalise isiku seksuaalelu kohta) puhul saame teie selgesõnalise nõusoleku (Opt-in), kui need andmed (i) edastatakse kolmandatele isikutele või (ii) kasutatakse muul eesmärgil, kui need algselt koguti või mille jaoks te hiljem oma nõusoleku andsite, tehes oma Opt-in valiku. Lisaks käsitleme kõiki kolmandatelt isikutelt saadud isikuandmeid tundlikena, kui kolmas isik need tundlikeks määrab ja käsitleb.

Teavitame teid siinkohal nõudest avaldada isikuandmeid valitsusasutuste seaduslike päringute korral, sealhulgas täita riikliku julgeoleku või õiguskaitse nõudeid.

Isikuandmete edastamisel kolmandale isikule, kes tegutseb vastutava töötlejana, järgime teavitamise ja valikuvõimaluse põhimõtteid (Principals). Samuti sõlmime vastutava töötlejaga lepingu, mis sätestab, et need andmed võib töödelda ainult piiratud ja kindlaksmääratud eesmärkidel vastavalt teie antud nõusolekule ja et saaja pakub samal tasemel kaitset kui DPF-Principals ning teavitab meid, kui ta leiab, et ta ei suuda seda kohustust enam täita. Leping sätestab, et vastutav töötleja lõpetab töötlemise või võtab muud asjakohased ja piisavad meetmed olukorra parandamiseks, kui selline olukord ilmneb.

Isikuandmete edastamisel kolmandale isikule, kes tegutseb esindaja või andmetöötlejana, (i) edastame need andmed ainult piiratud ja kindlaksmääratud eesmärkidel; (ii) veendume, et esindaja või andmetöötleja on kohustatud tagama vähemalt samal tasemel andmekaitse, nagu nõutud DPF-Principals; (iii) võtame asjakohased ja piisavad meetmed, et tagada esindaja või andmetöötleja tegelik isikuandmete töötlemine viisil, mis on kooskõlas meie kohustustega vastavalt DPF-Principals; (iv) nõuame esindajalt või andmetöötlejalt meie organisatsiooni teavitamist, kui ta leiab, et ta ei suuda enam täita kohustust pakkuda samal tasemel kaitset nagu nõutud DPF-Principals; (v) teate saamisel, sealhulgas punktis (iv) nimetatud teate puhul, võtame asjakohased ja piisavad meetmed loata töötlemise


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

peatamiseks ja olukorra parandamiseks; ning (vi) DPF Departmenti taotlusel esitame kokkuvõtte või esindusliku eksemplari asjakohastest andmekaitse sätetest lepingus selle esindajaga.

Kooskõlas EU-U.S. DPF ja/või UK Extension to the EU-U.S. DPF ja/või Swiss-U.S. DPF-ga kohustub meie organisatsioon tegema koostööd Euroopa andmekaitseasutuste ja Briti Information Commissioner's Office (ICO) ning Šveitsi Federal Data Protection and Information Commissioner (EDÖB) poolt loodud organitega ja järgima nende nõuandeid seoses lahendamata kaebustega meie isikuandmete töötlemise kohta seoses töösuhetega, mida me saame tuginedes EU-U.S. DPF-le, UK Extension to the EU-U.S. DPF-le ja Swiss-U.S. DPF-le.

Kõigil andmesubjektidel, kes viibivad ajutiselt Euroopa Liidus (EL), Euroopa Majanduspiirkonnas (EMP) või Ühendkuningriigis või kelle alaline või peamine elukoht on seal, on õigus meie läbipaistvusdokumendis avaldatud õigustele ja andmesubjekti õigustele, mis tulenevad ka isikuandmete kaitse üldmääruse artiklitest 15-22, sealhulgas õigus tutvuda isikuandmetega. Me oleme teinud selle teabe kättesaadavaks kõigis ELi ja EMP keeltes. Ingliskeelne versioon kehtib Ühendkuningriigis.

Kõigil andmesubjektidel, kes elavad ajutiselt Šveitsis või kelle alaline või peamine elukoht on seal, on õigus kasutada Šveitsi andmekaitseseadusest ja Šveitsi andmekaitsemäärusest tulenevaid õigusi ja andmesubjekti õigusi, mis on avaldatud meie läbipaistvusdokumendis, sealhulgas õigus tutvuda isikuandmetega. Oleme esitanud selle teabe kolmes Šveitsi ametlikus keeles (saksa, itaalia ja prantsuse keeles).


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

# ESTONIAN: Teave töötajate ja taotlejate isikuandmete töötlemise kohta (GDPR artiklid 13, 14)

Lugupeetud härra või proua,

Töötajate ja taotlejate isikuandmed väärivad erilist kaitset. Meie eesmärk on hoida meie andmekaitse tase kõrgel tasemel. Seetõttu arendame rutiinselt oma andmekaitse- ja andmeturbe kontseptsioone.

Loomulikult järgime me seaduslikke sätteid andmekaitse kohta. Vastavalt GDPR artiklitele 13, 14 peavad vastutavad töötlejad isikuandmete töötlemisel täitma konkreetseid teavitamisnõudeid. Käesolev dokument täidab neid kohustusi.

Õigusliku reguleerimise terminoloogia on keeruline. Kahjuks ei saanud käesoleva dokumendi koostamisel loobuda juriidiliste terminite kasutamisest. Seetõttu soovime juhtida tähelepanu sellele, et olete alati teretulnud meiega ühendust võtma kõigi küsimuste korral, mis puudutavad käesolevat dokumenti, kasutatud termineid või sõnastusi.

## I. Teave, mis tuleb anda juhul, kui isikuandmed on kogutud andmesubjektilt (GDPR artikkel 13)

### A. Vastutava töötleja ning kui kohaldatav, siis vastutava töötleja esindaja nimi ja kontaktandmed (GDPR artikli 13 lõike 1 punkt a)

Vt eespool

### B. Asjakohasel juhul andmekaitseametniku kontaktandmed (isikuandmete kaitse üldmääruse artikli 13 lõike 1 punkt b).

Vt eespool

### C. Isikuandmete töötlemise eesmärk ja õiguslik alus (isikuandmete kaitse üldmääruse artikli 13 lõike 1 punkt c).

Kandidaatide andmete puhul on andmete töötlemise eesmärk taotluse läbivaatamine värbamisprotsessi käigus. Sel eesmärgil töötleme kõiki teie poolt esitatud andmeid. Värbamisprotsessi käigus esitatud andmete põhjal kontrollime, kas teid kutsutakse tööintervjuule (valikuprotsessi osa). Üldiselt sobivate kandidaatide puhul, eelkõige tööintervjuu raames, töötleme teatud muid teie poolt esitatud isikuandmeid,


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

mis on meie valikuotsuse tegemiseks olulised. Kui teid võetakse tööle, muutuvad kandidaadi andmed automaatselt töötaja andmeteks. Värbamisprotsessi raames töötleme teie kohta muid isikuandmeid, mida me teilt küsime ja mis on vajalikud teie lepingu algatamiseks või täitmiseks (näiteks isikukoodid või maksunumbrid). Töötaja andmete puhul on andmete töötlemise eesmärk töölepingu täitmine või muude töösuhte suhtes kohaldatavate õigusnormide (nt maksuseadus) täitmine ning teie isikuandmete kasutamine teiega sõlmitud töölepingu täitmiseks (nt teie nime ja kontaktandmete avaldamine ettevõttes või klientidele). Töötaja andmeid säilitatakse pärast töösuhte lõppemist, et täita seaduslikke säilitustähtaegu.

Andmete töötlemise õiguslik alus on GDPR artikli 6 lõike 1 punkt b, GDPR artikli 9 lõike 2 punktid b ja h, GDPR artikli 88 lõige 1 ja siseriiklikud õigusaktid, näiteks Saksamaa puhul BDSG § 26 (Saksamaa Liitvabariigi andmekaitseseadus).

## D. Asjakohasel juhul teave isikuandmete vastuvõtjate või vastuvõtjate kategooriate kohta (isikuandmete kaitse üldmääruse artikli 13 lõike 1 punkt e)

Riigiasutused

Välised asutused

Täiendavad välised asutused

Sisemine töötlemine

Kontsernisisene töötlemine

Muud asutused

Meie volitatud töötlejate ja andmete saajate nimekiri kolmandates riikides ja vajaduse korral rahvusvaheliste organisatsioonide nimekiri on avaldatud meie veebilehel või seda saab meilt tasuta küsida. Selle nimekirja taotlemiseks võtke palun ühendust meie andmekaitseametnikuga.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## E. Asjakohasel juhul teave selle kohta, et vastutav töötleja kavatseb edastada isikuandmed kolmandale riigile või rahvusvahelisele organisatsioonile, ning teave kaitse piisavust käsitleva komisjoni otsuse olemasolu või puudumise kohta või artiklis 46 või 47 või artikli 49 lõike 1 teises lõigus osutatud edastamise korral viide asjakohastele või sobivatele kaitsemeetmetele ja nende koopia saamise viisile või kohale, kus need on tehtud kättesaadavaks (isikuandmete kaitse üldmääruse artikli 13 lõike 1 punkt f, artikli 46 lõige 1, artikli 46 lõike 2 punkt c).

Kõik meie kontserni kuuluvad ettevõtted ja filiaalid (edaspidi "kontserni ettevõtted"), mille tegevuskoht või kontor asub kolmandas riigis, võivad kuuluda isikuandmete vastuvõtjate hulka. Kõigi kontserni ettevõtete või vastuvõtjate nimekirja saab meilt küsida.

Vastavalt isikuandmete kaitse üldmääruse artikli 46 lõikele 1 võib vastutav töötleja või volitatud töötleja edastada isikuandmeid kolmandale riigile üksnes juhul, kui vastutav töötleja või volitatud töötleja on näinud ette asjakohased kaitsemeetmed ja tingimusel, et andmesubjektidele on kättesaadavad jõustatavad andmesubjekti õigused ja tõhusad õiguskaitsevahendid. Asjakohased kaitsemeetmed võib sätestada ilma järelevalveasutuse eriluba nõudmata, kasutades selleks standardseid lepingutingimusi, isikuandmete kaitse üldmääruse artikli 46 lõike 2 punkt c.

Kõigi kolmandatest riikidest pärit vastuvõtjatega lepitakse enne isikuandmete esmakordset edastamist kokku Euroopa Liidu standardsetes lepingutingimustes või muudes asjakohastes kaitsemeetmetes. Seega on tagatud asjakohased kaitsemeetmed, jõustatavad andmesubjekti õigused ja tõhusad õiguskaitsevahendid andmesubjektidele. Iga andmesubjekt võib meilt saada koopia tüüplepinguklauslitest. Lepingustandardklauslid on kättesaadavad ka Euroopa Liidu Teatajas.

Andmekaitse üldmääruse artikli 45 lõige 3 annab Euroopa Komisjonile õiguse otsustada rakendusaktiga, et väljaspool ELi asuv riik tagab piisava kaitsetaseme. See tähendab isikuandmete kaitse taset, mis on üldjoontes samaväärne ELi tasemega. Piisava kaitsetaseme tuvastamise otsuste tagajärjeks on see, et isikuandmed võivad vabalt liikuda EList (ja Norrast, Liechtensteinist ja Islandist) kolmandasse riiki ilma täiendavate takistusteta. Sarnaseid eeskirju kohaldatakse Ühendkuningriigis, Šveitsis ja mõnes teises riigis.

Juhul kui Euroopa Komisjon või mõne muu riigi valitsus otsustab, et kolmas riik pakub piisavat kaitsetaset, ja kohaldatava raamistiku (nt EU-U.S. Data Privacy Framework, Swiss-U.S. Data Privacy Framework, UK Extension to the EU-U.S. Data Privacy Framework) puhul põhinevad kõik meie poolt selliste raamistike liikmetele (nt isesertifitseeritud üksused) tehtavad edastused üksnes nende üksuste liikmelisusel asjaomases raamistikus. Juhul kui meie või üks meie kontserni kuuluvatest üksustest on sellise raamistiku liige, põhinevad kõik edastused meile või meie kontserni kuuluvale üksusele üksnes selle üksuse liikmelisusel sellises raamistikus.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

Iga andmesubjekt võib meilt saada raamistiku koopia. Lisaks on raamistikud kättesaadavad ka Euroopa Liidu Teatajas või avaldatud õigusmaterjalides või järelevalveasutuste või muude pädevate asutuste või institutsioonide veebisaitidel.

## F. Isikuandmete säilitamise ajavahemik või, kui see ei ole võimalik, sellise ajavahemiku määramise kriteeriumid (isikuandmete kaitse üldmääruse artikli 13 lõike 2 punkt a).

Taotlejate isikuandmete säilitamise kestus on 6 kuud. Töötajate andmete puhul kohaldatakse vastavat seadusjärgset säilitamisperioodi. Pärast selle tähtaja möödumist kustutatakse vastavad andmed rutiinselt, kui need ei ole enam vajalikud lepingu täitmiseks või lepingu algatamiseks.

## G. Teave õiguse kohta taotleda vastutavalt töötlejalt juurdepääsu andmesubjekti puudutavatele isikuandmetele ning nende parandamist või kustutamist või isikuandmete töötlemise piiramist või esitada vastuväide selliste isikuandmete töötlemisele, samuti teave isikuandmete ülekandmise õiguse kohta (isikuandmete kaitse üldmääruse artikli 13 lõike 2 punkt b).

Kõigil andmesubjektidel on järgmised õigused:

***Juurdepääsuõigus***

Igal andmesubjektil on õigus tutvuda teda puudutavate isikuandmetega. Juurdepääsuõigus laieneb kõigile meie poolt töödeldavatele andmetele. Seda õigust saab kasutada lihtsalt ja mõistlike ajavahemike järel, et olla teadlik töötlemise seaduslikkusest ja seda kontrollida (isikuandmete kaitse üldmääruse põhjendus 63). See õigus tuleneb art. 15 GDPR. Andmesubjekt võib meiega ühendust võtta, et kasutada juurdepääsuõigust.

***Õigus andmete parandamisele***

GDPR artikli 16 lause 1 kohaselt on andmesubjektil õigus saada vastutavalt töötlejalt põhjendamatu viivituseta teda puudutavate ebatäpsete isikuandmete parandamine. Lisaks on GDPRi artikli 16 lause 2 kohaselt andmesubjektil õigus, võttes arvesse töötlemise eesmärke, saada puudulikud isikuandmed täiendatud, sealhulgas täiendava avalduse esitamise teel. Andmesubjekt võib meiega ühendust võtta, et kasutada õigust andmete parandamisele.

***Õigus andmete kustutamisele (õigus olla unustatud)***

Lisaks on andmesubjektidel õigus andmete kustutamisele ja unustamisele vastavalt art. 17 GDPR. Seda õigust saab samuti kasutada, võttes meiega ühendust. Siinkohal soovime siiski rõhutada, et see õigus ei kehti, kui töötlemine on vajalik meie ettevõtte suhtes kehtiva juriidilise kohustuse täitmiseks, GDPR artikli 17 lõike 3 punkt b. See tähendab, et me saame kustutamise taotluse heaks kiita alles pärast seadusest tuleneva säilitamisperioodi lõppu.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

***Õigus töötlemise piiramisele***

Vastavalt GDPR artiklile 18 on igal andmesubjektil õigus töötlemise piiramisele. Töötlemise piiramist võib nõuda, kui on täidetud üks GDPRi artikli 18 lõike 1 punktides a-d sätestatud tingimustest. Andmesubjekt võib meiega ühendust võtta, et kasutada õigust töötlemise piiramisele.

***Õigus esitada vastuväiteid***

Lisaks sellele on artikkel. 21 GDPR tagab õiguse esitada vastuväiteid. Andmesubjekt võib meiega ühendust võtta, et kasutada vastuväite esitamise õigust.

***Õigus andmete ülekantavusele***

Art. 20 GDPR annab andmesubjektile õiguse andmete ülekantavusele. Selle sätte kohaselt on andmesubjektil üldmääruse artikli 20 lõike 1 punktides a ja b sätestatud tingimustel õigus saada teda puudutavad isikuandmed, mille ta on vastutavale töötlejale esitanud, struktureeritud, üldkasutatavas ja masinloetavas vormingus ning õigus edastada need andmed teisele vastutavale töötlejale, ilma et vastutav töötleja, kellele isikuandmed esitati, neid takistaks. Andmesubjekt võib meiega ühendust võtta, et kasutada õigust andmete ülekandmisele.

## H. Kui isikuandmete töötlemine põhineb artikli 6 lõike 1 punktil a või artikli 9 lõike 2 punktil a, siis teave õiguse kohta nõusolek igal ajal tagasi võtta, ilma et see mõjutaks enne tagasivõtmist nõusoleku alusel toimunud töötlemise seaduslikkust (GDPRi artikli 13 lõike 2 punkt c).

Kui isikuandmete töötlemise aluseks on art. 6 lõike 1 punkti a GDPR, mis on nii, kui andmesubjekt on andnud nõusoleku isikuandmete töötlemiseks ühel või mitmel konkreetsel eesmärgil, või põhineb see GDPR artikli 9 lõike 2 punkti a alusel, mis reguleerib selgesõnalist nõusolekut isikuandmete eriliikide töötlemiseks, on andmesubjektil vastavalt GDPR artikli 7 lõike 3 esimesele lausele 1 õigus oma nõusolek igal ajal tagasi võtta.

Nõusoleku tagasivõtmine ei mõjuta nõusolekul põhineva töötlemise seaduslikkust enne selle tagasivõtmist, isikuandmete kaitse üldmääruse artikli 7 lõike 3 lause 2. Nõusoleku tagasivõtmine peab olema sama lihtne kui selle andmine, art. 7 lõike 3 lause 4 GDPR. Seega võib nõusoleku tagasivõtmine alati toimuda samal viisil, nagu nõusolek on antud, või muul viisil, mida andmesubjekt peab lihtsamaks. Tänapäeva infoühiskonnas on tõenäoliselt kõige lihtsam viis nõusoleku tagasivõtmiseks lihtne e-kiri. Kui andmesubjekt soovib oma meile antud nõusolekut tagasi võtta, piisab lihtsast e-kirjast meile. Alternatiivina võib andmesubjekt valida mis tahes muu viisi oma nõusoleku tagasivõtmisest teatamiseks.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## I. Teave õiguse kohta esitada kaebus järelevalveasutusele (isikuandmete kaitse üldmääruse artikli 13 lõike 2 punkt d, artikli 77 lõige 1).

Vastutava töötlejana oleme kohustatud teavitama andmesubjekti õigusest esitada kaebus järelevalveasutusele, GDPR artikli 13 lõike 2 punkt d. Õigus esitada kaebus järelevalveasutusele on reguleeritud GDPRi artikli 77 lõikega 1. Selle sätte kohaselt on igal andmesubjektil õigus esitada kaebus järelevalveasutusele, eelkõige oma alalise elukoha, töökoha või väidetava rikkumise koha liikmesriigis, kui andmesubjekt leiab, et teda puudutavate isikuandmete töötlemine on vastuolus isikuandmete kaitse üldmäärusega, ilma et see piiraks muude haldus- või õiguskaitsevahendite kasutamist. Õigus esitada kaebus järelevalveasutusele on liidu õigusega piiratud ainult selliselt, et seda saab kasutada ainult ühe järelevalveasutuse ees (isikuandmete kaitse üldmääruse põhjenduse 141 lause 1). Selle reegli eesmärk on vältida sama andmesubjekti topeltkaebusi samas küsimuses. Kui andmesubjekt soovib esitada meie kohta kaebuse, palume seetõttu pöörduda ainult ühe järelevalveasutuse poole.

## J. Teave selle kohta, kas isikuandmete esitamine on õigusaktist või lepingust tulenev kohustus või lepingu sõlmimiseks vajalik nõue, samuti selle kohta, kas andmesubjekt on kohustatud kõnealuseid isikuandmeid esitama, ning selliste andmete esitamata jätmise võimalike tagajärgede kohta, ning (isikuandmete kaitse üldmääruse artikli 13 lõike 2 punkt e).

Selgitame, et isikuandmete esitamist nõuab osaliselt seadus (nt maksueeskirjad) või see võib tuleneda ka lepingulistest sätetest (nt teave lepingupartneri kohta).

Mõnikord võib lepingu sõlmimiseks olla vajalik, et andmesubjekt edastab meile isikuandmeid, mida peame seejärel töötlema. Andmesubjekt on näiteks kohustatud esitama meile isikuandmeid, kui meie ettevõte sõlmib temaga lepingu. Isikuandmete esitamata jätmine tooks kaasa selle, et lepingut andmesubjektiga ei saa sõlmida.

Enne kui andmesubjekt esitab isikuandmed, peab ta meiega ühendust võtma. Selgitame andmesubjektile, kas isikuandmete esitamine on seadusest või lepingust tulenevalt nõutav või lepingu sõlmimiseks vajalik, kas isikuandmete esitamine on kohustuslik ja millised on isikuandmete esitamata jätmise tagajärjed.

## K. Teave artikli 22 lõigetes 1 ja 4 osutatud automatiseeritud otsuste, sealhulgas profiilianalüüsi tegemise kohta ning vähemalt nendel juhtudel sisuline teave kasutatava loogika ja selle kohta, millised on sellise isikuandmete töötlemise tähtsus ja prognoositavad tagajärjed andmesubjekti jaoks (GDPR artikli 13 lõike 2 punkt f).

Vastutustundliku ettevõttena ei kasuta me tavaliselt automatiseeritud otsuste tegemist ega profiilide koostamist. Kui erandjuhtudel kasutame automatiseeritud otsuste tegemist või profiilianalüüsi, teavitame


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

sellest andmesubjekti kas eraldi või meie privaatsuspoliitika alajaotuse kaudu (meie veebisaidil). Sellisel juhul kohaldatakse järgmist:

Automatiseeritud otsuste tegemine - sealhulgas profiilianalüüs - võib toimuda, kui 1) see on vajalik andmesubjekti ja meie vahelise lepingu sõlmimiseks või täitmiseks või 2) see on lubatud liidu või liikmesriigi õigusega, mida me kohaldame ja mis sätestab ka sobivad meetmed andmesubjekti õiguste ja vabaduste ning õigustatud huvide kaitsmiseks, või 3) see põhineb andmesubjekti selgesõnalisel nõusolekul.

GDPR artikli 22 lõike 2 punktides a ja c osutatud juhtudel rakendame sobivaid meetmeid andmesubjekti õiguste ja vabaduste ning õigustatud huvide kaitsmiseks. Sellistel juhtudel on teil õigus saada vastutava töötleja poolset inimlikku sekkumist, väljendada oma seisukohta ja vaidlustada otsus.

Meie privaatsuspoliitikas on esitatud sisuline teave asjaomase loogika kohta, samuti sellise töötlemise tähtsus ja kavandatud tagajärjed andmesubjektile.

## II. Teave, mis tuleb esitada juhul, kui isikuandmed ei ole saadud andmesubjektilt (GDPR artikkel 14)

### A. Vastutava töötleja ning asjakohasel juhul vastutava töötleja esindaja nimi ja kontaktandmed (GDPR artikli 14 lõike 1 punkt a)

Vt eespool

### B. Asjakohasel juhul andmekaitseametniku kontaktandmed (isikuandmete kaitse üldmääruse artikli 14 lõike 1 punkt b).

Vt eespool

### C. Isikuandmete töötlemise eesmärk ja õiguslik alus (isikuandmete kaitse üldmääruse artikli 14 lõike 1 punkt c).

Taotleja andmete puhul, mida ei ole kogutud andmesubjektilt, on andmete töötlemise eesmärk taotluse läbivaatamine värbamisprotsessi käigus. Sel eesmärgil võime töödelda andmeid, mida ei ole kogutud teilt. Värbamisprotsessi käigus töödeldavate andmete põhjal kontrollime, kas teid kutsutakse tööintervjuule (valikuprotsessi osa). Kui teid võetakse tööle, muutuvad kandidaadi andmed automaatselt töötaja andmeteks. Töötaja andmete puhul on andmete töötlemise eesmärk töölepingu täitmine või muude töösuhte suhtes kohaldatavate õigusnormide täitmine. Töötaja andmeid säilitatakse pärast töösuhte lõppemist, et täita seaduslikke säilitustähtaegu.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

Andmete töötlemise õiguslik alus on isikuandmete kaitse üldmääruse artikli 6 lõike 1 punktide b ja f, artikli 9 lõike 2 punktide b ja h, artikli 88 lõike 1 ja siseriiklike õigusaktide, näiteks Saksamaa puhul § 26 BDSG (föderaalne andmekaitseseadus).

## D. Asjaomaste isikuandmete liigid (GDPR artikli 14 lõike 1 punkt d)

Taotleja andmed

Töötajate andmed

## E. Asjakohasel juhul teave isikuandmete vastuvõtjate või vastuvõtjate kategooriate kohta (isikuandmete kaitse üldmääruse artikli 14 lõike 1 punkt e).

Riigiasutused

Välised asutused

Täiendavad välised asutused

Sisemine töötlemine

Kontsernisisene töötlemine

Muud asutused

Meie volitatud töötlejate ja andmete saajate nimekiri kolmandates riikides ja vajaduse korral rahvusvaheliste organisatsioonide nimekiri on avaldatud meie veebilehel või seda saab meilt tasuta küsida. Selle nimekirja taotlemiseks võtke palun ühendust meie andmekaitseametnikuga.


© All rights reserved by Heiko Maniero.

## F. Asjakohasel juhul teave selle kohta, et vastutav töötleja kavatseb edastada isikuandmed kolmandas riigis asuvale vastuvõtjale või rahvusvahelisele organisatsioonile, ning teave kaitse piisavust käsitleva komisjoni otsuse olemasolu või puudumise kohta või artiklis 46 või 47 või artikli 49 lõike 1 teises lõigus osutatud edastamise korral viide asjakohastele või sobivatele kaitsemeetmetele ja nende koopia saamise viisile või kohale, kus need on tehtud kättesaadavaks (isikuandmete kaitse üldmääruse artikli 14 lõike 1 punkt f, artikli 46 lõige 1, artikli 46 lõike 2 punkt c).

Kõik meie kontserni kuuluvad ettevõtted ja filiaalid (edaspidi "kontserni ettevõtted"), mille tegevuskoht või kontor asub kolmandas riigis, võivad kuuluda isikuandmete vastuvõtjate hulka. Kõigi kontserni ettevõtete või vastuvõtjate nimekirja saab meilt küsida.

Vastavalt isikuandmete kaitse üldmääruse artikli 46 lõikele 1 võib vastutav töötleja või volitatud töötleja edastada isikuandmeid kolmandale riigile üksnes juhul, kui vastutav töötleja või volitatud töötleja on näinud ette asjakohased kaitsemeetmed ja tingimusel, et andmesubjektidele on kättesaadavad jõustatavad andmesubjekti õigused ja tõhusad õiguskaitsevahendid. Asjakohaseid kaitsemeetmeid võib pakkuda ilma järelevalveasutuse eriluba nõudmata, kasutades selleks standardseid andmekaitseklausleid, isikuandmete kaitse üldmääruse artikli 46 lõike 2 punkt c.

Kõigi kolmandatest riikidest pärit vastuvõtjatega lepitakse enne isikuandmete esmakordset edastamist kokku Euroopa Liidu standardsetes lepingutingimustes või muudes asjakohastes kaitsemeetmetes. Seega on tagatud asjakohased kaitsemeetmed, jõustatavad andmesubjekti õigused ja tõhusad õiguskaitsevahendid andmesubjektidele. Iga andmesubjekt võib meilt saada koopia tüüplepinguklauslitest. Lepingustandardklauslid on kättesaadavad ka Euroopa Liidu Teatajas.

Andmekaitse üldmääruse artikli 45 lõige 3 annab Euroopa Komisjonile õiguse otsustada rakendusaktiga, et väljaspool ELi asuv riik tagab piisava kaitsetaseme. See tähendab isikuandmete kaitse taset, mis on üldjoontes samaväärne ELi tasemega. Piisava kaitsetaseme tuvastamise otsuste tagajärjeks on see, et isikuandmed võivad vabalt liikuda EList (ja Norrast, Liechtensteinist ja Islandist) kolmandasse riiki ilma täiendavate takistusteta. Sarnaseid eeskirju kohaldatakse Ühendkuningriigis, Šveitsis ja mõnes teises riigis.

Juhul kui Euroopa Komisjon või mõne muu riigi valitsus otsustab, et kolmas riik pakub piisavat kaitsetaset, ja kohaldatava raamistiku (nt EU-U.S. Data Privacy Framework, Swiss-U.S. Data Privacy Framework, UK Extension to the EU-U.S. Data Privacy Framework) puhul põhinevad kõik meie poolt selliste raamistike liikmetele (nt isesertifitseeritud üksused) tehtavad edastused üksnes nende üksuste liikmelisusel asjaomases raamistikus. Juhul kui meie või üks meie kontserni kuuluvatest üksustest on sellise raamistiku liige, põhinevad kõik edastused meile või meie kontserni kuuluvale üksusele üksnes selle üksuse liikmelisusel sellises raamistikus.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

Iga andmesubjekt võib meilt saada raamistiku koopia. Lisaks on raamistikud kättesaadavad ka Euroopa Liidu Teatajas või avaldatud õigusmaterjalides või järelevalveasutuste või muude pädevate asutuste või institutsioonide veebisaitidel.

## G. Isikuandmete säilitamise ajavahemik või, kui see ei ole võimalik, sellise ajavahemiku määramise kriteeriumid (isikuandmete kaitse üldmääruse artikli 14 lõike 2 punkt a).

Taotlejate isikuandmete säilitamise kestus on 6 kuud. Töötajate andmete puhul kohaldatakse vastavat seadusjärgset säilitamisperioodi. Pärast selle tähtaja möödumist kustutatakse vastavad andmed rutiinselt, kui need ei ole enam vajalikud lepingu täitmiseks või lepingu algatamiseks.

## H. Kui isikuandmete töötlemine põhineb artikli 6 lõike 1 punktil f, siis teave vastutava töötleja või kolmanda isiku õigustatud huvide kohta (isikuandmete kaitse üldmääruse artikli 14 lõike 2 punkt b).

Vastavalt isikuandmete kaitse üldmääruse artikli 6 lõike 1 punktile f on töötlemine seaduslik ainult siis, kui töötlemine on vajalik vastutava töötleja või kolmanda isiku õigustatud huvide kaitseks, välja arvatud juhul, kui need huvid on ülimuslikud seoses andmesubjekti huvide või põhiõiguste ja -vabadustega, mis nõuavad isikuandmete kaitset. Vastavalt isikuandmete kaitse üldmääruse põhjenduse 47 teisele lausele võib õigustatud huvi olla olemas, kui andmesubjekti ja vastutava töötleja vahel on asjakohane ja asjakohane suhe, näiteks olukorras, kus andmesubjekt on vastutava töötleja klient. Kõigil juhtudel, mil meie ettevõte töötleb kandidaadi andmeid GDPRi artikli 6 lõike 1 punkti f alusel, on meie õigustatud huvi sobivate töötajate ja spetsialistide töölevõtmine.

## I. Teave õiguse kohta taotleda vastutavalt töötlejalt juurdepääsu andmesubjekti puudutavatele isikuandmetele ning nende parandamist või kustutamist või isikuandmete töötlemise piiramist ning esitada vastuväide selliste isikuandmete töötlemisele, samuti teave isikuandmete ülekandmise õiguse kohta (isikuandmete kaitse üldmääruse artikli 14 lõike 2 punkt c).

Kõigil andmesubjektidel on järgmised õigused:

***Juurdepääsuõigus***

Igal andmesubjektil on õigus tutvuda teda puudutavate isikuandmetega. Juurdepääsuõigus laieneb kõigile meie poolt töödeldavatele andmetele. Seda õigust saab kasutada lihtsalt ja mõistlike ajavahemike järel, et olla teadlik töötlemise seaduslikkusest ja seda kontrollida (isikuandmete kaitse üldmääruse


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

põhjendus 63). See õigus tuleneb art. 15 GDPR. Andmesubjekt võib meiega ühendust võtta, et kasutada juurdepääsuõigust.

***Õigus andmete parandamisele***

GDPR artikli 16 lause 1 kohaselt on andmesubjektil õigus saada vastutavalt töötlejalt põhjendamatu viivituseta teda puudutavate ebatäpsete isikuandmete parandamine. Lisaks on GDPRi artikli 16 lause 2 kohaselt andmesubjektil õigus, võttes arvesse töötlemise eesmärke, saada puudulikud isikuandmed täiendatud, sealhulgas täiendava avalduse esitamise teel. Andmesubjekt võib meiega ühendust võtta, et kasutada õigust andmete parandamisele.

***Õigus andmete kustutamisele (õigus olla unustatud)***

Lisaks on andmesubjektidel õigus andmete kustutamisele ja unustamisele vastavalt art. 17 GDPR. Seda õigust saab samuti kasutada, võttes meiega ühendust. Siinkohal soovime siiski rõhutada, et see õigus ei kehti, kui töötlemine on vajalik meie ettevõtte suhtes kehtiva juriidilise kohustuse täitmiseks, GDPR artikli 17 lõike 3 punkt b. See tähendab, et me saame kustutamise taotluse heaks kiita alles pärast seadusest tuleneva säilitamisperioodi lõppu.

***Õigus töötlemise piiramisele***

Vastavalt GDPR artiklile 18 on igal andmesubjektil õigus töötlemise piiramisele. Töötlemise piiramist võib nõuda, kui on täidetud üks GDPRi artikli 18 lõike 1 punktides a-d sätestatud tingimustest. Andmesubjekt võib meiega ühendust võtta, et kasutada õigust töötlemise piiramisele.

***Õigus esitada vastuväiteid***

Lisaks sellele on artikkel. 21 GDPR tagab õiguse esitada vastuväiteid. Andmesubjekt võib meiega ühendust võtta, et kasutada vastuväite esitamise õigust.

***Õigus andmete ülekantavusele***

Art. 20 GDPR annab andmesubjektile õiguse andmete ülekantavusele. Selle sätte kohaselt on andmesubjektil üldmääruse artikli 20 lõike 1 punktides a ja b sätestatud tingimustel õigus saada teda puudutavad isikuandmed, mille ta on vastutavale töötlejale esitanud, struktureeritud, üldkasutatavas ja masinloetavas vormingus ning õigus edastada need andmed teisele vastutavale töötlejale, ilma et vastutav töötleja, kellele isikuandmed esitati, neid takistaks. Andmesubjekt võib meiega ühendust võtta, et kasutada õigust andmete ülekandmisele.

## J. Kui isikuandmete töötlemine põhineb artikli 6 lõike 1 punktil a või artikli 9 lõike 2 punktil a, siis teave õiguse kohta nõusolek igal ajal tagasi võtta, ilma et see mõjutaks enne tagasivõtmist nõusoleku alusel toimunud isikuandmete töötlemise seaduslikkust (GDPRi artikli 14 lõike 2 punkt d).

Kui isikuandmete töötlemise aluseks on art. 6 lõike 1 punkti a GDPR, mis on nii, kui andmesubjekt on andnud nõusoleku isikuandmete töötlemiseks ühel või mitmel konkreetsel eesmärgil, või põhineb see


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

GDPR artikli 9 lõike 2 punkti a alusel, mis reguleerib selgesõnalist nõusolekut isikuandmete eriliikide töötlemiseks, on andmesubjektil vastavalt GDPR artikli 7 lõike 3 esimesele lausele 1 õigus oma nõusolek igal ajal tagasi võtta.

Nõusoleku tagasivõtmine ei mõjuta nõusolekul põhineva töötlemise seaduslikkust enne selle tagasivõtmist, isikuandmete kaitse üldmääruse artikli 7 lõike 3 lause 2. Nõusoleku tagasivõtmine peab olema sama lihtne kui selle andmine, art. 7 lõike 3 lause 4 GDPR. Seega võib nõusoleku tagasivõtmine alati toimuda samal viisil, nagu nõusolek on antud, või muul viisil, mida andmesubjekt peab lihtsamaks. Tänapäeva infoühiskonnas on tõenäoliselt kõige lihtsam viis nõusoleku tagasivõtmiseks lihtne e-kiri. Kui andmesubjekt soovib oma meile antud nõusolekut tagasi võtta, piisab lihtsast e-kirjast meile. Alternatiivina võib andmesubjekt valida mis tahes muu viisi oma nõusoleku tagasivõtmisest teatamiseks.

## K. Teave õiguse kohta esitada kaebus järelevalveasutusele (isikuandmete kaitse üldmääruse artikli 14 lõike 2 punkt e, artikli 77 lõige 1).

Vastutava töötlejana oleme kohustatud teavitama andmesubjekti õigusest esitada kaebus järelevalveasutusele, GDPR artikli 14 lõike 2 punkt e. Õigus esitada kaebus järelevalveasutusele on reguleeritud GDPRi artikli 77 lõikega 1. Selle sätte kohaselt on igal andmesubjektil õigus esitada kaebus järelevalveasutusele, eelkõige oma alalise elukoha, töökoha või väidetava rikkumise koha liikmesriigis, kui andmesubjekt leiab, et teda puudutavate isikuandmete töötlemine on vastuolus üldise andmekaitse määrusega, ilma et see piiraks muude haldus- või õiguskaitsevahendite kasutamise võimalust, kui andmesubjekt leiab, et teda puudutavate isikuandmete töötlemine on vastuolus üldise andmekaitse määrusega. Õigus esitada kaebus järelevalveasutusele on liidu õigusega piiratud ainult selliselt, et seda saab kasutada ainult ühe järelevalveasutuse ees (isikuandmete kaitse üldmääruse põhjenduse 141 lause 1). Selle reegli eesmärk on vältida sama andmesubjekti topeltkaebusi samas küsimuses. Kui andmesubjekt soovib esitada meie kohta kaebuse, palume seetõttu pöörduda ainult ühe järelevalveasutuse poole.

## L. Teave isikuandmete päritoluallika ning asjakohasel juhul selle kohta, kas need pärinevad avalikult kättesaadavatest allikatest (isikuandmete kaitse üldmääruse artikli 14 lõike 2 punkt f).

Põhimõtteliselt kogutakse isikuandmeid otse andmesubjektilt või koostöös asutusega (nt andmete hankimine ametlikust registrist). Muud andmed andmesubjektide kohta saadakse kontserni äriühingute andmete edastamisest. Selle üldise teabe kontekstis on isikuandmete päritolu täpsete allikate nimetamine kas võimatu või tähendaks ebaproportsionaalselt suurt pingutust art. 14 lõike 5 punkti b tähenduses. Põhimõtteliselt ei kogu me isikuandmeid avalikult kättesaadavatest allikatest.

Iga andmesubjekt võib meiega igal ajal ühendust võtta, et saada täpsemat teavet teda puudutavate isikuandmete täpsete allikate kohta. Kui andmesubjektile ei ole võimalik esitada isikuandmete päritolu,


© All rights reserved by Heiko Maniero.

sest on kasutatud erinevaid allikaid, tuleks esitada üldine teave (isikuandmete kaitse üldmääruse põhjendus 61, 4. lause).

### M. Teave artikli 22 lõigetes 1 ja 4 osutatud automatiseeritud otsuste, sealhulgas profiilianalüüsi tegemise kohta ning vähemalt nendel juhtudel sisuline teave kasutatava loogika ja selle kohta, millised on sellise töötlemise tähtsus ja prognoositavad tagajärjed andmesubjekti jaoks (GDPR artikli 14 lõike 2 punkt g).

Vastutustundliku ettevõttena ei kasuta me tavaliselt automatiseeritud otsuste tegemist ega profiilide koostamist. Kui erandjuhtudel kasutame automatiseeritud otsuste tegemist või profiilianalüüsi, teavitame sellest andmesubjekti kas eraldi või meie privaatsuspoliitika alajaotuse kaudu (meie veebisaidil). Sellisel juhul kohaldatakse järgmist:

Automatiseeritud otsuste tegemine - sealhulgas profiilianalüüs - võib toimuda, kui 1) see on vajalik andmesubjekti ja meie vahelise lepingu sõlmimiseks või täitmiseks või 2) see on lubatud liidu või liikmesriigi õigusega, mida me kohaldame ja mis sätestab ka sobivad meetmed andmesubjekti õiguste ja vabaduste ning õigustatud huvide kaitsmiseks, või 3) see põhineb andmesubjekti selgesõnalisel nõusolekul.

GDPR artikli 22 lõike 2 punktides a ja c osutatud juhtudel rakendame sobivaid meetmeid andmesubjekti õiguste ja vabaduste ning õigustatud huvide kaitsmiseks. Sellistel juhtudel on teil õigus saada vastutava töötleja poolset inimlikku sekkumist, väljendada oma seisukohta ja vaidlustada otsus.

Meie privaatsuspoliitikas on esitatud sisuline teave asjaomase loogika kohta, samuti sellise töötlemise tähtsus ja kavandatud tagajärjed andmesubjektile.

## III. EU-U.S. Data Privacy Framework (EU-U.S. DPF), UK Extension to the EU-U.S. DPF, Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF)

Kui meie organisatsioon on EU-U.S. Data Privacy Framework (EU-U.S. DPF) ja/või UK Extension to the EU-U.S. DPF ja/või Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF) sertifitseeritud liige, kehtib järgmine:

Me järgime EU-U.S. Data Privacy Framework (EU-U.S. DPF), UK Extension to the EU-U.S. DPF ja Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF) vastavalt U.S. Department of Commerce kehtestatud nõuetele. Meie ettevõte on USA Kaubandusministeeriumile kinnitanud, et see järgib EU-U.S. Data Privacy Framework Principles (EU-U.S. DPF Principles) isikuandmete töötlemisel, mida ta saab Euroopa Liidust ja Ühendkuningriigist, tuginedes EU-U.S. DPF ja UK Extension to the EU-U.S. DPF-le. Meie ettevõte on USA Kaubandusministeeriumile kinnitanud, et see järgib Swiss-U.S. Data Privacy


© All rights reserved by Heiko Maniero.

Framework Principles (Swiss-U.S. DPF Principles) isikuandmete töötlemisel, mida ta saab Šveitsist, tuginedes Swiss-U.S. DPF-le. Kui meie privaatsuspoliitika sätted on vastuolus EU-U.S. DPF Principles ja/või Swiss-U.S. DPF Principles-ga, on määravad Principles.

Et rohkem teada saada Data Privacy Framework (DPF) programmi kohta ja meie sertifikaati vaadata, külastage palun https://www.dataprivacyframework.gov/.

Meie ettevõtte teised USA üksused või tütarettevõtted, mis samuti järgivad EU-U.S. DPF Principles, sealhulgas UK Extension to the EU-U.S. DPF ja Swiss-U.S. DPF Principles, kui neid on, on meie privaatsuspoliitikas nimetatud.

Kooskõlas EU-U.S. DPF, UK Extension to the EU-U.S. DPF ja Swiss-U.S. DPF-ga kohustub meie ettevõte tegema koostööd Euroopa andmekaitseasutuste ja Briti Information Commissioner's Office (ICO) ning Šveitsi Federal Data Protection and Information Commissioner (EDÖB) poolt loodud organitega ja järgima nende nõuandeid seoses lahendamata kaebustega meie isikuandmete töötlemise kohta, mida me saame tuginedes EU-U.S. DPF-le, UK Extension to the EU-U.S. DPF-le ja Swiss-U.S. DPF-le.

Me teavitame asjaosalisi isikuid pädevatest Euroopa andmekaitseasutustest, mis vastutavad meie organisatsiooni isikuandmete töötlemise kaebuste lahendamise eest, selle läbipaistvusdokumendi ülaosas ja sellest, et me pakume asjaosalistele isikutele asjakohaseid ja tasuta õiguskaitsevahendeid.

Me teavitame kõiki asjaosalisi isikuid, et meie ettevõte allub Federal Trade Commission (FTC) uurimis- ja täitevvõimudele.

Asjaosalised isikud saavad teatud tingimustel taotleda siduvat vahekohtu menetlust. Meie organisatsioon on kohustatud lahendama nõudeid ja järgima DPF-Principals lisa I tingimusi, kui asjaosaline isik on taotlenud siduvat vahekohtu menetlust, teavitades sellest meie organisatsiooni ja järgides lisa I Principles tingimusi ja protseduure.

Me teavitame kõiki asjaosalisi isikuid meie organisatsiooni vastutusest isikuandmete edastamisel kolmandatele isikutele.

Asjaosaliste isikute või andmekaitseasutuste küsimuste puhul oleme määranud kohalikke esindajaid, kes on nimetatud selle läbipaistvusdokumendi ülaosas.

Pakume teile võimalust valida (Opt-out), kas teie isikuandmeid (i) edastatakse kolmandatele isikutele või (ii) kasutatakse eesmärgil, mis erineb oluliselt sellest, milleks need algselt koguti või mille jaoks te hiljem oma nõusoleku andsite. Teie valikuvõimaluse kasutamiseks selge, hästi nähtav ja kergesti ligipääsetav mehhanism on meie andmekaitseametnikuga (DSB) e-posti teel ühendust võtmine. Teil ei ole valikuvõimalust ja me ei ole kohustatud seda tegema, kui andmed edastatakse kolmandale isikule, kes tegutseb meie nimel ja meie juhiste järgi. Siiski sõlmime alati sellise esindaja või andmetöötlejaga lepingu.

Tundlike andmete (s.t. isikuandmed, mis sisaldavad teavet tervisliku seisundi, rassilise või etnilise päritolu, poliitiliste vaadete, usuliste või filosoofiliste veendumuste, ametiühingu liikmelisuse või


© All rights reserved by Heiko Maniero.

asjaosalise isiku seksuaalelu kohta) puhul saame teie selgesõnalise nõusoleku (Opt-in), kui need andmed (i) edastatakse kolmandatele isikutele või (ii) kasutatakse muul eesmärgil, kui need algselt koguti või mille jaoks te hiljem oma nõusoleku andsite, tehes oma Opt-in valiku. Lisaks käsitleme kõiki kolmandatelt isikutelt saadud isikuandmeid tundlikena, kui kolmas isik need tundlikeks määrab ja käsitleb.

Teavitame teid siinkohal nõudest avaldada isikuandmeid valitsusasutuste seaduslike päringute korral, sealhulgas täita riikliku julgeoleku või õiguskaitse nõudeid.

Isikuandmete edastamisel kolmandale isikule, kes tegutseb vastutava töötlejana, järgime teavitamise ja valikuvõimaluse põhimõtteid (Principals). Samuti sõlmime vastutava töötlejaga lepingu, mis sätestab, et need andmed võib töödelda ainult piiratud ja kindlaksmääratud eesmärkidel vastavalt teie antud nõusolekule ja et saaja pakub samal tasemel kaitset kui DPF-Principals ning teavitab meid, kui ta leiab, et ta ei suuda seda kohustust enam täita. Leping sätestab, et vastutav töötleja lõpetab töötlemise või võtab muud asjakohased ja piisavad meetmed olukorra parandamiseks, kui selline olukord ilmneb.

Isikuandmete edastamisel kolmandale isikule, kes tegutseb esindaja või andmetöötlejana, (i) edastame need andmed ainult piiratud ja kindlaksmääratud eesmärkidel; (ii) veendume, et esindaja või andmetöötleja on kohustatud tagama vähemalt samal tasemel andmekaitse, nagu nõutud DPF-Principals; (iii) võtame asjakohased ja piisavad meetmed, et tagada esindaja või andmetöötleja tegelik isikuandmete töötlemine viisil, mis on kooskõlas meie kohustustega vastavalt DPF-Principals; (iv) nõuame esindajalt või andmetöötlejalt meie organisatsiooni teavitamist, kui ta leiab, et ta ei suuda enam täita kohustust pakkuda samal tasemel kaitset nagu nõutud DPF-Principals; (v) teate saamisel, sealhulgas punktis (iv) nimetatud teate puhul, võtame asjakohased ja piisavad meetmed loata töötlemise peatamiseks ja olukorra parandamiseks; ning (vi) DPF Departmenti taotlusel esitame kokkuvõtte või esindusliku eksemplari asjakohastest andmekaitse sätetest lepingus selle esindajaga.

Kooskõlas EU-U.S. DPF ja/või UK Extension to the EU-U.S. DPF ja/või Swiss-U.S. DPF-ga kohustub meie organisatsioon tegema koostööd Euroopa andmekaitseasutuste ja Briti Information Commissioner's Office (ICO) ning Šveitsi Federal Data Protection and Information Commissioner (EDÖB) poolt loodud organitega ja järgima nende nõuandeid seoses lahendamata kaebustega meie isikuandmete töötlemise kohta seoses töösuhetega, mida me saame tuginedes EU-U.S. DPF-le, UK Extension to the EU-U.S. DPF-le ja Swiss-U.S. DPF-le.

Kõigil andmesubjektidel, kes viibivad ajutiselt Euroopa Liidus (EL), Euroopa Majanduspiirkonnas (EMP) või Ühendkuningriigis või kelle alaline või peamine elukoht on seal, on õigus meie läbipaistvusdokumendis avaldatud õigustele ja andmesubjekti õigustele, mis tulenevad ka isikuandmete kaitse üldmääruse artiklitest 15-22, sealhulgas õigus tutvuda isikuandmetega. Me oleme teinud selle teabe kättesaadavaks kõigis ELi ja EMP keeltes. Ingliskeelne versioon kehtib Ühendkuningriigis.

Kõigil andmesubjektidel, kes elavad ajutiselt Šveitsis või kelle alaline või peamine elukoht on seal, on õigus kasutada Šveitsi andmekaitseseadusest ja Šveitsi andmekaitsemäärusest tulenevaid õigusi ja andmesubjekti õigusi, mis on avaldatud meie läbipaistvusdokumendis, sealhulgas õigus tutvuda


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

isikuandmetega. Oleme esitanud selle teabe kolmes Šveitsi ametlikus keeles (saksa, itaalia ja prantsuse keeles).


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

# SWEDISH: Information om behandling av personuppgifter (artikel 13, 14 GDPR)

Kära herr eller fru,

Personuppgifterna för varje person som befinner sig i ett avtalsförhållande, ett föravtalsförhållande eller ett annat förhållande med vårt företag förtjänar särskilt skydd. Vårt mål är att hålla vår dataskyddsnivå på en hög nivå. Därför utvecklar vi rutinmässigt våra koncept för dataskydd och datasäkerhet.

Självklart följer vi de lagstadgade bestämmelserna om dataskydd. Enligt artikel 13 och 14 GDPR ska registeransvariga uppfylla särskilda informationskrav när de samlar in personuppgifter. Detta dokument uppfyller dessa skyldigheter.

Terminologin i de rättsliga bestämmelserna är komplicerad. Tyvärr kunde man inte undvika att använda juridiska termer vid utarbetandet av detta dokument. Därför vill vi påpeka att du alltid är välkommen att kontakta oss för alla frågor om detta dokument, de använda termerna eller formuleringarna.

## I. Information som ska tillhandahållas om personuppgifterna samlas in från den registrerade (artikel 13 GDPR)

### A. Identitet och kontaktuppgifter för den personuppgiftsansvarige och i tillämpliga fall för dennes företrädare (artikel 13.1 a GDPR)

Se ovan.

### B. Kontaktuppgifter för dataskyddsombudet, i tillämpliga fall (artikel 13.1 b GDPR)

Se ovan.

### C. Ändamålen med den behandling för vilken personuppgifterna är avsedda samt den rättsliga grunden för behandlingen (artikel 13.1 c GDPR)

Syftet med behandlingen av personuppgifter är att hantera all verksamhet som rör den personuppgiftsansvarige, kunder, potentiella kunder, affärspartner eller andra avtalsmässiga eller prekontraktuella förbindelser mellan de nämnda grupperna (i vidaste bemärkelse) eller den personuppgiftsansvariges rättsliga skyldigheter.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

Konst. 6(1) lit. a GDPR fungerar som rättslig grund för behandlingar för vilka vi erhåller samtycke för ett specifikt behandlingsändamål. Om behandlingen av personuppgifter är nödvändig för att fullgöra ett avtal i vilket den registrerade är part, vilket är fallet t.ex. när behandlingen är nödvändig för att leverera varor eller tillhandahålla någon annan tjänst, grundar sig behandlingen på artikel 6.1 b GDPR. Detsamma gäller för sådan behandling som är nödvändig för att genomföra åtgärder före avtalstillfället, till exempel vid förfrågningar om våra produkter eller tjänster. Om vårt företag är föremål för en rättslig förpliktelse som kräver behandling av personuppgifter, t.ex. för att uppfylla skattemässiga skyldigheter, grundar sig behandlingen på art. 6(1) lit. c GDPR.

I sällsynta fall kan behandlingen av personuppgifter vara nödvändig för att skydda den registrerades eller en annan fysisk persons vitala intressen. Detta skulle till exempel vara fallet om en besökare skadar sig i vårt företag och hans namn, ålder, sjukförsäkringsuppgifter eller annan viktig information måste överlämnas till en läkare, ett sjukhus eller en annan tredje part. Då skulle behandlingen baseras på art. 6(1) lit. d GDPR.

Om behandlingen är nödvändig för att utföra en uppgift som utförs av allmänt intresse eller för att utöva myndighet som tillkommer den registeransvarige, är den rättsliga grunden art. 6(1) lit. e GDPR.

Slutligen kan behandlingen baseras på artikel 6.1 f GDPR. Denna rättsliga grund används för behandlingar som inte omfattas av någon av de ovan nämnda rättsliga grunderna, om behandlingen är nödvändig för de legitima intressen som vårt företag eller en tredje part har, utom när dessa intressen åsidosätts av den registrerades intressen eller grundläggande rättigheter och friheter som kräver skydd av personuppgifter. Sådana behandlingar är särskilt tillåtna eftersom de har nämnts särskilt av den europeiska lagstiftaren. Han ansåg att ett legitimt intresse kunde antas om den registrerade är en kund till den registeransvarige (skäl 47, andra meningen GDPR).

## D. Om behandlingen är baserad på artikel 6.1 f, den personuppgiftsansvariges eller en tredje parts berättigade intressen (artikel 13.1 d GDPR)

När behandlingen av personuppgifter baseras på artikel 6.1 f GDPR är vårt legitima intresse att bedriva vår verksamhet för att främja välbefinnandet hos alla våra anställda och aktieägare.

## E. Mottagarna eller de kategorier av mottagare som ska ta del av personuppgifterna, i förekommande fall (artikel 13.1 e GDPR)

Offentliga myndigheter

Externa organ

Ytterligare externa organ


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

Intern bearbetning

Förädling inom en grupp

Andra organ

En förteckning över våra personuppgiftsbiträden och datamottagare i tredje land och, i förekommande fall, internationella organisationer finns antingen publicerad på vår webbplats eller kan begäras kostnadsfritt från oss. Kontakta vår dataskyddsansvarige för att begära denna lista.

## F. I tillämpliga fall att den personuppgiftsansvarige avser att överföra personuppgifter till ett tredjeland eller en internationell organisation och huruvida ett beslut av kommissionen om adekvat skyddsnivå föreligger eller saknas eller, när det gäller de överföringar som avses i artikel 46, 47 eller artikel 49.1 andra stycket, hänvisning till lämpliga eller passande skyddsåtgärder och hur en kopia av dem kan erhållas eller var dessa har gjorts tillgängliga (artikel 13.1 f, 46.1, 46.2 c GDPR).

Alla företag och filialer som ingår i vår koncern (nedan kallade "koncernföretag") och som har sitt säte eller kontor i ett tredjeland kan höra till mottagarna av personuppgifter. En förteckning över alla koncernbolag eller mottagare kan begäras från oss.

Enligt artikel 46.1 GDPR får en personuppgiftsansvarig eller ett personuppgiftsbiträde överföra personuppgifter till ett tredjeland endast om den personuppgiftsansvarige eller personuppgiftsbiträdet har tillhandahållit lämpliga skyddsåtgärder och på villkor att det finns verkställbara rättigheter för registrerade och effektiva rättsmedel för registrerade. Lämpliga skyddsåtgärder kan tillhandahållas utan att det krävs något särskilt tillstånd från en tillsynsmyndighet genom standardavtalsklausuler, artikel 46.2 c GDPR.

Europeiska unionens standardavtalsklausuler eller andra lämpliga skyddsåtgärder avtalas med alla mottagare från tredjeländer före den första överföringen av personuppgifter. På så sätt säkerställs lämpliga skyddsåtgärder, verkställbara rättigheter för registrerade personer och effektiva rättsmedel för registrerade personer. Varje registrerad person kan få en kopia av standardavtalsklausulerna från oss. Standardavtalsklausulerna finns också tillgängliga i Europeiska unionens officiella tidning.

Enligt artikel 45.3 i den allmänna dataskyddsförordningen (GDPR) har Europeiska kommissionen befogenhet att genom en genomförandeakt besluta att ett land utanför EU säkerställer en adekvat skyddsnivå. Detta innebär en skyddsnivå för personuppgifter som i allt väsentligt är likvärdig med skyddsnivån inom EU. Effekten av beslut om adekvat skyddsnivå är att personuppgifter kan flöda fritt från EU (och Norge, Liechtenstein och Island) till ett tredje land utan ytterligare hinder. Liknande regler finns för Storbritannien, Schweiz och vissa andra länder.

Om Europeiska kommissionen eller regeringen i ett annat land har beslutat att ett tredje land säkerställer en adekvat skyddsnivå och ett giltigt ramverk finns på plats (t.ex. EU-U.S. Data Privacy Framework,


© All rights reserved by Heiko Maniero.

Swiss-U.S. Data Privacy Framework, UK Extension to the EU-U.S. Data Privacy Framework), är alla överföringar från oss till medlemmarna i sådana ramverk (t.ex. självcertifierade enheter) uteslutande baserade på den enhetens medlemskap i respektive ramverk. Om vi eller en av våra koncernenheter är medlem i ett sådant ramverk, baseras alla överföringar till oss eller vår koncernenhet uteslutande på enhetens medlemskap i ett sådant ramverk.

Alla registrerade kan få en kopia av ramverken från oss. Ramarna finns också tillgängliga i Europeiska unionens officiella tidning eller i publicerat rättsligt material eller på tillsynsmyndigheternas eller andra behöriga myndigheters eller institutioners webbplatser.

## G. Den period under vilken personuppgifterna kommer att lagras eller, om detta inte är möjligt, de kriterier som används för att fastställa denna period (artikel 13.2 a GDPR)

Kriteriet som används för att fastställa lagringsperioden för personuppgifter är respektive lagstadgad lagringsperiod. Efter att denna period har löpt ut raderas motsvarande uppgifter rutinmässigt, så länge de inte längre är nödvändiga för att fullgöra avtalet eller inleda ett avtal.

Om det inte finns någon lagstadgad lagringstid är kriteriet den avtalsenliga eller interna lagringstiden.

## H. Att det föreligger en rätt att av den personuppgiftsansvarige begära tillgång till och rättelse eller radering av personuppgifter eller begränsning av behandling som rör den registrerade eller att invända mot behandling samt rätten till dataportabilitet (artikel 13.2 b GDPR)

Alla registrerade har följande rättigheter:

***Rätt till tillgång***

Varje registrerad person har rätt att få tillgång till de personuppgifter som rör honom eller henne. Rätten till tillgång gäller alla uppgifter som behandlas av oss. Rätten kan utövas enkelt och med rimliga intervall för att få kännedom om och kontrollera att behandlingen är laglig (skäl 63 GDPR). Denna rätt följer av art. 15 GDPR. Den registrerade kan kontakta oss för att utöva rätten till insyn.

***Rätt till rättelse***

Enligt artikel 16 första meningen GDPR har den registrerade rätt att från den personuppgiftsansvarige utan onödigt dröjsmål få rättelse av felaktiga personuppgifter om honom eller henne. Vidare föreskrivs i artikel 16 andra meningen GDPR att den registrerade, med hänsyn till ändamålen med behandlingen, har rätt att få ofullständiga personuppgifter kompletterade, bland annat genom att tillhandahålla en kompletterande förklaring. Den registrerade kan kontakta oss för att utöva sin rätt till rättelse.


© All rights reserved by Heiko Maniero.

***Rätt till radering (rätt att bli bortglömd)***

Dessutom har de registrerade rätt till radering och till att bli bortglömda enligt artikel. 17 GDPR. Denna rätt kan också utövas genom att kontakta oss. I detta läge vill vi dock påpeka att denna rätt inte gäller i den mån behandlingen är nödvändig för att uppfylla en rättslig förpliktelse som vårt företag är föremål för, artikel 17.3 b GDPR. Detta innebär att vi kan godkänna en ansökan om radering först efter det att den lagstadgade lagringsperioden har löpt ut.

***Rätt till begränsning av behandlingen***

Enligt artikel 18 GDPR har varje registrerad person rätt till en begränsning av behandlingen. Begränsningen av behandlingen kan begäras om ett av de villkor som anges i artikel 18.1 a-d GDPR är uppfyllda. Den registrerade kan kontakta oss för att utöva rätten till begränsning av behandlingen.

***Rätt till invändningar***

Vidare anges i artikel. 21 GDPR garanterar rätten till invändningar. Den registrerade kan kontakta oss för att utöva sin rätt till invändning.

***Rätt till dataportabilitet***

Konst. 20 GDPR ger den registrerade rätt till dataportabilitet. Enligt denna bestämmelse har den registrerade på de villkor som anges i artikel 20.1 a och b GDPR rätt att få de personuppgifter om honom eller henne som han eller hon har lämnat till en registeransvarig i ett strukturerat, allmänt använt och maskinläsbart format och har rätt att överföra dessa uppgifter till en annan registeransvarig utan att den registeransvarige som personuppgifterna har lämnats till hindrar detta. Den registrerade kan kontakta oss för att utöva rätten till dataportabilitet.

## I. Om behandlingen grundar sig på artikel 6.1 a eller artikel 9.2 a, att det föreligger en rätt att när som helst återkalla sitt samtycke, utan att detta påverkar lagligheten av behandlingen på grundval av samtycket, innan detta återkallades (artikel 13.2 c GDPR).

Om behandlingen av personuppgifter grundar sig på artikel. 6.1 a GDPR, vilket är fallet, om den registrerade har gett sitt samtycke till behandling av personuppgifter för ett eller flera specifika ändamål eller om den baseras på artikel 9.2 a GDPR, som reglerar uttryckligt samtycke till behandling av särskilda kategorier av personuppgifter, har den registrerade enligt artikel 7.3 första meningen GDPR rätt att när som helst återkalla sitt samtycke.

Återkallande av samtycke ska inte påverka lagligheten av behandling som grundar sig på samtycke före återkallandet, artikel 7.3 andra meningen GDPR. Det ska vara lika lätt att återkalla som att ge samtycke, artikel 7.2.2. 7.3 fjärde meningen GDPR. Återkallandet av samtycket kan därför alltid ske på samma sätt som samtycket har getts eller på något annat sätt som den registrerade anser vara enklare. I dagens informationssamhälle är förmodligen det enklaste sättet att återkalla samtycke ett enkelt e-postmeddelande. Om den registrerade vill återkalla sitt samtycke till oss räcker det med ett enkelt e-


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

postmeddelande till oss. Alternativt kan den registrerade välja något annat sätt att meddela oss att han eller hon återkallar sitt samtycke.

## J. Rätten att inge klagomål till en tillsynsmyndighet (artikel 13.2 d, 77.1 GDPR)

Som registeransvarig är vi skyldiga att informera den registrerade om rätten att lämna in ett klagomål till en tillsynsmyndighet, artikel 13.2 d GDPR. Rätten att lämna in ett klagomål till en tillsynsmyndighet regleras av artikel 77.1 GDPR. Enligt denna bestämmelse ska varje registrerad person, utan att det påverkar andra administrativa eller rättsliga åtgärder, ha rätt att lämna in ett klagomål till en tillsynsmyndighet, särskilt i den medlemsstat där han eller hon har sin vanliga vistelseort, sin arbetsplats eller den plats där den påstådda överträdelsen äger rum, om den registrerade anser att behandlingen av personuppgifter som rör honom eller henne strider mot den allmänna dataskyddsförordningen. Rätten att lämna in ett klagomål till en tillsynsmyndighet begränsades endast av unionsrätten på så sätt att den endast kan utövas inför en enda tillsynsmyndighet (skäl 141 första meningen GDPR). Syftet med denna regel är att undvika dubbla klagomål från samma registrerade i samma ärende. Om en registrerad person vill lämna in ett klagomål mot oss, uppmanas vi därför att kontakta endast en enda tillsynsmyndighet.

## K. Huruvida tillhandahållandet av personuppgifter är ett lagstadgat eller avtalsenligt krav eller ett krav som är nödvändigt för att ingå ett avtal samt huruvida den registrerade är skyldig att tillhandahålla personuppgifterna och de möjliga följderna av att sådana uppgifter inte lämnas (artikel 13.2 e GDPR)

Vi klargör att tillhandahållandet av personuppgifter delvis krävs enligt lag (t.ex. skattelagstiftning) eller kan också följa av avtalsbestämmelser (t.ex. information om avtalspartnern).

Ibland kan det vara nödvändigt för att ingå ett avtal att den registrerade förser oss med personuppgifter, som sedan måste behandlas av oss. Den registrerade är till exempel skyldig att förse oss med personuppgifter när vårt företag tecknar ett avtal med honom eller henne. Om personuppgifterna inte lämnas ut skulle detta få till följd att avtalet med den registrerade inte kan ingås.

Innan den registrerade lämnar personuppgifter måste den registrerade kontakta oss. Vi klargör för den registrerade om tillhandahållandet av personuppgifter krävs enligt lag eller avtal eller om det är nödvändigt för att ingå avtalet, om det finns en skyldighet att tillhandahålla personuppgifterna och konsekvenserna av att inte tillhandahålla personuppgifterna.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

### L. Förekomsten av automatiserat beslutsfattande, inbegripet profilering enligt artikel 22.1 och 22.4, varvid det åtminstone i dessa fall ska lämnas meningsfull information om logiken bakom samt betydelsen och de förutsedda följderna av sådan behandling för den registrerade (artikel 13.2 f GDPR).

Som ett ansvarsfullt företag använder vi vanligtvis inte automatiserat beslutsfattande eller profilering. Om vi i undantagsfall använder automatiserat beslutsfattande eller profilering kommer vi att informera den registrerade antingen separat eller via ett underavsnitt i vår integritetspolicy (på vår webbplats). I detta fall gäller följande:

Automatiserat beslutsfattande - inklusive profilering - får ske om (1) detta är nödvändigt för att ingå eller fullgöra ett avtal mellan den registrerade och oss, eller (2) detta är tillåtet enligt unionsrätten eller medlemsstaternas nationella rätt som vi omfattas av och som också fastställer lämpliga åtgärder för att skydda den registrerades rättigheter och friheter och berättigade intressen, eller (3) detta grundas på den registrerades uttryckliga samtycke.

I de fall som avses i artikel 22.2 a och c i GDPR ska vi vidta lämpliga åtgärder för att skydda den registrerades rättigheter och friheter samt berättigade intressen. I dessa fall har du rätt att få mänskligt ingripande från den personuppgiftsansvarige, att uttrycka din ståndpunkt och att bestrida beslutet.

Meningsfull information om den logik som ingår, liksom betydelsen och de förutsedda konsekvenserna av sådan behandling för den registrerade, anges i vår integritetspolicy.

## II. Information som ska tillhandahållas om personuppgifterna inte har erhållits från den registrerade (artikel 14 GDPR)

### A. Identitet och kontaktuppgifter för den personuppgiftsansvarige och i tillämpliga fall för dennes företrädare (artikel 14.1 a GDPR).

Se ovan.

### B. Kontaktuppgifter för dataskyddsombudet, i tillämpliga fall (artikel 14.1 b GDPR)

Se ovan.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## C. Ändamålen med den behandling för vilken personuppgifterna är avsedda samt den rättsliga grunden för behandlingen (artikel 14.1 c GDPR)

Syftet med behandlingen av personuppgifter är att hantera all verksamhet som rör den personuppgiftsansvarige, kunder, potentiella kunder, affärspartner eller andra avtalsmässiga eller prekontraktuella förbindelser mellan de nämnda grupperna (i vidaste bemärkelse) eller den personuppgiftsansvariges rättsliga skyldigheter.

Om behandlingen av personuppgifter är nödvändig för att fullgöra ett avtal i vilket den registrerade är part, vilket är fallet till exempel när behandlingen är nödvändig för att leverera varor eller tillhandahålla någon annan tjänst, grundar sig behandlingen på artikel 6.1 b GDPR. Detsamma gäller för sådan behandling som är nödvändig för att genomföra åtgärder före avtalstillfället, till exempel vid förfrågningar om våra produkter eller tjänster. Om vårt företag är föremål för en rättslig förpliktelse som kräver behandling av personuppgifter, t.ex. för att uppfylla skattemässiga skyldigheter, grundar sig behandlingen på art. 6(1) lit. c GDPR.

I sällsynta fall kan behandlingen av personuppgifter vara nödvändig för att skydda den registrerades eller en annan fysisk persons vitala intressen. Detta skulle till exempel vara fallet om en besökare skadar sig i vårt företag och hans namn, ålder, sjukförsäkringsuppgifter eller annan viktig information måste överlämnas till en läkare, ett sjukhus eller en annan tredje part. Då skulle behandlingen baseras på art. 6(1) lit. d GDPR.

Om behandlingen är nödvändig för att utföra en uppgift som utförs av allmänt intresse eller för att utöva myndighet som tillkommer den registeransvarige, är den rättsliga grunden art. 6(1) lit. e GDPR.

Slutligen kan behandlingen baseras på artikel 6.1 f GDPR. Denna rättsliga grund används för behandlingar som inte omfattas av någon av de ovan nämnda rättsliga grunderna, om behandlingen är nödvändig för de legitima intressen som vårt företag eller en tredje part har, utom när dessa intressen åsidosätts av den registrerades intressen eller grundläggande rättigheter och friheter som kräver skydd av personuppgifter. Sådana behandlingar är särskilt tillåtna eftersom de har nämnts särskilt av den europeiska lagstiftaren. Han ansåg att ett legitimt intresse kunde antas om den registrerade är en kund till den registeransvarige (skäl 47, andra meningen GDPR).

## D. De kategorier av personuppgifter som behandlingen gäller (artikel 14.1 d GDPR)

Kunduppgifter

Uppgifter om potentiella kunder

Uppgifter om anställda

Uppgifter om leverantörer


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## E. Mottagarna eller de kategorier av mottagare som ska ta del av personuppgifterna, i förekommande fall (artikel 14.1 e GDPR)

Offentliga myndigheter

Externa organ

Ytterligare externa organ

Intern bearbetning

Förädling inom en grupp

Andra organ

En förteckning över våra personuppgiftsbiträden och datamottagare i tredje land och, i förekommande fall, internationella organisationer finns antingen publicerad på vår webbplats eller kan begäras kostnadsfritt från oss. Kontakta vår dataskyddsansvarige för att begära denna lista.

## F. I tillämpliga fall att den personuppgiftsansvarige avser att överföra personuppgifter till en mottagare i ett tredjeland eller en internationell organisation och huruvida ett beslut av kommissionen om adekvat skyddsnivå föreligger eller saknas eller, när det gäller de överföringar som avses i artiklarna 46, 47 eller artikel 49.1 andra stycket, hänvisning till lämpliga eller passande skyddsåtgärder och hur en kopia av dem kan erhållas eller var dessa har gjorts tillgängliga (artikel 14.1 f, 46.1 och 46.2 c GDPR).

Alla företag och filialer som ingår i vår koncern (nedan kallade "koncernföretag") och som har sitt säte eller kontor i ett tredjeland kan höra till mottagarna av personuppgifter. En förteckning över alla koncernbolag kan begäras från oss.

Enligt artikel 46.1 GDPR får en personuppgiftsansvarig eller ett personuppgiftsbiträde överföra personuppgifter till ett tredjeland endast om den personuppgiftsansvarige eller personuppgiftsbiträdet har tillhandahållit lämpliga skyddsåtgärder och på villkor att det finns verkställbara rättigheter för registrerade och effektiva rättsmedel för registrerade. Lämpliga skyddsåtgärder kan tillhandahållas utan att det krävs något särskilt tillstånd från en tillsynsmyndighet genom standardiserade dataskyddsklausuler, artikel 46.2 c GDPR.

Europeiska unionens standardavtalsklausuler eller andra lämpliga skyddsåtgärder avtalas med alla mottagare från tredjeländer före den första överföringen av personuppgifter. På så sätt säkerställs lämpliga skyddsåtgärder, verkställbara rättigheter för registrerade personer och effektiva rättsmedel för


© All rights reserved by Heiko Maniero.

registrerade personer. Varje registrerad person kan få en kopia av standardavtalsklausulerna från oss. Standardavtalsklausulerna finns också tillgängliga i Europeiska unionens officiella tidning.

Enligt artikel 45.3 i den allmänna dataskyddsförordningen (GDPR) har Europeiska kommissionen befogenhet att genom en genomförandeakt besluta att ett land utanför EU säkerställer en adekvat skyddsnivå. Detta innebär en skyddsnivå för personuppgifter som i allt väsentligt är likvärdig med skyddsnivån inom EU. Effekten av beslut om adekvat skyddsnivå är att personuppgifter kan flöda fritt från EU (och Norge, Liechtenstein och Island) till ett tredje land utan ytterligare hinder. Liknande regler finns för Storbritannien, Schweiz och vissa andra länder.

Om Europeiska kommissionen eller regeringen i ett annat land har beslutat att ett tredje land säkerställer en adekvat skyddsnivå och ett giltigt ramverk finns på plats (t.ex. EU-U.S. Data Privacy Framework, Swiss-U.S. Data Privacy Framework, UK Extension to the EU-U.S. Data Privacy Framework), är alla överföringar från oss till medlemmarna i sådana ramverk (t.ex. självcertifierade enheter) uteslutande baserade på den enhetens medlemskap i respektive ramverk. Om vi eller en av våra koncernenheter är medlem i ett sådant ramverk, baseras alla överföringar till oss eller vår koncernenhet uteslutande på enhetens medlemskap i ett sådant ramverk.

Alla registrerade kan få en kopia av ramverken från oss. Ramarna finns också tillgängliga i Europeiska unionens officiella tidning eller i publicerat rättsligt material eller på tillsynsmyndigheternas eller andra behöriga myndigheters eller institutioners webbplatser.

## G. Den period under vilken personuppgifterna kommer att lagras eller, om detta inte är möjligt, de kriterier som används för att fastställa denna period (artikel 14.2 a GDPR)

Kriteriet som används för att fastställa lagringsperioden för personuppgifter är respektive lagstadgad lagringsperiod. Efter att denna period har löpt ut raderas motsvarande uppgifter rutinmässigt, så länge de inte längre är nödvändiga för att fullgöra avtalet eller inleda ett avtal.

Om det inte finns någon lagstadgad lagringstid är kriteriet den avtalsenliga eller interna lagringstiden.

## H. Om behandlingen grundar sig på artikel 6.1 f, den personuppgiftsansvariges eller en tredje parts berättigade intressen (artikel 14.2 b GDPR).

Enligt artikel 6.1 f GDPR ska behandlingen vara laglig endast om den är nödvändig för att tillgodose den personuppgiftsansvariges eller en tredje parts berättigade intressen, utom när dessa intressen åsidosätts av den registrerades intressen eller grundläggande rättigheter och friheter som kräver skydd av personuppgifter. Enligt skäl 47, andra meningen i skäl 47 GDPR kan ett legitimt intresse föreligga om det finns ett relevant och lämpligt förhållande mellan den registrerade och den registeransvarige, t.ex. i situationer där den registrerade är en kund till den registeransvarige. I alla fall där vårt företag behandlar


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

personuppgifter på grundval av artikel 6.1 lit. f GDPR är vårt legitima intresse att bedriva vår verksamhet till förmån för alla våra anställdas och aktieägares välbefinnande.

## I. Förekomsten av rätten att av den personuppgiftsansvarige begära tillgång till och rättelse eller radering av personuppgifter eller begränsning av behandling som rör den registrerade och att invända mot behandling samt rätten till dataportabilitet (artikel 14.2 c GDPR)

Alla registrerade har följande rättigheter:

***Rätt till tillgång***

Varje registrerad person har rätt att få tillgång till de personuppgifter som rör honom eller henne. Rätten till tillgång omfattar alla uppgifter som behandlas av oss. Rätten kan utövas enkelt och med rimliga intervall för att få kännedom om och kontrollera att behandlingen är laglig (skäl 63 GDPR). Denna rätt följer av art. 15 GDPR. Den registrerade kan kontakta oss för att utöva rätten till insyn.

***Rätt till rättelse***

Enligt artikel 16 första meningen GDPR har den registrerade rätt att från den personuppgiftsansvarige utan onödigt dröjsmål få rättelse av felaktiga personuppgifter om honom eller henne. Vidare föreskrivs i artikel 16 andra meningen GDPR att den registrerade, med hänsyn till ändamålen med behandlingen, har rätt att få ofullständiga personuppgifter kompletterade, bland annat genom att tillhandahålla en kompletterande förklaring. Den registrerade kan kontakta oss för att utöva sin rätt till rättelse.

***Rätt till radering (rätt att bli bortglömd)***

Dessutom har de registrerade rätt till radering och till att bli bortglömda enligt artikel. 17 GDPR. Denna rätt kan också utövas genom att kontakta oss. I detta läge vill vi dock påpeka att denna rätt inte gäller i den mån behandlingen är nödvändig för att uppfylla en rättslig förpliktelse som vårt företag är föremål för, artikel 17.3 b GDPR. Detta innebär att vi kan godkänna en ansökan om radering först efter det att den lagstadgade lagringsperioden har löpt ut.

***Rätt till begränsning av behandlingen***

Enligt artikel 18 GDPR har alla registrerade rätt att begränsa behandlingen. Begränsningen av behandlingen kan krävas om ett av de villkor som anges i artikel 18.1 a-d GDPR är uppfyllda. Den registrerade kan kontakta oss för att utöva rätten till begränsning av behandlingen.

***Rätt till invändningar***

Vidare anges i artikel. 21 GDPR rätten att göra invändningar. Den registrerade kan kontakta oss för att utöva sin rätt till invändning.

***Rätt till dataportabilitet***

Konst. 20 GDPR ger den registrerade rätt till dataportabilitet. Enligt denna bestämmelse har den registrerade på de villkor som anges i artikel 20.1 a och b GDPR rätt att få de personuppgifter som rör


© All rights reserved by Heiko Maniero.

honom eller henne och som han eller hon har lämnat till en registeransvarig i ett strukturerat, allmänt använt och maskinläsbart format och har rätt att överföra dessa uppgifter till en annan registeransvarig utan hinder från den registeransvarige till vilken personuppgifterna har lämnats. Den registrerade kan kontakta oss för att utöva rätten till dataportabilitet.

## J. Om behandlingen grundar sig på artikel 6.1 a eller artikel 9.2 a, rätten att när som helst återkalla sitt samtycke, utan att detta påverkar lagligheten av behandlingen på grundval av samtycket, innan detta återkallades (artikel 14.2 d GDPR).

Om behandlingen av personuppgifter grundar sig på artikel. 6.1 a GDPR, vilket är fallet, om den registrerade har gett sitt samtycke till behandling av personuppgifter för ett eller flera specifika ändamål eller om den baseras på artikel 9.2 a GDPR, som reglerar uttryckligt samtycke till behandling av särskilda kategorier av personuppgifter, har den registrerade enligt artikel 7.3 första meningen GDPR rätt att när som helst återkalla sitt samtycke.

Återkallande av samtycke ska inte påverka lagligheten av behandling som grundar sig på samtycke före återkallandet, artikel 7.3 andra meningen GDPR. Det ska vara lika lätt att återkalla som att ge samtycke, artikel 7.2.2. 7.3 fjärde meningen GDPR. Återkallandet av samtycket kan därför alltid ske på samma sätt som samtycket har getts eller på något annat sätt som den registrerade anser vara enklare. I dagens informationssamhälle är förmodligen det enklaste sättet att återkalla samtycke ett enkelt e-postmeddelande. Om den registrerade vill återkalla sitt samtycke till oss räcker det med ett enkelt e-postmeddelande till oss. Alternativt kan den registrerade välja något annat sätt att meddela oss att han eller hon återkallar sitt samtycke.

## K. Rätten att inge klagomål till en tillsynsmyndighet (artikel 14.2 e, 77.1 GDPR)

Som registeransvarig är vi skyldiga att informera den registrerade om rätten att lämna in ett klagomål till en tillsynsmyndighet, artikel 14.2 e GDPR. Rätten att lämna in ett klagomål till en tillsynsmyndighet regleras av artikel 77.1 GDPR. Enligt denna bestämmelse ska varje registrerad person, utan att det påverkar andra administrativa eller rättsliga åtgärder, ha rätt att lämna in ett klagomål till en tillsynsmyndighet, särskilt i den medlemsstat där han eller hon har sin vanliga vistelseort, sin arbetsplats eller den plats där den påstådda överträdelsen äger rum, om den registrerade anser att behandlingen av personuppgifter som rör honom eller henne strider mot den allmänna dataskyddsförordningen. Rätten att lämna in ett klagomål till en tillsynsmyndighet begränsades endast av unionsrätten på så sätt att den endast kan utövas inför en enda tillsynsmyndighet (skäl 141 första meningen GDPR). Syftet med denna regel är att undvika dubbla klagomål från samma registrerade i samma ärende. Om en registrerad person vill lämna in ett klagomål mot oss, uppmanas vi därför att kontakta endast en enda tillsynsmyndighet.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## L. Varifrån personuppgifterna kommer och i förekommande fall huruvida de har sitt ursprung i allmänt tillgängliga källor (artikel 14.2 f GDPR)

I princip samlas personuppgifter in direkt från den registrerade eller i samarbete med en myndighet (t.ex. genom att hämta uppgifter från ett officiellt register). Andra uppgifter om registrerade personer kommer från överföringar av koncernföretag. I samband med denna allmänna information är det antingen omöjligt eller skulle innebära en oproportionerligt stor ansträngning enligt artikel 3.1 i EG-fördraget att ange de exakta källorna till personuppgifterna. 14(5) lit. b GDPR. I princip samlar vi inte in personuppgifter från offentligt tillgängliga källor.

Varje registrerad person kan när som helst kontakta oss för att få mer detaljerad information om de exakta källorna till de personuppgifter som rör honom eller henne. Om den registrerade inte kan få veta varifrån personuppgifterna kommer eftersom olika källor har använts, bör allmän information lämnas (skäl 61, fjärde meningen GDPR).

## M. Förekomsten av automatiserat beslutsfattande, inbegripet profilering enligt artikel 22.1 och 22.4, varvid det åtminstone i dessa fall ska lämnas meningsfull information om logiken bakom samt betydelsen och de förutsedda följderna av sådan behandling för den registrerade (artikel 14.2 g GDPR).

Som ett ansvarsfullt företag använder vi vanligtvis inte automatiserat beslutsfattande eller profilering. Om vi i undantagsfall använder automatiserat beslutsfattande eller profilering kommer vi att informera den registrerade antingen separat eller via ett underavsnitt i vår integritetspolicy (på vår webbplats). I detta fall gäller följande:

Automatiserat beslutsfattande - inklusive profilering - får ske om (1) detta är nödvändigt för att ingå eller fullgöra ett avtal mellan den registrerade och oss, eller (2) detta är tillåtet enligt unionsrätten eller medlemsstaternas nationella rätt som vi omfattas av och som också fastställer lämpliga åtgärder för att skydda den registrerades rättigheter och friheter och berättigade intressen, eller (3) detta grundas på den registrerades uttryckliga samtycke.

I de fall som avses i artikel 22.2 a och c i GDPR ska vi vidta lämpliga åtgärder för att skydda den registrerades rättigheter och friheter samt berättigade intressen. I dessa fall har du rätt att få mänskligt ingripande från den personuppgiftsansvarige, att uttrycka din ståndpunkt och att bestrida beslutet.

Meningsfull information om den logik som ingår, liksom betydelsen och de förutsedda konsekvenserna av sådan behandling för den registrerade, anges i vår integritetspolicy.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## III. EU-U.S. Data Privacy Framework (EU-U.S. DPF), UK Extension to the EU-U.S. DPF, Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF)

Om vår organisation är ett certifierat medlem av EU-U.S. Data Privacy Framework (EU-U.S. DPF) och/eller UK Extension to the EU-U.S. DPF och/eller Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF) gäller följande:

Vi följer EU-U.S. Data Privacy Framework (EU-U.S. DPF) och UK Extension to the EU-U.S. DPF samt Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF) som fastställts av U.S. Department of Commerce. Vårt företag har bekräftat för det amerikanska handelsdepartementet att det följer EU-U.S. Data Privacy Framework Principles (EU-U.S. DPF Principles) avseende behandlingen av personuppgifter som det erhåller från Europeiska unionen och Storbritannien under åberopande av EU-U.S. DPF och UK Extension to the EU-U.S. DPF. Vårt företag har bekräftat för det amerikanska handelsdepartementet att det följer Swiss-U.S. Data Privacy Framework Principles (Swiss-U.S. DPF Principles) avseende behandlingen av personuppgifter som det erhåller från Schweiz under åberopande av Swiss-U.S. DPF. I händelse av en konflikt mellan bestämmelserna i vår sekretesspolicy och EU-U.S. DPF Principles och/eller Swiss-U.S. DPF Principles, är Principles överordnade.

För att lära dig mer om Data Privacy Framework (DPF) programmet och för att se vår certifiering, besök https://www.dataprivacyframework.gov/.

Andra amerikanska enheter eller dotterbolag i vårt företag som också följer EU-U.S. DPF Principals, inklusive UK Extension to the EU-U.S. DPF och Swiss-U.S. DPF Principals, om tillämpligt, anges i vår sekretesspolicy.

I enlighet med EU-U.S. DPF och UK Extension to the EU-U.S. DPF samt Swiss-U.S. DPF förbinder sig vårt företag att samarbeta med den panel som inrättats av EU

dataskyddsmyndigheter och det brittiska Information Commissioner's Office (ICO) samt den federala dataskydds- och informationskommissionären (EDÖB) och följa deras råd angående olösta klagomål om vår hantering av personuppgifter som vi erhåller under åberopande av EU-U.S. DPF och UK Extension to the EU-U.S. DPF och Swiss-U.S. DPF.

Vi informerar de berörda personerna om de relevanta europeiska dataskyddsmyndigheterna som är ansvariga för att hantera klagomål om vår organisations hantering av personuppgifter i den övre delen av detta transparensdokument och om att vi erbjuder berörda personer ett lämpligt och kostnadsfritt rättsmedel.

Vi informerar alla berörda personer om att vårt företag är underkastat undersöknings- och verkställighetsbefogenheterna hos Federal Trade Commission (FTC).


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

Berörda personer har under vissa förutsättningar möjlighet att utnyttja en bindande skiljedom. Vår organisation är skyldig att lösa krav och följa villkoren enligt Bilaga I till DPF-Principals, om den berörda personen har begärt en bindande skiljedom genom att meddela vår organisation och har följt förfarandena och villkoren enligt Bilaga I till Principals.

Vi informerar härmed alla berörda personer om vår organisations ansvar i händelse av överföring av personuppgifter till tredje part.

För frågor från berörda personer eller dataskyddsmyndigheter har vi namngivit de lokala representanterna som anges högst upp i detta transparensdokument.

Vi erbjuder dig möjligheten att välja (Opt-out) om dina personuppgifter (i) ska överföras till tredje part eller (ii) användas för ett syfte som avsevärt skiljer sig från det/den syfte(n) för vilket de ursprungligen samlades in eller senare godkändes av dig. Den tydliga, väl synliga och lättillgängliga mekanismen för att utöva ditt val är att kontakta vår dataskyddsombud (DSB) via e-post. Du har inget val och vi är inte skyldiga att göra detta om uppgifterna överförs till en tredje part som agerar som agent eller bearbetare på våra vägnar och enligt våra instruktioner. Vi ingår dock alltid ett avtal med en sådan agent eller bearbetare.

För känsliga uppgifter (dvs. personuppgifter som innehåller information om hälsostatus, ras eller etniskt ursprung, politiska åsikter, religiösa eller filosofiska övertygelser, medlemskap i en fackförening eller information om sexualliv hos den berörda personen) begär vi ditt uttryckliga samtycke (Opt-in) när dessa uppgifter (i) ska överföras till tredje part eller (ii) användas för ett annat syfte än det för vilket de ursprungligen samlades in eller för vilket du senare har gett ditt godkännande genom att göra ditt Opt-in-val. Dessutom behandlar vi alla personuppgifter som vi mottar från tredje part som känsliga, om den tredje parten har identifierat och behandlat dem som sådana.

Vi informerar dig härmed om kravet att avslöja personuppgifter som svar på lagliga förfrågningar från myndigheter, inklusive att uppfylla krav från nationell säkerhet eller brottsbekämpning.

När vi överför personuppgifter till en tredje part som agerar som kontrollerande, följer vi Principals för meddelande och val. Dessutom ingår vi ett avtal med den tredje parten som är ansvarig för behandlingen, som stipulerar att dessa data endast får behandlas för begränsade och angivna syften i enlighet med det samtycke du har gett och att mottagaren måste tillhandahålla samma skyddsnivå som DPF Principals och informera oss om han finner att han inte längre kan uppfylla denna skyldighet. Avtalet föreskriver att den tredje parten, som är ansvarig, ska upphöra med behandlingen eller vidta andra lämpliga och adekvata åtgärder för att rätta till situationen om en sådan upptäckt görs.

Vid överföring av personuppgifter till en tredje part som agerar som agent eller processor, (i) överför vi dessa data endast för begränsade och angivna syften; (ii) säkerställer vi att agenten eller processorn är skyldig att tillhandahålla åtminstone samma skyddsnivå som krävs av DPF Principals; (iii) vidtar vi lämpliga och adekvata åtgärder för att säkerställa att agenten eller processorn faktiskt behandlar de överförda personuppgifterna på ett sätt som är förenligt med våra skyldigheter enligt DPF Principals; (iv)


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

kräver vi att agenten eller processorn informerar vår organisation om han finner att han inte längre kan uppfylla skyldigheten att tillhandahålla samma skyddsnivå som DPF Principals förutser; (v) efter en sådan notifiering, även enligt (iv), vidtar vi lämpliga och adekvata åtgärder för att stoppa obehörig behandling och åtgärda situationen; och (vi) tillhandahåller DPF Department på begäran en sammanfattning eller ett representativt exempel på de relevanta dataskyddsbestämmelserna i sitt avtal med denna agent.

I enlighet med EU-U.S. DPF och/eller UK Extension to the EU-U.S. DPF och/eller Swiss-U.S. DPF förbinder sig vår organisation att samarbeta med panelen inrättad av EU

dataskyddsmyndigheter och det brittiska Information Commissioner's Office (ICO) respektive den federala dataskydds- och informationskommissionären (EDÖB) och följa dess råd gällande olösta klagomål om vår hantering av personuppgifter, som vi har mottagit i samband med anställningsförhållanden, under åberopande av EU-U.S. DPF och UK Extension to the EU-U.S. DPF och Swiss-U.S. DPF.

Alla registrerade som tillfälligt befinner sig i Europeiska unionen (EU), Europeiska ekonomiska samarbetsområdet (EES) eller Storbritannien, eller som har sin hemvist eller vanliga vistelseort där, har rätt till de rättigheter och den registrerades rättigheter som publiceras i vårt transparensdokument, som också följer av artiklarna 15-22 i GDPR, inklusive rätten att få tillgång till personuppgifter. Vi har gjort denna information tillgänglig på alla EU- och EES-språk. Den engelska språkversionen gäller för Storbritannien.

Alla registrerade som är tillfälligt bosatta i Schweiz eller har sin hemvist eller vanliga vistelseort där har rätt till de rättigheter och den registrerades rättigheter enligt den schweiziska dataskyddslagen (DPA) och den schweiziska dataskyddsförordningen (DPR) som publiceras i vårt transparensdokument, inklusive rätten att få tillgång till personuppgifter. Vi har tillhandahållit denna information på de tre officiella språken i Schweiz (tyska, italienska och franska).


© All rights reserved by Heiko Maniero.

# SWEDISH: Information om behandling av personuppgifter för anställda och sökande (artikel 13, 14 GDPR)

Kära herr eller fru,

Personuppgifter om anställda och sökande förtjänar särskilt skydd. Vårt mål är att hålla vår dataskyddsnivå på en hög nivå. Därför utvecklar vi rutinmässigt våra koncept för dataskydd och datasäkerhet.

Självklart följer vi de lagstadgade bestämmelserna om dataskydd. Enligt artikel 13 och 14 GDPR ska registeransvariga uppfylla särskilda informationskrav när de behandlar personuppgifter. Detta dokument uppfyller dessa skyldigheter.

Terminologin för rättslig reglering är komplicerad. Tyvärr kunde man inte undvika att använda juridiska termer vid utarbetandet av detta dokument. Därför vill vi påpeka att du alltid är välkommen att kontakta oss för alla frågor om detta dokument, de använda termerna eller formuleringar.

## I. Information som ska tillhandahållas om personuppgifterna samlas in från den registrerade (artikel 13 GDPR)

### A. Identitet och kontaktuppgifter för den personuppgiftsansvarige och i tillämpliga fall för dennes företrädare (artikel 13.1 a GDPR)

Se ovan.

### B. Kontaktuppgifter för dataskyddsombudet, i tillämpliga fall (artikel 13.1 b GDPR)

Se ovan.

### C. Ändamålen med den behandling för vilken personuppgifterna är avsedda samt den rättsliga grunden för behandlingen (artikel 13.1 c GDPR)

När det gäller uppgifter om sökande är syftet med databehandlingen att granska ansökan under rekryteringsprocessen. För detta ändamål behandlar vi alla uppgifter som du lämnat. På grundval av de uppgifter som lämnats under rekryteringsprocessen kontrollerar vi om du blir inbjuden till en anställningsintervju (del av urvalsprocessen). När det gäller allmänt lämpliga kandidater, särskilt i samband med anställningsintervjun, behandlar vi vissa andra personuppgifter som du lämnat, vilka är nödvändiga för vårt urvalsbeslut. Om du anställs av oss kommer uppgifter om sökande automatiskt att


© All rights reserved by Heiko Maniero.

ändras till uppgifter om anställda. Som en del av rekryteringsprocessen kommer vi att behandla andra personuppgifter om dig som vi begär av dig och som krävs för att inleda eller fullgöra ditt kontrakt (t.ex. personnummer eller skattenummer). När det gäller uppgifter om anställda är syftet med databehandlingen att fullgöra anställningsavtalet eller följa andra rättsliga bestämmelser som är tillämpliga på anställningsförhållandet (t.ex. skattelagstiftning) samt att använda dina personuppgifter för att fullgöra det anställningsavtal som ingåtts med dig (t.ex. publicering av ditt namn och dina kontaktuppgifter inom företaget eller till kunder). Anställdas uppgifter lagras efter det att anställningsförhållandet har upphört för att uppfylla lagstadgade lagringsperioder.

Den rättsliga grunden för databehandlingen är artikel 6.1 b GDPR, artikel 9.2 b och h GDPR, artikel 88.1 GDPR och nationell lagstiftning, t.ex. i Tyskland § 26 BDSG (Federal Data Protection Act).

## D. Mottagarna eller de kategorier av mottagare som ska ta del av personuppgifterna, i förekommande fall (artikel 13.1 e GDPR)

Offentliga myndigheter

Externa organ

Ytterligare externa organ

Intern bearbetning

Förädling inom en grupp

Andra organ

En förteckning över våra personuppgiftsbiträden och datamottagare i tredje land och, i förekommande fall, internationella organisationer finns antingen publicerad på vår webbplats eller kan begäras kostnadsfritt från oss. Kontakta vår dataskyddsansvarige för att begära denna lista.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## E. I tillämpliga fall att den personuppgiftsansvarige avser att överföra personuppgifter till ett tredjeland eller en internationell organisation och huruvida ett beslut av kommissionen om adekvat skyddsnivå föreligger eller saknas eller, när det gäller de överföringar som avses i artikel 46, 47 eller artikel 49.1 andra stycket, hänvisning till lämpliga eller passande skyddsåtgärder och hur en kopia av dem kan erhållas eller var dessa har gjorts tillgängliga (artikel 13.1 f, 46.1, 46.2 c GDPR).

Alla företag och filialer som ingår i vår koncern (nedan kallade "koncernföretag") och som har sitt säte eller kontor i ett tredjeland kan höra till mottagarna av personuppgifter. En förteckning över alla koncernbolag eller mottagare kan begäras från oss.

Enligt artikel 46.1 GDPR får en personuppgiftsansvarig eller ett personuppgiftsbiträde överföra personuppgifter till ett tredjeland endast om den personuppgiftsansvarige eller personuppgiftsbiträdet har tillhandahållit lämpliga skyddsåtgärder och på villkor att det finns verkställbara rättigheter för registrerade och effektiva rättsmedel för registrerade. Lämpliga skyddsåtgärder kan tillhandahållas utan att det krävs något särskilt tillstånd från en tillsynsmyndighet genom standardavtalsklausuler, artikel 46.2 c GDPR.

Europeiska unionens standardavtalsklausuler eller andra lämpliga skyddsåtgärder avtalas med alla mottagare från tredjeländer före den första överföringen av personuppgifter. På så sätt säkerställs lämpliga skyddsåtgärder, verkställbara rättigheter för registrerade personer och effektiva rättsmedel för registrerade personer. Varje registrerad person kan få en kopia av standardavtalsklausulerna från oss. Standardavtalsklausulerna finns också tillgängliga i Europeiska unionens officiella tidning.

Enligt artikel 45.3 i den allmänna dataskyddsförordningen (GDPR) har Europeiska kommissionen befogenhet att genom en genomförandeakt besluta att ett land utanför EU säkerställer en adekvat skyddsnivå. Detta innebär en skyddsnivå för personuppgifter som i allt väsentligt är likvärdig med skyddsnivån inom EU. Effekten av beslut om adekvat skyddsnivå är att personuppgifter kan flöda fritt från EU (och Norge, Liechtenstein och Island) till ett tredje land utan ytterligare hinder. Liknande regler finns för Storbritannien, Schweiz och vissa andra länder.

Om Europeiska kommissionen eller regeringen i ett annat land har beslutat att ett tredje land säkerställer en adekvat skyddsnivå och ett giltigt ramverk finns på plats (t.ex. EU-U.S. Data Privacy Framework, Swiss-U.S. Data Privacy Framework, UK Extension to the EU-U.S. Data Privacy Framework), är alla överföringar från oss till medlemmarna i sådana ramverk (t.ex. självcertifierade enheter) uteslutande baserade på den enhetens medlemskap i respektive ramverk. Om vi eller en av våra koncernenheter är medlem i ett sådant ramverk, baseras alla överföringar till oss eller vår koncernenhet uteslutande på enhetens medlemskap i ett sådant ramverk.

Alla registrerade kan få en kopia av ramverken från oss. Ramarna finns också tillgängliga i Europeiska unionens officiella tidning eller i publicerat rättsligt material eller på tillsynsmyndigheternas eller andra behöriga myndigheters eller institutioners webbplatser.


© All rights reserved by Heiko Maniero.

## F. Den period under vilken personuppgifterna kommer att lagras eller, om detta inte är möjligt, de kriterier som används för att fastställa denna period (artikel 13.2 a GDPR)

Personuppgifter om sökande lagras i sex månader. För uppgifter om anställda gäller respektive lagstadgad lagringstid. Efter utgången av denna period raderas motsvarande uppgifter rutinmässigt, så länge de inte längre är nödvändiga för att fullgöra avtalet eller inleda ett avtal.

## G. Att det föreligger en rätt att av den personuppgiftsansvarige begära tillgång till och rättelse eller radering av personuppgifter eller begränsning av behandling som rör den registrerade eller att invända mot behandling samt rätten till dataportabilitet (artikel 13.2 b GDPR).

Alla registrerade har följande rättigheter:

***Rätt till tillgång***

Varje registrerad person har rätt att få tillgång till de personuppgifter som rör honom eller henne. Rätten till tillgång omfattar alla uppgifter som behandlas av oss. Rätten kan utövas enkelt och med rimliga intervall för att få kännedom om och kontrollera att behandlingen är laglig (skäl 63 GDPR). Denna rätt följer av art. 15 GDPR. Den registrerade kan kontakta oss för att utöva rätten till insyn.

***Rätt till rättelse***

Enligt artikel 16 första meningen GDPR har den registrerade rätt att från den personuppgiftsansvarige utan onödigt dröjsmål få rättelse av felaktiga personuppgifter om honom eller henne. Vidare föreskrivs i artikel 16 andra meningen GDPR att den registrerade, med hänsyn till ändamålen med behandlingen, har rätt att få ofullständiga personuppgifter kompletterade, bland annat genom att tillhandahålla en kompletterande förklaring. Den registrerade kan kontakta oss för att utöva sin rätt till rättelse.

***Rätt till radering (rätt att bli bortglömd)***

Dessutom har de registrerade rätt till radering och till att bli bortglömda enligt artikel. 17 GDPR. Denna rätt kan också utövas genom att kontakta oss. I detta läge vill vi dock påpeka att denna rätt inte gäller i den mån behandlingen är nödvändig för att uppfylla en rättslig förpliktelse som vårt företag är föremål för, artikel 17.3 b GDPR. Detta innebär att vi kan godkänna en ansökan om radering först efter det att den lagstadgade lagringsperioden har löpt ut.

***Rätt till begränsning av behandlingen***

Enligt artikel 18 GDPR har alla registrerade rätt att få en begränsning av behandlingen. Begränsningen av behandlingen kan begäras om ett av de villkor som anges i artikel 18.1 a-d GDPR är uppfyllda. Den registrerade kan kontakta oss för att utöva rätten till begränsning av behandlingen.

***Rätt till invändningar***

Vidare anges i artikel. 21 GDPR rätten att göra invändningar. Den registrerade kan kontakta oss för att utöva sin rätt till invändning.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

***Rätt till dataportabilitet***

Konst. 20 GDPR ger den registrerade rätt till dataportabilitet. Enligt denna bestämmelse har den registrerade på de villkor som anges i artikel 20.1 a och b GDPR rätt att få de personuppgifter om honom eller henne som han eller hon har lämnat till en registeransvarig i ett strukturerat, allmänt använt och maskinläsbart format och har rätt att överföra dessa uppgifter till en annan registeransvarig utan att den registeransvarige som personuppgifterna har lämnats till hindrar detta. Den registrerade kan kontakta oss för att utöva rätten till dataportabilitet.

## H. Om behandlingen grundar sig på artikel 6.1 a eller artikel 9.2 a, att det föreligger en rätt att när som helst återkalla sitt samtycke, utan att detta påverkar lagligheten av behandlingen på grundval av samtycket, innan detta återkallades (artikel 13.2 c GDPR).

Om behandlingen av personuppgifter grundar sig på artikel. 6.1 a GDPR, vilket är fallet, om den registrerade har gett sitt samtycke till behandling av personuppgifter för ett eller flera specifika ändamål, eller om behandlingen grundar sig på artikel 9.2 a GDPR, som reglerar uttryckligt samtycke till behandling av särskilda kategorier av personuppgifter, har den registrerade enligt artikel 7.3 första meningen GDPR rätt att när som helst återkalla sitt samtycke.

Återkallande av samtycke ska inte påverka lagligheten av behandling som grundar sig på samtycke före återkallandet, artikel 7.3 andra meningen GDPR. Det ska vara lika lätt att återkalla som att ge samtycke, artikel 7.2.2. 7.3 fjärde meningen GDPR. Återkallandet av samtycket kan därför alltid ske på samma sätt som samtycket har getts eller på något annat sätt som den registrerade anser vara enklare. I dagens informationssamhälle är förmodligen det enklaste sättet att återkalla samtycke ett enkelt e-postmeddelande. Om den registrerade vill återkalla sitt samtycke till oss räcker det med ett enkelt e-postmeddelande till oss. Alternativt kan den registrerade välja något annat sätt att meddela oss att han eller hon återkallar sitt samtycke.

## I. Rätten att inge klagomål till en tillsynsmyndighet (artikel 13.2 d, 77.1 GDPR)

Som registeransvarig är vi skyldiga att informera den registrerade om rätten att lämna in ett klagomål till en tillsynsmyndighet, artikel 13.2 d GDPR. Rätten att lämna in ett klagomål till en tillsynsmyndighet regleras av artikel 77.1 GDPR. Enligt denna bestämmelse ska varje registrerad person, utan att det påverkar andra administrativa eller rättsliga åtgärder, ha rätt att lämna in ett klagomål till en tillsynsmyndighet, särskilt i den medlemsstat där han eller hon har sin vanliga vistelseort, sin arbetsplats eller den plats där den påstådda överträdelsen äger rum, om den registrerade anser att behandlingen av personuppgifter som rör honom eller henne strider mot den allmänna dataskyddsförordningen. Rätten att lämna in ett klagomål till en tillsynsmyndighet begränsades endast av unionsrätten på så sätt att den endast kan utövas inför en enda tillsynsmyndighet (skäl 141 första meningen GDPR). Syftet med denna regel är att undvika dubbla klagomål från samma registrerade i samma ärende. Om en registrerad person vill lämna in ett klagomål mot oss, uppmanas vi därför att kontakta endast en enda tillsynsmyndighet.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## J. Huruvida tillhandahållandet av personuppgifter är ett lagstadgat eller avtalsenligt krav eller ett krav som är nödvändigt för att ingå ett avtal samt huruvida den registrerade är skyldig att tillhandahålla personuppgifterna och de möjliga följderna av att sådana uppgifter inte lämnas (artikel 13.2 e GDPR)

Vi klargör att tillhandahållandet av personuppgifter delvis krävs enligt lag (t.ex. skattelagstiftning) eller kan också följa av avtalsbestämmelser (t.ex. information om avtalspartnern).

Ibland kan det vara nödvändigt för att ingå ett avtal att den registrerade förser oss med personuppgifter, som sedan måste behandlas av oss. Den registrerade är till exempel skyldig att förse oss med personuppgifter när vårt företag tecknar ett avtal med honom eller henne. Om personuppgifterna inte lämnas ut skulle detta få till följd att avtalet med den registrerade inte kan ingås.

Innan den registrerade lämnar personuppgifter måste den registrerade kontakta oss. Vi klargör för den registrerade om tillhandahållandet av personuppgifter krävs enligt lag eller avtal eller om det är nödvändigt för att ingå avtalet, om det finns en skyldighet att tillhandahålla personuppgifterna och konsekvenserna av att inte tillhandahålla personuppgifterna.

## K. Förekomsten av automatiserat beslutsfattande, inbegripet profilering enligt artikel 22.1 och 22.4, varvid det åtminstone i dessa fall ska lämnas meningsfull information om logiken bakom samt betydelsen och de förutsedda följderna av sådan behandling för den registrerade (artikel 13.2 f GDPR).

Som ett ansvarsfullt företag använder vi vanligtvis inte automatiserat beslutsfattande eller profilering. Om vi i undantagsfall använder automatiserat beslutsfattande eller profilering kommer vi att informera den registrerade antingen separat eller via ett underavsnitt i vår integritetspolicy (på vår webbplats). I detta fall gäller följande:

Automatiserat beslutsfattande - inklusive profilering - får ske om (1) detta är nödvändigt för att ingå eller fullgöra ett avtal mellan den registrerade och oss, eller (2) detta är tillåtet enligt unionsrätten eller medlemsstaternas nationella rätt som vi omfattas av och som också fastställer lämpliga åtgärder för att skydda den registrerades rättigheter och friheter och berättigade intressen, eller (3) detta grundas på den registrerades uttryckliga samtycke.

I de fall som avses i artikel 22.2 a och c i GDPR ska vi vidta lämpliga åtgärder för att skydda den registrerades rättigheter och friheter samt berättigade intressen. I dessa fall har du rätt att få mänskligt ingripande från den personuppgiftsansvarige, att uttrycka din ståndpunkt och att bestrida beslutet.

Meningsfull information om den logik som ingår, liksom betydelsen och de förutsedda konsekvenserna av sådan behandling för den registrerade, anges i vår integritetspolicy.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## II. Information som ska tillhandahållas om personuppgifterna inte har erhållits från den registrerade (artikel 14 GDPR)

### A. Identitet och kontaktuppgifter för den personuppgiftsansvarige och i tillämpliga fall för dennes företrädare (artikel 14.1 a GDPR).

Se ovan.

### B. Kontaktuppgifter för dataskyddsombudet, i tillämpliga fall (artikel 14.1 b GDPR)

Se ovan.

### C. Ändamålen med den behandling för vilken personuppgifterna är avsedda samt den rättsliga grunden för behandlingen (artikel 14.1 c GDPR)

När det gäller uppgifter om sökande som inte samlats in från den registrerade är syftet med behandlingen av uppgifterna att granska ansökan under rekryteringsprocessen. För detta ändamål kan vi behandla uppgifter som inte samlats in från dig. På grundval av de uppgifter som behandlas under rekryteringsprocessen kommer vi att kontrollera om du blir inbjuden till en anställningsintervju (del av urvalsprocessen). Om du anställs av oss kommer uppgifter om sökande automatiskt att omvandlas till uppgifter om anställda. När det gäller uppgifter om anställda är syftet med databehandlingen att fullgöra anställningsavtalet eller att följa andra rättsliga bestämmelser som är tillämpliga på anställningsförhållandet. Anställdas uppgifter lagras efter anställningsförhållandets upphörande för att uppfylla lagstadgade lagringsperioder.

Den rättsliga grunden för databehandlingen är artikel 6.1 b och f GDPR, artikel 9.2 b och h GDPR, artikel 88.1 GDPR och nationell lagstiftning, t.ex. i Tyskland § 26 BDSG (Federal Data Protection Act).

### D. De kategorier av personuppgifter som behandlingen gäller (artikel 14.1 d GDPR)

Uppgifter om den sökande

Uppgifter om anställda


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## E. Mottagarna eller de kategorier av mottagare som ska ta del av personuppgifterna, i förekommande fall (artikel 14.1 e GDPR)

Offentliga myndigheter

Externa organ

Ytterligare externa organ

Intern bearbetning

Förädling inom en grupp

Andra organ

En förteckning över våra personuppgiftsbiträden och datamottagare i tredje land och, i förekommande fall, internationella organisationer finns antingen publicerad på vår webbplats eller kan begäras kostnadsfritt från oss. Kontakta vår dataskyddsansvarige för att begära denna lista.

## F. I tillämpliga fall att den personuppgiftsansvarige avser att överföra personuppgifter till en mottagare i ett tredjeland eller en internationell organisation och huruvida ett beslut av kommissionen om adekvat skyddsnivå föreligger eller saknas eller, när det gäller de överföringar som avses i artiklarna 46, 47 eller artikel 49.1 andra stycket, hänvisning till lämpliga eller passande skyddsåtgärder och hur en kopia av dem kan erhållas eller var dessa har gjorts tillgängliga (artikel 14.1 f, 46.1 och 46.2 c GDPR).

Alla företag och filialer som ingår i vår koncern (nedan kallade "koncernföretag") och som har sitt säte eller kontor i ett tredjeland kan höra till mottagarna av personuppgifter. En förteckning över alla koncernbolag eller mottagare kan begäras från oss.

Enligt artikel 46.1 GDPR får en personuppgiftsansvarig eller ett personuppgiftsbiträde överföra personuppgifter till ett tredjeland endast om den personuppgiftsansvarige eller personuppgiftsbiträdet har tillhandahållit lämpliga skyddsåtgärder och på villkor att det finns verkställbara rättigheter för registrerade och effektiva rättsmedel för registrerade. Lämpliga skyddsåtgärder kan tillhandahållas utan att det krävs något särskilt tillstånd från en tillsynsmyndighet genom standardiserade dataskyddsklausuler, artikel 46.2 c GDPR.

Europeiska unionens standardavtalsklausuler eller andra lämpliga skyddsåtgärder avtalas med alla mottagare från tredjeländer före den första överföringen av personuppgifter. På så sätt säkerställs lämpliga skyddsåtgärder, verkställbara rättigheter för registrerade personer och effektiva rättsmedel för


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

registrerade personer. Varje registrerad person kan få en kopia av standardavtalsklausulerna från oss. Standardavtalsklausulerna finns också tillgängliga i Europeiska unionens officiella tidning.

Enligt artikel 45.3 i den allmänna dataskyddsförordningen (GDPR) har Europeiska kommissionen befogenhet att genom en genomförandeakt besluta att ett land utanför EU säkerställer en adekvat skyddsnivå. Detta innebär en skyddsnivå för personuppgifter som i allt väsentligt är likvärdig med skyddsnivån inom EU. Effekten av beslut om adekvat skyddsnivå är att personuppgifter kan flöda fritt från EU (och Norge, Liechtenstein och Island) till ett tredje land utan ytterligare hinder. Liknande regler finns för Storbritannien, Schweiz och vissa andra länder.

Om Europeiska kommissionen eller regeringen i ett annat land har beslutat att ett tredje land säkerställer en adekvat skyddsnivå och ett giltigt ramverk finns på plats (t.ex. EU-U.S. Data Privacy Framework, Swiss-U.S. Data Privacy Framework, UK Extension to the EU-U.S. Data Privacy Framework), är alla överföringar från oss till medlemmarna i sådana ramverk (t.ex. självcertifierade enheter) uteslutande baserade på den enhetens medlemskap i respektive ramverk. Om vi eller en av våra koncernenheter är medlem i ett sådant ramverk, baseras alla överföringar till oss eller vår koncernenhet uteslutande på enhetens medlemskap i ett sådant ramverk.

Alla registrerade kan få en kopia av ramverken från oss. Ramarna finns också tillgängliga i Europeiska unionens officiella tidning eller i publicerat rättsligt material eller på tillsynsmyndigheternas eller andra behöriga myndigheters eller institutioners webbplatser.

## G. Den period under vilken personuppgifterna kommer att lagras eller, om detta inte är möjligt, de kriterier som används för att fastställa denna period (artikel 14.2 a GDPR)

Personuppgifter om sökande lagras i sex månader. För uppgifter om anställda gäller respektive lagstadgad lagringstid. Efter utgången av denna period raderas motsvarande uppgifter rutinmässigt, så länge de inte längre är nödvändiga för att fullgöra avtalet eller inleda ett avtal.

## H. Om behandlingen grundar sig på artikel 6.1 f, den personuppgiftsansvariges eller en tredje parts berättigade intressen (artikel 14.2 b GDPR).

Enligt artikel 6.1 f GDPR ska behandlingen vara laglig endast om den är nödvändig för att tillgodose den personuppgiftsansvariges eller en tredje parts berättigade intressen, utom när dessa intressen åsidosätts av den registrerades intressen eller grundläggande rättigheter och friheter som kräver skydd av personuppgifter. Enligt skäl 47, andra meningen i skäl 47 GDPR kan ett legitimt intresse föreligga om det finns ett relevant och lämpligt förhållande mellan den registrerade och den registeransvarige, t.ex. i situationer där den registrerade är en kund till den registeransvarige. I alla fall där vårt företag behandlar uppgifter om sökande på grundval av artikel 6.1 lit. f GDPR är vårt legitima intresse att anställa lämplig personal och yrkesutövare.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## I. Förekomsten av rätten att av den personuppgiftsansvarige begära tillgång till och rättelse eller radering av personuppgifter eller begränsning av behandling som rör den registrerade och att invända mot behandling samt rätten till dataportabilitet (artikel 14.2 c GDPR)

Alla registrerade har följande rättigheter:

***Rätt till tillgång***

Varje registrerad person har rätt att få tillgång till de personuppgifter som rör honom eller henne. Rätten till tillgång omfattar alla uppgifter som behandlas av oss. Rätten kan utövas enkelt och med rimliga intervall för att få kännedom om och kontrollera att behandlingen är laglig (skäl 63 GDPR). Denna rätt följer av art. 15 GDPR. Den registrerade kan kontakta oss för att utöva rätten till insyn.

***Rätt till rättelse***

Enligt artikel 16 första meningen GDPR har den registrerade rätt att från den personuppgiftsansvarige utan onödigt dröjsmål få rättelse av felaktiga personuppgifter om honom eller henne. Vidare föreskrivs i artikel 16 andra meningen GDPR att den registrerade, med hänsyn till ändamålen med behandlingen, har rätt att få ofullständiga personuppgifter kompletterade, bland annat genom att tillhandahålla en kompletterande förklaring. Den registrerade kan kontakta oss för att utöva sin rätt till rättelse.

***Rätt till radering (rätt att bli bortglömd)***

Dessutom har de registrerade rätt till radering och till att bli bortglömda enligt artikel. 17 GDPR. Denna rätt kan också utövas genom att kontakta oss. I detta läge vill vi dock påpeka att denna rätt inte gäller i den mån behandlingen är nödvändig för att uppfylla en rättslig förpliktelse som vårt företag är föremål för, artikel 17.3 b GDPR. Detta innebär att vi kan godkänna en ansökan om radering först efter det att den lagstadgade lagringsperioden har löpt ut.

***Rätt till begränsning av behandlingen***

Enligt artikel 18 GDPR har alla registrerade rätt att begränsa behandlingen. Begränsningen av behandlingen kan begäras om ett av de villkor som anges i artikel 18.1 a-d GDPR är uppfyllda. Den registrerade kan kontakta oss för att utöva rätten till begränsning av behandlingen.

***Rätt till invändningar***

Vidare anges i artikel. 21 GDPR rätten att göra invändningar. Den registrerade kan kontakta oss för att utöva sin rätt till invändning.

***Rätt till dataportabilitet***

Konst. 20 GDPR ger den registrerade rätt till dataportabilitet. Enligt denna bestämmelse har den registrerade på de villkor som anges i artikel 20.1 a och b GDPR rätt att få de personuppgifter som rör honom eller henne och som han eller hon har lämnat till en registeransvarig i ett strukturerat, allmänt använt och maskinläsbart format och har rätt att överföra dessa uppgifter till en annan registeransvarig


© All rights reserved by Heiko Maniero.

utan hinder från den registeransvarige till vilken personuppgifterna har lämnats. Den registrerade kan kontakta oss för att utöva rätten till dataportabilitet.

## J. Om behandlingen grundar sig på artikel 6.1 a eller artikel 9.2 a, rätten att när som helst återkalla sitt samtycke, utan att detta påverkar lagligheten av behandlingen på grundval av samtycket, innan detta återkallades (artikel 14.2 d GDPR).

Om behandlingen av personuppgifter grundar sig på artikel. 6.1 a GDPR, vilket är fallet, om den registrerade har gett sitt samtycke till behandling av personuppgifter för ett eller flera specifika ändamål eller om den baseras på artikel 9.2 a GDPR, som reglerar uttryckligt samtycke till behandling av särskilda kategorier av personuppgifter, har den registrerade enligt artikel 7.3 första meningen GDPR rätt att när som helst återkalla sitt samtycke.

Återkallande av samtycke ska inte påverka lagligheten av behandling som grundar sig på samtycke före återkallandet, artikel 7.3 andra meningen GDPR. Det ska vara lika lätt att återkalla som att ge samtycke, artikel 7.2.2. 7.3 fjärde meningen GDPR. Återkallandet av samtycket kan därför alltid ske på samma sätt som samtycket har getts eller på något annat sätt som den registrerade anser vara enklare. I dagens informationssamhälle är förmodligen det enklaste sättet att återkalla samtycke ett enkelt e-postmeddelande. Om den registrerade vill återkalla sitt samtycke till oss räcker det med ett enkelt e-postmeddelande till oss. Alternativt kan den registrerade välja något annat sätt att meddela oss att han eller hon återkallar sitt samtycke.

## K. Rätten att inge klagomål till en tillsynsmyndighet (artikel 14.2 e, 77.1 GDPR)

Som registeransvarig är vi skyldiga att informera den registrerade om rätten att lämna in ett klagomål till en tillsynsmyndighet, artikel 14.2 e GDPR. Rätten att lämna in ett klagomål till en tillsynsmyndighet regleras av artikel 77.1 GDPR. Enligt denna bestämmelse ska varje registrerad person, utan att det påverkar andra administrativa eller rättsliga åtgärder, ha rätt att lämna in ett klagomål till en tillsynsmyndighet, särskilt i den medlemsstat där han eller hon har sin vanliga vistelseort, sin arbetsplats eller den plats där den påstådda överträdelsen äger rum, om den registrerade anser att behandlingen av personuppgifter som rör honom eller henne strider mot den allmänna dataskyddsförordningen. Rätten att lämna in ett klagomål till en tillsynsmyndighet begränsades endast av unionsrätten på så sätt att den endast kan utövas inför en enda tillsynsmyndighet (skäl 141 första meningen GDPR). Syftet med denna regel är att undvika dubbla klagomål från samma registrerade i samma ärende. Om en registrerad person vill lämna in ett klagomål mot oss, uppmanas vi därför att kontakta endast en enda tillsynsmyndighet.


© All rights reserved by Heiko Maniero.

## L. Varifrån personuppgifterna kommer och i förekommande fall huruvida de har sitt ursprung i allmänt tillgängliga källor (artikel 14.2 f GDPR)

I princip samlas personuppgifter in direkt från den registrerade eller i samarbete med en myndighet (t.ex. genom att hämta uppgifter från ett officiellt register). Andra uppgifter om registrerade personer kommer från överföringar av koncernföretag. I samband med denna allmänna information är det antingen omöjligt eller skulle innebära en oproportionerligt stor ansträngning enligt artikel 3.1 i fördraget att ange de exakta källorna till personuppgifterna. 14(5) lit. b GDPR. I princip samlar vi inte in personuppgifter från offentligt tillgängliga källor.

Varje registrerad person kan när som helst kontakta oss för att få mer detaljerad information om de exakta källorna till de personuppgifter som rör honom eller henne. Om den registrerade inte kan få veta varifrån personuppgifterna kommer eftersom olika källor har använts, bör allmän information lämnas (skäl 61, fjärde meningen GDPR).

## M. Förekomsten av automatiserat beslutsfattande, inbegripet profilering enligt artikel 22.1 och 22.4, varvid det åtminstone i dessa fall ska lämnas meningsfull information om logiken bakom samt betydelsen och de förutsedda följderna av sådan behandling för den registrerade (artikel 14.2 g GDPR).

Som ett ansvarsfullt företag använder vi vanligtvis inte automatiserat beslutsfattande eller profilering. Om vi i undantagsfall använder automatiserat beslutsfattande eller profilering kommer vi att informera den registrerade antingen separat eller via ett underavsnitt i vår integritetspolicy (på vår webbplats). I detta fall gäller följande:

Automatiserat beslutsfattande - inklusive profilering - får ske om (1) detta är nödvändigt för att ingå eller fullgöra ett avtal mellan den registrerade och oss, eller (2) detta är tillåtet enligt unionsrätten eller medlemsstaternas nationella rätt som vi omfattas av och som också fastställer lämpliga åtgärder för att skydda den registrerades rättigheter och friheter och berättigade intressen, eller (3) detta grundas på den registrerades uttryckliga samtycke.

I de fall som avses i artikel 22.2 a och c i GDPR ska vi vidta lämpliga åtgärder för att skydda den registrerades rättigheter och friheter samt berättigade intressen. I dessa fall har du rätt att få mänskligt ingripande från den personuppgiftsansvarige, att uttrycka din ståndpunkt och att bestrida beslutet.

Meningsfull information om den logik som ingår, liksom betydelsen och de förutsedda konsekvenserna av sådan behandling för den registrerade, anges i vår integritetspolicy.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## III. EU-U.S. Data Privacy Framework (EU-U.S. DPF), UK Extension to the EU-U.S. DPF, Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF)

Om vår organisation är ett certifierat medlem av EU-U.S. Data Privacy Framework (EU-U.S. DPF) och/eller UK Extension to the EU-U.S. DPF och/eller Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF) gäller följande:

Vi följer EU-U.S. Data Privacy Framework (EU-U.S. DPF) och UK Extension to the EU-U.S. DPF samt Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF) som fastställts av U.S. Department of Commerce. Vårt företag har bekräftat för det amerikanska handelsdepartementet att det följer EU-U.S. Data Privacy Framework Principles (EU-U.S. DPF Principles) avseende behandlingen av personuppgifter som det erhåller från Europeiska unionen och Storbritannien under åberopande av EU-U.S. DPF och UK Extension to the EU-U.S. DPF. Vårt företag har bekräftat för det amerikanska handelsdepartementet att det följer Swiss-U.S. Data Privacy Framework Principles (Swiss-U.S. DPF Principles) avseende behandlingen av personuppgifter som det erhåller från Schweiz under åberopande av Swiss-U.S. DPF. I händelse av en konflikt mellan bestämmelserna i vår sekretesspolicy och EU-U.S. DPF Principles och/eller Swiss-U.S. DPF Principles, är Principles överordnade.

För att lära dig mer om Data Privacy Framework (DPF) programmet och för att se vår certifiering, besök https://www.dataprivacyframework.gov/.

Andra amerikanska enheter eller dotterbolag i vårt företag som också följer EU-U.S. DPF Principals, inklusive UK Extension to the EU-U.S. DPF och Swiss-U.S. DPF Principals, om tillämpligt, anges i vår sekretesspolicy.

I enlighet med EU-U.S. DPF och UK Extension to the EU-U.S. DPF samt Swiss-U.S. DPF förbinder sig vårt företag att samarbeta med den panel som inrättats av EU

dataskyddsmyndigheter och det brittiska Information Commissioner's Office (ICO) samt den federala dataskydds- och informationskommissionären (EDÖB) och följa deras råd angående olösta klagomål om vår hantering av personuppgifter som vi erhåller under åberopande av EU-U.S. DPF och UK Extension to the EU-U.S. DPF och Swiss-U.S. DPF.

Vi informerar de berörda personerna om de relevanta europeiska dataskyddsmyndigheterna som är ansvariga för att hantera klagomål om vår organisations hantering av personuppgifter i den övre delen av detta transparensdokument och om att vi erbjuder berörda personer ett lämpligt och kostnadsfritt rättsmedel.

Vi informerar alla berörda personer om att vårt företag är underkastat undersöknings- och verkställighetsbefogenheterna hos Federal Trade Commission (FTC).


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

Berörda personer har under vissa förutsättningar möjlighet att utnyttja en bindande skiljedom. Vår organisation är skyldig att lösa krav och följa villkoren enligt Bilaga I till DPF-Principals, om den berörda personen har begärt en bindande skiljedom genom att meddela vår organisation och har följt förfarandena och villkoren enligt Bilaga I till Principals.

Vi informerar härmed alla berörda personer om vår organisations ansvar i händelse av överföring av personuppgifter till tredje part.

För frågor från berörda personer eller dataskyddsmyndigheter har vi namngivit de lokala representanterna som anges högst upp i detta transparensdokument.

Vi erbjuder dig möjligheten att välja (Opt-out) om dina personuppgifter (i) ska överföras till tredje part eller (ii) användas för ett syfte som avsevärt skiljer sig från det/den syfte(n) för vilket de ursprungligen samlades in eller senare godkändes av dig. Den tydliga, väl synliga och lättillgängliga mekanismen för att utöva ditt val är att kontakta vår dataskyddsombud (DSB) via e-post. Du har inget val och vi är inte skyldiga att göra detta om uppgifterna överförs till en tredje part som agerar som agent eller bearbetare på våra vägnar och enligt våra instruktioner. Vi ingår dock alltid ett avtal med en sådan agent eller bearbetare.

För känsliga uppgifter (dvs. personuppgifter som innehåller information om hälsostatus, ras eller etniskt ursprung, politiska åsikter, religiösa eller filosofiska övertygelser, medlemskap i en fackförening eller information om sexualliv hos den berörda personen) begär vi ditt uttryckliga samtycke (Opt-in) när dessa uppgifter (i) ska överföras till tredje part eller (ii) användas för ett annat syfte än det för vilket de ursprungligen samlades in eller för vilket du senare har gett ditt godkännande genom att göra ditt Opt-in-val. Dessutom behandlar vi alla personuppgifter som vi mottar från tredje part som känsliga, om den tredje parten har identifierat och behandlat dem som sådana.

Vi informerar dig härmed om kravet att avslöja personuppgifter som svar på lagliga förfrågningar från myndigheter, inklusive att uppfylla krav från nationell säkerhet eller brottsbekämpning.

När vi överför personuppgifter till en tredje part som agerar som kontrollerande, följer vi Principals för meddelande och val. Dessutom ingår vi ett avtal med den tredje parten som är ansvarig för behandlingen, som stipulerar att dessa data endast får behandlas för begränsade och angivna syften i enlighet med det samtycke du har gett och att mottagaren måste tillhandahålla samma skyddsnivå som DPF Principals och informera oss om han finner att han inte längre kan uppfylla denna skyldighet. Avtalet föreskriver att den tredje parten, som är ansvarig, ska upphöra med behandlingen eller vidta andra lämpliga och adekvata åtgärder för att rätta till situationen om en sådan upptäckt görs.

Vid överföring av personuppgifter till en tredje part som agerar som agent eller processor, (i) överför vi dessa data endast för begränsade och angivna syften; (ii) säkerställer vi att agenten eller processorn är skyldig att tillhandahålla åtminstone samma skyddsnivå som krävs av DPF Principals; (iii) vidtar vi lämpliga och adekvata åtgärder för att säkerställa att agenten eller processorn faktiskt behandlar de överförda personuppgifterna på ett sätt som är förenligt med våra skyldigheter enligt DPF Principals; (iv)


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

kräver vi att agenten eller processorn informerar vår organisation om han finner att han inte längre kan uppfylla skyldigheten att tillhandahålla samma skyddsnivå som DPF Principals förutser; (v) efter en sådan notifiering, även enligt (iv), vidtar vi lämpliga och adekvata åtgärder för att stoppa obehörig behandling och åtgärda situationen; och (vi) tillhandahåller DPF Department på begäran en sammanfattning eller ett representativt exempel på de relevanta dataskyddsbestämmelserna i sitt avtal med denna agent.

I enlighet med EU-U.S. DPF och/eller UK Extension to the EU-U.S. DPF och/eller Swiss-U.S. DPF förbinder sig vår organisation att samarbeta med panelen inrättad av EU

dataskyddsmyndigheter och det brittiska Information Commissioner's Office (ICO) respektive den federala dataskydds- och informationskommissionären (EDÖB) och följa dess råd gällande olösta klagomål om vår hantering av personuppgifter, som vi har mottagit i samband med anställningsförhållanden, under åberopande av EU-U.S. DPF och UK Extension to the EU-U.S. DPF och Swiss-U.S. DPF.

Alla registrerade som tillfälligt befinner sig i Europeiska unionen (EU), Europeiska ekonomiska samarbetsområdet (EES) eller Storbritannien, eller som har sin hemvist eller vanliga vistelseort där, har rätt till de rättigheter och den registrerades rättigheter som publiceras i vårt transparensdokument, som också följer av artiklarna 15-22 i GDPR, inklusive rätten att få tillgång till personuppgifter. Vi har gjort denna information tillgänglig på alla EU- och EES-språk. Den engelska språkversionen gäller för Storbritannien.

Alla registrerade som är tillfälligt bosatta i Schweiz eller har sin hemvist eller vanliga vistelseort där har rätt till de rättigheter och den registrerades rättigheter enligt den schweiziska dataskyddslagen (DPA) och den schweiziska dataskyddsförordningen (DPR) som publiceras i vårt transparensdokument, inklusive rätten att få tillgång till personuppgifter. Vi har tillhandahållit denna information på de tre officiella språken i Schweiz (tyska, italienska och franska).


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

# SLOVENIAN: Informacije o obdelavi osebnih podatkov (13., 14. člen SUVP)

Spoštovani gospod ali gospa,

Osebni podatki vsakega posameznika, ki je z našim podjetjem v pogodbenem, predpogodbenem ali drugem razmerju, so posebej zaščiteni. Naš cilj je ohraniti visoko raven varstva podatkov. Zato rutinsko razvijamo svoje koncepte varstva podatkov in varnosti podatkov.

Seveda upoštevamo zakonske določbe o varstvu podatkov. V skladu s členoma 13 in 14 SUVP morajo upravljavci pri zbiranju osebnih podatkov izpolnjevati posebne zahteve glede informacij. S tem dokumentom so te obveznosti izpolnjene.

Terminologija pravnih predpisov je zapletena. Žal se pri pripravi tega dokumenta ni bilo mogoče izogniti uporabi pravnih izrazov. Zato poudarjamo, da se lahko za vsa vprašanja v zvezi s tem dokumentom, uporabljenimi izrazi ali formulacijami vedno obrnete na nas.

## I. Informacije, ki se zagotovijo, kadar se osebni podatki pridobijo od posameznika, na katerega se nanašajo osebni podatki (člen 13 Splošne uredbe o varstvu podatkov)

### A. Identiteto in kontaktne podatke upravljavca in njegovega predstavnika, kadar ta obstaja (člen 13(1)(a) SUVP)

Glej zgoraj.

### B. Kontaktne podatke pooblaščene osebe za varstvo podatkov, kadar ta obstaja (člen 13(1)(b) SUVP)

Glej zgoraj.

### C. Namene, za katere se osebni podatki obdelujejo, kakor tudi pravno podlago za njihovo obdelavo (člen 13(1)(c) SUVP)

Namen obdelave osebnih podatkov je izvajanje vseh postopkov, ki zadevajo upravljavca, stranke, potencialne stranke, poslovne partnerje ali druga pogodbena ali predpogodbena razmerja med navedenimi skupinami (v najširšem smislu) ali pravne obveznosti upravljavca.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

Art. 6(1)(a) Splošne uredbe o varstvu podatkov je pravna podlaga za postopke obdelave, za katere pridobimo soglasje za določen namen obdelave. Če je obdelava osebnih podatkov potrebna za izvajanje pogodbe, katere stranka je posameznik, na katerega se nanašajo osebni podatki, kot na primer, ko so postopki obdelave potrebni za dobavo blaga ali zagotavljanje katere koli druge storitve, obdelava temelji na členu 6(1)(b) SUVP. Enako velja za takšna dejanja obdelave, ki so potrebna za izvajanje predpogodbenih ukrepov, na primer v primeru poizvedb v zvezi z našimi izdelki ali storitvami. Ali za naše podjetje velja zakonska obveznost, po kateri je potrebna obdelava osebnih podatkov, na primer za izpolnjevanje davčnih obveznosti, obdelava temelji na členu 6(1) Uredbe (ES) št. 6(1)(c) Splošne uredbe o varstvu podatkov.

V redkih primerih je lahko obdelava osebnih podatkov potrebna za zaščito življenjskih interesov posameznika, na katerega se nanašajo osebni podatki, ali druge fizične osebe. Tako bi bilo na primer, če bi se obiskovalec v našem podjetju poškodoval in bi bilo treba njegovo ime, starost, podatke o zdravstvenem zavarovanju ali druge življenjsko pomembne informacije posredovati zdravniku, bolnišnici ali drugi tretji osebi. Takrat bi obdelava temeljila na členu. 6(1)(d) Splošne uredbe o varstvu podatkov.

Kadar je obdelava potrebna za izvajanje naloge, ki se izvaja v javnem interesu ali pri izvajanju javne oblasti, dodeljene upravljavcu, je pravna podlaga čl. 6(1)(e) Splošne uredbe o varstvu podatkov.

Nazadnje, dejanja obdelave lahko temeljijo na členu 6(1)(f) Splošne uredbe o varstvu podatkov. Ta pravna podlaga se uporablja za dejanja obdelave, ki niso zajeta v nobeni od zgoraj navedenih pravnih podlag, če je obdelava potrebna za namene zakonitih interesov, za katere si prizadeva naše podjetje ali tretja oseba, razen kadar nad takimi interesi prevladajo interesi ali temeljne pravice in svoboščine posameznika, na katerega se nanašajo osebni podatki, ki zahtevajo varstvo osebnih podatkov. Takšna dejanja obdelave so še posebej dovoljena, ker jih je evropski zakonodajalec izrecno omenil. Menil je, da je mogoče domnevati zakonit interes, če je posameznik, na katerega se nanašajo osebni podatki, stranka upravljavca (uvodna izjava 47, drugi stavek SUVP).

## D. Kadar obdelava temelji na točki (f) člena 6(1), zakonite interese, za uveljavljanje katerih si prizadeva upravljavec ali tretja oseba (točka d člena 13(1) SUVP)

Kadar obdelava osebnih podatkov temelji na členu 6(1)(f) Splošne uredbe o varstvu podatkov, je naš zakoniti interes, da izvajamo svoje poslovanje v korist dobrega počutja vseh zaposlenih in delničarjev.

## E. Uporabnike ali kategorije uporabnikov osebnih podatkov, če obstajajo (člen 13(1)(e) SUVP)

Javni organi


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

Zunanji organi

Drugi zunanji organi

Notranja obdelava

Obdelava znotraj skupine

Drugi organi

Seznam naših obdelovalcev in prejemnikov podatkov v tretjih državah ter po potrebi mednarodnih organizacij je objavljen na našem spletnem mestu ali pa ga lahko brezplačno zahtevate od nas. Če želite zahtevati ta seznam, se obrnite na našo pooblaščeno osebo za varstvo podatkov.

## F. Kadar je ustrezno, dejstvo, da upravljavec namerava prenesti osebne podatke v tretjo državo ali mednarodno organizacijo, ter obstoj ali neobstoj sklepa Komisije o ustreznosti ali v primeru prenosov iz člena 46 ali 47 ali drugega pododstavka člena 49(1) sklic na ustrezne ali primerne zaščitne ukrepe in sredstva za pridobitev njihove kopije ali kje so na voljo (člen 13(1)(f), člen 46(1), člen 46(2)(c) SUVP)

Med prejemniki osebnih podatkov so lahko vsa podjetja in podružnice, ki so del naše skupine (v nadaljevanju "podjetja v skupini") in imajo sedež ali pisarno v tretji državi. Seznam vseh družb v skupini ali prejemnikov lahko zahtevate od nas.

V skladu s členom 46(1) SUVP lahko upravljavec ali obdelovalec prenese osebne podatke v tretjo državo le, če je zagotovil ustrezne zaščitne ukrepe in pod pogojem, da so na voljo izvršljive pravice posameznikov, na katere se nanašajo osebni podatki, ter učinkovita pravna sredstva za posameznike, na katere se nanašajo osebni podatki. Ustrezni zaščitni ukrepi se lahko zagotovijo, ne da bi bilo potrebno posebno dovoljenje nadzornega organa, s standardnimi pogodbenimi klavzulami, člen 46(2)(c) SUVP.

Z vsemi prejemniki iz tretjih držav se pred prvim prenosom osebnih podatkov dogovorimo o standardnih pogodbenih klavzulah Evropske unije ali drugih ustreznih zaščitnih ukrepih. Posledično je zagotovljeno, da so posameznikom, na katere se nanašajo osebni podatki, zagotovljeni ustrezni zaščitni ukrepi, izvršljive pravice posameznikov, na katere se nanašajo osebni podatki, in učinkovita pravna sredstva. Vsak posameznik, na katerega se nanašajo osebni podatki, lahko pri nas dobi kopijo standardnih pogodbenih klavzul. Standardne pogodbene klavzule so na voljo tudi v Uradnem listu Evropske unije.

Člen 45(3) Splošne uredbe o varstvu podatkov (GDPR) daje Evropski komisiji pooblastilo, da z izvedbenim aktom odloči, da država, ki ni članica EU, zagotavlja ustrezno raven varstva. To pomeni raven varstva osebnih podatkov, ki je v bistvu enakovredna ravni varstva v EU. Učinek sklepov o ustreznosti je, da se lahko osebni podatki iz EU (ter Norveške, Lihtenštajna in Islandije) prosto in brez dodatnih ovir pretakajo v tretjo državo. Podobna pravila veljajo za Združeno kraljestvo, Švico in nekatere druge države.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

Če je Evropska komisija ali vlada druge države odločila, da tretja država zagotavlja ustrezno raven varstva, in je vzpostavljen veljaven okvir (npr. EU-U.S. Data Privacy Framework, Swiss-U.S. Data Privacy Framework, UK Extension to the EU-U.S. Data Privacy Framework), vsi naši prenosi članom teh okvirov (npr. samopotrjenim subjektom) temeljijo izključno na članstvu teh subjektov v zadevnem okviru. Če smo mi ali eno od naših upravičenj v skupini član takega okvira, vsi prenosi nam ali našemu upravičencu v skupini temeljijo izključno na članstvu tega subjekta v takem okviru.

Vsak posameznik, na katerega se nanašajo osebni podatki, lahko pri nas dobi kopijo okvirov. Poleg tega so okviri na voljo tudi v Uradnem listu Evropske unije ali v objavljenem pravnem gradivu ali na spletnih mestih nadzornih organov ali drugih pristojnih organov ali institucij.

## G. Obdobje hrambe osebnih podatkov ali, kadar to ni mogoče, merila, ki se uporabijo za določitev tega obdobja (člen 13(2)(a) SUVP)

Merilo za določitev obdobja hrambe osebnih podatkov je ustrezno zakonsko določeno obdobje hrambe. Po izteku tega obdobja se ustrezni podatki rutinsko izbrišejo, če niso več potrebni za izpolnitev pogodbe ali začetek pogodbe.

Če zakonsko določeno obdobje hrambe ne obstaja, je merilo pogodbeno ali interno obdobje hrambe.

## H. Obstoj pravice, da se od upravljavca zahtevajo dostop do osebnih podatkov in popravek ali izbris osebnih podatkov ali omejitev obdelave v zvezi s posameznikom, na katerega se nanašajo osebni podatki, ali obstoj pravice do ugovora obdelavi in pravice do prenosljivosti podatkov (člen 13(2)(b) SUVP)

Vsi posamezniki, na katere se nanašajo osebni podatki, imajo naslednje pravice:

***Pravica do dostopa***

Vsak posameznik, na katerega se nanašajo osebni podatki, ima pravico do dostopa do osebnih podatkov, ki se nanašajo nanj. Pravica do dostopa velja za vse podatke, ki jih obdelujemo. Pravico je mogoče uveljavljati enostavno in v razumnih časovnih presledkih, da bi se seznanili z zakonitostjo obdelave in jo preverili (uvodna izjava 63 Splošne uredbe o varstvu podatkov). Ta pravica izhaja iz člena 3(1)(a) Uredbe (ES) št. 15 SPLOŠNE UREDBE O VARSTVU PODATKOV. Posameznik, na katerega se nanašajo osebni podatki, se lahko za uveljavljanje pravice do dostopa obrne na nas.

***Pravica do popravka***

V skladu s členom 16, stavek 1 SUVP ima posameznik, na katerega se nanašajo osebni podatki, pravico, da od upravljavca brez nepotrebnega odlašanja zahteva popravek netočnih osebnih podatkov v zvezi z njim. Poleg tega člen 16, stavek 2 SUVP določa, da ima posameznik, na katerega se nanašajo osebni podatki, ob upoštevanju namenov obdelave pravico do dopolnitve nepopolnih osebnih podatkov, tudi z


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

zagotovitvijo dodatne izjave. Posameznik, na katerega se nanašajo osebni podatki, se lahko za uveljavljanje pravice do popravka obrne na nas.

***Pravica do izbrisa (pravica biti pozabljen)***

Poleg tega imajo posamezniki, na katere se nanašajo osebni podatki, pravico do izbrisa in do pozabe v skladu s čl. 17 SPLOŠNE UREDBE O VARSTVU PODATKOV. To pravico lahko uveljavljate tudi tako, da se obrnete na nas. Na tem mestu pa želimo poudariti, da ta pravica ne velja, če je obdelava potrebna za izpolnitev pravne obveznosti, ki velja za naše podjetje, člen 17(3)(b) SUVP. To pomeni, da lahko zahtevek za izbris odobrimo šele po izteku zakonsko določenega obdobja hrambe.

***Pravica do omejitve obdelave***

V skladu s členom 18 SUVP ima vsak posameznik, na katerega se nanašajo osebni podatki, pravico do omejitve obdelave. Omejitev obdelave se lahko zahteva, če je izpolnjen eden od pogojev iz člena 18(1)(a-d) SUVP. Posameznik, na katerega se nanašajo osebni podatki, se lahko za uveljavljanje pravice do omejitve obdelave obrne na nas.

***Pravica do ugovora***

Poleg tega je člen. 21 Splošne uredbe o varstvu podatkov zagotavlja pravico do ugovora. Posameznik, na katerega se nanašajo osebni podatki, se lahko za uveljavljanje pravice do ugovora obrne na nas.

***Pravica do prenosljivosti podatkov***

Art. 20 Splošne uredbe o varstvu podatkov posamezniku, na katerega se nanašajo osebni podatki, daje pravico do prenosljivosti podatkov. V skladu s to določbo ima posameznik, na katerega se nanašajo osebni podatki, pod pogoji iz člena 20(1)(a) in (b) SUVP pravico prejeti osebne podatke v zvezi z njim, ki jih je posredoval upravljavcu, v strukturirani, splošno uporabljani in strojno berljivi obliki ter pravico, da te podatke posreduje drugemu upravljavcu brez ovir s strani upravljavca, ki so mu bili osebni podatki posredovani. Posameznik, na katerega se nanašajo osebni podatki, se lahko za uveljavljanje pravice do prenosljivosti podatkov obrne na nas.

## I. Kadar obdelava temelji na točki (a) člena 6(1) ali točki (a) člena 9(2), obstoj pravice, da se lahko privolitev kadar koli prekliče, ne da bi to vplivalo na zakonitost obdelave podatkov, ki se je na podlagi privolitve izvajala do njenega preklica (člen 13(2)(c) SUVP)

Če obdelava osebnih podatkov temelji na členu. a, kar je v primeru, če je posameznik, na katerega se nanašajo osebni podatki, privolil v obdelavo osebnih podatkov za enega ali več posebnih namenov, ali če temelji na členu 9(2)(a) SUVP, ki ureja izrecno privolitev v obdelavo posebnih vrst osebnih podatkov, ima posameznik, na katerega se nanašajo osebni podatki, v skladu s členom 7(3), stavek 1 SUVP pravico kadar koli preklicati svojo privolitev.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

Preklic privolitve ne vpliva na zakonitost obdelave na podlagi privolitve pred njenim preklicem, člen 7(3), stavek 2 SUVP. Preklic soglasja mora biti enako enostaven kot dajanje soglasja, čl. 7(3), stavek 4 Splošne uredbe o varstvu podatkov. Zato se lahko preklic privolitve vedno izvede na enak način, kot je bila dana privolitev, ali na kateri koli drug način, ki se posamezniku, na katerega se nanašajo osebni podatki, zdi enostavnejši. V današnji informacijski družbi je verjetno najpreprostejši način preklica privolitve preprosto elektronsko sporočilo. Če želi posameznik, na katerega se nanašajo osebni podatki, preklicati soglasje, ki nam ga je dal, zadostuje, da nam pošlje preprosto elektronsko sporočilo. Posameznik, na katerega se nanašajo osebni podatki, lahko izbere tudi kakršen koli drug način, da nam sporoči svoj preklic privolitve.

## J. Pravico do vložitve pritožbe pri nadzornem organu (člen 13(2)(d), 77(1) SUVP)

Kot upravljavec moramo posameznika, na katerega se nanašajo osebni podatki, obvestiti o pravici do vložitve pritožbe pri nadzornem organu, člen 13(2)(d) SUVP. Pravico do vložitve pritožbe pri nadzornem organu ureja člen 77(1) SUVP. V skladu s to določbo ima vsak posameznik, na katerega se nanašajo osebni podatki, brez poseganja v katero koli drugo upravno ali sodno pravno sredstvo pravico vložiti pritožbo pri nadzornem organu, zlasti v državi članici svojega običajnega prebivališča, kraja dela ali kraja domnevne kršitve, če meni, da obdelava osebnih podatkov v zvezi z njim krši Splošno uredbo o varstvu podatkov. Pravica do vložitve pritožbe pri nadzornem organu je bila s pravom Unije omejena le tako, da jo je mogoče uveljavljati le pri enem nadzornem organu (uvodna izjava 141, stavek 1 Splošne uredbe o varstvu podatkov). Namen tega pravila je preprečiti dvojne pritožbe istega posameznika, na katerega se nanašajo osebni podatki, v isti zadevi. Če želi posameznik, na katerega se nanašajo osebni podatki, vložiti pritožbo zoper nas, smo ga zato pozvali, naj se obrne le na en nadzorni organ.

## K. Ali je zagotovitev osebnih podatkov statutarna ali pogodbena obveznost ali pa obveznost, ki je potrebna za sklenitev pogodbe, ter ali mora posameznik, na katerega se nanašajo osebni podatki, zagotoviti osebne podatke ter kakšne so morebitne posledice, če se taki podatki ne zagotovijo, in (člen 13(2)(e) SUVP)

Pojasnjujemo, da je posredovanje osebnih podatkov delno zahtevano z zakonom (npr. davčni predpisi), lahko pa izhaja tudi iz pogodbenih določb (npr. informacije o pogodbenem partnerju).

Včasih je za sklenitev pogodbe potrebno, da nam posameznik, na katerega se nanašajo osebni podatki, posreduje osebne podatke, ki jih moramo nato obdelati. Posameznik, na katerega se nanašajo osebni podatki, nam mora na primer posredovati osebne podatke, ko naše podjetje z njim podpiše pogodbo. Neposredovanje osebnih podatkov bi imelo za posledico, da pogodbe s posameznikom, na katerega se nanašajo osebni podatki, ne bi bilo mogoče skleniti.

Preden posameznik, na katerega se nanašajo osebni podatki, posreduje osebne podatke, se mora obrniti na nas. Posamezniku, na katerega se nanašajo osebni podatki, pojasnimo, ali je posredovanje osebnih


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

podatkov zahtevano z zakonom ali pogodbo ali je potrebno za sklenitev pogodbe, ali obstaja obveznost posredovanja osebnih podatkov in kakšne so posledice, če osebnih podatkov ne posreduje.

### L. Obstoj avtomatiziranega sprejemanja odločitev, vključno z oblikovanjem profilov iz člena 22(1) in (4), ter vsaj v takih primerih smiselne informacije o razlogih zanj, kot tudi pomen in predvidene posledice take obdelave za posameznika, na katerega se nanašajo osebni podatki (člen 13(2)(f) SUVP)

Kot odgovorno podjetje običajno ne uporabljamo avtomatiziranega odločanja ali profiliranja. Če v izjemnih primerih izvajamo avtomatizirano odločanje ali profiliranje, bomo posameznika, na katerega se nanašajo osebni podatki, o tem obvestili ločeno ali prek pododdelka v naši politiki zasebnosti (na naši spletni strani). V tem primeru velja naslednje:

Avtomatizirano sprejemanje odločitev - vključno z oblikovanjem profilov - se lahko izvede, če (1) je to potrebno za sklenitev ali izvajanje pogodbe med posameznikom, na katerega se nanašajo osebni podatki, in nami, ali (2) je to dovoljeno z zakonodajo Unije ali države članice, ki velja za nas in ki določa tudi ustrezne ukrepe za zaščito pravic in svoboščin ter zakonitih interesov posameznika, na katerega se nanašajo osebni podatki, ali (3) to temelji na izrecni privolitvi posameznika, na katerega se nanašajo osebni podatki.

V primerih iz člena 22(2)(a) in (c) GDPR izvedemo ustrezne ukrepe za zaščito pravic in svoboščin ter zakonitih interesov posameznika, na katerega se nanašajo osebni podatki. V teh primerih imate pravico do človeškega posredovanja s strani upravljavca, da izrazite svoje stališče in izpodbijate odločitev.

Smiselne informacije o vključeni logiki ter pomenu in predvidenih posledicah takšne obdelave za posameznika, na katerega se nanašajo osebni podatki, so navedene v naši politiki zasebnosti.

## II. Informacije, ki jih je treba zagotoviti, kadar osebni podatki niso bili pridobljeni od posameznika, na katerega se ti nanašajo (člen 14 Splošne uredbe o varstvu podatkov)

### A. Istovetnost in kontaktne podatke upravljavca in njegovega predstavnika, kadar ta obstaja (člen 14(1)(a) SUVP)

Glej zgoraj.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## B. Kontaktne podatke pooblaščene osebe za varstvo podatkov, kadar ta obstaja (člen 14(1)(b) SUVP)

Glej zgoraj.

## C. Namene, za katere se osebni podatki obdelujejo, kakor tudi pravno podlago za njihovo obdelavo (člen 14(1)(c) SUVP)

Namen obdelave osebnih podatkov je izvajanje vseh postopkov, ki zadevajo upravljavca, stranke, potencialne stranke, poslovne partnerje ali druga pogodbena ali predpogodbena razmerja med navedenimi skupinami (v najširšem smislu) ali pravne obveznosti upravljavca.

Če je obdelava osebnih podatkov potrebna za izvajanje pogodbe, katere stranka je posameznik, na katerega se nanašajo osebni podatki, kot na primer, ko so postopki obdelave potrebni za dobavo blaga ali zagotavljanje katere koli druge storitve, obdelava temelji na členu 6(1)(b) SUVP. Enako velja za takšna dejanja obdelave, ki so potrebna za izvajanje predpogodbenih ukrepov, na primer v primeru poizvedb v zvezi z našimi izdelki ali storitvami. Ali za naše podjetje velja zakonska obveznost, po kateri je potrebna obdelava osebnih podatkov, na primer za izpolnjevanje davčnih obveznosti, obdelava temelji na členu 6(1) Uredbe (ES) št. 6(1)(c) Splošne uredbe o varstvu podatkov.

V redkih primerih je lahko obdelava osebnih podatkov potrebna za zaščito življenjskih interesov posameznika, na katerega se nanašajo osebni podatki, ali druge fizične osebe. Tako bi bilo na primer, če bi se obiskovalec v našem podjetju poškodoval in bi bilo treba njegovo ime, starost, podatke o zdravstvenem zavarovanju ali druge življenjsko pomembne informacije posredovati zdravniku, bolnišnici ali drugi tretji osebi. Takrat bi obdelava temeljila na členu. 6(1)(d) Splošne uredbe o varstvu podatkov.

Kadar je obdelava potrebna za izvajanje naloge, ki se izvaja v javnem interesu ali pri izvajanju javne oblasti, dodeljene upravljavcu, je pravna podlaga čl. 6(1)(e) Splošne uredbe o varstvu podatkov.

Nazadnje, dejanja obdelave lahko temeljijo na členu 6(1)(f) Splošne uredbe o varstvu podatkov. Ta pravna podlaga se uporablja za dejanja obdelave, ki niso zajeta v nobeni od zgoraj navedenih pravnih podlag, če je obdelava potrebna za namene zakonitih interesov, za katere si prizadeva naše podjetje ali tretja oseba, razen kadar nad takimi interesi prevladajo interesi ali temeljne pravice in svoboščine posameznika, na katerega se nanašajo osebni podatki, ki zahtevajo varstvo osebnih podatkov. Takšna dejanja obdelave so še posebej dovoljena, ker jih je evropski zakonodajalec izrecno omenil. Menil je, da je mogoče domnevati zakonit interes, če je posameznik, na katerega se nanašajo osebni podatki, stranka upravljavca (uvodna izjava 47, drugi stavek SUVP).

## D. Vrste zadevnih osebnih podatkov (člen 14(1)(d) SUVP)


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

Podatki o strankah

Podatki o potencialnih strankah

Podatki o zaposlenih

Podatki o dobaviteljih

## E. Uporabnike ali kategorije uporabnikov osebnih podatkov, kadar obstajajo (člen 14(1)(e) SUVP)

Javni organi

Zunanji organi

Drugi zunanji organi

Notranja obdelava

Obdelava znotraj skupine

Drugi organi

Seznam naših obdelovalcev in prejemnikov podatkov v tretjih državah ter po potrebi mednarodnih organizacij je objavljen na našem spletnem mestu ali pa ga lahko brezplačno zahtevate od nas. Če želite zahtevati ta seznam, se obrnite na našo pooblaščeno osebo za varstvo podatkov.

## F. Kadar je ustrezno, informacije o tem, da namerava upravljavec prenesti osebne podatke uporabniku v tretji državi ali mednarodni organizaciji, ter o obstoju ali neobstoju sklepa Komisije o ustreznosti ali v primeru prenosov iz člena 46 ali 47 ali drugega pododstavka člena 49(1) sklic na ustrezne ali primerne zaščitne ukrepe in sredstva za pridobitev njihove kopije ali kje so na voljo (člen 14(1)(f), člen 46(1), člen 46(2)(c) SUVP)

Med prejemniki osebnih podatkov so lahko vsa podjetja in podružnice, ki so del naše skupine (v nadaljevanju "podjetja v skupini") in imajo sedež ali poslovalnico v tretji državi. Seznam vseh družb v skupini lahko zahtevate pri nas.

V skladu s členom 46(1) SUVP lahko upravljavec ali obdelovalec prenese osebne podatke v tretjo državo le, če je zagotovil ustrezne zaščitne ukrepe in pod pogojem, da so na voljo izvršljive pravice posameznikov, na katere se nanašajo osebni podatki, ter učinkovita pravna sredstva za posameznike, na katere se nanašajo osebni podatki. Ustrezni zaščitni ukrepi se lahko zagotovijo, ne da bi bilo potrebno


© All rights reserved by Heiko Maniero.

posebno dovoljenje nadzornega organa, s standardnimi klavzulami o varstvu podatkov, člen 46(2)(c) SUVP.

Z vsemi prejemniki iz tretjih držav se pred prvim prenosom osebnih podatkov dogovorimo o standardnih pogodbenih klavzulah Evropske unije ali drugih ustreznih zaščitnih ukrepih. Posledično je zagotovljeno, da so posameznikom, na katere se nanašajo osebni podatki, zagotovljeni ustrezni zaščitni ukrepi, izvršljive pravice posameznikov, na katere se nanašajo osebni podatki, in učinkovita pravna sredstva. Vsak posameznik, na katerega se nanašajo osebni podatki, lahko pri nas dobi kopijo standardnih pogodbenih klavzul. Standardne pogodbene klavzule so na voljo tudi v Uradnem listu Evropske unije.

Člen 45(3) Splošne uredbe o varstvu podatkov (GDPR) daje Evropski komisiji pooblastilo, da z izvedbenim aktom odloči, da država, ki ni članica EU, zagotavlja ustrezno raven varstva. To pomeni raven varstva osebnih podatkov, ki je v bistvu enakovredna ravni varstva v EU. Učinek sklepov o ustreznosti je, da se lahko osebni podatki iz EU (ter Norveške, Lihtenštajna in Islandije) prosto in brez dodatnih ovir pretakajo v tretjo državo. Podobna pravila veljajo za Združeno kraljestvo, Švico in nekatere druge države.

Če je Evropska komisija ali vlada druge države odločila, da tretja država zagotavlja ustrezno raven varstva, in je vzpostavljen veljaven okvir (npr. EU-U.S. Data Privacy Framework, Swiss-U.S. Data Privacy Framework, UK Extension to the EU-U.S. Data Privacy Framework), vsi naši prenosi članom teh okvirov (npr. samopotrjenim subjektom) temeljijo izključno na članstvu teh subjektov v zadevnem okviru. Če smo mi ali eno od naših upravičenj v skupini član takega okvira, vsi prenosi nam ali našemu upravičencu v skupini temeljijo izključno na članstvu tega subjekta v takem okviru.

Vsak posameznik, na katerega se nanašajo osebni podatki, lahko pri nas dobi kopijo okvirov. Poleg tega so okviri na voljo tudi v Uradnem listu Evropske unije ali v objavljenem pravnem gradivu ali na spletnih mestih nadzornih organov ali drugih pristojnih organov ali institucij.

## G. Obdobje hrambe osebnih podatkov ali, če to ni mogoče, merila, ki se uporabijo za določitev tega obdobja (člen 14(2)(a) SUVP)

Merilo za določitev obdobja hrambe osebnih podatkov je ustrezno zakonsko določeno obdobje hrambe. Po izteku tega obdobja se ustrezni podatki rutinsko izbrišejo, če niso več potrebni za izpolnitev pogodbe ali začetek pogodbe.

Če zakonsko določeno obdobje hrambe ne obstaja, je merilo pogodbeno ali interno obdobje hrambe.

## H. Kadar obdelava temelji na točki (f) člena 6(1), zakonite interese, za uveljavljanje katerih si prizadeva upravljavec ali tretja oseba (člen 14(2)(b) SUVP)

V skladu s členom 6(1)(f) SUVP je obdelava zakonita le, če je obdelava potrebna za namene zakonitih interesov, za katere si prizadeva upravljavec ali tretja oseba, razen če nad takimi interesi prevladajo


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

interesi ali temeljne pravice in svoboščine posameznika, na katerega se nanašajo osebni podatki, ki zahtevajo varstvo osebnih podatkov. V skladu z uvodno izjavo 47, drugi stavek, Splošne uredbe o varstvu podatkov bi lahko zakoniti interes obstajal, kadar obstaja ustrezno in primerno razmerje med posameznikom, na katerega se nanašajo osebni podatki, in upravljavcem, npr. v primerih, ko je posameznik, na katerega se nanašajo osebni podatki, stranka upravljavca. V vseh primerih, ko naše podjetje obdeluje osebne podatke na podlagi člena 6(1)(f) SUVP, je naš zakoniti interes izvajanje dejavnosti v korist dobrega počutja vseh zaposlenih in delničarjev.

## I. Obstoj pravice, da se od upravljavca zahtevajo dostop do osebnih podatkov in popravek ali izbris osebnih podatkov ali omejitev obdelave v zvezi s posameznikom, na katerega se nanašajo osebni podatki, in obstoj pravice do ugovora obdelavi ter pravice do prenosljivosti podatkov (člen 14(2)(c) SUVP)

Vsi posamezniki, na katere se nanašajo osebni podatki, imajo naslednje pravice:

***Pravica do dostopa***

Vsak posameznik, na katerega se nanašajo osebni podatki, ima pravico do dostopa do osebnih podatkov, ki se nanašajo nanj. Pravica do dostopa velja za vse podatke, ki jih obdelujemo. Pravico je mogoče uveljavljati enostavno in v razumnih časovnih presledkih, da bi se seznanili z zakonitostjo obdelave in jo preverili (uvodna izjava 63 Splošne uredbe o varstvu podatkov). Ta pravica izhaja iz člena 3(1)(a) Uredbe (ES) št. 15 SPLOŠNE UREDBE O VARSTVU PODATKOV. Posameznik, na katerega se nanašajo osebni podatki, se lahko za uveljavljanje pravice do dostopa obrne na nas.

***Pravica do popravka***

V skladu s členom 16, stavek 1 SUVP ima posameznik, na katerega se nanašajo osebni podatki, pravico, da od upravljavca brez nepotrebnega odlašanja zahteva popravek netočnih osebnih podatkov v zvezi z njim. Poleg tega člen 16, stavek 2 SUVP določa, da ima posameznik, na katerega se nanašajo osebni podatki, ob upoštevanju namenov obdelave pravico do dopolnitve nepopolnih osebnih podatkov, tudi z zagotovitvijo dodatne izjave. Posameznik, na katerega se nanašajo osebni podatki, se lahko za uveljavljanje pravice do popravka obrne na nas.

***Pravica do izbrisa (pravica biti pozabljen)***

Poleg tega imajo posamezniki, na katere se nanašajo osebni podatki, pravico do izbrisa in do pozabe v skladu s čl. 17 SPLOŠNE UREDBE O VARSTVU PODATKOV. To pravico lahko uveljavljate tudi tako, da nas kontaktirate. Na tem mestu pa želimo poudariti, da ta pravica ne velja, če je obdelava potrebna za izpolnitev pravne obveznosti, ki velja za naše podjetje, člen 17(3)(b) SUVP. To pomeni, da lahko zahtevek za izbris odobrimo šele po izteku zakonsko določenega obdobja hrambe.

***Pravica do omejitve obdelave***

V skladu s členom 18 SUVP ima vsak posameznik, na katerega se nanašajo osebni podatki, pravico do omejitve obdelave. Omejitev obdelave se lahko zahteva, če je izpolnjen eden od pogojev iz člena 18(1)(a-


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

d) SUVP. Posameznik, na katerega se nanašajo osebni podatki, se lahko za uveljavljanje pravice do omejitve obdelave obrne na nas.

***Pravica do ugovora***

Poleg tega je člen. 21 Splošne uredbe o varstvu podatkov zagotavlja pravico do ugovora. Posameznik, na katerega se nanašajo osebni podatki, se lahko za uveljavljanje pravice do ugovora obrne na nas.

***Pravica do prenosljivosti podatkov***

Art. 20 Splošne uredbe o varstvu podatkov posamezniku, na katerega se nanašajo osebni podatki, daje pravico do prenosljivosti podatkov. V skladu s to določbo ima posameznik, na katerega se nanašajo osebni podatki, pod pogoji iz člena 20(1)(a) in (b) SUVP pravico prejeti osebne podatke v zvezi z njim, ki jih je posredoval upravljavcu, v strukturirani, splošno uporabljani in strojno berljivi obliki ter pravico, da te podatke posreduje drugemu upravljavcu brez ovir s strani upravljavca, ki so mu bili osebni podatki posredovani. Posameznik, na katerega se nanašajo osebni podatki, se lahko za uveljavljanje pravice do prenosljivosti podatkov obrne na nas.

## J. Kadar obdelava temelji na točki (a) člena 6(1) ali točki (a) člena 9(2), obstoj pravice, da se lahko privolitev kadar koli prekliče, ne da bi to vplivalo na zakonitost obdelave podatkov, ki se je na podlagi privolitve izvajala do njenega preklica (člen 14(2)(d) SUVP)

Če obdelava osebnih podatkov temelji na členu. a, kar je v primeru, če je posameznik, na katerega se nanašajo osebni podatki, privolil v obdelavo osebnih podatkov za enega ali več posebnih namenov, ali če temelji na členu 9(2)(a) SUVP, ki ureja izrecno privolitev v obdelavo posebnih vrst osebnih podatkov, ima posameznik, na katerega se nanašajo osebni podatki, v skladu s členom 7(3), stavek 1 SUVP pravico kadar koli preklicati svojo privolitev.

Preklic privolitve ne vpliva na zakonitost obdelave na podlagi privolitve pred njenim preklicem, člen 7(3), stavek 2 SUVP. Preklic soglasja mora biti enako enostaven kot dajanje soglasja, čl. 7(3), stavek 4 Splošne uredbe o varstvu podatkov. Zato se lahko preklic privolitve vedno izvede na enak način, kot je bila dana privolitev, ali na kateri koli drug način, ki se posamezniku, na katerega se nanašajo osebni podatki, zdi enostavnejši. V današnji informacijski družbi je verjetno najpreprostejši način preklica privolitve preprosto elektronsko sporočilo. Če želi posameznik, na katerega se nanašajo osebni podatki, preklicati soglasje, ki nam ga je dal, zadostuje, da nam pošlje preprosto elektronsko sporočilo. Posameznik, na katerega se nanašajo osebni podatki, lahko izbere tudi kakršen koli drug način, da nam sporoči svoj preklic privolitve.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## K. Pravico do vložitve pritožbe pri nadzornem organu (člen 14(2)(e), 77(1) SUVP)

Kot upravljavec moramo posameznika, na katerega se nanašajo osebni podatki, obvestiti o pravici do vložitve pritožbe pri nadzornem organu, člen 14(2)(e) SUVP. Pravico do vložitve pritožbe pri nadzornem organu ureja člen 77(1) SUVP. V skladu s to določbo ima vsak posameznik, na katerega se nanašajo osebni podatki, brez poseganja v katero koli drugo upravno ali sodno pravno sredstvo pravico vložiti pritožbo pri nadzornem organu, zlasti v državi članici svojega običajnega prebivališča, kraja dela ali kraja domnevne kršitve, če meni, da obdelava osebnih podatkov v zvezi z njim krši Splošno uredbo o varstvu podatkov. Pravica do vložitve pritožbe pri nadzornem organu je bila s pravom Unije omejena le tako, da jo je mogoče uveljavljati le pri enem nadzornem organu (uvodna izjava 141, stavek 1 Splošne uredbe o varstvu podatkov). Namen tega pravila je preprečiti dvojne pritožbe istega posameznika, na katerega se nanašajo osebni podatki, v isti zadevi. Če želi posameznik, na katerega se nanašajo osebni podatki, vložiti pritožbo zoper nas, smo ga zato prosili, naj se obrne samo na en nadzorni organ.

## L. Od kje izvirajo osebni podatki in po potrebi, ali izvirajo iz javno dostopnih virov, in (člen 14(2)(f) Splošne uredbe o varstvu podatkov)

Načeloma se osebni podatki zbirajo neposredno od posameznika, na katerega se nanašajo, ali v sodelovanju z organom (npr. pridobivanje podatkov iz uradnega registra). Drugi podatki o posameznikih, na katere se nanašajo osebni podatki, se pridobijo s prenosi podjetij v skupini. V okviru teh splošnih informacij navajanje natančnih virov, iz katerih izvirajo osebni podatki, ni mogoče ali pa bi zahtevalo nesorazmeren napor v smislu člena 3(1)(2)(a) Direktive 95/46/ES. 14(5)(b) Splošne uredbe o varstvu podatkov. Načeloma osebnih podatkov ne zbiramo iz javno dostopnih virov.

Vsak posameznik, na katerega se nanašajo osebni podatki, se lahko kadar koli obrne na nas in pridobi podrobnejše informacije o natančnih virih osebnih podatkov, ki se nanašajo nanj. Kadar posamezniku, na katerega se nanašajo osebni podatki, ni mogoče zagotoviti izvora osebnih podatkov, ker so bili uporabljeni različni viri, je treba zagotoviti splošne informacije (uvodna izjava 61, stavek 4 Splošne uredbe o varstvu podatkov).

## M. Obstoj avtomatiziranega sprejemanja odločitev, vključno z oblikovanjem profilov iz člena 22(1) in (4), ter vsaj v takih primerih smiselne informacije o razlogih zanj, kot tudi pomen in predvidene posledice take obdelave za posameznika, na katerega se nanašajo osebni podatki (člen 14(2)(g) SUVP)

Kot odgovorno podjetje običajno ne uporabljamo avtomatiziranega odločanja ali profiliranja. Če v izjemnih primerih izvajamo avtomatizirano odločanje ali profiliranje, bomo posameznika, na katerega se nanašajo osebni podatki, o tem obvestili ločeno ali prek pododdelka v naši politiki zasebnosti (na naši spletni strani). V tem primeru velja naslednje:


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

Avtomatizirano sprejemanje odločitev - vključno z oblikovanjem profilov - se lahko izvede, če (1) je to potrebno za sklenitev ali izvajanje pogodbe med posameznikom, na katerega se nanašajo osebni podatki, in nami, ali (2) je to dovoljeno z zakonodajo Unije ali države članice, ki velja za nas in ki določa tudi ustrezne ukrepe za zaščito pravic in svoboščin ter zakonitih interesov posameznika, na katerega se nanašajo osebni podatki, ali (3) to temelji na izrecni privolitvi posameznika, na katerega se nanašajo osebni podatki.

V primerih iz člena 22(2)(a) in (c) GDPR izvedemo ustrezne ukrepe za zaščito pravic in svoboščin ter zakonitih interesov posameznika, na katerega se nanašajo osebni podatki. V teh primerih imate pravico do človeškega posredovanja s strani upravljavca, da izrazite svoje stališče in izpodbijate odločitev.

Smiselne informacije o vključeni logiki ter pomenu in predvidenih posledicah takšne obdelave za posameznika, na katerega se nanašajo osebni podatki, so navedene v naši politiki zasebnosti.

## III. EU-U.S. Data Privacy Framework (EU-U.S. DPF), UK Extension to the EU-U.S. DPF, Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF)

Če je naša organizacija certificirani član EU-U.S. Data Privacy Framework (EU-U.S. DPF) in/ali UK Extension to the EU-U.S. DPF in/ali Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF), velja naslednje:

Držimo se EU-U.S. Data Privacy Framework (EU-U.S. DPF) in UK Extension to the EU-U.S. DPF ter Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF), kot je določilo U.S. Department of Commerce. Naše podjetje je ameriškemu ministrstvu za trgovino potrdilo, da spoštuje EU-U.S. Data Privacy Framework Principles (EU-U.S. DPF Principles) v zvezi z obdelavo osebnih podatkov, ki jih prejema iz Evropske unije in Združenega kraljestva v skladu z EU-U.S. DPF in UK Extension to the EU-U.S. DPF. Naše podjetje je ameriškemu ministrstvu za trgovino potrdilo, da spoštuje Swiss-U.S. Data Privacy Framework Principles (Swiss-U.S. DPF Principles) v zvezi z obdelavo osebnih podatkov, ki jih prejema iz Švice v skladu s Swiss-U.S. DPF. V primeru nasprotja med določili naše politike zasebnosti in EU-U.S. DPF Principles in/ali Swiss-U.S. DPF Principles prevladujejo Principles.

Za več informacij o programu Data Privacy Framework (DPF) in ogled našega certifikata obiščite https://www.dataprivacyframework.gov/.

Druge ameriške enote ali hčerinske družbe našega podjetja, ki prav tako spoštujejo EU-U.S. DPF Principals, vključno z UK Extension to the EU-U.S. DPF in Swiss-U.S. DPF Principals, če obstajajo, so navedene v naši politiki zasebnosti.

V skladu z EU-U.S. DPF in UK Extension to the EU-U.S. DPF ter Swiss-U.S. DPF se naše podjetje zavezuje, da bo sodelovalo z organom, ki ga ustanovijo evropski organi za varstvo podatkov in britanski


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

Information Commissioner's Office (ICO) ter Švicarski zvezni pooblaščenec za varstvo podatkov in za informacije (EDÖB), ter upoštevalo njihova priporočila glede nerešenih pritožb o našem ravnanju z osebnimi podatki, ki jih prejmemo na podlagi EU-U.S. DPF in UK Extension to the EU-U.S. DPF in Swiss-U.S. DPF.

Obveščamo prizadete osebe o pristojnih evropskih organih za varstvo podatkov, ki so odgovorni za obravnavanje pritožb o ravnanju naše organizacije z osebnimi podatki, na zgornjem delu tega dokumenta o transparentnosti in o tem, da prizadetim osebam nudimo ustrezno in brezplačno pravno sredstvo.

Vse prizadete osebe obveščamo, da je naše podjetje podrejeno preiskovalnim in izvršilnim pristojnostim Federal Trade Commission (FTC).

Prizadete osebe imajo pod določenimi pogoji možnost zahtevati zavezujočo arbitražo. Naša organizacija je dolžna reševati zahtevke in upoštevati pogoje v skladu z Dodatkom I k DPF-Principals, če prizadeta oseba zahteva zavezujočo arbitražo tako, da obvesti našo organizacijo in so upoštevani postopki in pogoji v skladu z Dodatkom I k Principals.

S tem obveščamo vse prizadete osebe o odgovornosti naše organizacije v primeru posredovanja osebnih podatkov tretjim osebam.

Za vprašanja prizadetih oseb ali organov za varstvo podatkov smo v tem dokumentu o transparentnosti navedli lokalne predstavnike.

Omogočamo vam izbiro (Opt-out), ali naj se vaši osebni podatki (i) posredujejo tretjim osebam ali (ii) uporabijo za namen, ki se bistveno razlikuje od namena/namenov, za katere so bili prvotno zbrani ali kasneje odobreni z vašim soglasjem. Jasen, dobro viden in lahko dostopen mehanizem za izvajanje vaše izbire je, da kontaktirate našega pooblaščenca za varstvo podatkov (DSB) po e-pošti. Nimate možnosti izbire in nismo dolžni to storiti, če se podatki posredujejo tretji osebi, ki deluje kot zastopnik ali obdelovalec v našem imenu in po naših navodilih. Vendar vedno sklenemo pogodbo s takim zastopnikom ali obdelovalcem.

Za občutljive podatke (tj. osebne podatke, ki vsebujejo informacije o zdravstvenem stanju, rasni ali etnični pripadnosti, političnih mnenjih, verskih ali filozofskih prepričanjih, članstvu v sindikatu ali podatke o spolnem življenju zadevne osebe) pridobimo vaše izrecno soglasje (Opt-in), če naj se ti podatki (i) posredujejo tretjim osebam ali (ii) uporabijo za drug namen, kot za katerega so bili prvotno zbrani ali za katerega ste kasneje dali svoje soglasje, tako da ste izbrali Opt-in. Poleg tega obravnavamo vse osebne podatke, ki jih prejmemo od tretjih oseb, kot občutljive, če jih je tretja oseba označila in obravnavala kot takšne.

Obveščamo vas o zahtevi, da se osebni podatki razkrijejo kot odziv на zakonite zahteve organov, vključno z izpolnjevanjem zahtev nacionalne varnosti ali kazenskega pregona.

Pri prenosu osebnih podatkov tretji osebi, ki deluje kot kontrolor, se držimo Principals obveščanja in izbire. Poleg tega sklenemo pogodbo s tretjo osebo, ki je odgovorna za obdelavo, ki določa, da se ti podatki


© All rights reserved by Heiko Maniero.

smejo obdelovati samo za omejene in določene namene v skladu z vašim soglasjem in da mora prejemnik zagotoviti enako raven zaščite kot Principals DPF in nas obvestiti, če ugotovi, da ne more več izpolnjevati te obveznosti. Pogodba predvideva, da mora tretja oseba, ki je kontrolor, prenehati z obdelavo ali sprejeti druge primerne in ustrezne ukrepe za odpravo težave, če je takšna ugotovitev narejena.

Pri prenosu osebnih podatkov tretji osebi, ki deluje kot zastopnik ali obdelovalec, (i) te podatke prenašamo samo za omejene in določene namene; (ii) zagotavljamo, da je zastopnik ali obdelovalec dolžan zagotoviti vsaj enako raven zaščite, kot jo zahtevajo DPF-Principals; (iii) sprejemamo ustrezne in primerne ukrepe, da zagotovimo, da zastopnik ali obdelovalec dejansko obdeluje prenesene osebne podatke na način, ki je skladen z našimi obveznostmi v skladu z DPF-Principals; (iv) zahtevamo od zastopnika ali obdelovalca, da nas obvesti, če ugotovi, da ne more več zagotavljati enake ravni zaščite, kot jo predvidevajo DPF-Principals; (v) po takšnem obvestilu, tudi pod (iv), sprejemamo ustrezne in primerne ukrepe za ustavitev nepooblaščene obdelave in odpravo težave; in (vi) na zahtevo DPF Department zagotavljamo povzetek ali reprezentativni primer ustreznih določb o varstvu podatkov iz naše pogodbe s tem zastopnikom.

V skladu z EU-U.S. DPF in/ali UK Extension to the EU-U.S. DPF in/ali Swiss-U.S. DPF se naša organizacija zavezuje, da bo sodelovala z organom, ki ga ustanovijo organi EU za varstvo podatkov in britanski Information Commissioner's Office (ICO) oz. Švicarski zvezni pooblaščenec za varstvo podatkov in informacije (EDÖB), in upoštevala njihova priporočila glede nerešenih pritožb o našem ravnanju z osebnimi podatki, ki smo jih prejeli v zvezi z delovnim razmerjem pod sklicevanjem na EU-U.S. DPF in UK Extension to the EU-U.S. DPF in Swiss-U.S. DPF.

Vsi posamezniki, na katere se nanašajo osebni podatki, ki so začasno v Evropski uniji (EU), Evropskem gospodarskem prostoru (EGP) ali Združenem kraljestvu ali imajo tam stalno ali običajno prebivališče, so upravičeni do pravic in pravic posameznikov, na katere se nanašajo osebni podatki, ki so objavljene v našem dokumentu o preglednosti in izhajajo tudi iz členov 15 do 22 SUVP, vključno s pravico do dostopa do osebnih podatkov. Te informacije smo dali na voljo v vseh jezikih EU in EGP. Angleška jezikovna različica velja za Združeno kraljestvo.

Vsi posamezniki, na katere se nanašajo osebni podatki, ki začasno prebivajo v Švici ali imajo tam stalno ali običajno prebivališče, so upravičeni do pravic in pravic posameznikov, na katere se nanašajo osebni podatki, v skladu s švicarskim zakonom o varstvu podatkov (DPA) in švicarsko uredbo o varstvu podatkov (DPR), ki sta objavljena v našem dokumentu o preglednosti, vključno s pravico do dostopa do osebnih podatkov. Te informacije smo zagotovili v treh uradnih jezikih Švice (nemščini, italijanščini in francoščini).


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

# SLOVENIAN: Informacije o obdelavi osebnih podatkov za zaposlene in kandidate (13., 14. člen SUVP)

Spoštovani gospod ali gospa,

Osebni podatki zaposlenih in prosilcev so posebej zaščiteni. Naš cilj je ohraniti visoko raven varstva podatkov. Zato rutinsko razvijamo svoje koncepte varstva in varnosti podatkov.

Seveda upoštevamo zakonske določbe o varstvu podatkov. V skladu s 13. in 14. členom SUVP upravljavci pri obdelavi osebnih podatkov izpolnjujejo posebne zahteve glede informacij. S tem dokumentom so te obveznosti izpolnjene.

Terminologija pravne ureditve je zapletena. Žal se pri pripravi tega dokumenta ni bilo mogoče izogniti uporabi pravnih izrazov. Zato poudarjamo, da se lahko za vsa vprašanja v zvezi s tem dokumentom, uporabljenimi izrazi ali formulacijami vedno obrnete na nas.

## I. Informacije, ki se zagotovijo, kadar se osebni podatki pridobijo od posameznika, na katerega se nanašajo osebni podatki (člen 13 Splošne uredbe o varstvu podatkov)

### A. Identiteto in kontaktne podatke upravljavca in njegovega predstavnika, kadar ta obstaja (člen 13(1)(a) SUVP)

Glej zgoraj.

### B. Kontaktne podatke pooblaščene osebe za varstvo podatkov, kadar ta obstaja (člen 13(1)(b) SUVP)

Glej zgoraj.

### C. Namene, za katere se osebni podatki obdelujejo, kakor tudi pravno podlago za njihovo obdelavo (člen 13(1)(c) SUVP)

Pri podatkih o prosilcih je namen obdelave podatkov preučitev prošnje med postopkom zaposlovanja. V ta namen obdelujemo vse podatke, ki ste nam jih posredovali. Na podlagi podatkov, predloženih med postopkom zaposlovanja, bomo preverili, ali ste povabljeni na razgovor za zaposlitev (del izbirnega postopka). V primeru splošno primernih kandidatov, zlasti v okviru razgovora za službo, obdelujemo


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

nekatere druge vaše osebne podatke, ki so bistveni za našo odločitev o izbiri. Če vas zaposlimo, se podatki kandidata samodejno spremenijo v podatke zaposlenega. V okviru postopka zaposlovanja bomo obdelali tudi druge vaše osebne podatke, ki jih zahtevamo od vas in so potrebni za začetek ali izpolnitev pogodbe (na primer osebne identifikacijske številke ali davčne številke). Pri podatkih zaposlenih je namen obdelave podatkov izpolnjevanje pogodbe o zaposlitvi ali upoštevanje drugih zakonskih določb, ki se uporabljajo za delovno razmerje (npr. davčna zakonodaja), ter uporaba vaših osebnih podatkov za izvajanje pogodbe o zaposlitvi, sklenjene z vami (npr. objava vašega imena in kontaktnih podatkov v podjetju ali za stranke). Podatki o zaposlenih se hranijo tudi po prenehanju delovnega razmerja, da se izpolnijo zakonski roki hrambe.

Pravna podlaga za obdelavo podatkov so člen 6(1)(b) SUVP, člen 9(2)(b) in (h) SUVP, člen 88(1) SUVP in nacionalna zakonodaja, kot je v Nemčiji člen 26 BDSG (zvezni zakon o varstvu podatkov).

## D. Uporabnike ali kategorije uporabnikov osebnih podatkov, če obstajajo (člen 13(1)(e) SUVP)

Javni organi

Zunanji organi

Drugi zunanji organi

Notranja obdelava

Obdelava znotraj skupine

Drugi organi

Seznam naših obdelovalcev in prejemnikov podatkov v tretjih državah ter po potrebi mednarodnih organizacij je objavljen na našem spletnem mestu ali pa ga lahko brezplačno zahtevate od nas. Če želite zahtevati ta seznam, se obrnite na našo pooblaščeno osebo za varstvo podatkov.


© All rights reserved by Heiko Maniero.

## E. Kadar je ustrezno, dejstvo, da upravljavec namerava prenesti osebne podatke v tretjo državo ali mednarodno organizacijo, ter obstoj ali neobstoj sklepa Komisije o ustreznosti ali v primeru prenosov iz člena 46 ali 47 ali drugega pododstavka člena 49(1) sklic na ustrezne ali primerne zaščitne ukrepe in sredstva za pridobitev njihove kopije ali kje so na voljo (člen 13(1)(f), člen 46(1), člen 46(2)(c) SUVP)

Med prejemniki osebnih podatkov so lahko vsa podjetja in podružnice, ki so del naše skupine (v nadaljevanju "podjetja v skupini") in imajo sedež ali pisarno v tretji državi. Seznam vseh družb v skupini ali prejemnikov lahko zahtevate od nas.

V skladu s členom 46(1) SUVP lahko upravljavec ali obdelovalec prenese osebne podatke v tretjo državo le, če je zagotovil ustrezne zaščitne ukrepe in pod pogojem, da so na voljo izvršljive pravice posameznikov, na katere se nanašajo osebni podatki, ter učinkovita pravna sredstva za posameznike, na katere se nanašajo osebni podatki. Ustrezni zaščitni ukrepi se lahko zagotovijo, ne da bi bilo potrebno posebno dovoljenje nadzornega organa, s standardnimi pogodbenimi klavzulami, člen 46(2)(c) SUVP.

Z vsemi prejemniki iz tretjih držav se pred prvim prenosom osebnih podatkov dogovorimo o standardnih pogodbenih klavzulah Evropske unije ali drugih ustreznih zaščitnih ukrepih. Posledično je zagotovljeno, da so posameznikom, na katere se nanašajo osebni podatki, zagotovljeni ustrezni zaščitni ukrepi, izvršljive pravice posameznikov, na katere se nanašajo osebni podatki, in učinkovita pravna sredstva. Vsak posameznik, na katerega se nanašajo osebni podatki, lahko pri nas dobi kopijo standardnih pogodbenih klavzul. Standardne pogodbene klavzule so na voljo tudi v Uradnem listu Evropske unije.

Člen 45(3) Splošne uredbe o varstvu podatkov (GDPR) daje Evropski komisiji pooblastilo, da z izvedbenim aktom odloči, da država, ki ni članica EU, zagotavlja ustrezno raven varstva. To pomeni raven varstva osebnih podatkov, ki je v bistvu enakovredna ravni varstva v EU. Učinek sklepov o ustreznosti je, da se lahko osebni podatki iz EU (ter Norveške, Lihtenštajna in Islandije) prosto in brez dodatnih ovir pretakajo v tretjo državo. Podobna pravila veljajo za Združeno kraljestvo, Švico in nekatere druge države.

Če je Evropska komisija ali vlada druge države odločila, da tretja država zagotavlja ustrezno raven varstva, in je vzpostavljen veljaven okvir (npr. EU-U.S. Data Privacy Framework, Swiss-U.S. Data Privacy Framework, UK Extension to the EU-U.S. Data Privacy Framework), vsi naši prenosi članom teh okvirov (npr. samopotrjenim subjektom) temeljijo izključno na članstvu teh subjektov v zadevnem okviru. Če smo mi ali eno od naših upravičenj v skupini član takega okvira, vsi prenosi nam ali našemu upravičencu v skupini temeljijo izključno na članstvu tega subjekta v takem okviru.

Vsak posameznik, na katerega se nanašajo osebni podatki, lahko pri nas dobi kopijo okvirov. Poleg tega so okviri na voljo tudi v Uradnem listu Evropske unije ali v objavljenem pravnem gradivu ali na spletnih mestih nadzornih organov ali drugih pristojnih organov ali institucij.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## F. Obdobje hrambe osebnih podatkov ali, kadar to ni mogoče, merila, ki se uporabijo za določitev tega obdobja (člen 13(2)(a) SUVP)

Rok hrambe osebnih podatkov prosilcev je 6 mesecev. Za podatke zaposlenih velja ustrezno zakonsko določeno obdobje hrambe. Po izteku tega obdobja se ustrezni podatki rutinsko izbrišejo, če niso več potrebni za izpolnitev pogodbe ali začetek pogodbe.

## G. Obstoj pravice, da se od upravljavca zahtevajo dostop do osebnih podatkov in popravek ali izbris osebnih podatkov ali omejitev obdelave v zvezi s posameznikom, na katerega se nanašajo osebni podatki, ali obstoj pravice do ugovora obdelavi in pravice do prenosljivosti podatkov (člen 13(2)(b) SUVP)

Vsi posamezniki, na katere se nanašajo osebni podatki, imajo naslednje pravice:

***Pravica do dostopa***

Vsak posameznik, na katerega se nanašajo osebni podatki, ima pravico do dostopa do osebnih podatkov, ki se nanašajo nanj. Pravica do dostopa velja za vse podatke, ki jih obdelujemo. Pravico je mogoče uveljavljati enostavno in v razumnih časovnih presledkih, da bi se seznanili z zakonitostjo obdelave in jo preverili (uvodna izjava 63 Splošne uredbe o varstvu podatkov). Ta pravica izhaja iz člena 3(1)(a) Uredbe (ES) št. 15 SPLOŠNE UREDBE O VARSTVU PODATKOV. Posameznik, na katerega se nanašajo osebni podatki, se lahko za uveljavljanje pravice do dostopa obrne na nas.

***Pravica do popravka***

V skladu s členom 16, stavek 1 SUVP ima posameznik, na katerega se nanašajo osebni podatki, pravico, da od upravljavca brez nepotrebnega odlašanja zahteva popravek netočnih osebnih podatkov v zvezi z njim. Poleg tega člen 16, stavek 2 SUVP določa, da ima posameznik, na katerega se nanašajo osebni podatki, ob upoštevanju namenov obdelave pravico do dopolnitve nepopolnih osebnih podatkov, tudi z zagotovitvijo dodatne izjave. Posameznik, na katerega se nanašajo osebni podatki, se lahko za uveljavljanje pravice do popravka obrne na nas.

***Pravica do izbrisa (pravica biti pozabljen)***

Poleg tega imajo posamezniki, na katere se nanašajo osebni podatki, pravico do izbrisa in do pozabe v skladu s čl. 17 SPLOŠNE UREDBE O VARSTVU PODATKOV. To pravico lahko uveljavljate tudi tako, da se obrnete na nas. Na tem mestu pa želimo poudariti, da ta pravica ne velja, če je obdelava potrebna za izpolnitev pravne obveznosti, ki velja za naše podjetje, člen 17(3)(b) SUVP. To pomeni, da lahko zahtevek za izbris odobrimo šele po izteku zakonsko določenega obdobja hrambe.

***Pravica do omejitve obdelave***

V skladu s členom 18 SUVP ima vsak posameznik, na katerega se nanašajo osebni podatki, pravico do omejitve obdelave. Omejitev obdelave se lahko zahteva, če je izpolnjen eden od pogojev iz člena 18(1)(a-d) SUVP. Posameznik, na katerega se nanašajo osebni podatki, se lahko za uveljavljanje pravice do omejitve obdelave obrne na nas.


© All rights reserved by Heiko Maniero.

***Pravica do ugovora***

Poleg tega je člen. 21 Splošne uredbe o varstvu podatkov zagotavlja pravico do ugovora. Posameznik, na katerega se nanašajo osebni podatki, se lahko za uveljavljanje pravice do ugovora obrne na nas.

***Pravica do prenosljivosti podatkov***

Art. 20 Splošne uredbe o varstvu podatkov posamezniku, na katerega se nanašajo osebni podatki, daje pravico do prenosljivosti podatkov. V skladu s to določbo ima posameznik, na katerega se nanašajo osebni podatki, pod pogoji iz člena 20(1)(a) in (b) SUVP pravico prejeti osebne podatke v zvezi z njim, ki jih je posredoval upravljavcu, v strukturirani, splošno uporabljani in strojno berljivi obliki ter pravico, da te podatke posreduje drugemu upravljavcu brez ovir s strani upravljavca, ki so mu bili osebni podatki posredovani. Posameznik, na katerega se nanašajo osebni podatki, se lahko za uveljavljanje pravice do prenosljivosti podatkov obrne na nas.

## H. Kadar obdelava temelji na točki (a) člena 6(1) ali točki (a) člena 9(2), obstoj pravice, da se lahko privolitev kadar koli prekliče, ne da bi to vplivalo na zakonitost obdelave podatkov, ki se je na podlagi privolitve izvajala do njenega preklica 6(1)(a) SUVP ali členu 9(2)(a) SUVP (člen 13(2)(c) SUVP)

Če obdelava osebnih podatkov temelji na členu. a, kar je v primeru, če je posameznik, na katerega se nanašajo osebni podatki, privolil v obdelavo osebnih podatkov za enega ali več posebnih namenov, ali če temelji na členu 9(2)(a) SUVP, ki ureja izrecno privolitev v obdelavo posebnih vrst osebnih podatkov, ima posameznik, na katerega se nanašajo osebni podatki, v skladu s členom 7(3), stavek 1 SUVP pravico kadar koli preklicati svojo privolitev.

Preklic privolitve ne vpliva na zakonitost obdelave na podlagi privolitve pred njenim preklicem, člen 7(3), stavek 2 SUVP. Preklic soglasja mora biti enako enostaven kot dajanje soglasja, čl. 7(3), stavek 4 Splošne uredbe o varstvu podatkov. Zato se lahko preklic privolitve vedno izvede na enak način, kot je bila dana privolitev, ali na kateri koli drug način, ki se posamezniku, na katerega se nanašajo osebni podatki, zdi enostavnejši. V današnji informacijski družbi je verjetno najpreprostejši način preklica privolitve preprosto elektronsko sporočilo. Če želi posameznik, na katerega se nanašajo osebni podatki, preklicati soglasje, ki nam ga je dal, zadostuje, da nam pošlje preprosto elektronsko sporočilo. Posameznik, na katerega se nanašajo osebni podatki, lahko izbere tudi kateri koli drug način, da nam sporoči svoj preklic privolitve.

## I. Pravico do vložitve pritožbe pri nadzornem organu (člen 13(2)(d), 77(1) SUVP)

Kot upravljavec moramo posameznika, na katerega se nanašajo osebni podatki, obvestiti o pravici do vložitve pritožbe pri nadzornem organu, člen 13(2)(d) SUVP. Pravico do vložitve pritožbe pri nadzornem organu ureja člen 77(1) SUVP. V skladu s to določbo ima vsak posameznik, na katerega se nanašajo osebni podatki, brez poseganja v katero koli drugo upravno ali sodno pravno sredstvo pravico vložiti


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

pritožbo pri nadzornem organu, zlasti v državi članici svojega običajnega prebivališča, kraja dela ali kraja domnevne kršitve, če meni, da obdelava osebnih podatkov v zvezi z njim krši Splošno uredbo o varstvu podatkov. Pravica do vložitve pritožbe pri nadzornem organu je bila s pravom Unije omejena le tako, da jo je mogoče uveljavljati le pri enem nadzornem organu (uvodna izjava 141, stavek 1 Splošne uredbe o varstvu podatkov). Namen tega pravila je preprečiti dvojne pritožbe istega posameznika, na katerega se nanašajo osebni podatki, v isti zadevi. Če želi posameznik, na katerega se nanašajo osebni podatki, vložiti pritožbo zoper nas, smo ga zato pozvali, naj se obrne le na en nadzorni organ.

## J. Ali je zagotovitev osebnih podatkov statutarna ali pogodbena obveznost ali pa obveznost, ki je potrebna za sklenitev pogodbe, ter ali mora posameznik, na katerega se nanašajo osebni podatki, zagotoviti osebne podatke ter kakšne so morebitne posledice, če se taki podatki ne zagotovijo, in (člen 13(2)(e) SUVP)

Pojasnjujemo, da je posredovanje osebnih podatkov delno zahtevano z zakonom (npr. davčni predpisi), lahko pa izhaja tudi iz pogodbenih določb (npr. informacije o pogodbenem partnerju).

Včasih je za sklenitev pogodbe potrebno, da nam posameznik, na katerega se nanašajo osebni podatki, posreduje osebne podatke, ki jih moramo nato obdelati. Posameznik, na katerega se nanašajo osebni podatki, nam mora na primer posredovati osebne podatke, ko naše podjetje z njim podpiše pogodbo. Neposredovanje osebnih podatkov bi imelo za posledico, da pogodbe s posameznikom, na katerega se nanašajo osebni podatki, ne bi bilo mogoče skleniti.

Preden posameznik, na katerega se nanašajo osebni podatki, posreduje osebne podatke, se mora obrniti na nas. Posamezniku, na katerega se nanašajo osebni podatki, pojasnimo, ali je posredovanje osebnih podatkov zahtevano z zakonom ali pogodbo ali je potrebno za sklenitev pogodbe, ali obstaja obveznost posredovanja osebnih podatkov in kakšne so posledice, če osebnih podatkov ne posreduje.

## K. Obstoj avtomatiziranega sprejemanja odločitev, vključno z oblikovanjem profilov iz člena 22(1) in (4), ter vsaj v takih primerih smiselne informacije o razlogih zanj, kot tudi pomen in predvidene posledice take obdelave za posameznika, na katerega se nanašajo osebni podatki (člen 13(2)(f) SUVP).

Kot odgovorno podjetje običajno ne uporabljamo avtomatiziranega odločanja ali profiliranja. Če v izjemnih primerih izvajamo avtomatizirano odločanje ali profiliranje, bomo posameznika, na katerega se nanašajo osebni podatki, o tem obvestili ločeno ali prek pododdelka v naši politiki zasebnosti (na naši spletni strani). V tem primeru velja naslednje:

Avtomatizirano sprejemanje odločitev - vključno z oblikovanjem profilov - se lahko izvede, če (1) je to potrebno za sklenitev ali izvajanje pogodbe med posameznikom, na katerega se nanašajo osebni podatki, in nami, ali (2) je to dovoljeno z zakonodajo Unije ali države članice, ki velja za nas in ki določa


© All rights reserved by Heiko Maniero.

tudi ustrezne ukrepe za zaščito pravic in svoboščin ter zakonitih interesov posameznika, na katerega se nanašajo osebni podatki, ali (3) to temelji na izrecni privolitvi posameznika, na katerega se nanašajo osebni podatki.

V primerih iz člena 22(2)(a) in (c) GDPR izvedemo ustrezne ukrepe za zaščito pravic in svoboščin ter zakonitih interesov posameznika, na katerega se nanašajo osebni podatki. V teh primerih imate pravico do človeškega posredovanja s strani upravljavca, da izrazite svoje stališče in izpodbijate odločitev.

Smiselne informacije o vključeni logiki ter pomenu in predvidenih posledicah takšne obdelave za posameznika, na katerega se nanašajo osebni podatki, so navedene v naši politiki zasebnosti.

## II. Informacije, ki jih je treba zagotoviti, kadar osebni podatki niso bili pridobljeni od posameznika, na katerega se ti nanašajo (člen 14 Splošne uredbe o varstvu podatkov)

### A. Istovetnost in kontaktne podatke upravljavca in njegovega predstavnika, kadar ta obstaja (člen 14(1)(a) SUVP)

Glej zgoraj.

### B. Kontaktne podatke pooblaščene osebe za varstvo podatkov, kadar ta obstaja (člen 14(1)(b) SUVP)

Glej zgoraj.

### C. Namene, za katere se osebni podatki obdelujejo, kakor tudi pravno podlago za njihovo obdelavo (člen 14(1)(c) SUVP)

Pri podatkih o prosilcu, ki jih posameznik, na katerega se nanašajo osebni podatki, ni zbral, je namen obdelave podatkov preučitev prošnje med postopkom zaposlovanja. V ta namen lahko obdelujemo podatke, ki niso zbrani od vas. Na podlagi podatkov, obdelanih med postopkom zaposlovanja, bomo preverili, ali ste povabljeni na razgovor za zaposlitev (del izbirnega postopka). Če vas bomo zaposlili, se bodo podatki kandidata samodejno pretvorili v podatke zaposlenega. Pri podatkih zaposlenih je namen obdelave podatkov izvajanje pogodbe o zaposlitvi ali spoštovanje drugih zakonskih določb, ki veljajo za delovno razmerje. Podatki o zaposlenih se hranijo po prenehanju delovnega razmerja, da se izpolnijo zakonski roki hrambe.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

Pravna podlaga za obdelavo podatkov je člen 6(1)(b) in (f) SUVP, člen 9(2)(b) in (h) SUVP, člen 88(1) SUVP in nacionalna zakonodaja, kot je v Nemčiji člen 26 BDSG (zvezni zakon o varstvu podatkov).

## D. Vrste zadevnih osebnih podatkov (člen 14(1)(d) SUVP)

Podatki vlagatelja

Podatki o zaposlenih

## E. Uporabnike ali kategorije uporabnikov osebnih podatkov, kadar obstajajo (člen 14(1)(e) SUVP)

Javni organi

Zunanji organi

Drugi zunanji organi

Notranja obdelava

Obdelava znotraj skupine

Drugi organi

Seznam naših obdelovalcev in prejemnikov podatkov v tretjih državah ter po potrebi mednarodnih organizacij je objavljen na našem spletnem mestu ali pa ga lahko brezplačno zahtevate od nas. Če želite zahtevati ta seznam, se obrnite na našo pooblaščeno osebo za varstvo podatkov.

## F. Kadar je ustrezno, informacije o tem, da namerava upravljavec prenesti osebne podatke uporabniku v tretji državi ali mednarodni organizaciji, ter o obstoju ali neobstoju sklepa Komisije o ustreznosti ali v primeru prenosov iz člena 46 ali 47 ali drugega pododstavka člena 49(1) sklic na ustrezne ali primerne zaščitne ukrepe in sredstva za pridobitev njihove kopije ali kje so na voljo (člen 14(1)(f), člen 46(1), člen 46(2)(c) SUVP)

Med prejemniki osebnih podatkov so lahko vsa podjetja in podružnice, ki so del naše skupine (v nadaljevanju "podjetja v skupini") in imajo sedež ali poslovalnico v tretji državi. Seznam vseh družb v skupini ali prejemnikov lahko zahtevate od nas.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

V skladu s členom 46(1) SUVP lahko upravljavec ali obdelovalec prenese osebne podatke v tretjo državo le, če je zagotovil ustrezne zaščitne ukrepe in pod pogojem, da so na voljo izvršljive pravice posameznikov, na katere se nanašajo osebni podatki, ter učinkovita pravna sredstva za posameznike, na katere se nanašajo osebni podatki. Ustrezni zaščitni ukrepi se lahko zagotovijo, ne da bi bilo potrebno posebno dovoljenje nadzornega organa, s standardnimi klavzulami o varstvu podatkov, člen 46(2)(c) SUVP.

Z vsemi prejemniki iz tretjih držav se pred prvim prenosom osebnih podatkov dogovorimo o standardnih pogodbenih klavzulah Evropske unije ali drugih ustreznih zaščitnih ukrepih. Posledično je zagotovljeno, da so posameznikom, na katere se nanašajo osebni podatki, zagotovljeni ustrezni zaščitni ukrepi, izvršljive pravice posameznikov, na katere se nanašajo osebni podatki, in učinkovita pravna sredstva. Vsak posameznik, na katerega se nanašajo osebni podatki, lahko pri nas dobi kopijo standardnih pogodbenih klavzul. Standardne pogodbene klavzule so na voljo tudi v Uradnem listu Evropske unije.

Člen 45(3) Splošne uredbe o varstvu podatkov (GDPR) daje Evropski komisiji pooblastilo, da z izvedbenim aktom odloči, da država, ki ni članica EU, zagotavlja ustrezno raven varstva. To pomeni raven varstva osebnih podatkov, ki je v bistvu enakovredna ravni varstva v EU. Učinek sklepov o ustreznosti je, da se lahko osebni podatki iz EU (ter Norveške, Lihtenštajna in Islandije) prosto in brez dodatnih ovir pretakajo v tretjo državo. Podobna pravila veljajo za Združeno kraljestvo, Švico in nekatere druge države.

Če je Evropska komisija ali vlada druge države odločila, da tretja država zagotavlja ustrezno raven varstva, in je vzpostavljen veljaven okvir (npr. EU-U.S. Data Privacy Framework, Swiss-U.S. Data Privacy Framework, UK Extension to the EU-U.S. Data Privacy Framework), vsi naši prenosi članom teh okvirov (npr. samopotrjenim subjektom) temeljijo izključno na članstvu teh subjektov v zadevnem okviru. Če smo mi ali eno od naših upravičenj v skupini član takega okvira, vsi prenosi nam ali našemu upravičencu v skupini temeljijo izključno na članstvu tega subjekta v takem okviru.

Vsak posameznik, na katerega se nanašajo osebni podatki, lahko pri nas dobi kopijo okvirov. Poleg tega so okviri na voljo tudi v Uradnem listu Evropske unije ali v objavljenem pravnem gradivu ali na spletnih mestih nadzornih organov ali drugih pristojnih organov ali institucij.

## G. Obdobje hrambe osebnih podatkov ali, če to ni mogoče, merila, ki se uporabijo za določitev tega obdobja (člen 14(2)(a) SUVP)

Rok hrambe osebnih podatkov prosilcev je 6 mesecev. Za podatke zaposlenih velja ustrezno zakonsko določeno obdobje hrambe. Po izteku tega obdobja se ustrezni podatki rutinsko izbrišejo, če niso več potrebni za izpolnitev pogodbe ali začetek pogodbe.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## H. Kadar obdelava temelji na točki (f) člena 6(1), zakonite interese, za uveljavljanje katerih si prizadeva upravljavec ali tretja oseba (člen 14(2)(b) SUVP)

V skladu s členom 6(1)(f) SUVP je obdelava zakonita le, če je obdelava potrebna za namene zakonitih interesov, za katere si prizadeva upravljavec ali tretja oseba, razen če nad takimi interesi prevladajo interesi ali temeljne pravice in svoboščine posameznika, na katerega se nanašajo osebni podatki, ki zahtevajo varstvo osebnih podatkov. V skladu z uvodno izjavo 47, drugi stavek, Splošne uredbe o varstvu podatkov bi lahko zakoniti interes obstajal, kadar obstaja ustrezno in primerno razmerje med posameznikom, na katerega se nanašajo osebni podatki, in upravljavcem, npr. v primerih, ko je posameznik, na katerega se nanašajo osebni podatki, stranka upravljavca. V vseh primerih, v katerih naše podjetje obdeluje podatke kandidatov na podlagi člena 6(1)(f) SUVP, je naš zakoniti interes zaposlitev ustreznega osebja in strokovnjakov.

## I. Obstoj pravice, da se od upravljavca zahtevajo dostop do osebnih podatkov in popravek ali izbris osebnih podatkov ali omejitev obdelave v zvezi s posameznikom, na katerega se nanašajo osebni podatki, in obstoj pravice do ugovora obdelavi ter pravice do prenosljivosti podatkov (člen 14(2)(c) SUVP)

Vsi posamezniki, na katere se nanašajo osebni podatki, imajo naslednje pravice:

***Pravica do dostopa***

Vsak posameznik, na katerega se nanašajo osebni podatki, ima pravico do dostopa do osebnih podatkov, ki se nanašajo nanj. Pravica do dostopa velja za vse podatke, ki jih obdelujemo. Pravico je mogoče uveljavljati enostavno in v razumnih časovnih presledkih, da bi se seznanili z zakonitostjo obdelave in jo preverili (uvodna izjava 63 Splošne uredbe o varstvu podatkov). Ta pravica izhaja iz člena 3(1)(a) Uredbe (ES) št. 15 SPLOŠNE UREDBE O VARSTVU PODATKOV. Posameznik, na katerega se nanašajo osebni podatki, se lahko za uveljavljanje pravice do dostopa obrne na nas.

***Pravica do popravka***

V skladu s členom 16, stavek 1 SUVP ima posameznik, na katerega se nanašajo osebni podatki, pravico, da od upravljavca brez nepotrebnega odlašanja zahteva popravek netočnih osebnih podatkov v zvezi z njim. Poleg tega člen 16, stavek 2 SUVP določa, da ima posameznik, na katerega se nanašajo osebni podatki, ob upoštevanju namenov obdelave pravico do dopolnitve nepopolnih osebnih podatkov, tudi z zagotovitvijo dodatne izjave. Posameznik, na katerega se nanašajo osebni podatki, se lahko za uveljavljanje pravice do popravka obrne na nas.

***Pravica do izbrisa (pravica biti pozabljen)***

Poleg tega imajo posamezniki, na katere se nanašajo osebni podatki, pravico do izbrisa in do pozabe v skladu s čl. 17 SPLOŠNE UREDBE O VARSTVU PODATKOV. To pravico lahko uveljavljate tudi tako, da nas kontaktirate. Na tem mestu pa želimo poudariti, da ta pravica ne velja, če je obdelava potrebna


© All rights reserved by Heiko Maniero.

za izpolnitev pravne obveznosti, ki velja za naše podjetje, člen 17(3)(b) SUVP. To pomeni, da lahko zahtevek za izbris odobrimo šele po izteku zakonsko določenega obdobja hrambe.

***Pravica do omejitve obdelave***

V skladu s členom 18 SUVP ima vsak posameznik, na katerega se nanašajo osebni podatki, pravico do omejitve obdelave. Omejitev obdelave se lahko zahteva, če je izpolnjen eden od pogojev iz člena 18(1)(a-d) SUVP. Posameznik, na katerega se nanašajo osebni podatki, se lahko za uveljavljanje pravice do omejitve obdelave obrne na nas.

***Pravica do ugovora***

Poleg tega je člen. 21 Splošne uredbe o varstvu podatkov zagotavlja pravico do ugovora. Posameznik, na katerega se nanašajo osebni podatki, se lahko za uveljavljanje pravice do ugovora obrne na nas.

***Pravica do prenosljivosti podatkov***

Čl. 20 Splošne uredbe o varstvu podatkov posamezniku, na katerega se nanašajo osebni podatki, daje pravico do prenosljivosti podatkov. V skladu s to določbo ima posameznik, na katerega se nanašajo osebni podatki, pod pogoji iz člena 20(1)(a) in (b) SUVP pravico prejeti osebne podatke v zvezi z njim, ki jih je posredoval upravljavcu, v strukturirani, splošno uporabljani in strojno berljivi obliki ter pravico, da te podatke posreduje drugemu upravljavcu brez ovir s strani upravljavca, ki so mu bili osebni podatki posredovani. Posameznik, na katerega se nanašajo osebni podatki, se lahko za uveljavljanje pravice do prenosljivosti podatkov obrne na nas.

## J. Kadar obdelava temelji na točki (a) člena 6(1) ali točki (a) člena 9(2), obstoj pravice, da se lahko privolitev kadar koli prekliče, ne da bi to vplivalo na zakonitost obdelave podatkov, ki se je na podlagi privolitve izvajala do njenega preklica (člen 14(2)(d) SUVP)

Če obdelava osebnih podatkov temelji na členu. a, kar je v primeru, če je posameznik, na katerega se nanašajo osebni podatki, privolil v obdelavo osebnih podatkov za enega ali več posebnih namenov, ali če temelji na členu 9(2)(a) SUVP, ki ureja izrecno privolitev v obdelavo posebnih vrst osebnih podatkov, ima posameznik, na katerega se nanašajo osebni podatki, v skladu s členom 7(3), stavek 1 SUVP pravico kadar koli preklicati svojo privolitev.

Preklic privolitve ne vpliva na zakonitost obdelave na podlagi privolitve pred njenim preklicem, člen 7(3), stavek 2 SUVP. Preklic soglasja mora biti enako enostaven kot dajanje soglasja, čl. 7(3), stavek 4 Splošne uredbe o varstvu podatkov. Zato se lahko preklic privolitve vedno izvede na enak način, kot je bila dana privolitev, ali na kateri koli drug način, ki se posamezniku, na katerega se nanašajo osebni podatki, zdi enostavnejši. V današnji informacijski družbi je verjetno najpreprostejši način preklica privolitve preprosto elektronsko sporočilo. Če želi posameznik, na katerega se nanašajo osebni podatki, preklicati soglasje, ki nam ga je dal, zadostuje, da nam pošlje preprosto elektronsko sporočilo.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

Posameznik, na katerega se nanašajo osebni podatki, lahko izbere tudi kateri koli drug način, da nam sporoči svoj preklic privolitve.

## K. Pravico do vložitve pritožbe pri nadzornem organu (člen 14(2)(e), 77(1) SUVP)

Kot upravljavec moramo posameznika, na katerega se nanašajo osebni podatki, obvestiti o pravici do vložitve pritožbe pri nadzornem organu, člen 14(2)(e) SUVP. Pravico do vložitve pritožbe pri nadzornem organu ureja člen 77(1) SUVP. V skladu s to določbo ima vsak posameznik, na katerega se nanašajo osebni podatki, brez poseganja v katero koli drugo upravno ali sodno pravno sredstvo pravico vložiti pritožbo pri nadzornem organu, zlasti v državi članici svojega običajnega prebivališča, kraja dela ali kraja domnevne kršitve, če meni, da obdelava osebnih podatkov v zvezi z njim krši Splošno uredbo o varstvu podatkov. Pravica do vložitve pritožbe pri nadzornem organu je bila s pravom Unije omejena le tako, da jo je mogoče uveljavljati le pri enem nadzornem organu (uvodna izjava 141, stavek 1 Splošne uredbe o varstvu podatkov). Namen tega pravila je preprečiti dvojne pritožbe istega posameznika, na katerega se nanašajo osebni podatki, v isti zadevi. Če želi posameznik, na katerega se nanašajo osebni podatki, vložiti pritožbo zoper nas, smo ga zato prosili, naj se obrne samo na en nadzorni organ.

## L. Od kje izvirajo osebni podatki in po potrebi, ali izvirajo iz javno dostopnih virov, in (člen 14(2)(f) Splošne uredbe o varstvu podatkov)

Načeloma se osebni podatki zbirajo neposredno od posameznika, na katerega se nanašajo, ali v sodelovanju z organom (npr. pridobivanje podatkov iz uradnega registra). Drugi podatki o posameznikih, na katere se nanašajo osebni podatki, se pridobijo s prenosi podjetij v skupini. V okviru teh splošnih informacij navajanje natančnih virov, iz katerih izvirajo osebni podatki, ni mogoče ali pa bi zahtevalo nesorazmeren napor v smislu člena 3(1)(2)(a) Direktive 95/46/ES. 14(5)(b) Splošne uredbe o varstvu podatkov. Načeloma osebnih podatkov ne zbiramo iz javno dostopnih virov.

Vsak posameznik, na katerega se nanašajo osebni podatki, se lahko kadar koli obrne na nas in pridobi podrobnejše informacije o natančnih virih osebnih podatkov, ki se nanašajo nanj. Kadar posamezniku, na katerega se nanašajo osebni podatki, ni mogoče zagotoviti izvora osebnih podatkov, ker so bili uporabljeni različni viri, je treba zagotoviti splošne informacije (uvodna izjava 61, stavek 4 Splošne uredbe o varstvu podatkov).


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## M. Obstoj avtomatiziranega sprejemanja odločitev, vključno z oblikovanjem profilov iz člena 22(1) in (4), ter vsaj v takih primerih smiselne informacije o razlogih zanj, kot tudi pomen in predvidene posledice take obdelave za posameznika, na katerega se nanašajo osebni podatki (člen 14(2)(g) SUVP)

Kot odgovorno podjetje običajno ne uporabljamo avtomatiziranega odločanja ali profiliranja. Če v izjemnih primerih izvajamo avtomatizirano odločanje ali profiliranje, bomo posameznika, na katerega se nanašajo osebni podatki, o tem obvestili ločeno ali prek pododdelka v naši politiki zasebnosti (na naši spletni strani). V tem primeru velja naslednje:

Avtomatizirano sprejemanje odločitev - vključno z oblikovanjem profilov - se lahko izvede, če (1) je to potrebno za sklenitev ali izvajanje pogodbe med posameznikom, na katerega se nanašajo osebni podatki, in nami, ali (2) je to dovoljeno z zakonodajo Unije ali države članice, ki velja za nas in ki določa tudi ustrezne ukrepe za zaščito pravic in svoboščin ter zakonitih interesov posameznika, na katerega se nanašajo osebni podatki, ali (3) to temelji na izrecni privolitvi posameznika, na katerega se nanašajo osebni podatki.

V primerih iz člena 22(2)(a) in (c) GDPR izvedemo ustrezne ukrepe za zaščito pravic in svoboščin ter zakonitih interesov posameznika, na katerega se nanašajo osebni podatki. V teh primerih imate pravico do človeškega posredovanja s strani upravljavca, da izrazite svoje stališče in izpodbijate odločitev.

Smiselne informacije o vključeni logiki ter pomenu in predvidenih posledicah takšne obdelave za posameznika, na katerega se nanašajo osebni podatki, so navedene v naši politiki zasebnosti.

# III. EU-U.S. Data Privacy Framework (EU-U.S. DPF), UK Extension to the EU-U.S. DPF, Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF)

Če je naša organizacija certificirani član EU-U.S. Data Privacy Framework (EU-U.S. DPF) in/ali UK Extension to the EU-U.S. DPF in/ali Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF), velja naslednje:

Držimo se EU-U.S. Data Privacy Framework (EU-U.S. DPF) in UK Extension to the EU-U.S. DPF ter Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF), kot je določilo U.S. Department of Commerce. Naše podjetje je ameriškemu ministrstvu za trgovino potrdilo, da spoštuje EU-U.S. Data Privacy Framework Principles (EU-U.S. DPF Principles) v zvezi z obdelavo osebnih podatkov, ki jih prejema iz Evropske unije in Združenega kraljestva v skladu z EU-U.S. DPF in UK Extension to the EU-U.S. DPF. Naše podjetje je ameriškemu ministrstvu za trgovino potrdilo, da spoštuje Swiss-U.S. Data Privacy Framework Principles (Swiss-U.S. DPF Principles) v zvezi z obdelavo osebnih podatkov, ki jih prejema iz Švice v skladu s Swiss-U.S. DPF. V primeru nasprotja med določili naše politike zasebnosti in EU-U.S. DPF Principles in/ali Swiss-U.S. DPF Principles prevladujejo Principles.


© All rights reserved by Heiko Maniero.

Za več informacij o programu Data Privacy Framework (DPF) in ogled našega certifikata obiščite https://www.dataprivacyframework.gov/.

Druge ameriške enote ali hčerinske družbe našega podjetja, ki prav tako spoštujejo EU-U.S. DPF Principals, vključno z UK Extension to the EU-U.S. DPF in Swiss-U.S. DPF Principals, če obstajajo, so navedene v naši politiki zasebnosti.

V skladu z EU-U.S. DPF in UK Extension to the EU-U.S. DPF ter Swiss-U.S. DPF se naše podjetje zavezuje, da bo sodelovalo z organom, ki ga ustanovijo evropski organi za varstvo podatkov in britanski Information Commissioner's Office (ICO) ter Švicarski zvezni pooblaščenec za varstvo podatkov in za informacije (EDÖB), ter upoštevalo njihova priporočila glede nerešenih pritožb o našem ravnanju z osebnimi podatki, ki jih prejmemo na podlagi EU-U.S. DPF in UK Extension to the EU-U.S. DPF in Swiss-U.S. DPF.

Obveščamo prizadete osebe o pristojnih evropskih organih za varstvo podatkov, ki so odgovorni za obravnavanje pritožb o ravnanju naše organizacije z osebnimi podatki, na zgornjem delu tega dokumenta o transparentnosti in o tem, da prizadetim osebam nudimo ustrezno in brezplačno pravno sredstvo.

Vse prizadete osebe obveščamo, da je naše podjetje podrejeno preiskovalnim in izvršilnim pristojnostim Federal Trade Commission (FTC).

Prizadete osebe imajo pod določenimi pogoji možnost zahtevati zavezujočo arbitražo. Naša organizacija je dolžna reševati zahtevke in upoštevati pogoje v skladu z Dodatkom I k DPF-Principals, če prizadeta oseba zahteva zavezujočo arbitražo tako, da obvesti našo organizacijo in so upoštevani postopki in pogoji v skladu z Dodatkom I k Principals.

S tem obveščamo vse prizadete osebe o odgovornosti naše organizacije v primeru posredovanja osebnih podatkov tretjim osebam.

Za vprašanja prizadetih oseb ali organov za varstvo podatkov smo v tem dokumentu o transparentnosti navedli lokalne predstavnike.

Omogočamo vam izbiro (Opt-out), ali naj se vaši osebni podatki (i) posredujejo tretjim osebam ali (ii) uporabijo za namen, ki se bistveno razlikuje od namena/namenov, za katere so bili prvotno zbrani ali kasneje odobreni z vašim soglasjem. Jasen, dobro viden in lahko dostopen mehanizem za izvajanje vaše izbire je, da kontaktirate našega pooblaščenca za varstvo podatkov (DSB) po e-pošti. Nimate možnosti izbire in nismo dolžni to storiti, če se podatki posredujejo tretji osebi, ki deluje kot zastopnik ali obdelovalec v našem imenu in po naših navodilih. Vendar vedno sklenemo pogodbo s takim zastopnikom ali obdelovalcem.

Za občutljive podatke (tj. osebne podatke, ki vsebujejo informacije o zdravstvenem stanju, rasni ali etnični pripadnosti, političnih mnenjih, verskih ali filozofskih prepričanjih, članstvu v sindikatu ali podatke o spolnem življenju zadevne osebe) pridobimo vaše izrecno soglasje (Opt-in), če naj se ti podatki (i) posredujejo tretjim osebam ali (ii) uporabijo za drug namen, kot za katerega so bili prvotno zbrani ali za


© All rights reserved by Heiko Maniero.

katerega ste kasneje dali svoje soglasje, tako da ste izbrali Opt-in. Poleg tega obravnavamo vse osebne podatke, ki jih prejmemo od tretjih oseb, kot občutljive, če jih je tretja oseba označila in obravnavala kot takšne.

Obveščamo vas o zahtevi, da se osebni podatki razkrijejo kot odziv на zakonite zahteve organov, vključno z izpolnjevanjem zahtev nacionalne varnosti ali kazenskega pregona.

Pri prenosu osebnih podatkov tretji osebi, ki deluje kot kontrolor, se držimo Principals obveščanja in izbire. Poleg tega sklenemo pogodbo s tretjo osebo, ki je odgovorna za obdelavo, ki določa, da se ti podatki smejo obdelovati samo za omejene in določene namene v skladu z vašim soglasjem in da mora prejemnik zagotoviti enako raven zaščite kot Principals DPF in nas obvestiti, če ugotovi, da ne more več izpolnjevati te obveznosti. Pogodba predvideva, da mora tretja oseba, ki je kontrolor, prenehati z obdelavo ali sprejeti druge primerne in ustrezne ukrepe za odpravo težave, če je takšna ugotovitev narejena.

Pri prenosu osebnih podatkov tretji osebi, ki deluje kot zastopnik ali obdelovalec, (i) te podatke prenašamo samo za omejene in določene namene; (ii) zagotavljamo, da je zastopnik ali obdelovalec dolžan zagotoviti vsaj enako raven zaščite, kot jo zahtevajo DPF-Principals; (iii) sprejemamo ustrezne in primerne ukrepe, da zagotovimo, da zastopnik ali obdelovalec dejansko obdeluje prenesene osebne podatke na način, ki je skladen z našimi obveznostmi v skladu z DPF-Principals; (iv) zahtevamo od zastopnika ali obdelovalca, da nas obvesti, če ugotovi, da ne more več zagotavljati enake ravni zaščite, kot jo predvidevajo DPF-Principals; (v) po takšnem obvestilu, tudi pod (iv), sprejemamo ustrezne in primerne ukrepe za ustavitev nepooblaščene obdelave in odpravo težave; in (vi) na zahtevo DPF Department zagotavljamo povzetek ali reprezentativni primer ustreznih določb o varstvu podatkov iz naše pogodbe s tem zastopnikom.

V skladu z EU-U.S. DPF in/ali UK Extension to the EU-U.S. DPF in/ali Swiss-U.S. DPF se naša organizacija zavezuje, da bo sodelovala z organom, ki ga ustanovijo organi EU za varstvo podatkov in britanski Information Commissioner's Office (ICO) oz. Švicarski zvezni pooblaščenec za varstvo podatkov in informacije (EDÖB), in upoštevala njihova priporočila glede nerešenih pritožb o našem ravnanju z osebnimi podatki, ki smo jih prejeli v zvezi z delovnim razmerjem pod sklicevanjem na EU-U.S. DPF in UK Extension to the EU-U.S. DPF in Swiss-U.S. DPF.

Vsi posamezniki, na katere se nanašajo osebni podatki, ki so začasno v Evropski uniji (EU), Evropskem gospodarskem prostoru (EGP) ali Združenem kraljestvu ali imajo tam stalno ali običajno prebivališče, so upravičeni do pravic in pravic posameznikov, na katere se nanašajo osebni podatki, ki so objavljene v našem dokumentu o preglednosti in izhajajo tudi iz členov 15 do 22 SUVP, vključno s pravico do dostopa do osebnih podatkov. Te informacije smo dali na voljo v vseh jezikih EU in EGP. Angleška jezikovna različica velja za Združeno kraljestvo.

Vsi posamezniki, na katere se nanašajo osebni podatki, ki začasno prebivajo v Švici ali imajo tam stalno ali običajno prebivališče, so upravičeni do pravic in pravic posameznikov, na katere se nanašajo osebni podatki, v skladu s švicarskim zakonom o varstvu podatkov (DPA) in švicarsko uredbo o varstvu podatkov


© All rights reserved by Heiko Maniero.

(DPR), ki sta objavljena v našem dokumentu o preglednosti, vključno s pravico do dostopa do osebnih podatkov. Te informacije smo zagotovili v treh uradnih jezikih Švice (nemščini, italijanščini in francoščini).


© All rights reserved by Heiko Maniero.

# SLOVAK: Informácie o spracovaní osobných údajov (článok 13, 14 GDPR)

Vážený pán alebo pani,

Osobné údaje každej osoby, ktorá je v zmluvnom, predzmluvnom alebo inom vzťahu s našou spoločnosťou, si zaslúžia osobitnú ochranu. Naším cieľom je udržiavať úroveň ochrany údajov na vysokej úrovni. Preto bežne rozvíjame naše koncepcie ochrany a bezpečnosti údajov.

Samozrejme, dodržiavame zákonné ustanovenia o ochrane údajov. Podľa článkov 13, 14 GDPR prevádzkovatelia pri zhromažďovaní osobných údajov spĺňajú osobitné informačné požiadavky. Tento dokument tieto povinnosti spĺňa.

Terminológia právnych predpisov je zložitá. Žiaľ, pri príprave tohto dokumentu nebolo možné upustiť od používania právnych termínov. Preto by sme vás radi upozornili, že v prípade akýchkoľvek otázok týkajúcich sa tohto dokumentu, použitých termínov alebo formulácií sa na nás môžete kedykoľvek obrátiť.

## I. Informácie, ktoré sa majú poskytovať pri získavaní osobných údajov od dotknutej osoby (článok 13 GDPR)

### A. Totožnosť a kontaktné údaje prevádzkovateľa a v príslušných prípadoch zástupcu prevádzkovateľa (článok 13 ods. 1 písm. a) GDPR)

Pozri vyššie

### B. Kontaktné údaje prípadnej zodpovednej osoby (článok 13 ods. 1 písm. b) GDPR)

Pozri vyššie

### C. Účely spracúvania, na ktoré sú osobné údaje určené, ako aj právny základ spracúvania (článok 13 ods. 1 písm. c) GDPR)

Účelom spracúvania osobných údajov je vybavovanie všetkých operácií, ktoré sa týkajú prevádzkovateľa, zákazníkov, potenciálnych zákazníkov, obchodných partnerov alebo iných zmluvných alebo predzmluvných vzťahov medzi uvedenými skupinami (v najširšom zmysle) alebo právnych povinností prevádzkovateľa.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

Čl. 6 ods. 1 písm. a) GDPR slúži ako právny základ pre spracovateľské operácie, na ktoré získavame súhlas na konkrétny účel spracovania. Ak je spracúvanie osobných údajov nevyhnutné na plnenie zmluvy, ktorej zmluvnou stranou je dotknutá osoba, ako je to napríklad v prípade, keď sú spracovateľské operácie potrebné na dodanie tovaru alebo poskytnutie inej služby, spracúvanie je založené na článku 6 ods. 1 písm. b) GDPR. To isté platí pre také operácie spracovania, ktoré sú potrebné na vykonanie opatrení pred uzavretím zmluvy, napríklad v prípade dopytov týkajúcich sa našich produktov alebo služieb. Podlieha naša spoločnosť zákonnej povinnosti, na základe ktorej sa vyžaduje spracovanie osobných údajov, napríklad na plnenie daňových povinností, spracovanie je založené na čl. 6 ods. 1 písm. c GDPR.

V ojedinelých prípadoch môže byť spracovanie osobných údajov nevyhnutné na ochranu životne dôležitých záujmov dotknutej osoby alebo inej fyzickej osoby. Išlo by napríklad o prípad, ak by sa návštevník v našej spoločnosti zranil a jeho meno, vek, údaje o zdravotnom poistení alebo iné životne dôležité informácie by bolo potrebné poskytnúť lekárovi, nemocnici alebo inej tretej strane. Vtedy by sa spracúvanie zakladalo na čl. 6 ods. 1 písm. d GDPR.

Ak je spracúvanie nevyhnutné na splnenie úlohy vykonávanej vo verejnom záujme alebo pri výkone verejnej moci zverenej prevádzkovateľovi, právnym základom je článok 2 ods. 6 ods. 1 písm. e) GDPR.

Nakoniec, operácie spracovania by mohli byť založené na článku 6 ods. 1 písm. f) GDPR. Tento právny základ sa používa na spracovateľské operácie, na ktoré sa nevzťahuje žiadny z vyššie uvedených právnych základov, ak je spracúvanie nevyhnutné na účely oprávnených záujmov, ktoré sleduje naša spoločnosť alebo tretia strana, okrem prípadov, keď nad takýmito záujmami prevažujú záujmy alebo základné práva a slobody dotknutej osoby, ktoré si vyžadujú ochranu osobných údajov. Takéto spracovateľské operácie sú obzvlášť prípustné, pretože ich európsky zákonodarca výslovne uviedol. Domnieval sa, že oprávnený záujem možno predpokladať, ak je dotknutá osoba klientom prevádzkovateľa (odôvodnenie 47 veta 2 GDPR).

## D. Ak sa spracúvanie zakladá na článku 6 ods. 1 písm. f), oprávnené záujmy, ktoré sleduje prevádzkovateľ alebo tretia strana (článok 13 ods. 1 písm. d) GDPR)

Ak je spracúvanie osobných údajov založené na článku 6 ods. 1 písm. f GDPR, naším oprávneným záujmom je vykonávať našu činnosť v prospech blaha všetkých našich zamestnancov a akcionárov.

## E. Príjemcovia alebo kategórie príjemcov osobných údajov, ak existujú (článok 13 ods. 1 písm. e) GDPR)

Verejné orgány


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

Externé orgány

Ďalšie externé orgány

Interné spracovanie

Vnútroskupinové spracovanie

Ostatné orgány

Zoznam našich spracovateľov a príjemcov údajov v tretích krajinách a prípadne medzinárodných organizácií je zverejnený na našej webovej stránke alebo si ho môžete od nás bezplatne vyžiadať. Ak chcete požiadať o tento zoznam, obráťte sa na nášho úradníka pre ochranu údajov.

## F. V relevantnom prípade informácia o tom, že prevádzkovateľ zamýšľa preniesť osobné údaje do tretej krajiny alebo medzinárodnej organizácii a informácia o existencii alebo neexistencii rozhodnutia Komisie o primeranosti alebo, v prípade prenosov uvedených v článku 46 alebo 47 či v článku 49 ods. 1 druhom pododseku odkaz na primerané alebo vhodné záruky a prostriedky na získanie ich kópie, alebo kde boli poskytnuté (článok 13 ods. 1 písm. f), článok 46 ods. 1, článok 46 ods. 2 písm. c) GDPR)

Medzi príjemcov osobných údajov môžu patriť všetky spoločnosti a pobočky, ktoré sú súčasťou našej skupiny (ďalej len "spoločnosti skupiny") a ktoré majú miesto podnikania alebo kanceláriu v tretej krajine. Zoznam všetkých spoločností skupiny alebo príjemcov si môžete vyžiadať od nás.

Podľa článku 46 ods. 1 GDPR môže prevádzkovateľ alebo sprostredkovateľ preniesť osobné údaje do tretej krajiny len vtedy, ak poskytol primerané záruky a pod podmienkou, že sú k dispozícii vymožiteľné práva dotknutých osôb a účinné právne prostriedky nápravy pre dotknuté osoby. Primerané záruky možno poskytnúť bez toho, aby sa vyžadovalo osobitné povolenie dozorného orgánu, prostredníctvom štandardných zmluvných doložiek, článok 46 ods. 2 písm. c) GDPR.

So všetkými príjemcami z tretích krajín sa pred prvým prenosom osobných údajov dohodneme na štandardných zmluvných doložkách Európskej únie alebo iných vhodných zárukách. Následne sa zabezpečí, aby boli zaručené primerané záruky, vymožiteľné práva dotknutých osôb a účinné právne prostriedky nápravy pre dotknuté osoby. Každá dotknutá osoba môže u nás získať kópiu štandardných zmluvných doložiek. Štandardné zmluvné doložky sú k dispozícii aj v Úradnom vestníku Európskej únie.

Článok 45 ods. 3 všeobecného nariadenia o ochrane údajov (GDPR) udeľuje Európskej komisii právomoc rozhodnúť prostredníctvom vykonávacieho aktu, že krajina, ktorá nie je členom EÚ, zabezpečuje primeranú úroveň ochrany. To znamená úroveň ochrany osobných údajov, ktorá je v podstate rovnocenná s úrovňou ochrany v rámci EÚ. Dôsledkom rozhodnutí o primeranosti je, že osobné


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

údaje môžu voľne prúdiť z EÚ (a Nórska, Lichtenštajnska a Islandu) do tretej krajiny bez ďalších prekážok. Podobné pravidlá platia pre Spojené kráľovstvo, Švajčiarsko a niektoré ďalšie krajiny.

Ak Európska komisia alebo vláda inej krajiny rozhodla, že tretia krajina zabezpečuje primeranú úroveň ochrany a existuje platný rámec (napr. EU-U.S. Data Privacy Framework, Swiss-U.S. Data Privacy Framework, UK Extension to the EU-U.S. Data Privacy Framework), všetky naše prenosy údajov členom týchto rámcov (napr. samostatne certifikovaným subjektom) sú založené výlučne na členstve tohto subjektu v príslušnom rámci. Ak sme my alebo niektorý zo subjektov našej skupiny členom takéhoto rámca, všetky prenosy nám alebo subjektu našej skupiny sú založené výlučne na členstve týchto subjektov v takomto rámci.

Každý subjekt údajov môže od nás získať kópiu rámcov. Okrem toho sú rámce k dispozícii aj v Úradnom vestníku Európskej únie alebo vo zverejnených právnych materiáloch alebo na webových stránkach dozorných orgánov alebo iných príslušných orgánov alebo inštitúcií.

## G. Doba uchovávania osobných údajov alebo, ak to nie je možné, kritériá na jej určenie (článok 13 ods. 2 písm. a) GDPR)

Kritériom na určenie doby uchovávania osobných údajov je príslušná zákonná doba uchovávania. Po uplynutí tejto lehoty sa príslušné údaje bežne vymažú, pokiaľ už nie sú potrebné na plnenie zmluvy alebo začatie zmluvy.

Ak neexistuje zákonná lehota uchovávania, kritériom je zmluvná alebo interná lehota uchovávania.

## H. Existencia práva požadovať od prevádzkovateľa prístup k osobným údajom týkajúcim sa dotknutej osoby a práva na ich opravu alebo vymazanie alebo obmedzenie spracúvania, alebo práva namietať proti spracúvaniu, ako aj práva na prenosnosť údajov (článok 13 ods. 2 písm. b) GDPR)

Všetky dotknuté osoby majú tieto práva:

***Právo na prístup***

Každá dotknutá osoba má právo na prístup k osobným údajom, ktoré sa jej týkajú. Právo na prístup sa vzťahuje na všetky nami spracúvané údaje. Toto právo možno uplatniť jednoducho a v primeraných intervaloch, aby ste sa mohli oboznámiť so zákonnosťou spracúvania a overiť si ju (odôvodnenie 63 GDPR). Toto právo vyplýva z čl. 15 GDPR. Dotknutá osoba nás môže kontaktovať, aby uplatnila právo na prístup.

***Právo na opravu***

Podľa článku 16 vety 1 GDPR má dotknutá osoba právo na to, aby prevádzkovateľ bez zbytočného odkladu opravil nesprávne osobné údaje, ktoré sa jej týkajú. Okrem toho sa v článku 16 veta 2 GDPR


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

stanovuje, že dotknutá osoba má s prihliadnutím na účely spracúvania právo na doplnenie neúplných osobných údajov, a to aj prostredníctvom poskytnutia dodatočného vyhlásenia. Dotknutá osoba sa na nás môže obrátiť s cieľom uplatniť právo na opravu.

***Právo na vymazanie (právo byť zabudnutý)***

Okrem toho majú dotknuté osoby právo na výmaz a právo byť zabudnutý podľa článku. 17 GDPR. Toto právo môžete uplatniť aj tak, že nás kontaktujete. Na tomto mieste by sme však chceli upozorniť, že toto právo sa neuplatňuje, pokiaľ je spracúvanie nevyhnutné na splnenie zákonnej povinnosti, ktorá sa vzťahuje na našu spoločnosť, článok 17 ods. 3 písm. b GDPR. To znamená, že žiadosť o vymazanie môžeme schváliť až po uplynutí zákonnej lehoty uchovávania.

***Právo na obmedzenie spracovania***

Podľa článku 18 GDPR má každá dotknutá osoba právo na obmedzenie spracovania. Obmedzenie spracúvania možno požadovať, ak je splnená jedna z podmienok uvedených v článku 18 ods. 1 písm. a-d GDPR. Dotknutá osoba nás môže kontaktovať, aby uplatnila právo na obmedzenie spracúvania.

***Právo vzniesť námietku***

Okrem toho sa v čl. 21 GDPR zaručuje právo na námietku. Dotknutá osoba nás môže kontaktovať, aby uplatnila právo na námietku.

***Právo na prenosnosť údajov***

Čl. 20 GDPR priznáva dotknutej osobe právo na prenosnosť údajov. Podľa tohto ustanovenia má dotknutá osoba za podmienok stanovených v článku 20 ods. 1 písm. a) a b) GDPR právo získať osobné údaje, ktoré sa jej týkajú a ktoré poskytla prevádzkovateľovi, v štruktúrovanom, bežne používanom a strojovo čitateľnom formáte a má právo preniesť tieto údaje inému prevádzkovateľovi bez toho, aby jej prevádzkovateľ, ktorému boli osobné údaje poskytnuté, bránil. Dotknutá osoba nás môže kontaktovať, aby si uplatnila právo na prenosnosť údajov.

## I. Ak je spracúvanie založené na článku 6 ods. 1 písm. a) alebo na článku 9 ods. 2 písm. a), existencia práva kedykoľvek svoj súhlas odvolať bez toho, aby to malo vplyv na zákonnosť spracúvania založeného na súhlase udelenom pred jeho odvolaním (článok 13 ods. 2 písm. c) GDPR)

Ak je spracúvanie osobných údajov založené na čl. 6 ods. 1 písm. a) GDPR, čo je prípad, ak dotknutá osoba udelila súhlas so spracovaním osobných údajov na jeden alebo viacero konkrétnych účelov, alebo je založené na čl. 9 ods. 2 písm. a) GDPR, ktorý upravuje výslovný súhlas so spracovaním osobitných kategórií osobných údajov, má dotknutá osoba podľa čl. 7 ods. 3 vety 1 GDPR právo svoj súhlas kedykoľvek odvolať.

Odvolanie súhlasu nemá vplyv na zákonnosť spracúvania založeného na súhlase pred jeho odvolaním, článok 7 ods. 3 veta 2 GDPR. Odvolanie súhlasu musí byť rovnako jednoduché ako jeho udelenie, čl. 7


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

ods. 3 veta 4 GDPR. Preto sa odvolanie súhlasu môže vždy uskutočniť rovnakým spôsobom, akým bol súhlas udelený, alebo akýmkoľvek iným spôsobom, ktorý dotknutá osoba považuje za jednoduchší. V dnešnej informačnej spoločnosti je pravdepodobne najjednoduchším spôsobom odvolania súhlasu jednoduchý e-mail. Ak si dotknutá osoba želá odvolať svoj súhlas, ktorý nám udelila, stačí nám poslať jednoduchý e-mail. Prípadne si dotknutá osoba môže zvoliť akýkoľvek iný spôsob, ako nám oznámiť odvolanie svojho súhlasu.

## J. Právo podať sťažnosť dozornému orgánu (článok 13 ods. 2 písm. d), článok 77 ods. 1 GDPR)

Ako prevádzkovateľ sme povinní informovať dotknutú osobu o práve podať sťažnosť dozornému orgánu, článok 13 ods. 2 písm. d) GDPR. Právo podať sťažnosť dozornému orgánu upravuje článok 77 ods. 1 GDPR. Podľa tohto ustanovenia bez toho, aby boli dotknuté akékoľvek iné správne alebo súdne prostriedky nápravy, má každá dotknutá osoba právo podať sťažnosť dozornému orgánu, najmä v členskom štáte svojho obvyklého pobytu, pracoviska alebo miesta údajného porušenia, ak sa dotknutá osoba domnieva, že spracúvanie osobných údajov, ktoré sa jej týka, porušuje všeobecné nariadenie o ochrane údajov. Právo podať sťažnosť dozornému orgánu bolo právom Únie obmedzené len tak, že ho možno uplatniť len u jedného dozorného orgánu (odôvodnenie 141 veta 1 GDPR). Cieľom tohto pravidla je zabrániť dvojitým sťažnostiam tej istej dotknutej osoby v tej istej veci. Ak chce dotknutá osoba podať na nás sťažnosť, požiadali sme ju preto, aby sa obrátila len na jeden dozorný orgán.

## K. Informácia o tom, či je poskytovanie osobných údajov zákonnou alebo zmluvnou požiadavkou, alebo požiadavkou, ktorá je potrebná na uzavretie zmluvy, či je dotknutá osoba povinná poskytnúť osobné údaje, ako aj možné následky neposkytnutia takýchto údajov (článok 13 ods. 2 písm. e) GDPR)

Vysvetľujeme, že poskytovanie osobných údajov sa čiastočne vyžaduje zo zákona (napr. daňové predpisy) alebo môže vyplývať aj zo zmluvných ustanovení (napr. informácie o zmluvnom partnerovi).

Niekedy môže byť na uzavretie zmluvy potrebné, aby nám dotknutá osoba poskytla osobné údaje, ktoré musíme následne spracovať. Dotknutá osoba je napríklad povinná poskytnúť nám osobné údaje, keď s ňou naša spoločnosť uzavrie zmluvu. Neposkytnutie osobných údajov by malo za následok, že zmluva so subjektom údajov by nemohla byť uzavretá.

Pred poskytnutím osobných údajov dotknutou osobou nás musí dotknutá osoba kontaktovať. Subjektu údajov vysvetlíme, či je poskytnutie osobných údajov vyžadované zákonom alebo zmluvou alebo je nevyhnutné na uzavretie zmluvy, či existuje povinnosť poskytnúť osobné údaje a aké sú dôsledky neposkytnutia osobných údajov.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

### L. Existencia automatizovaného rozhodovania vrátane profilovania uvedeného v článku 22 ods. 1 a 4 a aspoň v týchto prípadoch zmysluplné informácie o použitom postupe, ako aj význame a predpokladaných dôsledkoch takéhoto spracúvania pre dotknutú osobu (článok 13 ods. 2 písm. f) GDPR)

Ako zodpovedná spoločnosť zvyčajne nepoužívame automatizované rozhodovanie ani profilovanie. Ak vo výnimočných prípadoch vykonávame automatizované rozhodovanie alebo profilovanie, informujeme o tom dotknutú osobu buď samostatne, alebo prostredníctvom pododdielu v našich zásadách ochrany osobných údajov (na našej webovej stránke). V takomto prípade platí nasledovné:

Automatizované rozhodovanie - vrátane profilovania - sa môže uskutočniť, ak (1) je to potrebné na uzavretie alebo plnenie zmluvy medzi dotknutou osobou a nami, alebo (2) je to povolené právom Únie alebo členského štátu, ktoré sa na nás vzťahuje a ktoré tiež stanovuje vhodné opatrenia na ochranu práv a slobôd a oprávnených záujmov dotknutej osoby, alebo (3) je to založené na výslovnom súhlase dotknutej osoby.

V prípadoch uvedených v článku 22 ods. 2 písm. a) a c) GDPR vykonáme vhodné opatrenia na ochranu práv a slobôd a oprávnených záujmov dotknutej osoby. V týchto prípadoch máte právo na ľudský zásah zo strany prevádzkovateľa, na vyjadrenie svojho názoru a na napadnutie rozhodnutia.

Významné informácie o príslušnej logike, ako aj o význame a predpokladaných dôsledkoch takéhoto spracúvania údajov pre dotknutú osobu sú uvedené v našich zásadách ochrany osobných údajov.

## II. Informácie, ktoré sa majú poskytnúť, ak osobné údaje neboli získané od dotknutej osoby (článok 14 GDPR)

### A. Totožnosť a kontaktné údaje prevádzkovateľa a v príslušných prípadoch zástupcu prevádzkovateľa (článok 14 ods. 1 písm. a) GDPR)

Pozri vyššie

### B. Kontaktné údaje prípadnej zodpovednej osoby (článok 14 ods. 1 písm. b) GDPR)

Pozri vyššie


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## C. Účely spracúvania, na ktoré sú osobné údaje určené, ako aj právny základ spracúvania (článok 14 ods. 1 písm. c) GDPR)

Účelom spracúvania osobných údajov je vybavovanie všetkých operácií, ktoré sa týkajú prevádzkovateľa, zákazníkov, potenciálnych zákazníkov, obchodných partnerov alebo iných zmluvných alebo predzmluvných vzťahov medzi uvedenými skupinami (v najširšom zmysle) alebo právnych povinností prevádzkovateľa.

Ak je spracúvanie osobných údajov nevyhnutné na plnenie zmluvy, ktorej zmluvnou stranou je dotknutá osoba, ako je to napríklad v prípade, keď sú spracovateľské operácie potrebné na dodanie tovaru alebo poskytnutie inej služby, spracúvanie je založené na článku 6 ods. 1 písm. b) GDPR. To isté platí pre také operácie spracovania, ktoré sú potrebné na vykonanie opatrení pred uzavretím zmluvy, napríklad v prípade dopytov týkajúcich sa našich produktov alebo služieb. Podlieha naša spoločnosť zákonnej povinnosti, na základe ktorej sa vyžaduje spracovanie osobných údajov, napríklad na plnenie daňových povinností, spracovanie je založené na čl. 6 ods. 1 písm. c GDPR.

V ojedinelých prípadoch môže byť spracovanie osobných údajov nevyhnutné na ochranu životne dôležitých záujmov dotknutej osoby alebo inej fyzickej osoby. Išlo by napríklad o prípad, ak by sa návštevník v našej spoločnosti zranil a jeho meno, vek, údaje o zdravotnom poistení alebo iné životne dôležité informácie by bolo potrebné poskytnúť lekárovi, nemocnici alebo inej tretej strane. Vtedy by sa spracúvanie zakladalo na čl. 6 ods. 1 písm. d GDPR.

Ak je spracúvanie nevyhnutné na splnenie úlohy vykonávanej vo verejnom záujme alebo pri výkone verejnej moci zverenej prevádzkovateľovi, právnym základom je článok 2 ods. 6 ods. 1 písm. e) GDPR.

Nakoniec, operácie spracovania by mohli byť založené na článku 6 ods. 1 písm. f) GDPR. Tento právny základ sa používa na spracovateľské operácie, na ktoré sa nevzťahuje žiadny z vyššie uvedených právnych základov, ak je spracúvanie nevyhnutné na účely oprávnených záujmov, ktoré sleduje naša spoločnosť alebo tretia strana, okrem prípadov, keď nad takýmito záujmami prevažujú záujmy alebo základné práva a slobody dotknutej osoby, ktoré si vyžadujú ochranu osobných údajov. Takéto spracovateľské operácie sú obzvlášť prípustné, pretože ich európsky zákonodarca výslovne uviedol. Domnieval sa, že oprávnený záujem možno predpokladať, ak je dotknutá osoba klientom prevádzkovateľa (odôvodnenie 47 veta 2 GDPR).

## D. Kategórie dotknutých osobných údajov (článok 14 ods. 1 písm. d) GDPR)

Údaje o zákazníkoch

Údaje o potenciálnych zákazníkoch

Údaje o zamestnancoch


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## E. Príjemcovia alebo kategórie príjemcov osobných údajov, ak existujú (článok 14 ods. 1 písm. e) GDPR)

Verejné orgány

Externé orgány

Ďalšie externé orgány

Interné spracovanie

Vnútroskupinové spracovanie

Ostatné orgány

Zoznam našich spracovateľov a príjemcov údajov v tretích krajinách a prípadne medzinárodných organizácií je zverejnený na našej webovej stránke alebo si ho môžete od nás bezplatne vyžiadať. Ak chcete požiadať o tento zoznam, obráťte sa na nášho úradníka pre ochranu údajov.

## F. V relevantnom prípade informácia, že prevádzkovateľ zamýšľa preniesť osobné údaje príjemcovi v tretej krajine alebo medzinárodnej organizácii a informácia o existencii alebo neexistencii rozhodnutia Komisie o primeranosti alebo, v prípade prenosov uvedených v článku 46 alebo 47 či v článku 49 ods. 1 druhom pododseku odkaz na primerané alebo vhodné záruky a prostriedky na získanie ich kópie, alebo kde boli poskytnuté (článok 14 ods. 1 písm. f).

Medzi príjemcov osobných údajov môžu patriť všetky spoločnosti a pobočky, ktoré sú súčasťou našej skupiny (ďalej len "spoločnosti skupiny") a ktoré majú miesto podnikania alebo kanceláriu v tretej krajine. Zoznam všetkých spoločností skupiny si môžete vyžiadať od nás.

Podľa článku 46 ods. 1 GDPR môže prevádzkovateľ alebo sprostredkovateľ preniesť osobné údaje do tretej krajiny len vtedy, ak poskytol primerané záruky a pod podmienkou, že sú k dispozícii vymožiteľné práva dotknutých osôb a účinné právne prostriedky nápravy pre dotknuté osoby. Primerané záruky možno poskytnúť bez toho, aby sa vyžadovalo osobitné povolenie dozorného orgánu, prostredníctvom štandardných doložiek o ochrane údajov, článok 46 ods. 2 písm. c) GDPR.

So všetkými príjemcami z tretích krajín sa pred prvým prenosom osobných údajov dohodneme na štandardných zmluvných doložkách Európskej únie alebo iných vhodných zárukách. Následne sa


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

zabezpečí, aby boli zaručené primerané záruky, vymožiteľné práva dotknutých osôb a účinné právne prostriedky nápravy pre dotknuté osoby. Každá dotknutá osoba môže u nás získať kópiu štandardných zmluvných doložiek. Štandardné zmluvné doložky sú k dispozícii aj v Úradnom vestníku Európskej únie.

Článok 45 ods. 3 všeobecného nariadenia o ochrane údajov (GDPR) udeľuje Európskej komisii právomoc rozhodnúť prostredníctvom vykonávacieho aktu, že krajina, ktorá nie je členom EÚ, zabezpečuje primeranú úroveň ochrany. To znamená úroveň ochrany osobných údajov, ktorá je v podstate rovnocenná s úrovňou ochrany v rámci EÚ. Dôsledkom rozhodnutí o primeranosti je, že osobné údaje môžu voľne prúdiť z EÚ (a Nórska, Lichtenštajnska a Islandu) do tretej krajiny bez ďalších prekážok. Podobné pravidlá platia pre Spojené kráľovstvo, Švajčiarsko a niektoré ďalšie krajiny.

Ak Európska komisia alebo vláda inej krajiny rozhodla, že tretia krajina zabezpečuje primeranú úroveň ochrany a existuje platný rámec (napr. EU-U.S. Data Privacy Framework, Swiss-U.S. Data Privacy Framework, UK Extension to the EU-U.S. Data Privacy Framework), všetky naše prenosy údajov členom týchto rámcov (napr. samostatne certifikovaným subjektom) sú založené výlučne na členstve tohto subjektu v príslušnom rámci. Ak sme my alebo niektorý zo subjektov našej skupiny členom takéhoto rámca, všetky prenosy nám alebo subjektu našej skupiny sú založené výlučne na členstve týchto subjektov v takomto rámci.

Každý subjekt údajov môže od nás získať kópiu rámcov. Okrem toho sú rámce k dispozícii aj v Úradnom vestníku Európskej únie alebo vo zverejnených právnych materiáloch alebo na webových stránkach dozorných orgánov alebo iných príslušných orgánov alebo inštitúcií.

## G. Doba uchovávania osobných údajov, alebo ak to nie je možné, kritériá na jej určenie (článok 14 ods. 2 písm. a) GDPR)

Kritériom na určenie doby uchovávania osobných údajov je príslušná zákonná doba uchovávania. Po uplynutí tejto lehoty sa príslušné údaje bežne vymažú, pokiaľ už nie sú potrebné na plnenie zmluvy alebo začatie zmluvy.

Ak neexistuje zákonná lehota uchovávania, kritériom je zmluvná alebo interná lehota uchovávania.

## H. Ak sa spracúvanie zakladá na článku 6 ods. 1 písm. f), oprávnené záujmy, ktoré sleduje prevádzkovateľ alebo tretia strana (článok 14 ods. 2 písm. b) GDPR)

Podľa článku 6 ods. 1 písm. f) GDPR je spracúvanie zákonné len vtedy, ak je spracúvanie nevyhnutné na účely oprávnených záujmov prevádzkovateľa alebo tretej strany s výnimkou prípadov, keď nad takýmito záujmami prevažujú záujmy alebo základné práva a slobody dotknutej osoby, ktoré si vyžadujú ochranu osobných údajov. Podľa odôvodnenia 47 vety 2 GDPR by oprávnený záujem mohol existovať, ak existuje relevantný a primeraný vzťah medzi dotknutou osobou a prevádzkovateľom, napr. v situáciách, keď je dotknutá osoba klientom prevádzkovateľa. Vo všetkých prípadoch, v ktorých naša


© All rights reserved by Heiko Maniero.

spoločnosť spracúva osobné údaje na základe článku 6 ods. 1 písm. f GDPR, je naším oprávneným záujmom vykonávanie našej činnosti v prospech blaha všetkých našich zamestnancov a akcionárov.

## I. Existencia práva požadovať od prevádzkovateľa prístup k osobným údajom týkajúcim sa dotknutej osoby a práva na ich opravu alebo vymazanie alebo obmedzenie spracúvania, a práva namietať proti spracúvaniu, ako aj práva na prenosnosť údajov (článok 14 ods. 2 písm. c) GDPR)

Všetky dotknuté osoby majú tieto práva:

***Právo na prístup***

Každá dotknutá osoba má právo na prístup k osobným údajom, ktoré sa jej týkajú. Právo na prístup sa vzťahuje na všetky nami spracúvané údaje. Toto právo možno uplatniť jednoducho a v primeraných intervaloch, aby ste sa mohli oboznámiť so zákonnosťou spracúvania a overiť si ju (odôvodnenie 63 GDPR). Toto právo vyplýva z čl. 15 GDPR. Dotknutá osoba nás môže kontaktovať, aby uplatnila právo na prístup.

***Právo na opravu***

Podľa článku 16 vety 1 GDPR má dotknutá osoba právo na to, aby prevádzkovateľ bez zbytočného odkladu opravil nesprávne osobné údaje, ktoré sa jej týkajú. Okrem toho sa v článku 16 veta 2 GDPR stanovuje, že dotknutá osoba má právo s prihliadnutím na účely spracúvania na doplnenie neúplných osobných údajov, a to aj prostredníctvom poskytnutia dodatočného vyhlásenia. Dotknutá osoba sa na nás môže obrátiť s cieľom uplatniť právo na opravu.

***Právo na vymazanie (právo byť zabudnutý)***

Okrem toho majú dotknuté osoby právo na výmaz a právo byť zabudnutý podľa článku. 17 GDPR. Toto právo môžete uplatniť aj tak, že nás kontaktujete. Na tomto mieste by sme však chceli upozorniť, že toto právo sa neuplatňuje, pokiaľ je spracúvanie nevyhnutné na splnenie zákonnej povinnosti, ktorá sa vzťahuje na našu spoločnosť, článok 17 ods. 3 písm. b GDPR. To znamená, že žiadosť o vymazanie môžeme schváliť až po uplynutí zákonnej lehoty uchovávania.

***Právo na obmedzenie spracovania***

Podľa článku 18 GDPR má každá dotknutá osoba právo na obmedzenie spracovania. Obmedzenie spracúvania možno požadovať, ak je splnená jedna z podmienok uvedených v článku 18 ods. 1 písm. a-d GDPR. Dotknutá osoba nás môže kontaktovať, aby uplatnila právo na obmedzenie spracúvania.

***Právo vzniesť námietku***

Okrem toho sa v čl. 21 GDPR zaručuje právo na námietku. Dotknutá osoba nás môže kontaktovať, aby uplatnila právo na námietku.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

***Právo na prenosnosť údajov***

Čl. 20 GDPR priznáva dotknutej osobe právo na prenosnosť údajov. Podľa tohto ustanovenia má dotknutá osoba za podmienok stanovených v článku 20 ods. 1 písm. a) a b) GDPR právo získať osobné údaje, ktoré sa jej týkajú a ktoré poskytla prevádzkovateľovi, v štruktúrovanom, bežne používanom a strojovo čitateľnom formáte a má právo preniesť tieto údaje inému prevádzkovateľovi bez toho, aby jej prevádzkovateľ, ktorému boli osobné údaje poskytnuté, bránil. Dotknutá osoba nás môže kontaktovať, aby si uplatnila právo na prenosnosť údajov.

## J. Ak je spracúvanie založené na článku 6 ods. 1 písm. a) alebo na článku 9 ods. 2 písm. a), existencia práva kedykoľvek svoj súhlas odvolať bez toho, aby to malo vplyv na zákonnosť spracúvania založeného na súhlase udelenom pred jeho odvolaním (článok 14 ods. 2 písm. d GDPR)

Ak je spracúvanie osobných údajov založené na čl. 6 ods. 1 písm. a) GDPR, čo je prípad, ak dotknutá osoba udelila súhlas so spracovaním osobných údajov na jeden alebo viacero konkrétnych účelov, alebo je založené na čl. 9 ods. 2 písm. a) GDPR, ktorý upravuje výslovný súhlas so spracovaním osobitných kategórií osobných údajov, má dotknutá osoba podľa čl. 7 ods. 3 vety 1 GDPR právo svoj súhlas kedykoľvek odvolať.

Odvolanie súhlasu nemá vplyv na zákonnosť spracúvania založeného na súhlase pred jeho odvolaním, článok 7 ods. 3 veta 2 GDPR. Odvolanie súhlasu musí byť rovnako jednoduché ako jeho udelenie, čl. 7 ods. 3 veta 4 GDPR. Preto sa odvolanie súhlasu môže vždy uskutočniť rovnakým spôsobom, akým bol súhlas udelený, alebo akýmkoľvek iným spôsobom, ktorý dotknutá osoba považuje za jednoduchší. V dnešnej informačnej spoločnosti je pravdepodobne najjednoduchším spôsobom odvolania súhlasu jednoduchý e-mail. Ak si dotknutá osoba želá odvolať svoj súhlas, ktorý nám udelila, stačí nám poslať jednoduchý e-mail. Prípadne si dotknutá osoba môže zvoliť akýkoľvek iný spôsob, ako nám oznámiť odvolanie svojho súhlasu.

## K. Právo podať sťažnosť dozornému orgánu (článok 14 ods. 2 písm. e), článok 77 ods. 1 GDPR)

Ako prevádzkovateľ sme povinní informovať dotknutú osobu o práve podať sťažnosť dozornému orgánu, článok 14 ods. 2 písm. e) GDPR. Právo podať sťažnosť dozornému orgánu upravuje článok 77 ods. 1 GDPR. Podľa tohto ustanovenia bez toho, aby boli dotknuté akékoľvek iné správne alebo súdne prostriedky nápravy, má každá dotknutá osoba právo podať sťažnosť dozornému orgánu, najmä v členskom štáte svojho obvyklého pobytu, pracoviska alebo miesta údajného porušenia, ak sa dotknutá osoba domnieva, že spracúvanie osobných údajov, ktoré sa jej týka, porušuje všeobecné nariadenie o ochrane údajov. Právo podať sťažnosť dozornému orgánu bolo právom Únie obmedzené len tak, že ho možno uplatniť len u jedného dozorného orgánu (odôvodnenie 141 veta 1 GDPR). Cieľom tohto pravidla


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

je zabrániť dvojitým sťažnostiam tej istej dotknutej osoby v tej istej veci. Ak chce dotknutá osoba podať na nás sťažnosť, požiadali sme ju preto, aby sa obrátila len na jeden dozorný orgán.

## L. Z akého zdroja pochádzajú osobné údaje, prípadne informácie o tom, či údaje pochádzajú z verejne prístupných zdrojov (článok 14 ods. 2 písm. f) GDPR)

Osobné údaje sa v zásade získavajú priamo od dotknutej osoby alebo v spolupráci s orgánom (napr. vyhľadaním údajov z úradného registra). Ostatné údaje o dotknutých osobách sa získavajú z prenosov spoločností skupiny. V súvislosti s týmito všeobecnými informáciami je vymenovanie presných zdrojov, z ktorých osobné údaje pochádzajú, buď nemožné, alebo by si vyžadovalo neprimerané úsilie v zmysle čl. 14 ods. 5 písm. b) GDPR. V zásade nezhromažďujeme osobné údaje z verejne prístupných zdrojov.

Každá dotknutá osoba nás môže kedykoľvek kontaktovať a získať podrobnejšie informácie o presných zdrojoch osobných údajov, ktoré sa jej týkajú. Ak nie je možné dotknutej osobe poskytnúť informácie o pôvode osobných údajov, pretože boli použité rôzne zdroje, mali by sa poskytnúť všeobecné informácie (odôvodnenie 61 veta 4 GDPR).

## M. Existencia automatizovaného rozhodovania vrátane profilovania uvedeného v článku 22 ods. 1 a 4 a aspoň v týchto prípadoch zmysluplné informácie o použitom postupe, ako aj význame a predpokladaných dôsledkoch takéhoto spracúvania pre dotknutú osobu (článok 14 ods. 2 písm. g) GDPR)

Ako zodpovedná spoločnosť zvyčajne nepoužívame automatizované rozhodovanie ani profilovanie. Ak vo výnimočných prípadoch vykonávame automatizované rozhodovanie alebo profilovanie, informujeme o tom dotknutú osobu buď samostatne, alebo prostredníctvom pododdielu v našich zásadách ochrany osobných údajov (na našej webovej stránke). V takomto prípade platí nasledovné:

Automatizované rozhodovanie - vrátane profilovania - sa môže uskutočniť, ak (1) je to potrebné na uzavretie alebo plnenie zmluvy medzi dotknutou osobou a nami, alebo (2) je to povolené právom Únie alebo členského štátu, ktoré sa na nás vzťahuje a ktoré tiež stanovuje vhodné opatrenia na ochranu práv a slobôd a oprávnených záujmov dotknutej osoby, alebo (3) je to založené na výslovnom súhlase dotknutej osoby.

V prípadoch uvedených v článku 22 ods. 2 písm. a) a c) GDPR vykonáme vhodné opatrenia na ochranu práv a slobôd a oprávnených záujmov dotknutej osoby. V týchto prípadoch máte právo na ľudský zásah zo strany prevádzkovateľa, na vyjadrenie svojho názoru a na napadnutie rozhodnutia.

Významné informácie o príslušnej logike, ako aj o význame a predpokladaných dôsledkoch takéhoto spracúvania údajov pre dotknutú osobu sú uvedené v našich zásadách ochrany osobných údajov.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## III. EU-U.S. Data Privacy Framework (EU-U.S. DPF), UK Extension to the EU-U.S. DPF, Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF)

Ak je naša organizácia certifikovaným členom EU-U.S. Data Privacy Framework (EU-U.S. DPF) a/alebo UK Extension to the EU-U.S. DPF a/alebo Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF), platí nasledovné:

Dodržiavame EU-U.S. Data Privacy Framework (EU-U.S. DPF) a UK Extension to the EU-U.S. DPF ako aj Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF), ako to stanovilo U.S. Department of Commerce. Naša spoločnosť potvrdila americkému ministerstvu obchodu, že dodržiava EU-U.S. Data Privacy Framework Principles (EU-U.S. DPF Principles) v súvislosti so spracovaním osobných údajov, ktoré prijíma z Európskej únie a Spojeného kráľovstva na základe EU-U.S. DPF a UK Extension to the EU-U.S. DPF. Naša spoločnosť potvrdila americkému ministerstvu obchodu, že dodržiava Swiss-U.S. Data Privacy Framework Principles (Swiss-U.S. DPF Principles) v súvislosti so spracovaním osobných údajov, ktoré prijíma zo Švajčiarska na základe Swiss-U.S. DPF. V prípade rozporu medzi ustanoveniami našej politiky ochrany osobných údajov a EU-U.S. DPF Principles a/alebo Swiss-U.S. DPF Principles sú Principles rozhodujúce.

Pre viac informácií o programe Data Privacy Framework (DPF) a pre zobrazenie našej certifikácie navštívte prosím https://www.dataprivacyframework.gov/.

Ostatné americké jednotky alebo dcérske spoločnosti našej spoločnosti, ktoré tiež dodržiavajú EU-U.S. DPF Principals, vrátane UK Extension to the EU-U.S. DPF a Swiss-U.S. DPF Principals, ak existujú, sú uvedené v našom vyhlásení o ochrane osobných údajov.

V súlade s EU-U.S. DPF a UK Extension to the EU-U.S. DPF a Swiss-U.S. DPF sa naša spoločnosť zaväzuje spolupracovať s orgánom zriadeným európskymi orgánmi pre ochranu údajov a britským úradom pre informácie (ICO) a švajčiarskym Federálnym komisárom pre ochranu údajov a informácie (EDÖB) a dodržiavať ich odporúčania ohľadom nevyriešených sťažností na naše zaobchádzanie s osobnými údajmi, ktoré sme prijali na základe EU-U.S. DPF a UK Extension to the EU-U.S. DPF a Swiss-U.S. DPF.

Informujeme dotknuté osoby o príslušných európskych orgánoch pre ochranu údajov, ktoré sú zodpovedné za riešenie sťažností na zaobchádzanie našej organizácie s osobnými údajmi, v hornej časti tohto dokumentu o transparentnosti a o tom, že dotknutým osobám poskytujeme primeraný a bezplatný právny prostriedok.

Informujeme všetky dotknuté osoby, že naša spoločnosť podlieha vyšetrovacím a presadzovacím právomociam Federal Trade Commission (FTC).

Dotknuté osoby majú za určitých podmienok možnosť požiadať o záväzné rozhodcovské konanie. Naša organizácia je povinná riešiť nároky a dodržiavať podmienky podľa Prílohy I k DPF-Principals, ak


© All rights reserved by Heiko Maniero.

dotknutá osoba požiadala o záväzné rozhodcovské konanie tým, že informovala našu organizáciu a boli dodržané postupy a podmienky podľa Prílohy I k Principals.

Týmto informujeme všetky dotknuté osoby o zodpovednosti našej organizácie v prípade odovzdania osobných údajov tretím stranám.

Pre otázky dotknutých osôb alebo orgánov na ochranu údajov sme v tomto dokumente o transparentnosti uviedli miestnych zástupcov.

Ponúkame vám možnosť vybrať si (Opt-out), či sa vaše osobné údaje (i) odovzdajú tretím stranám alebo (ii) použijú na účel, ktorý sa podstatne líši od účelu/účelov, na ktoré boli pôvodne zhromaždené alebo neskôr schválené vami. Jasný, dobre viditeľný a ľahko prístupný mechanizmus na uplatnenie vášho výberu spočíva v tom, že kontaktujete nášho zodpovedného pracovníka pre ochranu údajov (DSB) e-mailom. Nemáte možnosť výberu a nie sme povinní to urobiť, ak sa údaje odovzdajú tretej strane, ktorá koná ako zástupca alebo spracovateľ v našom mene a podľa našich pokynov. Vždy však uzatvoríme zmluvu s takýmto zástupcom alebo spracovateľom.

Pre citlivé údaje (t. j. osobné údaje, ktoré obsahujú informácie o zdravotnom stave, rasovom alebo etnickom pôvode, politických názoroch, náboženských alebo filozofických presvedčeniach, členstve v odbore alebo informácie o sexuálnom živote dotknutej osoby) získavame váš výslovný súhlas (Opt-in), keď sa tieto údaje (i) odovzdajú tretím stranám alebo (ii) použijú na iný účel, ako na ktorý boli pôvodne zhromaždené alebo na ktorý ste neskôr dali svoj súhlas tým, že ste si vybrali možnosť Opt-in. Navyše, všetky osobné údaje, ktoré prijmeme od tretích strán, považujeme za citlivé, ak ich tretia strana identifikovala a spracovala ako také.

Týmto vás informujeme o požiadavke na zverejnenie osobných údajov ako reakcie na zákonné požiadavky orgánov, vrátane splnenia požiadaviek národnej bezpečnosti alebo trestného stíhania.

Pri prenose osobných údajov tretej strane, ktorá koná ako zodpovedná osoba, dodržiavame Principals oznamovania a voľby. Okrem toho uzatvárame zmluvu s treťou stranou, ktorá je zodpovedná za spracovanie, ktorá stanovuje, že tieto údaje sa môžu spracúvať len pre obmedzené a určené účely v súlade so súhlasom, ktorý ste poskytli, a že príjemca musí poskytnúť rovnakú úroveň ochrany ako Principals DPF a informovať nás, ak zistí, že už nemôže splniť túto povinnosť. Zmluva predpokladá, že treťa strana, ktorá je zodpovednou osobou, zastaví spracovanie alebo prijme iné primerané a vhodné opatrenia na nápravu, ak sa takéto zistenie urobí.

Pri prenose osobných údajov tretej strane, ktorá koná ako zástupca alebo spracovateľ, (i) prenášame tieto údaje iba pre obmedzené a určené účely; (ii) zabezpečujeme, aby zástupca alebo spracovateľ bol povinný poskytovať aspoň rovnakú úroveň ochrany údajov, ako vyžadujú DPF-Principals; (iii) prijímame primerané a vhodné opatrenia, aby sme zabezpečili, že zástupca alebo spracovateľ skutočne spracováva prenesené osobné údaje spôsobom, ktorý je v súlade s našimi záväzkami podľa DPF-Principals; (iv) vyžadujeme od zástupcu alebo spracovateľa, aby nás informoval, ak zistí, že už nemôže poskytovať rovnakú úroveň ochrany, ako predpokladajú DPF-Principals; (v) po takomto oznámení, vrátane pod (iv),


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

prijímame primerané a vhodné kroky na zastavenie neoprávneného spracovania a na nápravu; a (vi) na požiadanie DPF Department poskytujeme súhrn alebo reprezentatívny príklad relevantných ustanovení o ochrane údajov z našej zmluvy s týmto zástupcom.

V súlade s EU-U.S. DPF a/alebo UK Extension to the EU-U.S. DPF a/alebo Swiss-U.S. DPF sa naša organizácia zaväzuje spolupracovať s orgánom, ktorý zriadili orgány EU pre ochranu údajov a britský úrad pre informácie (ICO) alebo švajčiarsky federálny komisár pre ochranu údajov a informácie (EDÖB), a dodržiavať ich odporúčania týkajúce sa nevyriešených sťažností na naše zaobchádzanie s osobnými údajmi, ktoré sme prijali v súvislosti s pracovným pomerom na základe EU-U.S. DPF a UK Extension to the EU-U.S. DPF a Swiss-U.S. DPF.

Všetky dotknuté osoby, ktoré sa dočasne nachádzajú v Európskej únii (EÚ), Európskom hospodárskom priestore (EHP) alebo v Spojenom kráľovstve, alebo ktoré tam majú bydlisko alebo obvyklý pobyt, majú nárok na práva a oprávnenia dotknutých osôb, ktoré sú zverejnené v našom dokumente o transparentnosti a ktoré vyplývajú aj z článkov 15 až 22 GDPR, vrátane práva na prístup k osobným údajom. Tieto informácie sme sprístupnili vo všetkých jazykoch EÚ a EHP. Anglická jazyková verzia sa vzťahuje na Spojené kráľovstvo.

Všetky dotknuté osoby, ktoré majú dočasný pobyt vo Švajčiarsku alebo tam majú bydlisko alebo obvyklý pobyt, majú nárok na práva a oprávnenia dotknutých osôb podľa švajčiarskeho zákona o ochrane údajov (DPA) a švajčiarskeho nariadenia o ochrane údajov (DPR), ktoré sú uverejnené v našom dokumente o transparentnosti, vrátane práva na prístup k osobným údajom. Tieto informácie sme poskytli v troch úradných jazykoch Švajčiarska (nemecky, taliansky a francúzsky).


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

# SLOVAK: Informácie o spracúvaní osobných údajov zamestnancov a uchádzačov (článok 13, 14 GDPR)

Vážený pán alebo pani,

Osobné údaje zamestnancov a uchádzačov si zaslúžia osobitnú ochranu. Naším cieľom je udržiavať úroveň ochrany údajov na vysokej úrovni. Preto bežne rozvíjame naše koncepcie ochrany a bezpečnosti údajov.

Samozrejme, dodržiavame zákonné ustanovenia o ochrane údajov. Podľa článkov 13, 14 GDPR prevádzkovatelia pri spracúvaní osobných údajov spĺňajú osobitné informačné požiadavky. Tento dokument tieto povinnosti spĺňa.

Terminológia právnej regulácie je zložitá. Žiaľ, pri príprave tohto dokumentu nebolo možné upustiť od používania právnych termínov. Preto by sme vás radi upozornili, že v prípade akýchkoľvek otázok týkajúcich sa tohto dokumentu, použitých termínov alebo formulácií sa na nás môžete kedykoľvek obrátiť.

## I. Informácie, ktoré sa majú poskytovať pri získavaní osobných údajov od dotknutej osoby (článok 13 GDPR)

### A. Totožnosť a kontaktné údaje prevádzkovateľa a v príslušných prípadoch zástupcu prevádzkovateľa (článok 13 ods. 1 písm. a) GDPR)

Pozri vyššie

### B. Kontaktné údaje prípadnej zodpovednej osoby (článok 13 ods. 1 písm. b) GDPR)

Pozri vyššie

### C. Účely spracúvania, na ktoré sú osobné údaje určené, ako aj právny základ spracúvania (článok 13 ods. 1 písm. c) GDPR)

V prípade údajov uchádzača je účelom spracovania údajov preskúmanie žiadosti počas náborového procesu. Na tento účel spracúvame všetky vami poskytnuté údaje. Na základe údajov poskytnutých počas náborového procesu overíme, či ste pozvaní na pracovný pohovor (súčasť výberového procesu). V prípade všeobecne vhodných uchádzačov, najmä v súvislosti s pracovným pohovorom, spracúvame niektoré ďalšie vami poskytnuté osobné údaje, ktoré sú nevyhnutné pre naše rozhodnutie o výbere. Ak vás zamestnáme, údaje uchádzača sa automaticky zmenia na údaje zamestnanca. V rámci výberového


© All rights reserved by Heiko Maniero.

konania budeme spracúvať aj ďalšie vaše osobné údaje, ktoré od vás požadujeme a ktoré sú potrebné na začatie alebo plnenie zmluvy (napríklad osobné identifikačné čísla alebo daňové čísla). V prípade údajov zamestnanca je účelom spracúvania údajov plnenie pracovnej zmluvy alebo dodržiavanie iných právnych predpisov vzťahujúcich sa na pracovný pomer (napr. daňové predpisy), ako aj použitie vašich osobných údajov na plnenie pracovnej zmluvy uzatvorenej s vami (napr. zverejnenie vášho mena a kontaktných údajov v rámci spoločnosti alebo zákazníkom). Údaje zamestnancov sa uchovávajú aj po skončení pracovného pomeru, aby sa splnili zákonné lehoty uchovávania.

Právnym základom pre spracovanie údajov je článok 6 ods. 1 písm. b) GDPR, článok 9 ods. 2 písm. b) a h) GDPR, článok 88 ods. 1 GDPR a vnútroštátne právne predpisy, ako napríklad v Nemecku článok 26 BDSG (Spolkový zákon o ochrane údajov).

## D. Príjemcovia alebo kategórie príjemcov osobných údajov, ak existujú (článok 13 ods. 1 písm. e) GDPR)

Verejné orgány

Externé orgány

Ďalšie externé orgány

Interné spracovanie

Vnútroskupinové spracovanie

Ostatné orgány

Zoznam našich spracovateľov a príjemcov údajov v tretích krajinách a prípadne medzinárodných organizácií je zverejnený na našej webovej stránke alebo si ho môžete od nás bezplatne vyžiadať. Ak chcete požiadať o tento zoznam, obráťte sa na nášho úradníka pre ochranu údajov.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## E. V relevantnom prípade informácia o tom, že prevádzkovateľ zamýšľa preniesť osobné údaje do tretej krajiny alebo medzinárodnej organizácii a informácia o existencii alebo neexistencii rozhodnutia Komisie o primeranosti alebo, v prípade prenosov uvedených v článku 46 alebo 47 či v článku 49 ods. 1 druhom pododseku odkaz na primerané alebo vhodné záruky a prostriedky na získanie ich kópie, alebo kde boli poskytnuté (článok 13 ods. 1 písm. f), článok 46 ods. 1, článok 46 ods. 2 písm. c) GDPR)

Medzi príjemcov osobných údajov môžu patriť všetky spoločnosti a pobočky, ktoré sú súčasťou našej skupiny (ďalej len "spoločnosti skupiny") a ktoré majú miesto podnikania alebo kanceláriu v tretej krajine. Zoznam všetkých spoločností skupiny alebo príjemcov si môžete vyžiadať od nás.

Podľa článku 46 ods. 1 GDPR môže prevádzkovateľ alebo sprostredkovateľ preniesť osobné údaje do tretej krajiny len vtedy, ak poskytol primerané záruky a pod podmienkou, že sú k dispozícii vymožiteľné práva dotknutých osôb a účinné právne prostriedky nápravy pre dotknuté osoby. Vhodné záruky možno poskytnúť bez toho, aby sa vyžadovalo osobitné povolenie dozorného orgánu, prostredníctvom štandardných zmluvných doložiek, článok 46 ods. 2 písm. c) GDPR.

So všetkými príjemcami z tretích krajín sa pred prvým prenosom osobných údajov dohodneme na štandardných zmluvných doložkách Európskej únie alebo iných vhodných zárukách. Následne sa zabezpečí, aby boli zaručené primerané záruky, vymožiteľné práva dotknutých osôb a účinné právne prostriedky nápravy pre dotknuté osoby. Každá dotknutá osoba môže u nás získať kópiu štandardných zmluvných doložiek. Štandardné zmluvné doložky sú k dispozícii aj v Úradnom vestníku Európskej únie.

Článok 45 ods. 3 všeobecného nariadenia o ochrane údajov (GDPR) udeľuje Európskej komisii právomoc rozhodnúť prostredníctvom vykonávacieho aktu, že krajina, ktorá nie je členom EÚ, zabezpečuje primeranú úroveň ochrany. To znamená úroveň ochrany osobných údajov, ktorá je v podstate rovnocenná s úrovňou ochrany v rámci EÚ. Dôsledkom rozhodnutí o primeranosti je, že osobné údaje môžu voľne prúdiť z EÚ (a Nórska, Lichtenštajnska a Islandu) do tretej krajiny bez ďalších prekážok. Podobné pravidlá platia pre Spojené kráľovstvo, Švajčiarsko a niektoré ďalšie krajiny.

Ak Európska komisia alebo vláda inej krajiny rozhodla, že tretia krajina zabezpečuje primeranú úroveň ochrany a existuje platný rámec (napr. EU-U.S. Data Privacy Framework, Swiss-U.S. Data Privacy Framework, UK Extension to the EU-U.S. Data Privacy Framework), všetky naše prenosy údajov členom týchto rámcov (napr. samostatne certifikovaným subjektom) sú založené výlučne na členstve tohto subjektu v príslušnom rámci. Ak sme my alebo niektorý zo subjektov našej skupiny členom takéhoto rámca, všetky prenosy nám alebo subjektu našej skupiny sú založené výlučne na členstve týchto subjektov v takomto rámci.

Každý subjekt údajov môže od nás získať kópiu rámcov. Okrem toho sú rámce k dispozícii aj v Úradnom vestníku Európskej únie alebo vo zverejnených právnych materiáloch alebo na webových stránkach dozorných orgánov alebo iných príslušných orgánov alebo inštitúcií.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## F. Doba uchovávania osobných údajov alebo, ak to nie je možné, kritériá na jej určenie (článok 13 ods. 2 písm. a) GDPR)

Doba uchovávania osobných údajov žiadateľov je 6 mesiacov. Pre údaje zamestnancov platí príslušná zákonná lehota uchovávania. Po uplynutí tejto lehoty sa príslušné údaje bežne vymažú, pokiaľ už nie sú potrebné na plnenie zmluvy alebo začatie zmluvy.

## G. Existencia práva požadovať od prevádzkovateľa prístup k osobným údajom týkajúcim sa dotknutej osoby a práva na ich opravu alebo vymazanie alebo obmedzenie spracúvania, alebo práva namietať proti spracúvaniu, ako aj práva na prenosnosť údajov (článok 13 ods. 2 písm. b) GDPR)

Všetky dotknuté osoby majú tieto práva:

***Právo na prístup***

Každá dotknutá osoba má právo na prístup k osobným údajom, ktoré sa jej týkajú. Právo na prístup sa vzťahuje na všetky nami spracúvané údaje. Toto právo možno uplatniť jednoducho a v primeraných intervaloch, aby ste sa mohli oboznámiť so zákonnosťou spracúvania a overiť si ju (odôvodnenie 63 GDPR). Toto právo vyplýva z čl. 15 GDPR. Dotknutá osoba nás môže kontaktovať, aby uplatnila právo na prístup.

***Právo na opravu***

Podľa článku 16 veta 1 GDPR má dotknutá osoba právo na to, aby prevádzkovateľ bez zbytočného odkladu opravil nesprávne osobné údaje, ktoré sa jej týkajú. Okrem toho sa v článku 16 veta 2 GDPR stanovuje, že dotknutá osoba má právo s prihliadnutím na účely spracúvania na doplnenie neúplných osobných údajov, a to aj prostredníctvom poskytnutia dodatočného vyhlásenia. Dotknutá osoba sa na nás môže obrátiť s cieľom uplatniť právo na opravu.

***Právo na vymazanie (právo byť zabudnutý)***

Okrem toho majú dotknuté osoby právo na výmaz a právo byť zabudnutý podľa článku. 17 GDPR. Toto právo môžete uplatniť aj tak, že nás kontaktujete. Na tomto mieste by sme však chceli upozorniť, že toto právo sa neuplatňuje, pokiaľ je spracúvanie nevyhnutné na splnenie zákonnej povinnosti, ktorá sa vzťahuje na našu spoločnosť, článok 17 ods. 3 písm. b GDPR. To znamená, že žiadosť o vymazanie môžeme schváliť až po uplynutí zákonnej lehoty uchovávania.

***Právo na obmedzenie spracovania***

Podľa článku 18 GDPR má každá dotknutá osoba právo na obmedzenie spracovania. Obmedzenie spracúvania možno požadovať, ak je splnená jedna z podmienok uvedených v článku 18 ods. 1 písm. a-d GDPR. Dotknutá osoba nás môže kontaktovať, aby uplatnila právo na obmedzenie spracúvania.


© All rights reserved by Heiko Maniero.

***Právo vzniesť námietku***

Okrem toho sa v čl. 21 GDPR zaručuje právo na námietku. Dotknutá osoba nás môže kontaktovať, aby uplatnila právo na námietku.

***Právo na prenosnosť údajov***

Čl. 20 GDPR priznáva dotknutej osobe právo na prenosnosť údajov. Podľa tohto ustanovenia má dotknutá osoba za podmienok stanovených v článku 20 ods. 1 písm. a) a b) GDPR právo získať osobné údaje, ktoré sa jej týkajú a ktoré poskytla prevádzkovateľovi, v štruktúrovanom, bežne používanom a strojovo čitateľnom formáte a má právo preniesť tieto údaje inému prevádzkovateľovi bez toho, aby jej prevádzkovateľ, ktorému boli osobné údaje poskytnuté, bránil. Dotknutá osoba nás môže kontaktovať, aby si uplatnila právo na prenosnosť údajov.

## H. Ak je spracúvanie založené na článku 6 ods. 1 písm. a) alebo na článku 9 ods. 2 písm. a), existencia práva kedykoľvek svoj súhlas odvolať bez toho, aby to malo vplyv na zákonnosť spracúvania založeného na súhlase udelenom pred jeho odvolaním (článok 13 ods. 2 písm. c) GDPR)

Ak je spracúvanie osobných údajov založené na čl. 6 ods. 1 písm. a) GDPR, čo je prípad, ak dotknutá osoba udelila súhlas so spracovaním osobných údajov na jeden alebo viacero konkrétnych účelov, alebo je založené na čl. 9 ods. 2 písm. a) GDPR, ktorý upravuje výslovný súhlas so spracovaním osobitných kategórií osobných údajov, má dotknutá osoba podľa čl. 7 ods. 3 vety 1 GDPR právo svoj súhlas kedykoľvek odvolať.

Odvolanie súhlasu nemá vplyv na zákonnosť spracúvania založeného na súhlase pred jeho odvolaním, článok 7 ods. 3 veta 2 GDPR. Odvolanie súhlasu musí byť rovnako jednoduché ako jeho udelenie, čl. 7 ods. 3 veta 4 GDPR. Preto sa odvolanie súhlasu môže vždy uskutočniť rovnakým spôsobom, akým bol súhlas udelený, alebo akýmkoľvek iným spôsobom, ktorý dotknutá osoba považuje za jednoduchší. V dnešnej informačnej spoločnosti je pravdepodobne najjednoduchším spôsobom odvolania súhlasu jednoduchý e-mail. Ak si dotknutá osoba želá odvolať svoj súhlas, ktorý nám udelila, stačí nám poslať jednoduchý e-mail. Prípadne si dotknutá osoba môže zvoliť akýkoľvek iný spôsob, ako nám oznámiť svoje odvolanie súhlasu.

## I. Právo podať sťažnosť dozornému orgánu (článok 13 ods. 2 písm. d), článok 77 ods. 1 GDPR)

Ako prevádzkovateľ sme povinní informovať dotknutú osobu o práve podať sťažnosť dozornému orgánu, článok 13 ods. 2 písm. d) GDPR. Právo podať sťažnosť dozornému orgánu upravuje článok 77 ods. 1 GDPR. Podľa tohto ustanovenia bez toho, aby boli dotknuté akékoľvek iné správne alebo súdne prostriedky nápravy, má každá dotknutá osoba právo podať sťažnosť dozornému orgánu, najmä v členskom štáte svojho obvyklého pobytu, pracoviska alebo miesta údajného porušenia, ak sa dotknutá


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

osoba domnieva, že spracúvanie osobných údajov, ktoré sa jej týka, porušuje všeobecné nariadenie o ochrane údajov. Právo podať sťažnosť dozornému orgánu bolo právom Únie obmedzené len tak, že ho možno uplatniť len u jedného dozorného orgánu (odôvodnenie 141 veta 1 GDPR). Cieľom tohto pravidla je zabrániť dvojitým sťažnostiam tej istej dotknutej osoby v tej istej veci. Ak chce dotknutá osoba podať na nás sťažnosť, požiadali sme ju preto, aby sa obrátila len na jeden dozorný orgán.

## J. Informácia o tom, či je poskytovanie osobných údajov zákonnou alebo zmluvnou požiadavkou, alebo požiadavkou, ktorá je potrebná na uzavretie zmluvy, či je dotknutá osoba povinná poskytnúť osobné údaje, ako aj možné následky neposkytnutia takýchto údajov (článok 13 ods. 2 písm. e) GDPR)

Vysvetľujeme, že poskytovanie osobných údajov sa čiastočne vyžaduje zo zákona (napr. daňové predpisy) alebo môže vyplývať aj zo zmluvných ustanovení (napr. informácie o zmluvnom partnerovi).

Niekedy môže byť na uzavretie zmluvy potrebné, aby nám dotknutá osoba poskytla osobné údaje, ktoré musíme následne spracovať. Dotknutá osoba je napríklad povinná poskytnúť nám osobné údaje, keď s ňou naša spoločnosť uzavrie zmluvu. Neposkytnutie osobných údajov by malo za následok, že zmluva so subjektom údajov by nemohla byť uzavretá.

Pred poskytnutím osobných údajov dotknutou osobou nás musí dotknutá osoba kontaktovať. Subjektu údajov vysvetlíme, či je poskytnutie osobných údajov vyžadované zákonom alebo zmluvou alebo je nevyhnutné na uzavretie zmluvy, či existuje povinnosť poskytnúť osobné údaje a aké sú dôsledky neposkytnutia osobných údajov.

## K. Existencia automatizovaného rozhodovania vrátane profilovania uvedeného v článku 22 ods. 1 a 4 a aspoň v týchto prípadoch zmysluplné informácie o použitom postupe, ako aj význame a predpokladaných dôsledkoch takéhoto spracúvania pre dotknutú osobu (článok 13 ods. 2 písm. f) GDPR)

Ako zodpovedná spoločnosť zvyčajne nepoužívame automatizované rozhodovanie ani profilovanie. Ak vo výnimočných prípadoch vykonávame automatizované rozhodovanie alebo profilovanie, informujeme o tom dotknutú osobu buď samostatne, alebo prostredníctvom pododdielu v našich zásadách ochrany osobných údajov (na našej webovej stránke). V takomto prípade platí nasledovné:

Automatizované rozhodovanie - vrátane profilovania - sa môže uskutočniť, ak (1) je to potrebné na uzavretie alebo plnenie zmluvy medzi dotknutou osobou a nami, alebo (2) je to povolené právom Únie alebo členského štátu, ktoré sa na nás vzťahuje a ktoré tiež stanovuje vhodné opatrenia na ochranu práv a slobôd a oprávnených záujmov dotknutej osoby, alebo (3) je to založené na výslovnom súhlase dotknutej osoby.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

V prípadoch uvedených v článku 22 ods. 2 písm. a) a c) GDPR vykonáme vhodné opatrenia na ochranu práv a slobôd a oprávnených záujmov dotknutej osoby. V týchto prípadoch máte právo na ľudský zásah zo strany prevádzkovateľa, na vyjadrenie svojho názoru a na napadnutie rozhodnutia.

Významné informácie o príslušnej logike, ako aj o význame a predpokladaných dôsledkoch takéhoto spracúvania údajov pre dotknutú osobu sú uvedené v našich zásadách ochrany osobných údajov.

## II. Informácie, ktoré sa majú poskytnúť, ak osobné údaje neboli získané od dotknutej osoby (článok 14 GDPR)

### A. Totožnosť a kontaktné údaje prevádzkovateľa a v príslušných prípadoch zástupcu prevádzkovateľa (článok 14 ods. 1 písm. a) GDPR)

Pozri vyššie

### B. Kontaktné údaje prípadnej zodpovednej osoby (článok 14 ods. 1 písm. b) GDPR)

Pozri vyššie

### C. Účely spracúvania, na ktoré sú osobné údaje určené, ako aj právny základ spracúvania (článok 14 ods. 1 písm. c) GDPR)

V prípade údajov uchádzača, ktoré neboli získané od dotknutej osoby, je účelom spracovania údajov vykonanie preskúmania žiadosti počas náborového procesu. Na tento účel môžeme spracúvať údaje, ktoré neboli získané od vás. Na základe údajov spracúvaných počas náborového procesu overíme, či ste pozvaní na pracovný pohovor (súčasť výberového procesu). Ak vás zamestnáme, údaje uchádzača sa automaticky premenia na údaje zamestnanca. V prípade údajov zamestnanca je účelom spracúvania údajov plnenie pracovnej zmluvy alebo dodržiavanie iných právnych ustanovení vzťahujúcich sa na pracovný pomer. Údaje zamestnancov sa uchovávajú po skončení pracovného pomeru, aby sa splnili zákonné lehoty uchovávania.

Právnym základom pre spracovanie údajov je článok 6 ods. 1 písm. b) a f) GDPR, článok 9 ods. 2 písm. b) a h) GDPR, článok 88 ods. 1 GDPR a vnútroštátne právne predpisy, ako napríklad v Nemecku článok 26 BDSG (Spolkový zákon o ochrane údajov).

### D. Kategórie dotknutých osobných údajov (článok 14 ods. 1 písm. d) GDPR)


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

Údaje žiadateľa

Údaje o zamestnancoch

## E. Príjemcovia alebo kategórie príjemcov osobných údajov, ak existujú (článok 14 ods. 1 písm. e) GDPR)

Verejné orgány

Externé orgány

Ďalšie externé orgány

Interné spracovanie

Vnútroskupinové spracovanie

Ostatné orgány

Zoznam našich spracovateľov a príjemcov údajov v tretích krajinách a prípadne medzinárodných organizácií je zverejnený na našej webovej stránke alebo si ho môžete od nás bezplatne vyžiadať. Ak chcete požiadať o tento zoznam, obráťte sa na nášho úradníka pre ochranu údajov.

## F. V relevantnom prípade informácia, že prevádzkovateľ zamýšľa preniesť osobné údaje príjemcovi v tretej krajine alebo medzinárodnej organizácii a informácia o existencii alebo neexistencii rozhodnutia Komisie o primeranosti alebo, v prípade prenosov uvedených v článku 46 alebo 47 či v článku 49 ods. 1 druhom pododseku odkaz na primerané alebo vhodné záruky a prostriedky na získanie ich kópie, alebo kde boli poskytnuté (článok 14 ods. 1 písm. f), článok 46 ods. 1, článok 46 ods. 2 písm. c) GDPR)

Medzi príjemcov osobných údajov môžu patriť všetky spoločnosti a pobočky, ktoré sú súčasťou našej skupiny (ďalej len "spoločnosti skupiny") a ktoré majú miesto podnikania alebo kanceláriu v tretej krajine. Zoznam všetkých spoločností skupiny alebo príjemcov si môžete vyžiadať od nás.

Podľa článku 46 ods. 1 GDPR môže prevádzkovateľ alebo sprostredkovateľ preniesť osobné údaje do tretej krajiny len vtedy, ak poskytol primerané záruky a pod podmienkou, že sú k dispozícii vymožiteľné práva dotknutých osôb a účinné právne prostriedky nápravy pre dotknuté osoby. Primerané záruky možno poskytnúť bez toho, aby sa vyžadovalo osobitné povolenie dozorného orgánu, prostredníctvom štandardných doložiek o ochrane údajov, článok 46 ods. 2 písm. c) GDPR.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

So všetkými príjemcami z tretích krajín sa pred prvým prenosom osobných údajov dohodneme na štandardných zmluvných doložkách Európskej únie alebo iných vhodných zárukách. Následne sa zabezpečí, aby boli zaručené primerané záruky, vymožiteľné práva dotknutých osôb a účinné právne prostriedky nápravy pre dotknuté osoby. Každá dotknutá osoba môže u nás získať kópiu štandardných zmluvných doložiek. Štandardné zmluvné doložky sú k dispozícii aj v Úradnom vestníku Európskej únie.

Článok 45 ods. 3 všeobecného nariadenia o ochrane údajov (GDPR) udeľuje Európskej komisii právomoc rozhodnúť prostredníctvom vykonávacieho aktu, že krajina, ktorá nie je členom EÚ, zabezpečuje primeranú úroveň ochrany. To znamená úroveň ochrany osobných údajov, ktorá je v podstate rovnocenná s úrovňou ochrany v rámci EÚ. Dôsledkom rozhodnutí o primeranosti je, že osobné údaje môžu voľne prúdiť z EÚ (a Nórska, Lichtenštajnska a Islandu) do tretej krajiny bez ďalších prekážok. Podobné pravidlá platia pre Spojené kráľovstvo, Švajčiarsko a niektoré ďalšie krajiny.

Ak Európska komisia alebo vláda inej krajiny rozhodla, že tretia krajina zabezpečuje primeranú úroveň ochrany a existuje platný rámec (napr. EU-U.S. Data Privacy Framework, Swiss-U.S. Data Privacy Framework, UK Extension to the EU-U.S. Data Privacy Framework), všetky naše prenosy údajov členom týchto rámcov (napr. samostatne certifikovaným subjektom) sú založené výlučne na členstve tohto subjektu v príslušnom rámci. Ak sme my alebo niektorý zo subjektov našej skupiny členom takéhoto rámca, všetky prenosy nám alebo subjektu našej skupiny sú založené výlučne na členstve týchto subjektov v takomto rámci.

Každý subjekt údajov môže od nás získať kópiu rámcov. Okrem toho sú rámce k dispozícii aj v Úradnom vestníku Európskej únie alebo vo zverejnených právnych materiáloch alebo na webových stránkach dozorných orgánov alebo iných príslušných orgánov alebo inštitúcií.

## G. Doba uchovávania osobných údajov, alebo ak to nie je možné, kritériá na jej určenie (článok 14 ods. 2 písm. a) GDPR)

Doba uchovávania osobných údajov žiadateľov je 6 mesiacov. Pre údaje zamestnancov platí príslušná zákonná lehota uchovávania. Po uplynutí tejto lehoty sa príslušné údaje bežne vymažú, pokiaľ už nie sú potrebné na plnenie zmluvy alebo začatie zmluvy.

## H. Ak sa spracúvanie zakladá na článku 6 ods. 1 písm. f), oprávnené záujmy, ktoré sleduje prevádzkovateľ alebo tretia strana (článok 14 ods. 2 písm. b) GDPR)

Podľa článku 6 ods. 1 písm. f) GDPR je spracúvanie zákonné len vtedy, ak je spracúvanie nevyhnutné na účely oprávnených záujmov prevádzkovateľa alebo tretej strany s výnimkou prípadov, keď nad takýmito záujmami prevažujú záujmy alebo základné práva a slobody dotknutej osoby, ktoré si vyžadujú ochranu osobných údajov. Podľa odôvodnenia 47 vety 2 GDPR by oprávnený záujem mohol existovať, ak existuje relevantný a primeraný vzťah medzi dotknutou osobou a prevádzkovateľom, napr. v


© All rights reserved by Heiko Maniero.

situáciách, keď je dotknutá osoba klientom prevádzkovateľa. Vo všetkých prípadoch, v ktorých naša spoločnosť spracúva údaje uchádzačov na základe článku 6 ods. 1 písm. f) GDPR, je naším oprávneným záujmom zamestnanie vhodných zamestnancov a odborníkov.

## I. Existencia práva požadovať od prevádzkovateľa prístup k osobným údajom týkajúcim sa dotknutej osoby a práva na ich opravu alebo vymazanie alebo obmedzenie spracúvania, a práva namietať proti spracúvaniu, ako aj práva na prenosnosť údajov (článok 14 ods. 2 písm. c) GDPR)

Všetky dotknuté osoby majú tieto práva:

***Právo na prístup***

Každá dotknutá osoba má právo na prístup k osobným údajom, ktoré sa jej týkajú. Právo na prístup sa vzťahuje na všetky nami spracúvané údaje. Toto právo možno uplatniť jednoducho a v primeraných intervaloch, aby ste sa mohli oboznámiť so zákonnosťou spracúvania a overiť si ju (odôvodnenie 63 GDPR). Toto právo vyplýva z čl. 15 GDPR. Dotknutá osoba nás môže kontaktovať, aby uplatnila právo na prístup.

***Právo na opravu***

Podľa článku 16 vety 1 GDPR má dotknutá osoba právo na to, aby prevádzkovateľ bez zbytočného odkladu opravil nesprávne osobné údaje, ktoré sa jej týkajú. Okrem toho sa v článku 16 veta 2 GDPR stanovuje, že dotknutá osoba má s prihliadnutím na účely spracúvania právo na doplnenie neúplných osobných údajov, a to aj prostredníctvom poskytnutia dodatočného vyhlásenia. Dotknutá osoba sa na nás môže obrátiť s cieľom uplatniť právo na opravu.

***Právo na vymazanie (právo byť zabudnutý)***

Okrem toho majú dotknuté osoby právo na výmaz a právo byť zabudnutý podľa článku. 17 GDPR. Toto právo môžete uplatniť aj tak, že nás kontaktujete. Na tomto mieste by sme však chceli upozorniť, že toto právo sa neuplatňuje, pokiaľ je spracúvanie nevyhnutné na splnenie zákonnej povinnosti, ktorá sa vzťahuje na našu spoločnosť, článok 17 ods. 3 písm. b GDPR. To znamená, že žiadosť o vymazanie môžeme schváliť až po uplynutí zákonnej lehoty uchovávania.

***Právo na obmedzenie spracovania***

Podľa článku 18 GDPR má každá dotknutá osoba právo na obmedzenie spracovania. Obmedzenie spracúvania možno požadovať, ak je splnená jedna z podmienok uvedených v článku 18 ods. 1 písm. a-d GDPR. Dotknutá osoba nás môže kontaktovať, aby uplatnila právo na obmedzenie spracúvania.

***Právo vzniesť námietku***

Okrem toho sa v čl. 21 GDPR zaručuje právo na námietku. Dotknutá osoba nás môže kontaktovať, aby uplatnila právo na námietku.


© All rights reserved by Heiko Maniero.

***Právo na prenosnosť údajov***

Čl. 20 GDPR priznáva dotknutej osobe právo na prenosnosť údajov. Podľa tohto ustanovenia má dotknutá osoba za podmienok stanovených v článku 20 ods. 1 písm. a) a b) GDPR právo získať osobné údaje, ktoré sa jej týkajú a ktoré poskytla prevádzkovateľovi, v štruktúrovanom, bežne používanom a strojovo čitateľnom formáte a má právo preniesť tieto údaje inému prevádzkovateľovi bez toho, aby jej prevádzkovateľ, ktorému boli osobné údaje poskytnuté, bránil. Dotknutá osoba nás môže kontaktovať, aby si uplatnila právo na prenosnosť údajov.

## J. Ak je spracúvanie založené na článku 6 ods. 1 písm. a) alebo na článku 9 ods. 2 písm. a), existencia práva kedykoľvek svoj súhlas odvolať bez toho, aby to malo vplyv na zákonnosť spracúvania založeného na súhlase udelenom pred jeho odvolaním (článok 14 ods. 2 písm. d) GDPR)

Ak je spracúvanie osobných údajov založené na čl. 6 ods. 1 písm. a) GDPR, čo je prípad, ak dotknutá osoba udelila súhlas so spracovaním osobných údajov na jeden alebo viacero konkrétnych účelov, alebo je založené na čl. 9 ods. 2 písm. a) GDPR, ktorý upravuje výslovný súhlas so spracovaním osobitných kategórií osobných údajov, má dotknutá osoba podľa čl. 7 ods. 3 vety 1 GDPR právo svoj súhlas kedykoľvek odvolať.

Odvolanie súhlasu nemá vplyv na zákonnosť spracúvania založeného na súhlase pred jeho odvolaním, článok 7 ods. 3 veta 2 GDPR. Odvolanie súhlasu musí byť rovnako jednoduché ako jeho udelenie, čl. 7 ods. 3 veta 4 GDPR. Preto sa odvolanie súhlasu môže vždy uskutočniť rovnakým spôsobom, akým bol súhlas udelený, alebo akýmkoľvek iným spôsobom, ktorý dotknutá osoba považuje za jednoduchší. V dnešnej informačnej spoločnosti je pravdepodobne najjednoduchším spôsobom odvolania súhlasu jednoduchý e-mail. Ak si dotknutá osoba želá odvolať svoj súhlas, ktorý nám udelila, stačí nám poslať jednoduchý e-mail. Prípadne si dotknutá osoba môže zvoliť akýkoľvek iný spôsob, ako nám oznámiť svoje odvolanie súhlasu.

## K. Právo podať sťažnosť dozornému orgánu (článok 14 ods. 2 písm. e), článok 77 ods. 1 GDPR)

Ako prevádzkovateľ sme povinní informovať dotknutú osobu o práve podať sťažnosť dozornému orgánu, článok 14 ods. 2 písm. e) GDPR. Právo podať sťažnosť dozornému orgánu upravuje článok 77 ods. 1 GDPR. Podľa tohto ustanovenia bez toho, aby boli dotknuté akékoľvek iné správne alebo súdne prostriedky nápravy, má každá dotknutá osoba právo podať sťažnosť dozornému orgánu, najmä v členskom štáte svojho obvyklého pobytu, pracoviska alebo miesta údajného porušenia, ak sa dotknutá osoba domnieva, že spracúvanie osobných údajov, ktoré sa jej týka, porušuje všeobecné nariadenie o ochrane údajov. Právo podať sťažnosť dozornému orgánu bolo právom Únie obmedzené len tak, že ho možno uplatniť len u jedného dozorného orgánu (odôvodnenie 141 veta 1 GDPR). Cieľom tohto pravidla


© All rights reserved by Heiko Maniero.

je zabrániť dvojitým sťažnostiam tej istej dotknutej osoby v tej istej veci. Ak chce dotknutá osoba podať na nás sťažnosť, požiadali sme ju preto, aby sa obrátila len na jeden dozorný orgán.

## L. Z akého zdroja pochádzajú osobné údaje, prípadne informácie o tom, či údaje pochádzajú z verejne prístupných zdrojov (článok 14 ods. 2 písm. f) GDPR)

Osobné údaje sa v zásade získavajú priamo od dotknutej osoby alebo v spolupráci s orgánom (napr. vyhľadaním údajov z úradného registra). Ostatné údaje o dotknutých osobách sa získavajú z prenosov spoločností skupiny. V súvislosti s týmito všeobecnými informáciami je vymenovanie presných zdrojov, z ktorých osobné údaje pochádzajú, buď nemožné, alebo by si vyžadovalo neprimerané úsilie v zmysle čl. 14 ods. 5 písm. b) GDPR. V zásade nezhromažďujeme osobné údaje z verejne prístupných zdrojov.

Každá dotknutá osoba nás môže kedykoľvek kontaktovať a získať podrobnejšie informácie o presných zdrojoch osobných údajov, ktoré sa jej týkajú. Ak nie je možné dotknutej osobe poskytnúť informácie o pôvode osobných údajov, pretože boli použité rôzne zdroje, mali by sa poskytnúť všeobecné informácie (odôvodnenie 61 veta 4 GDPR).

## M. Existencia automatizovaného rozhodovania vrátane profilovania uvedeného v článku 22 ods. 1 a 4 a aspoň v týchto prípadoch zmysluplné informácie o použitom postupe, ako aj význame a predpokladaných dôsledkoch takéhoto spracúvania pre dotknutú osobu (článok 14 ods. 2 písm. g) GDPR)

Ako zodpovedná spoločnosť zvyčajne nepoužívame automatizované rozhodovanie ani profilovanie. Ak vo výnimočných prípadoch vykonávame automatizované rozhodovanie alebo profilovanie, informujeme o tom dotknutú osobu buď samostatne, alebo prostredníctvom pododdielu v našich zásadách ochrany osobných údajov (na našej webovej stránke). V takomto prípade platí nasledovné:

Automatizované rozhodovanie - vrátane profilovania - sa môže uskutočniť, ak (1) je to potrebné na uzavretie alebo plnenie zmluvy medzi dotknutou osobou a nami, alebo (2) je to povolené právom Únie alebo členského štátu, ktoré sa na nás vzťahuje a ktoré tiež stanovuje vhodné opatrenia na ochranu práv a slobôd a oprávnených záujmov dotknutej osoby, alebo (3) je to založené na výslovnom súhlase dotknutej osoby.

V prípadoch uvedených v článku 22 ods. 2 písm. a) a c) GDPR vykonáme vhodné opatrenia na ochranu práv a slobôd a oprávnených záujmov dotknutej osoby. V týchto prípadoch máte právo na ľudský zásah zo strany prevádzkovateľa, na vyjadrenie svojho názoru a na napadnutie rozhodnutia.

Významné informácie o príslušnej logike, ako aj o význame a predpokladaných dôsledkoch takéhoto spracúvania údajov pre dotknutú osobu sú uvedené v našich zásadách ochrany osobných údajov.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## III. EU-U.S. Data Privacy Framework (EU-U.S. DPF), UK Extension to the EU-U.S. DPF, Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF)

Ak je naša organizácia certifikovaným členom EU-U.S. Data Privacy Framework (EU-U.S. DPF) a/alebo UK Extension to the EU-U.S. DPF a/alebo Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF), platí nasledovné:

Dodržiavame EU-U.S. Data Privacy Framework (EU-U.S. DPF) a UK Extension to the EU-U.S. DPF ako aj Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF), ako to stanovilo U.S. Department of Commerce. Naša spoločnosť potvrdila americkému ministerstvu obchodu, že dodržiava EU-U.S. Data Privacy Framework Principles (EU-U.S. DPF Principles) v súvislosti so spracovaním osobných údajov, ktoré prijíma z Európskej únie a Spojeného kráľovstva na základe EU-U.S. DPF a UK Extension to the EU-U.S. DPF. Naša spoločnosť potvrdila americkému ministerstvu obchodu, že dodržiava Swiss-U.S. Data Privacy Framework Principles (Swiss-U.S. DPF Principles) v súvislosti so spracovaním osobných údajov, ktoré prijíma zo Švajčiarska na základe Swiss-U.S. DPF. V prípade rozporu medzi ustanoveniami našej politiky ochrany osobných údajov a EU-U.S. DPF Principles a/alebo Swiss-U.S. DPF Principles sú Principles rozhodujúce.

Pre viac informácií o programe Data Privacy Framework (DPF) a pre zobrazenie našej certifikácie navštívte prosím https://www.dataprivacyframework.gov/.

Ostatné americké jednotky alebo dcérske spoločnosti našej spoločnosti, ktoré tiež dodržiavajú EU-U.S. DPF Principals, vrátane UK Extension to the EU-U.S. DPF a Swiss-U.S. DPF Principals, ak existujú, sú uvedené v našom vyhlásení o ochrane osobných údajov.

V súlade s EU-U.S. DPF a UK Extension to the EU-U.S. DPF a Swiss-U.S. DPF sa naša spoločnosť zaväzuje spolupracovať s orgánom zriadeným európskymi orgánmi pre ochranu údajov a britským úradom pre informácie (ICO) a švajčiarskym Federálnym komisárom pre ochranu údajov a informácie (EDÖB) a dodržiavať ich odporúčania ohľadom nevyriešených sťažností na naše zaobchádzanie s osobnými údajmi, ktoré sme prijali na základe EU-U.S. DPF a UK Extension to the EU-U.S. DPF a Swiss-U.S. DPF.

Informujeme dotknuté osoby o príslušných európskych orgánoch pre ochranu údajov, ktoré sú zodpovedné za riešenie sťažností na zaobchádzanie našej organizácie s osobnými údajmi, v hornej časti tohto dokumentu o transparentnosti a o tom, že dotknutým osobám poskytujeme primeraný a bezplatný právny prostriedok.

Informujeme všetky dotknuté osoby, že naša spoločnosť podlieha vyšetrovacím a presadzovacím právomociam Federal Trade Commission (FTC).

Dotknuté osoby majú za určitých podmienok možnosť požiadať o záväzné rozhodcovské konanie. Naša organizácia je povinná riešiť nároky a dodržiavať podmienky podľa Prílohy I k DPF-Principals, ak


© All rights reserved by Heiko Maniero.

dotknutá osoba požiadala o záväzné rozhodcovské konanie tým, že informovala našu organizáciu a boli dodržané postupy a podmienky podľa Prílohy I k Principals.

Týmto informujeme všetky dotknuté osoby o zodpovednosti našej organizácie v prípade odovzdania osobných údajov tretím stranám.

Pre otázky dotknutých osôb alebo orgánov na ochranu údajov sme v tomto dokumente o transparentnosti uviedli miestnych zástupcov.

Ponúkame vám možnosť vybrať si (Opt-out), či sa vaše osobné údaje (i) odovzdajú tretím stranám alebo (ii) použijú na účel, ktorý sa podstatne líši od účelu/účelov, na ktoré boli pôvodne zhromaždené alebo neskôr schválené vami. Jasný, dobre viditeľný a ľahko prístupný mechanizmus na uplatnenie vášho výberu spočíva v tom, že kontaktujete nášho zodpovedného pracovníka pre ochranu údajov (DSB) e-mailom. Nemáte možnosť výberu a nie sme povinní to urobiť, ak sa údaje odovzdajú tretej strane, ktorá koná ako zástupca alebo spracovateľ v našom mene a podľa našich pokynov. Vždy však uzatvoríme zmluvu s takýmto zástupcom alebo spracovateľom.

Pre citlivé údaje (t. j. osobné údaje, ktoré obsahujú informácie o zdravotnom stave, rasovom alebo etnickom pôvode, politických názoroch, náboženských alebo filozofických presvedčeniach, členstve v odbore alebo informácie o sexuálnom živote dotknutej osoby) získavame váš výslovný súhlas (Opt-in), keď sa tieto údaje (i) odovzdajú tretím stranám alebo (ii) použijú na iný účel, ako na ktorý boli pôvodne zhromaždené alebo na ktorý ste neskôr dali svoj súhlas tým, že ste si vybrali možnosť Opt-in. Navyše, všetky osobné údaje, ktoré prijmeme od tretích strán, považujeme za citlivé, ak ich tretia strana identifikovala a spracovala ako také.

Týmto vás informujeme o požiadavke na zverejnenie osobných údajov ako reakcie na zákonné požiadavky orgánov, vrátane splnenia požiadaviek národnej bezpečnosti alebo trestného stíhania.

Pri prenose osobných údajov tretej strane, ktorá koná ako zodpovedná osoba, dodržiavame Principals oznamovania a voľby. Okrem toho uzatvárame zmluvu s treťou stranou, ktorá je zodpovedná za spracovanie, ktorá stanovuje, že tieto údaje sa môžu spracúvať len pre obmedzené a určené účely v súlade so súhlasom, ktorý ste poskytli, a že príjemca musí poskytnúť rovnakú úroveň ochrany ako Principals DPF a informovať nás, ak zistí, že už nemôže splniť túto povinnosť. Zmluva predpokladá, že treťa strana, ktorá je zodpovednou osobou, zastaví spracovanie alebo prijme iné primerané a vhodné opatrenia na nápravu, ak sa takéto zistenie urobí.

Pri prenose osobných údajov tretej strane, ktorá koná ako zástupca alebo spracovateľ, (i) prenášame tieto údaje iba pre obmedzené a určené účely; (ii) zabezpečujeme, aby zástupca alebo spracovateľ bol povinný poskytovať aspoň rovnakú úroveň ochrany údajov, ako vyžadujú DPF-Principals; (iii) prijímame primerané a vhodné opatrenia, aby sme zabezpečili, že zástupca alebo spracovateľ skutočne spracováva prenesené osobné údaje spôsobom, ktorý je v súlade s našimi záväzkami podľa DPF-Principals; (iv) vyžadujeme od zástupcu alebo spracovateľa, aby nás informoval, ak zistí, že už nemôže poskytovať rovnakú úroveň ochrany, ako predpokladajú DPF-Principals; (v) po takomto oznámení, vrátane pod (iv),


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

prijímame primerané a vhodné kroky na zastavenie neoprávneného spracovania a na nápravu; a (vi) na požiadanie DPF Department poskytujeme súhrn alebo reprezentatívny príklad relevantných ustanovení o ochrane údajov z našej zmluvy s týmto zástupcom.

V súlade s EU-U.S. DPF a/alebo UK Extension to the EU-U.S. DPF a/alebo Swiss-U.S. DPF sa naša organizácia zaväzuje spolupracovať s orgánom, ktorý zriadili orgány EU pre ochranu údajov a britský úrad pre informácie (ICO) alebo švajčiarsky federálny komisár pre ochranu údajov a informácie (EDÖB), a dodržiavať ich odporúčania týkajúce sa nevyriešených sťažností na naše zaobchádzanie s osobnými údajmi, ktoré sme prijali v súvislosti s pracovným pomerom na základe EU-U.S. DPF a UK Extension to the EU-U.S. DPF a Swiss-U.S. DPF.

Všetky dotknuté osoby, ktoré sa dočasne nachádzajú v Európskej únii (EÚ), Európskom hospodárskom priestore (EHP) alebo v Spojenom kráľovstve, alebo ktoré tam majú bydlisko alebo obvyklý pobyt, majú nárok na práva a oprávnenia dotknutých osôb, ktoré sú zverejnené v našom dokumente o transparentnosti a ktoré vyplývajú aj z článkov 15 až 22 GDPR, vrátane práva na prístup k osobným údajom. Tieto informácie sme sprístupnili vo všetkých jazykoch EÚ a EHP. Anglická jazyková verzia sa vzťahuje na Spojené kráľovstvo.

Všetky dotknuté osoby, ktoré majú dočasný pobyt vo Švajčiarsku alebo tam majú bydlisko alebo obvyklý pobyt, majú nárok na práva a oprávnenia dotknutých osôb podľa švajčiarskeho zákona o ochrane údajov (DPA) a švajčiarskeho nariadenia o ochrane údajov (DPR), ktoré sú uverejnené v našom dokumente o transparentnosti, vrátane práva na prístup k osobným údajom. Tieto informácie sme poskytli v troch úradných jazykoch Švajčiarska (nemecky, taliansky a francúzsky).


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

# PORTUGUESE: Informação sobre o Processamento de Dados Pessoais (Artigo 13, 14 GDPR)

Caro Senhor ou Senhora,

Os dados pessoais de cada indivíduo que se encontra numa relação contratual, pré-contratual ou outra com a nossa empresa merecem uma protecção especial. O nosso objectivo é manter o nosso nível de protecção de dados a um nível elevado. Por conseguinte, estamos rotineiramente a desenvolver os nossos conceitos de protecção de dados e segurança de dados.

Obviamente, cumprimos as disposições estatutárias sobre protecção de dados. De acordo com o Artigo 13, 14 GDPR, os responsáveis pelo tratamento cumprem requisitos específicos de informação ao recolherem dados pessoais. O presente documento cumpre estas obrigações.

A terminologia dos regulamentos legais é complicada. Infelizmente, o uso de termos legais não pôde ser dispensado na preparação deste documento. Por conseguinte, gostaríamos de salientar que é sempre bem-vindo a contactar-nos para todas as questões relativas a este documento, os termos ou formulações utilizados.

## I. Informações a facultar quando os dados pessoais são recolhidos junto do titular (Artigo 13º do GDPR)

### A. A identidade e os contactos do responsável pelo tratamento e, se for caso disso, do seu representante (Artigo 13(1) aceso a GDPR)

Ver acima

### B. Os contactos do encarregado da proteção de dados, se for caso disso (Artigo 13(1) aceso b GDPR)

Ver acima

### C. As finalidades do tratamento a que os dados pessoais se destinam, bem como o fundamento jurídico para o tratamento (Artigo 13(1) aceso c GDPR)

A finalidade do tratamento de dados pessoais é o tratamento de todas as operações que dizem respeito ao responsável pelo tratamento, clientes, potenciais clientes, parceiros comerciais ou outras relações


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

contratuais ou pré-contratuais entre os grupos designados (no sentido mais lato) ou obrigações legais do responsável pelo tratamento.

Arte. 6(1) aceso a GDPR serve como base legal para operações de processamento para as quais obtemos consentimento para um fim de processamento específico. Se o tratamento de dados pessoais for necessário para a execução de um contrato em que a pessoa em causa é parte, como é o caso, por exemplo, quando as operações de tratamento são necessárias para o fornecimento de bens ou para a prestação de qualquer outro serviço, o tratamento é baseado no Artigo 6(1) aceso. b GDPR. O mesmo se aplica a tais operações de tratamento que são necessárias para a realização de medidas pré-contratuais, por exemplo no caso de inquéritos relativos aos nossos produtos ou serviços. A nossa empresa está sujeita a uma obrigação legal pela qual o processamento de dados pessoais é necessário, tal como para o cumprimento de obrigações fiscais, o processamento é baseado no Artigo 6. 6(1) aceso c GDPR.

Em casos raros, o tratamento de dados pessoais pode ser necessário para proteger os interesses vitais do titular dos dados ou de outra pessoa singular. Este seria o caso, por exemplo, se um visitante fosse ferido na nossa empresa e o seu nome, idade, dados de seguro de saúde ou outras informações vitais tivessem de ser transmitidas a um médico, hospital ou outro terceiro. O processamento seria então baseado na Arte. 6(1) aceso d GDPR.

Se o tratamento for necessário para o desempenho de uma tarefa de interesse público ou para o exercício da autoridade pública de que está investido o responsável pelo tratamento, a base jurídica é o Art. 6(1) lit. e GDPR.

Finalmente, as operações de processamento poderiam basear-se no Artigo 6(1) aceso f GDPR. Esta base jurídica é utilizada para operações de tratamento não abrangidas por nenhum dos fundamentos jurídicos acima mencionados, se o tratamento for necessário para os fins dos interesses legítimos prosseguidos pela nossa empresa ou por terceiros, excepto se tais interesses forem anulados pelos interesses ou direitos e liberdades fundamentais da pessoa em causa que exigem a protecção de dados pessoais. Tais operações de tratamento são particularmente admissíveis porque foram especificamente mencionadas pelo legislador europeu. Ele considerou que um interesse legítimo pode ser assumido se a pessoa em causa for cliente do responsável pelo tratamento (Considerando 47 Sentença 2 GDPR).

## D. Se o tratamento dos dados se basear no Artigo 6.o, n.o 1, alínea f), os interesses legítimos do responsável pelo tratamento ou de um terceiro (Artigo 13(1) aceso d GDPR)

Quando o tratamento de dados pessoais se baseia no Artigo 6(1) aceso. f GDPR o nosso interesse legítimo é realizar o nosso negócio em favor do bem-estar de todos os nossos empregados e dos accionistas.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## E. Os destinatários ou categorias de destinatários dos dados pessoais, se os houver (Artigo 13(1) aceso e GDPR)

Autoridades públicas

Organismos externos

Outros organismos externos

Processamento interno

Processamento intragrupo

Outros organismos

Uma lista dos nossos subcontratantes e destinatários de dados em países terceiros e, se aplicável, de organizações internacionais está publicada no nosso sítio Web ou pode ser-nos solicitada gratuitamente. Para solicitar esta lista, contacte o nosso responsável pela proteção de dados.

## F. Se for caso disso, o facto de o responsável pelo tratamento tencionar transferir dados pessoais para um país terceiro ou uma organização internacional, e a existência ou não de uma decisão de adequação adotada pela Comissão ou, no caso das transferências mencionadas nos Artigos 46.o ou 47.o, ou no Artigo 49.o, n.o 1, segundo parágrafo, a referência às garantias apropriadas ou adequadas e aos meios de obter cópia das mesmas, ou onde foram disponibilizadas (Artigo 13(1) aceso f, 46(1), 46(2) aceso c GDPR)

Todas as empresas e sucursais que fazem parte do nosso grupo (doravante referidas como "empresas do grupo") que tenham o seu local de actividade ou um escritório num país terceiro podem pertencer aos destinatários dos dados pessoais. Uma lista de todas as empresas ou destinatários do grupo pode ser-nos solicitada.

Nos termos do n.o 1 do Artigo 46.o da GDPR, um responsável pelo tratamento ou processador só pode transferir dados pessoais para um país terceiro se o responsável pelo tratamento ou processador tiver fornecido garantias adequadas, e na condição de estarem disponíveis direitos executórios para as pessoas em causa e recursos legais eficazes para as mesmas. Podem ser previstas salvaguardas adequadas sem necessidade de qualquer autorização específica de uma autoridade de controlo, através de cláusulas contratuais-tipo, Artigo 46(2) aceso. c GDPR.

As cláusulas contratuais-tipo da União Europeia ou outras salvaguardas apropriadas são acordadas com todos os destinatários de países terceiros antes da primeira transmissão de dados pessoais.


© All rights reserved by Heiko Maniero.

Consequentemente, é garantido que as garantias adequadas, os direitos executórios do titular dos dados e os recursos legais eficazes para o mesmo são garantidos. Todos os titulares dos dados podem obter uma cópia das cláusulas contratuais-tipo da nossa parte. As cláusulas contratuais-tipo estão também disponíveis no Jornal Oficial da União Europeia.

O artigo 45.º, n.º 3, do Regulamento Geral sobre a Proteção de Dados (RGPD) confere à Comissão Europeia o poder de decidir, através de um ato de execução, que um país terceiro assegura um nível de proteção adequado. Isto significa um nível de proteção dos dados pessoais que é essencialmente equivalente ao nível de proteção na UE. O efeito das decisões de adequação é que os dados pessoais podem circular livremente da UE (e da Noruega, Liechtenstein e Islândia) para um país terceiro sem mais obstáculos. Existem regras semelhantes para o Reino Unido, a Suíça e alguns outros países.

Sempre que a Comissão Europeia ou o governo de outro país decidir que um país terceiro assegura um nível de proteção adequado e existir um quadro válido (por exemplo, EU-U.S. Data Privacy Framework, Swiss-U.S. Data Privacy Framework, UK Extension to the EU-U.S. Data Privacy Framework), todas as transferências efectuadas por nós para os membros desses quadros (por exemplo, entidades autocertificadas) baseiam-se exclusivamente na adesão dessas entidades ao respetivo quadro. Quando nós ou uma das entidades do nosso grupo for membro de tal quadro, todas as transferências para nós ou para a entidade do nosso grupo baseiam-se exclusivamente na adesão da entidade a esse quadro.

Qualquer pessoa a quem os dados digam respeito pode obter uma cópia dos quadros de referência junto de nós. Além disso, os quadros também estão disponíveis no Jornal Oficial da União Europeia ou nos materiais jurídicos publicados ou nos sítios Web das autoridades de controlo ou de outras autoridades ou instituições competentes.

## G. Prazo de conservação dos dados pessoais ou, se não for possível, os critérios usados para definir esse prazo (Artigo 13(2) aceso a GDPR)

O critério utilizado para determinar o período de armazenamento de dados pessoais é o respectivo período de retenção legal. Após o termo desse período, os dados correspondentes são rotineiramente apagados, desde que já não sejam necessários para o cumprimento do contrato ou para o início de um contrato.

Se não existir um período de conservação legal, o critério é o período de conservação contratual ou interno.


© All rights reserved by Heiko Maniero.

## H. A existência do direito de solicitar ao responsável pelo tratamento acesso aos dados pessoais que lhe digam respeito, bem como a sua retificação ou o seu apagamento, e a limitação do tratamento no que disser respeito ao titular dos dados, ou do direito de se opor ao tratamento, bem como do direito à portabilidade dos dados (Artigo 13(2) aceso. b GDPR)

Todos os titulares dos dados têm os seguintes direitos:

***Direito de acesso***

Cada pessoa interessada tem o direito de aceder aos dados pessoais que lhe dizem respeito. O direito de acesso estende-se a todos os dados por nós processados. O direito pode ser exercido facilmente e a intervalos razoáveis, a fim de se conhecer e verificar a legalidade do tratamento (Considerando 63 GDPR). Este direito resulta da Arte. 15 GDPR. O titular dos dados pode contactar-nos para exercer o direito de acesso.

***Direito à rectificação***

De acordo com o Artigo 16 Sentença 1 GDPR, a pessoa em causa tem o direito de obter do responsável pelo tratamento, sem atrasos indevidos, a rectificação de dados pessoais inexactos que lhe digam respeito. Além disso, a frase 2 do Artigo 16º da GDPR prevê que a pessoa em causa tem o direito, tendo em conta as finalidades do tratamento, de ver completados dados pessoais incompletos, inclusive mediante a apresentação de uma declaração suplementar. A pessoa em causa pode contactar-nos para exercer o direito de rectificação.

***Direito ao apagamento (direito a ser esquecido)***

Além disso, as pessoas em causa têm direito a um direito de apagamento e a serem esquecidas ao abrigo da Arte. 17 GDPR. Este direito também pode ser exercido contactando-nos. Neste ponto, contudo, gostaríamos de salientar que este direito não se aplica na medida em que o processamento seja necessário para cumprir uma obrigação legal a que a nossa empresa está sujeita, Artigo 17(3) aceso. b GDPR. Isto significa que só podemos aprovar um pedido de eliminação após o termo do período de retenção legal.

***Direito à restrição do processamento***

De acordo com o Artigo 18 GDPR, qualquer pessoa tem direito a uma restrição do tratamento de dados. A restrição do tratamento pode ser exigida se uma das condições estabelecidas no Artigo 18(1) aceso a-d GDPR for cumprida. A pessoa em causa pode contactar-nos para exercer o direito à restrição do tratamento.

***Direito de objecção***

Além disso, Arte. 21 GDPR garante o direito de objecção. O titular dos dados pode contactar-nos para exercer o direito de oposição.


© All rights reserved by Heiko Maniero.

***Direito à portabilidade dos dados***

Arte. 20 GDPR concede ao sujeito dos dados o direito à portabilidade dos dados. Nos termos desta disposição, a pessoa em causa tem, nas condições estabelecidas no n.º 1 do Artigo 20º iluminado a e b GDPR, o direito de receber os dados pessoais que lhe digam respeito, que tenha fornecido a um responsável pelo tratamento, num formato estruturado, comummente utilizado e legível por máquina, e tem o direito de transmitir esses dados a outro responsável pelo tratamento sem impedimento por parte do responsável pelo tratamento ao qual os dados pessoais tenham sido fornecidos. O titular dos dados pode contactar-nos para exercer o direito à portabilidade dos dados.

## I. Se o tratamento dos dados se basear no Artigo 6.o, n.o 1, alínea a), ou no Artigo 9.o, n.o 2, alínea a), a existência do direito de retirar consentimento em qualquer altura, sem comprometer a licitude do tratamento efetuado com base no consentimento previamente dado (Artigo 13(2) aceso c GDPR)

Se o tratamento de dados pessoais se basear na Arte. 6(1) aceso a GDPR, que é o caso, se a pessoa em causa tiver dado consentimento para o tratamento de dados pessoais para um ou mais fins específicos ou se se basear no Artigo 9(2) aceso a GDPR, que regula o consentimento explícito para o tratamento de categorias especiais de dados pessoais, a pessoa em causa tem, de acordo com o Artigo 7(3) Sentença 1 GDPR, o direito de retirar o seu consentimento em qualquer altura.

A retirada do consentimento não afecta a legalidade do processamento baseado no consentimento antes da sua retirada, Artigo 7(3) Sentença 2 GDPR. Será tão fácil retirar o consentimento como dar o consentimento, Art. 7(3) Sentença 4 GDPR. Por conseguinte, a retirada do consentimento pode sempre ter lugar da mesma forma que o consentimento foi dado ou de qualquer outra forma, que seja considerada mais simples pela pessoa a quem os dados dizem respeito. Na sociedade de informação de hoje, provavelmente a forma mais simples de retirar o consentimento é um simples correio electrónico. Se o titular dos dados desejar retirar o seu consentimento que nos foi concedido, basta um simples correio electrónico para nós. Em alternativa, o titular dos dados pode escolher qualquer outra forma de nos comunicar a sua retirada de consentimento.

## J. O direito de apresentar reclamação a uma autoridade de controlo (Artigo 13(2) aceso d, 77(1) GDPR)

Como responsável pelo tratamento, somos obrigados a notificar a pessoa em causa do direito de apresentar uma queixa a uma autoridade de controlo, Artigo 13(2) aceso d GDPR. O direito de apresentar uma queixa junto de uma autoridade de controlo é regulado pelo Artigo 77(1) GDPR. Nos termos desta disposição, sem prejuízo de qualquer outro recurso administrativo ou judicial, qualquer pessoa em causa terá o direito de apresentar queixa a uma autoridade de controlo, em particular no Estado-Membro da sua residência habitual, local de trabalho ou local da alegada infracção, se a pessoa


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

em causa considerar que o tratamento dos dados pessoais que lhe dizem respeito viola o Regulamento Geral sobre Protecção de Dados. O direito de apresentar uma queixa a uma autoridade de controlo só foi limitado pela lei da União de tal forma, que só pode ser exercido perante uma única autoridade de controlo (Considerando 141 Sentença 1 GDPR). Esta regra destina-se a evitar reclamações duplas da mesma pessoa em relação ao mesmo assunto. Se uma pessoa em causa quiser apresentar uma queixa sobre nós, pedimos, portanto, para contactar apenas uma única autoridade de controlo.

## K. Se a comunicação de dados pessoais constitui ou não uma obrigação legal ou contratual, ou um requisito necessário para celebrar um contrato, bem como se o titular está obrigado a fornecer os dados pessoais e as eventuais consequências de não fornecer esses dados (Art. 13(2) aceso e GDPR)

Esclarecemos que o fornecimento de dados pessoais é em parte exigido por lei (por exemplo, regulamentos fiscais) ou pode também resultar de disposições contratuais (por exemplo, informações sobre o parceiro contratual).

Por vezes pode ser necessário celebrar um contrato que a pessoa em causa nos forneça dados pessoais, os quais devem ser posteriormente tratados por nós. O titular dos dados é, por exemplo, obrigado a fornecer-nos dados pessoais quando a nossa empresa assina um contrato com ele. O não fornecimento dos dados pessoais teria como consequência que o contrato com o titular dos dados não poderia ser celebrado.

Antes de os dados pessoais serem fornecidos pela pessoa em causa, a pessoa em causa deve contactar-nos. Esclarecemos ao titular dos dados se o fornecimento dos dados pessoais é exigido por lei ou contrato ou é necessário para a celebração do contrato, se existe uma obrigação de fornecer os dados pessoais e as consequências da não prestação dos dados pessoais.

## L. A existência de decisões automatizadas, incluindo a definição de perfis, referida no Artigo 22.o, n.os 1 e 4, e, pelo menos nesses casos, informações úteis relativas à lógica subjacente, bem como a importância e as consequências previstas de tal tratamento para o titular dos dados (Artigo 13(2) aceso f GDPR)

Como empresa responsável, normalmente não utilizamos decisões automatizadas ou definição de perfis. Se, em casos excepcionais, procedermos a decisões ou perfis automatizados, informaremos a pessoa em causa separadamente ou através de uma subsecção na nossa política de privacidade (no nosso sítio Web). Neste caso, aplica-se o seguinte:

A tomada de decisões automatizada - incluindo a definição de perfis - pode ocorrer se (1) for necessária para a celebração ou execução de um contrato entre o titular dos dados e nós, ou (2) for autorizada pela legislação da União ou do Estado-Membro a que estamos sujeitos e que também estabelece medidas


© All rights reserved by Heiko Maniero.

adequadas para salvaguardar os direitos e liberdades e os interesses legítimos do titular dos dados; ou (3) se for baseada no consentimento explícito do titular dos dados.

Nos casos referidos no artigo 22.º, n.º 2, alíneas a) e c) do RGPD, implementaremos medidas adequadas para salvaguardar os direitos e liberdades e os interesses legítimos da pessoa em causa. Nestes casos, o utilizador tem o direito de obter intervenção humana por parte do responsável pelo tratamento, de expressar o seu ponto de vista e de contestar a decisão.

A nossa política de privacidade contém informações significativas sobre a lógica envolvida, bem como sobre o significado e as consequências previstas de tal processamento para a pessoa em causa.

## II. Informações a facultar quando os dados pessoais não são recolhidos junto do titular (Artigo 14 GDPR)

### A. A identidade e os contactos do responsável pelo tratamento e, se for caso disso, do seu representante (Artigo 14(1) aceso a GDPR)

Ver acima

### B. Os contactos do encarregado da proteção de dados, se for caso disso (Artigo 14(1) aceso b GDPR)

Ver acima

### C. As finalidades do tratamento a que os dados pessoais se destinam, bem como o fundamento jurídico para o tratamento (Artigo 14(1) aceso c GDPR)

A finalidade do tratamento de dados pessoais é o tratamento de todas as operações que dizem respeito ao responsável pelo tratamento, clientes, potenciais clientes, parceiros comerciais ou outras relações contratuais ou pré-contratuais entre os grupos designados (no sentido mais lato) ou obrigações legais do responsável pelo tratamento.

Se o tratamento de dados pessoais for necessário para a execução de um contrato em que a pessoa em causa é parte, como é o caso, por exemplo, quando as operações de tratamento são necessárias para o fornecimento de bens ou para prestar qualquer outro serviço, o tratamento é baseado no Artigo 6(1) aceso b GDPR. O mesmo se aplica a tais operações de tratamento que são necessárias para a realização de medidas pré-contratuais, por exemplo no caso de inquéritos relativos aos nossos produtos ou serviços. A nossa empresa está sujeita a uma obrigação legal pela qual o processamento de dados


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

pessoais é necessário, tal como para o cumprimento de obrigações fiscais, o processamento é baseado no Artigo 6. 6(1) aceso c GDPR.

Em casos raros, o tratamento de dados pessoais pode ser necessário para proteger os interesses vitais do titular dos dados ou de outra pessoa singular. Este seria o caso, por exemplo, se um visitante fosse ferido na nossa empresa e o seu nome, idade, dados de seguro de saúde ou outras informações vitais tivessem de ser transmitidas a um médico, hospital ou outro terceiro. O processamento seria então baseado na Arte. 6(1) aceso d GDPR.

Se o tratamento for necessário para o desempenho de uma tarefa de interesse público ou para o exercício da autoridade pública de que está investido o responsável pelo tratamento, a base jurídica é o Art. 6(1) lit. e GDPR.

Finalmente, as operações de processamento poderiam basear-se no Artigo 6(1) aceso f GDPR. Esta base jurídica é utilizada para operações de tratamento não abrangidas por nenhum dos fundamentos jurídicos acima mencionados, se o tratamento for necessário para os fins dos interesses legítimos prosseguidos pela nossa empresa ou por terceiros, excepto se tais interesses forem anulados pelos interesses ou direitos e liberdades fundamentais da pessoa em causa que exigem a protecção de dados pessoais. Tais operações de tratamento são particularmente admissíveis porque foram especificamente mencionadas pelo legislador europeu. Ele considerou que um interesse legítimo pode ser assumido se a pessoa em causa for cliente do responsável pelo tratamento (Considerando 47 Sentença 2 GDPR).

## D. As categorias dos dados pessoais em questão (Artigo 14(1) aceso d GDPR)

Dados do cliente

Dados de potenciais clientes

Dados dos empregados

Dados dos fornecedores

## E. Os destinatários ou categorias de destinatários dos dados pessoais, se os houver (Artigo 14(1) aceso e GDPR)

Autoridades públicas

Organismos externos

Outros organismos externos


© All rights reserved by Heiko Maniero.

Processamento interno

Processamento intragrupo

Outros organismos

Uma lista dos nossos subcontratantes e destinatários de dados em países terceiros e, se aplicável, de organizações internacionais está publicada no nosso sítio Web ou pode ser-nos solicitada gratuitamente. Para solicitar esta lista, contacte o nosso responsável pela proteção de dados.

## F. Se for caso disso, o facto de o responsável pelo tratamento tencionar transferir dados pessoais para um país terceiro ou uma organização internacional, e a existência ou não de uma decisão de adequação adotada pela Comissão ou, no caso das transferências mencionadas nos artigos 46.o ou 47.o, ou no artigo 49.o, n.o 1, segundo parágrafo, a referência às garantias apropriadas ou adequadas e aos meios de obter cópia das mesmas, ou onde foram disponibilizadas (Artigo 14(1) aceso f, 46(1), 46(2) aceso c GDPR)

Todas as empresas e sucursais que fazem parte do nosso grupo (doravante referidas como "empresas do grupo") que tenham o seu local de actividade ou um escritório num país terceiro podem pertencer aos destinatários dos dados pessoais. Uma lista de todas as empresas do grupo pode ser-nos solicitada.

Nos termos do n.o 1 do Artigo 46.o da GDPR, um responsável pelo tratamento ou processador só pode transferir dados pessoais para um país terceiro se o responsável pelo tratamento ou processador tiver fornecido garantias adequadas, e na condição de estarem disponíveis direitos executórios para as pessoas em causa e recursos legais eficazes para as mesmas. Podem ser previstas salvaguardas adequadas sem necessidade de qualquer autorização específica de uma autoridade de controlo, através de cláusulas-tipo de protecção de dados, Artigo 46(2) aceso. c GDPR.

As cláusulas contratuais-tipo da União Europeia ou outras salvaguardas apropriadas são acordadas com todos os destinatários de países terceiros antes da primeira transmissão de dados pessoais. Consequentemente, é garantido que as garantias adequadas, os direitos executórios do titular dos dados e os recursos legais eficazes para o mesmo são garantidos. Todos os titulares dos dados podem obter uma cópia das cláusulas contratuais-tipo da nossa parte. As cláusulas contratuais-tipo estão também disponíveis no Jornal Oficial da União Europeia.

O artigo 45.º, n.º 3, do Regulamento Geral sobre a Proteção de Dados (RGPD) confere à Comissão Europeia o poder de decidir, através de um ato de execução, que um país terceiro assegura um nível de proteção adequado. Isto significa um nível de proteção dos dados pessoais que é essencialmente equivalente ao nível de proteção na UE. O efeito das decisões de adequação é que os dados pessoais


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

podem circular livremente da UE (e da Noruega, Liechtenstein e Islândia) para um país terceiro sem mais obstáculos. Existem regras semelhantes para o Reino Unido, a Suíça e alguns outros países.

Sempre que a Comissão Europeia ou o governo de outro país decidir que um país terceiro assegura um nível de proteção adequado e existir um quadro válido (por exemplo, EU-U.S. Data Privacy Framework, Swiss-U.S. Data Privacy Framework, UK Extension to the EU-U.S. Data Privacy Framework), todas as transferências efectuadas por nós para os membros desses quadros (por exemplo, entidades autocertificadas) baseiam-se exclusivamente na adesão dessas entidades ao respetivo quadro. Quando nós ou uma das entidades do nosso grupo for membro de tal quadro, todas as transferências para nós ou para a entidade do nosso grupo baseiam-se exclusivamente na adesão da entidade a esse quadro.

Qualquer pessoa a quem os dados digam respeito pode obter uma cópia dos quadros de referência junto de nós. Além disso, os quadros também estão disponíveis no Jornal Oficial da União Europeia ou nos materiais jurídicos publicados ou nos sítios Web das autoridades de controlo ou de outras autoridades ou instituições competentes.

## G. Prazo de conservação dos dados pessoais ou, se não for possível, os critérios usados para fixar esse prazo (Artigo 14(2) aceso a GDPR)

O critério utilizado para determinar o período de armazenamento de dados pessoais é o respectivo período de retenção legal. Após o termo desse período, os dados correspondentes são rotineiramente apagados, desde que já não sejam necessários para o cumprimento do contrato ou para o início de um contrato.

Se não existir um período de conservação legal, o critério é o período de conservação contratual ou interno.

## H. Se o tratamento dos dados se basear no artigo 6.o, n.o 1, alínea f), os interesses legítimos do responsável pelo tratamento ou de um terceiro (Art. 14(2) aceso b GDPR)

Nos termos do n.º 1 do Artigo 6.º aceso f GDPR, o tratamento só será lícito se for necessário para os fins de interesses legítimos prosseguidos pelo responsável pelo tratamento ou por terceiros, excepto se tais interesses forem anulados pelos interesses ou direitos e liberdades fundamentais da pessoa em causa que exijam a protecção de dados pessoais. De acordo com o Considerando 47 Sentença 2 GDPR, poderá existir um interesse legítimo quando existe uma relação relevante e adequada entre a pessoa em causa e o responsável pelo tratamento, por exemplo, em situações em que a pessoa em causa é cliente do responsável pelo tratamento. Em todos os casos em que a nossa empresa processe dados pessoais com base no n.º 1 do Artigo 6. f GDPR, o nosso interesse legítimo é exercer a nossa actividade em prol do bem-estar de todos os nossos empregados e dos accionistas.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## I. A existência do direito de solicitar ao responsável pelo tratamento o acesso aos dados pessoais que lhe digam respeito, e a retificação ou o apagamento, ou a limitação do tratamentor no que disser respeito ao titular dos dados, e do direito de se opor ao tratamento, bem como do direito à portabilidade dos dados (Art. 14(2) aceso c GDPR)

Todos os titulares dos dados têm os seguintes direitos:

***Direito de acesso***

Cada pessoa interessada tem o direito de aceder aos dados pessoais que lhe dizem respeito. O direito de acesso estende-se a todos os dados por nós processados. O direito pode ser exercido facilmente e a intervalos razoáveis, a fim de se conhecer e verificar a legalidade do tratamento (Considerando 63 GDPR). Este direito resulta da Arte. 15 GDPR. O titular dos dados pode contactar-nos para exercer o direito de acesso.

***Direito à rectificação***

De acordo com o Artigo 16 Sentença 1 GDPR, a pessoa em causa tem o direito de obter do responsável pelo tratamento, sem atrasos indevidos, a rectificação de dados pessoais inexactos que lhe digam respeito. Além disso, a frase 2 do Artigo 16º da GDPR prevê que a pessoa em causa tem o direito, tendo em conta as finalidades do tratamento, de ver completados dados pessoais incompletos, inclusive mediante a apresentação de uma declaração suplementar. A pessoa em causa pode contactar-nos para exercer o direito de rectificação.

***Direito ao apagamento (direito a ser esquecido)***

Além disso, as pessoas em causa têm direito a um direito de apagamento e a serem esquecidas ao abrigo da Arte. 17 GDPR. Este direito também pode ser exercido contactando-nos. Neste ponto, contudo, gostaríamos de salientar que este direito não se aplica na medida em que o processamento seja necessário para cumprir uma obrigação legal a que a nossa empresa está sujeita, Artigo 17(3) aceso. b GDPR. Isto significa que só podemos aprovar um pedido de eliminação após o termo do período de retenção legal.

***Direito à restrição do processamento***

De acordo com o Artigo 18 GDPR qualquer pessoa tem direito à restrição do processamento de dados. A restrição do tratamento pode ser exigida se uma das condições estabelecidas no Artigo 18(1) aceso a-d GDPR for cumprida. A pessoa em causa pode contactar-nos para exercer o direito à restrição do tratamento.

***Direito de objecção***

Além disso, Arte. 21 GDPR garante o direito de objecção. O titular dos dados pode contactar-nos para exercer o direito de oposição.

***Direito à portabilidade dos dados***

Arte. 20 GDPR concede ao sujeito dos dados o direito à portabilidade dos dados. De acordo com esta disposição, a pessoa em causa tem, nas condições estabelecidas no n.º 1 do Artigo 20º aceso, a e b


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

GDPR, o direito de receber os dados pessoais que lhe digam respeito, que tenha fornecido a um responsável pelo tratamento, num formato estruturado, comummente utilizado e legível por máquina, e tem o direito de transmitir esses dados a outro responsável pelo tratamento sem impedimento por parte do responsável pelo tratamento ao qual os dados pessoais tenham sido fornecidos. O titular dos dados pode contactar-nos para exercer o direito à portabilidade dos dados.

## J. Se o tratamento dos dados se basear no artigo 6.o, n.o 1, alínea a), ou no artigo 9.o, n.o 2, alínea a), a existência do direito de retirar consentimento em qualquer altura, sem comprometer a licitude do tratamento efetuado com base no consentimento previamente dado (Art. 14(2) aceso d GDPR)

Se o tratamento de dados pessoais se basear na Arte. 6(1) aceso a GDPR, que é o caso, se a pessoa em causa tiver dado consentimento para o tratamento de dados pessoais para um ou mais fins específicos ou se se basear no Artigo 9(2) aceso a GDPR, que regula o consentimento explícito para o tratamento de categorias especiais de dados pessoais, a pessoa em causa tem, de acordo com o Artigo 7(3) Sentença 1 GDPR, o direito de retirar o seu consentimento em qualquer altura.

A retirada do consentimento não afecta a legalidade do processamento baseado no consentimento antes da sua retirada, Artigo 7(3) Sentença 2 GDPR. Será tão fácil de retirar como de dar o consentimento, Art. 7(3) Sentença 4 GDPR. Por conseguinte, a retirada do consentimento pode sempre ter lugar da mesma forma que o consentimento foi dado ou de qualquer outra forma, que seja considerada mais simples pela pessoa a quem os dados dizem respeito. Na sociedade de informação de hoje, provavelmente a forma mais simples de retirar o consentimento é um simples correio electrónico. Se o titular dos dados desejar retirar o seu consentimento que nos foi concedido, basta um simples correio electrónico para nós. Em alternativa, o titular dos dados pode escolher qualquer outra forma de nos comunicar a sua retirada de consentimento.

## K. O direito de apresentar reclamação a uma autoridade de controlo (Artigo 14(2) aceso e, 77(1) GDPR)

Como responsável pelo tratamento, somos obrigados a notificar a pessoa em causa do direito de apresentar uma queixa a uma autoridade de controlo, Artigo 14(2) aceso e GDPR. O direito de apresentar uma queixa a uma autoridade de controlo é regulado pelo Artigo 77(1) da GDPR. Nos termos desta disposição, sem prejuízo de qualquer outro recurso administrativo ou judicial, qualquer pessoa em causa terá o direito de apresentar queixa a uma autoridade de controlo, em particular no Estado-Membro da sua residência habitual, local de trabalho ou local da alegada infracção, se a pessoa em causa considerar que o tratamento dos dados pessoais que lhe dizem respeito viola o Regulamento Geral de Protecção de Dados. O direito de apresentar uma queixa a uma autoridade de controlo só foi limitado pela lei da União de tal forma, que só pode ser exercido perante uma única autoridade de controlo


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

(Considerando 141 Sentença 1 GDPR). Esta regra destina-se a evitar reclamações duplas da mesma pessoa em relação ao mesmo assunto. Se uma pessoa em causa quiser apresentar uma queixa sobre nós, pedimos, portanto, para contactar apenas uma única autoridade de controlo.

## L. A origem dos dados pessoais e, eventualmente, se provêm de fontes acessíveis ao público (Artigo 14(2) aceso f GDPR)

Em princípio, os dados pessoais são recolhidos directamente da pessoa em causa ou em cooperação com uma autoridade (por exemplo, a recuperação de dados de um registo oficial). Outros dados sobre as pessoas em causa são derivados de transferências de empresas do grupo. No contexto desta informação geral, a designação das fontes exactas de onde provêm os dados pessoais é impossível ou implicaria um esforço desproporcionado na acepção da Arte. 14(5) aceso b GDPR. Em princípio, não recolhemos dados pessoais a partir de fontes publicamente acessíveis.

Qualquer pessoa interessada pode contactar-nos em qualquer altura para obter informações mais detalhadas sobre as fontes exactas dos dados pessoais que lhe dizem respeito. Quando a origem dos dados pessoais não puder ser fornecida à pessoa em causa por terem sido utilizadas várias fontes, devem ser fornecidas informações gerais (Considerando 61 Sentença 4 GDPR).

## M. A existência de decisões automatizadas, incluindo a definição de perfis referida no artigo 22.o, n.os 1 e 4, e, pelo menos nesses casos, informações úteis relativas à lógica subjacente, bem como a importância e as consequências previstas de tal tratamento para o titular dos dados (Artigo 14 (2) aceso g GDPR)

Como empresa responsável, normalmente não utilizamos decisões automatizadas ou definição de perfis. Se, em casos excepcionais, procedermos a decisões ou perfis automatizados, informaremos a pessoa em causa separadamente ou através de uma subsecção na nossa política de privacidade (no nosso sítio Web). Neste caso, aplica-se o seguinte:

A tomada de decisões automatizada - incluindo a definição de perfis - pode ocorrer se (1) for necessária para a celebração ou execução de um contrato entre o titular dos dados e nós, ou (2) for autorizada pela legislação da União ou do Estado-Membro a que estamos sujeitos e que também estabelece medidas adequadas para salvaguardar os direitos e liberdades e os interesses legítimos do titular dos dados; ou (3) se for baseada no consentimento explícito do titular dos dados.

Nos casos referidos no artigo 22.º, n.º 2, alíneas a) e c) do RGPD, implementaremos medidas adequadas para salvaguardar os direitos e liberdades e os interesses legítimos da pessoa em causa. Nestes casos, o utilizador tem o direito de obter intervenção humana por parte do responsável pelo tratamento, de expressar o seu ponto de vista e de contestar a decisão.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

A nossa política de privacidade contém informações significativas sobre a lógica envolvida, bem como sobre o significado e as consequências previstas de tal processamento para a pessoa em causa.

## III. EU-U.S. Data Privacy Framework (EU-U.S. DPF), UK Extension to the EU-U.S. DPF, Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF)

Se a nossa organização for um membro certificado do EU-U.S. Data Privacy Framework (EU-U.S. DPF) e/ou da UK Extension to the EU-U.S. DPF e/ou do Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF), aplica-se o seguinte:

Cumprimos o EU-U.S. Data Privacy Framework (EU-U.S. DPF) e a UK Extension to the EU-U.S. DPF, bem como o Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF), conforme estabelecido pelo U.S. Department of Commerce. A nossa empresa confirmou ao Departamento de Comércio dos EUA que cumpre os EU-U.S. Data Privacy Framework Principles (EU-U.S. DPF Principles) no que diz respeito ao tratamento de dados pessoais recebidos da União Europeia e do Reino Unido, com base no EU-U.S. DPF e na UK Extension to the EU-U.S. DPF. A nossa empresa confirmou ao Departamento de Comércio dos EUA que cumpre os Swiss-U.S. Data Privacy Framework Principles (Swiss-U.S. DPF Principles) no que diz respeito ao tratamento de dados pessoais recebidos da Suíça com base no Swiss-U.S. DPF. Em caso de conflito entre as disposições da nossa política de privacidade e os EU-U.S. DPF Principles e/ou os Swiss-U.S. DPF Principles, os Principles prevalecem.

Para saber mais sobre o programa Data Privacy Framework (DPF) e para ver a nossa certificação, visite https://www.dataprivacyframework.gov/.

As outras unidades ou subsidiárias dos EUA da nossa empresa que também cumprem os EU-U.S. DPF Principals, incluindo a UK Extension to the EU-U.S. DPF e os Swiss-U.S. DPF Principals, se houver, são mencionadas na nossa política de privacidade.

Em conformidade com o EU-U.S. DPF e a UK Extension to the EU-U.S. DPF, bem como o Swiss-U.S. DPF, a nossa empresa compromete-se a colaborar com o painel estabelecido pelas autoridades de proteção de dados da UE e pelo Information Commissioner's Office (ICO) do Reino Unido, bem como pelo Comissário Federal para a Proteção de Dados e Informação (EDÖB) da Suíça, e a seguir os seus conselhos sobre reclamações não resolvidas relativas ao nosso tratamento de dados pessoais que recebemos com base no EU-U.S. DPF e na UK Extension to the EU-U.S. DPF e no Swiss-U.S. DPF.

Informamos as pessoas afetadas sobre as autoridades europeias de proteção de dados competentes, responsáveis pelo tratamento de reclamações sobre o tratamento de dados pessoais pela nossa organização, na parte superior deste documento de transparência e que oferecemos às pessoas afetadas um recurso adequado e gratuito.


© All rights reserved by Heiko Maniero.

Informamos todas as pessoas afetadas de que a nossa empresa está sujeita aos poderes de investigação e execução da Federal Trade Commission (FTC).

As pessoas afetadas têm, em determinadas circunstâncias, a possibilidade de recorrer à arbitragem vinculativa. A nossa organização é obrigada a resolver as reclamações e a cumprir as condições estabelecidas no Anexo I dos DPF-Principals, caso a pessoa afetada solicite uma arbitragem vinculativa, notificando a nossa organização e cumprindo os procedimentos e condições estabelecidos no Anexo I dos Principals.

Informamos por este meio todas as pessoas afetadas sobre a responsabilidade da nossa organização em caso de transferência de dados pessoais para terceiros.

Para perguntas das pessoas afetadas ou das autoridades de supervisão de dados, nomeamos os representantes locais mencionados acima neste documento de transparência.

Oferecemos-lhe a possibilidade de optar (Opt-out) por não ter os seus dados pessoais (i) transferidos para terceiros ou (ii) utilizados para um propósito que seja significativamente diferente do(s) propósito(s) para o qual/quais foram originalmente recolhidos ou posteriormente autorizados por si. O mecanismo claro, visível e de fácil acesso para exercer a sua escolha consiste em contactar o nosso Encarregado de Proteção de Dados (DPO) por e-mail. Não tem opção de escolha e não somos obrigados a fazê-lo se os dados forem transferidos para um terceiro que atue como agente ou processador em nosso nome e de acordo com as nossas instruções. No entanto, celebramos sempre um contrato com tal agente ou processador.

Para dados sensíveis (ou seja, dados pessoais que contenham informações sobre o estado de saúde, origem racial ou étnica, opiniões políticas, crenças religiosas ou filosóficas, filiação sindical ou informações sobre a vida sexual da pessoa em questão), obtemos o seu consentimento explícito (Opt-in) quando esses dados (i) são transferidos para terceiros ou (ii) são utilizados para um propósito diferente daquele para o qual foram originalmente recolhidos ou para o qual deu posteriormente o seu consentimento, escolhendo a opção Opt-in. Além disso, tratamos todos os dados pessoais que recebemos de terceiros como sensíveis, se o terceiro os identificar e tratar como sensíveis.

Informamos por este meio sobre a necessidade de divulgar dados pessoais em resposta a solicitações legais de autoridades, incluindo o cumprimento de requisitos de segurança nacional ou aplicação da lei.

Ao transferir dados pessoais para um terceiro que atue como controlador, cumprimos os Principals de notificação e escolha. Além disso, celebramos um contrato com o terceiro responsável pelo tratamento que prevê que esses dados só possam ser tratados para fins limitados e especificados, de acordo com o consentimento que deu, e que o destinatário deve fornecer o mesmo nível de proteção que os Principals do DPF e nos notificar se determinar que já não pode cumprir essa obrigação. O contrato prevê que o terceiro, responsável pelo tratamento, interrompa o tratamento ou tome outras medidas adequadas e apropriadas para corrigir a situação se essa determinação for feita.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

Ao transferir dados pessoais para um terceiro que atue como agente ou processador, (i) transferimos esses dados apenas para fins limitados e especificados; (ii) asseguramos que o agente ou processador é obrigado a fornecer pelo menos o mesmo nível de proteção de dados exigido pelos DPF-Principals; (iii) tomamos medidas adequadas e apropriadas para garantir que o agente ou processador realmente processa os dados pessoais transferidos de uma maneira que esteja em conformidade com as nossas obrigações de acordo com os DPF-Principals; (iv) exigimos que o agente ou processador notifique a nossa organização se determinar que já não pode cumprir a obrigação de fornecer o mesmo nível de proteção que os DPF-Principals prevêem; (v) após tal notificação, inclusive sob (iv), tomamos medidas adequadas e apropriadas para interromper o processamento não autorizado e corrigir a situação; e (vi) fornecemos ao DPF Department, mediante solicitação, um resumo ou um exemplar representativo das disposições relevantes de proteção de dados do nosso contrato com esse agente.

Em conformidade com o EU-U.S. DPF e/ou a UK Extension to the EU-U.S. DPF e/ou o Swiss-U.S. DPF, a nossa organização compromete-se a colaborar com o painel estabelecido pelas autoridades de proteção de dados da UE e pelo Information Commissioner's Office (ICO) do Reino Unido, bem como pelo Comissário Federal para a Proteção de Dados e Informação (EDÖB) da Suíça, e a seguir os seus conselhos sobre reclamações não resolvidas relativas ao nosso tratamento de dados pessoais recebidos no contexto da relação de trabalho, com base no EU-U.S. DPF e na UK Extension to the EU-U.S. DPF e no Swiss-U.S. DPF.

Todos os titulares de dados que se encontrem temporariamente na União Europeia (UE), no Espaço Económico Europeu (EEE) ou no Reino Unido, ou que aí tenham o seu domicílio ou residência habitual, têm direito aos direitos e aos direitos dos titulares de dados publicados no nosso Documento de Transparência, que também decorrem dos artigos 15º a 22º do RGPD, incluindo o direito de acesso aos dados pessoais. Disponibilizámos esta informação em todas as línguas da UE e do EEE. A versão em inglês aplica-se ao Reino Unido.

Todos os titulares de dados que residam temporariamente na Suíça ou que aí tenham o seu domicílio ou residência habitual beneficiam dos direitos e das prerrogativas dos titulares de dados ao abrigo da Lei de Proteção de Dados suíça (DPA) e do Regulamento de Proteção de Dados suíço (DPR), publicados no nosso Documento de Transparência, incluindo o direito de acesso aos dados pessoais. Disponibilizámos esta informação nas três línguas oficiais da Suíça (alemão, italiano e francês).


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

# PORTUGUESE: Informação sobre o Processamento de Dados Pessoais para Empregados e Candidatos (Artigo 13, 14 GDPR)

Caro Senhor ou Senhora,

Os dados pessoais dos empregados e candidatos merecem uma protecção especial. O nosso objectivo é manter o nosso nível de protecção de dados a um nível elevado. Por conseguinte, estamos rotineiramente a desenvolver os nossos conceitos de protecção de dados e segurança de dados.

Obviamente, cumprimos as disposições estatutárias sobre protecção de dados. De acordo com o Artigo 13, 14 GDPR, os responsáveis pelo tratamento cumprem os requisitos específicos de informação quando processam dados pessoais. O presente documento cumpre estas obrigações.

A terminologia da regulamentação legal é complicada. Infelizmente, o uso de termos legais não pôde ser dispensado na preparação deste documento. Por conseguinte, gostaríamos de salientar que é sempre bem-vindo a contactar-nos para todas as questões relativas a este documento, os termos utilizados ou formulações.

## I. Informações a facultar quando os dados pessoais são recolhidos junto do titular (Artigo 13º do GDPR)

### A. A identidade e os contactos do responsável pelo tratamento e, se for caso disso, do seu representante (Artigo 13(1) aceso a GDPR)

Ver acima

### B. Os contactos do encarregado da proteção de dados, se for caso disso (Artigo 13(1) aceso b GDPR)

Ver acima

### C. As finalidades do tratamento a que os dados pessoais se destinam, bem como o fundamento jurídico para o tratamento (Artigo 13(1) aceso c GDPR)

Para os dados do candidato, a finalidade do tratamento de dados é conduzir um exame da candidatura durante o processo de recrutamento. Para este efeito, processamos todos os dados fornecidos pelo


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

candidato. Com base nos dados submetidos durante o processo de recrutamento, verificaremos se é convidado para uma entrevista de emprego (parte do processo de selecção). No caso de candidatos geralmente adequados, em particular no contexto da entrevista de emprego, processamos alguns outros dados pessoais fornecidos pelo candidato, que são essenciais para a nossa decisão de selecção. Se for contratado por nós, os dados do candidato serão automaticamente transformados em dados do empregado. Como parte do processo de recrutamento, processaremos outros dados pessoais do candidato que lhe solicitarmos e que sejam necessários para iniciar ou cumprir o seu contrato (tais como números de identificação pessoal ou números de identificação fiscal). Para os dados do empregado, a finalidade do processamento de dados é a execução do contrato de trabalho ou o cumprimento de outras disposições legais aplicáveis à relação de trabalho (por exemplo, lei fiscal), bem como a utilização dos seus dados pessoais para executar o contrato de trabalho celebrado consigo (por exemplo, publicação do seu nome e das informações de contacto dentro da empresa ou aos clientes). Os dados dos empregados são armazenados após a cessação da relação de trabalho para cumprir os períodos legais de retenção.

A base jurídica para o processamento de dados é o Artigo 6(1) aceso b GDPR, Artigo 9(2) aceso b e h GDPR, Artigo 88(1) GDPR e legislação nacional, tal como para a Alemanha Secção 26 BDSG (Lei Federal de Protecção de Dados).

## D. Os destinatários ou categorias de destinatários dos dados pessoais, se os houver (Artigo 13(1) aceso e GDPR)

Autoridades públicas

Organismos externos

Outros organismos externos

Processamento interno

Processamento intragrupo

Outros organismos

Uma lista dos nossos subcontratantes e destinatários de dados em países terceiros e, se aplicável, de organizações internacionais está publicada no nosso sítio Web ou pode ser-nos solicitada gratuitamente. Para solicitar esta lista, contacte o nosso responsável pela proteção de dados.


© All rights reserved by Heiko Maniero.

## E. Se for caso disso, o facto de o responsável pelo tratamento tencionar transferir dados pessoais para um país terceiro ou uma organização internacional, e a existência ou não de uma decisão de adequação adotada pela Comissão ou, no caso das transferências mencionadas nos Artigos 46.o ou 47.o, ou no Artigo 49.o, n.o 1, segundo parágrafo, a referência às garantias apropriadas ou adequadas e aos meios de obter cópia das mesmas, ou onde foram disponibilizadas (Artigo 13(1) aceso f, 46(1), 46(2) aceso c GDPR)

Todas as empresas e sucursais que fazem parte do nosso grupo (doravante referidas como "empresas do grupo") que tenham o seu local de actividade ou um escritório num país terceiro podem pertencer aos destinatários dos dados pessoais. Uma lista de todas as empresas ou destinatários do grupo pode ser-nos solicitada.

Nos termos do n.o 1 do Artigo 46.o da GDPR, um responsável pelo tratamento ou processador só pode transferir dados pessoais para um país terceiro se o responsável pelo tratamento ou processador tiver fornecido garantias adequadas, e na condição de estarem disponíveis direitos executórios para as pessoas em causa e recursos legais eficazes para as mesmas. Podem ser previstas salvaguardas adequadas sem necessidade de qualquer autorização específica de uma autoridade de controlo, através de cláusulas contratuais-tipo, Artigo 46(2) aceso. c GDPR.

As cláusulas contratuais-tipo da União Europeia ou outras salvaguardas apropriadas são acordadas com todos os destinatários de países terceiros antes da primeira transmissão de dados pessoais. Consequentemente, é garantido que as garantias adequadas, os direitos executórios do titular dos dados e os recursos legais eficazes para o mesmo são garantidos. Todos os titulares dos dados podem obter uma cópia das cláusulas contratuais-tipo da nossa parte. As cláusulas contratuais-tipo estão também disponíveis no Jornal Oficial da União Europeia.

O artigo 45.º, n.º 3, do Regulamento Geral sobre a Proteção de Dados (RGPD) confere à Comissão Europeia o poder de decidir, através de um ato de execução, que um país terceiro assegura um nível de proteção adequado. Isto significa um nível de proteção dos dados pessoais que é essencialmente equivalente ao nível de proteção na UE. O efeito das decisões de adequação é que os dados pessoais podem circular livremente da UE (e da Noruega, Liechtenstein e Islândia) para um país terceiro sem mais obstáculos. Existem regras semelhantes para o Reino Unido, a Suíça e alguns outros países.

Sempre que a Comissão Europeia ou o governo de outro país decidir que um país terceiro assegura um nível de proteção adequado e existir um quadro válido (por exemplo, EU-U.S. Data Privacy Framework, Swiss-U.S. Data Privacy Framework, UK Extension to the EU-U.S. Data Privacy Framework), todas as transferências efectuadas por nós para os membros desses quadros (por exemplo, entidades autocertificadas) baseiam-se exclusivamente na adesão dessas entidades ao respetivo quadro. Quando nós ou uma das entidades do nosso grupo for membro de tal quadro, todas as transferências para nós ou para a entidade do nosso grupo baseiam-se exclusivamente na adesão da entidade a esse quadro.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

Qualquer pessoa a quem os dados digam respeito pode obter uma cópia dos quadros de referência junto de nós. Além disso, os quadros também estão disponíveis no Jornal Oficial da União Europeia ou nos materiais jurídicos publicados ou nos sítios Web das autoridades de controlo ou de outras autoridades ou instituições competentes.

## F. Prazo de conservação dos dados pessoais ou, se não for possível, os critérios usados para definir esse prazo (Artigo 13(2) aceso a GDPR)

A duração do armazenamento dos dados pessoais dos candidatos é de 6 meses. Para os dados de empregados aplica-se o respectivo período de retenção legal. Após a expiração desse período, os dados correspondentes são rotineiramente apagados, desde que já não sejam necessários para o cumprimento do contrato ou para o início de um contrato.

## G. A existência do direito de solicitar ao responsável pelo tratamento acesso aos dados pessoais que lhe digam respeito, bem como a sua retificação ou o seu apagamento, e a limitação do tratamento no que disser respeito ao titular dos dados, ou do direito de se opor ao tratamento, bem como do direito à portabilidade dos dados (Artigo 13(2) aceso b GDPR)

Todos os titulares dos dados têm os seguintes direitos:

***Direito de acesso***

Cada pessoa interessada tem o direito de aceder aos dados pessoais que lhe dizem respeito. O direito de acesso estende-se a todos os dados por nós processados. O direito pode ser exercido facilmente e a intervalos razoáveis, a fim de se conhecer e verificar a legalidade do tratamento (Considerando 63 GDPR). Este direito resulta da Arte. 15 GDPR. O titular dos dados pode contactar-nos para exercer o direito de acesso.

***Direito à rectificação***

De acordo com o Artigo 16 Sentença 1 GDPR, a pessoa em causa tem o direito de obter do responsável pelo tratamento, sem atrasos indevidos, a rectificação de dados pessoais inexactos que lhe digam respeito. Além disso, a frase 2 do Artigo 16º da GDPR prevê que a pessoa em causa tem o direito, tendo em conta as finalidades do tratamento, de ver completados dados pessoais incompletos, inclusive mediante a apresentação de uma declaração suplementar. A pessoa em causa pode contactar-nos para exercer o direito de rectificação.

***Direito ao apagamento (direito a ser esquecido)***

Além disso, as pessoas em causa têm direito a um direito de apagamento e a serem esquecidas ao abrigo da Arte. 17 GDPR. Este direito também pode ser exercido contactando-nos. Neste ponto, contudo, gostaríamos de salientar que este direito não se aplica na medida em que o processamento seja


© All rights reserved by Heiko Maniero.

necessário para cumprir uma obrigação legal a que a nossa empresa está sujeita, Artigo 17(3) aceso. b GDPR. Isto significa que só podemos aprovar um pedido de eliminação após o termo do período de retenção legal.

***Direito à restrição do processamento***

De acordo com o Artigo 18 GDPR, qualquer pessoa tem direito a uma restrição do tratamento de dados. A restrição do tratamento pode ser exigida se uma das condições estabelecidas no Artigo 18(1) aceso a-d GDPR for cumprida. A pessoa em causa pode contactar-nos para exercer o direito à restrição do tratamento.

***Direito de objecção***

Além disso, Arte. 21 GDPR garante o direito de objecção. O titular dos dados pode contactar-nos para exercer o direito de oposição.

***Direito à portabilidade dos dados***

Arte. 20 GDPR concede ao sujeito dos dados o direito à portabilidade dos dados. Nos termos desta disposição, a pessoa em causa tem, nas condições estabelecidas no n.º 1 do Artigo 20º iluminado a e b GDPR, o direito de receber os dados pessoais que lhe digam respeito, que tenha fornecido a um responsável pelo tratamento, num formato estruturado, comummente utilizado e legível por máquina, e tem o direito de transmitir esses dados a outro responsável pelo tratamento, sem impedimentos por parte do responsável ao qual os dados pessoais tenham sido fornecidos. O titular dos dados pode contactar-nos para exercer o direito à portabilidade dos dados.

## H. Se o tratamento dos dados se basear no Artigo 6.o, n.o 1, alínea a), ou no Artigo 9.o, n.o 2, alínea a), a existência do direito de retirar consentimento em qualquer altura, sem comprometer a licitude do tratamento efetuado com base no consentimento previamente dado (Artigo 13(2) aceso c GDPR)

Se o tratamento de dados pessoais se basear na Arte. 6(1) aceso a GDPR, que é o caso, se a pessoa em causa tiver dado consentimento para o tratamento de dados pessoais para um ou mais fins específicos ou se se basear no Artigo 9(2) aceso a GDPR, que regula o consentimento explícito para o tratamento de categorias especiais de dados pessoais, a pessoa em causa tem, de acordo com o Artigo 7(3) Sentença 1 GDPR, o direito de retirar o seu consentimento em qualquer altura.

A retirada do consentimento não afecta a legalidade do processamento baseado no consentimento antes da sua retirada, Artigo 7(3) Sentença 2 GDPR. Será tão fácil de retirar como de dar o consentimento, Art. 7(3) Sentença 4 GDPR. Por conseguinte, a retirada do consentimento pode sempre ter lugar da mesma forma que o consentimento foi dado ou de qualquer outra forma, que seja considerada mais simples pela pessoa a quem os dados dizem respeito. Na sociedade de informação actual, a forma mais simples de retirar o consentimento é provavelmente um simples correio electrónico. Se o titular dos dados desejar retirar o seu consentimento que nos foi concedido, basta um simples correio electrónico


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

para nós. Em alternativa, o titular dos dados pode escolher qualquer outra forma de nos comunicar a sua retirada de consentimento.

## I. O direito de apresentar reclamação a uma autoridade de controlo (Artigo 13(2) aceso d, 77(1) GDPR)

Como responsável pelo tratamento, somos obrigados a notificar a pessoa em causa do direito de apresentar uma queixa a uma autoridade de controlo, Artigo 13(2) aceso d GDPR. O direito de apresentar uma queixa junto de uma autoridade de controlo é regulado pelo Artigo 77(1) GDPR. Nos termos desta disposição, sem prejuízo de qualquer outro recurso administrativo ou judicial, qualquer pessoa em causa terá o direito de apresentar queixa a uma autoridade de controlo, em particular no Estado-Membro da sua residência habitual, local de trabalho ou local da alegada infracção, se a pessoa em causa considerar que o tratamento dos dados pessoais que lhe dizem respeito viola o Regulamento Geral de Protecção de Dados. O direito de apresentar uma queixa a uma autoridade de controlo só foi limitado pela lei da União de tal forma, que só pode ser exercido perante uma única autoridade de controlo (Considerando 141 Sentença 1 GDPR). Esta regra destina-se a evitar reclamações duplas da mesma pessoa em relação ao mesmo assunto. Se uma pessoa em causa quiser apresentar uma queixa sobre nós, pedimos, portanto, para contactar apenas uma única autoridade de controlo.

## J. Se a comunicação de dados pessoais constitui ou não uma obrigação legal ou contratual, ou um requisito necessário para celebrar um contrato, bem como se o titular está obrigado a fornecer os dados pessoais e as eventuais consequências de não fornecer esses dados (Art. 13(2) aceso e GDPR)

Esclarecemos que o fornecimento de dados pessoais é em parte exigido por lei (por exemplo, regulamentos fiscais) ou pode também resultar de disposições contratuais (por exemplo, informações sobre o parceiro contratual).

Por vezes pode ser necessário celebrar um contrato que a pessoa em causa nos forneça dados pessoais, os quais devem ser posteriormente tratados por nós. O titular dos dados é, por exemplo, obrigado a fornecer-nos dados pessoais quando a nossa empresa assina um contrato com ele. O não fornecimento dos dados pessoais teria como consequência que o contrato com o titular dos dados não poderia ser celebrado.

Antes de os dados pessoais serem fornecidos pela pessoa em causa, a pessoa em causa deve contactar-nos. Esclarecemos ao titular dos dados se o fornecimento dos dados pessoais é exigido por lei ou contrato ou é necessário para a celebração do contrato, se existe uma obrigação de fornecer os dados pessoais e as consequências da não prestação dos dados pessoais.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

### K. A existência de decisões automatizadas, incluindo a definição de perfis, referida no Artigo 22.o, n.os 1 e 4, e, pelo menos nesses casos, informações úteis relativas à lógica subjacente, bem como a importância e as consequências previstas de tal tratamento para o titular dos dados (Artigo 13 (2) aceso f GDPR)

Como empresa responsável, normalmente não utilizamos decisões automatizadas ou definição de perfis. Se, em casos excepcionais, procedermos a decisões ou perfis automatizados, informaremos a pessoa em causa separadamente ou através de uma subsecção na nossa política de privacidade (no nosso sítio Web). Neste caso, aplica-se o seguinte:

A tomada de decisões automatizada - incluindo a definição de perfis - pode ocorrer se (1) for necessária para a celebração ou execução de um contrato entre o titular dos dados e nós, ou (2) for autorizada pela legislação da União ou do Estado-Membro a que estamos sujeitos e que também estabelece medidas adequadas para salvaguardar os direitos e liberdades e os interesses legítimos do titular dos dados; ou (3) se for baseada no consentimento explícito do titular dos dados.

Nos casos referidos no artigo 22.º, n.º 2, alíneas a) e c) do RGPD, implementaremos medidas adequadas para salvaguardar os direitos e liberdades e os interesses legítimos da pessoa em causa. Nestes casos, o utilizador tem o direito de obter intervenção humana por parte do responsável pelo tratamento, de expressar o seu ponto de vista e de contestar a decisão.

A nossa política de privacidade contém informações significativas sobre a lógica envolvida, bem como sobre o significado e as consequências previstas de tal processamento para a pessoa em causa.

## II. Informações a facultar quando os dados pessoais não são recolhidos junto do titular (Artigo 14 GDPR)

### A. A identidade e os contactos do responsável pelo tratamento e, se for caso disso, do seu representante (Artigo 14(1) aceso a GDPR)

Ver acima

### B. Os contactos do encarregado da proteção de dados, se for caso disso (Artigo 14(1) aceso b GDPR)

Ver acima


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## C. As finalidades do tratamento a que os dados pessoais se destinam, bem como o fundamento jurídico para o tratamento (Artigo 14(1) aceso c GDPR)

Para os dados do candidato não recolhidos junto da pessoa em causa, a finalidade do tratamento de dados é conduzir um exame da candidatura durante o processo de recrutamento. Para este efeito, podemos tratar dados não recolhidos junto do candidato. Com base nos dados processados durante o processo de recrutamento, verificaremos se é convidado para uma entrevista de emprego (parte do processo de selecção). Se for contratado por nós, os dados do candidato serão automaticamente convertidos em dados do empregado. Para os dados do empregado, a finalidade do processamento de dados é a execução do contrato de trabalho ou o cumprimento de outras disposições legais aplicáveis à relação de trabalho. Os dados dos empregados são armazenados após a cessação da relação de trabalho para cumprir os períodos legais de retenção.

A base jurídica para o processamento de dados é o Artigo 6(1) aceso b e f GDPR, Artigo 9(2) aceso b e h GDPR, Artigo 88(1) GDPR e legislação nacional, tal como para a Alemanha Secção 26 BDSG (Lei Federal de Protecção de Dados).

## D. As categorias dos dados pessoais em questão (Artigo 14(1) aceso d GDPR)

Dados do candidato

Dados dos empregados

## E. Os destinatários ou categorias de destinatários dos dados pessoais, se os houver (Artigo 14(1) aceso e GDPR)

Autoridades públicas

Organismos externos

Outros organismos externos

Processamento interno

Processamento intragrupo

Outros organismos


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

Uma lista dos nossos subcontratantes e destinatários de dados em países terceiros e, se aplicável, de organizações internacionais está publicada no nosso sítio Web ou pode ser-nos solicitada gratuitamente. Para solicitar esta lista, contacte o nosso responsável pela proteção de dados.

## F. Se for caso disso, o facto de o responsável pelo tratamento tencionar transferir dados pessoais para um país terceiro ou uma organização internacional, e a existência ou não de uma decisão de adequação adotada pela Comissão ou, no caso das transferências mencionadas nos artigos 46.o ou 47.o, ou no artigo 49.o, n.o 1, segundo parágrafo, a referência às garantias apropriadas ou adequadas e aos meios de obter cópia das mesmas, ou onde foram disponibilizadas (Artigo 14(1) aceso f, 46(1), 46(2) aceso c GDPR)

Todas as empresas e sucursais que fazem parte do nosso grupo (doravante referidas como "empresas do grupo") que tenham o seu local de actividade ou um escritório num país terceiro podem pertencer aos destinatários dos dados pessoais. Uma lista de todas as empresas ou destinatários do grupo pode ser-nos solicitada.

Nos termos do n.o 1 do Artigo 46.o da GDPR, um responsável pelo tratamento ou processador só pode transferir dados pessoais para um país terceiro se o responsável pelo tratamento ou processador tiver fornecido garantias adequadas, e na condição de estarem disponíveis direitos executórios para as pessoas em causa e recursos legais eficazes para as mesmas. Podem ser previstas salvaguardas adequadas sem necessidade de qualquer autorização específica de uma autoridade de controlo, através de cláusulas-tipo de protecção de dados, Artigo 46(2) aceso. c GDPR.

As cláusulas contratuais-tipo da União Europeia ou outras salvaguardas apropriadas são acordadas com todos os destinatários de países terceiros antes da primeira transmissão de dados pessoais. Consequentemente, é garantido que as garantias adequadas, os direitos executórios do titular dos dados e os recursos legais eficazes para o mesmo são garantidos. Todos os titulares dos dados podem obter uma cópia das cláusulas contratuais-tipo da nossa parte. As cláusulas contratuais-tipo estão também disponíveis no Jornal Oficial da União Europeia.

O artigo 45.º, n.º 3, do Regulamento Geral sobre a Proteção de Dados (RGPD) confere à Comissão Europeia o poder de decidir, através de um ato de execução, que um país terceiro assegura um nível de proteção adequado. Isto significa um nível de proteção dos dados pessoais que é essencialmente equivalente ao nível de proteção na UE. O efeito das decisões de adequação é que os dados pessoais podem circular livremente da UE (e da Noruega, Liechtenstein e Islândia) para um país terceiro sem mais obstáculos. Existem regras semelhantes para o Reino Unido, a Suíça e alguns outros países.

Sempre que a Comissão Europeia ou o governo de outro país decidir que um país terceiro assegura um nível de proteção adequado e existir um quadro válido (por exemplo, EU-U.S. Data Privacy Framework,


© All rights reserved by Heiko Maniero.

Swiss-U.S. Data Privacy Framework, UK Extension to the EU-U.S. Data Privacy Framework), todas as transferências efectuadas por nós para os membros desses quadros (por exemplo, entidades autocertificadas) baseiam-se exclusivamente na adesão dessas entidades ao respetivo quadro. Quando nós ou uma das entidades do nosso grupo for membro de tal quadro, todas as transferências para nós ou para a entidade do nosso grupo baseiam-se exclusivamente na adesão da entidade a esse quadro.

Qualquer pessoa a quem os dados digam respeito pode obter uma cópia dos quadros de referência junto de nós. Além disso, os quadros também estão disponíveis no Jornal Oficial da União Europeia ou nos materiais jurídicos publicados ou nos sítios Web das autoridades de controlo ou de outras autoridades ou instituições competentes.

## G. Prazo de conservação dos dados pessoais ou, se não for possível, os critérios usados para fixar esse prazo (Artigo 14(2) aceso a GDPR)

A duração do armazenamento dos dados pessoais dos candidatos é de 6 meses. Para os dados dos funcionários aplica-se o respectivo período de retenção legal. Após a expiração desse período, os dados correspondentes são rotineiramente apagados, desde que já não sejam necessários para o cumprimento do contrato ou para o início de um contrato.

## H. Se o tratamento dos dados se basear no artigo 6.o, n.o 1, alínea f), os interesses legítimos do responsável pelo tratamento ou de um terceiro (Art. 14(2) aceso b GDPR)

Nos termos do n.º 1 do Artigo 6.º aceso f GDPR, o tratamento só será lícito se for necessário para os fins de interesses legítimos prosseguidos pelo responsável pelo tratamento ou por terceiros, excepto se tais interesses forem anulados pelos interesses ou direitos e liberdades fundamentais da pessoa em causa que exijam a protecção de dados pessoais. De acordo com o Considerando 47 Sentença 2 GDPR, poderá existir um interesse legítimo quando existe uma relação relevante e adequada entre a pessoa em causa e o responsável pelo tratamento, por exemplo, em situações em que a pessoa em causa é cliente do responsável pelo tratamento. Em todos os casos em que a nossa empresa processe os dados do requerente com base no Artigo 6(1) aceso f GDPR, o nosso interesse legítimo é o emprego de pessoal e profissionais adequados.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## I. A existência do direito de solicitar ao responsável pelo tratamento o acesso aos dados pessoais que lhe digam respeito, e a retificação ou o apagamento, ou a limitação do tratamentor no que disser respeito ao titular dos dados, e do direito de se opor ao tratamento, bem como do direito à portabilidade dos dados (Artigo 14 (2) aceso c GDPR)

Todos os titulares dos dados têm os seguintes direitos:

***Direito de acesso***

Cada pessoa interessada tem o direito de aceder aos dados pessoais que lhe dizem respeito. O direito de acesso estende-se a todos os dados por nós processados. O direito pode ser exercido facilmente e a intervalos razoáveis, a fim de se conhecer e verificar a legalidade do tratamento (Considerando 63 GDPR). Este direito resulta da Arte. 15 GDPR. O titular dos dados pode contactar-nos para exercer o direito de acesso.

***Direito à rectificação***

De acordo com o Artigo 16 Sentença 1 GDPR, a pessoa em causa tem o direito de obter do responsável pelo tratamento, sem atrasos indevidos, a rectificação de dados pessoais inexactos que lhe digam respeito. Além disso, a frase 2 do Artigo 16º da GDPR prevê que a pessoa em causa tem o direito, tendo em conta as finalidades do tratamento, de ver completados dados pessoais incompletos, inclusive mediante a apresentação de uma declaração suplementar. A pessoa em causa pode contactar-nos para exercer o direito de rectificação.

***Direito ao apagamento (direito a ser esquecido)***

Além disso, as pessoas em causa têm direito a um direito de apagamento e a serem esquecidas ao abrigo da Arte. 17 GDPR. Este direito também pode ser exercido contactando-nos. Neste ponto, contudo, gostaríamos de salientar que este direito não se aplica na medida em que o processamento seja necessário para cumprir uma obrigação legal a que a nossa empresa está sujeita, Artigo 17(3) aceso. b GDPR. Isto significa que só podemos aprovar um pedido de eliminação após o termo do período de retenção legal.

***Direito à restrição do processamento***

De acordo com o Artigo 18 GDPR qualquer pessoa tem direito à restrição do processamento de dados. A restrição do tratamento pode ser exigida se uma das condições estabelecidas no Artigo 18(1) aceso a-d GDPR for cumprida. A pessoa em causa pode contactar-nos para exercer o direito à restrição do tratamento.

***Direito de objecção***

Além disso, Arte. 21 GDPR garante o direito de objecção. O titular dos dados pode contactar-nos para exercer o direito de oposição.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

***Direito à portabilidade dos dados***

Arte. 20 GDPR concede ao sujeito dos dados o direito à portabilidade dos dados. De acordo com esta disposição, a pessoa em causa tem, nas condições estabelecidas no n.º 1 do Artigo 20º aceso, a e b GDPR, o direito de receber os dados pessoais que lhe digam respeito, que tenha fornecido a um responsável pelo tratamento, num formato estruturado, comummente utilizado e legível por máquina, e tem o direito de transmitir esses dados a outro responsável pelo tratamento sem impedimento por parte do responsável pelo tratamento ao qual os dados pessoais tenham sido fornecidos. O titular dos dados pode contactar-nos para exercer o direito à portabilidade dos dados.

## J. Se o tratamento dos dados se basear no artigo 6.o, n.o 1, alínea a), ou no artigo 9.o, n.o 2, alínea a), a existência do direito de retirar consentimento em qualquer altura, sem comprometer a licitude do tratamento efetuado com base no consentimento previamente dado (Art. 14(2) aceso d GDPR)

Se o tratamento de dados pessoais se basear na Arte. 6(1) aceso a GDPR, que é o caso, se a pessoa em causa tiver dado consentimento para o tratamento de dados pessoais para um ou mais fins específicos ou se se basear no Artigo 9(2) aceso a GDPR, que regula o consentimento explícito para o tratamento de categorias especiais de dados pessoais, a pessoa em causa tem, de acordo com o Artigo 7(3) Sentença 1 GDPR, o direito de retirar o seu consentimento a qualquer momento.

A retirada do consentimento não afecta a legalidade do processamento baseado no consentimento antes da sua retirada, Artigo 7(3) Sentença 2 GDPR. Será tão fácil de retirar como de dar o consentimento, Art. 7(3) Sentença 4 GDPR. Por conseguinte, a retirada do consentimento pode sempre ter lugar da mesma forma que o consentimento foi dado ou de qualquer outra forma, que seja considerada mais simples pela pessoa a quem os dados dizem respeito. Na sociedade de informação actual, provavelmente a forma mais simples de retirar o consentimento é um simples correio electrónico. Se o titular dos dados desejar retirar o seu consentimento que nos foi concedido, basta um simples correio electrónico para nós. Em alternativa, o titular dos dados pode escolher qualquer outra forma de nos comunicar a sua retirada de consentimento.

## K. O direito de apresentar reclamação a uma autoridade de controlo (Artigo 14(2) aceso e, 77(1) GDPR)

Como responsável pelo tratamento, somos obrigados a notificar a pessoa em causa do direito de apresentar uma queixa a uma autoridade de controlo, Artigo 14(2) aceso e GDPR. O direito de apresentar uma queixa a uma autoridade de controlo é regulado pelo Artigo 77(1) da GDPR. Nos termos desta disposição, sem prejuízo de qualquer outro recurso administrativo ou judicial, qualquer pessoa em causa terá o direito de apresentar queixa a uma autoridade de controlo, em particular no Estado-Membro da sua residência habitual, local de trabalho ou local da alegada infracção, se a pessoa em causa


© All rights reserved by Heiko Maniero.

considerar que o tratamento dos dados pessoais que lhe dizem respeito viola o Regulamento Geral sobre Protecção de Dados. O direito de apresentar uma queixa a uma autoridade de controlo só foi limitado pela lei da União de tal forma, que só pode ser exercido perante uma única autoridade de controlo (Considerando 141 Sentença 1 GDPR). Esta regra destina-se a evitar reclamações duplas da mesma pessoa em relação ao mesmo assunto. Se uma pessoa em causa quiser apresentar uma queixa sobre nós, pedimos, portanto, para contactar apenas uma única autoridade de controlo.

## L. A origem dos dados pessoais e, eventualmente, se provêm de fontes acessíveis ao público (Artigo 14(2) aceso f GDPR)

Em princípio, os dados pessoais são recolhidos directamente da pessoa em causa ou em cooperação com uma autoridade (por exemplo, a recuperação de dados de um registo oficial). Outros dados sobre as pessoas em causa são derivados de transferências de empresas do grupo. No contexto desta informação geral, a designação das fontes exactas de onde provêm os dados pessoais é impossível ou implicaria um esforço desproporcionado na acepção da Arte. 14(5) aceso b GDPR. Em princípio, não recolhemos dados pessoais a partir de fontes publicamente acessíveis.

Qualquer pessoa interessada pode contactar-nos em qualquer altura para obter informações mais detalhadas sobre as fontes exactas dos dados pessoais que lhe dizem respeito. Quando a origem dos dados pessoais não puder ser fornecida à pessoa em causa por terem sido utilizadas várias fontes, devem ser fornecidas informações gerais (Considerando 61 Sentença 4 GDPR).

## M. A existência de decisões automatizadas, incluindo a definição de perfis referida no artigo 22.o, n.os 1 e 4, e, pelo menos nesses casos, informações úteis relativas à lógica subjacente, bem como a importância e as consequências previstas de tal tratamento para o titular dos dados (Artigo 14(2) aceso g GDPR)

Como empresa responsável, normalmente não utilizamos decisões automatizadas ou definição de perfis. Se, em casos excepcionais, procedermos a decisões ou perfis automatizados, informaremos a pessoa em causa separadamente ou através de uma subsecção na nossa política de privacidade (no nosso sítio Web). Neste caso, aplica-se o seguinte:

A tomada de decisões automatizada - incluindo a definição de perfis - pode ocorrer se (1) for necessária para a celebração ou execução de um contrato entre o titular dos dados e nós, ou (2) for autorizada pela legislação da União ou do Estado-Membro a que estamos sujeitos e que também estabelece medidas adequadas para salvaguardar os direitos e liberdades e os interesses legítimos do titular dos dados; ou (3) se for baseada no consentimento explícito do titular dos dados.

Nos casos referidos no artigo 22.º, n.º 2, alíneas a) e c) do RGPD, implementaremos medidas adequadas para salvaguardar os direitos e liberdades e os interesses legítimos da pessoa em causa. Nestes casos,


© All rights reserved by Heiko Maniero.

o utilizador tem o direito de obter intervenção humana por parte do responsável pelo tratamento, de expressar o seu ponto de vista e de contestar a decisão.

A nossa política de privacidade contém informações significativas sobre a lógica envolvida, bem como sobre o significado e as consequências previstas de tal processamento para a pessoa em causa.

## III. EU-U.S. Data Privacy Framework (EU-U.S. DPF), UK Extension to the EU-U.S. DPF, Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF)

Se a nossa organização for um membro certificado do EU-U.S. Data Privacy Framework (EU-U.S. DPF) e/ou da UK Extension to the EU-U.S. DPF e/ou do Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF), aplica-se o seguinte:

Cumprimos o EU-U.S. Data Privacy Framework (EU-U.S. DPF) e a UK Extension to the EU-U.S. DPF, bem como o Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF), conforme estabelecido pelo U.S. Department of Commerce. A nossa empresa confirmou ao Departamento de Comércio dos EUA que cumpre os EU-U.S. Data Privacy Framework Principles (EU-U.S. DPF Principles) no que diz respeito ao tratamento de dados pessoais recebidos da União Europeia e do Reino Unido, com base no EU-U.S. DPF e na UK Extension to the EU-U.S. DPF. A nossa empresa confirmou ao Departamento de Comércio dos EUA que cumpre os Swiss-U.S. Data Privacy Framework Principles (Swiss-U.S. DPF Principles) no que diz respeito ao tratamento de dados pessoais recebidos da Suíça com base no Swiss-U.S. DPF. Em caso de conflito entre as disposições da nossa política de privacidade e os EU-U.S. DPF Principles e/ou os Swiss-U.S. DPF Principles, os Principles prevalecem.

Para saber mais sobre o programa Data Privacy Framework (DPF) e para ver a nossa certificação, visite https://www.dataprivacyframework.gov/.

As outras unidades ou subsidiárias dos EUA da nossa empresa que também cumprem os EU-U.S. DPF Principals, incluindo a UK Extension to the EU-U.S. DPF e os Swiss-U.S. DPF Principals, se houver, são mencionadas na nossa política de privacidade.

Em conformidade com o EU-U.S. DPF e a UK Extension to the EU-U.S. DPF, bem como o Swiss-U.S. DPF, a nossa empresa compromete-se a colaborar com o painel estabelecido pelas autoridades de proteção de dados da UE e pelo Information Commissioner's Office (ICO) do Reino Unido, bem como pelo Comissário Federal para a Proteção de Dados e Informação (EDÖB) da Suíça, e a seguir os seus conselhos sobre reclamações não resolvidas relativas ao nosso tratamento de dados pessoais que recebemos com base no EU-U.S. DPF e na UK Extension to the EU-U.S. DPF e no Swiss-U.S. DPF.

Informamos as pessoas afetadas sobre as autoridades europeias de proteção de dados competentes, responsáveis pelo tratamento de reclamações sobre o tratamento de dados pessoais pela nossa


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

organização, na parte superior deste documento de transparência e que oferecemos às pessoas afetadas um recurso adequado e gratuito.

Informamos todas as pessoas afetadas de que a nossa empresa está sujeita aos poderes de investigação e execução da Federal Trade Commission (FTC).

As pessoas afetadas têm, em determinadas circunstâncias, a possibilidade de recorrer à arbitragem vinculativa. A nossa organização é obrigada a resolver as reclamações e a cumprir as condições estabelecidas no Anexo I dos DPF-Principals, caso a pessoa afetada solicite uma arbitragem vinculativa, notificando a nossa organização e cumprindo os procedimentos e condições estabelecidos no Anexo I dos Principals.

Informamos por este meio todas as pessoas afetadas sobre a responsabilidade da nossa organização em caso de transferência de dados pessoais para terceiros.

Para perguntas das pessoas afetadas ou das autoridades de supervisão de dados, nomeamos os representantes locais mencionados acima neste documento de transparência.

Oferecemos-lhe a possibilidade de optar (Opt-out) por não ter os seus dados pessoais (i) transferidos para terceiros ou (ii) utilizados para um propósito que seja significativamente diferente do(s) propósito(s) para o qual/quais foram originalmente recolhidos ou posteriormente autorizados por si. O mecanismo claro, visível e de fácil acesso para exercer a sua escolha consiste em contactar o nosso Encarregado de Proteção de Dados (DPO) por e-mail. Não tem opção de escolha e não somos obrigados a fazê-lo se os dados forem transferidos para um terceiro que atue como agente ou processador em nosso nome e de acordo com as nossas instruções. No entanto, celebramos sempre um contrato com tal agente ou processador.

Para dados sensíveis (ou seja, dados pessoais que contenham informações sobre o estado de saúde, origem racial ou étnica, opiniões políticas, crenças religiosas ou filosóficas, filiação sindical ou informações sobre a vida sexual da pessoa em questão), obtemos o seu consentimento explícito (Opt-in) quando esses dados (i) são transferidos para terceiros ou (ii) são utilizados para um propósito diferente daquele para o qual foram originalmente recolhidos ou para o qual deu posteriormente o seu consentimento, escolhendo a opção Opt-in. Além disso, tratamos todos os dados pessoais que recebemos de terceiros como sensíveis, se o terceiro os identificar e tratar como sensíveis.

Informamos por este meio sobre a necessidade de divulgar dados pessoais em resposta a solicitações legais de autoridades, incluindo o cumprimento de requisitos de segurança nacional ou aplicação da lei.

Ao transferir dados pessoais para um terceiro que atue como controlador, cumprimos os Principals de notificação e escolha. Além disso, celebramos um contrato com o terceiro responsável pelo tratamento que prevê que esses dados só possam ser tratados para fins limitados e especificados, de acordo com o consentimento que deu, e que o destinatário deve fornecer o mesmo nível de proteção que os Principals do DPF e nos notificar se determinar que já não pode cumprir essa obrigação. O contrato


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

prevê que o terceiro, responsável pelo tratamento, interrompa o tratamento ou tome outras medidas adequadas e apropriadas para corrigir a situação se essa determinação for feita.

Ao transferir dados pessoais para um terceiro que atue como agente ou processador, (i) transferimos esses dados apenas para fins limitados e especificados; (ii) asseguramos que o agente ou processador é obrigado a fornecer pelo menos o mesmo nível de proteção de dados exigido pelos DPF-Principals; (iii) tomamos medidas adequadas e apropriadas para garantir que o agente ou processador realmente processa os dados pessoais transferidos de uma maneira que esteja em conformidade com as nossas obrigações de acordo com os DPF-Principals; (iv) exigimos que o agente ou processador notifique a nossa organização se determinar que já não pode cumprir a obrigação de fornecer o mesmo nível de proteção que os DPF-Principals prevêem; (v) após tal notificação, inclusive sob (iv), tomamos medidas adequadas e apropriadas para interromper o processamento não autorizado e corrigir a situação; e (vi) fornecemos ao DPF Department, mediante solicitação, um resumo ou um exemplar representativo das disposições relevantes de proteção de dados do nosso contrato com esse agente.

Em conformidade com o EU-U.S. DPF e/ou a UK Extension to the EU-U.S. DPF e/ou o Swiss-U.S. DPF, a nossa organização compromete-se a colaborar com o painel estabelecido pelas autoridades de proteção de dados da UE e pelo Information Commissioner's Office (ICO) do Reino Unido, bem como pelo Comissário Federal para a Proteção de Dados e Informação (EDÖB) da Suíça, e a seguir os seus conselhos sobre reclamações não resolvidas relativas ao nosso tratamento de dados pessoais recebidos no contexto da relação de trabalho, com base no EU-U.S. DPF e na UK Extension to the EU-U.S. DPF e no Swiss-U.S. DPF.

Todos os titulares de dados que se encontrem temporariamente na União Europeia (UE), no Espaço Económico Europeu (EEE) ou no Reino Unido, ou que aí tenham o seu domicílio ou residência habitual, têm direito aos direitos e aos direitos dos titulares de dados publicados no nosso Documento de Transparência, que também decorrem dos artigos 15º a 22º do RGPD, incluindo o direito de acesso aos dados pessoais. Disponibilizámos esta informação em todas as línguas da UE e do EEE. A versão em inglês aplica-se ao Reino Unido.

Todos os titulares de dados que residam temporariamente na Suíça ou que aí tenham o seu domicílio ou residência habitual beneficiam dos direitos e das prerrogativas dos titulares de dados ao abrigo da Lei de Proteção de Dados suíça (DPA) e do Regulamento de Proteção de Dados suíço (DPR), publicados no nosso Documento de Transparência, incluindo o direito de acesso aos dados pessoais. Disponibilizámos esta informação nas três línguas oficiais da Suíça (alemão, italiano e francês).


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

# MALTESE: Informazzjoni dwar l-Ipproċessar tad-Data Personali (Artikolu 13, 14 GDPR)

Għażiż Sinjur jew Sinjura,

Id-dejta personali ta' kull individwu li jinsab f'relazzjoni kuntrattwali, prekuntrattwali jew relazzjoni oħra mal-kumpanija tagħna jistħoqqilha protezzjoni speċjali. L-għan tagħna huwa li nżommu l-livell ta' protezzjoni tad-dejta tagħna għal standard għoli. Għalhekk, qed niżviluppaw rutina il-kunċetti tagħna dwar il-protezzjoni tad-dejta u s-sigurtà tad-dejta.

Naturalment, aħna nikkonformaw mad-dispożizzjonijiet statutorji dwar il-protezzjoni tad-dejta. Skont Artikolu 13, 14 tal-GDPR, il-kontrolluri jissodisfaw rekwiżiti speċifiċi ta' informazzjoni meta jiġbru d-dejta personali. Dan id-dokument iwettaq dawn l-obbligi.

It-terminoloġija tar-regolamenti legali hija kkumplikata. Sfortunatament, l-użu ta' termini legali ma setax jiġi eliminat fit-tħejjija ta' dan id-dokument. Għalhekk, nixtiequ nirrimarkaw li inti dejjem mistieden tikkuntattjana għall-mistoqsijiet kollha dwar dan id-dokument, it-termini jew formulazzjonijiet użati.

## I. Informazzjoni li għandha tiġi pprovduta fejn tinġabar data personali mis-suġġett tad-data (Artikolu 13 GDPR)

### A. l-identità u d-dettalji ta' kuntatt tal-kontrollur u, fejn applikabbli, tar-rappreżentant tal-kontrollur (Artikolu 13(1) lit. a GDPR)

Ara hawn fuq

### B. Id-dettalji ta' kuntatt tal-uffiċjal tal-protezzjoni tad-data, fejn applikabbli (Artikolu 1 3(1) lit. b GDPR)

Ara hawn fuq

### C. l-għanijiet tal-ipproċessar li għalihom hija maħsuba d-data personali kif ukoll il-bażi legali għall-ipproċessar (Artikolu 13(1) lit. c GDPR)

L-għan tal-ipproċessar tad-dejta personali huwa l-immaniġġjar tal-operazzjonijiet kollha li jikkonċernaw lill-kontrollur, klijenti, klijenti prospettivi, imsieħba fin-negozju jew relazzjonijiet kuntrattwali jew prekuntrattwali oħra bejn il-gruppi msemmija (fl-iktar sens wiesa') jew obbligi legali tal-kontrollur.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

Art. 6(1) lit. GDPR iservi bħala l-bażi legali għall-operazzjonijiet ta' pproċessar li għalihom niksbu l-kunsens għal skop speċifiku ta' pproċessar. Jekk l-ipproċessar tad-dejta personali huwa meħtieġ għat-twettiq ta' kuntratt li għalih is-suġġett tad-dejta huwa parti, kif inhu l-każ, pereżempju, meta l-operazzjonijiet tal-ipproċessar huma meħtieġa għall-provvista ta' oġġetti jew biex jipprovdu kwalunkwe servizz ieħor, l-ipproċessar huwa ibbażat fuq Artikolu 6(1) lit. b GDPR. L-istess japplika għal tali operazzjonijiet ta' pproċessar li huma meħtieġa għat-twettiq ta' miżuri prekuntrattwali, pereżempju fil-każ ta' mistoqsijiet li jikkonċernaw il-prodotti jew is-servizzi tagħna. Il-kumpanija tagħna hija soġġetta għal obbligu legali li permezz tiegħu l-ipproċessar tad-dejta personali huwa meħtieġ, bħal għat-twettiq tal-obbligi tat-taxxa, l-ipproċessar huwa bbażat fuq l-Art. 6(1) lit. c GDPR.

F'każijiet rari, l-ipproċessar ta' data personali jista' jkun meħtieġ biex jipproteġi l-interessi vitali tas-suġġett tad-data jew ta' persuna fiżika oħra. Dan ikun il-każ, pereżempju, jekk viżitatur weġġa' fil-kumpanija tagħna u ismu, l-età, id-dejta tal-assigurazzjoni tas-saħħa jew informazzjoni vitali oħra jkollhom jiġu mgħoddija lil tabib, sptar jew parti terza oħra. Imbagħad l-ipproċessar ikun ibbażat fuq l-Art. 6(1) lit. d GDPR.

Fejn l-ipproċessar ikun meħtieġ għat-twettiq ta' kompitu mwettaq fl-interess pubbliku jew fl-eżerċizzju ta' awtorità uffiċjali vestita fil-kontrollur, il-bażi legali hija l-Art. 6(1) lit. e GDPR.

Fl-aħħar nett, operazzjonijiet ta' pproċessar jistgħu jkunu bbażati fuq Artikolu 6(1) lit. f GDPR. Din il-bażi legali tintuża għal operazzjonijiet ta' pproċessar li mhumiex koperti minn xi waħda mir-raġunijiet legali msemmija hawn fuq, jekk l-ipproċessar ikun meħtieġ għall-finijiet tal-interessi leġittimi segwiti mill-kumpanija tagħna jew minn parti terza, ħlief fejn dawn l-interessi jiġu ssuperati mill-interessi. jew id-drittijiet u l-libertajiet fundamentali tas-suġġett tad-data li jeħtieġu protezzjoni tad-data personali. Operazzjonijiet ta' pproċessar bħal dawn huma partikolarment permissibbli minħabba li ġew imsemmija speċifikament mil-leġiżlatur Ewropew. Huwa kkunsidra li jista' jiġi preżunt interess leġittimu jekk is-suġġett tad-dejta jkun klijent tal-kontrollur (Premessa 47 Sentenza 2 GDPR).

## D. Fejn l-ipproċessar ikun ibbażat fuq il-punt (f) taArtikolu 6(1), l-interessi leġittimi segwiti mill-kontrollur jew minn parti terza (Artikolu 13(1) lit. d GDPR)

Fejn l-ipproċessar tad-dejta personali huwa bbażat fuq Artikolu 6(1) lit. f GDPR l-interess leġittimu tagħna huwa li nwettqu n-negozju tagħna favur il-benessri tal-impjegati kollha tagħna u l-azzjonisti.

## E. Ir-riċevituri jew il-kategoriji ta' riċevituri tad-data personali, jekk jeżistu (Artikolu 13(1) lit. e GDPR)

Awtoritajiet pubbliċi


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

Korpi esterni

Aktar korpi esterni

Ipproċessar intern

Ipproċessar intragrupp

Korpi oħra

Lista tal-proċessuri u r-riċevituri tad-dejta tagħna f'pajjiżi terzi u, jekk applikabbli, organizzazzjonijiet internazzjonali jew tiġi ppubblikata fuq il-websajt tagħna jew tista' tintalab mingħandna mingħajr ħlas. Jekk jogħġbok ikkuntattja lill-uffiċjal tal-protezzjoni tad-dejta tagħna biex titlob din il-lista.

## F. Fejn applikabbli, il-fatt li l-kontrollur għandu l-ħsieb li jittrasferixxi data personali lejn pajjiż terz jew organizzazzjoni internazzjonali u l-eżistenza jew l-assenza ta' deċiżjoni ta' adegwatezza mill-Kummissjoni, jew fil-każ ta' trasferimenti msemmija fl-Artikolu 46 jew 47, jew it-tieni subparagrafu tal-Artikolu 49(1), referenza għas-salvagwardji xierqa jew adatti u l-mezzi li bihom tinkiseb kopja tagħhom jew fejn dawn ikunu saru disponibbli (Artikolu 13(1) lit. f, 46(1), 46 (2) lit.c GDPR)

Il-kumpaniji u l-fergħat kollha li huma parti mill-grupp tagħna (minn hawn 'il quddiem imsejħa "kumpaniji tal-grupp") li għandhom il-post tan-negozju tagħhom jew uffiċċju f'pajjiż terz jistgħu jappartjenu għar-riċevituri tad-dejta personali. Lista tal-kumpaniji kollha tal-grupp jew riċevituri tista' tintalab mingħandna.

Skont Artikolu 46(1) GDPR kontrollur jew proċessur jista' jittrasferixxi data personali biss lil pajjiż terz jekk il-kontrollur jew proċessur ikun ipprovda salvagwardji xierqa, u bil-kundizzjoni li jkunu disponibbli drittijiet infurzabbli tas-suġġett tad-data u rimedji legali effettivi għas-suġġetti tad-data. Jistgħu jiġu pprovduti salvagwardji xierqa mingħajr ma tkun meħtieġa xi awtorizzazzjoni speċifika minn awtorità superviżorja permezz ta' klawsoli kuntrattwali standard, Artikolu 46(2) lit. c GDPR.

Il-klawsoli kuntrattwali standard tal-Unjoni Ewropea jew salvagwardji xierqa oħra huma miftiehma mar-riċevituri kollha minn pajjiżi terzi qabel l-ewwel trażmissjoni tad-dejta personali. Konsegwentement, huwa żgurat li jkunu garantiti salvagwardji xierqa, drittijiet infurzabbli tas-suġġett tad-data u rimedji legali effettivi għas-suġġetti tad-data. Kull suġġett tad-dejta jista' jikseb kopja tal-klawsoli kuntrattwali standard mingħandna. Il-klawsoli kuntrattwali standard huma wkoll disponibbli fil-Ġurnal Uffiċjali tal-Unjoni Ewropea.

L-Artikolu 45(3) tar-Regolament Ġenerali dwar il-Protezzjoni tad-Dejta (GDPR) jagħti lill-Kummissjoni Ewropea s-setgħa li tiddeċiedi, permezz ta' att ta' implimentazzjoni, li pajjiż mhux tal-UE jiżgura livell adegwat ta' protezzjoni. Dan ifisser livell ta' protezzjoni għad-dejta personali li huwa essenzjalment ekwivalenti għal-livell ta' protezzjoni fl-UE. L-effett tad-deċiżjonijiet dwar l-adegwatezza huwa li d-dejta


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

personali tista' tiċċirkola liberament mill-UE (u n-Norveġja, il-Liechtenstein u l-Islanda) lejn pajjiż terz mingħajr aktar ostakli. Regoli simili jeżistu għar-Renju Unit, l-Isvizzera u xi Pajjiżi oħra.

Fejn il-Kummissjoni Ewropea jew il-gvern ta' pajjiż ieħor iddeċieda li pajjiż terz jiżgura livell adegwat ta' protezzjoni, u Qafas validu jkun fis-seħħ (eż. EU-U.S. Data Privacy Framework, Swiss-U.S. Data Privacy Framework, UK Extension to the EU-U.S. Data Privacy Framework), it-trasferimenti kollha minna lill-membri ta' tali oqfsa (eż. entitajiet awtoċertifikati) huma bbażati esklussivament fuq is-sħubija ta' dik l-entitajiet fil-qafas rispettiv. Fejn aħna jew waħda mill-entitajiet tal-grupp tagħna tkun membru ta' tali qafas, it-trasferimenti kollha lilna jew lill-entità tal-grupp tagħna huma bbażati esklussivament fuq is-sħubija tal-entitajiet f'tali qafas.

Kwalunkwe suġġett tad-dejta jista' jikseb kopja tal-oqfsa mingħandna. Barra minn hekk, l-oqfsa huma wkoll disponibbli fil-Ġurnal Uffiċjali tal-Unjoni Ewropea jew fil-materjali legali ppubblikati jew fuq il-websajts tal-awtoritajiet superviżorji jew awtoritajiet jew istituzzjonijiet kompetenti oħra.

## G. Il-perijodu li matulu d-data personali tkun ser tinħażen, jew jekk dak ma jkunx possibbli, il-kriterji użati biex jiġi ddeterminat dak il-perijodu (Artikolu 13(2) lit. a GDPR)

Il-kriterji użati biex jiġi ddeterminat il-perjodu ta' ħażna ta' data personali huwa l-perjodu ta' żamma statutorju rispettiv. Wara li jiskadi dak il-perjodu, id-dejta korrispondenti titħassar b'mod regolari, sakemm ma tibqax meħtieġa għat-twettiq tal-kuntratt jew għall-bidu ta' kuntratt.

Jekk ma jkunx hemm perjodu statutorju ta' żamma, il-kriterju huwa l-perjodu ta' żamma kuntrattwali jew intern.

## H. L-eżistenza tad-dritt li jitlob mingħand il-kontrollur aċċess jew rettifika jew tħassir ta' data personali jew restrizzjoni tal-ipproċessar rigward is-suġġett tad-data jew li joġġezzjona għall-ipproċessar kif ukoll id-dritt għall-portabbiltà tad-data (Artikolu 13(2) lit. b GDPR)

Is-suġġetti tad-dejta kollha għandhom id-drittijiet li ġejjin:

***Dritt għall-aċċess***

Kull suġġett tad-dejta għandu dritt li jaċċessa d-dejta personali li tikkonċernah jew lilha. Id-dritt għall-aċċess jestendi għad-dejta kollha pproċessata minna. Id-dritt jista' jiġi eżerċitat faċilment u f'intervalli raġonevoli, sabiex tkun konxju ta', u tivverifika, il-legalità tal-ipproċessar (Premessa 63 GDPR). Dan id-dritt jirriżulta mill-Art. 15 GDPR. Is-suġġett tad-dejta jista' jikkuntattjana biex jeżerċita d-dritt ta' aċċess.

***Dritt għal rettifika***

Skont Artikolu 16 Sentenza 1 GDPR is-suġġett tad-dejta għandu d-dritt li jikseb mingħand il-kontrollur mingħajr dewmien żejjed ir-rettifika ta' data personali mhux eżatta li tikkonċernah. Barra minn hekk,


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

Artikolu 16 Sentenza 2 tal-GDPR jipprovdi li s-suġġett tad-data huwa intitolat, b'kont meħud tal-għanijiet tal-ipproċessar, li jimtela data personali mhux kompluta, inkluż permezz tal-għoti ta' dikjarazzjoni supplimentari. Is-suġġett tad-dejta jista' jikkuntattjana biex jeżerċita d-dritt ta' rettifika.

***Dritt għat-tħassir (dritt li jintesa)***

Barra minn hekk, is-suġġetti tad-data huma intitolati għal dritt għat-tħassir u li jintesew taħt l-Art. 17 GDPR. Dan id-dritt jista' jiġi eżerċitat ukoll billi tikkuntattjana. F'dan il-punt, madankollu, nixtiequ nirrimarkaw li dan id-dritt ma japplikax safejn l-ipproċessar huwa meħtieġ biex tissodisfa obbligu legali li l-kumpanija tagħna hija soġġetta għalih, Artikolu 17(3) lit. b GDPR. Dan ifisser li nistgħu napprovaw applikazzjoni biex titħassar biss wara li jiskadi l-perjodu statutorju ta' żamma.

***Dritt gJal restrizzjoni ta' pro'essar***

Skont Artikolu 18 tal-GDPR kull suġġett tad-dejta huwa intitolat għal restrizzjoni tal-ipproċessar. Ir-restrizzjoni tal-ipproċessar tista' tintalab jekk waħda mill-kundizzjonijiet stipulati fArtikolu 18(1) lit. ad GDPR huwa sodisfatt. Is-suġġett tad-dejta jista' jikkuntattjana biex jeżerċita d-dritt għal restrizzjoni tal-ipproċessar.

***Dritt ta' oġġezzjoni***

Barra minn hekk, l-Art. 21 GDPR jiggarantixxi d-dritt ta' oġġezzjoni. Is-suġġett tad-dejta jista' jikkuntattjana biex jeżerċita d-dritt li joġġezzjona.

***Dritt għall-portabbiltà tad-data***

Art. 20 GDPR jagħti lis-suġġett tad-dejta d-dritt għall-portabbiltà tad-dejta. Skont din id-dispożizzjoni, is-suġġett tad-data għandu taħt il-kundizzjonijiet stabbiliti fArtikolu 20(1) lit. a u b GDPR id-dritt li jirċievi d-dejta personali li tikkonċernah, li huwa jkun ipprovda lil kontrollur, f'format strutturat, użat komunement u li jinqara mill-magni u jkollu d-dritt li jittrasmetti dik id-dejta lil kontrollur ieħor mingħajr xkiel mill-kontrollur li lilu tkun ġiet ipprovduta d-dejta personali. Is-suġġett tad-dejta jista' jikkuntattjana biex jeżerċita d-dritt għall-portabbiltà tad-dejta.

## I. Fejn l-ipproċessar ikun ibbażat fuq il-punt (a) tal-Artikolu 6(1) jew il-punt (a) tal-Artikolu 9(2), l-eżistenza tad-dritt li jiġi irtirat il-kunsens fi kwalunkwe ħin, mingħajr ma tiġi affettwata l-legalità tal-ipproċessar abbażi ta' kunsens qabel l-irtirar tiegħu (Artikolu 13(2) lit. c GDPR)

Jekk l-ipproċessar tad-dejta personali huwa bbażat fuq l-Art. 6(1) lit. GDPR, li huwa l-każ, jekk is-suġġett tad-data jkun ta l-kunsens għall-ipproċessar ta' data personali għal skop speċifiku wieħed jew aktar jew ikun ibbażat fuq Artikolu 9(2) lit. a GDPR, li jirregola l-kunsens espliċitu għall-ipproċessar ta' kategoriji speċjali ta ' data personali, is-suġġett tad-data għandu skont Artikolu 7(3) Sentenza 1 GDPR id-dritt li jirtira l-kunsens tiegħu jew tagħha fi kwalunkwe ħin.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

L-irtirar tal-kunsens m'għandux jaffettwa l-legalità tal-ipproċessar ibbażat fuq il-kunsens qabel l-irtirar tiegħu, Artikolu 7(3) Sentenza 2 GDPR. Għandu jkun faċli li tirtira daqskemm jingħata l-kunsens, Art. 7(3) Sentenza 4 GDPR. Għalhekk, l-irtirar tal-kunsens jista' dejjem iseħħ bl-istess mod kif ikun ingħata l-kunsens jew b'xi mod ieħor, li jitqies mis-suġġett tad-data bħala aktar sempliċi. Fis -soċjetà tal-informazzjoni tal -lum , probabbilment l-aktar mod sempliċi biex tirtira l-kunsens huwa email sempliċi. Jekk is-suġġett tad-dejta jixtieq jirtira l-kunsens tiegħu jew tagħha mogħti lilna, email sempliċi lilna hija biżżejjed. Inkella, is-suġġett tad-dejta jista' jagħżel kwalunkwe mod ieħor biex jikkomunika lilna l-irtirar tal-kunsens tiegħu jew tagħha.

## J. Id-dritt li jitressaq ilment quddiem awtorità superviżorja (Artikolu 13(2) lit. d, 77(1) GDPR)

Bħala l-kontrollur, aħna obbligati ninnotifikaw lis-suġġett tad-dejta bid-dritt li jitressaq ilment ma' awtorità ta' superviżjoni, Artikolu 13(2) lit. d GDPR. Id-dritt li jitressaq ilment ma' awtorità superviżorja huwa rregolat milArtikolu 77(1) GDPR. Skont din id-dispożizzjoni, mingħajr preġudizzju għal kwalunkwe rimedju amministrattiv jew ġudizzjarju ieħor, kull suġġett tad-data għandu jkollu d-dritt li jressaq ilment ma' awtorità ta' superviżjoni, b'mod partikolari fl-Istat Membru tar-residenza abitwali tiegħu jew tagħha, il-post tax-xogħol jew il-post ta' l-allegat ksur jekk is-suġġett tad-dejta jikkunsidra li l-ipproċessar tad-dejta personali relatata miegħu jew tagħha jikser ir-Regolament Ġenerali dwar il-Protezzjoni tad-Data. Id-dritt li jitressaq ilment ma' awtorità superviżorja kien limitat biss mil-liġi tal-Unjoni b'tali mod, li jista' jiġi eżerċitat biss quddiem awtorità superviżorja waħda (Premessa 141 Sentenza 1 GDPR). Din ir-regola hija maħsuba biex tevita lmenti doppji tal-istess suġġett tad-dejta fl-istess kwistjoni. Jekk suġġett tad-dejta jrid iressaq ilment dwarna, għalhekk tlabna nikkuntattjaw awtorità superviżorja waħda biss.

## K. Jekk il-forniment ta' data personali huwiex rekwiżit statutorju jew kuntrattwali, jew rekwiżit meħtieġ biex wieħed jidħol f'kuntratt, kif ukoll jekk is-suġġett tad-data huwiex obbligat jipprovdi d-data personali u l-konsegwenzi possibbli meta wieħed jonqos milli jipprovdi tali data (Art. 13(2) lit. e GDPR)

Aħna niċċaraw li l-provvista ta' data personali hija parzjalment meħtieġa mil-liġi ( eż. regolamenti tat-taxxa) jew tista' tirriżulta wkoll minn dispożizzjonijiet kuntrattwali (eż. informazzjoni dwar is-sieħeb kuntrattwali).

Xi drabi jista' jkun meħtieġ li jiġi konklużż kuntratt li s-suġġett tad-dejta jipprovdilna data personali, li sussegwentement trid tiġi pproċessata minna. Is-suġġett tad-data huwa, pereżempju, obbligat li jipprovdilna data personali meta l-kumpanija tagħna tiffirma kuntratt miegħu jew magħha. In-nuqqas ta' forniment tad-dejta personali jkollu l-konsegwenza li l-kuntratt mas-suġġett tad-dejta ma jistax jiġi konklużż.

Qabel ma tiġi pprovduta d-dejta personali mis-suġġett tad-dejta, is-suġġett tad-dejta għandu jikkuntattjana. Aħna niċċaraw lis-suġġett tad-dejta jekk il-provvista tad-dejta personali hijiex meħtieġa mil-


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

liġi jew bil-kuntratt jew jekk huwiex meħtieġ għall-konklużjoni tal-kuntratt, jekk hemmx obbligu li tiġi pprovduta d-dejta personali u l- konsegwenzi tan-nuqqas ta' forniment tad-dejta personali. data.

### L. L-eżistenza ta' teħid awtomatizzat ta' deċiżjonijiet inkluż it-tfassil ta' profili msemmi fl-Artikolu 22(1) u (4) u għall-inqas f'dawk il-każijiet, l-informazzjoni importanti dwar il-loġika involuta, kif ukoll is-sinifikat u l-konsegwenzi previsti ta' tali proċessar għas-suġġett tad-data (Artikolu 13 (2) lit. f GDPR)

Bħala kumpanija responsabbli, ġeneralment ma nużawx teħid ta' deċiżjonijiet jew profili awtomatizzati. Jekk, f'każijiet eċċezzjonali, inwettqu teħid ta' deċiżjonijiet jew tfassil ta' profili awtomatizzati, aħna se ninfurmaw lis-suġġett tad-dejta jew separatament jew permezz ta' sottosezzjoni fil-politika ta' privatezza tagħna (fuq il-websajt tagħna). F'dan il-każ, japplika dan li ġej:

Teħid ta' deċiżjonijiet awtomatizzat - inkluż it-tfassil ta' profili - jista' jseħħ jekk (1) dan ikun meħtieġ għad-dħul fi, jew it-twettiq ta', kuntratt bejn is-suġġett tad-data u magħna, jew (2) dan huwa awtorizzat mil-liġi tal-Unjoni jew tal-Istat Membru li għaliha aħna huma suġġetti u li jistabbilixxi wkoll miżuri xierqa biex jissalvagwardjaw id-drittijiet u l-libertajiet u l-interessi leġittimi tas-suġġett tad-dejta; jew (3) dan huwa bbażat fuq il-kunsens espliċitu tas-suġġett tad-dejta.

Fil-każijiet imsemmija fl-Artikolu 22(2) (a) u (c) GDPR, aħna nimplimentaw miżuri xierqa biex nissalvagwardjaw id-drittijiet u l-libertajiet u l-interessi leġittimi tas-suġġett tad-data. F'dawn il-każijiet, għandek id-dritt li tikseb intervent uman min-naħa tal-kontrollur, li tesprimi l-opinjoni tiegħek u li tikkontesta d-deċiżjoni.

Informazzjoni sinifikanti dwar il-loġika involuta, kif ukoll is-sinifikat u l-konsegwenzi previsti ta 'tali ipproċessar għas-suġġett tad-data hija stabbilita fil-politika ta' privatezza tagħna.

## II. Informazzjoni li għandha tiġi pprovduta fejn id-data personali ma tkunx inkisbet mis-suġġett tad-data (Artikolu 14 tal-GDPR)

### A. L-identità u d-dettalji ta' kuntatt tal-kontrollur u, fejn applikabbli, tar-rappreżentant tal-kontrollur (Artikolu 14(1) lit. a GDPR)

Ara hawn fuq


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## B. Id-dettalji ta' kuntatt tal-uffiċjal tal-protezzjoni tad-data, fejn applikabbli (Artikolu 14(1) lit. b GDPR)

Ara hawn fuq

## C. L-għanijiet tal-ipproċessar li għalihom hija maħsuba d-data personali kif ukoll il-bażi legali għall-ipproċessar (Artikolu 14(1) lit. c GDPR)

L-għan tal-ipproċessar tad-dejta personali huwa l-immaniġġjar tal-operazzjonijiet kollha li jikkonċernaw lill-kontrollur, klijenti, klijenti prospettivi, imsieħba fin-negozju jew relazzjonijiet kuntrattwali jew prekuntrattwali oħra bejn il-gruppi msemmija (fl-iktar sens wiesa') jew obbligi legali tal-kontrollur.

Jekk l-ipproċessar tad-dejta personali huwa meħtieġ għat-twettiq ta' kuntratt li għalih is-suġġett tad-dejta huwa parti, kif inhu l-każ, pereżempju, meta l-operazzjonijiet tal-ipproċessar huma meħtieġa għall-provvista ta' oġġetti jew biex jipprovdu kwalunkwe servizz ieħor, l-ipproċessar huwa ibbażat fuq Artikolu 6(1) lit. b GDPR. L-istess japplika għal tali operazzjonijiet ta' pproċessar li huma meħtieġa għat-twettiq ta' miżuri prekuntrattwali, pereżempju fil-każ ta' mistoqsijiet li jikkonċernaw il-prodotti jew is-servizzi tagħna. Il-kumpanija tagħna hija soġġetta għal obbligu legali li permezz tiegħu l-ipproċessar tad-dejta personali huwa meħtieġ, bħal għat-twettiq tal-obbligi tat-taxxa, l-ipproċessar huwa bbażat fuq l-Art. 6(1) lit. c GDPR.

F'każijiet rari, l-ipproċessar ta' data personali jista' jkun meħtieġ biex jipproteġi l-interessi vitali tas-suġġett tad-data jew ta' persuna fiżika oħra. Dan ikun il-każ, pereżempju, jekk viżitatur weġġa' fil-kumpanija tagħna u ismu, l-età, id-dejta tal-assigurazzjoni tas-saħħa jew informazzjoni vitali oħra jkollhom jiġu mgħoddija lil tabib, sptar jew parti terza oħra. Imbagħad l-ipproċessar ikun ibbażat fuq l-Art. 6(1) lit. d GDPR.

Fejn l-ipproċessar ikun meħtieġ għat-twettiq ta' kompitu mwettaq fl-interess pubbliku jew fl-eżerċizzju ta' awtorità uffiċjali vestita fil-kontrollur, il-bażi legali hija l-Art. 6(1) lit. e GDPR.

Fl-aħħar nett, operazzjonijiet ta' pproċessar jistgħu jkunu bbażati fuq Artikolu 6(1) lit. f GDPR. Din il-bażi legali tintuża għal operazzjonijiet ta' pproċessar li mhumiex koperti minn xi waħda mir-raġunijiet legali msemmija hawn fuq, jekk l-ipproċessar ikun meħtieġ għall-finijiet tal-interessi leġittimi segwiti mill-kumpanija tagħna jew minn parti terza, ħlief fejn dawn l-interessi jiġu ssuperati mill-interessi. jew id-drittijiet u l-libertajiet fundamentali tas-suġġett tad-data li jeħtieġu protezzjoni tad-data personali. Operazzjonijiet ta' pproċessar bħal dawn huma partikolarment permissibbli minħabba li ġew imsemmija speċifikament mil-leġiżlatur Ewropew. Huwa kkunsidra li jista' jiġi preżunt interess leġittimu jekk is-suġġett tad-dejta jkun klijent tal-kontrollur (Premessa 47 Sentenza 2 GDPR).

## D. Il-kategoriji ta' data personali inkwistjoni (Artikolu 14(1) lit. d GDPR)


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

Data tal-klijent

Data ta' klijenti potenzjali

Data tal-impjegati

Data tal-forniturі

## E. Ir-riċevituri jew il-kategoriji ta' riċevituri tad-data personali, jekk jeżistu (Artikolu 14(1) lit. e GDPR)

Awtoritajiet pubbliċi

Korpi esterni

Aktar korpi esterni

Ipproċessar intern

Ipproċessar intragrupp

Korpi oħra

Lista tal-proċessuri u r-riċevituri tad-dejta tagħna f'pajjiżi terzi u, jekk applikabbli, organizzazzjonijiet internazzjonali jew tiġi ppubblikata fuq il-websajt tagħna jew tista' tintalab mingħandna mingħajr ħlas. Jekk jogħġbok ikkuntattja lill-uffiċjal tal-protezzjoni tad-dejta tagħna biex titlob din il-lista.

## F. Fejn applikabbli, il-fatt li l-kontrollur għandu l-ħsieb li jittrasferixxi data personali lil riċevitur f'pajjiż terz jew organizzazzjoni internazzjonali u l-eżistenza jew l-assenza ta' deċiżjoni ta' adegwatezza mill-Kummissjoni, jew fil-każ ta' trasferimenti msemmija fl-Artikolu 46 jew 47, jew it-tieni subparagrafu tal-Artikolu 49(1), referenza għas-salvagwardji xierqa jew adatti u l-mezzi biex tinkiseb kopja tagħhom jew fejn dawn ikunu saru disponibbli (Artikolu 14(1) lit. f, 46(1), 46(2) lit. c GDPR)

Il-kumpaniji u l-fergħat kollha li huma parti mill-grupp tagħna (minn hawn 'il quddiem imsejħa "kumpaniji tal-grupp") li għandhom il-post tan-negozju tagħhom jew uffiċċju f'pajjiż terz jistgħu jappartjenu għar-riċevituri tad-dejta personali. Lista tal-kumpaniji kollha tal-grupp tista' tintalab mingħandna.

Skont Artikolu 46(1) GDPR kontrollur jew proċessur jista’ jittrasferixxi data personali biss lil pajjiż terz jekk il-kontrollur jew proċessur ikun ipprovda salvagwardji xierqa, u bil-kundizzjoni li jkunu disponibbli drittijiet infurzabbli tas-suġġett tad-data u rimedji legali effettivi għas-suġġetti tad-data. Jistgħu jiġu pprovduti


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

salvagwardji xierqa mingħajr ma tkun meħtieġa xi awtorizzazzjoni speċifika minn awtorità superviżorja permezz ta' klawsoli standard ta' protezzjoni tad-dejta, Artikolu 46(2) lit. c GDPR.

Il-klawsoli kuntrattwali standard tal-Unjoni Ewropea jew salvagwardji xierqa oħra huma miftiehma marriċevituri kollha minn pajjiżi terzi qabel l-ewwel trażmissjoni tad-dejta personali. Konsegwentement, huwa żgurat li jkunu garantiti salvagwardji xierqa, drittijiet infurzabbli tas-suġġett tad-data u rimedji legali effettivi għas-suġġetti tad-data. Kull suġġett tad-dejta jista' jikseb kopja tal-klawsoli kuntrattwali standard mingħandna. Il-klawsoli kuntrattwali standard huma wkoll disponibbli fil-Ġurnal Uffiċjali tal-Unjoni Ewropea.

L-Artikolu 45(3) tar-Regolament Ġenerali dwar il-Protezzjoni tad-Dejta (GDPR) jagħti lill-Kummissjoni Ewropea s-setgħa li tiddeċiedi, permezz ta' att ta' implimentazzjoni, li pajjiż mhux tal-UE jiżgura livell adegwat ta' protezzjoni. Dan ifisser livell ta' protezzjoni għad-dejta personali li huwa essenzjalment ekwivalenti għal-livell ta' protezzjoni fl-UE. L-effett tad-deċiżjonijiet dwar l-adegwatezza huwa li d-dejta personali tista' tiċċirkola liberament mill-UE (u n-Norveġja, il-Liechtenstein u l-Islanda) lejn pajjiż terz mingħajr aktar ostakli. Regoli simili jeżistu għar-Renju Unit, l-Isvizzera u xi Pajjiżi oħra.

Fejn il-Kummissjoni Ewropea jew il-gvern ta' pajjiż ieħor iddeċieda li pajjiż terz jiżgura livell adegwat ta' protezzjoni, u Qafas validu jkun fis-seħħ (eż. EU-U.S. Data Privacy Framework, Swiss-U.S. Data Privacy Framework, UK Extension to the EU-U.S. Data Privacy Framework), it-trasferimenti kollha minna lill-membri ta' tali oqfsa (eż. entitajiet awtoċertifikati) huma bbażati esklussivament fuq is-sħubija ta' dik l-entitajiet fil-qafas rispettiv. Fejn aħna jew waħda mill-entitajiet tal-grupp tagħna tkun membru ta' tali qafas, it-trasferimenti kollha lilna jew lill-entità tal-grupp tagħna huma bbażati esklussivament fuq is-sħubija tal-entitajiet f'tali qafas.

Kwalunkwe suġġett tad-dejta jista' jikseb kopja tal-oqfsa mingħandna. Barra minn hekk, l-oqfsa huma wkoll disponibbli fil-Ġurnal Uffiċjali tal-Unjoni Ewropea jew fil-materjali legali ppubblikati jew fuq il-websajts tal-awtoritajiet superviżorji jew awtoritajiet jew istituzzjonijiet kompetenti oħra.

## G. Il-perijodu li matulu d-data personali tkun ser tinħażen, jew jekk dak ma jkunx possibbli, il-kriterji użati biex jiġi ddeterminat dak il-perijodu (Artikolu 14(2) lit. a GDPR)

Il-kriterji użati biex jiġi ddeterminat il-perjodu ta' ħażna ta' data personali huwa l-perjodu ta' żamma statutorju rispettiv. Wara li jiskadi dak il-perjodu, id-dejta korrispondenti titħassar b'mod regolari, sakemm ma tibqax meħtieġa għat-twettiq tal-kuntratt jew għall-bidu ta' kuntratt.

Jekk ma jkunx hemm perjodu statutorju ta' żamma, il-kriterju huwa l-perjodu ta' żamma kuntrattwali jew intern.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## H. Fejn l-ipproċessar ikun ibbażat fuq il-punt (f) tal-Artikolu 6(1), l-interessi leġittimi segwiti mill-kontrollur jew minn parti terza (Art. 14(2) lit. b GDPR)

Skont Artikolu 6(1) lit. f GDPR, l-ipproċessar għandu jkun legali biss jekk l-ipproċessar ikun meħtieġ għall-iskopijiet ta' interessi leġittimi segwiti mill-kontrollur jew minn parti terza, ħlief fejn dawn l-interessi huma megħluba mill-interessi jew id-drittijiet u l-libertajiet fundamentali tas-suġġett tad-data li jeħtieġu protezzjoni tad-data personali. Skont il-Premessa 47 Sentenza 2 GDPR jista' jeżisti interess leġittimu fejn ikun hemm relazzjoni rilevanti u xierqa bejn is-suġġett tad-dejta u l-kontrollur, eż. f'sitwazzjonijiet fejn is-suġġett tad-dejta huwa klijent tal-kontrollur. Fil-każijiet kollha li fihom il-kumpanija tagħna tipproċessa data personali bbażata fuq Artikolu 6(1) lit. f GDPR, l-interess leġittimu tagħna huwa li nwettqu n-negozju tagħna favur il-benessri tal-impjegati kollha tagħna u l-azzjonisti.

## I. L-eżistenza tad-dritt li jitlob mingħand il-kontrollur aċċess jew rettifika jew tħassir ta' data personali jew restrizzjoni tal-ipproċessar rigward is-suġġett tad-data u li joġġezzjona għall-ipproċessar kif ukoll id-dritt għall-portabbiltà tad-data (Artikolu 14(2) lit. c GDPR)

Is-suġġetti tad-dejta kollha għandhom id-drittijiet li ġejjin:

***Dritt għall-aċċess***

Kull suġġett tad-dejta għandu dritt li jaċċessa d-dejta personali li tikkonċernah jew lilha. Id-dritt għall-aċċess jestendi għad-dejta kollha pproċessata minna. Id-dritt jista' jiġi eżerċitat faċilment u f'intervalli raġonevoli, sabiex tkun konxju ta', u tivverifika, il-legalità tal-ipproċessar (Premessa 63 GDPR). Dan id-dritt jirriżulta mill-Art. 15 GDPR. Is-suġġett tad-dejta jista' jikkuntattjana biex jeżerċita d-dritt ta' aċċess.

***Dritt għal rettifika***

Skont Artikolu 16 Sentenza 1 GDPR is-suġġett tad-dejta għandu d-dritt li jikseb mingħand il-kontrollur mingħajr dewmien żejjed ir-rettifika ta' data personali mhux eżatta li tikkonċernah. Barra minn hekk, Artikolu 16 Sentenza 2 tal-GDPR jipprovdi li s-suġġett tad-data huwa intitolat, b'kont meħud tal-għanijiet tal-ipproċessar, li jimtela data personali mhux kompluta, inkluż permezz tal-għoti ta' dikjarazzjoni supplimentari. Is-suġġett tad-dejta jista' jikkuntattjana biex jeżerċita d-dritt ta' rettifika.

***Dritt għat-tħassir (dritt li jintesa)***

Barra minn hekk, is-suġġetti tad-data huma intitolati għal dritt għat-tħassir u li jintesew taħt l-Art. 17 GDPR. Dan id-dritt jista' jiġi eżerċitat ukoll billi tikkuntattjana. F'dan il-punt, madankollu, nixtiequ nirrimarkaw li dan id-dritt ma japplikax safejn l-ipproċessar huwa meħtieġ biex tissodisfa obbligu legali li l-kumpanija tagħna hija soġġetta għalih, Artikolu 17(3) lit. b GDPR. Dan ifisser li nistgħu napprovaw applikazzjoni biex titħassar biss wara li jiskadi l-perjodu statutorju ta' żamma.

***Dritt g]al restrizzjoni ta' pro'essar***

Skont Artikolu 18 tal-GDPR kull suġġett tad-dejta huwa intitolat għal restrizzjoni tal-ipproċessar. Ir-restrizzjoni tal-ipproċessar tista' tintalab jekk waħda mill-kundizzjonijiet stipulati fArtikolu 18(1) lit. ad


© All rights reserved by Heiko Maniero.

GDPR huwa sodisfatt. Is-suġġett tad-dejta jista' jikkuntattjana biex jeżerċita d-dritt għal restrizzjoni tal-ipproċessar.

***Dritt ta' oġġezzjoni***

Barra minn hekk, l-Art. 21 GDPR jiggarantixxi d-dritt ta' oġġezzjoni. Is-suġġett tad-dejta jista' jikkuntattjana biex jeżerċita d-dritt li joġġezzjona.

***Dritt għall-portabbiltà tad-data***

Art. 20 GDPR jagħti lis-suġġett tad-dejta d-dritt għall-portabbiltà tad-dejta. Skont din id-dispożizzjoni s-suġġett tad-dejta għandu taħt il-kundizzjonijiet stabbiliti fArtikolu 20(1) lit. a u b GDPR id-dritt li jirċievi d-dejta personali li tikkonċernah, li huwa jkun ipprovda lil kontrollur, f'format strutturat, użat komunement u li jinqara mill-magni u jkollu d-dritt li jittrasmetti dik id-dejta lil kontrollur ieħor mingħajr xkiel mill-kontrollur li lilu tkun ġiet ipprovduta d-dejta personali. Is-suġġett tad-dejta jista' jikkuntattjana biex jeżerċita d-dritt għall-portabbiltà tad-dejta.

## J. Fejn l-ipproċessar ikun ibbażat fuq il-punt (a) tal-Artikolu 6(1) jew il-punt (a) tal-Artikolu 9(2), l-eżistenza tad-dritt li jiġi irtirat il-kunsens fi kwalunkwe ħin, mingħajr ma tiġi affettwata l-legalità tal-ipproċessar abbażi ta' kunsens qabel l-irtirar tiegħu (Art. 14(2) lit. d GDPR)

Jekk l-ipproċessar tad-dejta personali huwa bbażat fuq l-Art. 6(1) lit. GDPR, li huwa l-każ, jekk is-suġġett tad-data jkun ta l-kunsens għall-ipproċessar ta' data personali għal skop speċifiku wieħed jew aktar jew ikun ibbażat fuq Artikolu 9(2) lit. a GDPR, li jirregola l-kunsens espliċitu għall-ipproċessar ta' kategoriji speċjali ta' data personali, is-suġġett tad-data għandu skont Artikolu 7(3) Sentenza 1 GDPR id-dritt li jirtira l-kunsens tiegħu jew tagħha fi kwalunkwe ħin.

L-irtirar tal-kunsens m'għandux jaffettwa l-legalità tal-ipproċessar ibbażat fuq il-kunsens qabel l-irtirar tiegħu, Artikolu 7(3) Sentenza 2 GDPR. Għandu jkun faċli li tirtira daqskemm jingħata l-kunsens, Art. 7(3) Sentenza 4 GDPR. Għalhekk, l-irtirar tal-kunsens jista' dejjem iseħħ bl-istess mod kif ikun ingħata l-kunsens jew b'xi mod ieħor, li jitqies mis-suġġett tad-data bħala aktar sempliċi. Fis -soċjetà tal-informazzjoni tal -lum , probabbilment l-aktar mod sempliċi biex tirtira l-kunsens huwa email sempliċi. Jekk is-suġġett tad-dejta jixtieq jirtira l-kunsens tiegħu jew tagħha mogħti lilna, email sempliċi lilna hija biżżejjed. Inkella, is-suġġett tad-dejta jista' jagħżel kwalunkwe mod ieħor biex jikkomunika lilna l-irtirar tal-kunsens tiegħu jew tagħha.

## K. Id-dritt li jitressaq ilment quddiem awtorità superviżorja (Artikolu 14(2) lit. e, 77(1) GDPR)

Bħala l-kontrollur, aħna obbligati li ninnotifikaw lis-suġġett tad-dejta bid-dritt li jressaq ilment ma' awtorità superviżorja, Artikolu 14(2) lit. e GDPR. Id-dritt li jitressaq ilment ma' awtorità superviżorja huwa rregolat


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

milArtikolu 77(1) GDPR. Skont din id-dispożizzjoni, mingħajr preġudizzju għal kwalunkwe rimedju amministrattiv jew ġudizzjarju ieħor, kull suġġett tad-data għandu jkollu d-dritt li jressaq ilment ma' awtorità ta' superviżjoni, b'mod partikolari fl-Istat Membru tar-residenza abitwali tiegħu jew tagħha, il-post tax-xogħol jew il-post ta' l-allegat ksur jekk is-suġġett tad-dejta jikkunsidra li l-ipproċessar tad-dejta personali relatata miegħu jew tagħha jikser ir-Regolament Ġenerali dwar il-Protezzjoni tad-Data. Id-dritt li jitressaq ilment ma' awtorità superviżorja kien limitat biss mil-liġi tal-Unjoni b'tali mod, li jista' jiġi eżerċitat biss quddiem awtorità superviżorja waħda (Premessa 141 Sentenza 1 GDPR). Din ir-regola hija maħsuba biex tevita lmenti doppji tal-istess suġġett tad-dejta fl-istess kwistjoni. Jekk suġġett tad-dejta jrid iressaq ilment dwarna, għalhekk tlabna nikkuntattjaw awtorità superviżorja waħda biss.

## L. Minn liema sors toriġina d-data personali, u fejn applikabbli jekk oriġinatx minn sorsi aċċessibbli għall-pubbliku (Artikolu 14(2) lit. f GDPR)

Fil-prinċipju, id-dejta personali tinġabar direttament mis-suġġett tad-dejta jew f'kooperazzjoni ma' awtorità (eż. irkupru ta' dejta minn reġistru uffiċjali). Data oħra dwar suġġetti tad-data huma derivati minn trasferimenti ta' kumpaniji tal-grupp. Fil-kuntest ta' din l-informazzjoni ġenerali, l-isem tas-sorsi eżatti li minnhom tkun oriġinat id-dejta personali huwa jew impossibbli jew ikun jinvolvi sforz sproporzjonat fis-sens tal-Art. 14(5) lit. b GDPR. Fil-prinċipju, aħna ma niġbrux data personali minn sorsi aċċessibbli għall-pubbliku.

Kwalunkwe suġġett tad-dejta jista' jikkuntattjana fi kwalunkwe ħin biex jikseb informazzjoni aktar dettaljata dwar is-sorsi eżatti tad-dejta personali li tikkonċernah jew lilha. Fejn l-oriġini tad-dejta personali ma tistax tiġi pprovduta lis-suġġett tad-dejta minħabba li jkunu ntużaw diversi sorsi, għandha tingħata informazzjoni ġenerali (Premessa 61 Sentenza 4 GDPR).

## M. L-eżistenza ta' teħid awtomatizzat ta' deċiżjonijiet inkluż it-tfassil ta' profili msemmi fl-Artikolu 22(1) u (4) u għall-inqas f'dawk il-każijiet, l-informazzjoni importanti dwar il-loġika involuta, kif ukoll is-sinifikat u l-konsegwenzi previsti ta' tali pproċessar għas-suġġett tad-dat (Artikolu 14(2) lit. g GDPR)

Bħala kumpanija responsabbli, ġeneralment ma nużawx teħid ta' deċiżjonijiet jew profili awtomatizzati. Jekk, f'każijiet eċċezzjonali, inwettqu teħid ta' deċiżjonijiet jew tfassil ta' profili awtomatizzati, aħna se ninfurmaw lis-suġġett tad-dejta jew separatament jew permezz ta' sottosezzjoni fil-politika ta' privatezza tagħna (fuq il-websajt tagħna). F'dan il-każ, japplika dan li ġej:

Teħid ta' deċiżjonijiet awtomatizzat - inkluż it-tfassil ta' profili - jista' jseħħ jekk (1) dan ikun meħtieġ għad-dħul fi, jew it-twettiq ta', kuntratt bejn is-suġġett tad-data u magħna, jew (2) dan huwa awtorizzat mil-liġi tal-Unjoni jew tal-Istat Membru li għaliha aħna huma suġġetti u li jistabbilixxi wkoll miżuri xierqa biex jissalvagwardjaw id-drittijiet u l-libertajiet u l-interessi leġittimi tas-suġġett tad-dejta; jew (3) dan huwa bbażat fuq il-kunsens espliċitu tas-suġġett tad-dejta.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

Fil-każijiet imsemmija fl-Artikolu 22(2) (a) u (c) GDPR, aħna nimplimentaw miżuri xierqa biex nissalvagwardjaw id-drittijiet u l-libertajiet u l-interessi leġittimi tas-suġġett tad-data. F'dawn il-każijiet, għandek id-dritt li tikseb intervent uman min-naħa tal-kontrollur, li tesprimi l-opinjoni tiegħek u li tikkontesta d-deċiżjoni.

Informazzjoni sinifikanti dwar il-loġika involuta, kif ukoll is-sinifikat u l-konsegwenzi previsti ta 'tali ipproċessar għas-suġġett tad-data hija stabbilita fil-politika ta' privatezza tagħna.

## III. EU-U.S. Data Privacy Framework (EU-U.S. DPF), UK Extension to the EU-U.S. DPF, Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF)

Jekk l-organizzazzjoni tagħna hija membru ċċertifikat tal-EU-U.S. Data Privacy Framework (EU-U.S. DPF) u/jew l-UK Extension to the EU-U.S. DPF u/jew il-Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF), japplika dan li ġej:

Aħna nżommu mal-EU-U.S. Data Privacy Framework (EU-U.S. DPF) u l-UK Extension to the EU-U.S. DPF kif ukoll il-Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF), kif stabbilit mill-U.S. Department of Commerce. Il-kumpanija tagħna kkonfermat mad-Dipartiment tal-Kummerċ tal-Istati Uniti li tikkonforma mal-EU-U.S. Data Privacy Framework Principles (EU-U.S. DPF Principles) fir-rigward tal-ipproċessar ta' data personali li tirċievi mill-Unjoni Ewropea u mir-Renju Unit taħt il-EU-U.S. DPF u l-UK Extension to the EU-U.S. DPF. Il-kumpanija tagħna kkonfermat mad-Dipartiment tal-Kummerċ tal-Istati Uniti li tikkonforma mal-Swiss-U.S. Data Privacy Framework Principles (Swiss-U.S. DPF Principles) fir-rigward tal-ipproċessar ta' data personali li tirċievi mill-Iżvizzera taħt il-Swiss-U.S. DPF. Fil-każ ta' kunflitt bejn id-dispożizzjonijiet tal-politika tal-privatezza tagħna u l-EU-U.S. DPF Principles u/jew il-Swiss-U.S. DPF Principles, il-Principles għandhom jipprevalu.

Biex titgħallem aktar dwar il-programm Data Privacy Framework (DPF) u biex tara ċ-ċertifikazzjoni tagħna, jekk jogħġbok żur https://www.dataprivacyframework.gov/.

L-unitajiet oħra tal-Istati Uniti jew is-sussidjarji tal-kumpanija tagħna li wkoll jikkonformaw mal-EU-U.S. DPF Principals, inklużi l-UK Extension to the EU-U.S. DPF u l-Swiss-U.S. DPF Principals, jekk applikabbli, huma mniżżla fil-politika tal-privatezza tagħna.

F'konformità mal-EU-U.S. DPF u l-UK Extension to the EU-U.S. DPF kif ukoll il-Swiss-U.S. DPF, il-kumpanija tagħna timpenja ruħha li tikkopera mal-panel stabbilit mill-awtoritajiet tal-protezzjoni tad-data tal-UE u l-Information Commissioner's Office (ICO) tar-Renju Unit, kif ukoll il-Kummissarju Federali għall-Protezzjoni tad-Data u l-Informazzjoni (EDÖB) tal-Iżvizzera, u li ssegwi l-pariri tagħhom dwar ilmenti mhux solvuti dwar it-trattament tagħna ta' data personali li nirċievu taħt il-EU-U.S. DPF u l-UK Extension to the EU-U.S. DPF u l-Swiss-U.S. DPF.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

Aħna ninformaw lill-persuni affettwati dwar l-awtoritajiet Ewropej kompetenti għall-protezzjoni tad-data li huma responsabbli għall-immaniġġjar ta' ilmenti dwar it-trattament tad-data personali mill-organizzazzjoni tagħna, fil-parti ta' fuq ta' dan id-dokument ta' trasparenza u li noffru lil persuni affettwati rimedju legali xieraq u bla ħlas.

Aħna ninformaw lill-persuni affettwati kollha li l-kumpanija tagħna hija suġġetta għall-poteri ta' investigazzjoni u infurzar tal-Federal Trade Commission (FTC).

Il-persuni affettwati għandhom, taħt ċerti kundizzjonijiet, il-possibbiltà li jagħmlu użu minn arbitraġġ vinkolanti. L-organizzazzjoni tagħna hija obbligata li tirrisolvi talbiet u tikkonforma mal-kundizzjonijiet stipulati fl-Anness I tal-DPF-Principals, jekk il-persuna affettwata titlob arbitraġġ vinkolanti billi tinforma lill-organizzazzjoni tagħna u l-proċeduri u l-kundizzjonijiet stipulati fl-Anness I tal-Principals ikunu ġew segwiti.

Aħna ninformaw b'dan lill-persuni affettwati kollha dwar ir-responsabbiltà tal-organizzazzjoni tagħna fil-każ ta' trasferiment ta' data personali lil partijiet terzi.

Għal mistoqsijiet tal-persuni affettwati jew tal-awtoritajiet superviżorji tad-data, aħna nnominaw lir-rappreżentanti lokali msemmija aktar 'il fuq f'dan id-dokument ta' trasparenza.

Noffrulek il-possibbiltà li tagħżel (Opt-out) jekk id-data personali tiegħek (i) għandhiex tiġi trasferita lil partijiet terzi jew (ii) għandhiex tiġi użata għal skop li jkun sostanzjalment differenti mill-iskop(i) għall-kwal/i tkun inġabret oriġinarjament jew aktar tard awtorizzajt int. Il-mekkaniżmu ċar, viżibbli u faċilment aċċessibbli biex teżerċita l-għażla tiegħek huwa li tikkuntattja lill-uffiċjal tal-protezzjoni tad-data tagħna (DSB) permezz ta' email. M'għandekx għażla u m'aħniex obbligati li nagħmlu dan jekk id-data tiġi trasferita lil parti terza li taġixxi bħala aġent jew proċessur f'isem tagħna u skont l-istruzzjonijiet tagħna. Madankollu, dejjem nagħmlu kuntratt ma' tali aġent jew proċessur.

Għal data sensittiva (jiġifieri data personali li fiha informazzjoni dwar l-istat tas-saħħa, l-oriġini razzjali jew etnika, opinjonijiet politiċi, twemmin reliġjuż jew filosofiku, sħubija fi trade union jew informazzjoni dwar il-ħajja sesswali tal-persuna kkonċernata) niksbu l-kunsens espliċitu tiegħek (Opt-in) meta din id-data (i) tiġi trasferita lil partijiet terzi jew (ii) tiġi użata għal skop differenti minn dak li għalih tkun inġabret oriġinarjament jew għal liema int aktar tard tajt il-kunsens tiegħek billi għażilt l-għażla Opt-in. Barra minn hekk, nittrattaw id-data personali kollha li nirċievu mingħand partijiet terzi bħala sensittiva jekk it-terza parti tidentifikaha u tittrattaha bħala sensittiva.

Aħna ninformawk b'dan dwar ir-rekwiżit li jiġu żvelati data personali bħala rispons għal talbiet legali mill-awtoritajiet, inklużi l-konformità mar-rekwiżiti ta' sigurtà nazzjonali jew infurzar tal-liġi.

Meta nittrasferixxu data personali lil parti terza li taġixxi bħala kontrollur, nikkonformaw mal-Principals ta' notifika u għażla. Barra minn hekk, nagħmlu kuntratt mal-parti terza li hija responsabbli għat-trattament li jipprovdi li din id-data tista' tiġi pproċessata biss għal skopijiet limitati u speċifikati skont il-kunsens mogħti minnek u li r-riċevitur irid jipprovdi l-istess livell ta' protezzjoni bħal Principals tad-DPF u jinfurmana jekk jiddetermina li ma jistax ikompli jikkonforma ma' din l-obbligazzjoni. Il-kuntratt jipprovdi li l-parti terza, li


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

hija responsabbli, tieqaf ipproċessar jew tieħu miżuri oħra xierqa u adegwati biex tirrimedja s-sitwazzjoni jekk ssir din id-determinazzjoni.

Meta nittrasferixxu data personali lil parti terza li taġixxi bħala aġent jew proċessur, (i) nittrasferixxu din id-data biss għal skopijiet limitati u speċifikati; (ii) niżguraw li l-aġent jew proċessur huwa obbligat jipprovdi mill-inqas l-istess livell ta' protezzjoni tad-data kif rikjest mill-DPF-Principals; (iii) nieħdu miżuri xierqa u adegwati biex niżguraw li l-aġent jew proċessur verament jipproċessa d-data personali trasferita b'mod li jkun konformi mal-obbligi tagħna skont il-DPF-Principals; (iv) nesiġu mill-aġent jew proċessur li jinforma lill-organizzazzjoni tagħna jekk jiddetermina li ma jistax ikompli jipprovdi l-istess livell ta' protezzjoni kif stipulat mid-DPF-Principals; (v) wara tali notifika, inkluż taħt (iv), nieħdu miżuri xierqa u adegwati biex nieqfu l-ipproċessar mhux awtorizzat u nirrimedjaw is-sitwazzjoni; u (vi) nipprovdu lill-DPF Department, fuq talba, sommarju jew kampjun rappreżentattiv tad-dispożizzjonijiet rilevanti dwar il-protezzjoni tad-data tal-kuntratt tagħna ma' dan l-aġent.

F'konformità mal-EU-U.S. DPF u/jew l-UK Extension to the EU-U.S. DPF u/jew il-Swiss-U.S. DPF, l-organizzazzjoni tagħna timpenja ruħha li tikkopera mal-panel stabbilit mill-awtoritajiet tal-protezzjoni tad-data tal-UE u l-Information Commissioner's Office (ICO) tar-Renju Unit jew il-Kummissarju Federali għall-Protezzjoni tad-Data u l-Informazzjoni (EDÖB) tal-Iżvizzera, u li ssegwi l-pariri tagħhom dwar ilmenti mhux solvuti rigward it-trattament tagħna ta' data personali relatati mal-impjieg li nirċievu taħt l-EU-U.S. DPF u l-UK Extension to the EU-U.S. DPF u l-Swiss-U.S. DPF.

Is-suġġetti tad-dejta kollha li huma temporanjament fl-Unjoni Ewropea (UE), fiż-Żona Ekonomika Ewropea (ŻEE) jew fir-Renju Unit, jew li għandhom id-domiċilju jew ir-residenza abitwali tagħhom hemmhekk, huma intitolati għad-drittijiet u d-drittijiet tas-suġġett tad-dejta li huma ppubblikati f'tagħna. Dokument ta' Trasparenza, li joħorġu wkoll mill-Artikoli 15 sa 22 tal-GDPR, inkluż id-dritt ta' aċċess għal data personali. Għamilna din l-informazzjoni disponibbli fil-lingwi kollha tal-UE u taż-ŻEE. Il-verżjoni bil-lingwa Ingliża tapplika għar-Renju Unit.

Is-suġġetti tad-dejta kollha li huma residenti temporanjament fl-Isvizzera jew li għandhom id-domiċilju jew ir-residenza abitwali tagħhom hemmhekk huma intitolati għad-drittijiet u d-drittijiet tas-suġġett tad-dejta taħt l-Att Żvizzeru dwar il-Protezzjoni tad-Data (DPA) u r-Regolament Żvizzeru dwar il-Protezzjoni tad-Data (DPR) li huma ppubblikati fit-Trasparenza tagħna. Dokument, inkluż id-dritt ta' aċċess għal data personali. Aħna pprovdejna din l-informazzjoni fit-tliet lingwi uffiċjali tal-Isvizzera (Ġermaniż, Taljan u Franċiż).


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

# MALTESE: Informazzjoni dwar l-Ipproċessar tad-Data Personali għall-Impjegati u l-Applikanti (Artikolu 13, 14 GDPR)

Għażiż Sinjur jew Sinjura,

Id-dejta personali tal-impjegati u l-applikanti jistħoqqilha protezzjoni speċjali. L-għan tagħna huwa li nżommu l-livell ta' protezzjoni tad-dejta tagħna għal standard għoli. Għalhekk, qed niżviluppaw rutina il-kunċetti tagħna dwar il-protezzjoni tad-dejta u s-sigurtà tad-dejta.

Naturalment, aħna nikkonformaw mad-dispożizzjonijiet statutorji dwar il-protezzjoni tad-dejta. Skont Artikolu 13, 14 GDPR, il-kontrolluri jissodisfaw rekwiżiti speċifiċi ta' informazzjoni meta jipproċessaw id-dejta personali. Dan id-dokument iwettaq dawn l-obbligi.

It-terminoloġija tar-regolamentazzjoni legali hija kkumplikata. Sfortunatament, l-użu ta' termini legali ma setax jiġi eliminat fit-tħejjija ta' dan id-dokument. Għalhekk, nixtiequ nirrimarkaw li inti dejjem mistieden tikkuntattjana għall-mistoqsijiet kollha dwar dan id-dokument, it-termini użati jew il-formulazzjonijiet.

## I. Informazzjoni li għandha tiġi pprovduta fejn tinġabar data personali mis-suġġett tad-data (Artikolu 13 GDPR)

### A. l-identità u d-dettalji ta' kuntatt tal-kontrollur u, fejn applikabbli, tar-rappreżentant tal-kontrollur (Artikolu 13(1) lit. a GDPR)

Ara hawn fuq

### B. Id-dettalji ta' kuntatt tal-uffiċjal tal-protezzjoni tad-data, fejn applikabbli (Artikolu 13(1) lit. b GDPR)

Ara hawn fuq

### C. l-għanijiet tal-ipproċessar li għalihom hija maħsuba d-data personali kif ukoll il-bażi legali għall-ipproċessar (Artikolu 13(1) lit. c GDPR)

Għad-dejta tal-applikant, l-iskop tal-ipproċessar tad-dejta huwa li jsir eżami tal-applikazzjoni matul il-proċess ta' reklutaġġ. Għal dan il-għan, aħna nipproċessaw id-dejta kollha pprovduta minnek. Abbażi tad-dejta sottomessa waqt il-proċess ta' reklutaġġ, aħna niċċekkjaw jekk intix mistieden għal intervista tax-


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

xogħol (parti mill-proċess tal-għażla). Fil-każ ta' kandidati ġeneralment adattati, b'mod partikolari fil-kuntest tal-intervista tax-xogħol, aħna nipproċessaw ċerta data personali oħra pprovduta minnek, li hija essenzjali għad-deċiżjoni tal-għażla tagħna. Jekk inti mikrija minna, id-dejta tal-applikant tinbidel awtomatikament f'dejta tal-impjegati. Bħala parti mill -proċess ta' reklutaġġ, aħna nipproċessaw data personali oħra dwarek li nitolbu mingħandek u li hija meħtieġa biex nibdew jew inwettqu l-kuntratt tiegħek (bħal numri ta' identifikazzjoni personali jew numri tat-taxxa). Għad-dejta tal-impjegati, l-iskop tal-ipproċessar tad-dejta huwa t-twettiq tal-kuntratt tax-xogħol jew il-konformità ma' dispożizzjonijiet legali oħra applikabbli għar-relazzjoni tal-impjieg ( eż. il-liġi tat-taxxa) kif ukoll l-użu tad-dejta personali tiegħek biex twettaq il-kuntratt tax-xogħol konkluż miegħek. (eż. pubblikazzjoni ta' ismek u l-informazzjoni ta' kuntatt fi ħdan il-kumpanija jew lill-klijenti). Id-dejta tal-impjegat tinħażen wara t-terminazzjoni tar-relazzjoni tal-impjieg biex jiġu sodisfatti perjodi ta' żamma legali.

Il-bażi legali għall-ipproċessar tad-data hija Artikolu 6(1) lit. b GDPR, Artikolu 9(2) lit. b u h GDPR, Artikolu 88 (1) GDPR u l-leġiżlazzjoni nazzjonali, bħal għall-Ġermanja Taqsima 26 BDSG (Att Federali dwar il-Protezzjoni tad-Data).

## D. Ir-riċevituri jew il-kategoriji ta' riċevituri tad-data personali, jekk jeżistu (Artikolu 13(1) lit. e GDPR)

Awtoritajiet pubbliċi

Korpi esterni

Aktar korpi esterni

Ipproċessar intern

Ipproċessar intragrupp

Korpi oħra

Lista tal-proċessuri u r-riċevituri tad-dejta tagħna f'pajjiżi terzi u, jekk applikabbli, organizzazzjonijiet internazzjonali jew tiġi ppubblikata fuq il-websajt tagħna jew tista' tintalab mingħandna mingħajr ħlas. Jekk jogħġbok ikkuntattja lill-uffiċjal tal-protezzjoni tad-dejta tagħna biex titlob din il-lista.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## E. Fejn applikabbli, il-fatt li l-kontrollur għandu l-ħsieb li jittrasferixxi data personali lejn pajjiż terz jew organizzazzjoni internazzjonali u l-eżistenza jew l-assenza ta' deċiżjoni ta' adegwatezza mill-Kummissjoni, jew fil-każ ta' trasferimenti msemmija fl-Artikolu 46 jew 47, jew it-tieni subparagrafu tal-Artikolu 49(1), referenza għas-salvagwardji xierqa jew adatti u l-mezzi li bihom tinkiseb kopja tagħhom jew fejn dawn ikunu saru disponibbli (Artikolu 13(1) lit. f, 46(1), 46 (2) lit.c GDPR)

Il-kumpaniji u l-fergħat kollha li huma parti mill-grupp tagħna (minn hawn 'il quddiem imsejħa "kumpaniji tal-grupp") li għandhom il-post tan-negozju tagħhom jew uffiċċju f'pajjiż terz jistgħu jappartjenu għar-riċevituri tad-dejta personali. Lista tal-kumpaniji kollha tal-grupp jew riċevituri tista' tintalab mingħandna.

Skont Artikolu 46(1) GDPR kontrollur jew proċessur jista' jittrasferixxi data personali biss lil pajjiż terz jekk il-kontrollur jew proċessur ikun ipprovda salvagwardji xierqa, u bil-kundizzjoni li jkunu disponibbli drittijiet infurzabbli tas-suġġett tad-data u rimedji legali effettivi għas-suġġetti tad-data. Jistgħu jiġu pprovduti salvagwardji xierqa mingħajr ma tkun meħtieġa xi awtorizzazzjoni speċifika minn awtorità superviżorja permezz ta' klawsoli kuntrattwali standard, Artikolu 46(2) lit. c GDPR.

Il-klawsoli kuntrattwali standard tal-Unjoni Ewropea jew salvagwardji xierqa oħra huma miftiehma mar-riċevituri kollha minn pajjiżi terzi qabel l-ewwel trażmissjoni tad-dejta personali. Konsegwentement, huwa żgurat li jkunu garantiti salvagwardji xierqa, drittijiet infurzabbli tas-suġġett tad-data u rimedji legali effettivi għas-suġġetti tad-data. Kull suġġett tad-dejta jista' jikseb kopja tal-klawsoli kuntrattwali standard mingħandna. Il-klawsoli kuntrattwali standard huma wkoll disponibbli fil-Ġurnal Uffiċjali tal-Unjoni Ewropea.

L-Artikolu 45(3) tar-Regolament Ġenerali dwar il-Protezzjoni tad-Dejta (GDPR) jagħti lill-Kummissjoni Ewropea s-setgħa li tiddeċiedi, permezz ta' att ta' implimentazzjoni, li pajjiż mhux tal-UE jiżgura livell adegwat ta' protezzjoni. Dan ifisser livell ta' protezzjoni għad-dejta personali li huwa essenzjalment ekwivalenti għal-livell ta' protezzjoni fl-UE. L-effett tad-deċiżjonijiet dwar l-adegwatezza huwa li d-dejta personali tista' tiċċirkola liberament mill-UE (u n-Norveġja, il-Liechtenstein u l-Islanda) lejn pajjiż terz mingħajr aktar ostakli. Regoli simili jeżistu għar-Renju Unit, l-Isvizzera u xi Pajjiżi oħra.

Fejn il-Kummissjoni Ewropea jew il-gvern ta' pajjiż ieħor iddeċieda li pajjiż terz jiżgura livell adegwat ta' protezzjoni, u Qafas validu jkun fis-seħħ (eż. EU-U.S. Data Privacy Framework, Swiss-U.S. Data Privacy Framework, UK Extension to the EU-U.S. Data Privacy Framework), it-trasferimenti kollha minna lill-membri ta' tali oqfsa (eż. entitajiet awtoċertifikati) huma bbażati esklussivament fuq is-sħubija ta' dik l-entitajiet fil-qafas rispettiv. Fejn aħna jew waħda mill-entitajiet tal-grupp tagħna tkun membru ta' tali qafas, it-trasferimenti kollha lilna jew lill-entità tal-grupp tagħna huma bbażati esklussivament fuq is-sħubija tal-entitajiet f'tali qafas.

Kwalunkwe suġġett tad-dejta jista' jikseb kopja tal-oqfsa mingħandna. Barra minn hekk, l-oqfsa huma wkoll disponibbli fil-Ġurnal Uffiċjali tal-Unjoni Ewropea jew fil-materjali legali ppubblikati jew fuq il-websajts tal-awtoritajiet superviżorji jew awtoritajiet jew istituzzjonijiet kompetenti oħra.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## F. Il-perijodu li matulu d-data personali tkun ser tinħażen, jew jekk dak ma jkunx possibbli, il-kriterji użati biex jiġi ddeterminat dak il-perijodu (Artikolu 13(2) lit. a GDPR)

It-tul tal-ħażna tad-dejta personali tal-applikanti huwa ta' 6 xhur. Għad-dejta tal-impjegati japplika l-perjodu statutorju rispettiv taż-żamma. Wara li jiskadi dak il-perjodu, id-dejta korrispondenti titħassar b'mod regolari, sakemm ma tibqax meħtieġa għat-twettiq tal-kuntratt jew għall-bidu ta' kuntratt.

## G. L-eżistenza tad-dritt li jitlob mingħand il-kontrollur aċċess jew rettifika jew tħassir ta' data personali jew restrizzjoni tal-ipproċessar rigward is-suġġett tad-data jew li joġġezzjona għall-ipproċessar kif ukoll id-dritt għall-portabbiltà tad-data (Artikolu 13(2) lit. b GDPR)

Is-suġġetti tad-dejta kollha għandhom id-drittijiet li ġejjin:

***Dritt għall-aċċess***

Kull suġġett tad-dejta għandu dritt li jaċċessa d-dejta personali li tikkonċernah jew lilha. Id-dritt għall-aċċess jestendi għad-dejta kollha pproċessata minna. Id-dritt jista' jiġi eżerċitat faċilment u f'intervalli raġonevoli, sabiex tkun konxju ta', u tivverifika, il-legalità tal-ipproċessar (Premessa 63 GDPR). Dan id-dritt jirriżulta mill-Art. 15 GDPR. Is-suġġett tad-dejta jista' jikkuntattjana biex jeżerċita d-dritt ta' aċċess.

***Dritt għal rettifika***

Skont Artikolu 16 Sentenza 1 GDPR is-suġġett tad-dejta għandu d-dritt li jikseb mingħand il-kontrollur mingħajr dewmien żejjed ir-rettifika ta' data personali mhux eżatta li tikkonċernah. Barra minn hekk, Artikolu 16 Sentenza 2 tal-GDPR jipprovdi li s-suġġett tad-data huwa intitolat, b'kont meħud tal-għanijiet tal-ipproċessar, li jimtela data personali mhux kompluta, inkluż permezz tal-għoti ta' dikjarazzjoni supplimentari. Is-suġġett tad-dejta jista' jikkuntattjana biex jeżerċita d-dritt ta' rettifika.

***Dritt għat-tħassir (dritt li jintesa)***

Barra minn hekk, is-suġġetti tad-data huma intitolati għal dritt għat-tħassir u li jintesew taħt l-Art. 17 GDPR. Dan id-dritt jista' jiġi eżerċitat ukoll billi tikkuntattjana. F'dan il-punt, madankollu, nixtiequ nirrimarkaw li dan id-dritt ma japplikax safejn l-ipproċessar huwa meħtieġ biex tissodisfa obbligu legali li l-kumpanija tagħna hija soġġetta għalih, Artikolu 17(3) lit. b GDPR. Dan ifisser li nistgħu napprovaw applikazzjoni biex titħassar biss wara li jiskadi l-perjodu statutorju ta' żamma.

***Dritt g]al restrizzjoni ta' pro'essar***

Skont Artikolu 18 tal-GDPR kull suġġett tad-dejta huwa intitolat għal restrizzjoni tal-ipproċessar. Ir-restrizzjoni tal-ipproċessar tista' tintalab jekk waħda mill-kundizzjonijiet stipulati fArtikolu 18(1) lit. ad GDPR huwa sodisfatt. Is-suġġett tad-dejta jista' jikkuntattjana biex jeżerċita d-dritt għal restrizzjoni tal-ipproċessar.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

***Dritt ta' oġġezzjoni***

Barra minn hekk, l-Art. 21 GDPR jiggarantixxi d-dritt ta' oġġezzjoni. Is-suġġett tad-dejta jista' jikkuntattjana biex jeżerċita d-dritt li joġġezzjona.

***Dritt għall-portabbiltà tad-data***

Art. 20 GDPR jagħti lis-suġġett tad-dejta d-dritt għall-portabbiltà tad-dejta. Skont din id-dispożizzjoni, is-suġġett tad-data għandu taħt il-kundizzjonijiet stabbiliti fArtikolu 20(1) lit. a u b GDPR id-dritt li jirċievi d-dejta personali li tikkonċernah, li huwa jkun ipprovda lil kontrollur, f'format strutturat, użat komunement u li jinqara mill-magni u jkollu d-dritt li jittrasmetti dik id-dejta lil kontrollur ieħor mingħajr xkiel mill-kontrollur li lilu tkun ġiet ipprovduta d-dejta personali. Is-suġġett tad-dejta jista' jikkuntattjana biex jeżerċita d-dritt għall-portabbiltà tad-dejta.

## H. Fejn l-ipproċessar ikun ibbażat fuq il-punt (a) tal-Artikolu 6(1) jew il-punt (a) tal-Artikolu 9(2), l-eżistenza tad-dritt li jiġi irtirat il-kunsens fi kwalunkwe ħin, mingħajr ma tiġi affettwata l-legalità tal-ipproċessar abbażi ta' kunsens qabel l-irtirar tiegħu (Artikolu 13(2) lit. c GDPR)

Jekk l-ipproċessar tad-dejta personali huwa bbażat fuq l-Art. 6(1) lit. GDPR, li huwa l-każ, jekk is-suġġett tad-data jkun ta l-kunsens għall-ipproċessar ta' data personali għal skop speċifiku wieħed jew aktar jew ikun ibbażat fuq Artikolu 9(2) lit. a GDPR, li jirregola l-kunsens espliċitu għall-ipproċessar ta' kategoriji speċjali ta' data personali, is-suġġett tad-data għandu skont Artikolu 7(3) Sentenza 1 GDPR id-dritt li jirtira l-kunsens tiegħu jew tagħha fi kwalunkwe ħin.

L-irtirar tal-kunsens m'għandux jaffettwa l-legalità tal-ipproċessar ibbażat fuq il-kunsens qabel l-irtirar tiegħu, Artikolu 7(3) Sentenza 2 GDPR. Għandu jkun faċli li tirtira daqskemm jingħata l-kunsens, Art. 7(3) Sentenza 4 GDPR. Għalhekk, l-irtirar tal-kunsens jista' dejjem iseħħ bl-istess mod kif ikun ingħata l-kunsens jew b'xi mod ieħor, li jitqies mis-suġġett tad-data bħala aktar sempliċi. Fis-soċjetà tal-informazzjoni tal-lum, probabbilment l-aktar mod sempliċi biex tirtira l-kunsens huwa email sempliċi. Jekk is-suġġett tad-dejta jixtieq jirtira l-kunsens tiegħu jew tagħha mogħti lilna, email sempliċi lilna hija biżżejjed. Inkella, is-suġġett tad-dejta jista' jagħżel kwalunkwe mod ieħor biex jikkomunika lilna l-irtirar tal-kunsens tiegħu jew tagħha.

## I. Id-dritt li jitressaq ilment quddiem awtorità superviżorja (Artikolu 13(2) lit. d, 77(1) GDPR)

Bħala l-kontrollur, aħna obbligati ninnotifikaw lis-suġġett tad-dejta bid-dritt li jitressaq ilment ma' awtorità ta' superviżjoni, Artikolu 13(2) lit. d GDPR. Id-dritt li jitressaq ilment ma' awtorità superviżorja huwa rregolat milArtikolu 77(1) GDPR. Skont din id-dispożizzjoni, mingħajr preġudizzju għal kwalunkwe rimedju amministrattiv jew ġudizzjarju ieħor, kull suġġett tad-data għandu jkollu d-dritt li jressaq ilment ma' awtorità ta' superviżjoni, b'mod partikolari fl-Istat Membru tar-residenza abitwali tiegħu jew tagħha, il-post


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

tax-xogħol jew il-post ta' l-allegat ksur jekk is-suġġett tad-dejta jikkunsidra li l-ipproċessar tad-dejta personali relatata miegħu jew tagħha jikser ir-Regolament Ġenerali dwar il-Protezzjoni tad-Data. Id-dritt li jitressaq ilment ma' awtorità superviżorja kien limitat biss mil-liġi tal-Unjoni b'tali mod, li jista' jiġi eżerċitat biss quddiem awtorità superviżorja waħda (Premessa 141 Sentenza 1 GDPR). Din ir-regola hija maħsuba biex tevita lmenti doppji tal-istess suġġett tad-dejta fl-istess kwistjoni. Jekk suġġett tad-dejta jrid iressaq ilment dwarna, għalhekk tlabna nikkuntattjaw awtorità superviżorja waħda biss.

## J. Jekk il-forniment ta' data personali huwiex rekwiżit statutorju jew kuntrattwali, jew rekwiżit meħtieġ biex wieħed jidħol f'kuntratt, kif ukoll jekk is-suġġett tad-data huwiex obbligat jipprovdi d-data personali u l-konsegwenzi possibbli meta wieħed jonqos milli jipprovdi tali data (Art. 13(2) lit. e GDPR)

Aħna niċċaraw li l-provvista ta' data personali hija parzjalment meħtieġa mil-liġi ( eż. regolamenti tat-taxxa) jew tista' tirriżulta wkoll minn dispożizzjonijiet kuntrattwali (eż. informazzjoni dwar is-sieħeb kuntrattwali).

Xi drabi jista' jkun meħtieġ li jiġi konklużż kuntratt li s-suġġett tad-dejta jipprovdilna data personali, li sussegwentement trid tiġi pproċessata minna. Is-suġġett tad-data huwa, pereżempju, obbligat li jipprovdilna data personali meta l-kumpanija tagħna tiffirma kuntratt miegħu jew magħha. In-nuqqas ta' forniment tad-dejta personali jkollu l-konsegwenza li l-kuntratt mas-suġġett tad-dejta ma jistax jiġi konklużż.

Qabel ma tiġi pprovduta d-dejta personali mis-suġġett tad-dejta, is-suġġett tad-dejta għandu jikkuntattjana. Aħna niċċaraw lis-suġġett tad-dejta jekk il-provvista tad-dejta personali hijiex meħtieġa bil-liġi jew bil-kuntratt jew jekk huwiex meħtieġ għall-konklużjoni tal-kuntratt, jekk hemmx obbligu li tiġi pprovduta d-dejta personali u l-konsegwenzi tan-nuqqas ta' forniment tad-dejta personali.

## K. L-eżistenza ta' teħid awtomatizzat ta' deċiżjonijiet inkluż it-tfassil ta' profili msemmi fl-Artikolu 22(1) u (4) u għall-inqas f'dawk il-każijiet, l-informazzjoni importanti dwar il-loġika involuta, kif ukoll is-sinifikat u l-konsegwenzi previsti ta' tali pproċessar għas-suġġett tad-data (Artikolu 13 (2) lit. f GDPR)

Bħala kumpanija responsabbli, ġeneralment ma nużawx teħid ta' deċiżjonijiet jew profili awtomatizzati. Jekk, f'każijiet eċċezzjonali, inwettqu teħid ta' deċiżjonijiet jew tfassil ta' profili awtomatizzati, aħna se ninfurmaw lis-suġġett tad-dejta jew separatament jew permezz ta' sottosezzjoni fil-politika ta' privatezza tagħna (fuq il-websajt tagħna). F'dan il-każ, japplika dan li ġej:

Teħid ta' deċiżjonijiet awtomatizzat - inkluż it-tfassil ta' profili - jista' jseħħ jekk (1) dan ikun meħtieġ għad-dħul fi, jew it-twettiq ta', kuntratt bejn is-suġġett tad-data u magħna, jew (2) dan huwa awtorizzat mil-liġi tal-Unjoni jew tal-Istat Membru li għaliha aħna huma suġġetti u li jistabbilixxi wkoll miżuri xierqa biex


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

jissalvagwardjaw id-drittijiet u l-libertajiet u l-interessi leġittimi tas-suġġett tad-dejta; jew (3) dan huwa bbażat fuq il-kunsens espliċitu tas-suġġett tad-dejta.

Fil-każijiet imsemmija fl-Artikolu 22(2) (a) u (c) GDPR, aħna nimplimentaw miżuri xierqa biex nissalvagwardjaw id-drittijiet u l-libertajiet u l-interessi leġittimi tas-suġġett tad-data. F'dawn il-każijiet, għandek id-dritt li tikseb intervent uman min-naħa tal-kontrollur, li tesprimi l-opinjoni tiegħek u li tikkontesta d-deċiżjoni.

Informazzjoni sinifikanti dwar il-loġika involuta, kif ukoll is-sinifikat u l-konsegwenzi previsti ta 'tali ipproċessar għas-suġġett tad-data hija stabbilita fil-politika ta' privatezza tagħna.

## II. Informazzjoni li għandha tiġi pprovduta fejn id-data personali ma tkunx inkisbet mis-suġġett tad-data (Artikolu 14 tal-GDPR)

### A. L-identità u d-dettalji ta' kuntatt tal-kontrollur u, fejn applikabbli, tar-rappreżentant tal-kontrollur (Artikolu 14(1) lit. a GDPR)

Ara hawn fuq

### B. Id-dettalji ta' kuntatt tal-uffiċjal tal-protezzjoni tad-data, fejn applikabbli (Artikolu 14(1) lit. b GDPR)

Ara hawn fuq

### C. L-għanijiet tal-ipproċessar li għalihom hija maħsuba d-data personali kif ukoll il-bażi legali għall-ipproċessar (Artikolu 14(1) lit. c GDPR)

Għad-dejta tal-applikant mhux miġbura mis-suġġett tad-dejta, l-iskop tal-ipproċessar tad-dejta huwa li jsir eżami tal-applikazzjoni matul il-proċess ta' reklutaġġ. Għal dan il-għan, nistgħu nipproċessaw data mhux miġbura mingħandek. Fuq il-bażi tad-dejta pproċessata matul il-proċess ta' reklutaġġ, aħna niċċekkjaw jekk intix mistieden għal intervista tax-xogħol (parti mill-proċess tal-għażla). Jekk inti mikrija minna, id-dejta tal-applikant awtomatikament tinbidel f'dejta tal-impjegati. Għad-dejta tal-impjegati, l-iskop tal-ipproċessar tad-dejta huwa t-twettiq tal-kuntratt tax-xogħol jew il-konformità ma' dispożizzjonijiet legali oħra applikabbli għar-relazzjoni tal-impjieg. Id-dejta tal-impjegat tinħażen wara t-terminazzjoni tar-relazzjoni tal-impjieg biex jiġu sodisfatti perjodi ta' żamma legali.

Il-bażi legali għall-ipproċessar tad-data hija Artikolu 6(1) lit. b uf GDPR, Artikolu 9(2) lit. b u h GDPR, Artikolu 88 (1) GDPR u l-leġiżlazzjoni nazzjonali, bħal għall-Ġermanja Taqsima 26 BDSG (Att Federali dwar il-Protezzjoni tad-Data).


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## D. Il-kategoriji ta' data personali inkwistjoni (Artikolu 14(1) lit. d GDPR)

Data tal-applikant

Dejta dwar l-impjegati

## E. Ir-riċevituri jew il-kategoriji ta' riċevituri tad-data personali, jekk jeżistu (Artikolu 14(1) lit. e GDPR)

Awtoritajiet pubbliċi

Korpi esterni

Aktar korpi esterni

Ipproċessar intern

Ipproċessar intragrupp

Korpi oħra

Lista tal-proċessuri u r-riċevituri tad-dejta tagħna f'pajjiżi terzi u, jekk applikabbli, organizzazzjonijiet internazzjonali jew tiġi ppubblikata fuq il-websajt tagħna jew tista' tintalab mingħandna mingħajr ħlas. Jekk jogħġbok ikkuntattja lill-uffiċjal tal-protezzjoni tad-dejta tagħna biex titlob din il-lista.

## F. Fejn applikabbli, il-fatt li l-kontrollur għandu l-ħsieb li jittrasferixxi data personali lil riċevitur f'pajjiż terz jew organizzazzjoni internazzjonali u l-eżistenza jew l-assenza ta' deċiżjoni ta' adegwatezza mill-Kummissjoni, jew fil-każ ta' trasferimenti msemmija fl-Artikolu 46 jew 47, jew it-tieni subparagrafu tal-Artikolu 49(1), referenza għas-salvagwardji xierqa jew adatti u l-mezzi biex tinkiseb kopja tagħhom jew fejn dawn ikunu saru disponibbli (Artikolu 14(1) lit. f, 46(1), 46(2) lit.c GDPR)

Il-kumpaniji u l-fergħat kollha li huma parti mill-grupp tagħna (minn hawn 'il quddiem imsejħa "kumpaniji tal-grupp") li għandhom il-post tan-negozju tagħhom jew uffiċċju f'pajjiż terz jistgħu jappartjenu għar-riċevituri tad-dejta personali. Lista tal-kumpaniji kollha tal-grupp jew riċevituri tista' tintalab mingħandna.

Skont Artikolu 46(1) GDPR kontrollur jew proċessur jista' jittrasferixxi data personali biss lil pajjiż terz jekk il-kontrollur jew proċessur ikun ipprovda salvagwardji xierqa, u bil-kundizzjoni li jkunu disponibbli drittijiet


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

infurzabbli tas-suġġett tad-data u rimedji legali effettivi għas-suġġetti tad-data. Jistgħu jiġu pprovduti salvagwardji xierqa mingħajr ma tkun meħtieġa xi awtorizzazzjoni speċifika minn awtorità superviżorja permezz ta' klawsoli standard ta' protezzjoni tad-dejta, Artikolu 46(2) lit. c GDPR.

Il-klawsoli kuntrattwali standard tal-Unjoni Ewropea jew salvagwardji xierqa oħra huma miftiehma marċevituri kollha minn pajjiżi terzi qabel l-ewwel trażmissjoni tad-dejta personali. Konsegwentement, huwa żgurat li jkunu garantiti salvagwardji xierqa, drittijiet infurzabbli tas-suġġett tad-data u rimedji legali effettivi għas-suġġetti tad-data. Kull suġġett tad-dejta jista' jikseb kopja tal-klawsoli kuntrattwali standard mingħandna. Il-klawsoli kuntrattwali standard huma wkoll disponibbli fil-Ġurnal Uffiċjali tal-Unjoni Ewropea.

L-Artikolu 45(3) tar-Regolament Ġenerali dwar il-Protezzjoni tad-Dejta (GDPR) jagħti lill-Kummissjoni Ewropea s-setgħa li tiddeċiedi, permezz ta' att ta' implimentazzjoni, li pajjiż mhux tal-UE jiżgura livell adegwat ta' protezzjoni. Dan ifisser livell ta' protezzjoni għad-dejta personali li huwa essenzjalment ekwivalenti għal-livell ta' protezzjoni fl-UE. L-effett tad-deċiżjonijiet dwar l-adegwatezza huwa li d-dejta personali tista' tiċċirkola liberament mill-UE (u n-Norveġja, il-Liechtenstein u l-Islanda) lejn pajjiż terz mingħajr aktar ostakli. Regoli simili jeżistu għar-Renju Unit, l-Isvizzera u xi Pajjiżi oħra.

Fejn il-Kummissjoni Ewropea jew il-gvern ta' pajjiż ieħor iddeċieda li pajjiż terz jiżgura livell adegwat ta' protezzjoni, u Qafas validu jkun fis-seħħ (eż. EU-U.S. Data Privacy Framework, Swiss-U.S. Data Privacy Framework, UK Extension to the EU-U.S. Data Privacy Framework), it-trasferimenti kollha minna lill-membri ta' tali oqfsa (eż. entitajiet awtoċertifikati) huma bbażati esklussivament fuq is-sħubija ta' dik l-entitajiet fil-qafas rispettiv. Fejn aħna jew waħda mill-entitajiet tal-grupp tagħna tkun membru ta' tali qafas, it-trasferimenti kollha lilna jew lill-entità tal-grupp tagħna huma bbażati esklussivament fuq is-sħubija tal-entitajiet f'tali qafas.

Kwalunkwe suġġett tad-dejta jista' jikseb kopja tal-oqfsa mingħandna. Barra minn hekk, l-oqfsa huma wkoll disponibbli fil-Ġurnal Uffiċjali tal-Unjoni Ewropea jew fil-materjali legali ppubblikati jew fuq il-websajts tal-awtoritajiet superviżorji jew awtoritajiet jew istituzzjonijiet kompetenti oħra.

## G. Il-perijodu li matulu d-data personali tkun ser tinħażen, jew jekk dak ma jkunx possibbli, il-kriterji użati biex jiġi ddeterminat dak il-perijodu (Artikolu 14(2) lit. a GDPR)

It-tul tal-ħażna tad-dejta personali tal-applikanti huwa ta' 6 xhur. Għad-dejta tal-impjegati japplika l-perjodu statutorju rispettiv taż-żamma. Wara li jiskadi dak il-perjodu, id-dejta korrispondenti titħassar b'mod regolari, sakemm ma tibqax meħtieġa għat-twettiq tal-kuntratt jew għall-bidu ta' kuntratt.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## H. Fejn l-ipproċessar ikun ibbażat fuq il-punt (f) tal-Artikolu 6(1), l-interessi leġittimi segwiti mill-kontrollur jew minn parti terza (Art. 14(2) lit. b GDPR)

Skont Artikolu 6(1) lit. f GDPR, l-ipproċessar għandu jkun legali biss jekk l-ipproċessar ikun meħtieġ għall-iskopijiet ta' interessi leġittimi segwiti mill-kontrollur jew minn parti terza, ħlief fejn dawn l-interessi huma megħluba mill-interessi jew id-drittijiet u l-libertajiet fundamentali tas-suġġett tad-data li jeħtieġu protezzjoni tad-data personali. Skont il-Premessa 47 Sentenza 2 GDPR jista' jeżisti interess leġittimu fejn ikun hemm relazzjoni rilevanti u xierqa bejn is-suġġett tad-dejta u l-kontrollur, eż. f'sitwazzjonijiet fejn is-suġġett tad-dejta huwa klijent tal-kontrollur. Fil-każijiet kollha li fihom il-kumpanija tagħna tipproċessa d-dejta tal-applikant ibbażata fuq Artikolu 6(1) lit. f GDPR, l-interess leġittimu tagħna huwa l-impjieg ta' persunal u professjonisti addattati.

## I. L-eżistenza tad-dritt li jitlob mingħand il-kontrollur aċċess jew rettifika jew tħassir ta' data personali jew restrizzjoni tal-ipproċessar rigward is-suġġett tad-data u li joġġezzjona għall-ipproċessar kif ukoll id-dritt għall-portabbiltà tad-data (Artikolu 14(2) lit. c GDPR)

Is-suġġetti tad-dejta kollha għandhom id-drittijiet li ġejjin:

***Dritt għall-aċċess***

Kull suġġett tad-dejta għandu dritt li jaċċessa d-dejta personali li tikkonċernah jew lilha. Id-dritt għall-aċċess jestendi għad-dejta kollha pproċessata minna. Id-dritt jista' jiġi eżerċitat faċilment u f'intervalli raġonevoli, sabiex tkun konxju ta', u tivverifika, il-legalità tal-ipproċessar (Premessa 63 GDPR). Dan id-dritt jirriżulta mill-Art. 15 GDPR. Is-suġġett tad-dejta jista' jikkuntattjana biex jeżerċita d-dritt ta' aċċess.

***Dritt għal rettifika***

Skont Artikolu 16 Sentenza 1 GDPR is-suġġett tad-dejta għandu d-dritt li jikseb mingħand il-kontrollur mingħajr dewmien żejjed ir-rettifika ta' data personali mhux eżatta li tikkonċernah. Barra minn hekk, Artikolu 16 Sentenza 2 tal-GDPR jipprovdi li s-suġġett tad-data huwa intitolat, b'kont meħud tal-għanijiet tal-ipproċessar, li jimtela data personali mhux kompluta, inkluż permezz tal-għoti ta' dikjarazzjoni supplimentari. Is-suġġett tad-dejta jista' jikkuntattjana biex jeżerċita d-dritt ta' rettifika.

***Dritt għat-tħassir (dritt li jintesa)***

Barra minn hekk, is-suġġetti tad-data huma intitolati għal dritt għat-tħassir u li jintesew taħt l-Art. 17 GDPR. Dan id-dritt jista' jiġi eżerċitat ukoll billi tikkuntattjana. F'dan il-punt, madankollu, nixtiequ nirrimarkaw li dan id-dritt ma japplikax safejn l-ipproċessar huwa meħtieġ biex tissodisfa obbligu legali li l-kumpanija tagħna hija soġġetta għalih, Artikolu 17(3) lit. b GDPR. Dan ifisser li nistgħu napprovaw applikazzjoni biex titħassar biss wara li jiskadi l-perjodu statutorju ta' żamma.

***Dritt g]al restrizzjoni ta' pro'essar***

Skont Artikolu 18 tal-GDPR kull suġġett tad-dejta huwa intitolat għal restrizzjoni tal-ipproċessar. Ir-restrizzjoni tal-ipproċessar tista' tintalab jekk waħda mill-kundizzjonijiet stipulati fArtikolu 18(1) lit. ad


© All rights reserved by Heiko Maniero.

GDPR huwa sodisfatt. Is-suġġett tad-dejta jista' jikkuntattjana biex jeżerċita d-dritt għal restrizzjoni tal-ipproċessar.

***Dritt ta' oġġezzjoni***

Barra minn hekk, l-Art. 21 GDPR jiggarantixxi d-dritt ta' oġġezzjoni. Is-suġġett tad-dejta jista' jikkuntattjana biex jeżerċita d-dritt li joġġezzjona.

***Dritt għall-portabbiltà tad-data***

Art. 20 GDPR jagħti lis-suġġett tad-dejta d-dritt għall-portabbiltà tad-dejta. Skont din id-dispożizzjoni s-suġġett tad-dejta għandu taħt il-kundizzjonijiet stabbiliti fArtikolu 20(1) lit. a u b GDPR id-dritt li jirċievi d-dejta personali li tikkonċernah, li huwa jkun ipprovda lil kontrollur, f'format strutturat, użat komunement u li jinqara mill-magni u jkollu d-dritt li jittrasmetti dik id-dejta lil kontrollur ieħor mingħajr xkiel mill-kontrollur li lilu tkun ġiet ipprovduta d-dejta personali. Is-suġġett tad-dejta jista' jikkuntattjana biex jeżerċita d-dritt għall-portabbiltà tad-dejta.

## J. Fejn l-ipproċessar ikun ibbażat fuq il-punt (a) tal-Artikolu 6(1) jew il-punt (a) tal-Artikolu 9(2), l-eżistenza tad-dritt li jiġi irtirat il-kunsens fi kwalunkwe ħin, mingħajr ma tiġi affettwata l-legalità tal-ipproċessar abbażi ta' kunsens qabel l-irtirar tiegħu (Art. 14(2) lit. d GDPR)

Jekk l-ipproċessar tad-dejta personali huwa bbażat fuq l-Art. 6(1) lit. GDPR, li huwa l-każ, jekk is-suġġett tad-data jkun ta l-kunsens għall-ipproċessar ta' data personali għal skop speċifiku wieħed jew aktar jew ikun ibbażat fuq Artikolu 9(2) lit. a GDPR, li jirregola l-kunsens espliċitu għall-ipproċessar ta' kategoriji speċjali ta' data personali, is-suġġett tad-data għandu skont Artikolu 7(3) Sentenza 1 GDPR id-dritt li jirtira l-kunsens tiegħu jew tagħha fi kwalunkwe ħin.

L-irtirar tal-kunsens m'għandux jaffettwa l-legalità tal-ipproċessar ibbażat fuq il-kunsens qabel l-irtirar tiegħu, Artikolu 7(3) Sentenza 2 GDPR. Għandu jkun faċli li tirtira daqskemm jingħata l-kunsens, Art. 7(3) Sentenza 4 GDPR. Għalhekk, l-irtirar tal-kunsens jista' dejjem iseħħ bl-istess mod kif ikun ingħata l-kunsens jew b'xi mod ieħor, li jitqies mis-suġġett tad-data bħala aktar sempliċi. Fis-soċjetà tal-informazzjoni tal-lum, probabbilment l-aktar mod sempliċi biex tirtira l-kunsens huwa email sempliċi. Jekk is-suġġett tad-dejta jixtieq jirtira l-kunsens tiegħu jew tagħha mogħti lilna, email sempliċi lilna hija biżżejjed. Inkella, is-suġġett tad-dejta jista' jagħżel kwalunkwe mod ieħor biex jikkomunika lilna l-irtirar tal-kunsens tiegħu jew tagħha.

## K. Id-dritt li jitressaq ilment quddiem awtorità superviżorja (Artikolu 14(2) lit. e, 77(1) GDPR)

Bħala l-kontrollur, aħna obbligati li ninnotifikaw lis-suġġett tad-dejta bid-dritt li jressaq ilment ma' awtorità superviżorja, Artikolu 14(2) lit. e GDPR. Id-dritt li jitressaq ilment ma' awtorità superviżorja huwa rregolat


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

milArtikolu 77(1) GDPR. Skont din id-dispożizzjoni, mingħajr preġudizzju għal kwalunkwe rimedju amministrattiv jew ġudizzjarju ieħor, kull suġġett tad-data għandu jkollu d-dritt li jressaq ilment ma' awtorità ta' superviżjoni, b'mod partikolari fl-Istat Membru tar-residenza abitwali tiegħu jew tagħha, il-post tax-xogħol jew il-post ta' l-allegat ksur jekk is-suġġett tad-dejta jikkunsidra li l-ipproċessar tad-dejta personali relatata miegħu jew tagħha jikser ir-Regolament Ġenerali dwar il-Protezzjoni tad-Data. Id-dritt li jitressaq ilment ma' awtorità superviżorja kien limitat biss mil-liġi tal-Unjoni b'tali mod, li jista' jiġi eżerċitat biss quddiem awtorità superviżorja waħda (Premessa 141 Sentenza 1 GDPR). Din ir-regola hija maħsuba biex tevita lmenti doppji tal-istess suġġett tad-dejta fl-istess kwistjoni. Jekk suġġett tad-dejta jrid iressaq ilment dwarna, għalhekk tlabna nikkuntattjaw awtorità superviżorja waħda biss.

## L. Minn liema sors toriġina d-data personali, u fejn applikabbli jekk oriġinatx minn sorsi aċċessibbli għall-pubbliku (Artikolu 14(2) lit. f GDPR)

Fil-prinċipju, id-dejta personali tinġabar direttament mis-suġġett tad-dejta jew f'kooperazzjoni ma' awtorità ( eż. irkupru ta' dejta minn reġistru uffiċjali). Data oħra dwar suġġetti tad-data huma derivati minn trasferimenti ta' kumpaniji tal-grupp. Fil-kuntest ta' din l-informazzjoni ġenerali, l-isem tas-sorsi eżatti li minnhom tkun oriġinat id-dejta personali huwa jew impossibbli jew ikun jinvolvi sforz sproporzjonat fis-sens tal-Art. 14(5) lit. b GDPR. Fil-prinċipju, aħna ma niġbrux data personali minn sorsi aċċessibbli għall-pubbliku.

Kwalunkwe suġġett tad-dejta jista' jikkuntattjana fi kwalunkwe ħin biex jikseb informazzjoni aktar dettaljata dwar is-sorsi eżatti tad-dejta personali li tikkonċernah jew lilha. Fejn l-oriġini tad-dejta personali ma tistax tiġi pprovduta lis-suġġett tad-dejta minħabba li jkunu ntużaw diversi sorsi, għandha tingħata informazzjoni ġenerali (Premessa 61 Sentenza 4 GDPR).

## M. L-eżistenza ta' teħid awtomatizzat ta' deċiżjonijiet inkluż it-tfassil ta' profili msemmi fl-Artikolu 22(1) u (4) u għall-inqas f'dawk il-każijiet, l-informazzjoni importanti dwar il-loġika involuta, kif ukoll is-sinifikat u l-konsegwenzi previsti ta' tali pproċessar għas-suġġett tad-dat (Artikolu 14(2) lit. g GDPR)

Bħala kumpanija responsabbli, ġeneralment ma nużawx teħid ta' deċiżjonijiet jew profili awtomatizzati. Jekk, f'każijiet eċċezzjonali, inwettqu teħid ta' deċiżjonijiet jew tfassil ta' profili awtomatizzati, aħna se ninfurmaw lis-suġġett tad-dejta jew separatament jew permezz ta' sottosezzjoni fil-politika ta' privatezza tagħna (fuq il-websajt tagħna). F'dan il-każ, japplika dan li ġej:

Teħid ta' deċiżjonijiet awtomatizzat - inkluż it-tfassil ta' profili - jista' jseħħ jekk (1) dan ikun meħtieġ għad-dħul fi, jew it-twettiq ta', kuntratt bejn is-suġġett tad-data u magħna, jew (2) dan huwa awtorizzat mil-liġi tal-Unjoni jew tal-Istat Membru li għaliha aħna huma suġġetti u li jistabbilixxi wkoll miżuri xierqa biex jissalvagwardjaw id-drittijiet u l-libertajiet u l-interessi leġittimi tas-suġġett tad-dejta; jew (3) dan huwa bbażat fuq il-kunsens espliċitu tas-suġġett tad-dejta.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

Fil-każijiet imsemmija fl-Artikolu 22(2) (a) u (c) GDPR, aħna nimplimentaw miżuri xierqa biex nissalvagwardjaw id-drittijiet u l-libertajiet u l-interessi leġittimi tas-suġġett tad-data. F'dawn il-każijiet, għandek id-dritt li tikseb intervent uman min-naħa tal-kontrollur, li tesprimi l-opinjoni tiegħek u li tikkontesta d-deċiżjoni.

Informazzjoni sinifikanti dwar il-loġika involuta, kif ukoll is-sinifikat u l-konsegwenzi previsti ta 'tali ipproċessar għas-suġġett tad-data hija stabbilita fil-politika ta' privatezza tagħna.

## III. EU-U.S. Data Privacy Framework (EU-U.S. DPF), UK Extension to the EU-U.S. DPF, Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF)

Jekk l-organizzazzjoni tagħna hija membru ċċertifikat tal-EU-U.S. Data Privacy Framework (EU-U.S. DPF) u/jew l-UK Extension to the EU-U.S. DPF u/jew il-Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF), japplika dan li ġej:

Aħna nżommu mal-EU-U.S. Data Privacy Framework (EU-U.S. DPF) u l-UK Extension to the EU-U.S. DPF kif ukoll il-Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF), kif stabbilit mill-U.S. Department of Commerce. Il-kumpanija tagħna kkonfermat mad-Dipartiment tal-Kummerċ tal-Istati Uniti li tikkonforma mal-EU-U.S. Data Privacy Framework Principles (EU-U.S. DPF Principles) fir-rigward tal-ipproċessar ta' data personali li tirċievi mill-Unjoni Ewropea u mir-Renju Unit taħt il-EU-U.S. DPF u l-UK Extension to the EU-U.S. DPF. Il-kumpanija tagħna kkonfermat mad-Dipartiment tal-Kummerċ tal-Istati Uniti li tikkonforma mal-Swiss-U.S. Data Privacy Framework Principles (Swiss-U.S. DPF Principles) fir-rigward tal-ipproċessar ta' data personali li tirċievi mill-Iżvizzera taħt il-Swiss-U.S. DPF. Fil-każ ta' kunflitt bejn id-dispożizzjonijiet tal-politika tal-privatezza tagħna u l-EU-U.S. DPF Principles u/jew il-Swiss-U.S. DPF Principles, il-Principles għandhom jipprevalu.

Biex titgħallem aktar dwar il-programm Data Privacy Framework (DPF) u biex tara ċ-ċertifikazzjoni tagħna, jekk jogħġbok żur https://www.dataprivacyframework.gov/.

L-unitajiet oħra tal-Istati Uniti jew is-sussidjarji tal-kumpanija tagħna li wkoll jikkonformaw mal-EU-U.S. DPF Principals, inklużi l-UK Extension to the EU-U.S. DPF u l-Swiss-U.S. DPF Principals, jekk applikabbli, huma mniżżla fil-politika tal-privatezza tagħna.

F'konformità mal-EU-U.S. DPF u l-UK Extension to the EU-U.S. DPF kif ukoll il-Swiss-U.S. DPF, il-kumpanija tagħna timpenja ruħha li tikkopera mal-panel stabbilit mill-awtoritajiet tal-protezzjoni tad-data tal-UE u l-Information Commissioner's Office (ICO) tar-Renju Unit, kif ukoll il-Kummissarju Federali għall-Protezzjoni tad-Data u l-Informazzjoni (EDÖB) tal-Iżvizzera, u li ssegwi l-pariri tagħhom dwar ilmenti mhux solvuti dwar it-trattament tagħna ta' data personali li nirċievu taħt il-EU-U.S. DPF u l-UK Extension to the EU-U.S. DPF u l-Swiss-U.S. DPF.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

Aħna ninformaw lill-persuni affettwati dwar l-awtoritajiet Ewropej kompetenti għall-protezzjoni tad-data li huma responsabbli għall-immaniġġjar ta' ilmenti dwar it-trattament tad-data personali mill-organizzazzjoni tagħna, fil-parti ta' fuq ta' dan id-dokument ta' trasparenza u li noffru lil persuni affettwati rimedju legali xieraq u bla ħlas.

Aħna ninformaw lill-persuni affettwati kollha li l-kumpanija tagħna hija suġġetta għall-poteri ta' investigazzjoni u infurzar tal-Federal Trade Commission (FTC).

Il-persuni affettwati għandhom, taħt ċerti kundizzjonijiet, il-possibbiltà li jagħmlu użu minn arbitraġġ vinkolanti. L-organizzazzjoni tagħna hija obbligata li tirrisolvi talbiet u tikkonforma mal-kundizzjonijiet stipulati fl-Anness I tal-DPF-Principals, jekk il-persuna affettwata titlob arbitraġġ vinkolanti billi tinforma lill-organizzazzjoni tagħna u l-proċeduri u l-kundizzjonijiet stipulati fl-Anness I tal-Principals ikunu ġew segwiti.

Aħna ninformaw b'dan lill-persuni affettwati kollha dwar ir-responsabbiltà tal-organizzazzjoni tagħna fil-każ ta' trasferiment ta' data personali lil partijiet terzi.

Għal mistoqsijiet tal-persuni affettwati jew tal-awtoritajiet superviżorji tad-data, aħna nnominaw lir-rappreżentanti lokali msemmija aktar 'il fuq f'dan id-dokument ta' trasparenza.

Noffrulek il-possibbiltà li tagħżel (Opt-out) jekk id-data personali tiegħek (i) għandhiex tiġi trasferita lil partijiet terzi jew (ii) għandhiex tiġi użata għal skop li jkun sostanzjalment differenti mill-iskop(i) għall-kwal/i tkun inġabret oriġinarjament jew aktar tard awtorizzajt int. Il-mekkaniżmu ċar, viżibbli u faċilment aċċessibbli biex teżerċita l-għażla tiegħek huwa li tikkuntattja lill-uffiċjal tal-protezzjoni tad-data tagħna (DSB) permezz ta' email. M'għandekx għażla u m'aħniex obbligati li nagħmlu dan jekk id-data tiġi trasferita lil parti terza li taġixxi bħala aġent jew proċessur f'isem tagħna u skont l-istruzzjonijiet tagħna. Madankollu, dejjem nagħmlu kuntratt ma' tali aġent jew proċessur.

Għal data sensittiva (jiġifieri data personali li fiha informazzjoni dwar l-istat tas-saħħa, l-oriġini razzjali jew etnika, opinjonijiet politiċi, twemmin reliġjuż jew filosofiku, sħubija fi trade union jew informazzjoni dwar il-ħajja sesswali tal-persuna kkonċernata) niksbu l-kunsens espliċitu tiegħek (Opt-in) meta din id-data (i) tiġi trasferita lil partijiet terzi jew (ii) tiġi użata għal skop differenti minn dak li għalih tkun inġabret oriġinarjament jew għal liema int aktar tard tajt il-kunsens tiegħek billi għażilt l-għażla Opt-in. Barra minn hekk, nittrattaw id-data personali kollha li nirċievu mingħand partijiet terzi bħala sensittiva jekk it-terza parti tidentifikaha u tittrattaha bħala sensittiva.

Aħna ninformawk b'dan dwar ir-rekwiżit li jiġu żvelati data personali bħala rispons għal talbiet legali mill-awtoritajiet, inklużi l-konformità mar-rekwiżiti ta' sigurtà nazzjonali jew infurzar tal-liġi.

Meta nittrasferixxu data personali lil parti terza li taġixxi bħala kontrollur, nikkonformaw mal-Principals ta' notifika u għażla. Barra minn hekk, nagħmlu kuntratt mal-parti terza li hija responsabbli għat-trattament li jipprovdi li din id-data tista' tiġi pproċessata biss għal skopijiet limitati u speċifikati skont il-kunsens mogħti minnek u li r-riċevitur irid jipprovdi l-istess livell ta' protezzjoni bħal Principals tad-DPF u jinfurmana jekk jiddetermina li ma jistax ikompli jikkonforma ma' din l-obbligazzjoni. Il-kuntratt jipprovdi li l-parti terza, li


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

hija responsabbli, tieqaf ipproċessar jew tieħu miżuri oħra xierqa u adegwati biex tirrimedja s-sitwazzjoni jekk ssir din id-determinazzjoni.

Meta nittrasferixxu data personali lil parti terza li taġixxi bħala aġent jew proċessur, (i) nittrasferixxu din id-data biss għal skopijiet limitati u speċifikati; (ii) niżguraw li l-aġent jew proċessur huwa obbligat jipprovdi mill-inqas l-istess livell ta' protezzjoni tad-data kif rikjest mill-DPF-Principals; (iii) nieħdu miżuri xierqa u adegwati biex niżguraw li l-aġent jew proċessur verament jipproċessa d-data personali trasferita b'mod li jkun konformi mal-obbligi tagħna skont il-DPF-Principals; (iv) nesiġu mill-aġent jew proċessur li jinforma lill-organizzazzjoni tagħna jekk jiddetermina li ma jistax ikompli jipprovdi l-istess livell ta' protezzjoni kif stipulat mid-DPF-Principals; (v) wara tali notifika, inkluż taħt (iv), nieħdu miżuri xierqa u adegwati biex nieqfu l-ipproċessar mhux awtorizzat u nirrimedjaw is-sitwazzjoni; u (vi) nipprovdu lill-DPF Department, fuq talba, sommarju jew kampjun rappreżentattiv tad-dispożizzjonijiet rilevanti dwar il-protezzjoni tad-data tal-kuntratt tagħna ma' dan l-aġent.

F'konformità mal-EU-U.S. DPF u/jew l-UK Extension to the EU-U.S. DPF u/jew il-Swiss-U.S. DPF, l-organizzazzjoni tagħna timpenja ruħha li tikkopera mal-panel stabbilit mill-awtoritajiet tal-protezzjoni tad-data tal-UE u l-Information Commissioner's Office (ICO) tar-Renju Unit jew il-Kummissarju Federali għall-Protezzjoni tad-Data u l-Informazzjoni (EDÖB) tal-Iżvizzera, u li ssegwi l-pariri tagħhom dwar ilmenti mhux solvuti rigward it-trattament tagħna ta' data personali relatati mal-impjieg li nirċievu taħt l-EU-U.S. DPF u l-UK Extension to the EU-U.S. DPF u l-Swiss-U.S. DPF.

Is-suġġetti tad-dejta kollha li huma temporanjament fl-Unjoni Ewropea (UE), fiż-Żona Ekonomika Ewropea (ŻEE) jew fir-Renju Unit, jew li għandhom id-domiċilju jew ir-residenza abitwali tagħhom hemmhekk, huma intitolati għad-drittijiet u d-drittijiet tas-suġġett tad-dejta li huma ppubblikati f'tagħna. Dokument ta' Trasparenza, li joħorġu wkoll mill-Artikoli 15 sa 22 tal-GDPR, inkluż id-dritt ta' aċċess għal data personali. Għamilna din l-informazzjoni disponibbli fil-lingwi kollha tal-UE u taż-ŻEE. Il-verżjoni bil-lingwa Ingliża tapplika għar-Renju Unit.

Is-suġġetti tad-dejta kollha li huma residenti temporanjament fl-Isvizzera jew li għandhom id-domiċilju jew ir-residenza abitwali tagħhom hemmhekk huma intitolati għad-drittijiet u d-drittijiet tas-suġġett tad-dejta taħt l-Att Żvizzeru dwar il-Protezzjoni tad-Data (DPA) u r-Regolament Żvizzeru dwar il-Protezzjoni tad-Data (DPR) li huma ppubblikati fit-Trasparenza tagħna. Dokument, inkluż id-dritt ta' aċċess għal data personali. Aħna pprovdejna din l-informazzjoni fit-tliet lingwi uffiċjali tal-Isvizzera (Ġermaniż, Taljan u Franċiż).


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

# LATVIAN: Informācija par personas datu apstrādi (VDAR 13., 14. pants)

Cienījamais kungs vai kundze,

Īpaši aizsargājami ir ikvienas personas dati, kas ir līgumiskās, pirmslīgumiskās vai citās attiecībās ar mūsu uzņēmumu. Mūsu mērķis ir nodrošināt augstu datu aizsardzības līmeni. Tāpēc mēs regulāri pilnveidojam savas datu aizsardzības un datu drošības koncepcijas.

Protams, mēs ievērojam likumā noteiktos datu aizsardzības noteikumus. Saskaņā ar VDAR 13., 14. pantu personas datu apstrādātāji, vācot personas datus, ievēro īpašas informācijas prasības. Ar šo dokumentu šie pienākumi ir izpildīti.

Tiesisko noteikumu terminoloģija ir sarežģīta. Diemžēl, sagatavojot šo dokumentu, nebija iespējams izvairīties no juridisko terminu lietošanas. Tāpēc vēlamies norādīt, ka vienmēr esat laipni aicināti sazināties ar mums par visiem jautājumiem saistībā ar šo dokumentu, izmantotajiem terminiem vai formulējumiem.

## I. Informācija, kas jāsniedz, ja personas dati ir iegūti no datu subjekta (VDAR 13. pants)

### A. Pārziņa un attiecīgā gadījumā pārziņa pārstāvja identitāte un kontaktinformācija (VDAR 13. panta 1. punkta a) VDAR)

Skatīt iepriekš

### B. Attiecīgā gadījumā – datu aizsardzības speciālista kontaktinformācija (VDAR 13. panta 1. punkta b) VDAR)

Skatīt iepriekš

### C. Apstrādes nolūki, kam paredzēti personas dati, kā arī apstrādes juridiskais pamats (VDAR 13. panta 1. punkta c) VDAR)

Personas datu apstrādes mērķis ir visu darbību veikšana, kas attiecas uz pārzini, klientiem, potenciālajiem klientiem, darījumu partneriem vai citām līgumiskām vai pirmslīgumiskām attiecībām starp minētajām grupām (visplašākajā nozīmē) vai pārziņa juridiskajām saistībām.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

Art. VDAR 6. panta 1. punkta a) VDAR kalpo kā juridiskais pamats apstrādes darbībām, kurām mēs saņemam piekrišanu konkrētam apstrādes nolūkam. Ja personas datu apstrāde ir nepieciešama, lai izpildītu līgumu, kurā datu subjekts ir līgumslēdzēja puse, kā tas ir, piemēram, ja apstrādes darbības ir nepieciešamas preču piegādei vai kāda cita pakalpojuma sniegšanai, apstrādes pamatā ir VDAR 6. panta 1. punkta b) VDAR. Tas pats attiecas uz tādām apstrādes darbībām, kas ir nepieciešamas, lai veiktu pasākumus pirms līguma noslēgšanas, piemēram, ja tiek veikti pieprasījumi par mūsu produktiem vai pakalpojumiem. Vai uz mūsu uzņēmumu attiecas juridisks pienākums, kura dēļ ir nepieciešama personas datu apstrāde, piemēram, nodokļu saistību izpildei, apstrāde pamatojas uz 6. panta 1. punktu. VDAR 6. panta 1. punkta c) apakšpunktu.

Retos gadījumos personas datu apstrāde var būt nepieciešama, lai aizsargātu datu subjekta vai citas fiziskas personas vitālas intereses. Tā tas būtu, piemēram, ja apmeklētājs mūsu uzņēmumā gūtu traumu un viņa vārds, vecums, veselības apdrošināšanas dati vai cita būtiska informācija būtu jānodod ārstam, slimnīcai vai citai trešai personai. Šādā gadījumā apstrāde būtu pamatota ar Regulas (EK) Nr. VDAR 6. panta 1. punkta d) apakšpunktu.

Ja apstrāde ir nepieciešama, lai izpildītu uzdevumu, ko veic sabiedrības interesēs vai īstenojot pārzinim piešķirtās oficiālās pilnvaras, juridiskais pamats ir Regulas (EK) Nr. VDAR 6. panta 1. punkta e) apakšpunkts.

Visbeidzot, apstrādes darbības varētu pamatoties uz VDAR 6. panta 1. punkta f) apakšpunktu. Šo juridisko pamatu izmanto apstrādes darbībām, uz kurām neattiecas neviens no iepriekš minētajiem juridiskajiem pamatiem, ja apstrāde ir nepieciešama mūsu uzņēmuma vai trešās personas likumīgo interešu nodrošināšanai, izņemot gadījumus, kad pār šādām interesēm prevalē datu subjekta intereses vai pamattiesības un pamatbrīvības, kas prasa personas datu aizsardzību. Šādas apstrādes darbības ir īpaši pieļaujamas, jo tās ir īpaši minētas Eiropas likumdevējā. Viņš uzskatīja, ka leģitīmas intereses var pieņemt, ja datu subjekts ir pārziņa klients (VDAR 47. apsvēruma 2. teikums).

## D. Pārziņa vai trešās personas leģitīmās intereses, ja apstrāde pamatojas uz 6. panta 1. punkta f) apakšpunktu (VDAR 13. panta 1. punkta d) VDAR).

Ja personas datu apstrādes pamatā ir VDAR 6. panta 1. punkta f) VDAR, mūsu leģitīmās intereses ir veikt uzņēmējdarbību, lai nodrošinātu visu mūsu darbinieku un akcionāru labklājību.

## E. Personas datu saņēmēji vai saņēmēju kategorijas, ja tādi ir (VDAR 13. panta 1. punkta e) VDAR)

Valsts iestādes


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

Ārējās struktūras

Citas ārējās struktūras

Iekšējā apstrāde

Apstrāde grupas iekšienē

Citas struktūras

Mūsu apstrādātāju un datu saņēmēju trešās valstīs un, attiecīgā gadījumā, starptautisko organizāciju saraksts ir publicēts mūsu tīmekļa vietnē vai arī to var pieprasīt no mums bez maksas. Lūdzu, sazinieties ar mūsu datu aizsardzības speciālistu, lai pieprasītu šo sarakstu.

## F. Attiecīgā gadījumā – informācija, ka pārzinis paredz nosūtīt personas datus uz trešo valsti vai starptautisku organizāciju, un informācija par to, ka eksistē vai neeksistē Komisijas lēmums par aizsardzības līmeņa pietiekamību, vai – 46. vai 47. pantā, vai 49. panta 1. punkta otrajā daļā minētās nosūtīšanas gadījumā – atsauce uz atbilstošām vai piemērotām garantijām un informācija par to, kā saņemt datu kopiju, vai to, kur tie ir darīti pieejami (VDAR 13. panta 1. punkta f) VDAR, 46. panta 1. punkts, 46. panta 2. punkta c) VDAR).

Visi mūsu grupas uzņēmumi un filiāles (turpmāk tekstā - "grupas uzņēmumi"), kuru uzņēmējdarbības vieta vai birojs atrodas trešā valstī, var būt personas datu saņēmēji. Visu grupas uzņēmumu vai saņēmēju sarakstu var pieprasīt no mums.

Saskaņā ar VDAR 46. panta 1. punktu pārzinis vai apstrādātājs var nosūtīt personas datus uz trešo valsti tikai tad, ja pārzinis vai apstrādātājs ir nodrošinājis atbilstošas garantijas un ar nosacījumu, ka datu subjektiem ir pieejamas īstenojamas datu subjekta tiesības un efektīvi tiesiskās aizsardzības līdzekļi. Piemērotus aizsardzības pasākumus var nodrošināt, neprasot īpašu uzraudzības iestādes atļauju, izmantojot standarta līguma klauzulas, VDAR 46. panta 2. punkta c) VDAR.

Ar visiem saņēmējiem no trešām valstīm pirms pirmās personas datu pārsūtīšanas tiek saskaņotas Eiropas Savienības standarta līguma klauzulas vai citi piemēroti drošības pasākumi. Tādējādi tiek nodrošināts, ka datu subjektiem tiek garantētas atbilstošas garantijas, īstenojamas datu subjektu tiesības un efektīvi tiesiskās aizsardzības līdzekļi. Katrs datu subjekts var saņemt no mums standarta līguma noteikumu kopiju. Standarta līguma klauzulas ir pieejamas arī Eiropas Savienības Oficiālajā Vēstnesī.

Vispārīgās datu aizsardzības regulas (VDAR) 45. panta 3. punktā Eiropas Komisijai ir piešķirtas pilnvaras ar īstenošanas aktu pieņemt lēmumu, ka valsts, kas nav ES dalībvalsts, nodrošina pietiekamu aizsardzības līmeni. Tas nozīmē tādu personas datu aizsardzības līmeni, kas būtībā ir līdzvērtīgs aizsardzības līmenim ES. Lēmumu par aizsardzības līmeņa pietiekamību rezultātā personas dati var brīvi


© All rights reserved by Heiko Maniero.

un bez papildu šķēršļiem pārvietoties no ES (un Norvēģijas, Lihtenšteinas un Islandes) uz trešo valsti. Līdzīgi noteikumi ir spēkā Apvienotajā Karalistē, Šveicē un dažās citās valstīs.

Ja Eiropas Komisija vai citas valsts valdība ir nolēmusi, ka trešā valsts nodrošina pietiekamu aizsardzības līmeni, un ir spēkā spēkā esoša sistēma (piemēram, EU-U.S. Data Privacy Framework, Swiss-U.S. Data Privacy Framework, UK Extension to the EU-U.S. Data Privacy Framework), visi mūsu veiktie datu pārsūtīšanas gadījumi šādu sistēmu dalībniekiem (piemēram, pašsertificētām struktūrām) ir balstīti tikai uz šo struktūru dalību attiecīgajā sistēmā. Ja mēs vai kāda no mūsu grupas struktūrām ir šādas sistēmas dalībniece, visi datu nodošanas gadījumi mums vai mūsu grupas struktūrai ir balstīti tikai uz šo struktūru dalību šādā sistēmā.

Jebkurš datu subjekts var saņemt no mums šo ietvaru kopiju. Turklāt pamatprincipu kopijas ir pieejamas arī Eiropas Savienības Oficiālajā Vēstnesī vai publicētajos juridiskajos materiālos, vai uzraudzības iestāžu vai citu kompetento iestāžu vai institūciju tīmekļa vietnēs.

## G. Laikposms, cik ilgi personas dati tiks glabāti, vai, ja tas nav iespējams, kritēriji, ko izmanto minētā laikposma noteikšanai (VDAR 13. panta 2. punkta a) VDAR)

Kritērijs, ko izmanto, lai noteiktu personas datu glabāšanas periodu, ir attiecīgais likumā noteiktais glabāšanas periods. Pēc šā perioda beigām attiecīgie dati tiek regulāri dzēsti, ja vien tie vairs nav nepieciešami līguma izpildei vai līguma uzsākšanai.

Ja nav ar likumu noteikta glabāšanas perioda, kritērijs ir līgumā noteiktais vai iekšējais glabāšanas periods.

## H. Tas, ka pastāv tiesības pieprasīt pārzinim piekļuvi datu subjekta personas datiem un to labošanu vai dzēšanu, vai apstrādes ierobežošanu attiecībā uz datu subjektu, vai tiesības iebilst pret apstrādi, kā arī tiesības uz datu pārnesamību (VDAR 13. panta 2. punkta b) VDAR).

Visiem datu subjektiem ir šādas tiesības:

***Piekļuves tiesības***

Katram datu subjektam ir tiesības piekļūt personas datiem, kas uz viņu attiecas. Piekļuves tiesības attiecas uz visiem mūsu apstrādātajiem datiem. Šīs tiesības var izmantot viegli un ar saprātīgiem intervāliem, lai uzzinātu un pārbaudītu apstrādes likumību (VDAR 63. apsvērums). Šīs tiesības izriet no Regulas (EK) Nr. VDAR 15. Datu subjekts var sazināties ar mums, lai izmantotu piekļuves tiesības.

***Tiesības uz labošanu***

Saskaņā ar VDAR 16. panta 1. teikumu datu subjektam ir tiesības no pārziņa bez nepamatotas kavēšanās saņemt neprecīzu personas datu labošanu, kas uz viņu attiecas. Turklāt VDAR 16. panta 2.


© All rights reserved by Heiko Maniero.

teikumā noteikts, ka datu subjektam, ņemot vērā apstrādes nolūkus, ir tiesības uz nepilnīgu personas datu papildināšanu, tostarp sniedzot papildu paziņojumu. Datu subjekts var sazināties ar mums, lai izmantotu tiesības uz labošanu.

***Tiesības uz dzēšanu (tiesības tikt aizmirstam)***

Turklāt datu subjektiem ir tiesības uz dzēšanu un aizmiršanu saskaņā ar Regulas (EK) Nr. 17 VDAR. Šīs tiesības var izmantot, sazinoties ar mums. Tomēr šajā brīdī vēlamies norādīt, ka šīs tiesības nav piemērojamas, ja apstrāde ir nepieciešama, lai izpildītu juridisku pienākumu, kas attiecas uz mūsu uzņēmumu, kā noteikts VDAR 17. panta 3. punkta b) apakšpunktā. Tas nozīmē, ka mēs varam apstiprināt pieteikumu par dzēšanu tikai pēc likumā noteiktā glabāšanas termiņa beigām.

***Tiesības uz apstrādes ierobežošanu***

Saskaņā ar VDAR 18. pantu jebkuram datu subjektam ir tiesības uz apstrādes ierobežošanu. Apstrādes ierobežošanu var pieprasīt, ja ir izpildīts viens no VDAR 18. panta 1. punkta a-d apakšpunktā minētajiem nosacījumiem. Datu subjekts var sazināties ar mums, lai izmantotu tiesības uz apstrādes ierobežošanu.

***Tiesības iebilst***

Turklāt saskaņā ar Regulas (EK) Nr. VDAR 21. pants garantē tiesības iebilst. Datu subjekts var sazināties ar mums, lai izmantotu tiesības iebilst.

***Tiesības uz datu pārnesamību***

Art. 20 VDAR datu subjektam piešķir tiesības uz datu pārnesamību. Saskaņā ar šo noteikumu datu subjektam saskaņā ar VDAR 20. panta 1. punkta a) un b) apakšpunktā paredzētajiem nosacījumiem ir tiesības saņemt personas datus, kas attiecas uz viņu un ko viņš ir sniedzis pārzinim, strukturētā, plaši izmantotā un mašīnlasāmā formātā, un tiesības nosūtīt šos datus citam pārzinim, netraucējot pārzinim, kuram personas dati ir sniegti. Datu subjekts var sazināties ar mums, lai izmantotu tiesības uz datu pārnesamību.

## I. Ja apstrāde pamatojas uz 6. panta 1. punkta a) apakšpunktu vai 9. panta 2. punkta a) apakšpunktu – tiesības jebkurā brīdī atsaukt piekrišanu, neietekmējot tādas apstrādes likumīgumu, kuras pamatā ir pirms atsaukuma sniegta piekrišana (VDAR 13. panta 2. punkta c) VDAR).

Ja personas datu apstrādes pamatā ir Regulas (EK) Nr. a panta 1. punkta a) apakšpunktu, kas ir gadījums, kad datu subjekts ir devis piekrišanu personas datu apstrādei vienam vai vairākiem konkrētiem nolūkiem, vai tā ir pamatota ar VDAR 9. panta 2. punkta a) apakšpunktu, kas reglamentē nepārprotamu piekrišanu īpašu kategoriju personas datu apstrādei, datu subjektam saskaņā ar VDAR 7. panta 3. punkta 1. teikuma 1. teikumu ir tiesības jebkurā laikā atsaukt savu piekrišanu.

Piekrišanas atsaukšana neietekmē tās apstrādes likumību, kuras pamatā ir piekrišana pirms tās atsaukšanas, VDAR 7. panta 3. punkta 2. teikums. Piekrišanu atsaukt ir tikpat viegli kā dot piekrišanu, 1.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

pants. VDAR 7. panta 3. punkta 4. teikums. Tāpēc piekrišanas atsaukšana vienmēr var notikt tādā pašā veidā, kādā piekrišana ir dota, vai jebkurā citā veidā, ko datu subjekts uzskata par vienkāršāku. Mūsdienu informācijas sabiedrībā, iespējams, vienkāršākais veids, kā atsaukt piekrišanu, ir vienkāršs e-pasts. Ja datu subjekts vēlas atsaukt mums doto piekrišanu, pietiek ar vienkāršu e-pasta vēstuli. Datu subjekts var arī izvēlēties jebkuru citu veidu, kā paziņot mums par piekrišanas atsaukšanu.

## J. Tiesības iesniegt sūdzību uzraudzības iestādei (VDAR 13. panta 2. punkta d) VDAR, 77. panta 1. punkts).

Mums kā pārzinim ir pienākums informēt datu subjektu par tiesībām iesniegt sūdzību uzraudzības iestādei, VDAR 13. panta 2. punkta d) VDAR. Tiesības iesniegt sūdzību uzraudzības iestādei reglamentē VDAR 77. panta 1. punkts. Saskaņā ar šo noteikumu, neskarot nekādus citus administratīvos vai tiesiskās aizsardzības līdzekļus, katram datu subjektam ir tiesības iesniegt sūdzību uzraudzības iestādei, jo īpaši dalībvalstī, kurā ir viņa pastāvīgā dzīvesvieta, darbavieta vai iespējamā pārkāpuma vieta, ja datu subjekts uzskata, ka ar viņu saistīto personas datu apstrāde pārkāpj Vispārīgo datu aizsardzības regulu. Tiesības iesniegt sūdzību uzraudzības iestādei Savienības tiesību aktos tika ierobežotas tikai tādā veidā, ka tās var izmantot tikai vienā uzraudzības iestādē (Vispārīgās datu aizsardzības regulas 141. apsvēruma 1. teikums). Šis noteikums ir paredzēts, lai izvairītos no viena un tā paša datu subjekta dubultām sūdzībām vienā un tajā pašā lietā. Tāpēc, ja datu subjekts vēlas iesniegt sūdzību par mums, mēs lūdzam vērsties tikai vienā uzraudzības iestādē.

## K. Informācija, vai personas datu sniegšana ir noteikta saskaņā ar likumu vai līgumu, vai tā ir priekšnosacījums, lai līgumu noslēgtu, kā arī informācija par to, vai datu subjektam ir pienākums personas datus sniegt un kādas sekas var būt gadījumos, kad šādi dati netiek sniegti (VDAR 13. panta 2. punkta e) VDAR)

Mēs paskaidrojam, ka personas datu sniegšana ir daļēji prasīta ar likumu (piemēram, nodokļu noteikumi) vai var izrietēt arī no līguma noteikumiem (piemēram, informācija par līguma partneri).

Dažkārt, lai noslēgtu līgumu, var būt nepieciešams, lai datu subjekts mums sniegtu personas datus, kas mums pēc tam jāapstrādā. Piemēram, datu subjektam ir pienākums sniegt mums personas datus, kad mūsu uzņēmums ar viņu slēdz līgumu. Personas datu nesniegšanas sekas būtu tādas, ka līgumu ar datu subjektu nevarētu noslēgt.

Pirms datu subjekts sniedz personas datus, datu subjektam ir jāsazinās ar mums. Mēs izskaidrojam datu subjektam, vai personas datu sniegšana ir prasīta ar likumu vai līgumu vai ir nepieciešama līguma noslēgšanai, vai ir pienākums sniegt personas datus un kādas ir personas datu nesniegšanas sekas.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

### L. Tas, ka pastāv automatizēta lēmumu pieņemšana, tostarp profilēšana, kas minēta 22. panta 1. un 4. punktā, un – vismaz minētajos gadījumos – jēgpilna informācija par tajā ietverto loģiku, kā arī šādas apstrādes nozīmīgumu un paredzamajām sekām attiecībā uz datu subjektu (VDAR 13. panta 2. punkta f) VDAR).

Kā atbildīgs uzņēmums mēs parasti neizmantojam automatizētu lēmumu pieņemšanu vai profilēšanu. Ja izņēmuma gadījumos mēs veicam automatizētu lēmumu pieņemšanu vai profilēšanu, mēs par to informēsim datu subjektu atsevišķi vai ar apakšsadaļas palīdzību mūsu privātuma politikā (mūsu tīmekļa vietnē). Šādā gadījumā piemēro šādus noteikumus:

Automatizēta lēmumu pieņemšana, tostarp profilēšana, var notikt, ja (1) tas ir nepieciešams, lai noslēgtu vai izpildītu līgumu starp datu subjektu un mums, vai (2) to atļauj Savienības vai dalībvalsts tiesību akti, kas uz mums attiecas un kas nosaka arī piemērotus pasākumus datu subjekta tiesību un brīvību un likumīgo interešu aizsardzībai, vai (3) tas ir pamatots ar datu subjekta skaidru piekrišanu.

Gadījumos, kas minēti VDAR 22. panta 2. punkta a) un c) apakšpunktā, mēs īstenojam piemērotus pasākumus, lai aizsargātu datu subjekta tiesības un brīvības un likumīgās intereses. Šādos gadījumos jums ir tiesības panākt pārziņa iejaukšanos, paust savu viedokli un apstrīdēt lēmumu.

Nozīmīga informācija par iesaistīto loģiku, kā arī par šādas apstrādes nozīmi un paredzamajām sekām datu subjektam ir izklāstīta mūsu privātuma politikā.

## II. Informācija, kas jāsniedz, ja personas dati nav iegūti no datu subjekta (VDAR 14. pants)

### A. Pārziņa un attiecīgā gadījumā pārziņa pārstāvja identitāte un kontaktinformācija (VDAR 14. panta 1. punkta a) VDAR)

Skatīt iepriekš

### B. Attiecīgā gadījumā – datu aizsardzības speciālista kontaktinformācija (VDAR 14. panta 1. punkta b) VDAR)

Skatīt iepriekš


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## C. Apstrādes nolūki, kam paredzēti personas dati, kā arī apstrādes juridiskais pamats (VDAR 14. panta 1. punkta c) VDAR)

Personas datu apstrādes mērķis ir visu darbību veikšana, kas attiecas uz pārzini, klientiem, potenciālajiem klientiem, darījumu partneriem vai citām līgumiskām vai pirmslīgumiskām attiecībām starp minētajām grupām (visplašākajā nozīmē) vai pārziņa juridiskajām saistībām.

Ja personas datu apstrāde ir nepieciešama, lai izpildītu līgumu, kurā datu subjekts ir līgumslēdzēja puse, kā tas ir, piemēram, ja apstrādes darbības ir nepieciešamas, lai piegādātu preces vai sniegtu kādu citu pakalpojumu, apstrāde pamatojas uz VDAR 6. panta 1. punkta b) apakšpunktu. Tas pats attiecas uz tādām apstrādes darbībām, kas ir nepieciešamas, lai veiktu pasākumus pirms līguma noslēgšanas, piemēram, ja tiek veikti pieprasījumi par mūsu produktiem vai pakalpojumiem. Vai uz mūsu uzņēmumu attiecas juridisks pienākums, kura dēļ ir nepieciešama personas datu apstrāde, piemēram, nodokļu saistību izpildei, apstrāde pamatojas uz 6. panta 1. punktu. VDAR 6. panta 1. punkta c) apakšpunktu.

Retos gadījumos personas datu apstrāde var būt nepieciešama, lai aizsargātu datu subjekta vai citas fiziskas personas vitālas intereses. Tā tas būtu, piemēram, ja apmeklētājs mūsu uzņēmumā gūtu traumu un viņa vārds, vecums, veselības apdrošināšanas dati vai cita būtiska informācija būtu jānodod ārstam, slimnīcai vai citai trešai personai. Šādā gadījumā apstrāde notiktu, pamatojoties uz Regulas (EK) Nr. VDAR 6. panta 1. punkta d) apakšpunktu.

Ja apstrāde ir nepieciešama, lai izpildītu uzdevumu, ko veic sabiedrības interesēs vai īstenojot pārzinim piešķirtās oficiālās pilnvaras, juridiskais pamats ir Regulas (EK) Nr. VDAR 6. panta 1. punkta e) apakšpunkts.

Visbeidzot, apstrādes darbības varētu pamatoties uz VDAR 6. panta 1. punkta f) apakšpunktu. Šo juridisko pamatu izmanto apstrādes darbībām, uz kurām neattiecas neviens no iepriekš minētajiem juridiskajiem pamatiem, ja apstrāde ir nepieciešama mūsu uzņēmuma vai trešās personas likumīgo interešu nodrošināšanai, izņemot gadījumus, kad pār šādām interesēm prevalē datu subjekta intereses vai pamattiesības un pamatbrīvības, kas prasa personas datu aizsardzību. Šādas apstrādes darbības ir īpaši pieļaujamas, jo tās ir īpaši minētas Eiropas likumdevējā. Viņš uzskatīja, ka leģitīmas intereses var pieņemt, ja datu subjekts ir pārziņa klients (VDAR 47. apsvēruma 2. teikums).

## D. Attiecīgo personas datu kategorijas (VDAR 14. panta 1. punkta d) VDAR)

Klientu dati

Potenciālo klientu dati

Darbinieku dati

Piegādātāju dati


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## E. Personas datu saņēmēji vai saņēmēju kategorijas, ja tādas ir (VDAR 14. panta 1. punkta e) VDAR)

Valsts iestādes

Ārējās struktūras

Citas ārējās struktūras

Iekšējā apstrāde

Apstrāde grupas iekšienē

Citas struktūras

Mūsu apstrādātāju un datu saņēmēju trešās valstīs un, attiecīgā gadījumā, starptautisko organizāciju saraksts ir publicēts mūsu tīmekļa vietnē vai arī to var pieprasīt no mums bez maksas. Lūdzu, sazinieties ar mūsu datu aizsardzības speciālistu, lai pieprasītu šo sarakstu.

## F. Attiecīgā gadījumā – informācija, ka pārzinis paredz nosūtīt personas datus saņēmējam trešā valstī vai starptautiskai organizācijai, un informācija par to, ka eksistē vai neeksistē Komisijas lēmums par aizsardzības līmeņa pietiekamību, vai – 46. vai 47. pantā, vai 49. panta 1. punkta otrajā daļā minētās nosūtīšanas gadījumā – atsauce uz atbilstošām vai piemērotām garantijām un informācija par to, kā saņemt datu kopiju, vai to, kur tie ir darīti pieejami (VDAR 14. panta 1. punkta f) VDAR, 46. panta 1. punkts, 46. panta 2. punkta c) VDAR).

Visi mūsu grupas uzņēmumi un filiāles (turpmāk tekstā - "grupas uzņēmumi"), kuru uzņēmējdarbības vieta vai birojs atrodas trešā valstī, var būt personas datu saņēmēji. Visu grupas uzņēmumu sarakstu var pieprasīt no mums.

Saskaņā ar VDAR 46. panta 1. punktu pārzinis vai apstrādātājs var nosūtīt personas datus uz trešo valsti tikai tad, ja pārzinis vai apstrādātājs ir nodrošinājis atbilstošas garantijas un ar nosacījumu, ka datu subjektiem ir pieejamas īstenojamas datu subjekta tiesības un efektīvi tiesiskās aizsardzības līdzekļi. Piemērotus aizsardzības pasākumus var nodrošināt, neprasot īpašu uzraudzības iestādes atļauju, izmantojot standarta datu aizsardzības klauzulas, VDAR 46. panta 2. punkta c) VDAR.

Ar visiem saņēmējiem no trešām valstīm pirms pirmās personas datu nosūtīšanas tiek saskaņotas Eiropas Savienības standarta līguma klauzulas vai citi atbilstoši aizsardzības pasākumi. Tādējādi tiek nodrošināts, ka datu subjektiem tiek garantētas atbilstošas garantijas, īstenojamas datu subjektu tiesības


© All rights reserved by Heiko Maniero.

un efektīvi tiesiskās aizsardzības līdzekļi. Katrs datu subjekts var saņemt no mums standarta līguma noteikumu kopiju. Standarta līguma klauzulas ir pieejamas arī Eiropas Savienības Oficiālajā Vēstnesī.

Vispārīgās datu aizsardzības regulas (VDAR) 45. panta 3. punktā Eiropas Komisijai ir piešķirtas pilnvaras ar īstenošanas aktu pieņemt lēmumu, ka valsts, kas nav ES dalībvalsts, nodrošina pietiekamu aizsardzības līmeni. Tas nozīmē tādu personas datu aizsardzības līmeni, kas būtībā ir līdzvērtīgs aizsardzības līmenim ES. Lēmumu par aizsardzības līmeņa pietiekamību rezultātā personas dati var brīvi un bez papildu šķēršļiem pārvietoties no ES (un Norvēģijas, Lihtenšteinas un Islandes) uz trešo valsti. Līdzīgi noteikumi ir spēkā Apvienotajā Karalistē, Šveicē un dažās citās valstīs.

Ja Eiropas Komisija vai citas valsts valdība ir nolēmusi, ka trešā valsts nodrošina pietiekamu aizsardzības līmeni, un ir spēkā spēkā esoša sistēma (piemēram, EU-U.S. Data Privacy Framework, Swiss-U.S. Data Privacy Framework, UK Extension to the EU-U.S. Data Privacy Framework), visi mūsu veiktie datu pārsūtīšanas gadījumi šādu sistēmu dalībniekiem (piemēram, pašsertificētām struktūrām) ir balstīti tikai uz šo struktūru dalību attiecīgajā sistēmā. Ja mēs vai kāda no mūsu grupas struktūrām ir šādas sistēmas dalībniece, visi datu nodošanas gadījumi mums vai mūsu grupas struktūrai ir balstīti tikai uz šo struktūru dalību šādā sistēmā.

Jebkurš datu subjekts var saņemt no mums šo ietvaru kopiju. Turklāt pamatprincipu kopijas ir pieejamas arī Eiropas Savienības Oficiālajā Vēstnesī vai publicētajos juridiskajos materiālos, vai uzraudzības iestāžu vai citu kompetento iestāžu vai institūciju tīmekļa vietnēs.

## G. Laikposms, cik ilgi personas dati tiks glabāti, vai, ja tas nav iespējams, kritēriji, ko izmanto minētā laikposma noteikšanai (VDAR 14. panta 2. punkta a) VDAR)

Kritērijs, ko izmanto, lai noteiktu personas datu glabāšanas periodu, ir attiecīgais likumā noteiktais glabāšanas periods. Pēc šā perioda beigām attiecīgie dati tiek regulāri dzēsti, ja vien tie vairs nav nepieciešami līguma izpildei vai līguma uzsākšanai.

Ja nav ar likumu noteikta glabāšanas perioda, kritērijs ir līgumā noteiktais vai iekšējais glabāšanas periods.

## H. Pārziņa vai trešās personas leģitīmās intereses, ja apstrāde pamatojas uz 6. panta 1. punkta f) apakšpunktu (VDAR 14. panta 2. punkta b) VDAR).

Saskaņā ar VDAR 6. panta 1. punkta f) apakšpunktu apstrāde ir likumīga tikai tad, ja apstrāde ir nepieciešama pārziņa vai trešās personas leģitīmo interešu nodrošināšanai, izņemot gadījumus, kad par šādām interesēm prevalē datu subjekta intereses vai pamattiesības un pamatbrīvības, kas prasa personas datu aizsardzību. Saskaņā ar VDAR 47. apsvēruma 2. teikumu leģitīmas intereses varētu pastāvēt, ja starp datu subjektu un pārzini pastāv attiecīgas un atbilstošas attiecības, piemēram, situācijās, kad datu subjekts ir pārziņa klients. Visos gadījumos, kad mūsu uzņēmums apstrādā personas


© All rights reserved by Heiko Maniero.

datus, pamatojoties uz VDAR 6. panta 1. punkta f) apakšpunktu, mūsu leģitīmā interese ir mūsu uzņēmējdarbības veikšana par labu visu mūsu darbinieku un akcionāru labklājībai.

## I. Tas, ka pastāv tiesības pieprasīt no pārziņa piekļuvi datu subjekta personas datiem un to labošanu vai dzēšanu, vai apstrādes ierobežošanu attiecībā uz datu subjektu un tiesības iebilst pret apstrādi, kā arī tiesības uz datu pārnesamību (VDAR 14. panta 2. punkta c) VDAR).

Visiem datu subjektiem ir šādas tiesības:

***Piekļuves tiesības***

Katram datu subjektam ir tiesības piekļūt personas datiem, kas uz viņu attiecas. Piekļuves tiesības attiecas uz visiem mūsu apstrādātajiem datiem. Šīs tiesības var izmantot viegli un ar saprātīgiem intervāliem, lai uzzinātu un pārbaudītu apstrādes likumību (VDAR 63. apsvērums). Šīs tiesības izriet no Regulas (EK) Nr. VDAR 15. Datu subjekts var sazināties ar mums, lai izmantotu piekļuves tiesības.

***Tiesības uz labošanu***

Saskaņā ar VDAR 16. panta 1. teikumu datu subjektam ir tiesības no pārziņa bez nepamatotas kavēšanās saņemt neprecīzu personas datu labošanu, kas uz viņu attiecas. Turklāt VDAR 16. panta 2. teikumā noteikts, ka datu subjektam, ņemot vērā apstrādes nolūkus, ir tiesības uz nepilnīgu personas datu papildināšanu, tostarp sniedzot papildu paziņojumu. Datu subjekts var sazināties ar mums, lai izmantotu tiesības uz labošanu.

***Tiesības uz dzēšanu (tiesības tikt aizmirstam)***

Turklāt datu subjektiem ir tiesības uz dzēšanu un aizmiršanu saskaņā ar Regulas (EK) Nr. 17 VDAR. Šīs tiesības var izmantot, sazinoties ar mums. Tomēr šajā brīdī vēlamies norādīt, ka šīs tiesības nav piemērojamas, ja apstrāde ir nepieciešama, lai izpildītu juridisku pienākumu, kas attiecas uz mūsu uzņēmumu, kā noteikts VDAR 17. panta 3. punkta b) apakšpunktā. Tas nozīmē, ka mēs varam apstiprināt pieteikumu par dzēšanu tikai pēc likumā noteiktā glabāšanas termiņa beigām.

***Tiesības uz apstrādes ierobežošanu***

Saskaņā ar VDAR 18. pantu jebkuram datu subjektam ir tiesības uz apstrādes ierobežošanu. Apstrādes ierobežošanu var pieprasīt, ja ir izpildīts viens no VDAR 18. panta 1. punkta a-d apakšpunktā minētajiem nosacījumiem. Datu subjekts var sazināties ar mums, lai izmantotu tiesības uz apstrādes ierobežošanu.

***Tiesības iebilst***

Turklāt saskaņā ar Regulas (EK) Nr. VDAR 21. pants garantē tiesības iebilst. Datu subjekts var sazināties ar mums, lai izmantotu tiesības iebilst.

***Tiesības uz datu pārnesamību***

Art. 20 VDAR datu subjektam piešķir tiesības uz datu pārnesamību. Saskaņā ar šo noteikumu datu subjektam saskaņā ar VDAR 20. panta 1. punkta a) un b) apakšpunktā paredzētajiem nosacījumiem ir


© All rights reserved by Heiko Maniero.

tiesības saņemt personas datus, kas attiecas uz viņu un ko viņš ir sniedzis pārzinim, strukturētā, plaši izmantotā un mašīnlasāmā formātā, un tiesības nosūtīt šos datus citam pārzinim, netraucējot pārzinim, kuram personas dati ir sniegti. Datu subjekts var sazināties ar mums, lai izmantotu tiesības uz datu pārnesamību.

## J. Ja apstrāde pamatojas uz 6. panta 1. punkta a) apakšpunktu vai 9. panta 2. punkta a) apakšpunktu – tiesības jebkurā brīdī atsaukt piekrišanu, neietekmējot tādas apstrādes likumīgumu, kuras pamatā ir pirms atsaukuma sniegta piekrišana (VDAR 14. panta 2. punkta d) VDAR).

Ja personas datu apstrādes pamatā ir Regulas (EK) Nr. a panta 1. punkta a) apakšpunktu, kas ir gadījums, kad datu subjekts ir devis piekrišanu personas datu apstrādei vienam vai vairākiem konkrētiem nolūkiem, vai tā ir pamatota ar VDAR 9. panta 2. punkta a) apakšpunktu, kas reglamentē nepārprotamu piekrišanu īpašu kategoriju personas datu apstrādei, datu subjektam saskaņā ar VDAR 7. panta 3. punkta 1. teikuma 1. teikumu ir tiesības jebkurā laikā atsaukt savu piekrišanu.

Piekrišanas atsaukšana neietekmē tās apstrādes likumību, kuras pamatā ir piekrišana pirms tās atsaukšanas, VDAR 7. panta 3. punkta 2. teikums. Piekrišanu atsaukt ir tikpat vienkārši kā dot piekrišanu, 1. pants. VDAR 7. panta 3. punkta 4. teikums. Tāpēc piekrišanas atsaukšana vienmēr var notikt tādā pašā veidā, kādā piekrišana ir dota, vai jebkurā citā veidā, ko datu subjekts uzskata par vienkāršāku. Mūsdienu informācijas sabiedrībā, iespējams, vienkāršākais veids, kā atsaukt piekrišanu, ir vienkāršs e-pasts. Ja datu subjekts vēlas atsaukt mums doto piekrišanu, pietiek ar vienkāršu e-pasta vēstuli. Datu subjekts var arī izvēlēties jebkuru citu veidu, kā paziņot mums par piekrišanas atsaukšanu.

## K. Tiesības iesniegt sūdzību uzraudzības iestādei (VDAR 14. panta 2. punkta e) VDAR, 77. panta 1. punkts)

Mums kā pārzinim ir pienākums informēt datu subjektu par tiesībām iesniegt sūdzību uzraudzības iestādei, kā noteikts VDAR 14. panta 2. punkta e) apakšpunktā. Tiesības iesniegt sūdzību uzraudzības iestādei reglamentē VDAR 77. panta 1. punkts. Saskaņā ar šo noteikumu, neskarot citus administratīvos vai tiesiskās aizsardzības līdzekļus, katram datu subjektam ir tiesības iesniegt sūdzību uzraudzības iestādei, jo īpaši dalībvalstī, kurā ir viņa pastāvīgā dzīvesvieta, darbavieta vai iespējamā pārkāpuma vieta, ja datu subjekts uzskata, ka ar viņu saistīto personas datu apstrāde pārkāpj Vispārīgo datu aizsardzības regulu. Tiesības iesniegt sūdzību uzraudzības iestādei Savienības tiesību aktos tika ierobežotas tikai tādā veidā, ka tās var izmantot tikai vienā uzraudzības iestādē (Vispārīgās datu aizsardzības regulas 141. apsvēruma 1. teikums). Šis noteikums ir paredzēts, lai izvairītos no tā paša datu subjekta dubultām sūdzībām vienā un tajā pašā lietā. Tāpēc, ja datu subjekts vēlas iesniegt sūdzību par mums, mēs lūdzam vērsties tikai vienā uzraudzības iestādē.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## L. Informācija par to, no kāda avota personas dati ir iegūti, un – attiecīgā gadījumā – informācija par to, vai dati iegūti no publiski pieejamiem avotiem (VDAR 14. panta 2. punkta f) VDAR)

Principā personas datus vāc tieši no datu subjekta vai sadarbībā ar iestādi (piemēram, iegūstot datus no oficiāla reģistra). Citi dati par datu subjektiem tiek iegūti, nododot datus no grupas uzņēmumiem. Šīs vispārīgās informācijas kontekstā precīzu avotu, no kuriem iegūti personas dati, norādīšana ir vai nu neiespējama, vai arī prasītu nesamērīgas pūles Regulas (EK) Nr. panta 5. punkta b) apakšpunktu VDAR. Principā mēs nevācam personas datus no publiski pieejamiem avotiem.

Jebkurš datu subjekts var jebkurā laikā sazināties ar mums, lai iegūtu sīkāku informāciju par precīziem personas datu avotiem, kas uz viņu attiecas. Ja personas datu izcelsmi datu subjektam nevar norādīt, jo ir izmantoti dažādi avoti, ir jāsniedz vispārīga informācija (VDAR 61. apsvēruma 4. teikums).

## M. Tas, ka pastāv automatizēta lēmumu pieņemšana, tostarp profilēšana, kas minēta 22. panta 1. un 4. punktā, un – vismaz minētajos gadījumos – jēgpilna informācija par tajā ietverto loģiku, kā arī šādas apstrādes nozīmīgumu un paredzamajām sekām attiecībā uz datu subjektu (VDAR 14. panta 2. punkta g) VDAR).

Kā atbildīgs uzņēmums mēs parasti neizmantojam automatizētu lēmumu pieņemšanu vai profilēšanu. Ja izņēmuma gadījumos mēs veicam automatizētu lēmumu pieņemšanu vai profilēšanu, mēs par to informēsim datu subjektu atsevišķi vai ar apakšsadaļas palīdzību mūsu privātuma politikā (mūsu tīmekļa vietnē). Šādā gadījumā piemēro šādus noteikumus:

Automatizēta lēmumu pieņemšana, tostarp profilēšana, var notikt, ja (1) tas ir nepieciešams, lai noslēgtu vai izpildītu līgumu starp datu subjektu un mums, vai (2) to atļauj Savienības vai dalībvalsts tiesību akti, kas uz mums attiecas un kas nosaka arī piemērotus pasākumus datu subjekta tiesību un brīvību un likumīgo interešu aizsardzībai, vai (3) tas ir pamatots ar datu subjekta skaidru piekrišanu.

Gadījumos, kas minēti VDAR 22. panta 2. punkta a) un c) apakšpunktā, mēs īstenojam piemērotus pasākumus, lai aizsargātu datu subjekta tiesības un brīvības un likumīgās intereses. Šādos gadījumos jums ir tiesības panākt pārziņa iejaukšanos, paust savu viedokli un apstrīdēt lēmumu.

Nozīmīga informācija par iesaistīto loģiku, kā arī par šādas apstrādes nozīmi un paredzamajām sekām datu subjektam ir izklāstīta mūsu privātuma politikā.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## III. EU-U.S. Data Privacy Framework (EU-U.S. DPF), UK Extension to the EU-U.S. DPF, Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF)

Ja mūsu organizācija ir sertificēts EU-U.S. Data Privacy Framework (EU-U.S. DPF) un/vai UK Extension to the EU-U.S. DPF un/vai Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF) dalībnieks, ir spēkā šādi noteikumi:

Mēs ievērojam EU-U.S. Data Privacy Framework (EU-U.S. DPF) un UK Extension to the EU-U.S. DPF, kā arī Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF), kā to ir noteikusi ASV Tirdzniecības departaments. Mūsu uzņēmums ir apliecinājis ASV Tirdzniecības departamentam, ka tas ievēro EU-U.S. Data Privacy Framework Principles (EU-U.S. DPF Principles) attiecībā uz personas datu apstrādi, ko tas saņem no Eiropas Savienības un Apvienotās Karalistes, pamatojoties uz EU-U.S. DPF un UK Extension to the EU-U.S. DPF. Mūsu uzņēmums ir apliecinājis ASV Tirdzniecības departamentam, ka tas ievēro Swiss-U.S. Data Privacy Framework Principles (Swiss-U.S. DPF Principles) attiecībā uz personas datu apstrādi, ko tas saņem no Šveices, pamatojoties uz Swiss-U.S. DPF. Gadījumā, ja pastāv pretrunas starp mūsu privātuma politikas noteikumiem un EU-U.S. DPF Principles un/vai Swiss-U.S. DPF Principles, noteicošie ir Principles.

Lai uzzinātu vairāk par Data Privacy Framework (DPF) programmu un apskatītu mūsu sertifikāciju, lūdzu, apmeklējiet https://www.dataprivacyframework.gov/.

Pārējās mūsu uzņēmuma ASV vienības vai meitasuzņēmumi, kas arī ievēro EU-U.S. DPF Principals, tostarp UK Extension to the EU-U.S. DPF un Swiss-U.S. DPF Principals, ja tādi ir, ir norādīti mūsu privātuma politikā.

Saskaņā ar EU-U.S. DPF un UK Extension to the EU-U.S. DPF, kā arī Swiss-U.S. DPF mūsu uzņēmums apņemas sadarboties ar ES datu aizsardzības iestāžu un Apvienotās Karalistes Information Commissioner's Office (ICO), kā arī Šveices Federālā datu aizsardzības un informācijas komisāra (EDÖB) izveidoto paneli un ievērot to ieteikumus attiecībā uz neatrisinātām sūdzībām par mūsu personas datu apstrādi, ko mēs saņemam, pamatojoties uz EU-U.S. DPF un UK Extension to the EU-U.S. DPF un Swiss-U.S. DPF.

Mēs informējam skartās personas par attiecīgajām Eiropas datu aizsardzības iestādēm, kas ir atbildīgas par sūdzību izskatīšanu par mūsu organizācijas personas datu apstrādi, šī pārredzamības dokumenta augšdaļā un par to, ka mēs piedāvājam skartajām personām atbilstošu un bezmaksas tiesisko aizsardzību.

Mēs informējam visas skartās personas, ka mūsu uzņēmums ir pakļauts Federal Trade Commission (FTC) izmeklēšanas un izpildes pilnvarām.

Skartajām personām ir noteiktos apstākļos iespēja izmantot saistošu šķīrējtiesu. Mūsu organizācija ir apņēmusies risināt prasības un ievērot noteikumus, kas izklāstīti DPF-Principals I pielikumā, ja skartā


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

persona ir pieprasījusi saistošu šķīrējtiesu, paziņojot par to mūsu organizācijai un ievērojot I pielikumā izklāstītos procedūras un noteikumus.

Ar šo mēs informējam visas skartās personas par mūsu organizācijas atbildību gadījumā, ja personas dati tiek nodoti trešajām personām.

Jautājumiem no skartajām personām vai datu aizsardzības uzraudzības iestādēm mēs esam norādījuši vietējos pārstāvjus, kas minēti šī pārredzamības dokumenta augšdaļā.

Mēs piedāvājam jums iespēju izvēlēties (Opt-out), vai jūsu personas dati (i) tiek nodoti trešajām personām vai (ii) tiek izmantoti mērķim, kas būtiski atšķiras no mērķa/mērķiem, kam tie sākotnēji tika savākti vai vēlāk jūsu apstiprināti. Skaidrs, labi redzams un viegli pieejams mehānisms, kā izmantot jūsu izvēli, ir sazināties ar mūsu datu aizsardzības speciālistu (DSB) pa e-pastu. Jums nav izvēles iespēju, un mēs neesam arī pienākuma to darīt, ja dati tiek nodoti trešajai pusei, kas darbojas kā aģents vai apstrādātājs mūsu vārdā un saskaņā ar mūsu norādījumiem. Tomēr mēs vienmēr slēdzam līgumu ar šādu aģentu vai apstrādātāju.

Attiecībā uz sensitīvajiem datiem (t.i., personas datiem, kas satur informāciju par veselības stāvokli, rasu vai etnisko izcelsmi, politiskajiem uzskatiem, reliģiskajiem vai filozofiskajiem uzskatiem, dalību arodbiedrībā vai informāciju par attiecīgās personas seksuālo dzīvi), mēs iegūstam jūsu skaidru piekrišanu (Opt-in), kad šie dati (i) tiek nodoti trešajām personām vai (ii) tiek izmantoti citam mērķim, nevis tam, kam tie sākotnēji tika savākti vai kam jūs vēlāk devāt piekrišanu, izvēloties Opt-in. Turklāt mēs visus personas datus, ko saņemam no trešajām personām, uzskatām par sensitīviem, ja trešā puse tos ir identificējusi un apstrādājusi kā tādus.

Mēs informējam jūs ar šo par prasību izpaust personas datus, reaģējot uz likumīgām iestāžu prasībām, tostarp izpildot nacionālās drošības vai tiesībaizsardzības prasības.

Nododot personas datus trešajai personai, kas darbojas kā pārzinis, mēs ievērojam Principals par paziņošanu un izvēli. Turklāt mēs slēdzam līgumu ar trešo personu, kas ir atbildīga par apstrādi, kurā paredzēts, ka šie dati drīkst tikt apstrādāti tikai ierobežotiem un noteiktiem mērķiem saskaņā ar jūsu sniegto piekrišanu un ka saņēmējam jānodrošina tāds pats aizsardzības līmenis kā DPF Principals un jāinformē mūs, ja tas konstatē, ka vairs nevar izpildīt šo pienākumu. Līgumā ir paredzēts, ka trešā persona, kas ir pārzinis, pārtrauc apstrādi vai veic citus piemērotus un atbilstošus pasākumus, lai novērstu situāciju, ja tiek izdarīts šāds secinājums.

Nododot personas datus trešajai personai, kas darbojas kā aģents vai apstrādātājs, (i) mēs nododam šos datus tikai ierobežotiem un noteiktiem mērķiem; (ii) mēs nodrošinām, ka aģents vai apstrādātājs ir pienākums nodrošināt vismaz tādu pašu datu aizsardzības līmeni, kādu pieprasa DPF-Principals; (iii) mēs veicam piemērotus un atbilstošus pasākumus, lai nodrošinātu, ka aģents vai apstrādātājs faktiski apstrādā pārsūtītos personas datus tādā veidā, kas atbilst mūsu saistībām saskaņā ar DPF-Principals; (iv) mēs pieprasām, lai aģents vai apstrādātājs informē mūsu organizāciju, ja tas konstatē, ka vairs nevar izpildīt pienākumu nodrošināt tādu pašu aizsardzības līmeni, kādu paredz DPF-Principals; (v) pēc šāda


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

paziņojuma, arī saskaņā ar (iv), mēs veicam piemērotus un atbilstošus pasākumus, lai pārtrauktu neatļautu apstrādi un novērstu situāciju; un (vi) pēc pieprasījuma mēs DPF Department sniedzam kopsavilkumu vai reprezentatīvu piemēru par atbilstošajiem datu aizsardzības noteikumiem no mūsu līguma ar šo aģentu.

Saskaņā ar EU-U.S. DPF un/vai UK Extension to the EU-U.S. DPF un/vai Swiss-U.S. DPF mūsu organizācija apņemas sadarboties ar ES datu aizsardzības iestāžu un Apvienotās Karalistes Information Commissioner's Office (ICO) vai Šveices Federālā datu aizsardzības un informācijas komisāra (EDÖB) izveidoto paneli un ievērot to ieteikumus attiecībā uz neatrisinātām sūdzībām par mūsu rīcību ar personāldatiem, ko mēs saņemam saistībā ar darba attiecībām, pamatojoties uz EU-U.S. DPF un UK Extension to the EU-U.S. DPF un Swiss-U.S. DPF.

Visiem datu subjektiem, kuri uz laiku atrodas Eiropas Savienībā (ES), Eiropas Ekonomikas zonā (EEZ) vai Apvienotajā Karalistē vai kuru domicils vai pastāvīgā dzīvesvieta ir tur, ir tiesības un datu subjekta tiesības, kas ir publicētas mūsu pārredzamības dokumentā un kas izriet arī no VDAR 15.-22. panta, tostarp tiesības piekļūt personas datiem. Mēs esam nodrošinājuši šīs informācijas pieejamību visās ES un EEZ valodās. Angļu valodas versija attiecas uz Apvienoto Karalisti.

Visiem datu subjektiem, kuri uz laiku uzturas Šveicē vai kuru dzīvesvieta vai pastāvīgā dzīvesvieta ir Šveicē, ir tiesības un datu subjekta tiesības saskaņā ar Šveices Datu aizsardzības likumu (DPA) un Šveices Datu aizsardzības regulu (DPR), kas ir publicētas mūsu pārredzamības dokumentā, tostarp tiesības piekļūt personas datiem. Mēs esam snieguši šo informāciju trīs Šveices oficiālajās valodās (vācu, itāļu un franču).


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

# LATVIAN: Informācija par darbinieku un pretendentu personas datu apstrādi (VDAR 13., 14. pants)

Cienījamais kungs vai kundze,

Darbinieku un pieteikumu iesniedzēju personas dati ir īpaši aizsargājami. Mūsu mērķis ir nodrošināt augstu datu aizsardzības līmeni. Tāpēc mēs regulāri pilnveidojam savas datu aizsardzības un datu drošības koncepcijas.

Protams, mēs ievērojam likumā noteiktos datu aizsardzības noteikumus. Saskaņā ar VDAR 13., 14. pantu pārziņi, apstrādājot personas datus, ievēro īpašas informācijas prasības. Ar šo dokumentu šie pienākumi ir izpildīti.

Tiesiskā regulējuma terminoloģija ir sarežģīta. Diemžēl, sagatavojot šo dokumentu, nebija iespējams izvairīties no juridisko terminu lietošanas. Tāpēc vēlamies norādīt, ka vienmēr esat laipni aicināti sazināties ar mums par visiem jautājumiem saistībā ar šo dokumentu, izmantotajiem terminiem vai formulējumiem.

## I. Informācija, kas jāsniedz, ja personas dati ir iegūti no datu subjekta (VDAR 13. pants)

### A. Pārziņa un attiecīgā gadījumā pārziņa pārstāvja identitāte un kontaktinformācija (VDAR 13. panta 1. punkta a) VDAR)

Skatīt iepriekš

### B. Attiecīgā gadījumā – datu aizsardzības speciālista kontaktinformācija (VDAR 13. panta 1. punkta b) VDAR)

Skatīt iepriekš

### C. Apstrādes nolūki, kam paredzēti personas dati, kā arī apstrādes juridiskais pamats (VDAR 13. panta 1. punkta c) VDAR)

Attiecībā uz pieteikuma iesniedzēja datiem datu apstrādes mērķis ir veikt pieteikuma pārbaudi darbā pieņemšanas procesā. Šim nolūkam mēs apstrādājam visus jūsu sniegtos datus. Pamatojoties uz darbā pieņemšanas procesā iesniegtajiem datiem, mēs pārbaudīsim, vai jūs esat uzaicināts uz darba interviju


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

(atlases procesa daļa). Vispārēji piemērotu kandidātu gadījumā, jo īpaši darba intervijas kontekstā, mēs apstrādājam noteiktus citus jūsu sniegtos personas datus, kas ir būtiski mūsu atlases lēmuma pieņemšanai. Ja jūs pie mums pieņemsim darbā, pretendenta dati automātiski pārtaps darbinieka datos. Kā daļu no darbā pieņemšanas procesa mēs apstrādāsim citus jūsu personas datus, kurus mēs no jums pieprasīsim un kuri ir nepieciešami, lai uzsāktu vai izpildītu līgumu (piemēram, personas identifikācijas numurus vai nodokļu maksātāja numurus). Attiecībā uz darbinieku datiem datu apstrādes mērķis ir darba līguma izpilde vai citu darba attiecībām piemērojamo tiesību normu (piemēram, nodokļu tiesību aktu) ievērošana, kā arī jūsu personas datu izmantošana, lai izpildītu ar jums noslēgto darba līgumu (piemēram, jūsu vārda un kontaktinformācijas publicēšana uzņēmumā vai klientiem). Darbinieka dati tiek glabāti arī pēc darba attiecību izbeigšanas, lai ievērotu likumā noteiktos glabāšanas termiņus.

Datu apstrādes juridiskais pamats ir VDAR 6. panta 1. punkta b) VDAR, VDAR 9. panta 2. punkta b) un h) VDAR, VDAR 88. panta 1. punkts un valsts tiesību akti, piemēram, Vācijas Federālā datu aizsardzības likuma (BDSG) 26. pants.

## D. Personas datu saņēmēji vai saņēmēju kategorijas, ja tādi ir (VDAR 13. panta 1. punkta e) VDAR)

Valsts iestādes

Ārējās struktūras

Citas ārējās struktūras

Iekšējā apstrāde

Apstrāde grupas iekšienē

Citas struktūras

Mūsu apstrādātāju un datu saņēmēju trešās valstīs un, attiecīgā gadījumā, starptautisko organizāciju saraksts ir publicēts mūsu tīmekļa vietnē vai arī to var pieprasīt no mums bez maksas. Lūdzu, sazinieties ar mūsu datu aizsardzības speciālistu, lai pieprasītu šo sarakstu.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## E. Attiecīgā gadījumā – informācija, ka pārzinis paredz nosūtīt personas datus uz trešo valsti vai starptautisku organizāciju, un informācija par to, ka eksistē vai neeksistē Komisijas lēmums par aizsardzības līmeņa pietiekamību, vai – 46. vai 47. pantā, vai 49. panta 1. punkta otrajā daļā minētās nosūtīšanas gadījumā – atsauce uz atbilstošām vai piemērotām garantijām un informācija par to, kā saņemt datu kopiju, vai to, kur tie ir darīti pieejami (VDAR 13. panta 1. punkta f) VDAR, 46. panta 1. punkts, 46. panta 2. punkta c) VDAR).

Visi mūsu grupas uzņēmumi un filiāles (turpmāk tekstā - "grupas uzņēmumi"), kuru uzņēmējdarbības vieta vai birojs atrodas trešā valstī, var būt personas datu saņēmēji. Visu grupas uzņēmumu vai saņēmēju sarakstu var pieprasīt no mums.

Saskaņā ar VDAR 46. panta 1. punktu pārzinis vai apstrādātājs var nosūtīt personas datus uz trešo valsti tikai tad, ja pārzinis vai apstrādātājs ir nodrošinājis atbilstošas garantijas un ar nosacījumu, ka datu subjektiem ir pieejamas īstenojamas datu subjekta tiesības un efektīvi tiesiskās aizsardzības līdzekļi. Piemērotus aizsardzības pasākumus var nodrošināt, neprasot īpašu uzraudzības iestādes atļauju, izmantojot standarta līguma klauzulas, VDAR 46. panta 2. punkta c) VDAR.

Ar visiem saņēmējiem no trešām valstīm pirms pirmās personas datu pārsūtīšanas tiek saskaņotas Eiropas Savienības standarta līguma klauzulas vai citi piemēroti drošības pasākumi. Tādējādi tiek nodrošināts, ka datu subjektiem tiek garantētas atbilstošas garantijas, īstenojamas datu subjektu tiesības un efektīvi tiesiskās aizsardzības līdzekļi. Katrs datu subjekts var saņemt no mums standarta līguma noteikumu kopiju. Standarta līguma klauzulas ir pieejamas arī Eiropas Savienības Oficiālajā Vēstnesī.

Vispārīgās datu aizsardzības regulas (VDAR) 45. panta 3. punktā Eiropas Komisijai ir piešķirtas pilnvaras ar īstenošanas aktu pieņemt lēmumu, ka valsts, kas nav ES dalībvalsts, nodrošina pietiekamu aizsardzības līmeni. Tas nozīmē tādu personas datu aizsardzības līmeni, kas būtībā ir līdzvērtīgs aizsardzības līmenim ES. Lēmumu par aizsardzības līmeņa pietiekamību rezultātā personas dati var brīvi un bez papildu šķēršļiem pārvietoties no ES (un Norvēģijas, Lihtenšteinas un Islandes) uz trešo valsti. Līdzīgi noteikumi ir spēkā Apvienotajā Karalistē, Šveicē un dažās citās valstīs.

Ja Eiropas Komisija vai citas valsts valdība ir nolēmusi, ka trešā valsts nodrošina pietiekamu aizsardzības līmeni, un ir spēkā spēkā esoša sistēma (piemēram, EU-U.S. Data Privacy Framework, Swiss-U.S. Data Privacy Framework, UK Extension to the EU-U.S. Data Privacy Framework), visi mūsu veiktie datu pārsūtīšanas gadījumi šādu sistēmu dalībniekiem (piemēram, pašsertificētām struktūrām) ir balstīti tikai uz šo struktūru dalību attiecīgajā sistēmā. Ja mēs vai kāda no mūsu grupas struktūrām ir šādas sistēmas dalībniece, visi datu nodošanas gadījumi mums vai mūsu grupas struktūrai ir balstīti tikai uz šo struktūru dalību šādā sistēmā.

Jebkurš datu subjekts var saņemt no mums šo ietvaru kopiju. Turklāt pamatprincipu kopijas ir pieejamas arī Eiropas Savienības Oficiālajā Vēstnesī vai publicētajos juridiskajos materiālos, vai uzraudzības iestāžu vai citu kompetento iestāžu vai institūciju tīmekļa vietnēs.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## F. Laikposms, cik ilgi personas dati tiks glabāti, vai, ja tas nav iespējams, kritēriji, ko izmanto minētā laikposma noteikšanai (VDAR 13. panta 2. punkta a) VDAR)

Pieteikumu iesniedzēju personas datu glabāšanas ilgums ir 6 mēneši. Darbinieku datiem piemēro attiecīgo likumā noteikto glabāšanas termiņu. Pēc šā termiņa beigām attiecīgie dati tiek regulāri dzēsti, ja vien tie vairs nav nepieciešami līguma izpildei vai līguma uzsākšanai.

## G. Tas, ka pastāv tiesības pieprasīt pārzinim piekļuvi datu subjekta personas datiem un to labošanu vai dzēšanu, vai apstrādes ierobežošanu attiecībā uz datu subjektu, vai tiesības iebilst pret apstrādi, kā arī tiesības uz datu pārnesamību (VDAR 13. panta 2. punkta b) VDAR).

Visiem datu subjektiem ir šādas tiesības:

***Piekļuves tiesības***

Katram datu subjektam ir tiesības piekļūt personas datiem, kas uz viņu attiecas. Piekļuves tiesības attiecas uz visiem mūsu apstrādātajiem datiem. Šīs tiesības var izmantot viegli un ar saprātīgiem intervāliem, lai uzzinātu un pārbaudītu apstrādes likumību (VDAR 63. apsvērums). Šīs tiesības izriet no Regulas (EK) Nr. VDAR 15. Datu subjekts var sazināties ar mums, lai izmantotu piekļuves tiesības.

***Tiesības uz labošanu***

Saskaņā ar VDAR 16. panta 1. teikumu datu subjektam ir tiesības no pārziņa bez nepamatotas kavēšanās saņemt neprecīzu personas datu labošanu, kas uz viņu attiecas. Turklāt VDAR 16. panta 2. teikumā noteikts, ka datu subjektam, ņemot vērā apstrādes nolūkus, ir tiesības uz nepilnīgu personas datu papildināšanu, tostarp sniedzot papildu paziņojumu. Datu subjekts var sazināties ar mums, lai izmantotu tiesības uz labošanu.

***Tiesības uz dzēšanu (tiesības tikt aizmirstam)***

Turklāt datu subjektiem ir tiesības uz dzēšanu un aizmiršanu saskaņā ar Regulas (EK) Nr. 17 VDAR. Šīs tiesības var izmantot, sazinoties ar mums. Tomēr šajā brīdī mēs vēlamies norādīt, ka šīs tiesības nav piemērojamas, ja apstrāde ir nepieciešama, lai izpildītu juridisku pienākumu, kas attiecas uz mūsu uzņēmumu, kā noteikts VDAR 17. panta 3. punkta b) apakšpunktā. Tas nozīmē, ka mēs varam apstiprināt pieteikumu par dzēšanu tikai pēc likumā noteiktā glabāšanas termiņa beigām.

***Tiesības uz apstrādes ierobežošanu***

Saskaņā ar VDAR 18. pantu jebkuram datu subjektam ir tiesības uz apstrādes ierobežošanu. Apstrādes ierobežošanu var pieprasīt, ja ir izpildīts viens no VDAR 18. panta 1. punkta a-d apakšpunktā minētajiem nosacījumiem. Datu subjekts var sazināties ar mums, lai izmantotu tiesības uz apstrādes ierobežošanu.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

***Tiesības iebilst***

Turklāt saskaņā ar Regulas (EK) Nr. VDAR 21. pants garantē tiesības iebilst. Datu subjekts var sazināties ar mums, lai izmantotu tiesības iebilst.

***Tiesības uz datu pārnesamību***

Art. 20 VDAR datu subjektam piešķir tiesības uz datu pārnesamību. Saskaņā ar šo noteikumu datu subjektam saskaņā ar VDAR 20. panta 1. punkta a) un b) apakšpunktā paredzētajiem nosacījumiem ir tiesības saņemt personas datus, kas attiecas uz viņu un ko viņš ir sniedzis pārzinim, strukturētā, plaši izmantotā un mašīnlasāmā formātā, un tiesības nosūtīt šos datus citam pārzinim, netraucējot pārzinim, kuram personas dati ir sniegti. Datu subjekts var sazināties ar mums, lai izmantotu tiesības uz datu pārnesamību.

## H. Ja apstrāde pamatojas uz 6. panta 1. punkta a) apakšpunktu vai 9. panta 2. punkta a) apakšpunktu – tiesības jebkurā brīdī atsaukt piekrišanu, neietekmējot tādas apstrādes likumīgumu, kuras pamatā ir pirms atsaukuma sniegta piekrišana (VDAR 13. panta 2. punkta c) VDAR).

Ja personas datu apstrādes pamatā ir Regulas (EK) Nr. a panta 1. punkta a) apakšpunktu, kas ir gadījums, kad datu subjekts ir devis piekrišanu personas datu apstrādei vienam vai vairākiem konkrētiem nolūkiem, vai tā ir pamatota ar VDAR 9. panta 2. punkta a) apakšpunktu, kas reglamentē skaidru piekrišanu īpašu kategoriju personas datu apstrādei, datu subjektam saskaņā ar VDAR 7. panta 3. punkta 1. teikuma 1. teikumu ir tiesības jebkurā laikā atsaukt savu piekrišanu.

Piekrišanas atsaukšana neietekmē tās apstrādes likumību, kuras pamatā ir piekrišana pirms tās atsaukšanas, VDAR 7. panta 3. punkta 2. teikums. Piekrišanu atsaukt ir tikpat vienkārši kā dot piekrišanu, 1. pants. VDAR 7. panta 3. punkta 4. teikums. Tāpēc piekrišanas atsaukšana vienmēr var notikt tādā pašā veidā, kādā piekrišana ir dota, vai jebkurā citā veidā, ko datu subjekts uzskata par vienkāršāku. Mūsdienu informācijas sabiedrībā, iespējams, vienkāršākais veids, kā atsaukt piekrišanu, ir vienkāršs e-pasts. Ja datu subjekts vēlas atsaukt mums doto piekrišanu, pietiek ar vienkāršu e-pasta vēstuli. Datu subjekts var arī izvēlēties jebkuru citu veidu, kā paziņot mums par piekrišanas atsaukšanu.

## I. Tiesības iesniegt sūdzību uzraudzības iestādei (VDAR 13. panta 2. punkta d) VDAR, 77. panta 1. punkts)

Mums kā pārzinim ir pienākums informēt datu subjektu par tiesībām iesniegt sūdzību uzraudzības iestādei, VDAR 13. panta 2. punkta d) VDAR. Tiesības iesniegt sūdzību uzraudzības iestādei reglamentē VDAR 77. panta 1. punkts. Saskaņā ar šo noteikumu, neskarot citus administratīvos vai tiesiskās aizsardzības līdzekļus, katram datu subjektam ir tiesības iesniegt sūdzību uzraudzības iestādei, jo īpaši dalībvalstī, kurā ir viņa pastāvīgā dzīvesvieta, darbavieta vai iespējamā pārkāpuma vieta, ja datu subjekts uzskata, ka ar viņu saistīto personas datu apstrāde pārkāpj Vispārīgo datu aizsardzības regulu. Tiesības


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

iesniegt sūdzību uzraudzības iestādei Savienības tiesību aktos tika ierobežotas tikai tādā veidā, ka tās var izmantot tikai vienā uzraudzības iestādē (Vispārīgās datu aizsardzības regulas 141. apsvēruma 1. teikums). Šis noteikums ir paredzēts, lai izvairītos no tā paša datu subjekta dubultām sūdzībām vienā un tajā pašā lietā. Tāpēc, ja datu subjekts vēlas iesniegt sūdzību par mums, mēs lūdzam vērsties tikai vienā uzraudzības iestādē.

## J. Informācija, vai personas datu sniegšana ir noteikta saskaņā ar likumu vai līgumu, vai tā ir priekšnosacījums, lai līgumu noslēgtu, kā arī informācija par to, vai datu subjektam ir pienākums personas datus sniegt un kādas sekas var būt gadījumos, kad šādi dati netiek sniegti (VDAR 13. panta 2. punkta e) VDAR)

Mēs paskaidrojam, ka personas datu sniegšana ir daļēji prasīta ar likumu (piemēram, nodokļu noteikumi) vai var izrietēt arī no līguma noteikumiem (piemēram, informācija par līguma partneri).

Dažkārt, lai noslēgtu līgumu, var būt nepieciešams, lai datu subjekts mums sniegtu personas datus, kas mums pēc tam jāapstrādā. Piemēram, datu subjektam ir pienākums sniegt mums personas datus, kad mūsu uzņēmums ar viņu slēdz līgumu. Personas datu nesniegšanas sekas būtu tādas, ka līgumu ar datu subjektu nevarētu noslēgt.

Pirms datu subjekts sniedz personas datus, datu subjektam ir jāsazinās ar mums. Mēs izskaidrojam datu subjektam, vai personas datu sniegšana ir prasīta ar likumu vai līgumu vai ir nepieciešama līguma noslēgšanai, vai ir pienākums sniegt personas datus un kādas ir personas datu nesniegšanas sekas.

## K. Tas, ka pastāv automatizēta lēmumu pieņemšana, tostarp profilēšana, kas minēta 22. panta 1. un 4. punktā, un – vismaz minētajos gadījumos – jēgpilna informācija par tajā ietverto loģiku, kā arī šādas apstrādes nozīmīgumu un paredzamajām sekām attiecībā uz datu subjektu (VDAR 13. panta 2. punkta f) VDAR).

Kā atbildīgs uzņēmums mēs parasti neizmantojam automatizētu lēmumu pieņemšanu vai profilēšanu. Ja izņēmuma gadījumos mēs veicam automatizētu lēmumu pieņemšanu vai profilēšanu, mēs par to informēsim datu subjektu atsevišķi vai ar apakšsadaļas palīdzību mūsu privātuma politikā (mūsu tīmekļa vietnē). Šādā gadījumā piemēro šādus noteikumus:

Automatizēta lēmumu pieņemšana, tostarp profilēšana, var notikt, ja (1) tas ir nepieciešams, lai noslēgtu vai izpildītu līgumu starp datu subjektu un mums, vai (2) to atļauj Savienības vai dalībvalsts tiesību akti, kas uz mums attiecas un kas nosaka arī piemērotus pasākumus datu subjekta tiesību un brīvību un likumīgo interešu aizsardzībai, vai (3) tas ir pamatots ar datu subjekta skaidru piekrišanu.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

Gadījumos, kas minēti VDAR 22. panta 2. punkta a) un c) apakšpunktā, mēs īstenojam piemērotus pasākumus, lai aizsargātu datu subjekta tiesības un brīvības un likumīgās intereses. Šādos gadījumos jums ir tiesības panākt pārziņa iejaukšanos, paust savu viedokli un apstrīdēt lēmumu.

Nozīmīga informācija par iesaistīto loģiku, kā arī par šādas apstrādes nozīmi un paredzamajām sekām datu subjektam ir izklāstīta mūsu privātuma politikā.

## II. Informācija, kas jāsniedz, ja personas dati nav iegūti no datu subjekta (VDAR 14. pants)

### A. Pārziņa un attiecīgā gadījumā pārziņa pārstāvja identitāte un kontaktinformācija

Skatīt iepriekš

### B. Attiecīgā gadījumā – datu aizsardzības speciālista kontaktinformācija (VDAR 14. panta 1. punkta b) VDAR)

Skatīt iepriekš

### C. Apstrādes nolūki, kam paredzēti personas dati, kā arī apstrādes juridiskais pamats (VDAR 14. panta 1. punkta c) VDAR)

Attiecībā uz pieteikuma iesniedzēja datiem, kas nav iegūti no datu subjekta, datu apstrādes mērķis ir veikt pieteikuma pārbaudi darbā pieņemšanas procesā. Šim nolūkam mēs varam apstrādāt datus, kas nav iegūti no jums. Pamatojoties uz darbā pieņemšanas procesā apstrādātajiem datiem, mēs pārbaudīsim, vai jūs esat uzaicināts uz darba interviju (atlases procesa daļa). Ja jūs pie mums pieņems darbā, pretendenta dati automātiski pārtaps darbinieka datos. Attiecībā uz darbinieku datiem datu apstrādes mērķis ir darba līguma izpilde vai citu darba attiecībām piemērojamo tiesību normu ievērošana. Darbinieku dati tiek glabāti pēc darba attiecību izbeigšanas, lai ievērotu juridiskos glabāšanas termiņus.

Datu apstrādes juridiskais pamats ir VDAR 6. panta 1. punkta b) un f) VDAR, VDAR 9. panta 2. punkta b) un h) VDAR, VDAR 88. panta 1. punkts un valsts tiesību akti, piemēram, Vācijas Federālā datu aizsardzības likuma (BDSG) 26. pants.

### D. Attiecīgo personas datu kategorijas (VDAR 14. panta 1. punkta d) VDAR)

Pieteikuma iesniedzēja dati


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## E. Personas datu saņēmēji vai saņēmēju kategorijas, ja tādas ir (VDAR 14. panta 1. punkta e) VDAR)

Valsts iestādes

Ārējās struktūras

Citas ārējās struktūras

Iekšējā apstrāde

Apstrāde grupas iekšienē

Citas struktūras

Mūsu apstrādātāju un datu saņēmēju trešās valstīs un, attiecīgā gadījumā, starptautisko organizāciju saraksts ir publicēts mūsu tīmekļa vietnē vai arī to var pieprasīt no mums bez maksas. Lūdzu, sazinieties ar mūsu datu aizsardzības speciālistu, lai pieprasītu šo sarakstu.

## F. Attiecīgā gadījumā – informācija, ka pārzinis paredz nosūtīt personas datus saņēmējam trešā valstī vai starptautiskai organizācijai, un informācija par to, ka eksistē vai neeksistē Komisijas lēmums par aizsardzības līmeņa pietiekamību, vai – 46. vai 47. pantā, vai 49. panta 1. punkta otrajā daļā minētās nosūtīšanas gadījumā – atsauce uz atbilstošām vai piemērotām garantijām un informācija par to, kā saņemt datu kopiju, vai to, kur tie ir darīti pieejami (VDAR 14. panta 1. punkta f) VDAR, 46. panta 1. punkts, 46. panta 2. punkta c) VDAR).

Visi mūsu grupas uzņēmumi un filiāles (turpmāk tekstā - "grupas uzņēmumi"), kuru uzņēmējdarbības vieta vai birojs atrodas trešā valstī, var būt personas datu saņēmēji. Visu grupas uzņēmumu vai saņēmēju sarakstu var pieprasīt no mums.

Saskaņā ar VDAR 46. panta 1. punktu pārzinis vai apstrādātājs var nosūtīt personas datus uz trešo valsti tikai tad, ja pārzinis vai apstrādātājs ir nodrošinājis atbilstošas garantijas un ar nosacījumu, ka datu subjektiem ir pieejamas īstenojamas datu subjekta tiesības un efektīvi tiesiskās aizsardzības līdzekļi. Piemērotus aizsardzības pasākumus var nodrošināt, neprasot īpašu uzraudzības iestādes atļauju, izmantojot standarta datu aizsardzības klauzulas, VDAR 46. panta 2. punkta c) VDAR.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

Ar visiem saņēmējiem no trešām valstīm pirms pirmās personas datu pārsūtīšanas tiek saskaņotas Eiropas Savienības standarta līguma klauzulas vai citi piemēroti drošības pasākumi. Tādējādi tiek nodrošināts, ka datu subjektiem tiek garantētas atbilstošas garantijas, īstenojamas datu subjektu tiesības un efektīvi tiesiskās aizsardzības līdzekļi. Katrs datu subjekts var saņemt no mums standarta līguma noteikumu kopiju. Standarta līguma klauzulas ir pieejamas arī Eiropas Savienības Oficiālajā Vēstnesī.

Vispārīgās datu aizsardzības regulas (VDAR) 45. panta 3. punktā Eiropas Komisijai ir piešķirtas pilnvaras ar īstenošanas aktu pieņemt lēmumu, ka valsts, kas nav ES dalībvalsts, nodrošina pietiekamu aizsardzības līmeni. Tas nozīmē tādu personas datu aizsardzības līmeni, kas būtībā ir līdzvērtīgs aizsardzības līmenim ES. Lēmumu par aizsardzības līmeņa pietiekamību rezultātā personas dati var brīvi un bez papildu šķēršļiem pārvietoties no ES (un Norvēģijas, Lihtenšteinas un Islandes) uz trešo valsti. Līdzīgi noteikumi ir spēkā Apvienotajā Karalistē, Šveicē un dažās citās valstīs.

Ja Eiropas Komisija vai citas valsts valdība ir nolēmusi, ka trešā valsts nodrošina pietiekamu aizsardzības līmeni, un ir spēkā spēkā esoša sistēma (piemēram, EU-U.S. Data Privacy Framework, Swiss-U.S. Data Privacy Framework, UK Extension to the EU-U.S. Data Privacy Framework), visi mūsu veiktie datu pārsūtīšanas gadījumi šādu sistēmu dalībniekiem (piemēram, pašsertificētām struktūrām) ir balstīti tikai uz šo struktūru dalību attiecīgajā sistēmā. Ja mēs vai kāda no mūsu grupas struktūrām ir šādas sistēmas dalībniece, visi datu nodošanas gadījumi mums vai mūsu grupas struktūrai ir balstīti tikai uz šo struktūru dalību šādā sistēmā.

Jebkurš datu subjekts var saņemt no mums šo ietvaru kopiju. Turklāt pamatprincipu kopijas ir pieejamas arī Eiropas Savienības Oficiālajā Vēstnesī vai publicētajos juridiskajos materiālos, vai uzraudzības iestāžu vai citu kompetento iestāžu vai institūciju tīmekļa vietnēs.

## G. Laikposms, cik ilgi personas dati tiks glabāti, vai, ja tas nav iespējams, kritēriji, ko izmanto minētā laikposma noteikšanai (VDAR 14. panta 2. punkta a) VDAR)

Pieteikumu iesniedzēju personas datu glabāšanas ilgums ir 6 mēneši. Darbinieku datiem piemēro attiecīgo likumā noteikto glabāšanas termiņu. Pēc šā termiņa beigām attiecīgie dati tiek regulāri dzēsti, ja vien tie vairs nav nepieciešami līguma izpildei vai līguma uzsākšanai.

## H. Pārziņa vai trešās personas leģitīmās intereses, ja apstrāde pamatojas uz 6. panta 1. punkta f) apakšpunktu (VDAR 14. panta 2. punkta b) VDAR).

Saskaņā ar VDAR 6. panta 1. punkta f) apakšpunktu apstrāde ir likumīga tikai tad, ja apstrāde ir nepieciešama pārziņa vai trešās personas leģitīmo interešu nodrošināšanai, izņemot gadījumus, kad par šādām interesēm prevalē datu subjekta intereses vai pamattiesības un pamatbrīvības, kas prasa personas datu aizsardzību. Saskaņā ar VDAR 47. apsvēruma 2. teikumu leģitīmas intereses varētu pastāvēt, ja starp datu subjektu un pārzini pastāv attiecīgas un atbilstošas attiecības, piemēram,


© All rights reserved by Heiko Maniero.

situācijās, kad datu subjekts ir pārziņa klients. Visos gadījumos, kad mūsu uzņēmums apstrādā pretendentu datus, pamatojoties uz VDAR 6. panta 1. punkta f) apakšpunktu, mūsu leģitīmā interese ir piemērota personāla un speciālistu nodarbināšana.

## I. Tas, ka pastāv tiesības pieprasīt no pārziņa piekļuvi datu subjekta personas datiem un to labošanu vai dzēšanu, vai apstrādes ierobežošanu attiecībā uz datu subjektu un tiesības iebilst pret apstrādi, kā arī tiesības uz datu pārnesamību (VDAR 14. panta 2. punkta c) VDAR).

Visiem datu subjektiem ir šādas tiesības:

***Piekļuves tiesības***

Katram datu subjektam ir tiesības piekļūt personas datiem, kas uz viņu attiecas. Piekļuves tiesības attiecas uz visiem mūsu apstrādātajiem datiem. Šīs tiesības var izmantot viegli un ar saprātīgiem intervāliem, lai uzzinātu un pārbaudītu apstrādes likumību (VDAR 63. apsvērums). Šīs tiesības izriet no Regulas (EK) Nr. VDAR 15. Datu subjekts var sazināties ar mums, lai izmantotu piekļuves tiesības.

***Tiesības uz labošanu***

Saskaņā ar VDAR 16. panta 1. teikumu datu subjektam ir tiesības no pārziņa bez nepamatotas kavēšanās saņemt neprecīzu personas datu labošanu, kas uz viņu attiecas. Turklāt VDAR 16. panta 2. teikumā noteikts, ka datu subjektam, ņemot vērā apstrādes nolūkus, ir tiesības uz nepilnīgu personas datu papildināšanu, tostarp sniedzot papildu paziņojumu. Datu subjekts var sazināties ar mums, lai izmantotu tiesības uz labošanu.

***Tiesības uz dzēšanu (tiesības tikt aizmirstam)***

Turklāt datu subjektiem ir tiesības uz dzēšanu un aizmiršanu saskaņā ar Regulas (EK) Nr. 17 VDAR. Šīs tiesības var izmantot, sazinoties ar mums. Tomēr šajā brīdī vēlamies norādīt, ka šīs tiesības nav piemērojamas, ja apstrāde ir nepieciešama, lai izpildītu juridisku pienākumu, kas attiecas uz mūsu uzņēmumu, kā noteikts VDAR 17. panta 3. punkta b) apakšpunktā. Tas nozīmē, ka mēs varam apstiprināt pieteikumu par dzēšanu tikai pēc likumā noteiktā glabāšanas termiņa beigām.

***Tiesības uz apstrādes ierobežošanu***

Saskaņā ar VDAR 18. pantu jebkuram datu subjektam ir tiesības uz apstrādes ierobežošanu. Apstrādes ierobežošanu var pieprasīt, ja ir izpildīts viens no VDAR 18. panta 1. punkta a-d apakšpunktā minētajiem nosacījumiem. Datu subjekts var sazināties ar mums, lai izmantotu tiesības uz apstrādes ierobežošanu.

***Tiesības iebilst***

Turklāt saskaņā ar Regulas (EK) Nr. VDAR 21. pants garantē tiesības iebilst. Datu subjekts var sazināties ar mums, lai izmantotu tiesības iebilst.


© All rights reserved by Heiko Maniero.

***Tiesības uz datu pārnesamību***

Art. 20 VDAR datu subjektam piešķir tiesības uz datu pārnesamību. Saskaņā ar šo noteikumu datu subjektam saskaņā ar VDAR 20. panta 1. punkta a) un b) apakšpunktā paredzētajiem nosacījumiem ir tiesības saņemt personas datus, kas attiecas uz viņu un ko viņš ir sniedzis pārzinim, strukturētā, plaši izmantotā un mašīnlasāmā formātā, un tiesības nosūtīt šos datus citam pārzinim, netraucējot pārzinim, kuram personas dati ir sniegti. Datu subjekts var sazināties ar mums, lai izmantotu tiesības uz datu pārnesamību.

## J. Ja apstrāde pamatojas uz 6. panta 1. punkta a) apakšpunktu vai 9. panta 2. punkta a) apakšpunktu – tiesības jebkurā brīdī atsaukt piekrišanu, neietekmējot tādas apstrādes likumīgumu, kuras pamatā ir pirms atsaukuma sniegta piekrišana (VDAR 14. panta 2. punkta d) VDAR).

Ja personas datu apstrādes pamatā ir Regulas (EK) Nr. a panta 1. punkta a) apakšpunktu, kas ir gadījums, kad datu subjekts ir devis piekrišanu personas datu apstrādei vienam vai vairākiem konkrētiem nolūkiem, vai tā ir pamatota ar VDAR 9. panta 2. punkta a) apakšpunktu, kas reglamentē skaidru piekrišanu īpašu kategoriju personas datu apstrādei, datu subjektam saskaņā ar VDAR 7. panta 3. punkta 1. teikuma 1. teikumu ir tiesības jebkurā laikā atsaukt savu piekrišanu.

Piekrišanas atsaukšana neietekmē tās apstrādes likumību, kuras pamatā ir piekrišana pirms tās atsaukšanas, VDAR 7. panta 3. punkta 2. teikums. Piekrišanu atsaukt ir tikpat viegli kā dot piekrišanu, 1. pants. VDAR 7. panta 3. punkta 4. teikums. Tāpēc piekrišanas atsaukšana vienmēr var notikt tādā pašā veidā, kādā piekrišana ir dota, vai jebkurā citā veidā, ko datu subjekts uzskata par vienkāršāku. Mūsdienu informācijas sabiedrībā, iespējams, vienkāršākais veids, kā atsaukt piekrišanu, ir vienkāršs e-pasts. Ja datu subjekts vēlas atsaukt mums doto piekrišanu, pietiek ar vienkāršu e-pasta vēstuli. Datu subjekts var arī izvēlēties jebkuru citu veidu, kā paziņot mums par piekrišanas atsaukšanu.

## K. Tiesības iesniegt sūdzību uzraudzības iestādei (VDAR 14. panta 2. punkta e) VDAR, 77. panta 1. punkts)

Mums kā pārzinim ir pienākums informēt datu subjektu par tiesībām iesniegt sūdzību uzraudzības iestādei, kā noteikts VDAR 14. panta 2. punkta e) apakšpunktā. Tiesības iesniegt sūdzību uzraudzības iestādei reglamentē VDAR 77. panta 1. punkts. Saskaņā ar šo noteikumu, neskarot nekādus citus administratīvos vai tiesiskās aizsardzības līdzekļus, katram datu subjektam ir tiesības iesniegt sūdzību uzraudzības iestādei, jo īpaši dalībvalstī, kurā ir viņa pastāvīgā dzīvesvieta, darbavieta vai iespējamā pārkāpuma vieta, ja datu subjekts uzskata, ka ar viņu saistīto personas datu apstrāde pārkāpj Vispārīgo datu aizsardzības regulu. Tiesības iesniegt sūdzību uzraudzības iestādei Savienības tiesību aktos tika ierobežotas tikai tādā veidā, ka tās var izmantot tikai vienā uzraudzības iestādē (Vispārīgās datu aizsardzības regulas 141. apsvēruma 1. teikums). Šis noteikums ir paredzēts, lai izvairītos no tā paša


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

datu subjekta dubultām sūdzībām vienā un tajā pašā lietā. Tāpēc, ja datu subjekts vēlas iesniegt sūdzību par mums, mēs lūdzam vērsties tikai vienā uzraudzības iestādē.

## L. Informācija par to, no kāda avota personas dati ir iegūti, un – attiecīgā gadījumā – informācija par to, vai dati iegūti no publiski pieejamiem avotiem (VDAR 14. panta 2. punkta f) VDAR)

Principā personas datus vāc tieši no datu subjekta vai sadarbībā ar iestādi (piemēram, iegūstot datus no oficiāla reģistra). Citi dati par datu subjektiem tiek iegūti, nododot datus no grupas uzņēmumiem. Šīs vispārīgās informācijas kontekstā precīzu avotu, no kuriem iegūti personas dati, nosaukšana ir vai nu neiespējama, vai arī prasītu nesamērīgas pūles Regulas (EK) Nr. panta 5. punkta b) apakšpunktu VDAR. Principā mēs nevācam personas datus no publiski pieejamiem avotiem.

Jebkurš datu subjekts var jebkurā laikā sazināties ar mums, lai iegūtu sīkāku informāciju par precīziem personas datu avotiem, kas uz viņu attiecas. Ja personas datu izcelsmi datu subjektam nevar norādīt, jo ir izmantoti dažādi avoti, ir jāsniedz vispārīga informācija (VDAR 61. apsvēruma 4. teikums).

## M. Tas, ka pastāv automatizēta lēmumu pieņemšana, tostarp profilēšana, kas minēta 22. panta 1. un 4. punktā, un – vismaz minētajos gadījumos – jēgpilna informācija par tajā ietverto loģiku, kā arī šādas apstrādes nozīmīgumu un paredzamajām sekām attiecībā uz datu subjektu (VDAR 14. panta 2. punkta g) VDAR).

Kā atbildīgs uzņēmums mēs parasti neizmantojam automatizētu lēmumu pieņemšanu vai profilēšanu. Ja izņēmuma gadījumos mēs veicam automatizētu lēmumu pieņemšanu vai profilēšanu, mēs par to informēsim datu subjektu atsevišķi vai ar apakšsadaļas palīdzību mūsu privātuma politikā (mūsu tīmekļa vietnē). Šādā gadījumā piemēro šādus noteikumus:

Automatizēta lēmumu pieņemšana, tostarp profilēšana, var notikt, ja (1) tas ir nepieciešams, lai noslēgtu vai izpildītu līgumu starp datu subjektu un mums, vai (2) to atļauj Savienības vai dalībvalsts tiesību akti, kas uz mums attiecas un kas nosaka arī piemērotus pasākumus datu subjekta tiesību un brīvību un likumīgo interešu aizsardzībai, vai (3) tas ir pamatots ar datu subjekta skaidru piekrišanu.

Gadījumos, kas minēti VDAR 22. panta 2. punkta a) un c) apakšpunktā, mēs īstenojam piemērotus pasākumus, lai aizsargātu datu subjekta tiesības un brīvības un likumīgās intereses. Šādos gadījumos jums ir tiesības panākt pārziņa iejaukšanos, paust savu viedokli un apstrīdēt lēmumu.

Nozīmīga informācija par iesaistīto loģiku, kā arī par šādas apstrādes nozīmi un paredzamajām sekām datu subjektam ir izklāstīta mūsu privātuma politikā.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## III. EU-U.S. Data Privacy Framework (EU-U.S. DPF), UK Extension to the EU-U.S. DPF, Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF)

Ja mūsu organizācija ir sertificēts EU-U.S. Data Privacy Framework (EU-U.S. DPF) un/vai UK Extension to the EU-U.S. DPF un/vai Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF) dalībnieks, ir spēkā šādi noteikumi:

Mēs ievērojam EU-U.S. Data Privacy Framework (EU-U.S. DPF) un UK Extension to the EU-U.S. DPF, kā arī Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF), kā to ir noteikusi ASV Tirdzniecības departaments. Mūsu uzņēmums ir apliecinājis ASV Tirdzniecības departamentam, ka tas ievēro EU-U.S. Data Privacy Framework Principles (EU-U.S. DPF Principles) attiecībā uz personas datu apstrādi, ko tas saņem no Eiropas Savienības un Apvienotās Karalistes, pamatojoties uz EU-U.S. DPF un UK Extension to the EU-U.S. DPF. Mūsu uzņēmums ir apliecinājis ASV Tirdzniecības departamentam, ka tas ievēro Swiss-U.S. Data Privacy Framework Principles (Swiss-U.S. DPF Principles) attiecībā uz personas datu apstrādi, ko tas saņem no Šveices, pamatojoties uz Swiss-U.S. DPF. Gadījumā, ja pastāv pretrunas starp mūsu privātuma politikas noteikumiem un EU-U.S. DPF Principles un/vai Swiss-U.S. DPF Principles, noteicošie ir Principles.

Lai uzzinātu vairāk par Data Privacy Framework (DPF) programmu un apskatītu mūsu sertifikāciju, lūdzu, apmeklējiet https://www.dataprivacyframework.gov/.

Pārējās mūsu uzņēmuma ASV vienības vai meitasuzņēmumi, kas arī ievēro EU-U.S. DPF Principals, tostarp UK Extension to the EU-U.S. DPF un Swiss-U.S. DPF Principals, ja tādi ir, ir norādīti mūsu privātuma politikā.

Saskaņā ar EU-U.S. DPF un UK Extension to the EU-U.S. DPF, kā arī Swiss-U.S. DPF mūsu uzņēmums apņemas sadarboties ar ES datu aizsardzības iestāžu un Apvienotās Karalistes Information Commissioner's Office (ICO), kā arī Šveices Federālā datu aizsardzības un informācijas komisāra (EDÖB) izveidoto paneli un ievērot to ieteikumus attiecībā uz neatrisinātām sūdzībām par mūsu personas datu apstrādi, ko mēs saņemam, pamatojoties uz EU-U.S. DPF un UK Extension to the EU-U.S. DPF un Swiss-U.S. DPF.

Mēs informējam skartās personas par attiecīgajām Eiropas datu aizsardzības iestādēm, kas ir atbildīgas par sūdzību izskatīšanu par mūsu organizācijas personas datu apstrādi, šī pārredzamības dokumenta augšdaļā un par to, ka mēs piedāvājam skartajām personām atbilstošu un bezmaksas tiesisko aizsardzību.

Mēs informējam visas skartās personas, ka mūsu uzņēmums ir pakļauts Federal Trade Commission (FTC) izmeklēšanas un izpildes pilnvarām.

Skartajām personām ir noteiktos apstākļos iespēja izmantot saistošu šķīrējtiesu. Mūsu organizācija ir apņēmusies risināt prasības un ievērot noteikumus, kas izklāstīti DPF-Principals I pielikumā, ja skartā


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

persona ir pieprasījusi saistošu šķīrējtiesu, paziņojot par to mūsu organizācijai un ievērojot I pielikumā izklāstītos procedūras un noteikumus.

Ar šo mēs informējam visas skartās personas par mūsu organizācijas atbildību gadījumā, ja personas dati tiek nodoti trešajām personām.

Jautājumiem no skartajām personām vai datu aizsardzības uzraudzības iestādēm mēs esam norādījuši vietējos pārstāvjus, kas minēti šī pārredzamības dokumenta augšdaļā.

Mēs piedāvājam jums iespēju izvēlēties (Opt-out), vai jūsu personas dati (i) tiek nodoti trešajām personām vai (ii) tiek izmantoti mērķim, kas būtiski atšķiras no mērķa/mērķiem, kam tie sākotnēji tika savākti vai vēlāk jūsu apstiprināti. Skaidrs, labi redzams un viegli pieejams mehānisms, kā izmantot jūsu izvēli, ir sazināties ar mūsu datu aizsardzības speciālistu (DSB) pa e-pastu. Jums nav izvēles iespēju, un mēs neesam arī pienākuma to darīt, ja dati tiek nodoti trešajai pusei, kas darbojas kā aģents vai apstrādātājs mūsu vārdā un saskaņā ar mūsu norādījumiem. Tomēr mēs vienmēr slēdzam līgumu ar šādu aģentu vai apstrādātāju.

Attiecībā uz sensitīvajiem datiem (t.i., personas datiem, kas satur informāciju par veselības stāvokli, rasu vai etnisko izcelsmi, politiskajiem uzskatiem, reliģiskajiem vai filozofiskajiem uzskatiem, dalību arodbiedrībā vai informāciju par attiecīgās personas seksuālo dzīvi), mēs iegūstam jūsu skaidru piekrišanu (Opt-in), kad šie dati (i) tiek nodoti trešajām personām vai (ii) tiek izmantoti citam mērķim, nevis tam, kam tie sākotnēji tika savākti vai kam jūs vēlāk devāt piekrišanu, izvēloties Opt-in. Turklāt mēs visus personas datus, ko saņemam no trešajām personām, uzskatām par sensitīviem, ja trešā puse tos ir identificējusi un apstrādājusi kā tādus.

Mēs informējam jūs ar šo par prasību izpaust personas datus, reaģējot uz likumīgām iestāžu prasībām, tostarp izpildot nacionālās drošības vai tiesībaizsardzības prasības.

Nododot personas datus trešajai personai, kas darbojas kā pārzinis, mēs ievērojam Principals par paziņošanu un izvēli. Turklāt mēs slēdzam līgumu ar trešo personu, kas ir atbildīga par apstrādi, kurā paredzēts, ka šie dati drīkst tikt apstrādāti tikai ierobežotiem un noteiktiem mērķiem saskaņā ar jūsu sniegto piekrišanu un ka saņēmējam jānodrošina tāds pats aizsardzības līmenis kā DPF Principals un jāinformē mūs, ja tas konstatē, ka vairs nevar izpildīt šo pienākumu. Līgumā ir paredzēts, ka trešā persona, kas ir pārzinis, pārtrauc apstrādi vai veic citus piemērotus un atbilstošus pasākumus, lai novērstu situāciju, ja tiek izdarīts šāds secinājums.

Nododot personas datus trešajai personai, kas darbojas kā aģents vai apstrādātājs, (i) mēs nododam šos datus tikai ierobežotiem un noteiktiem mērķiem; (ii) mēs nodrošinām, ka aģents vai apstrādātājs ir pienākums nodrošināt vismaz tādu pašu datu aizsardzības līmeni, kādu pieprasa DPF-Principals; (iii) mēs veicam piemērotus un atbilstošus pasākumus, lai nodrošinātu, ka aģents vai apstrādātājs faktiski apstrādā pārsūtītos personas datus tādā veidā, kas atbilst mūsu saistībām saskaņā ar DPF-Principals; (iv) mēs pieprasām, lai aģents vai apstrādātājs informē mūsu organizāciju, ja tas konstatē, ka vairs nevar izpildīt pienākumu nodrošināt tādu pašu aizsardzības līmeni, kādu paredz DPF-Principals; (v) pēc šāda


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

paziņojuma, arī saskaņā ar (iv), mēs veicam piemērotus un atbilstošus pasākumus, lai pārtrauktu neatļautu apstrādi un novērstu situāciju; un (vi) pēc pieprasījuma mēs DPF Department sniedzam kopsavilkumu vai reprezentatīvu piemēru par atbilstošajiem datu aizsardzības noteikumiem no mūsu līguma ar šo aģentu.

Saskaņā ar EU-U.S. DPF un/vai UK Extension to the EU-U.S. DPF un/vai Swiss-U.S. DPF mūsu organizācija apņemas sadarboties ar ES datu aizsardzības iestāžu un Apvienotās Karalistes Information Commissioner's Office (ICO) vai Šveices Federālā datu aizsardzības un informācijas komisāra (EDÖB) izveidoto paneli un ievērot to ieteikumus attiecībā uz neatrisinātām sūdzībām par mūsu rīcību ar personāldatiem, ko mēs saņemam saistībā ar darba attiecībām, pamatojoties uz EU-U.S. DPF un UK Extension to the EU-U.S. DPF un Swiss-U.S. DPF.

Visiem datu subjektiem, kuri uz laiku atrodas Eiropas Savienībā (ES), Eiropas Ekonomikas zonā (EEZ) vai Apvienotajā Karalistē vai kuru domicils vai pastāvīgā dzīvesvieta ir tur, ir tiesības un datu subjekta tiesības, kas ir publicētas mūsu pārredzamības dokumentā un kas izriet arī no VDAR 15.-22. panta, tostarp tiesības piekļūt personas datiem. Mēs esam nodrošinājuši šīs informācijas pieejamību visās ES un EEZ valodās. Angļu valodas versija attiecas uz Apvienoto Karalisti.

Visiem datu subjektiem, kuri uz laiku uzturas Šveicē vai kuru dzīvesvieta vai pastāvīgā dzīvesvieta ir Šveicē, ir tiesības un datu subjekta tiesības saskaņā ar Šveices Datu aizsardzības likumu (DPA) un Šveices Datu aizsardzības regulu (DPR), kas ir publicētas mūsu pārredzamības dokumentā, tostarp tiesības piekļūt personas datiem. Mēs esam snieguši šo informāciju trīs Šveices oficiālajās valodās (vācu, itāļu un franču).


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

# LITHUANIAN: INFORMACIJA APIE ASMENS DUOMENŲ Tvarkymą (BDAR 13, 14 straipsniai)

Gerbiamasis pone arba ponia,

Kiekvieno asmens, su kuriuo mūsų įmonė palaiko sutartinius, ikisutartinius ar kitokius santykius, asmens duomenys turi būti ypatingai saugomi. Mūsų tikslas - išlaikyti aukštą duomenų apsaugos lygį. Todėl reguliāri tobuliname savo duomenų apsaugos ir duomenų saugumo koncepcijas.

Žinoma, mes laikomės įstatyminių nuostatų dėl duomenų apsaugos. Pagal BDAR 13, 14 straipsnius duomenų valdytojai, rinkdami asmens duomenis, laikosi konkrečių informavimo reikalavimų. Šiuo dokumentu šie įpareigojimai įvykdomi.

Teisinio reguliavimo terminologija yra sudėtinga. Deja, rengiant šį dokumentą nebuvo galima atsisakyti teisinių terminų vartojimo. Todėl norėtume pabrėžti, kad visais klausimais, susijusiais su šiuo dokumentu, vartojamais terminais ar formuluotėmis, visada galite kreiptis į mus.

## I. Informacija, kuri turi būti pateikta, kai asmens duomenys renkami iš duomenų subjekto (BDAR 13 straipsnis)

### A. Duomenų valdytojo ir, jeigu taikoma, duomenų valdytojo atstovo tapatybę ir kontaktinius duomenis (BDAR 13 straipsnio 1 dalies a punktas)

Žr. pirmiau

### B. Duomenų apsaugos pareigūno, jeigu taikoma, kontaktinius duomenis (BDAR 13 straipsnio 1 dalies b punktas)

Žr. pirmiau

### C. Duomenų tvarkymo tikslus, dėl kurių ketinama tvarkyti asmens duomenis, taip pat duomenų tvarkymo teisinį pagrindą (BDAR 13 straipsnio 1 dalies c punktas)

Asmens duomenų tvarkymo tikslas - tvarkyti visas operacijas, susijusias su duomenų valdytoju, klientais, potencialiais klientais, verslo partneriais arba kitais sutartiniais ar ikisutartiniais santykiais tarp išvardytų grupių (plačiąja prasme) arba duomenų valdytojo teisinėmis prievolėmis.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

Straipsnis. 6 straipsnio 1 dalies a punktas BDAR yra teisinis pagrindas duomenų tvarkymo operacijoms, dėl kurių gauname sutikimą dėl konkretaus duomenų tvarkymo tikslo. Jei asmens duomenis tvarkyti būtina sutarčiai, kurios šalis yra duomenų subjektas, vykdyti, kaip, pavyzdžiui, kai duomenų tvarkymo operacijos yra būtinos prekėms tiekti arba kitoms paslaugoms teikti, duomenų tvarkymas grindžiamas BDAR 6 straipsnio 1 dalies b punktu. Tas pats galioja ir tokioms duomenų tvarkymo operacijoms, kurios yra būtinos ikisutartinėms priemonėms atlikti, pavyzdžiui, užklausų apie mūsų produktus ar paslaugas atveju. Ar mūsų įmonei taikoma teisinė prievolė, pagal kurią būtina tvarkyti asmens duomenis, pavyzdžiui, siekiant įvykdyti mokestines prievoles, duomenų tvarkymas grindžiamas 6 straipsnio 1 dalimi. BDAR 6 straipsnio 1 dalies c punktu.

Retais atvejais asmens duomenis gali būti būtina tvarkyti siekiant apsaugoti gyvybiškai svarbius duomenų subjekto ar kito fizinio asmens interesus. Taip būtų, pavyzdžiui, jei lankytojas susižeistų mūsų įmonėje ir jo vardą, pavardę, amžių, sveikatos draudimo duomenis ar kitą gyvybiškai svarbią informaciją reikėtų perduoti gydytojui, ligoninei ar kitai trečiajai šaliai. Tuomet duomenų tvarkymas būtų grindžiamas 6 straipsnio 1 dalimi. BDAR 6 straipsnio 1 dalies d punktu.

Kai tvarkyti duomenis būtina siekiant atlikti užduotį, vykdomą viešojo intereso labui arba vykdant duomenų valdytojui pavestas viešosios valdžios funkcijas, teisinis pagrindas yra 6 straipsnio 1 dalimi. BDAR 6 straipsnio 1 dalies e punktu.

Galiausiai duomenų tvarkymo operacijos gali būti grindžiamos BDAR 6 straipsnio 1 dalies f punktu. Šis teisinis pagrindas naudojamas duomenų tvarkymo operacijoms, kurioms netaikomas nė vienas iš pirmiau minėtų teisinių pagrindų, jei tvarkyti duomenis būtina dėl mūsų įmonės arba trečiosios šalies siekiamų teisėtų interesų, išskyrus atvejus, kai prieš tokius interesus nusveria duomenų subjekto interesai arba pagrindinės teisės ir laisvės, dėl kurių būtina užtikrinti asmens duomenų apsaugą. Tokios duomenų tvarkymo operacijos yra ypač leidžiamos, nes jas konkrečiai paminėjo Europos teisės aktų leidėjas. Jis manė, kad teisėtas interesas gali būti preziumuojamas, jei duomenų subjektas yra duomenų valdytojo klientas (BDAR 47 konstatuojamosios dalies 2 sakinys).

## D. Kai duomenų tvarkymas atliekamas pagal 6 straipsnio 1 dalies f punktą, teisėtus duomenų valdytojo arba trečiosios šalies interesus (BDAR 13 straipsnio 1 dalies d punktas)

Kai asmens duomenys tvarkomi remiantis BDAR 6 straipsnio 1 dalies f punktu, mūsų teisėtas interesas yra vykdyti savo verslą, siekiant užtikrinti visų mūsų darbuotojų ir akcininkų gerovę.

## E. Jei yra, asmens duomenų gavėjus arba asmens duomenų gavėjų kategorijas (BDAR 13 straipsnio 1 dalies e punktas)


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

Valdžios institucijos

Išorės įstaigos

Kitos išorės įstaigos

Vidinis apdorojimas

Grupės vidaus apdorojimas

Kitos įstaigos

Mūsų duomenų tvarkytojų ir duomenų gavėjų trečiosiose šalyse bei, jei taikoma, tarptautinių organizacijų sąrašas skelbiamas mūsų interneto svetainėje arba jo galima nemokamai paprašyti iš mūsų. Norėdami paprašyti šio sąrašo, kreipkitės į mūsų duomenų apsaugos pareigūną.

## F. Kai taikoma, apie duomenų valdytojo ketinimą asmens duomenis perduoti į trečiąją valstybę arba tarptautinei organizacijai ir Komisijos sprendimo dėl tinkamumo buvimą ar nebuvimą, arba 46 ar 47 straipsniuose arba 49 straipsnio 1 dalies antroje pastraipoje nurodytų perdavimų atveju – tinkamas arba pritaikytas apsaugos priemones ir būdus, kaip gauti jų kopiją arba kur suteikiama galimybė su jais susipažinti (BDAR 13 straipsnio 1 dalies f punktas, 46 straipsnio 1 dalis, 46 straipsnio 2 dalies c punktas)

Visos mūsų grupei priklausančios įmonės ir filialai (toliau - grupės įmonės), kurių verslo vieta arba biuras yra trečiojoje šalyje, gali būti asmens duomenų gavėjai. Visų grupės įmonių arba gavėjų sąrašo galite paprašyti iš mūsų.

Pagal BDAR 46 straipsnio 1 dalį duomenų valdytojas arba duomenų tvarkytojas gali perduoti asmens duomenis į trečiąją šalį tik tuo atveju, jei duomenų valdytojas arba duomenų tvarkytojas yra numatęs tinkamas apsaugos priemones ir su sąlyga, kad duomenų subjektai gali naudotis įgyvendinamomis duomenų subjekto teisėmis ir veiksmingomis teisių gynimo priemonėmis. Tinkamos apsaugos priemonės gali būti numatytos nereikalaujant jokio konkretaus priežiūros institucijos leidimo, taikant standartines sutarčių sąlygas, BDAR 46 straipsnio 2 dalies c punktas.

Prieš pirmą kartą perduodant asmens duomenis su visais gavėjais iš trečiųjų šalių susitariama dėl standartinių Europos Sąjungos sutarčių sąlygų arba kitų tinkamų apsaugos priemonių. Todėl užtikrinama, kad duomenų subjektams būtų užtikrintos tinkamos apsaugos priemonės, įgyvendinamos duomenų subjekto teisės ir veiksmingos teisinės gynybos priemonės. Kiekvienas duomenų subjektas gali iš mūsų gauti standartinių sutarties sąlygų kopiją. Su standartinėmis sutarčių sąlygomis taip pat galima susipažinti Europos Sąjungos oficialiajame leidinyje.

Bendrojo duomenų apsaugos reglamento (BDAR) 45 straipsnio 3 dalimi Europos Komisijai suteikiami įgaliojimai įgyvendinimo aktu nuspręsti, kad ES nepriklausanti šalis užtikrina tinkamą apsaugos lygį. Tai


© All rights reserved by Heiko Maniero.

reiškia, kad asmens duomenų apsaugos lygis yra iš esmės lygiavertis apsaugos lygiui ES. Sprendimų dėl tinkamumo poveikis yra tas, kad asmens duomenys gali laisvai ir be jokių papildomų kliūčių judėti iš ES (ir Norvegijos, Lichtenšteino bei Islandijos) į trečiąją šalį. Panašios taisyklės taikomos Jungtinei Karalystei, Šveicarijai ir kai kurioms kitoms šalims.

Jei Europos Komisija arba kitos šalies vyriausybė nusprendė, kad trečioji šalis užtikrina tinkamą apsaugos lygį, ir yra galiojanti sistema (pvz., EU-U.S. Data Privacy Framework, Swiss-U.S. Data Privacy Framework, UK Extension to the EU-U.S. Data Privacy Framework), visi mūsų atliekami duomenų perdavimai tokių sistemų nariams (pvz., savarankiškai sertifikuotiems subjektams) grindžiami tik to subjekto naryste atitinkamoje sistemoje. Jei mes arba vienas iš mūsų grupės subjektų yra tokios sistemos narys, visi duomenų perdavimai mums arba mūsų grupės subjektui yra grindžiami tik šio subjekto naryste tokioje sistemoje.

Bet kuris duomenų subjektas gali iš mūsų gauti rėmų kopiją. Be to, su šiomis sistemomis taip pat galima susipažinti Europos Sąjungos oficialiajame leidinyje, paskelbtoje teisinėje medžiagoje arba priežiūros institucijų ar kitų kompetentingų institucijų ar įstaigų interneto svetainėse.

## G. Asmens duomenų saugojimo laikotarpį arba, jei tai neįmanoma, kriterijus, taikomus tam laikotarpiui nustatyti (BDAR 13 straipsnio 2 dalies a punktas)

Kriterijai, kuriais remiantis nustatomas asmens duomenų saugojimo laikotarpis, yra atitinkamas teisės aktuose nustatytas saugojimo laikotarpis. Pasibaigus šiam laikotarpiui, atitinkami duomenys įprastai ištrinami, jei jie nebereikalingi sutarčiai įvykdyti arba sutarčiai inicijuoti.

Jei teisės aktais nustatytas saugojimo laikotarpis nenustatytas, kriterijus yra sutartinis arba vidinis saugojimo laikotarpis.

## H. Teisę prašyti, kad duomenų valdytojas leistų susipažinti su duomenų subjekto asmens duomenimis ir juos ištaisytų arba ištrintų, arba apribotų duomenų tvarkymą, arba teisę nesutikti, kad duomenys būtų tvarkomi, taip pat teisę į duomenų perkeliamumą (BDAR 13 straipsnio 2 dalies b punktas) egzistavimas

Visi duomenų subjektai turi šias teises:

***Teisė į prieigą***

Kiekvienas duomenų subjektas turi teisę susipažinti su savo asmens duomenimis. Teisė susipažinti taikoma visiems mūsų tvarkomiems duomenims. Šia teise galima naudotis lengvai ir pagrįstais laiko tarpais, kad būtų galima sužinoti ir patikrinti duomenų tvarkymo teisėtumą (BDAR 63 konstatuojamoji dalis). Ši teisė išplaukia iš Europos Sąjungos teisės aktų rinkinio (toliau - ES teisės aktai) 3 straipsnio 2 dalies. 15 BDAR. Duomenų subjektas, norėdamas pasinaudoti prieigos teise, gali kreiptis į mus.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

***Teisė į ištaisymą***

Pagal BDAR 16 straipsnio 1 sakinį duomenų subjektas turi teisę iš duomenų valdytojo nepagrįstai nedelsdamas reikalauti, kad duomenų valdytojas ištaisytų netikslius jo asmens duomenis. Be to, BDAR 16 straipsnio 2 sakinyje numatyta, kad duomenų subjektas, atsižvelgiant į duomenų tvarkymo tikslus, turi teisę reikalauti, kad neišsamūs asmens duomenys būtų papildyti, be kita ko, pateikiant papildomą pareiškimą. Duomenų subjektas gali kreiptis į mus, kad pasinaudotų teise ištaisyti duomenis.

***Teisė į ištrynimą (teisė būti pamirštam)***

Be to, duomenų subjektai turi teisę į ištrynimą ir teisę būti pamiršti pagal Reglamento (EB) Nr. 17 BDAR. Šia teise taip pat galima pasinaudoti kreipiantis į mus. Tačiau šioje vietoje norėtume atkreipti dėmesį, kad ši teisė netaikoma, jei tvarkyti duomenis būtina, kad būtų įvykdyta teisinė prievolė, kuri taikoma mūsų įmonei, BDAR 17 straipsnio 3 dalies b punktas. Tai reiškia, kad prašymą ištrinti duomenis galime patenkinti tik pasibaigus teisės aktuose nustatytam saugojimo laikotarpiui.

***Teisė apriboti duomenų tvarkymą***

Pagal BDAR 18 straipsnį bet kuris duomenų subjektas turi teisę apriboti duomenų tvarkymą. Apriboti duomenų tvarkymą galima reikalauti, jei tenkinama viena iš BDAR 18 straipsnio 1 dalies a-d punktuose nustatytų sąlygų. Duomenų subjektas gali susisiekti su mumis, kad pasinaudotų teise apriboti duomenų tvarkymą.

***Teisė prieštarauti***

Be to, CK 6.2 str. 21 BDAR garantuojama teisė nesutikti. Duomenų subjektas gali susisiekti su mumis, kad pasinaudotų teise nesutikti.

***Teisė į duomenų perkeliamumą***

Straipsnis. 20 BDAR suteikia duomenų subjektui teisę į duomenų perkeliamumą. Pagal šią nuostatą duomenų subjektas BDAR 20 straipsnio 1 dalies a ir b punktuose nustatytomis sąlygomis turi teisę gauti su juo susijusius asmens duomenis, kuriuos jis pateikė duomenų valdytojui, susistemintu, įprastai naudojamu ir kompiuterio skaitomu formatu ir turi teisę perduoti tuos duomenis kitam duomenų valdytojui netrukdomas duomenų valdytojo, kuriam asmens duomenys buvo pateikti. Duomenų subjektas gali susisiekti su mumis, kad pasinaudotų teise į duomenų perkeliamumą.

## I. Kai duomenų tvarkymas grindžiamas 6 straipsnio 1 dalies a punktu arba 9 straipsnio 2 dalies a punktu, teisę bet kuriuo metu atšaukti sutikimą, nedarant poveikio sutikimu grindžiamo duomenų tvarkymo iki sutikimo atšaukimo teisėtumui (BDAR 13 straipsnio 2 dalies c punktas)

Jei asmens duomenų tvarkymas grindžiamas CK 2.5 str. 6 straipsnio 1 dalies a punktu, t. y. jei duomenų subjektas davė sutikimą tvarkyti asmens duomenis vienu ar keliais konkrečiais tikslais, arba yra grindžiamas BDAR 9 straipsnio 2 dalies a punktu, kuris reglamentuoja aiškų sutikimą tvarkyti specialių


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

kategorijų asmens duomenis, duomenų subjektas pagal BDAR 7 straipsnio 3 dalies 1 sakinį turi teisę bet kuriuo metu atšaukti savo sutikimą.

Sutikimo atšaukimas neturi įtakos duomenų tvarkymo, pagrįsto sutikimu prieš jo atšaukimą, teisėtumui, BDAR 7 straipsnio 3 dalies 2 sakinys. Atšaukti sutikimą turi būti taip pat paprasta, kaip ir duoti sutikimą, 3 straipsnis. BDAR 7 straipsnio 3 dalies 4 sakinys. Todėl atšaukti sutikimą visada galima tuo pačiu būdu, kuriuo buvo duotas sutikimas, arba bet kuriuo kitu būdu, kurį duomenų subjektas laiko paprastesniu. Šiuolaikinėje informacinėje visuomenėje tikriausiai paprasčiausias būdas atšaukti sutikimą yra paprastas elektroninis laiškas. Jei duomenų subjektas nori atšaukti mums duotą sutikimą, pakanka mums išsiųsti paprastą elektroninį laišką. Arba duomenų subjektas gali pasirinkti bet kokį kitą būdą, kuriuo jis mums praneša apie savo sutikimo atšaukimą.

## J. Teisę pateikti skundą priežiūros institucijai (Bendrojo duomenų apsaugos reglamento 13 straipsnio 2 dalies d punktas, 77 straipsnio 1 dalis)

Kaip duomenų valdytojas, privalome pranešti duomenų subjektui apie teisę pateikti skundą priežiūros institucijai, BDAR 13 straipsnio 2 dalies d punktas. Teisė pateikti skundą priežiūros institucijai reglamentuojama BDAR 77 straipsnio 1 dalyje. Pagal šią nuostatą, nepažeidžiant jokių kitų administracinių ar teisminių teisių gynimo priemonių, kiekvienas duomenų subjektas turi teisę pateikti skundą priežiūros institucijai, visų pirma valstybėje narėje, kurioje yra jo nuolatinė gyvenamoji vieta, darbo vieta arba įtariamo pažeidimo vieta, jeigu duomenų subjektas mano, kad su juo susijusių asmens duomenų tvarkymas pažeidžia Bendrąjį duomenų apsaugos reglamentą. Teisė pateikti skundą priežiūros institucijai Sąjungos teisėje buvo apribota tik taip, kad ja galima pasinaudoti tik vienoje priežiūros institucijoje (Bendrojo duomenų apsaugos reglamento 141 konstatuojamosios dalies 1 sakinys). Šia taisykle siekiama išvengti dvigubų to paties duomenų subjekto skundų tuo pačiu klausimu. Todėl, jei duomenų subjektas nori pateikti skundą dėl mūsų, prašome kreiptis tik į vieną priežiūros instituciją.

## K. Tai, ar asmens duomenų pateikimas yra teisės aktais arba sutartyje numatytas reikalavimas, ar reikalavimas, kurį būtina įvykdyti norint sudaryti sutartį, taip pat tai, ar duomenų subjektas privalo pateikti asmens duomenis, ir informaciją apie galimas tokių duomenų nepateikimo pasekmes (BDAR 13 straipsnio 2 dalies e punktas)

Paaiškiname, kad asmens duomenų teikimo iš dalies reikalaujama pagal įstatymus (pvz., mokesčių teisės aktus) arba tai gali būti susiję su sutartinėmis nuostatomis (pvz., informacija apie sutarties partnerį).

Kartais, norint sudaryti sutartį, gali prireikti, kad duomenų subjektas pateiktų mums asmens duomenis, kuriuos vėliau turime tvarkyti. Pavyzdžiui, duomenų subjektas privalo mums pateikti asmens duomenis, kai mūsų įmonė su juo pasirašo sutartį. Nepateikus asmens duomenų, sutartis su duomenų subjektu negalėtų būti sudaryta.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

Prieš duomenų subjektui pateikiant asmens duomenis, duomenų subjektas turi su mumis susisiekti. Duomenų subjektui paaiškiname, ar asmens duomenis pateikti reikalaujama pagal įstatymą ar sutartį, ar jie būtini sutarčiai sudaryti, ar yra prievolė pateikti asmens duomenis ir kokios bus asmens duomenų nepateikimo pasekmės.

### L. Tai, kad esama 22 straipsnio 1 ir 4 dalyse nurodyto automatizuoto sprendimų priėmimo, įskaitant profiliavimą, ir, bent tais atvejais, prasmingą informaciją apie loginį jo pagrindimą, taip pat tokio duomenų tvarkymo reikšmę ir numatomas pasekmes duomenų subjektui (BDAR 13 straipsnio 2 dalies f punktas)

Būdami atsakinga įmonė, paprastai nenaudojame automatizuoto sprendimų priėmimo ar profiliavimo. Jei išimtiniais atvejais vykdome automatizuotą sprendimų priėmimą ar profiliavimą, informuosime duomenų subjektą atskirai arba savo privatumo politikos (mūsų interneto svetainėje) poskyryje. Šiuo atveju taikoma toliau nurodyta tvarka:

Automatinis sprendimų priėmimas, įskaitant profiliavimą, gali būti vykdomas, jei: 1) tai būtina duomenų subjekto ir mūsų sutarčiai sudaryti arba vykdyti; arba 2) tai leidžiama pagal Sąjungos arba valstybės narės teisę, kuri mums taikoma ir kurioje taip pat nustatytos tinkamos priemonės duomenų subjekto teisėms ir laisvėms bei teisėtiems interesams apsaugoti; arba 3) tai grindžiama aiškiu duomenų subjekto sutikimu.

BDAR 22 straipsnio 2 dalies a ir c punktuose nurodytais atvejais įgyvendiname tinkamas priemones duomenų subjekto teisėms ir laisvėms bei teisėtiems interesams apsaugoti. Tokiais atvejais turite teisę reikalauti, kad duomenų valdytojas imtųsi žmogiškųjų veiksmų, pareikšti savo nuomonę ir užginčyti sprendimą.

Reikšminga informacija apie susijusią logiką, taip pat tokio duomenų tvarkymo reikšmę ir numatomus padarinius duomenų subjektui pateikiama mūsų privatumo politikoje.

## II. Informacija, kuri turi būti pateikta, kai asmens duomenys yra gauti ne iš duomenų subjekto (BDAR 14 straipsnis)

### A. Duomenų valdytojo ir duomenų valdytojo atstovo, jei taikoma, tapatybę ir kontaktinius duomenis (BDAR 14 straipsnio 1 dalies a punktas)

Žr. pirmiau


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## B. Duomenų apsaugos pareigūno, jei taikoma, kontaktinius duomenis (BDAR 14 straipsnio 1 dalies b punktas)

Žr. pirmiau

## C. Duomenų tvarkymo tikslus, kuriais ketinama tvarkyti asmens duomenis, taip pat duomenų tvarkymo teisinį pagrindą (BDAR 14 straipsnio 1 dalies c punktas)

Asmens duomenų tvarkymo tikslas - tvarkyti visas operacijas, susijusias su duomenų valdytoju, klientais, potencialiais klientais, verslo partneriais arba kitais sutartiniais ar ikisutartiniais santykiais tarp išvardytų grupių (plačiąja prasme) arba duomenų valdytojo teisinėmis prievolėmis.

Jei asmens duomenis tvarkyti būtina, kad būtų įvykdyta sutartis, kurios šalis yra duomenų subjektas, pavyzdžiui, kai duomenų tvarkymo operacijos yra būtinos prekėms tiekti arba kitoms paslaugoms teikti, duomenų tvarkymas grindžiamas BDAR 6 straipsnio 1 dalies b punktu. Tas pats galioja ir tokioms duomenų tvarkymo operacijoms, kurios yra būtinos ikisutartinėms priemonėms atlikti, pavyzdžiui, užklausų apie mūsų produktus ar paslaugas atveju. Ar mūsų įmonei taikoma teisinė prievolė, pagal kurią būtina tvarkyti asmens duomenis, pavyzdžiui, siekiant įvykdyti mokestines prievoles, duomenų tvarkymas grindžiamas 6 straipsnio 1 dalimi. BDAR 6 straipsnio 1 dalies c punktu.

Retais atvejais asmens duomenis gali būti būtina tvarkyti siekiant apsaugoti gyvybiškai svarbius duomenų subjekto ar kito fizinio asmens interesus. Taip būtų, pavyzdžiui, jei lankytojas susižeistų mūsų įmonėje ir jo vardą, pavardę, amžių, sveikatos draudimo duomenis ar kitą gyvybiškai svarbią informaciją reikėtų perduoti gydytojui, ligoninei ar kitai trečiajai šaliai. Tuomet duomenų tvarkymas būtų grindžiamas CK 6.5 str. BDAR 6 straipsnio 1 dalies d punktu.

Kai tvarkyti duomenis būtina siekiant atlikti užduotį, vykdomą viešojo intereso labui arba vykdant duomenų valdytojui pavestas viešosios valdžios funkcijas, teisinis pagrindas yra 6 straipsnio 1 dalimi. BDAR 6 straipsnio 1 dalies e punktu.

Galiausiai duomenų tvarkymo operacijos gali būti grindžiamos BDAR 6 straipsnio 1 dalies f punktu. Šis teisinis pagrindas naudojamas duomenų tvarkymo operacijoms, kurioms netaikomas nė vienas iš pirmiau minėtų teisinių pagrindų, jei tvarkyti duomenis būtina dėl mūsų įmonės arba trečiosios šalies siekiamų teisėtų interesų, išskyrus atvejus, kai prieš tokius interesus nusveria duomenų subjekto interesai arba pagrindinės teisės ir laisvės, dėl kurių būtina užtikrinti asmens duomenų apsaugą. Tokios duomenų tvarkymo operacijos yra ypač leidžiamos, nes jas konkrečiai paminėjo Europos teisės aktų leidėjas. Jis manė, kad teisėtas interesas gali būti preziumuojamas, jei duomenų subjektas yra duomenų valdytojo klientas (BDAR 47 konstatuojamosios dalies 2 sakinys).


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## D. Atitinkamų asmens duomenų kategorijas (BDAR 14 straipsnio 1 dalies d punktas)

Klientų duomenys

Potencialių klientų duomenys

Darbuotojų duomenys

Tiekėjų duomenys

## E. Jei jos yra, asmens duomenų gavėjus arba asmens duomenų gavėjų kategorijas (BDAR 14 straipsnio 1 dalies e punktas)

Valdžios institucijos

Išorės įstaigos

Kitos išorės įstaigos

Vidinis apdorojimas

Grupės vidaus apdorojimas

Kitos įstaigos

Mūsų duomenų tvarkytojų ir duomenų gavėjų trečiosiose šalyse bei, jei taikoma, tarptautinių organizacijų sąrašas skelbiamas mūsų interneto svetainėje arba jo galima nemokamai paprašyti iš mūsų. Norėdami paprašyti šio sąrašo, kreipkitės į mūsų duomenų apsaugos pareigūną.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## F. Kai taikoma, apie duomenų valdytojo ketinimą asmens duomenis perduoti gavėjui trečiojoje valstybėje arba tarptautinei organizacijai ir Komisijos sprendimo dėl tinkamumo buvimą ar nebuvimą, o 46 ar 47 straipsniuose arba 49 straipsnio 1 dalies antroje pastraipoje nurodytų perdavimų atveju – tinkamas arba pritaikytas apsaugos priemones ir būdus, kaip gauti jų kopiją arba kur suteikiama galimybė su jais susipažinti (BDAR 14 straipsnio 1 dalies f punktas, 46 straipsnio 1 dalis, 46 straipsnio 2 dalies c punktas)

Visos mūsų grupei priklausančios įmonės ir filialai (toliau - grupės įmonės), kurių verslo vieta arba biuras yra trečiojoje šalyje, gali būti asmens duomenų gavėjai. Visų grupės įmonių sąrašo galite paprašyti iš mūsų.

Pagal BDAR 46 straipsnio 1 dalį duomenų valdytojas arba duomenų tvarkytojas gali perduoti asmens duomenis į trečiąją šalį tik tuo atveju, jei duomenų valdytojas arba duomenų tvarkytojas yra numatęs tinkamas apsaugos priemones ir su sąlyga, kad duomenų subjektai gali naudotis įgyvendinamomis duomenų subjekto teisėmis ir veiksmingomis teisių gynimo priemonėmis. Tinkamos apsaugos priemonės gali būti numatytos nereikalaujant jokio konkretaus priežiūros institucijos leidimo, naudojant standartines duomenų apsaugos sąlygas, BDAR 46 straipsnio 2 dalies c punktas.

Prieš pirmą kartą perduodant asmens duomenis su visais gavėjais iš trečiųjų šalių susitariama dėl standartinių Europos Sąjungos sutarčių sąlygų arba kitų tinkamų apsaugos priemonių. Todėl užtikrinama, kad duomenų subjektams būtų užtikrintos tinkamos apsaugos priemonės, įgyvendinamos duomenų subjekto teisės ir veiksmingos teisinės gynybos priemonės. Kiekvienas duomenų subjektas iš mūsų gali gauti standartinių sutarties sąlygų kopiją. Su standartinėmis sutarčių sąlygomis taip pat galima susipažinti Europos Sąjungos oficialiajame leidinyje.

Bendrojo duomenų apsaugos reglamento (BDAR) 45 straipsnio 3 dalimi Europos Komisijai suteikiami įgaliojimai įgyvendinimo aktu nuspręsti, kad ES nepriklausanti šalis užtikrina tinkamą apsaugos lygį. Tai reiškia, kad asmens duomenų apsaugos lygis yra iš esmės lygiavertis apsaugos lygiui ES. Sprendimų dėl tinkamumo poveikis yra tas, kad asmens duomenys gali laisvai ir be jokių papildomų kliūčių judėti iš ES (ir Norvegijos, Lichtenšteino bei Islandijos) į trečiąją šalį. Panašios taisyklės taikomos Jungtinei Karalystei, Šveicarijai ir kai kurioms kitoms šalims.

Jei Europos Komisija arba kitos šalies vyriausybė nusprendė, kad trečioji šalis užtikrina tinkamą apsaugos lygį, ir yra galiojanti sistema (pvz., EU-U.S. Data Privacy Framework, Swiss-U.S. Data Privacy Framework, UK Extension to the EU-U.S. Data Privacy Framework), visi mūsų atliekami duomenų perdavimai tokių sistemų nariams (pvz., savarankiškai sertifikuotiems subjektams) grindžiami tik to subjekto naryste atitinkamoje sistemoje. Jei mes arba vienas iš mūsų grupės subjektų yra tokios sistemos narys, visi duomenų perdavimai mums arba mūsų grupės subjektui yra grindžiami tik šio subjekto naryste tokioje sistemoje.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

Bet kuris duomenų subjektas gali iš mūsų gauti rėmų kopiją. Be to, su šiomis sistemomis taip pat galima susipažinti Europos Sąjungos oficialiajame leidinyje, paskelbtoje teisinėje medžiagoje arba priežiūros institucijų ar kitų kompetentingų institucijų ar įstaigų interneto svetainėse.

## G. Asmens duomenų saugojimo laikotarpį arba, jei tai neįmanoma, kriterijus, taikomus tam laikotarpiui nustatyti (BDAR 14 straipsnio 2 dalies a punktas)

Kriterijai, kuriais remiantis nustatomas asmens duomenų saugojimo laikotarpis, yra atitinkamas teisės aktuose nustatytas saugojimo laikotarpis. Pasibaigus šiam laikotarpiui, atitinkami duomenys įprastai ištrinami, jei jie nebereikalingi sutarčiai įvykdyti arba sutarčiai inicijuoti.

Jei teisės aktais nustatytas saugojimo laikotarpis nenustatytas, kriterijus yra sutartinis arba vidinis saugojimo laikotarpis.

## H. Kai duomenų tvarkymas atliekamas pagal 6 straipsnio 1 dalies f punktą, teisėtus duomenų valdytojo arba trečiosios šalies interesus (BDAR 14 straipsnio 2 dalies b punktas)

Pagal BDAR 6 straipsnio 1 dalies f punktą duomenų tvarkymas yra teisėtas tik tuo atveju, jei duomenų tvarkymas yra būtinas duomenų valdytojo arba trečiosios šalies teisėtų interesų, kurių siekia duomenų valdytojas arba trečioji šalis, tikslais, išskyrus atvejus, kai už tokius interesus yra viršesni duomenų subjekto interesai arba pagrindinės teisės ir laisvės, dėl kurių būtina užtikrinti asmens duomenų apsaugą. Pagal BDAR 47 konstatuojamosios dalies 2 sakinį teisėtas interesas gali egzistuoti, kai duomenų subjektą ir duomenų valdytoją sieja atitinkami ir tinkami santykiai, pavyzdžiui, kai duomenų subjektas yra duomenų valdytojo klientas. Visais atvejais, kai mūsų įmonė tvarko asmens duomenis remdamasi BDAR 6 straipsnio 1 dalies f punktu, mūsų teisėtas interesas yra vykdyti verslą visų darbuotojų ir akcininkų gerovės labui.

## I. Teisę prašyti, kad duomenų valdytojas leistų susipažinti su duomenų subjekto asmens duomenimis ir juos ištaisytų arba ištrintų, arba apribotų duomenų tvarkymą, ir teisę nesutikti, kad duomenys būtų tvarkomi, taip pat teisę į į duomenų perkeliamumą (BDAR 14 straipsnio 2 dalies c punktas) egzistavimas

Visi duomenų subjektai turi šias teises:

***Teisė į prieigą***

Kiekvienas duomenų subjektas turi teisę susipažinti su savo asmens duomenimis. Teisė susipažinti taikoma visiems mūsų tvarkomiems duomenims. Šia teise galima naudotis lengvai ir pagrįstais laiko tarpais, kad būtų galima sužinoti ir patikrinti duomenų tvarkymo teisėtumą (BDAR 63 konstatuojamoji


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

dalis). Ši teisė išplaukia iš Europos Sąjungos teisės aktų rinkinio (toliau - ES teisės aktai) 3 straipsnio 2 dalies. 15 BDAR. Duomenų subjektas, norėdamas pasinaudoti prieigos teise, gali kreiptis į mus.

***Teisė į ištaisymą***

Pagal BDAR 16 straipsnio 1 sakinį duomenų subjektas turi teisę iš duomenų valdytojo nepagrįstai nedelsdamas reikalauti, kad duomenų valdytojas ištaisytų netikslius jo asmens duomenis. Be to, BDAR 16 straipsnio 2 sakinyje numatyta, kad duomenų subjektas, atsižvelgiant į duomenų tvarkymo tikslus, turi teisę reikalauti, kad neišsamūs asmens duomenys būtų papildyti, be kita ko, pateikiant papildomą pareiškimą. Duomenų subjektas gali kreiptis į mus, kad pasinaudotų teise ištaisyti duomenis.

***Teisė į ištrynimą (teisė būti pamirštam)***

Be to, duomenų subjektai turi teisę į duomenų ištrynimą ir teisę būti pamirštiems pagal Reglamento (EB) Nr. 17 BDAR. Šia teise taip pat galima pasinaudoti kreipiantis į mus. Tačiau šioje vietoje norėtume atkreipti dėmesį, kad ši teisė netaikoma, jei tvarkyti duomenis būtina, kad būtų įvykdyta teisinė prievolė, kuri taikoma mūsų įmonei, BDAR 17 straipsnio 3 dalies b punktas. Tai reiškia, kad prašymą ištrinti duomenis galime patenkinti tik pasibaigus teisės aktuose nustatytam saugojimo laikotarpiui.

***Teisė apriboti duomenų tvarkymą***

Pagal BDAR 18 straipsnį bet kuris duomenų subjektas turi teisę apriboti duomenų tvarkymą. Apriboti duomenų tvarkymą galima reikalauti, jei tenkinama viena iš BDAR 18 straipsnio 1 dalies a-d punktuose nustatytų sąlygų. Duomenų subjektas gali susisiekti su mumis, kad pasinaudotų teise apriboti duomenų tvarkymą.

***Teisė prieštarauti***

Be to, CK 6.2 str. 21 BDAR garantuojama teisė nesutikti. Duomenų subjektas gali susisiekti su mumis, kad pasinaudotų teise nesutikti.

***Teisė į duomenų perkeliamumą***

Straipsnis. 20 BDAR suteikia duomenų subjektui teisę į duomenų perkeliamumą. Pagal šią nuostatą duomenų subjektas BDAR 20 straipsnio 1 dalies a ir b punktuose nustatytomis sąlygomis turi teisę gauti su juo susijusius asmens duomenis, kuriuos jis pateikė duomenų valdytojui, susistemintu, įprastai naudojamu ir kompiuterio skaitomu formatu ir turi teisę perduoti tuos duomenis kitam duomenų valdytojui netrukdomas duomenų valdytojo, kuriam asmens duomenys buvo pateikti. Duomenų subjektas gali susisiekti su mumis, kad pasinaudotų teise į duomenų perkeliamumą.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## J. Kai duomenų tvarkymas grindžiamas 6 straipsnio 1 dalies a punktu arba 9 straipsnio 2 dalies a punktu, teisę bet kuriuo metu atšaukti sutikimą, nedarant poveikio sutikimu grindžiamo duomenų tvarkymo iki sutikimo atšaukimo teisėtumui (BDAR 14 straipsnio 2 dalies d punktas)

Jei asmens duomenų tvarkymas grindžiamas CK 2.5 str. 6 straipsnio 1 dalies a punktu, t. y. jei duomenų subjektas davė sutikimą tvarkyti asmens duomenis vienu ar keliais konkrečiais tikslais, arba yra grindžiamas BDAR 9 straipsnio 2 dalies a punktu, kuris reglamentuoja aiškų sutikimą tvarkyti specialių kategorijų asmens duomenis, duomenų subjektas pagal BDAR 7 straipsnio 3 dalies 1 sakinį turi teisę bet kuriuo metu atšaukti savo sutikimą.

Sutikimo atšaukimas neturi įtakos duomenų tvarkymo, pagrįsto sutikimu prieš jo atšaukimą, teisėtumui, BDAR 7 straipsnio 3 dalies 2 sakinys. Atšaukti sutikimą turi būti taip pat paprasta, kaip ir duoti sutikimą, 1 straipsnis. BDAR 7 straipsnio 3 dalies 4 sakinys. Todėl atšaukti sutikimą visada galima tuo pačiu būdu, kuriuo buvo duotas sutikimas, arba bet kuriuo kitu būdu, kurį duomenų subjektas laiko paprastesniu. Šiuolaikinėje informacinėje visuomenėje tikriausiai paprasčiausias būdas atšaukti sutikimą yra paprastas elektroninis laiškas. Jei duomenų subjektas nori atšaukti mums duotą sutikimą, pakanka mums išsiųsti paprastą elektroninį laišką. Arba duomenų subjektas gali pasirinkti bet kokį kitą būdą, kuriuo jis mums praneša apie savo sutikimo atšaukimą.

## K. Teisę pateikti skundą priežiūros institucijai (Bendrojo duomenų apsaugos reglamento 14 straipsnio 2 dalies e punktas, 77 straipsnio 1 dalis)

Kaip duomenų valdytojas, privalome pranešti duomenų subjektui apie teisę pateikti skundą priežiūros institucijai pagal BDAR 14 straipsnio 2 dalies e punktą. Teisė pateikti skundą priežiūros institucijai reglamentuojama BDAR 77 straipsnio 1 dalyje. Pagal šią nuostatą, nepažeidžiant jokių kitų administracinių ar teisminių teisių gynimo priemonių, kiekvienas duomenų subjektas turi teisę pateikti skundą priežiūros institucijai, visų pirma valstybėje narėje, kurioje yra jo nuolatinė gyvenamoji vieta, darbo vieta arba įtariamo pažeidimo vieta, jei duomenų subjektas mano, kad su juo susijusių asmens duomenų tvarkymas pažeidžia Bendrąjį duomenų apsaugos reglamentą. Teisė pateikti skundą priežiūros institucijai Sąjungos teisėje buvo apribota tik taip, kad ja galima pasinaudoti tik vienoje priežiūros institucijoje (Bendrojo duomenų apsaugos reglamento 141 konstatuojamosios dalies 1 sakinys). Šia taisykle siekiama išvengti dvigubų to paties duomenų subjekto skundų tuo pačiu klausimu. Todėl, jei duomenų subjektas nori pateikti skundą dėl mūsų, prašome kreiptis tik į vieną priežiūros instituciją.

## L. Koks yra asmens duomenų kilmės šaltinis, ir, jei taikoma, ar duomenys gauti iš viešai prieinamų šaltinių (BDAR 14 straipsnio 2 dalies f punktas)

Iš esmės asmens duomenys renkami tiesiogiai iš duomenų subjekto arba bendradarbiaujant su institucija (pvz., gaunant duomenis iš oficialaus registro). Kiti duomenys apie duomenų subjektus gaunami


© All rights reserved by Heiko Maniero.

perduodant grupės įmonių duomenis. Atsižvelgiant į šią bendrą informaciją, įvardyti tikslius šaltinius, iš kurių gaunami asmens duomenys, yra neįmanoma arba tai pareikalautų neproporcingų pastangų, kaip apibrėžta Reglamento (EB) Nr. 14 straipsnio 5 dalies b punktą. Iš esmės nerenkame asmens duomenų iš viešai prieinamų šaltinių.

Bet kuris duomenų subjektas gali bet kuriuo metu kreiptis į mus, kad gautų išsamesnės informacijos apie tikslius su juo susijusių asmens duomenų šaltinius. Jei duomenų subjektui negalima nurodyti asmens duomenų kilmės, nes buvo naudotasi įvairiais šaltiniais, turėtų būti pateikta bendra informacija (BDAR 61 konstatuojamosios dalies 4 sakinys).

### M. Tai, kad esama 22 straipsnio 1 ir 4 dalyse nurodyto automatizuoto sprendimų priėmimo, įskaitant profiliavimą, ir, bent tais atvejais, prasmingą informaciją apie loginį jo pagrindimą, taip pat tokio duomenų tvarkymo reikšmę ir numatomas pasekmes duomenų subjektui (BDAR 14 straipsnio 2 dalies g punktas).

Būdami atsakinga įmonė, paprastai nenaudojame automatizuoto sprendimų priėmimo ar profiliavimo. Jei išimtiniais atvejais vykdome automatizuotą sprendimų priėmimą ar profiliavimą, informuosime duomenų subjektą atskirai arba savo privatumo politikos (mūsų interneto svetainėje) poskyryje. Šiuo atveju taikoma toliau nurodyta tvarka:

Automatinis sprendimų priėmimas, įskaitant profiliavimą, gali būti vykdomas, jei: 1) tai būtina duomenų subjekto ir mūsų sutarčiai sudaryti arba vykdyti; arba 2) tai leidžiama pagal Sąjungos arba valstybės narės teisę, kuri mums taikoma ir kurioje taip pat nustatytos tinkamos priemonės duomenų subjekto teisėms ir laisvėms bei teisėtiems interesams apsaugoti; arba 3) tai grindžiama aiškiu duomenų subjekto sutikimu.

BDAR 22 straipsnio 2 dalies a ir c punktuose nurodytais atvejais įgyvendiname tinkamas priemones duomenų subjekto teisėms ir laisvėms bei teisėtiems interesams apsaugoti. Tokiais atvejais turite teisę reikalauti, kad duomenų valdytojas imtųsi žmogiškųjų veiksmų, pareikšti savo nuomonę ir užginčyti sprendimą.

Reikšminga informacija apie susijusią logiką, taip pat tokio duomenų tvarkymo reikšmę ir numatomus padarinius duomenų subjektui pateikiama mūsų privatumo politikoje.

## III. EU-U.S. Data Privacy Framework (EU-U.S. DPF), UK Extension to the EU-U.S. DPF, Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF)


© All rights reserved by Heiko Maniero.

Jei mūsų organizacija yra sertifikuotas EU-U.S. Data Privacy Framework (EU-U.S. DPF) ir/arba UK Extension to the EU-U.S. DPF ir/arba Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF) narys, galioja šie punktai:

Mes laikomės EU-U.S. Data Privacy Framework (EU-U.S. DPF) ir UK Extension to the EU-U.S. DPF bei Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF), kaip nustatyta JAV prekybos departamento. Mūsų įmonė patvirtino JAV prekybos departamentui, kad laikosi EU-U.S. Data Privacy Framework Principles (EU-U.S. DPF Principles) asmens duomenų tvarkymo, gaunamų iš Europos Sąjungos ir Jungtinės Karalystės, pagal EU-U.S. DPF ir UK Extension to the EU-U.S. DPF, atžvilgiu. Mūsų įmonė patvirtino JAV prekybos departamentui, kad laikosi Swiss-U.S. Data Privacy Framework Principles (Swiss-U.S. DPF Principles) asmens duomenų tvarkymo, gaunamų iš Šveicarijos, pagal Swiss-U.S. DPF, atžvilgiu. Jei mūsų privatumo politikos nuostatos prieštarauja EU-U.S. DPF Principles ir/arba Swiss-U.S. DPF Principles, pirmenybė teikiama Principles.

Norėdami sužinoti daugiau apie Data Privacy Framework (DPF) programą ir peržiūrėti mūsų sertifikatą, apsilankykite https://www.dataprivacyframework.gov/.

Kitos mūsų įmonės JAV padaliniai ar dukterinės įmonės, kurios taip pat laikosi EU-U.S. DPF Principals, įskaitant UK Extension to the EU-U.S. DPF ir Swiss-U.S. DPF Principals, jei tokių yra, nurodytos mūsų privatumo politikoje.

Vadovaujantis EU-U.S. DPF ir UK Extension to the EU-U.S. DPF bei Swiss-U.S. DPF, mūsų įmonė įsipareigoja bendradarbiauti su ES duomenų apsaugos institucijų ir Jungtinės Karalystės Information Commissioner's Office (ICO) bei Šveicarijos federaliniu duomenų apsaugos ir informacijos komisaru (EDÖB) įsteigta komisija ir laikytis jų rekomendacijų dėl neišspręstų skundų apie mūsų asmens duomenų tvarkymą, gaunamų pagal EU-U.S. DPF ir UK Extension to the EU-U.S. DPF bei Swiss-U.S. DPF.

Mes informuojame suinteresuotas šalis apie atitinkamas Europos duomenų apsaugos institucijas, atsakingas už skundų dėl mūsų organizacijos asmens duomenų tvarkymo nagrinėjimą, šio skaidrumo dokumento viršuje ir kad suteikiame suinteresuotoms šalims tinkamą ir nemokamą teisinę apsaugą.

Mes informuojame visas suinteresuotas šalis, kad mūsų įmonė yra pavaldžios Federal Trade Commission (FTC) tyrimo ir vykdymo įgaliojimams.

Suinteresuotos šalys tam tikromis sąlygomis turi galimybę pasinaudoti privalomu arbitražu. Mūsų organizacija įsipareigoja spręsti reikalavimus ir laikytis DPF-Principals I priedo sąlygų, jei suinteresuota šalis pateikia privalomo arbitražo prašymą, informuodama mūsų organizaciją ir laikydamasi I priedo procedūrų ir sąlygų.

Mes šiuo informuojame visas suinteresuotas šalis apie mūsų organizacijos atsakomybę perduodant asmens duomenis trečiosioms šalims.

Klausimams iš suinteresuotų šalių ar duomenų apsaugos priežiūros institucijų, mes paskyrėme vietinius atstovus, nurodytus šio skaidrumo dokumento viršuje.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

Mes suteikiame jums galimybę pasirinkti (Opt-out), ar jūsų asmens duomenys (i) turėtų būti perduodami trečiosioms šalims, ar (ii) turėtų būti naudojami tikslui, kuris iš esmės skiriasi nuo to/tų tikslo/tikslų, kuriam/kurie buvo iš pradžių surinkti arba vėliau jūsų patvirtinti. Aiškus, gerai matomas ir lengvai prieinamas mechanizmas, leidžiantis naudotis savo pasirinkimu, yra susisiekti su mūsų duomenų apsaugos pareigūnu (DSB) el. paštu. Jūs neturite pasirinkimo galimybės, ir mes neprivalome to daryti, jei duomenys perduodami trečiajai šaliai, kuri veikia kaip mūsų vardu ir pagal mūsų nurodymus atliekantis agentas ar tvarkytojas. Tačiau mes visada sudarome sutartį su tokiu agentu ar tvarkytoju.

Dėl jautrių duomenų (t. y. asmens duomenų, kuriuose yra informacijos apie sveikatos būklę, rasinę ar etninę kilmę, politines pažiūras, religinius ar filosofinius įsitikinimus, narystę profesinėje sąjungoje arba informaciją apie asmens lytinį gyvenimą) mes gauname jūsų aiškų sutikimą (Opt-in), kai šie duomenys (i) perduodami trečiosioms šalims arba (ii) naudojami kitam tikslui, nei buvo iš pradžių surinkti arba kuriam jūs vėliau sutikote, pasirinkdami Opt-in. Be to, mes visus asmens duomenis, kuriuos gauname iš trečiųjų šalių, laikome jautriais, jei trečioji šalis juos identifikuoja ir tvarko kaip jautrius.

Mes informuojame jus šiuo apie reikalavimą atskleisti asmens duomenis reaguojant į teisėtus valdžios institucijų prašymus, įskaitant nacionalinio saugumo ar teisėsaugos reikalavimų vykdymą.

Perduodant asmens duomenis trečiajai šaliai, kuri veikia kaip valdytojas, mes laikomės Principals apie pranešimą ir pasirinkimą. Be to, mes sudarome sutartį su trečiaja šalimi, atsakinga už tvarkymą, kurioje nustatyta, kad šie duomenys gali būti tvarkomi tik ribotais ir apibrėžtais tikslais, atsižvelgiant į jūsų duotą sutikimą, ir kad gavėjas turi užtikrinti tokį pat apsaugos lygį, kaip DPF Principals ir mus informuoti, jei nustato, kad nebegali vykdyti šio įsipareigojimo. Sutartis numato, kad trečioji šalis, atsakinga už tvarkymą, nutraukia tvarkymą arba imasi kitų tinkamų ir adekvačių priemonių situacijai ištaisyti, jei toks nustatymas atliekamas.

Perduodant asmens duomenis trečiajai šaliai, kuri veikia kaip agentas arba tvarkytojas, (i) mes perduodame šiuos duomenis tik ribotais ir apibrėžtais tikslais; (ii) mes užtikriname, kad agentas arba tvarkytojas privalo užtikrinti bent jau tokį patį duomenų apsaugos lygį, kokį reikalauja DPF-Principals; (iii) mes imsimės tinkamų ir adekvačių priemonių, kad užtikrintume, jog agentas arba tvarkytojas iš tikrųjų tvarko perduotus asmens duomenis tokiu būdu, kuris atitinka mūsų įsipareigojimus pagal DPF-Principals; (iv) mes reikalaujame, kad agentas arba tvarkytojas informuotų mūsų organizaciją, jei nustato, kad nebegali užtikrinti tokio pat apsaugos lygio, kokį numato DPF-Principals; (v) gavę tokį pranešimą, taip pat ir pagal (iv), mes imsimės tinkamų ir adekvačių veiksmų, kad nutrauktume neteisėtą tvarkymą ir ištaisytume situaciją; ir (vi) DPF Department prašymu pateiksime santrauką arba reprezentatyvų atitinkamų duomenų apsaugos nuostatų iš mūsų sutarties su šiuo agentu pavyzdį.

Vadovaujantis EU-U.S. DPF ir/arba UK Extension to the EU-U.S. DPF ir/arba Swiss-U.S. DPF, mūsų organizacija įsipareigoja bendradarbiauti su ES duomenų apsaugos institucijų ir Jungtinės Karalystės Information Commissioner's Office (ICO) arba Šveicarijos federalinio duomenų apsaugos ir informacijos komisaro (EDÖB) įsteigta komisija ir laikytis jų rekomendacijų dėl neišspręstų skundų apie mūsų elgesį


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

su asmens duomenimis, gaunamais pagal EU-U.S. DPF ir UK Extension to the EU-U.S. DPF ir Swiss-U.S. DPF, susijusius su darbo santykiais.

Visi duomenų subjektai, kurie laikinai yra Europos Sąjungoje (ES), Europos ekonominėje erdvėje (EEE) ar Jungtinėje Karalystėje arba kurių nuolatinė ar įprastinė gyvenamoji vieta yra ten, turi teisę naudotis mūsų skaidrumo dokumente paskelbtomis teisėmis ir duomenų subjekto teisėmis, kurios taip pat kyla iš BDAR 15-22 straipsnių, įskaitant teisę susipažinti su asmens duomenimis. Šią informaciją pateikėme visomis ES ir EEE kalbomis. Versija anglų kalba taikoma Jungtinei Karalystei.

Visi duomenų subjektai, kurie laikinai gyvena Šveicarijoje arba kurių nuolatinė ar įprastinė gyvenamoji vieta yra Šveicarijoje, turi teises ir duomenų subjekto teises pagal Šveicarijos duomenų apsaugos įstatymą (DPA) ir Šveicarijos duomenų apsaugos reglamentą (DPR), kurie skelbiami mūsų skaidrumo dokumente, įskaitant teisę susipažinti su asmens duomenimis. Šią informaciją pateikėme trimis oficialiomis Šveicarijos kalbomis (vokiečių, italų ir prancūzų).


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

# LITHUANIAN: Informacija apie darbuotojų ir kandidatų asmens duomenų tvarkymą (BDAR 13, 14 straipsniai)

Gerbiamasis pone arba ponia,

Darbuotojų ir pareiškėjų asmens duomenys turi būti ypač saugomi. Mūsų tikslas - išlaikyti aukštą duomenų apsaugos lygį. Todėl regulāri tobuliname savo duomenų apsaugos ir duomenų saugumo koncepcijas.

Žinoma, mes laikomės įstatyminių nuostatų dėl duomenų apsaugos. Pagal BDAR 13, 14 straipsnius duomenų valdytojai, tvarkydami asmens duomenis, laikosi konkrečių informavimo reikalavimų. Šiuo dokumentu šie įpareigojimai įvykdomi.

Teisinio reguliavimo terminologija yra sudėtinga. Deja, rengiant šį dokumentą nebuvo galima atsisakyti teisinių terminų vartojimo. Todėl norėtume pabrėžti, kad visais klausimais, susijusiais su šiuo dokumentu, vartojamais terminais ar formuluotėmis, visada galite kreiptis į mus.

## I. Informacija, kuri turi būti pateikta, kai asmens duomenys renkami iš duomenų subjekto (BDAR 13 straipsnis)

### A. Duomenų valdytojo ir, jeigu taikoma, duomenų valdytojo atstovo tapatybę ir kontaktinius duomenis (BDAR 13 straipsnio 1 dalies a punktas)

Žr. pirmiau

### B. Duomenų apsaugos pareigūno, jeigu taikoma, kontaktinius duomenis (BDAR 13 straipsnio 1 dalies b punktas)

Žr. pirmiau

### C. Duomenų tvarkymo tikslus, dėl kurių ketinama tvarkyti asmens duomenis, taip pat duomenų tvarkymo teisinį pagrindą (BDAR 13 straipsnio 1 dalies c punktas)

Pareiškėjo duomenų atveju duomenų tvarkymo tikslas - atlikti paraiškos nagrinėjimą įdarbinimo proceso metu. Šiuo tikslu tvarkome visus jūsų pateiktus duomenis. Remdamiesi įdarbinimo proceso metu pateiktais duomenimis, patikrinsime, ar esate kviečiamas į darbo pokalbį (atrankos proceso dalis). Jei kandidatai iš esmės yra tinkami, ypač darbo pokalbio metu, tvarkome tam tikrus kitus jūsų pateiktus


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

asmens duomenis, kurie yra būtini mūsų atrankos sprendimui priimti. Jei būsite mūsų įdarbintas, kandidato duomenys automatiškai pasikeis į darbuotojo duomenis. Įdarbinimo proceso metu tvarkysime kitus jūsų asmens duomenis, kurių prašome iš jūsų ir kurie reikalingi sutarčiai inicijuoti arba vykdyti (pavyzdžiui, asmens identifikacinius numerius arba mokesčių mokėtojo numerius). Darbuotojų duomenų atveju duomenų tvarkymo tikslas yra darbo sutarties vykdymas arba kitų teisinių nuostatų, taikomų darbo santykiams (pvz., mokesčių teisės aktų), laikymasis, taip pat jūsų asmens duomenų naudojimas su jumis sudarytai darbo sutarčiai vykdyti (pvz., jūsų vardo ir pavardės bei kontaktinės informacijos skelbimas įmonėje arba klientams). Darbuotojų duomenys saugomi pasibaigus darbo santykiams, kad būtų laikomasi teisinių saugojimo terminų.

Duomenų tvarkymo teisinis pagrindas yra BDAR 6 straipsnio 1 dalies b punktas, BDAR 9 straipsnio 2 dalies b ir h punktai, BDAR 88 straipsnio 1 dalis ir nacionaliniai teisės aktai, pavyzdžiui, Vokietijos BDSG (Federalinio duomenų apsaugos įstatymo) 26 straipsnis.

## D. Jei yra, asmens duomenų gavėjus arba asmens duomenų gavėjų kategorijas (BDAR 13 straipsnio 1 dalies e punktas)

Valdžios institucijos

Išorės įstaigos

Kitos išorės įstaigos

Vidinis apdorojimas

Grupės vidaus apdorojimas

Kitos įstaigos

Mūsų duomenų tvarkytojų ir duomenų gavėjų trečiosiose šalyse bei, jei taikoma, tarptautinių organizacijų sąrašas skelbiamas mūsų interneto svetainėje arba jo galima nemokamai paprašyti iš mūsų. Norėdami paprašyti šio sąrašo, kreipkitės į mūsų duomenų apsaugos pareigūną.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## E. Kai taikoma, apie duomenų valdytojo ketinimą asmens duomenis perduoti į trečiąją valstybę arba tarptautinei organizacijai ir Komisijos sprendimo dėl tinkamumo buvimą ar nebuvimą, arba 46 ar 47 straipsniuose arba 49 straipsnio 1 dalies antroje pastraipoje nurodytų perdavimų atveju – tinkamas arba pritaikytas apsaugos priemones ir būdus, kaip gauti jų kopiją arba kur suteikiama galimybė su jais susipažinti (BDAR 13 straipsnio 1 dalies f punktas, 46 straipsnio 1 dalis, 46 straipsnio 2 dalies c punktas)

Visos mūsų grupei priklausančios įmonės ir filialai (toliau - grupės įmonės), kurių verslo vieta arba biuras yra trečiojoje šalyje, gali būti asmens duomenų gavėjai. Visų grupės įmonių arba gavėjų sąrašo galite paprašyti iš mūsų.

Pagal BDAR 46 straipsnio 1 dalį duomenų valdytojas arba duomenų tvarkytojas gali perduoti asmens duomenis į trečiąją šalį tik tuo atveju, jei duomenų valdytojas arba duomenų tvarkytojas yra numatęs tinkamas apsaugos priemones ir su sąlyga, kad duomenų subjektai gali naudotis įgyvendinamomis duomenų subjekto teisėmis ir veiksmingomis teisių gynimo priemonėmis. Tinkamos apsaugos priemonės gali būti numatytos nereikalaujant jokio konkretaus priežiūros institucijos leidimo, naudojant standartines sutarčių sąlygas, BDAR 46 straipsnio 2 dalies c punktas.

Prieš pirmą kartą perduodant asmens duomenis su visais gavėjais iš trečiųjų šalių susitariama dėl standartinių Europos Sąjungos sutarčių sąlygų arba kitų tinkamų apsaugos priemonių. Todėl užtikrinama, kad duomenų subjektams būtų užtikrintos tinkamos apsaugos priemonės, įgyvendinamos duomenų subjekto teisės ir veiksmingos teisinės gynybos priemonės. Kiekvienas duomenų subjektas gali iš mūsų gauti standartinių sutarties sąlygų kopiją. Su standartinėmis sutarčių sąlygomis taip pat galima susipažinti Europos Sąjungos oficialiajame leidinyje.

Bendrojo duomenų apsaugos reglamento (BDAR) 45 straipsnio 3 dalimi Europos Komisijai suteikiami įgaliojimai įgyvendinimo aktu nuspręsti, kad ES nepriklausanti šalis užtikrina tinkamą apsaugos lygį. Tai reiškia, kad asmens duomenų apsaugos lygis yra iš esmės lygiavertis apsaugos lygiui ES. Sprendimų dėl tinkamumo poveikis yra tas, kad asmens duomenys gali laisvai ir be jokių papildomų kliūčių judėti iš ES (ir Norvegijos, Lichtenšteino bei Islandijos) į trečiąją šalį. Panašios taisyklės taikomos Jungtinei Karalystei, Šveicarijai ir kai kurioms kitoms šalims.

Jei Europos Komisija arba kitos šalies vyriausybė nusprendė, kad trečioji šalis užtikrina tinkamą apsaugos lygį, ir yra galiojanti sistema (pvz., EU-U.S. Data Privacy Framework, Swiss-U.S. Data Privacy Framework, UK Extension to the EU-U.S. Data Privacy Framework), visi mūsų atliekami duomenų perdavimai tokių sistemų nariams (pvz., savarankiškai sertifikuotiems subjektams) grindžiami tik to subjekto naryste atitinkamoje sistemoje. Jei mes arba vienas iš mūsų grupės subjektų yra tokios sistemos narys, visi duomenų perdavimai mums arba mūsų grupės subjektui yra grindžiami tik šio subjekto naryste tokioje sistemoje.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

Bet kuris duomenų subjektas gali iš mūsų gauti rėmų kopiją. Be to, su šiomis sistemomis taip pat galima susipažinti Europos Sąjungos oficialiajame leidinyje, paskelbtoje teisinėje medžiagoje arba priežiūros institucijų ar kitų kompetentingų institucijų ar įstaigų interneto svetainėse.

## F. Asmens duomenų saugojimo laikotarpį arba, jei tai neįmanoma, kriterijus, taikomus tam laikotarpiui nustatyti (BDAR 13 straipsnio 2 dalies a punktas)

Pareiškėjų asmens duomenys saugomi 6 mėnesius. Darbuotojų duomenims taikomas atitinkamas teisės aktuose nustatytas saugojimo laikotarpis. Pasibaigus šiam laikotarpiui, atitinkami duomenys įprastai ištrinami, jei jie nebereikalingi sutarčiai įvykdyti arba sutarčiai inicijuoti.

## G. Teisę prašyti, kad duomenų valdytojas leistų susipažinti su duomenų subjekto asmens duomenimis ir juos ištaisytų arba ištrintų, arba apribotų duomenų tvarkymą, arba teisę nesutikti, kad duomenys būtų tvarkomi, taip pat teisę į duomenų perkeliamumą (BDAR 13 straipsnio 2 dalies b punktas) egzistavimas

Visi duomenų subjektai turi šias teises:

***Teisė į prieigą***

Kiekvienas duomenų subjektas turi teisę susipažinti su savo asmens duomenimis. Teisė susipažinti taikoma visiems mūsų tvarkomiems duomenims. Šia teise galima naudotis lengvai ir pagrįstais laiko tarpais, kad būtų galima sužinoti ir patikrinti duomenų tvarkymo teisėtumą (BDAR 63 konstatuojamoji dalis). Ši teisė išplaukia iš Europos Sąjungos teisės aktų rinkinio (toliau - ES teisės aktai) 3 straipsnio 2 dalies. 15 BDAR. Duomenų subjektas, norėdamas pasinaudoti prieigos teise, gali kreiptis į mus.

***Teisė į ištaisymą***

Pagal BDAR 16 straipsnio 1 sakinį duomenų subjektas turi teisę iš duomenų valdytojo nepagrįstai nedelsdamas reikalauti, kad duomenų valdytojas ištaisytų netikslius jo asmens duomenis. Be to, BDAR 16 straipsnio 2 sakinyje numatyta, kad duomenų subjektas, atsižvelgiant į duomenų tvarkymo tikslus, turi teisę reikalauti, kad neišsamūs asmens duomenys būtų papildyti, be kita ko, pateikiant papildomą pareiškimą. Duomenų subjektas gali kreiptis į mus, kad pasinaudotų teise ištaisyti duomenis.

***Teisė į ištrynimą (teisė būti pamirštam)***

Be to, duomenų subjektai turi teisę į duomenų ištrynimą ir teisę būti pamirštiems pagal Reglamento (EB) Nr. 17 BDAR. Šia teise taip pat galima pasinaudoti kreipiantis į mus. Tačiau šioje vietoje norėtume atkreipti dėmesį, kad ši teisė netaikoma, jei tvarkyti duomenis būtina, kad būtų įvykdyta teisinė prievolė, kuri taikoma mūsų įmonei, BDAR 17 straipsnio 3 dalies b punktas. Tai reiškia, kad prašymą ištrinti duomenis galime patenkinti tik pasibaigus teisės aktuose nustatytam saugojimo laikotarpiui.


© All rights reserved by Heiko Maniero.

***Teisė apriboti duomenų tvarkymą***

Pagal BDAR 18 straipsnį bet kuris duomenų subjektas turi teisę apriboti duomenų tvarkymą. Apriboti duomenų tvarkymą galima reikalauti, jei tenkinama viena iš BDAR 18 straipsnio 1 dalies a-d punktuose nustatytų sąlygų. Duomenų subjektas gali susisiekti su mumis, kad pasinaudotų teise apriboti duomenų tvarkymą.

***Teisė prieštarauti***

Be to, CK 6.2 str. 21 BDAR garantuojama teisė nesutikti. Duomenų subjektas gali susisiekti su mumis, kad pasinaudotų teise nesutikti.

***Teisė į duomenų perkeliamumą***

Straipsnis. 20 BDAR suteikia duomenų subjektui teisę į duomenų perkeliamumą. Pagal šią nuostatą duomenų subjektas BDAR 20 straipsnio 1 dalies a ir b punktuose nustatytomis sąlygomis turi teisę gauti su juo susijusius asmens duomenis, kuriuos jis pateikė duomenų valdytojui, susistemintu, įprastai naudojamu ir kompiuterio skaitomu formatu ir turi teisę perduoti tuos duomenis kitam duomenų valdytojui netrukdomas duomenų valdytojo, kuriam asmens duomenys buvo pateikti. Duomenų subjektas gali susisiekti su mumis, kad pasinaudotų teise į duomenų perkeliamumą.

## H. Kai duomenų tvarkymas grindžiamas 6 straipsnio 1 dalies a punktu arba 9 straipsnio 2 dalies a punktu, teisę bet kuriuo metu atšaukti sutikimą, nedarant poveikio sutikimu grindžiamo duomenų tvarkymo iki sutikimo atšaukimo teisėtumui (BDAR 13 straipsnio 2 dalies c punktas).

Jei asmens duomenų tvarkymas grindžiamas CK 2.5 str. 6 straipsnio 1 dalies a punktu, t. y. jei duomenų subjektas davė sutikimą tvarkyti asmens duomenis vienu ar keliais konkrečiais tikslais, arba yra grindžiamas BDAR 9 straipsnio 2 dalies a punktu, kuris reglamentuoja aiškų sutikimą tvarkyti specialių kategorijų asmens duomenis, duomenų subjektas pagal BDAR 7 straipsnio 3 dalies 1 sakinį turi teisę bet kuriuo metu atšaukti savo sutikimą.

Sutikimo atšaukimas neturi įtakos duomenų tvarkymo, pagrįsto sutikimu prieš jo atšaukimą, teisėtumui, BDAR 7 straipsnio 3 dalies 2 sakinys. Atšaukti sutikimą turi būti taip pat paprasta, kaip ir duoti sutikimą, 1 straipsnis. BDAR 7 straipsnio 3 dalies 4 sakinys. Todėl atšaukti sutikimą visada galima tuo pačiu būdu, kuriuo buvo duotas sutikimas, arba bet kuriuo kitu būdu, kurį duomenų subjektas laiko paprastesniu. Šiuolaikinėje informacinėje visuomenėje bene paprasčiausias sutikimo atšaukimo būdas yra paprastas elektroninis laiškas. Jei duomenų subjektas nori atšaukti mums duotą sutikimą, pakanka mums išsiųsti paprastą elektroninį laišką. Arba duomenų subjektas gali pasirinkti bet kurį kitą būdą, kuriuo jis mums praneša apie savo sutikimo atšaukimą.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## I. Teisę pateikti skundą priežiūros institucijai (Bendrojo duomenų apsaugos reglamento 13 straipsnio 2 dalies d punktas, 77 straipsnio 1 dalis)

Kaip duomenų valdytojas, privalome pranešti duomenų subjektui apie teisę pateikti skundą priežiūros institucijai, BDAR 13 straipsnio 2 dalies d punktas. Teisė pateikti skundą priežiūros institucijai reglamentuojama BDAR 77 straipsnio 1 dalyje. Pagal šią nuostatą, nepažeidžiant jokių kitų administracinių ar teisminių teisių gynimo priemonių, kiekvienas duomenų subjektas turi teisę pateikti skundą priežiūros institucijai, visų pirma valstybėje narėje, kurioje yra jo nuolatinė gyvenamoji vieta, darbo vieta arba įtariamo pažeidimo vieta, jei duomenų subjektas mano, kad su juo susijusių asmens duomenų tvarkymas pažeidžia Bendrąjį duomenų apsaugos reglamentą. Teisė pateikti skundą priežiūros institucijai Sąjungos teisėje buvo apribota tik taip, kad ja galima pasinaudoti tik vienoje priežiūros institucijoje (Bendrojo duomenų apsaugos reglamento 141 konstatuojamosios dalies 1 sakinys). Šia taisykle siekiama išvengti dvigubų to paties duomenų subjekto skundų tuo pačiu klausimu. Todėl, jei duomenų subjektas nori pateikti skundą dėl mūsų, prašome kreiptis tik į vieną priežiūros instituciją.

## J. Tai, ar asmens duomenų pateikimas yra teisės aktais arba sutartyje numatytas reikalavimas, ar reikalavimas, kurį būtina įvykdyti norint sudaryti sutartį, taip pat tai, ar duomenų subjektas privalo pateikti asmens duomenis, ir informaciją apie galimas tokių duomenų nepateikimo pasekmes (BDAR 13 straipsnio 2 dalies e punktas)

Paaiškiname, kad asmens duomenų teikimo iš dalies reikalaujama pagal įstatymus (pvz., mokesčių teisės aktus) arba tai gali būti susiję su sutartinėmis nuostatomis (pvz., informacija apie sutarties partnerį).

Kartais, norint sudaryti sutartį, gali prireikti, kad duomenų subjektas pateiktų mums asmens duomenis, kuriuos vėliau turime tvarkyti. Pavyzdžiui, duomenų subjektas privalo mums pateikti asmens duomenis, kai mūsų įmonė su juo pasirašo sutartį. Nepateikus asmens duomenų, sutartis su duomenų subjektu negalėtų būti sudaryta.

Prieš duomenų subjektui pateikiant asmens duomenis, duomenų subjektas turi su mumis susisiekti. Duomenų subjektui paaiškiname, ar asmens duomenis pateikti reikalaujama pagal įstatymą ar sutartį, ar jie būtini sutarčiai sudaryti, ar yra prievolė pateikti asmens duomenis ir kokios bus asmens duomenų nepateikimo pasekmės.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

### K. Tai, kad esama 22 straipsnio 1 ir 4 dalyse nurodyto automatizuoto sprendimų priėmimo, įskaitant profiliavimą, ir, bent tais atvejais, prasmingą informaciją apie loginį jo pagrindimą, taip pat tokio duomenų tvarkymo reikšmę ir numatomas pasekmes duomenų subjektui (Bendrojo duomenų apsaugos reglamento 13 straipsnio 2 dalies f punktas).

Būdami atsakinga įmonė, paprastai nenaudojame automatizuoto sprendimų priėmimo ar profiliavimo. Jei išimtiniais atvejais vykdome automatizuotą sprendimų priėmimą ar profiliavimą, informuosime duomenų subjektą atskirai arba savo privatumo politikos (mūsų interneto svetainėje) poskyryje. Šiuo atveju taikoma toliau nurodyta tvarka:

Automatinis sprendimų priėmimas, įskaitant profiliavimą, gali būti vykdomas, jei: 1) tai būtina duomenų subjekto ir mūsų sutarčiai sudaryti arba vykdyti; arba 2) tai leidžiama pagal Sąjungos arba valstybės narės teisę, kuri mums taikoma ir kurioje taip pat nustatytos tinkamos priemonės duomenų subjekto teisėms ir laisvėms bei teisėtiems interesams apsaugoti; arba 3) tai grindžiama aiškiu duomenų subjekto sutikimu.

BDAR 22 straipsnio 2 dalies a ir c punktuose nurodytais atvejais įgyvendiname tinkamas priemones duomenų subjekto teisėms ir laisvėms bei teisėtiems interesams apsaugoti. Tokiais atvejais turite teisę reikalauti, kad duomenų valdytojas imtųsi žmogiškųjų veiksmų, pareikšti savo nuomonę ir užginčyti sprendimą.

Reikšminga informacija apie susijusią logiką, taip pat tokio duomenų tvarkymo reikšmę ir numatomus padarinius duomenų subjektui pateikiama mūsų privatumo politikoje.

## II. Informacija, kuri turi būti pateikta, kai asmens duomenys yra gauti ne iš duomenų subjekto (BDAR 14 straipsnis)

### A. Duomenų valdytojo ir duomenų valdytojo atstovo, jei taikoma, tapatybę ir kontaktinius duomenis (BDAR 14 straipsnio 1 dalies a punktas)

Žr. pirmiau

### B. Duomenų apsaugos pareigūno, jei taikoma, kontaktinius duomenis (BDAR 14 straipsnio 1 dalies b punktas)

Žr. pirmiau


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## C. Duomenų tvarkymo tikslus, kuriais ketinama tvarkyti asmens duomenis, taip pat duomenų tvarkymo teisinį pagrindą (BDAR 14 straipsnio 1 dalies c punktas)

Iš duomenų subjekto nerinktų pareiškėjo duomenų atveju duomenų tvarkymo tikslas - atlikti paraiškos nagrinėjimą įdarbinimo proceso metu. Šiuo tikslu galime tvarkyti ne iš jūsų surinktus duomenis. Remdamiesi įdarbinimo proceso metu tvarkomais duomenimis, patikrinsime, ar esate kviečiamas į darbo pokalbį (atrankos proceso dalis). Jei būsite pas mus įdarbintas, pretendento duomenys automatiškai bus paversti darbuotojo duomenimis. Darbuotojų duomenų atveju duomenų tvarkymo tikslas yra darbo sutarties vykdymas arba kitų darbo santykiams taikomų teisinių nuostatų laikymasis. Darbuotojų duomenys saugomi pasibaigus darbo santykiams, kad būtų laikomasi teisinių saugojimo terminų.

Duomenų tvarkymo teisinis pagrindas yra BDAR 6 straipsnio 1 dalies b ir f punktai, BDAR 9 straipsnio 2 dalies b ir h punktai, BDAR 88 straipsnio 1 dalis ir nacionaliniai teisės aktai, pavyzdžiui, Vokietijos BDSG (Federalinis duomenų apsaugos įstatymas) 26 straipsnis.

## D. Atitinkamų asmens duomenų kategorijas (BDAR 14 straipsnio 1 dalies d punktas)

Pareiškėjo duomenys

Darbuotojų duomenys

## E. Jei jos yra, asmens duomenų gavėjus arba asmens duomenų gavėjų kategorijas (BDAR 14 straipsnio 1 dalies e punktas)

Valdžios institucijos

Išorės įstaigos

Kitos išorės įstaigos

Vidinis apdorojimas

Grupės vidaus apdorojimas

Kitos įstaigos

Mūsų duomenų tvarkytojų ir duomenų gavėjų trečiosiose šalyse bei, jei taikoma, tarptautinių organizacijų sąrašas skelbiamas mūsų interneto svetainėje arba jo galima nemokamai paprašyti iš mūsų. Norėdami paprašyti šio sąrašo, kreipkitės į mūsų duomenų apsaugos pareigūną.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## F. Kai taikoma, apie duomenų valdytojo ketinimą asmens duomenis perduoti gavėjui trečiojoje valstybėje arba tarptautinei organizacijai ir Komisijos sprendimo dėl tinkamumo buvimą ar nebuvimą, o 46 ar 47 straipsniuose arba 49 straipsnio 1 dalies antroje pastraipoje nurodytų perdavimų atveju – tinkamas arba pritaikytas apsaugos priemones ir būdus, kaip gauti jų kopiją arba kur suteikiama galimybė su jais susipažinti (BDAR 14 straipsnio 1 dalies f punktas, 46 straipsnio 1 dalis, 46 straipsnio 2 dalies c punktas)

Visos mūsų grupei priklausančios įmonės ir filialai (toliau - grupės įmonės), kurių verslo vieta arba biuras yra trečiojoje šalyje, gali būti asmens duomenų gavėjai. Visų grupės įmonių arba gavėjų sąrašo galite paprašyti iš mūsų.

Pagal BDAR 46 straipsnio 1 dalį duomenų valdytojas arba duomenų tvarkytojas gali perduoti asmens duomenis į trečiąją šalį tik tuo atveju, jei duomenų valdytojas arba duomenų tvarkytojas yra numatęs tinkamas apsaugos priemones ir su sąlyga, kad duomenų subjektai gali naudotis įgyvendinamomis duomenų subjekto teisėmis ir veiksmingomis teisių gynimo priemonėmis. Tinkamos apsaugos priemonės gali būti numatytos nereikalaujant jokio konkretaus priežiūros institucijos leidimo, naudojant standartines duomenų apsaugos sąlygas, BDAR 46 straipsnio 2 dalies c punktas.

Prieš pirmą kartą perduodant asmens duomenis su visais gavėjais iš trečiųjų šalių susitariama dėl standartinių Europos Sąjungos sutarčių sąlygų arba kitų tinkamų apsaugos priemonių. Todėl užtikrinama, kad duomenų subjektams būtų užtikrintos tinkamos apsaugos priemonės, įgyvendinamos duomenų subjekto teisės ir veiksmingos teisinės gynybos priemonės. Kiekvienas duomenų subjektas gali iš mūsų gauti standartinių sutarties sąlygų kopiją. Su standartinėmis sutarčių sąlygomis taip pat galima susipažinti Europos Sąjungos oficialiajame leidinyje.

Bendrojo duomenų apsaugos reglamento (BDAR) 45 straipsnio 3 dalimi Europos Komisijai suteikiami įgaliojimai įgyvendinimo aktu nuspręsti, kad ES nepriklausanti šalis užtikrina tinkamą apsaugos lygį. Tai reiškia, kad asmens duomenų apsaugos lygis yra iš esmės lygiavertis apsaugos lygiui ES. Sprendimų dėl tinkamumo poveikis yra tas, kad asmens duomenys gali laisvai ir be jokių papildomų kliūčių judėti iš ES (ir Norvegijos, Lichtenšteino bei Islandijos) į trečiąją šalį. Panašios taisyklės taikomos Jungtinei Karalystei, Šveicarijai ir kai kurioms kitoms šalims.

Jei Europos Komisija arba kitos šalies vyriausybė nusprendė, kad trečioji šalis užtikrina tinkamą apsaugos lygį, ir yra galiojanti sistema (pvz., EU-U.S. Data Privacy Framework, Swiss-U.S. Data Privacy Framework, UK Extension to the EU-U.S. Data Privacy Framework), visi mūsų atliekami duomenų perdavimai tokių sistemų nariams (pvz., savarankiškai sertifikuotiems subjektams) grindžiami tik to subjekto naryste atitinkamoje sistemoje. Jei mes arba vienas iš mūsų grupės subjektų yra tokios sistemos narys, visi duomenų perdavimai mums arba mūsų grupės subjektui yra grindžiami tik šio subjekto naryste tokioje sistemoje.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

Bet kuris duomenų subjektas gali iš mūsų gauti rėmų kopiją. Be to, su šiomis sistemomis taip pat galima susipažinti Europos Sąjungos oficialiajame leidinyje, paskelbtoje teisinėje medžiagoje arba priežiūros institucijų ar kitų kompetentingų institucijų ar įstaigų interneto svetainėse.

## G. Asmens duomenų saugojimo laikotarpį arba, jei tai neįmanoma, kriterijus, taikomus tam laikotarpiui nustatyti (BDAR 14 straipsnio 2 dalies a punktas)

Pareiškėjų asmens duomenys saugomi 6 mėnesius. Darbuotojų duomenims taikomas atitinkamas teisės aktuose nustatytas saugojimo laikotarpis. Pasibaigus šiam laikotarpiui, atitinkami duomenys įprastai ištrinami, jei jie nebereikalingi sutarčiai įvykdyti arba sutarčiai inicijuoti.

## H. Kai duomenų tvarkymas atliekamas pagal 6 straipsnio 1 dalies f punktą, teisėtus duomenų valdytojo arba trečiosios šalies interesus (BDAR 14 straipsnio 2 dalies b punktas)

Pagal BDAR 6 straipsnio 1 dalies f punktą duomenų tvarkymas yra teisėtas tik tuo atveju, jei duomenų tvarkymas yra būtinas duomenų valdytojo arba trečiosios šalies teisėtų interesų, kurių siekia duomenų valdytojas arba trečioji šalis, tikslais, išskyrus atvejus, kai už tokius interesus yra viršesni duomenų subjekto interesai arba pagrindinės teisės ir laisvės, dėl kurių būtina užtikrinti asmens duomenų apsaugą. Pagal BDAR 47 konstatuojamosios dalies 2 sakinį teisėtas interesas gali egzistuoti, kai duomenų subjektą ir duomenų valdytoją sieja atitinkami ir tinkami santykiai, pavyzdžiui, kai duomenų subjektas yra duomenų valdytojo klientas. Visais atvejais, kai mūsų įmonė tvarko pareiškėjo duomenis remdamasi BDAR 6 straipsnio 1 dalies f punktu, mūsų teisėtas interesas yra tinkamų darbuotojų ir specialistų įdarbinimas.

## I. Teisę prašyti, kad duomenų valdytojas leistų susipažinti su duomenų subjekto asmens duomenimis ir juos ištaisytų arba ištrintų, arba apribotų duomenų tvarkymą, ir teisę nesutikti, kad duomenys būtų tvarkomi, taip pat teisę į į duomenų perkeliamumą (BDAR 14 straipsnio 2 dalies c punktas) egzistavimas

Visi duomenų subjektai turi šias teises:

***Teisė į prieigą***

Kiekvienas duomenų subjektas turi teisę susipažinti su savo asmens duomenimis. Teisė susipažinti taikoma visiems mūsų tvarkomiems duomenims. Šia teise galima naudotis lengvai ir pagrįstais laiko tarpais, kad būtų galima sužinoti ir patikrinti duomenų tvarkymo teisėtumą (BDAR 63 konstatuojamoji dalis). Ši teisė išplaukia iš Europos Sąjungos teisės aktų rinkinio (toliau - ES teisės aktai) 3 straipsnio 2 dalies. 15 BDAR. Duomenų subjektas, norėdamas pasinaudoti prieigos teise, gali kreiptis į mus.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

***Teisė į ištaisymą***

Pagal BDAR 16 straipsnio 1 sakinį duomenų subjektas turi teisę iš duomenų valdytojo nepagrįstai nedelsdamas reikalauti, kad duomenų valdytojas ištaisytų netikslius jo asmens duomenis. Be to, BDAR 16 straipsnio 2 sakinyje numatyta, kad duomenų subjektas, atsižvelgiant į duomenų tvarkymo tikslus, turi teisę reikalauti, kad neišsamūs asmens duomenys būtų papildyti, be kita ko, pateikiant papildomą pareiškimą. Duomenų subjektas gali kreiptis į mus, kad pasinaudotų teise ištaisyti duomenis.

***Teisė į ištrynimą (teisė būti pamirštam)***

Be to, duomenų subjektai turi teisę į duomenų ištrynimą ir teisę būti pamirštiems pagal Reglamento (EB) Nr. 17 BDAR. Šia teise taip pat galima pasinaudoti kreipiantis į mus. Tačiau šioje vietoje norėtume atkreipti dėmesį, kad ši teisė netaikoma, jei tvarkyti duomenis būtina, kad būtų įvykdyta teisinė prievolė, kuri taikoma mūsų įmonei, BDAR 17 straipsnio 3 dalies b punktas. Tai reiškia, kad prašymą ištrinti duomenis galime patenkinti tik pasibaigus teisės aktuose nustatytam saugojimo laikotarpiui.

***Teisė apriboti duomenų tvarkymą***

Pagal BDAR 18 straipsnį bet kuris duomenų subjektas turi teisę apriboti duomenų tvarkymą. Apriboti duomenų tvarkymą galima reikalauti, jei tenkinama viena iš BDAR 18 straipsnio 1 dalies a-d punktuose nustatytų sąlygų. Duomenų subjektas gali susisiekti su mumis, kad pasinaudotų teise apriboti duomenų tvarkymą.

***Teisė prieštarauti***

Be to, CK 6.2 str. 21 BDAR garantuojama teisė nesutikti. Duomenų subjektas gali susisiekti su mumis, kad pasinaudotų teise nesutikti.

***Teisė į duomenų perkeliamumą***

Straipsnis. 20 BDAR suteikia duomenų subjektui teisę į duomenų perkeliamumą. Pagal šią nuostatą duomenų subjektas BDAR 20 straipsnio 1 dalies a ir b punktuose nustatytomis sąlygomis turi teisę gauti su juo susijusius asmens duomenis, kuriuos jis pateikė duomenų valdytojui, susistemintu, įprastai naudojamu ir kompiuterio skaitomu formatu ir turi teisę perduoti tuos duomenis kitam duomenų valdytojui netrukdomas duomenų valdytojo, kuriam asmens duomenys buvo pateikti. Duomenų subjektas gali susisiekti su mumis, kad pasinaudotų teise į duomenų perkeliamumą.

## J. Kai duomenų tvarkymas grindžiamas 6 straipsnio 1 dalies a punktu arba 9 straipsnio 2 dalies a punktu, teisę bet kuriuo metu atšaukti sutikimą, nedarant poveikio sutikimu grindžiamo duomenų tvarkymo iki sutikimo atšaukimo teisėtumui (BDAR 14 straipsnio 2 dalies d punktas)

Jei asmens duomenų tvarkymas grindžiamas CK 2.5 str. 6 straipsnio 1 dalies a punktu, t. y. jei duomenų subjektas davė sutikimą tvarkyti asmens duomenis vienu ar keliais konkrečiais tikslais, arba yra grindžiamas BDAR 9 straipsnio 2 dalies a punktu, kuris reglamentuoja aiškų sutikimą tvarkyti specialių


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

kategorijų asmens duomenis, duomenų subjektas pagal BDAR 7 straipsnio 3 dalies 1 sakinį turi teisę bet kuriuo metu atšaukti savo sutikimą.

Sutikimo atšaukimas neturi įtakos duomenų tvarkymo, pagrįsto sutikimu prieš jo atšaukimą, teisėtumui, BDAR 7 straipsnio 3 dalies 2 sakinys. Atšaukti sutikimą turi būti taip pat paprasta, kaip ir duoti sutikimą, 1 straipsnis. BDAR 7 straipsnio 3 dalies 4 sakinys. Todėl atšaukti sutikimą visada galima tuo pačiu būdu, kuriuo buvo duotas sutikimas, arba bet kuriuo kitu būdu, kurį duomenų subjektas laiko paprastesniu. Šiuolaikinėje informacinėje visuomenėje bene paprasčiausias sutikimo atšaukimo būdas yra paprastas elektroninis laiškas. Jei duomenų subjektas nori atšaukti mums duotą sutikimą, pakanka mums išsiųsti paprastą elektroninį laišką. Arba duomenų subjektas gali pasirinkti bet kokį kitą būdą, kuriuo jis mums praneša apie savo sutikimo atšaukimą.

## K. Teisę pateikti skundą priežiūros institucijai (Bendrojo duomenų apsaugos reglamento 14 straipsnio 2 dalies e punktas, 77 straipsnio 1 dalis)

Kaip duomenų valdytojas, privalome pranešti duomenų subjektui apie teisę pateikti skundą priežiūros institucijai, kaip numatyta BDAR 14 straipsnio 2 dalies e punkte. Teisė pateikti skundą priežiūros institucijai reglamentuojama BDAR 77 straipsnio 1 dalyje. Pagal šią nuostatą, nepažeidžiant jokių kitų administracinių ar teisminių teisių gynimo priemonių, kiekvienas duomenų subjektas turi teisę pateikti skundą priežiūros institucijai, visų pirma valstybėje narėje, kurioje yra jo nuolatinė gyvenamoji vieta, darbo vieta arba įtariamo pažeidimo vieta, jeigu duomenų subjektas mano, kad su juo susijusių asmens duomenų tvarkymas pažeidžia Bendrąjį duomenų apsaugos reglamentą. Teisė pateikti skundą priežiūros institucijai Sąjungos teisėje buvo apribota tik taip, kad ja galima pasinaudoti tik vienoje priežiūros institucijoje (Bendrojo duomenų apsaugos reglamento 141 konstatuojamosios dalies 1 sakinys). Šia taisykle siekiama išvengti dvigubų to paties duomenų subjekto skundų tuo pačiu klausimu. Todėl, jei duomenų subjektas nori pateikti skundą dėl mūsų, prašome kreiptis tik į vieną priežiūros instituciją.

## L. Koks yra asmens duomenų kilmės šaltinis, ir, jei taikoma, ar duomenys gauti iš viešai prieinamų šaltinių (BDAR 14 straipsnio 2 dalies f punktas)

Iš esmės asmens duomenys renkami tiesiogiai iš duomenų subjekto arba bendradarbiaujant su institucija (pvz., gaunant duomenis iš oficialaus registro). Kiti duomenys apie duomenų subjektus gaunami perduodant grupės įmonių duomenis. Atsižvelgiant į šią bendrą informaciją, įvardyti tikslius šaltinius, iš kurių gaunami asmens duomenys, yra neįmanoma arba tai pareikalautų neproporcingų pastangų, kaip apibrėžta Reglamento (EB) Nr. 14 straipsnio 5 dalies b punktą. Iš esmės nerenkame asmens duomenų iš viešai prieinamų šaltinių.

Bet kuris duomenų subjektas gali bet kuriuo metu kreiptis į mus, kad gautų išsamesnės informacijos apie tikslius su juo susijusių asmens duomenų šaltinius. Jei duomenų subjektui negalima nurodyti asmens


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

duomenų kilmės, nes buvo naudotasi įvairiais šaltiniais, turėtų būti pateikta bendra informacija (BDAR 61 konstatuojamosios dalies 4 sakinys).

### M. Tai, kad esama 22 straipsnio 1 ir 4 dalyse nurodyto automatizuoto sprendimų priėmimo, įskaitant profiliavimą, ir, bent tais atvejais, prasmingą informaciją apie loginį jo pagrindimą, taip pat tokio duomenų tvarkymo reikšmę ir numatomas pasekmes duomenų subjektui (BDAR 14 straipsnio 2 dalies g punktas).

Būdami atsakinga įmonė, paprastai nenaudojame automatizuoto sprendimų priėmimo ar profiliavimo. Jei išimtiniais atvejais vykdome automatizuotą sprendimų priėmimą ar profiliavimą, informuosime duomenų subjektą atskirai arba savo privatumo politikos (mūsų interneto svetainėje) poskyryje. Šiuo atveju taikoma toliau nurodyta tvarka:

Automatinis sprendimų priėmimas, įskaitant profiliavimą, gali būti vykdomas, jei: 1) tai būtina duomenų subjekto ir mūsų sutarčiai sudaryti arba vykdyti; arba 2) tai leidžiama pagal Sąjungos arba valstybės narės teisę, kuri mums taikoma ir kurioje taip pat nustatytos tinkamos priemonės duomenų subjekto teisėms ir laisvėms bei teisėtiems interesams apsaugoti; arba 3) tai grindžiama aiškiu duomenų subjekto sutikimu.

BDAR 22 straipsnio 2 dalies a ir c punktuose nurodytais atvejais įgyvendiname tinkamas priemones duomenų subjekto teisėms ir laisvėms bei teisėtiems interesams apsaugoti. Tokiais atvejais turite teisę reikalauti, kad duomenų valdytojas imtųsi žmogiškųjų veiksmų, pareikšti savo nuomonę ir užginčyti sprendimą.

Reikšminga informacija apie susijusią logiką, taip pat tokio duomenų tvarkymo reikšmę ir numatomus padarinius duomenų subjektui pateikiama mūsų privatumo politikoje.

## III. EU-U.S. Data Privacy Framework (EU-U.S. DPF), UK Extension to the EU-U.S. DPF, Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF)

Jei mūsų organizacija yra sertifikuotas EU-U.S. Data Privacy Framework (EU-U.S. DPF) ir/arba UK Extension to the EU-U.S. DPF ir/arba Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF) narys, galioja šie punktai:

Mes laikomės EU-U.S. Data Privacy Framework (EU-U.S. DPF) ir UK Extension to the EU-U.S. DPF bei Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF), kaip nustatyta JAV prekybos departamento. Mūsų įmonė patvirtino JAV prekybos departamentui, kad laikosi EU-U.S. Data Privacy Framework Principles (EU-U.S. DPF Principles) asmens duomenų tvarkymo, gaunamų iš Europos Sąjungos ir Jungtinės Karalystės, pagal EU-U.S. DPF ir UK Extension to the EU-U.S. DPF, atžvilgiu. Mūsų įmonė


© All rights reserved by Heiko Maniero.

patvirtino JAV prekybos departamentui, kad laikosi Swiss-U.S. Data Privacy Framework Principles (Swiss-U.S. DPF Principles) asmens duomenų tvarkymo, gaunamų iš Šveicarijos, pagal Swiss-U.S. DPF, atžvilgiu. Jei mūsų privatumo politikos nuostatos prieštarauja EU-U.S. DPF Principles ir/arba Swiss-U.S. DPF Principles, pirmenybė teikiama Principles.

Norėdami sužinoti daugiau apie Data Privacy Framework (DPF) programą ir peržiūrėti mūsų sertifikatą, apsilankykite https://www.dataprivacyframework.gov/.

Kitos mūsų įmonės JAV padaliniai ar dukterinės įmonės, kurios taip pat laikosi EU-U.S. DPF Principals, įskaitant UK Extension to the EU-U.S. DPF ir Swiss-U.S. DPF Principals, jei tokių yra, nurodytos mūsų privatumo politikoje.

Vadovaujantis EU-U.S. DPF ir UK Extension to the EU-U.S. DPF bei Swiss-U.S. DPF, mūsų įmonė įsipareigoja bendradarbiauti su ES duomenų apsaugos institucijų ir Jungtinės Karalystės Information Commissioner's Office (ICO) bei Šveicarijos federaliniu duomenų apsaugos ir informacijos komisaru (EDÖB) įsteigta komisija ir laikytis jų rekomendacijų dėl neišspręstų skundų apie mūsų asmens duomenų tvarkymą, gaunamų pagal EU-U.S. DPF ir UK Extension to the EU-U.S. DPF bei Swiss-U.S. DPF.

Mes informuojame suinteresuotas šalis apie atitinkamas Europos duomenų apsaugos institucijas, atsakingas už skundų dėl mūsų organizacijos asmens duomenų tvarkymo nagrinėjimą, šio skaidrumo dokumento viršuje ir kad suteikiame suinteresuotoms šalims tinkamą ir nemokamą teisinę apsaugą.

Mes informuojame visas suinteresuotas šalis, kad mūsų įmonė yra pavaldžios Federal Trade Commission (FTC) tyrimo ir vykdymo įgaliojimams.

Suinteresuotos šalys tam tikromis sąlygomis turi galimybę pasinaudoti privalomu arbitražu. Mūsų organizacija įsipareigoja spręsti reikalavimus ir laikytis DPF-Principals I priedo sąlygų, jei suinteresuota šalis pateikia privalomo arbitražo prašymą, informuodama mūsų organizaciją ir laikydamasi I priedo procedūrų ir sąlygų.

Mes šiuo informuojame visas suinteresuotas šalis apie mūsų organizacijos atsakomybę perduodant asmens duomenis trečiosioms šalims.

Klausimams iš suinteresuotų šalių ar duomenų apsaugos priežiūros institucijų, mes paskyrėme vietinius atstovus, nurodytus šio skaidrumo dokumento viršuje.

Mes suteikiame jums galimybę pasirinkti (Opt-out), ar jūsų asmens duomenys (i) turėtų būti perduodami trečiosioms šalims, ar (ii) turėtų būti naudojami tikslui, kuris iš esmės skiriasi nuo to/tų tikslo/tikslų, kuriam/kurie buvo iš pradžių surinkti arba vėliau jūsų patvirtinti. Aiškus, gerai matomas ir lengvai prieinamas mechanizmas, leidžiantis naudotis savo pasirinkimu, yra susisiekti su mūsų duomenų apsaugos pareigūnu (DSB) el. paštu. Jūs neturite pasirinkimo galimybės, ir mes neprivalome to daryti, jei duomenys perduodami trečiajai šaliai, kuri veikia kaip mūsų vardu ir pagal mūsų nurodymus atliekantis agentas ar tvarkytojas. Tačiau mes visada sudarome sutartį su tokiu agentu ar tvarkytoju.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

Dėl jautrių duomenų (t. y. asmens duomenų, kuriuose yra informacijos apie sveikatos būklę, rasinę ar etninę kilmę, politines pažiūras, religinius ar filosofinius įsitikinimus, narystę profesinėje sąjungoje arba informaciją apie asmens lytinį gyvenimą) mes gauname jūsų aiškų sutikimą (Opt-in), kai šie duomenys (i) perduodami trečiosioms šalims arba (ii) naudojami kitam tikslui, nei buvo iš pradžių surinkti arba kuriam jūs vėliau sutikote, pasirinkdami Opt-in. Be to, mes visus asmens duomenis, kuriuos gauname iš trečiųjų šalių, laikome jautriais, jei trečioji šalis juos identifikuoja ir tvarko kaip jautrius.

Mes informuojame jus šiuo apie reikalavimą atskleisti asmens duomenis reaguojant į teisėtus valdžios institucijų prašymus, įskaitant nacionalinio saugumo ar teisėsaugos reikalavimų vykdymą.

Perduodant asmens duomenis trečiajai šaliai, kuri veikia kaip valdytojas, mes laikomės Principals apie pranešimą ir pasirinkimą. Be to, mes sudarome sutartį su trečiąja šalimi, atsakinga už tvarkymą, kurioje nustatyta, kad šie duomenys gali būti tvarkomi tik ribotais ir apibrėžtais tikslais, atsižvelgiant į jūsų duotą sutikimą, ir kad gavėjas turi užtikrinti tokį pat apsaugos lygį, kaip DPF Principals ir mus informuoti, jei nustato, kad nebegali vykdyti šio įsipareigojimo. Sutartis numato, kad trečioji šalis, atsakinga už tvarkymą, nutraukia tvarkymą arba imasi kitų tinkamų ir adekvačių priemonių situacijai ištaisyti, jei toks nustatymas atliekamas.

Perduodant asmens duomenis trečiajai šaliai, kuri veikia kaip agentas arba tvarkytojas, (i) mes perduodame šiuos duomenis tik ribotais ir apibrėžtais tikslais; (ii) mes užtikriname, kad agentas arba tvarkytojas privalo užtikrinti bent jau tokį patį duomenų apsaugos lygį, kokį reikalauja DPF-Principals; (iii) mes imsimės tinkamų ir adekvačių priemonių, kad užtikrintume, jog agentas arba tvarkytojas iš tikrųjų tvarko perduotus asmens duomenis tokiu būdu, kuris atitinka mūsų įsipareigojimus pagal DPF-Principals; (iv) mes reikalaujame, kad agentas arba tvarkytojas informuotų mūsų organizaciją, jei nustato, kad nebegali užtikrinti tokio pat apsaugos lygio, kokį numato DPF-Principals; (v) gavę tokį pranešimą, taip pat ir pagal (iv), mes imsimės tinkamų ir adekvačių veiksmų, kad nutrauktume neteisėtą tvarkymą ir ištaisytume situaciją; ir (vi) DPF Department prašymu pateiksime santrauką arba reprezentatyvų atitinkamų duomenų apsaugos nuostatų iš mūsų sutarties su šiuo agentu pavyzdį.

Vadovaujantis EU-U.S. DPF ir/arba UK Extension to the EU-U.S. DPF ir/arba Swiss-U.S. DPF, mūsų organizacija įsipareigoja bendradarbiauti su ES duomenų apsaugos institucijų ir Jungtinės Karalystės Information Commissioner's Office (ICO) arba Šveicarijos federalinio duomenų apsaugos ir informacijos komisaro (EDÖB) įsteigta komisija ir laikytis jų rekomendacijų dėl neišspręstų skundų apie mūsų elgesį su asmens duomenimis, gaunamais pagal EU-U.S. DPF ir UK Extension to the EU-U.S. DPF ir Swiss-U.S. DPF, susijusius su darbo santykiais.

Visi duomenų subjektai, kurie laikinai yra Europos Sąjungoje (ES), Europos ekonominėje erdvėje (EEE) ar Jungtinėje Karalystėje arba kurių nuolatinė ar įprastinė gyvenamoji vieta yra ten, turi teisę naudotis mūsų skaidrumo dokumente paskelbtomis teisėmis ir duomenų subjekto teisėmis, kurios taip pat kyla iš BDAR 15-22 straipsnių, įskaitant teisę susipažinti su asmens duomenimis. Šią informaciją pateikėme visomis ES ir EEE kalbomis. Versija anglų kalba taikoma Jungtinei Karalystei.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

Visi duomenų subjektai, kurie laikinai gyvena Šveicarijoje arba kurių nuolatinė ar įprastinė gyvenamoji vieta yra Šveicarijoje, turi teises ir duomenų subjekto teises pagal Šveicarijos duomenų apsaugos įstatymą (DPA) ir Šveicarijos duomenų apsaugos reglamentą (DPR), kurie skelbiami mūsų skaidrumo dokumente, įskaitant teisę susipažinti su asmens duomenimis. Šią informaciją pateikėme trimis oficialiomis Šveicarijos kalbomis (vokiečių, italų ir prancūzų).


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

# IRISH: Faisnéis faoi Phróiseáil Sonraí Pearsanta (Airteagal 13, 14 GDPR)

A dhuine uasail nó a bhean uasail,

Tá cosaint speisialta tuillte ag sonraí pearsanta gach duine aonair atá i gcaidreamh conarthach, réamhchonarthach nó eile lenár gcuideachta. Is é an sprioc atá againn ár leibhéal cosanta sonraí a choinneáil ar ardchaighdeán. Dá bhrí sin, táimid i go rialta ag forbairt ár gcoincheapa um chosaint sonraí agus slándáil sonraí.

Ar ndóigh, comhlíonaimid na forálacha reachtúla maidir le cosaint sonraí. De réir Airteagal 13, 14 GDPR, comhlíonann rialaitheoirí ceanglais shonracha faisnéise agus iad ag bailiú sonraí pearsanta. Comhlíonann an doiciméad seo na hoibleagáidí sin.

Tá téarmaíocht na rialachán dlíthiúil casta. Ar an drochuair, níorbh fhéidir úsáid téarmaí dlí a ligean thar ceal agus an doiciméad seo á ullmhú. Mar sin, ba mhaith linn a chur in iúl go bhfuil fáilte romhat teagmháil a dhéanamh linn i gcónaí maidir le gach ceist a bhaineann leis an doiciméad seo, na téarmaí nó na foirmlí a úsáideadh.

## I. An fhaisnéis a bheidh le soláthar i gcás go mbailítear sonraí ón ábhar sonraí (Airteagal 13 GDPR)

### A. Céannacht agus sonraí teagmhála an rialaitheora agus, i gcás inarb ábhartha, céannacht agus sonraí teagmhála ionadaí an rialaitheora (Airteagal 13(1) lit. a GDPR)

Féach thuas

### B. Sonraí teagmhála an oifigigh cosanta sonraí, i gcás inarb ábhartha (Airteagal 13(1) lit. b GDPR)

Féach thuas

### C. Críocha na próiseála dá bhfuil na sonraí pearsanta beartaithe chomh maith leis an mbunús dlí don phróiseáil (Airteagal 13(1) lit. c GDPR)

Is é an cuspóir atá le sonraí pearsanta a phróiseáil ná láimhseáil na n-oibríochtaí go léir a bhaineann leis an rialaitheoir, le custaiméirí, le custaiméirí ionchasacha, le comhpháirtithe gnó nó le caidreamh


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

conarthach nó réamhchonarthach eile idir na grúpaí ainmnithe (sa chiall is leithne) nó oibleagáidí dlíthiúla an rialaitheora.

Ealaín. 6(1) lit. feidhmíonn GDPR mar bhunús dlí le haghaidh oibríochtaí próiseála a bhfaighimid toiliú ina leith chun críche próiseála ar leith. Más gá sonraí pearsanta a phróiseáil chun conradh a chomhlíonadh a bhfuil an t-ábhar sonraí ina pháirtí ann, mar atá an cás, mar shampla, nuair a bhíonn gá le hoibríochtaí próiseála chun earraí a sholáthar nó chun aon seirbhís eile a sholáthar, déantar an phróiseáil a dhéanamh. bunaithe ar Airteagal 6(1) lit. b GDPR. Baineann an rud céanna le hoibríochtaí próiseála den sórt sin atá riachtanach chun bearta réamhchonarthacha a dhéanamh, mar shampla i gcás fiosrúchán a bhaineann lenár dtáirgí nó ár seirbhísí. An bhfuil ár gcuideachta faoi réir oibleagáid dhlíthiúil faoina bhfuil gá le próiseáil sonraí pearsanta, mar shampla chun oibleagáidí cánach a chomhlíonadh, tá an phróiseáil bunaithe ar Airteagal 6(1) lit. c GDPR.

I gcásanna neamhchoitianta, d'fhéadfadh go mbeadh gá le próiseáil sonraí pearsanta chun leasanna ríthábhachtacha an ábhair sonraí nó duine nádúrtha eile a chosaint. Bheadh sé seo amhlaidh, mar shampla, dá ndéanfaí cuairteoir a ghortú inár gcuideachta agus dá mbeadh a ainm, a aois, a shonraí árachais sláinte nó faisnéis ríthábhachtach eile le cur ar aghaidh chuig dochtúir, ospidéal nó tríú páirtí eile. Ansin bheadh an phróiseáil bunaithe ar Airteagal 6(1) lit. d GDPR.

I gcás inar gá an phróiseáil chun cúram a chur i gcrích ar mhaithe le leas an phobail nó i bhfeidhmiú údaráis oifigiúil atá dílsithe don rialaitheoir, is é Airt. 6(1) lit. agus GDPR.

Ar deireadh, d'fhéadfaí oibríochtaí próiseála a bhunú ar Airteagal 6(1) lit. f GDPR. Úsáidtear an bunús dlí seo le haghaidh oibríochtaí próiseála nach bhfuil clúdaithe ag aon cheann de na forais dlí thuasluaite, má tá próiseáil riachtanach chun críocha na leasanna dlisteanacha atá á saothrú ag ár gcuideachta nó ag tríú páirtí, ach amháin i gcás ina sáraítear leasanna den sórt sin ag na leasanna. nó cearta agus saoirsí bunúsacha an duine is ábhar do na sonraí a éilíonn cosaint sonraí pearsanta. Tá oibríochtaí próiseála den sórt sin ceadaithe go háirithe toisc go bhfuil siad luaite go sonrach ag an reachtóir Eorpach. Mheas sé go bhféadfaí leas dlisteanach a ghlacadh más cliant de chuid an rialaitheora é an t-ábhar sonraí (Aithris 47 Pianbhreith 2 GDPR).

## D. I gcás ina bhfuil an phróiseáil bunaithe ar phointe (f) d'Airteagal 6(1), na leasanna dlisteanacha atá á saothrú ag an rialaitheoir nó ag triú páirtí (Airteagal 13(1) lit. d GDPR)

I gcás ina bhfuil próiseáil sonraí pearsanta bunaithe ar Airteagal 6(1) lit. f Is é ár leas dlisteanach an GDPR ár ngnó a dhéanamh ar mhaithe le leas ár bhfostaithe go léir agus na scairshealbhóirí.

## E. I gcás inarb infheidhme, faighteoirí na sonraí pearsanta nó catagóirí fhaighteoirí na sonraí pearsanta, más ann dóibh (Airteagal 13(1) lit. e GDPR)


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

Údaráis phoiblí

Comhlachtaí seachtracha

Tuilleadh comhlachtaí seachtracha

Próiseáil inmheánach

Próiseáil inghrúpa

Comhlachtaí eile

Foilsítear liosta dár bpróiseálaithe agus dár bhfaighteoirí sonraí i dtríú tíortha agus, más infheidhme, eagraíochtaí idirnáisiúnta ar ár suíomh Gréasáin nó is féidir é a iarraidh orainn saor in aisce. Déan teagmháil lenár n-oifigeach cosanta sonraí le do thoil chun an liosta seo a iarraidh.

## F. I gcás inarb infheidhme, go bhfuil sé beartaithe ag an rialaitheoir sonraí pearsanta a aistriú chuig tríú tír nó chuig eagraíocht idirnáisiúnta agus cibé arb ann nó nach ann do chinneadh leordhóthanachta ón gCoimisiún, nó i gcás na n-aistrithe dá dtagraítear in Airteagal 46 nó in Airteagal 47, nó sa dara fomhír d'Airteagal 49(1), tagairt do na coimircí iomchuí nó oiriúnacha agus na bealaí inar féidir chun cóip díobh a fháil nó an áit inar cuireadh iad ar fáil (Airteagal 13(1) lit. f, 46(1), 46(2) lit. c GDPR)

Féadfaidh gach cuideachta agus brainse atá mar chuid dár ngrúpa (dá ngairtear “grúpchuideachtaí” anseo feasta) a bhfuil a n-áit ghnó nó oifig i dtríú tír bheith ina mbaill d’fhaighteoirí sonraí pearsanta. Is féidir liosta de na cuideachtaí grúpa nó na faighteoirí go léir a iarraidh uainn.

De réir Airteagal 46(1) GDPR ní fhéadfaidh rialaitheoir nó próiseálaí sonraí pearsanta a aistriú chuig tríú tír ach amháin má tá coimircí iomchuí curtha ar fáil ag an rialaitheoir nó ag an bpróiseálaí, agus ar an gcoinníoll go bhfuil cearta infhorghníomhaithe damhna sonraí agus leigheasanna dlí éifeachtacha ar fáil do dhaoine is ábhar do na sonraí. Féadfar coimircí iomchuí a sholáthar gan aon údarú sonrach a éileamh ó údarás maoirseachta trí bhíthin clásail chaighdeánacha chonarthacha, Airteagal 46(2) lit. c GDPR.

Comhaontaítear clásail chaighdeánacha chonarthacha an Aontais Eorpaigh nó cosaintí iomchuí eile le gach faighteoir ó thríú tíortha roimh an gcéad tarchur sonraí pearsanta. Dá bhrí sin, áirithítear go ráthaítear cosaintí iomchuí, cearta infhorghníomhaithe ábhar sonraí agus leigheasanna éifeachtacha dlí do dhaoine is ábhar do na sonraí. Is féidir le gach ábhar sonraí cóip de na clásail chaighdeánacha chonarthacha a fháil uainn. Tá na clásail chaighdeánacha chonarthacha ar fáil freisin in Iris Oifigiúil an Aontais Eorpaigh.

Tugann Airteagal 45(3) den Rialachán Ginearálta um Chosaint Sonraí (GDPR) an chumhacht don Choimisiún Eorpach a chinneadh, trí bhíthin gnímh cur chun feidhme, go n-áirithíonn tír nach bhfuil san AE leibhéal leordhóthanach cosanta. Ciallaíonn sé seo leibhéal cosanta do shonraí pearsanta atá


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

comhionann go bunúsach leis an leibhéal cosanta laistigh den AE. Is é éifeacht na gcinntí leordhóthanachta gur féidir le sonraí pearsanta sreabhadh gan bhac ón AE (agus ón Iorua, ó Lichtinstéin agus ón Íoslainn) chuig tríú tír gan a thuilleadh constaicí. Tá rialacha comhchosúla ann don Ríocht Aontaithe, don Eilvéis agus do thíortha áirithe eile.

I gcás inar chinn an Coimisiún Eorpach nó rialtas tíre eile go n-áirithíonn tríú tír leibhéal leordhóthanach cosanta, agus go bhfuil Creat bailí i bhfeidhm (m.sh. EU-U.S. Data Privacy Framework, Swiss-U.S. Data Privacy Framework, UK Extension to the EU-U.S. Data Privacy Framework), tá gach aistriú a dhéanaimid chuig comhaltaí creata den sórt sin (m.sh. eintitis fhéindheimhnithe) bunaithe go heisiach ar bhallraíocht an eintitis sin sa chreat faoi seach. Sa chás go bhfuilimid nó ceann dár ngrúpa-eintitis mar bhall de chreat den sórt sin, tá gach aistriú chugainn nó chuig ár ngrúpa eintiteas bunaithe go heisiach ar bhallraíocht na n-eintiteas sa chreat sin.

Is féidir le haon ábhar sonraí cóip de na creataí a fháil uainn. Ina theannta sin, tá na creataí ar fáil freisin in Iris Oifigiúil an Aontais Eorpaigh nó sna hábhair dhlíthiúla a foilsíodh nó ar shuíomhanna gréasáin na n-údarás maoirseachta nó na n-údarás inniúil nó na n-institiúidí inniúla eile.

## G. Tréimhse stórála na sonraí pearsanta, nó murarb indéanta sin, na critéir a úsáidtear chun an tréimhse sin a chinneadh (Airteagal 13(2) lit. a GDPR).

Is iad na critéir a úsáidtear chun tréimhse stórála sonraí pearsanta a chinneadh ná an tréimhse choinneála reachtúil faoi seach. Tar éis don tréimhse sin dul in éag, scriostar na sonraí comhfhreagracha go rialta, fad nach bhfuil gá leo a thuilleadh chun an conradh a chomhlíonadh nó chun conradh a thionscnamh.

Mura bhfuil aon tréimhse choinneála reachtúil ann, is é an critéar an tréimhse choinneála chonarthach nó inmheánach.

## H. Is ann don cheart rochtain ar shonraí pearsanta a bhaineann leis ábhar sonraí agus go ndéanfaí ceartú nó léirscriosadh na sonraí sin, a iarraidh ar an rialaitheoir, nó srianadh ar phróiseáil maidir leis an ábhar sonraí agus is ann don cheart agóid a dhéanamh i gcoinne na próiseála chomh maith leis an gceart chun iniomparthacht sonraí (Airteagal 13(2) lit. b. GDPR)

Tá na cearta seo a leanas ag gach ábhar sonraí:

***Ceart rochtana***

Tá sé de cheart ag gach ábhar sonraí rochtain a fháil ar na sonraí pearsanta a bhaineann leis nó léi. Síneann an ceart rochtana chuig na sonraí go léir a phróiseálann muid. Is féidir an ceart a fheidhmiú go héasca agus ag eatraimh réasúnacha, chun a bheith feasach ar dhlíthiúlacht na próiseála agus chun a

fhíorú (Aithris 63 GDPR). Eascraíonn an ceart seo as Art. 15 GDPR. Féadfaidh an t-ábhar sonraí teagmháil a dhéanamh linn chun an ceart rochtana a fheidhmiú.

***Ceart chun ceartúcháin***

De réir Airteagal 16 Pianbhreith 1 GDPR tá an ceart ag an ábhar sonraí ceartú sonraí pearsanta míchruinn a bhaineann leis nó léi a fháil ón rialaitheoir gan mhoill mhíchuí. Ina theannta sin, foráiltear le hAirteagal 16 Pianbhreith 2 GDPR go bhfuil an t-ábhar sonraí i dteideal, ag cur críocha na próiseála san áireamh, sonraí pearsanta neamhiomlána a bheith comhlánaithe, lena n-áirítear trí bhíthin ráiteas forlíontach a sholáthar. Féadfaidh an t-ábhar sonraí teagmháil a dhéanamh linn chun an ceart ceartúcháin a fheidhmiú.

***An ceart chun scriosta (ceart chun dearmad a dhéanamh)***

Ina theannta sin, tá daoine is ábhar do na sonraí i dteideal ceart scriosta agus chun dearmad a dhéanamh orthu faoi Airteagal 17 GDPR. Is féidir an ceart seo a fheidhmiú freisin trí theagmháil a dhéanamh linn. Ag an bpointe seo, áfach, ba mhaith linn a chur in iúl nach bhfuil feidhm ag an gceart seo a mhéid is gá an phróiseáil chun oibleagáid dhlíthiúil a bhfuil ár gcuideachta faoina réir a chomhlíonadh, Airteagal 17(3) lit. b GDPR. Ciallaíonn sé seo nach féidir linn iarratas a scriosadh a cheadú ach amháin tar éis don tréimhse choinneála reachtúil dul in éag.

***An ceart chun próiseáil a shrianadh***

De réir Airteagal 18 GDPR tá aon ábhar sonraí i dteideal srianta próiseála. Féadfar srianadh ar phróiseáil a éileamh má tá ceann de na coinníollacha atá leagtha amach in Airteagal 18(1) lit. ad go bhfuil an GDPR comhlíonta. Féadfaidh an t-ábhar sonraí teagmháil a dhéanamh linn chun an ceart chun srianadh ar phróiseáil a fheidhmiú.

***Ceart agóid a dhéanamh***

Ina theannta sin, Art. 21 Ráthaíonn GDPR an ceart agóide. Féadfaidh an t-ábhar sonraí teagmháil a dhéanamh linn chun an ceart agóide a fheidhmiú.

***Ceart chun iniomparthacht sonraí***

Ealaín. Tugann 20 GDPR an ceart chun iniomparthacht sonraí don duine is ábhar do na sonraí. Faoin bhforáil seo, tá an duine is ábhar do na sonraí faoi na coinníollacha atá leagtha síos in Airteagal 20(1) lit. a agus b GDPR an ceart chun na sonraí pearsanta a bhaineann leis nó léi, a sholáthair sé nó sí do rialaitheoir, a fháil i bhformáid struchtúrtha, a úsáidtear go coitianta agus atá inléite ag meaisín agus an ceart chun na sonraí sin a tharchur chuig rialaitheoir eile gan bhac. ón rialaitheoir ar soláthraíodh na sonraí pearsanta dó. Féadfaidh an t-ábhar sonraí teagmháil a dhéanamh linn chun an ceart chun iniomparthacht sonraí a fheidhmiú.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

I. I gcás ina bhfuil an phróiseáil bunaithe ar phointe (a) d'Airteagal 6(1) nó ar phointe (a) d'Airteagal 9(2), beidh sé de cheart an toiliú a tharraingt siar tráth ar bith, gan difear a dhéanamh do dhlíthiúlacht na próiseála atá bunaithe ar an toiliú sin a fháil roimh an tarraingt siar a dhéanamh (Airteagal 13(2) lit. c GDPR)

Má tá próiseáil sonraí pearsanta bunaithe ar Airteagal 6(1) lit. GDPR, is é sin an cás, má tá toiliú tugtha ag an duine is ábhar do na sonraí le próiseáil sonraí pearsanta chun críoch sonrach amháin nó níos mó nó an bhfuil sé bunaithe ar Airteagal 9(2) lit. GDPR, a rialaíonn toiliú sainráite le próiseáil catagóirí speisialta sonraí pearsanta, tá sé de cheart ag an ábhar sonraí de réir Airteagal 7(3) Pianbhreith 1 GDPR a thoiliú nó a toiliú a tharraingt siar tráth ar bith.

Ní dhéanfaidh sé difear do dhlíthiúlacht na próiseála atá bunaithe ar an toiliú roimh é a tharraingt siar, Airteagal 7(3) Pianbhreith 2 GDPR. Beidh sé chomh héasca tarraingt siar agus toiliú a thabhairt, Airteagal 7(3) Pianbhreith 4 GDPR. Dá bhrí sin, is féidir i gcónaí an toiliú a tharraingt siar ar an mbealach céanna agus a tugadh an toiliú nó ar aon bhealach eile, a mheasann an t-ábhar sonraí a bheith níos simplí. I sochaí faisnéise an lae inniu , is dócha gurb é an bealach is simplí toiliú a tharraingt siar ná ríomhphost simplí. Más mian leis an ábhar sonraí an toiliú a tugadh dúinn a tharraingt siar, is leor ríomhphost simplí a chur chugainn. Mar mhalairt air sin, féadfaidh an t-ábhar sonraí bealach ar bith eile a roghnú chun a toiliú a tharraingt siar a chur in iúl dúinn.

## J. An ceart gearán a thaisceadh le húdarás maoirseachta (Airteagal 13(2) lit. d, 77(1) GDPR)

Mar an rialaitheoir, tá oibleagáid orainn fógra a thabhairt don ábhar sonraí maidir leis an gceart chun gearán a dhéanamh le húdarás maoirseachta, Airteagal 13(2) lit. d GDPR. Tá an ceart chun gearán a dhéanamh le húdarás maoirseachta arna rialú ag Airteagal 77(1) GDPR. De réir na forála seo, gan dochar d'aon leigheas riaracháin nó breithiúnach eile, beidh an ceart ag gach duine is ábhar do na sonraí gearán a dhéanamh le húdarás maoirseachta, go háirithe sa Bhallstát ina bhfuil gnáthchónaí, áit oibre nó áit oibre aige nó aici. an sárú líomhnaithe má mheasann an duine is ábhar do na sonraí go sáraíonn próiseáil sonraí pearsanta a bhaineann leis nó léi an Rialachán Ginearálta maidir le Cosaint Sonraí. Ní raibh an ceart chun gearán a dhéanamh le húdarás maoirseachta teoranta ach amháin ag dlí an Aontais sa chaoi is nach bhféadfar é a fheidhmiú ach amháin os comhair údaráis mhaoirseachta aonair (Aithris 141 Pianbhreith 1 GDPR). Tá an riail seo beartaithe chun gearáin dhúbailte ón ábhar sonraí céanna a sheachaint san ábhar céanna. Más mian le duine is ábhar do na sonraí gearán a dhéanamh fúinn, d'iarramar mar sin teagmháil a dhéanamh le húdarás maoirseachta amháin.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## K. An ceanglas reachtach nó conarthach é an ceanglas sonraí pearsanta a sholáthar, nó an ceanglas é ar gá é le go ndéanfaí i gconradh, agus an bhfuil oibleagáid ar an ábhar sonraí na sonraí pearsanta sin a sholáthar mar aon leis na hiarmhairtí a d'fhéadfadh a bheith ann i gcás nár soláthraíodh na sonraí sin; agus (Airteagal 13(2) lit. e GDPR)

Soiléirímid go bhfuil soláthar sonraí pearsanta riachtanach go páirteach de réir an dlí ( m.sh. rialacháin chánach) nó go bhféadfadh sé tarlú freisin ó fhorálacha conartha (m.sh. faisnéis ar an gcomhpháirtí conarthach).

Uaireanta b'fhéidir go mbeadh sé riachtanach conradh a thabhairt i gcrích go soláthraíonn an damhna sonraí sonraí pearsanta dúinn, nach mór dúinn a phróiseáil ina dhiaidh sin. Tá oibleagáid ar an ábhar sonraí, mar shampla, sonraí pearsanta a sholáthar dúinn nuair a shíníonn ár gcuideachta conradh leis nó léi. Bheadh sé mar thoradh ar neamhsholáthar na sonraí pearsanta nach bhféadfaí an conradh leis an ábhar sonraí a thabhairt i gcrích.

Sula gcuireann an t-ábhar sonraí sonraí pearsanta ar fáil, ní mór don ábhar sonraí teagmháil a dhéanamh linn. Soiléirímid don duine is ábhar do na sonraí cibé an bhfuil gá le soláthar na sonraí pearsanta de réir an dlí nó an chonartha nó an bhfuil gá leis chun an conradh a thabhairt i gcrích, an bhfuil oibleagáid ann na sonraí pearsanta a sholáthar agus na hiarmhairtí a bhaineann le neamhsholáthar an chonartha. sonraí.

## L. Is ann do chinnteoireacht uathoibrithe, lena n-áirítear próifíliú, dá dtagraítear in Airteagal 22(1) agus (4) agus, sna cásanna sin ar a laghad, d'fhaisnéis fhónta faoin loighic a bheidh i gceist, chomh maith le suntasacht na próiseála sin agus na hiarmhairtí a mheastar a bheadh aici ar an ábhar sonraí (Airteagal 13(2) lit. f GDPR)

Mar chuideachta fhreagrach, de ghnáth ní úsáidimid cinnteoireacht nó próifíliú uathoibrithe. Más rud é, i gcásanna eisceachtúla, go ndéanaimid cinnteoireacht nó próifíliú uathoibrithe, cuirfimid an t-ábhar sonraí ar an eolas go leithleach nó trí fho-alt inár mbeartas príobháideachta (ar ár suíomh Gréasáin). Sa chás seo, tá feidhm ag an méid seo a leanas:

Féadfaidh cinnteoireacht uathoibrithe - lena n-áirítear próifíliú - tarlú (1) má tá sé seo riachtanach chun conradh a dhéanamh, nó chun conradh a chomhlíonadh idir an duine is ábhar do na sonraí agus sinne, nó (2) má údaraítear é seo le dlí an Aontais nó an Bhallstáit lena mbaineann muid. atá faoina réir agus a leagann síos freisin bearta oiriúnacha chun cearta agus saoirsí agus leasanna dlisteanacha an duine is ábhar do na sonraí a chosaint; nó (3) tá sé seo bunaithe ar thoiliú sainráite an ábhair sonraí.

Sna cásanna dá dtagraítear in Airteagal 22(2)(a) agus (c) den GDPR, cuirfimid bearta oiriúnacha i bhfeidhm chun cearta agus saoirsí agus leasanna dlisteanacha an duine is ábhar do na sonraí a chosaint.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

Sna cásanna seo, tá sé de cheart agat idirghabháil dhaonna a fháil ó thaobh an rialaitheora, do dhearcadh a chur in iúl agus cur in aghaidh an chinnidh.

Tá faisnéis bhríoch faoin loighic atá i gceist, chomh maith leis an tábhacht agus na hiarmhairtí a shamhlaítear lena leithéid de phróiseáil don ábhar sonraí leagtha amach inár mbeartas príobháideachta.

## II. An fhaisnéis a bheidh le soláthar i gcás nár bailíodh na sonraí ón ábhar sonraí (Airteagal 14 GDPR)

### A. Céannacht agus sonraí teagmhála an rialaitheora agus, i gcás inarb infheidhme, céannacht agus sonraí teagmhála ionadaí an rialaitheora (Airteagal 14(1) lit. a GDPR)

Féach thuas

### B. Sonraí teagmhála an oifigigh cosanta sonraí, más ann dó, más infheidhme (Airteagal 14(1) lit. b GDPR)

Féach thuas

### C. Críocha na próiseála dá bhfuil na sonraí pearsanta beartaithe chomh maith leis an mbunús dlí don phróiseáil (Airteagal 14(1) lit. c GDPR)

Is é an cuspóir atá le sonraí pearsanta a phróiseáil ná láimhseáil na n-oibríochtaí go léir a bhaineann leis an rialaitheoir, le custaiméirí, le custaiméirí ionchasacha, le comhpháirtithe gnó nó le caidreamh conarthach nó réamhchonarthach eile idir na grúpaí ainmnithe (sa chiall is leithne) nó oibleagáidí dlíthiúla an rialaitheora.

Más gá sonraí pearsanta a phróiseáil chun conradh a chomhlíonadh a bhfuil an t-ábhar sonraí ina pháirtí ann, mar atá an cás, mar shampla, nuair a bhíonn gá le hoibríochtaí próiseála chun earraí a sholáthar nó chun aon seirbhís eile a sholáthar, déantar an phróiseáil a dhéanamh. bunaithe ar Airteagal 6(1) lit. b GDPR. Baineann an rud céanna le hoibríochtaí próiseála den sórt sin atá riachtanach chun bearta réamhchonarthacha a dhéanamh, mar shampla i gcás fiosrúchán a bhaineann lenár dtáirgí nó ár seirbhísí. An bhfuil ár gcuideachta faoi réir oibleagáid dhlíthiúil faoina bhfuil gá le próiseáil sonraí pearsanta, mar shampla chun oibleagáidí cánach a chomhlíonadh, tá an phróiseáil bunaithe ar Airteagal 6(1) lit. c GDPR.

I gcásanna neamhchoitianta, d'fhéadfadh go mbeadh gá le próiseáil sonraí pearsanta chun leasanna ríthábhachtacha an ábhair sonraí nó duine nádúrtha eile a chosaint. Bheadh sé seo amhlaidh, mar shampla, dá ndéanfaí cuairteoir a ghortú inár gcuideachta agus dá mbeadh a ainm, a aois, a shonraí


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

árachais sláinte nó faisnéis ríthábhachtach eile le cur ar aghaidh chuig dochtúir, ospidéal nó tríú páirtí eile. Ansin bheadh an phróiseáil bunaithe ar Airteagal 6(1) lit. d GDPR.

I gcás inar gá an phróiseáil chun cúram a chur i gcrích ar mhaithe le leas an phobail nó i bhfeidhmiú údaráis oifigiúil atá dílsithe don rialaitheoir, is é Airt. 6(1) lit. agus GDPR.

Ar deireadh, d'fhéadfaí oibríochtaí próiseála a bhunú ar Airteagal 6(1) lit. f GDPR. Úsáidtear an bunús dlí seo le haghaidh oibríochtaí próiseála nach bhfuil clúdaithe ag aon cheann de na forais dlí thuasluaite, má tá próiseáil riachtanach chun críocha na leasanna dlisteanacha atá á saothrú ag ár gcuideachta nó ag tríú páirtí, ach amháin i gcás ina sáraítear leasanna den sórt sin ag na leasanna. nó cearta agus saoirsí bunúsacha an duine is ábhar do na sonraí a éilíonn cosaint sonraí pearsanta. Tá oibríochtaí próiseála den sórt sin ceadaithe go háirithe toisc go bhfuil siad luaite go sonrach ag an reachtóir Eorpach. Mheas sé go bhféadfaí leas dlisteanach a ghlacadh más cliant de chuid an rialaitheora é an t-ábhar sonraí (Aithris 47 Pianbhreith 2 GDPR).

## D. Catagóirí na sonraí pearsanta lena mbaineann (Airteagal 14(1) lit. d GDPR)

Sonraí custaiméirí

Sonraí custaiméirí féideartha

Sonraí na bhfostaithe

Sonraí soláthraithe

## E. Faighteoirí nó catagóirí fhaighteoirí na sonraí pearsanta, más ann dóibh (Airteagal 14(1) lit. e GDPR)

Údaráis phoiblí

Comhlachtaí seachtracha

Tuilleadh comhlachtaí seachtracha

Próiseáil inmheánach

Próiseáil inghrúpa

Comhlachtaí eile


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

Foilsítear liosta dár bpróiseálaithe agus dár bhfaighteoirí sonraí i dtríú tíortha agus, más infheidhme, eagraíochtaí idirnáisiúnta ar ár suíomh Gréasáin nó is féidir é a iarraidh orainn saor in aisce. Déan teagmháil lenár n-oifigeach cosanta sonraí le do thoil chun an liosta seo a iarraidh.

## F. I gcás inarb infheidhme, go bhfuil sé beartaithe ag an rialaitheoir sonraí pearsanta a aistriú chuig faighteoir i dtríú tír nó in eagraíocht idirnáisiúnta agus cibé arb ann nó nach ann do chinneadh leordhóthanachta, nó i gcás na n-aistrithe dá dtagraítear in Airteagal 46 nó in Airteagal 47, nó sa dara fomhír d'Airteagal 49(1), tagairt do na coimircí iomchuí nó oiriúnacha agus na bealaí chun cóip díobh a fháil nó cá bhfuil siad ar fáil (Airteagal 14(1) lit. f, 46(1), 46(2) lit. c GDPR)

Féadfaidh gach cuideachta agus brainse atá mar chuid dár ngrúpa (dá ngairtear “grúpchuideachtaí” anseo feasta) a bhfuil a n-áit ghnó nó oifig i dtríú tír bheith ina mbaill d’fhaighteoirí sonraí pearsanta. Is féidir liosta de na cuideachtaí grúpa go léir a iarraidh uainn.

De réir Airteagal 46(1) GDPR ní fhéadfaidh rialaitheoir nó próiseálaí sonraí pearsanta a aistriú chuig tríú tír ach amháin má tá coimircí iomchuí curtha ar fáil ag an rialaitheoir nó ag an bpróiseálaí, agus ar an gcoinníoll go bhfuil cearta infhorghníomhaithe damhna sonraí agus leigheasanna dlí éifeachtacha ar fáil do dhaoine is ábhar do na sonraí. Féadfar coimircí iomchuí a sholáthar gan aon údarú sonrach a éileamh ó údarás maoirseachta trí bhíthin clásail chaighdeánacha um chosaint sonraí, Airteagal 46(2) lit. c GDPR.

Comhaontaítear clásail chaighdeánacha chonarthacha an Aontais Eorpaigh nó cosaintí iomchuí eile le gach faighteoir ó thríú tíortha roimh an gcéad tarchur sonraí pearsanta. Dá bhrí sin, áirithítear go ráthaítear cosaintí iomchuí, cearta infhorghníomhaithe ábhar sonraí agus leigheasanna éifeachtacha dlí do dhaoine is ábhar do na sonraí. Is féidir le gach ábhar sonraí cóip de na clásail chaighdeánacha chonarthacha a fháil uainn. Tá na clásail chaighdeánacha chonarthacha ar fáil freisin in Iris Oifigiúil an Aontais Eorpaigh.

Tugann Airteagal 45(3) den Rialachán Ginearálta um Chosaint Sonraí (GDPR) an chumhacht don Choimisiún Eorpach a chinneadh, trí bhíthin gnímh cur chun feidhme, go n-áirithíonn tír nach bhfuil san AE leibhéal leordhóthanach cosanta. Ciallaíonn sé seo leibhéal cosanta do shonraí pearsanta atá comhionann go bunúsach leis an leibhéal cosanta laistigh den AE. Is é éifeacht na gcinntí leordhóthanachta gur féidir le sonraí pearsanta sreabhadh gan bhac ón AE (agus ón Iorua, ó Lichtinstéin agus ón Íoslainn) chuig tríú tír gan a thuilleadh constaicí. Tá rialacha comhchosúla ann don Ríocht Aontaithe, don Eilvéis agus do thíortha áirithe eile.

I gcás inar chinn an Coimisiún Eorpach nó rialtas tíre eile go n-áirithíonn tríú tír leibhéal leordhóthanach cosanta, agus go bhfuil Creat bailí i bhfeidhm (m.sh. EU-U.S. Data Privacy Framework, Swiss-U.S. Data Privacy Framework, UK Extension to the EU-U.S. Data Privacy Framework), tá gach aistriú a dhéanaimid chuig comhaltaí creata den sórt sin (m.sh. eintitis fhéindheimhnithe) bunaithe go heisiach ar bhallraíocht an eintitis sin sa chreat faoi seach. Sa chás go bhfuilimid nó ceann dár ngrúpa-eintitis mar bhall de chreat


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

den sórt sin, tá gach aistriú chugainn nó chuig ár ngrúpa eintiteas bunaithe go heisiach ar bhallraíocht na n-eintiteas sa chreat sin.

Is féidir le haon ábhar sonraí cóip de na creataí a fháil uainn. Ina theannta sin, tá na creataí ar fáil freisin in Iris Oifigiúil an Aontais Eorpaigh nó sna hábhair dhlíthiúla a foilsíodh nó ar shuíomhanna gréasáin na n-údarás maoirseachta nó na n-údarás inniúil nó na n-institiúidí inniúla eile.

## G. Tréimhse stórála na sonraí pearsanta, nó murarb indéanta sin, na critéir a úsáidtear chun an tréimhse sin a chinneadh (Airteagal 14(2) lit. a GDPR).

Is iad na critéir a úsáidtear chun tréimhse stórála sonraí pearsanta a chinneadh ná an tréimhse choinneála reachtúil faoi seach. Tar éis don tréimhse sin dul in éag, scriostar na sonraí comhfhreagracha go rialta, fad nach bhfuil gá leo a thuilleadh chun an conradh a chomhlíonadh nó chun conradh a thionscnamh.

Mura bhfuil aon tréimhse choinneála reachtúil ann, is é an critéar an tréimhse choinneála chonarthach nó inmheánach.

## H. I gcás ina bhfuil an phróiseáil bunaithe ar phointe (f) d'Airteagal 6(1), na leasanna dlisteanacha atá á saothrú ag an rialaitheoir nó ag triú páirtí (Airteagal 14(2) lit. b GDPR)

De réir Airteagal 6(1) lit. f GDPR, ní bheidh an phróiseáil dleathach ach amháin má tá gá leis an bpróiseáil chun críocha leasanna dlisteanacha arna saothrú ag an rialaitheoir nó ag tríú páirtí, ach amháin i gcás ina sáraítear leasanna den sórt sin ag leasanna nó cearta bunúsacha agus saoirsí an ábhair sonraí a éilíonn cosaint. de shonraí pearsanta. De réir Aithris 47 Pianbhreith 2 GDPR d'fhéadfadh leas dlisteanach a bheith ann i gcás ina bhfuil gaol ábhartha agus iomchuí idir an duine is ábhar do na sonraí agus an rialaitheoir, m.sh. i gcásanna inar cliant de chuid an rialaitheora an t-ábhar sonraí. I ngach cás ina bpróiseálann ár gcuideachta sonraí pearsanta bunaithe ar Airteagal 6(1) lit. f GDPR, is é an leas dlisteanach atá againn ná ár ngnó a dhéanamh ar mhaithe le leas ár bhfostaithe go léir agus na scairshealbhóirí.

## I. Is ann don cheart rochtain ar shonraí pearsanta a bhaineann leis an ábhair sonraí agus ceartú nó léirscriosadh na sonraí pearsanta sin, a iarraidh ar an rialaitheoir, nó srianadh ar phróiseáil maidir leis an ábhar sonraí agus is ann don cheart agóid a dhéanamh i gcoinne na próiseála chomh maith leis an gceart chun iniomparthacht sonra (Airteagal 14(2) lit. c. GDPR)

Tá na cearta seo a leanas ag gach ábhar sonraí:


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

***Ceart rochtana***

Tá sé de cheart ag gach ábhar sonraí rochtain a fháil ar na sonraí pearsanta a bhaineann leis nó léi. Síneann an ceart rochtana chuig na sonraí go léir a phróiseálann muid. Is féidir an ceart a fheidhmiú go héasca agus ag eatraimh réasúnacha, chun a bheith feasach ar dhlíthiúlacht na próiseála agus chun a fhíorú (Aithris 63 GDPR). Eascraíonn an ceart seo as Art. 15 GDPR. Féadfaidh an t-ábhar sonraí teagmháil a dhéanamh linn chun an ceart rochtana a fheidhmiú.

***Ceart chun ceartúcháin***

De réir Airteagal 16 Pianbhreith 1 GDPR tá an ceart ag an ábhar sonraí ceartú sonraí pearsanta míchruinn a bhaineann leis nó léi a fháil ón rialaitheoir gan mhoill mhíchuí. Ina theannta sin, foráiltear le hAirteagal 16 Pianbhreith 2 GDPR go bhfuil an t-ábhar sonraí i dteideal, ag cur críocha na próiseála san áireamh, sonraí pearsanta neamhiomlána a bheith comhlánaithe, lena n-áirítear trí bhíthin ráiteas forlíontach a sholáthar. Féadfaidh an t-ábhar sonraí teagmháil a dhéanamh linn chun an ceart ceartúcháin a fheidhmiú.

***An ceart chun scriosta (an ceart chun dearmad a dhéanamh)***

Ina theannta sin, tá daoine is ábhar do na sonraí i dteideal ceart scriosta agus chun dearmad a dhéanamh orthu faoi Airteagal 17 GDPR. Is féidir an ceart seo a fheidhmiú freisin trí theagmháil a dhéanamh linn. Ag an bpointe seo, áfach, ba mhaith linn a chur in iúl nach bhfuil feidhm ag an gceart seo a mhéid is gá an phróiseáil chun oibleagáid dhlíthiúil a bhfuil ár gcuideachta faoina réir a chomhlíonadh, Airteagal 17(3) lit. b GDPR. Ciallaíonn sé seo nach féidir linn iarratas a scriosadh a cheadú ach amháin tar éis don tréimhse choinneála reachtúil dul in éag.

***An ceart chun próiseáil a shrianadh***

De réir Airteagal 18 GDPR tá aon ábhar sonraí i dteideal srian a chur ar phróiseáil. Féadfar srianadh ar phróiseáil a éileamh má tá ceann de na coinníollacha atá leagtha amach in Airteagal 18(1) lit. ad go bhfuil an GDPR comhlíonta. Féadfaidh an t-ábhar sonraí teagmháil a dhéanamh linn chun an ceart chun srianadh ar phróiseáil a fheidhmiú.

***Ceart agóid a dhéanamh***

Ina theannta sin, Art. 21 Ráthaíonn GDPR an ceart agóide. Féadfaidh an t-ábhar sonraí teagmháil a dhéanamh linn chun an ceart agóide a fheidhmiú.

***Ceart chun iniomparthacht sonraí***

Ealaín. Tugann 20 GDPR an ceart chun iniomparthacht sonraí don duine is ábhar do na sonraí. De réir na forála seo tá an duine is ábhar do na sonraí faoi na coinníollacha atá leagtha síos in Airteagal 20(1) lit. a agus b GDPR an ceart chun na sonraí pearsanta a bhaineann leis nó léi, a sholáthair sé nó sí do rialaitheoir, a fháil i bhformáid struchtúrtha, a úsáidtear go coitianta agus atá inléite ag meaisín agus an ceart chun na sonraí sin a tharchur chuig rialaitheoir eile gan bhac. ón rialaitheoir ar soláthraíodh na sonraí pearsanta dó. Féadfaidh an t-ábhar sonraí teagmháil a dhéanamh linn chun an ceart chun iniomparthacht sonraí a fheidhmiú.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## J. I gcás ina bhfuil an phróiseáil bunaithe ar phointe (a) d'Airteagal 6(1) nó ar phointe (a) d'Airteagal 9(2), beidh sé de cheart an toiliú a tharraingt siar tráth ar bith, gan difear a dhéanamh do dhlíthiúlacht na próiseála atá bunaithe ar an toiliú sin a fháil roimh an tarraingt siar a dhéanamh (Airteagal 14(2) lit. d GDPR)

Má tá próiseáil sonraí pearsanta bunaithe ar Airteagal 6(1) lit. GDPR, is é sin an cás, má tá toiliú tugtha ag an duine is ábhar do na sonraí le próiseáil sonraí pearsanta chun críoch sonrach amháin nó níos mó nó an bhfuil sé bunaithe ar Airteagal 9(2) lit. GDPR, a rialaíonn toiliú sainráite le próiseáil catagóirí speisialta sonraí pearsanta, tá sé de cheart ag an ábhar sonraí de réir Airteagal 7(3) Pianbhreith 1 GDPR a thoiliú nó a toiliú a tharraingt siar tráth ar bith.

Ní dhéanfaidh toiliú a tharraingt siar difear do dhlíthiúlacht na próiseála atá bunaithe ar thoiliú roimh é a tharraingt siar, Airteagal 7(3) Pianbhreith 2 GDPR. Beidh sé chomh héasca tarraingt siar agus toiliú a thabhairt, Airteagal 7(3) Pianbhreith 4 GDPR. Dá bhrí sin, is féidir i gcónaí an toiliú a tharraingt siar ar an mbealach céanna agus a tugadh an toiliú nó ar aon bhealach eile, a mheasann an t-ábhar sonraí a bheith níos simplí. I sochaí faisnéise an lae inniu , is dócha gurb é an bealach is simplí toiliú a tharraingt siar ná ríomhphost simplí. Más mian leis an ábhar sonraí an toiliú a tugadh dúinn a tharraingt siar, is leor ríomhphost simplí a chur chugainn. Mar mhalairt air sin, féadfaidh an t-ábhar sonraí bealach ar bith eile a roghnú chun a toiliú a tharraingt siar a chur in iúl dúinn.

## K. An ceart gearán a thaisceadh le húdarás maoirseachta (Airteagal 14(2) lit. e, 77(1) GDPR)

Mar an rialaitheoir, tá oibleagáid orainn fógra a thabhairt don ábhar sonraí maidir leis an gceart chun gearán a dhéanamh le húdarás maoirseachta, Airteagal 14(2) lit. agus GDPR. Tá an ceart chun gearán a dhéanamh le húdarás maoirseachta arna rialú ag Airteagal 77(1) GDPR. De réir na forála seo, gan dochar d'aon leigheas riaracháin nó breithiúnach eile, beidh an ceart ag gach duine is ábhar do na sonraí gearán a dhéanamh le húdarás maoirseachta, go háirithe sa Bhallstát ina bhfuil gnáthchónaí, áit oibre nó áit oibre aige nó aici. an sárú líomhnaithe má mheasann an duine is ábhar do na sonraí go sáraíonn próiseáil sonraí pearsanta a bhaineann leis nó léi an Rialachán Ginearálta maidir le Cosaint Sonraí. Ní raibh an ceart chun gearán a dhéanamh le húdarás maoirseachta teoranta ach amháin ag dlí an Aontais sa chaoi is nach bhféadfar é a fheidhmiú ach amháin os comhair údaráis mhaoirseachta aonair (Aithris 141 Pianbhreith 1 GDPR). Tá an riail seo beartaithe chun gearáin dhúbailte ón ábhar sonraí céanna a sheachaint san ábhar céanna. Más mian le duine is ábhar do na sonraí gearán a dhéanamh fúinn, d'iarramar mar sin teagmháil a dhéanamh le húdarás maoirseachta amháin.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## L. An fhoinse as ar tháinig na sonraí pearsanta, agus más infheidhme, ar tháinig na sonraí as foinsí a bhfuil rochtain ag an bpobal orthu; agus (Airteagal 14(2) lit. f GDPR)

I bprionsabal, bailítear sonraí pearsanta go díreach ón ábhar sonraí nó i gcomhar le húdarás ( eg sonraí a aisghabháil ó chlár oifigiúil). Tá sonraí eile ar ábhair sonraí díorthaithe ó aistrithe cuideachtaí grúpa. I gcomhthéacs na faisnéise ginearálta seo, tá sé dodhéanta na foinsí beachta as a dtáinig sonraí pearsanta a ainmniú nó bheadh iarracht dhíréireach de réir bhrí Airt i gceist leis. 14(5) lit. b GDPR. I bprionsabal, ní bhailímid sonraí pearsanta ó fhoinsí atá inrochtana go poiblí.

Is féidir le haon ábhar sonraí teagmháil a dhéanamh linn am ar bith chun faisnéis níos mionsonraithe a fháil faoi fhoinsí cruinne na sonraí pearsanta a bhaineann leis nó léi. I gcás nach féidir tionscnamh na sonraí pearsanta a sholáthar don ábhar sonraí toisc gur úsáideadh foinsí éagsúla, ba cheart faisnéis ghinearálta a sholáthar (Aithris 61 Abairt 4 GDPR).

## M. Is ann do chinnteoireacht uathoibrithe, lena n-áirítear próifíliú dá dtagraítear in Airteagal 22(1) agus (4) agus sna cásanna sin ar a laghad, d'fhaisnéis a bhaineann leis an loighic a bheidh i gceist, chomh maith le suntasacht na próiseála sin agus na hiarmhairtí a mheastar a bheadh aici ar an ábhar sonraí (Airteagal 14(2) lit. g GDPR)

Mar chuideachta fhreagrach, de ghnáth ní úsáidimid cinnteoireacht nó próifíliú uathoibrithe. Más rud é, i gcásanna eisceachtúla, go ndéanaimid cinnteoireacht nó próifíliú uathoibrithe, cuirfimid an t-ábhar sonraí ar an eolas go leithleach nó trí fho-alt inár mbeartas príobháideachta (ar ár suíomh Gréasáin). Sa chás seo, tá feidhm ag an méid seo a leanas:

Féadfaidh cinnteoireacht uathoibrithe - lena n-áirítear próifíliú - tarlú (1) má tá sé seo riachtanach chun conradh a dhéanamh, nó chun conradh a chomhlíonadh idir an duine is ábhar do na sonraí agus sinne, nó (2) má údaraítear é seo le dlí an Aontais nó an Bhallstáit lena mbaineann muid. atá faoina réir agus a leagann síos freisin bearta oiriúnacha chun cearta agus saoirsí agus leasanna dlisteanacha an duine is ábhar do na sonraí a chosaint; nó (3) tá sé seo bunaithe ar thoiliú sainráite an ábhair sonraí.

Sna cásanna dá dtagraítear in Airteagal 22(2)(a) agus (c) den GDPR, cuirfimid bearta oiriúnacha i bhfeidhm chun cearta agus saoirsí agus leasanna dlisteanacha an duine is ábhar do na sonraí a chosaint. Sna cásanna seo, tá sé de cheart agat idirghabháil dhaonna a fháil ó thaobh an rialaitheora, do dhearcadh a chur in iúl agus cur in aghaidh an chinnidh.

Tá faisnéis bhríoch faoin loighic atá i gceist, chomh maith leis an tábhacht agus na hiarmhairtí a shamhlaítear lena leithéid de phróiseáil don ábhar sonraí leagtha amach inár mbeartas príobháideachta.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## III. EU-U.S. Data Privacy Framework (EU-U.S. DPF), UK Extension to the EU-U.S. DPF, Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF)

Má tá ár n-eagraíocht ina ball deimhnithe de EU-U.S. Data Privacy Framework (EU-U.S. DPF) agus/nó UK Extension to the EU-U.S. DPF agus/nó Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF), tá na nithe seo a leanas i bhfeidhm:

Cloíonn muid leis an EU-U.S. Data Privacy Framework (EU-U.S. DPF) agus an UK Extension to the EU-U.S. DPF chomh maith leis an Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF), mar atá leagtha síos ag an U.S. Department of Commerce. Tá ár gcuideachta tar éis a dhearbhú leis an Roinn Trádála na Stát Aontaithe go gcloíonn sí leis na EU-U.S. Data Privacy Framework Principles (EU-U.S. DPF Principles) maidir le próiseáil sonraí pearsanta a fhaigheann sí ón Aontas Eorpach agus an Ríocht Aontaithe de réir EU-U.S. DPF agus an UK Extension to the EU-U.S. DPF. Tá ár gcuideachta tar éis a dhearbhú leis an Roinn Trádála na Stát Aontaithe go gcloíonn sí leis na Swiss-U.S. Data Privacy Framework Principles (Swiss-U.S. DPF Principles) maidir le próiseáil sonraí pearsanta a fhaigheann sí ón Eilvéis de réir Swiss-U.S. DPF. I gcás coimhlint idir forálacha ár bpolasaí príobháideachta agus na EU-U.S. DPF Principles agus/nó na Swiss-U.S. DPF Principles, tá na Principles cinntitheach.

Chun tuilleadh eolais a fháil faoin gclár Data Privacy Framework (DPF) agus chun ár ndeimhniú a fheiceáil, tabhair cuairt ar https://www.dataprivacyframework.gov/.

Luafar na haonaid nó na fochuideachtaí eile de chuid na Stát Aontaithe de chuid ár gcuideachta a chloíonn freisin leis na EU-U.S. DPF Principals, lena n-áirítear an UK Extension to the EU-U.S. DPF agus na Swiss-U.S. DPF Principals, más ann dóibh, inár bpolasaí príobháideachta.

De réir an EU-U.S. DPF agus an UK Extension to the EU-U.S. DPF chomh maith leis an Swiss-U.S. DPF, geallann ár gcuideachta comhoibriú leis an bpainéal arna bhunú ag údaráis cosanta sonraí an AE agus an Information Commissioner's Office (ICO) na Breataine chomh maith leis an gCoimisinéir Feidearálach Cosanta Sonraí agus Faisnéise (EDÖB) na hEilvéise agus comhairle an phainéil maidir le gearáin neamhchinnte faoi ár láimhseáil sonraí pearsanta a fhaighimid de réir an EU-U.S. DPF agus an UK Extension to the EU-U.S. DPF agus an Swiss-U.S. DPF a leanúint.

Cuirimid na daoine lena mbaineann ar an eolas faoi na húdaráis cosanta sonraí Eorpacha ábhartha atá freagrach as gearáin a bhaineann le láimhseáil sonraí pearsanta ár n-eagraíochta a phróiseáil, ag barr an doiciméid trédhearcachta seo agus go dtugann muid leigheas dlíthiúil cuí agus saor in aisce do na daoine lena mbaineann.

Cuirimid na daoine lena mbaineann ar an eolas go bhfuil ár gcuideachta faoi réir na gcumhachtaí imscrúdaithe agus forfheidhmithe ag an Federal Trade Commission (FTC).

Tá deis ag daoine lena mbaineann, faoi choinníollacha áirithe, dul i muinín eadrána cheangailteacha. Tá ár n-eagraíocht faoi dhliteanas éilimh a réiteach agus na coinníollacha a leagtar amach in Iarscríbhinn I


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

de na DPF-Principals a chomhlíonadh má tá éileamh eadrána cheangailteacha curtha isteach ag an duine lena mbaineann trí chur in iúl dár n-eagraíocht agus na nósanna imeachta agus na coinníollacha atá leagtha amach in Iarscríbhinn I de na Principals a chomhlíonadh.

Cuirimid na daoine lena mbaineann ar an eolas faoin dliteanas atá ar ár n-eagraíocht i gcás go ndéantar sonraí pearsanta a aistriú chuig tríú páirtithe.

Maidir le ceisteanna ó dhaoine lena mbaineann nó ó údaráis maoirseachta sonraí, tá ár n-ionadaithe áitiúla luaite thuas sa doiciméad trédhearcachta seo.

Cuirimid an rogha ar fáil duit (Opt-out) maidir le cibé ar cheart do shonraí pearsanta (i) a bheith aistrithe chuig tríú páirtithe nó (ii) a úsáid chun críche a bhíonn go mór difriúil ó na críche/críocha ar bhailigh siad iad ar dtús nó ar ceadaíodh níos déanaí duit. Is é an mheicníocht shoiléir, shoiléir agus inrochtana go héasca chun do rogha a fheidhmiú ná teagmháil a dhéanamh lenár n-oifigeach cosanta sonraí (DSB) trí ríomhphost. Níl aon rogha agat agus níl orainn é sin a dhéanamh más rud é go ndéantar na sonraí a aistriú chuig tríú páirtí a ghníomhaíonn mar ghníomhaire nó próiseálaí thar ár gceann agus de réir ár dtreoracha. Mar sin féin, déanaimid conradh i gcónaí le gníomhaire nó próiseálaí den sórt sin.

Maidir le sonraí íogaire (i.e. sonraí pearsanta a chuimsíonn faisnéis faoi staid sláinte, bunús ciníoch nó eitneach, tuairimí polaitiúla, creideamh reiligiúnach nó fealsúnachta, ballraíocht in aontas ceardchumann nó faisnéis faoi shaol gnéasach an duine lena mbaineann) faighimid do thoiliú sainráite (Opt-in) nuair a dhéantar na sonraí sin (i) a aistriú chuig tríú páirtithe nó (ii) a úsáid chun críche difriúil ná an ceann ar bailíodh iad ar dtús nó an ceann ar thug tú do thoiliú níos déanaí dó trí do rogha Opt-in a roghnú. Ina theannta sin, déileálfaimid le gach sonra pearsanta a fhaighimid ó thríú páirtithe mar íogair má dhéanann an tríú páirtí iad a aithint agus a láimhseáil mar íogair.

Cuirimid in iúl duit faoin riachtanas sonraí pearsanta a nochtadh mar fhreagairt ar iarratais dhlíthiúla ó údaráis, lena n-áirítear comhlíonadh riachtanais slándála náisiúnta nó forfheidhmithe dlí.

Nuair a aistrímid sonraí pearsanta chuig tríú páirtí a ghníomhaíonn mar rialaitheoir, cloímid leis na Principals fógra agus rogha. Ina theannta sin, déanaimid conradh leis an tríú páirtí atá freagrach as an bpróiseáil, a fhorálann go ndéantar na sonraí sin a phróiseáil ach amháin chun críocha teoranta agus sonracha de réir do thoilithe agus go gcaithfidh an faighteoir an leibhéal céanna cosanta a chur ar fáil leis na Principals an DPF agus cuir in iúl dúinn má chinneann sé nach féidir leis an oibleagáid sin a chomhlíonadh a thuilleadh. Foráiltear sa chonradh go gcaithfidh an tríú páirtí, atá freagrach, an phróiseáil a stopadh nó bearta cuí agus iomchuí eile a dhéanamh chun an cás a leigheas má dhéantar a leithéid de chinneadh.

Nuair a aistrímid sonraí pearsanta chuig tríú páirtí a ghníomhaíonn mar ghníomhaire nó próiseálaí, (i) ní dhéanaimid na sonraí sin a aistriú ach amháin chun críocha teoranta agus sonracha; (ii) cinntímid go bhfuil ar an ngníomhaire nó ar an bpróiseálaí an leibhéal céanna cosanta sonraí a chur ar fáil ar a laghad agus a éilíonn na DPF-Principals; (iii) glacaimid bearta cuí agus iomchuí chun a chinntiú go bpróiseálann an gníomhaire nó an próiseálaí na sonraí pearsanta a aistríodh i ndáiríre ar bhealach atá i gcomhréir


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

lenár n-oibleagáidí de réir na DPF-Principals; (iv) éilímid ar an ngníomhaire nó ar an bpróiseálaí ár n-eagraíocht a chur ar an eolas má chinneann sé nach féidir leis an leibhéal céanna cosanta a thuilleadh a chur ar fáil, mar a fhoráiltear i na DPF-Principals; (v) tar éis fógra den sórt sin, lena n-áirítear faoi (iv), glacaimid bearta cuí agus iomchuí chun an phróiseáil neamhúdaraithe a stopadh agus chun an cás a leigheas; agus (vi) cuirimid ar fáil don DPF Department, ar iarratas, achoimre nó sampla ionadaíoch de na forálacha ábhartha cosanta sonraí ó ár gconradh leis an ngníomhaire seo.

De réir an EU-U.S. DPF agus/nó an UK Extension to the EU-U.S. DPF agus/nó an Swiss-U.S. DPF, geallann ár n-eagraíocht comhoibriú leis an bpainéal arna bhunú ag údaráis cosanta sonraí an AE agus an Information Commissioner's Office (ICO) na Breataine nó an Coimisinéir Feidearálach Cosanta Sonraí agus Faisnéise (EDÖB) na hEilvéise agus cloí lena gcomhairle maidir le gearáin neamhchinnte faoi láimhseáil sonraí pearsanta a fhaighimid maidir le caidreamh fostaíochta de réir an EU-U.S. DPF agus an UK Extension to the EU-U.S. DPF agus an Swiss-U.S. DPF.

Tá gach ábhar sonraí atá san Aontas Eorpach (AE), sa Limistéar Eorpach Eacnamaíoch (LEE) nó sa Ríocht Aontaithe go sealadach, nó a bhfuil a sainchónaí nó a ngnáthchónaí ann, i dteideal na gceart agus na cearta damhna sonraí atá foilsithe inár Doiciméad Trédhearcachta, a eascraíonn freisin ó Airteagail 15 go 22 GDPR, lena n-áirítear an ceart chun rochtain a fháil ar shonraí pearsanta. Tá an fhaisnéis seo curtha ar fáil againn i dteangacha uile an AE agus LEE. Baineann an leagan Béarla leis an Ríocht Aontaithe.

Tá gach ábhar sonraí a bhfuil cónaí orthu go sealadach san Eilvéis nó a bhfuil a sainchónaí nó a ngnáthchónaí ann i dteideal na gceart agus na cearta damhna sonraí faoi Acht um Chosaint Sonraí na hEilvéise (DPA) agus faoi Rialachán na hEilvéise um Chosaint Sonraí (DPR) a fhoilsítear inár dTrédhearcacht. Doiciméad, lena n-áirítear an ceart chun rochtain a fháil ar shonraí pearsanta. Tá an fhaisnéis seo curtha ar fáil againn i dtrí theanga oifigiúla na hEilvéise (Gearmáinis, Iodáilis agus Fraincis).


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

# IRISH: Eolas faoi Phróiseáil Sonraí Pearsanta le haghaidh Fostaithe agus Iarratasóirí (Airteagal 13, 14 GDPR)

A dhuine uasail nó a bhean uasail,

Tá cosaint speisialta tuillte ag sonraí pearsanta fostaithe agus iarratasóirí. Is é an sprioc atá againn ár leibhéal cosanta sonraí a choinneáil ar ardchaighdeán. Dá bhrí sin, táimid i go rialta ag forbairt ár gcoincheapa um chosaint sonraí agus slándáil sonraí.

Ar ndóigh, comhlíonaimid na forálacha reachtúla maidir le cosaint sonraí. De réir Airteagal 13, 14 GDPR, comhlíonann rialaitheoirí ceanglais shonracha faisnéise agus iad ag próiseáil sonraí pearsanta. Comhlíonann an doiciméad seo na hoibleagáidí sin.

Tá téarmaíocht an rialacháin dhlíthiúil casta. Ar an drochuair, níorbh fhéidir úsáid téarmaí dlí a ligean thar ceal agus an doiciméad seo á ullmhú. Mar sin, ba mhaith linn a chur in iúl go bhfuil fáilte romhat teagmháil a dhéanamh linn i gcónaí maidir le gach ceist a bhaineann leis an doiciméad seo, na téarmaí a úsáidtear nó na foirmlí.

## I. An fhaisnéis a bheidh le soláthar i gcás go mbailítear sonraí ón ábhar sonraí (Airteagal 13 GDPR)

### A. Céannacht agus sonraí teagmhála an rialaitheora agus, i gcás inarb ábhartha, céannacht agus sonraí teagmhála ionadaí an rialaitheora (Airteagal 13(1) lit. a GDPR)

Féach thuas

### B. Sonraí teagmhála an oifigigh cosanta sonraí, i gcás inarb ábhartha (Airteagal 13(1) lit. b GDPR)

Féach thuas

### C. Críocha na próiseála dá bhfuil na sonraí pearsanta beartaithe chomh maith leis an mbunús dlí don phróiseáil (Airteagal 13(1) lit. c GDPR)

Maidir le sonraí an iarratasóra, is é cuspóir na próiseála sonraí scrúdú a dhéanamh ar an iarratas le linn an phróisis earcaíochta. Chun na críche sin, déanaimid próiseáil ar na sonraí go léir a sholáthraíonn tú. Bunaithe ar na sonraí a cuireadh isteach le linn an phróisis earcaíochta, seiceálfaimid an dtugtar cuireadh


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

duit chuig agallamh poist (cuid den phróiseas roghnóireachta). I gcás iarrthóirí atá oiriúnach go ginearálta, go háirithe i gcomhthéacs an agallaimh poist, próiseálaimid sonraí pearsanta áirithe eile a sholáthraíonn tú, rud atá riachtanach dár gcinneadh roghnóireachta. Má tá tú fostaithe againn, athrófar sonraí an iarratasóra go huathoibríoch go sonraí fostaithe. Mar chuid den phróiseas earcaíochta, próiseálfaimid sonraí pearsanta eile fút a iarraimid uait agus a theastaíonn chun do chonradh a thionscnamh nó a chomhlíonadh (amhail uimhreacha aitheantais pearsanta nó uimhreacha cánach). Maidir le sonraí fostaithe, is é an cuspóir atá le sonraí a phróiseáil ná feidhmíocht an chonartha fostaíochta nó comhlíonadh forálacha dlíthiúla eile is infheidhme maidir leis an gcaidreamh fostaíochta ( m.sh. dlí cánach) chomh maith le húsáid do shonraí pearsanta chun an conradh fostaíochta a tugadh i gcrích leat a dhéanamh. (m.sh. d'ainm agus an fhaisnéis teagmhála a fhoilsiú laistigh den chuideachta nó do chustaiméirí). Stóráiltear sonraí fostaithe tar éis foirceannadh an chaidrimh fostaíochta chun tréimhsí coinneála dlíthiúla a chomhlíonadh.

Is é Airteagal 6(1) lit an bunús dlí le próiseáil sonraí. b GDPR, Airteagal 9(2) lit. b agus h GDPR, Airteagal 88(1) GDPR agus reachtaíocht náisiúnta, amhail don Ghearmáin Alt 26 BDSG (An tAcht um Chosaint Sonraí Chónaidhme).

## D. I gcás inarb infheidhme, faighteoirí na sonraí pearsanta nó catagóirí fhaighteoirí na sonraí pearsanta, más ann dóibh (Airteagal 13(1) lit. e GDPR)

Údaráis phoiblí

Comhlachtaí seachtracha

Tuilleadh comhlachtaí seachtracha

Próiseáil inmheánach

Próiseáil inghrúpa

Comhlachtaí eile

Foilsítear liosta dár bpróiseálaithe agus dár bhfaighteoirí sonraí i dtríú tíortha agus, más infheidhme, eagraíochtaí idirnáisiúnta ar ár suíomh Gréasáin nó is féidir é a iarraidh orainn saor in aisce. Déan teagmháil lenár n-oifigeach cosanta sonraí le do thoil chun an liosta seo a iarraidh.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## E. I gcás inarb infheidhme, go bhfuil sé beartaithe ag an rialaitheoir sonraí pearsanta a aistriú chuig tríú tír nó chuig eagraíocht idirnáisiúnta agus cibé arb ann nó nach ann do chinneadh leordhóthanachta ón gCoimisiún, nó i gcás na n-aistrithe dá dtagraítear in Airteagal 46 nó in Airteagal 47, nó sa dara fomhír d'Airteagal 49(1), tagairt do na coimircí iomchuí nó oiriúnacha agus na bealaí inar féidir chun cóip díobh a fháil nó an áit inar cuireadh iad ar fáil (Airteagal 13(1) lit. f, 46(1), 46(2) lit . c GDPR)

Féadfaidh gach cuideachta agus brainse atá mar chuid dár ngrúpa (dá ngairtear “grúpchuideachtaí” anseo feasta) a bhfuil a n-áit ghnó nó oifig i dtríú tír bheith ina mbaill d’fhaighteoirí sonraí pearsanta. Is féidir liosta de na cuideachtaí grúpa nó na faighteoirí go léir a iarraidh uainn.

De réir Airteagal 46(1) GDPR ní fhéadfaidh rialaitheoir nó próiseálaí sonraí pearsanta a aistriú chuig tríú tír ach amháin má tá coimircí iomchuí curtha ar fáil ag an rialaitheoir nó ag an bpróiseálaí, agus ar an gcoinníoll go bhfuil cearta infhorghníomhaithe damhna sonraí agus leigheasanna dlí éifeachtacha ar fáil do dhaoine is ábhar do na sonraí. Féadfar coimircí iomchuí a sholáthar gan aon údarú sonrach a éileamh ó údarás maoirseachta trí bhíthin clásail chaighdeánacha chonarthacha, Airteagal 46(2) lit. c GDPR.

Comhaontaítear clásail chaighdeánacha chonarthacha an Aontais Eorpaigh nó cosaintí iomchuí eile le gach faighteoir ó thríú tíortha roimh an gcéad tarchur sonraí pearsanta. Dá bhrí sin, áirithítear go ráthaítear cosaintí iomchuí, cearta infhorghníomhaithe ábhar sonraí agus leigheasanna éifeachtacha dlí do dhaoine is ábhar do na sonraí. Is féidir le gach ábhar sonraí cóip de na clásail chaighdeánacha chonarthacha a fháil uainn. Tá na clásail chaighdeánacha chonarthacha ar fáil freisin in Iris Oifigiúil an Aontais Eorpaigh.

Tugann Airteagal 45(3) den Rialachán Ginearálta um Chosaint Sonraí (GDPR) an chumhacht don Choimisiún Eorpach a chinneadh, trí bhíthin gnímh cur chun feidhme, go n-áirithíonn tír nach bhfuil san AE leibhéal leordhóthanach cosanta. Ciallaíonn sé seo leibhéal cosanta do shonraí pearsanta atá comhionann go bunúsach leis an leibhéal cosanta laistigh den AE. Is é éifeacht na gcinntí leordhóthanachta gur féidir le sonraí pearsanta sreabhadh gan bhac ón AE (agus ón Iorua, ó Lichtinstéin agus ón Íoslainn) chuig tríú tír gan a thuilleadh constaicí. Tá rialacha comhchosúla ann don Ríocht Aontaithe, don Eilvéis agus do thíortha áirithe eile.

I gcás inar chinn an Coimisiún Eorpach nó rialtas tíre eile go n-áirithíonn tríú tír leibhéal leordhóthanach cosanta, agus go bhfuil Creat bailí i bhfeidhm (m.sh. EU-U.S. Data Privacy Framework, Swiss-U.S. Data Privacy Framework, UK Extension to the EU-U.S. Data Privacy Framework), tá gach aistriú a dhéanaimid chuig comhaltaí creata den sórt sin (m.sh. eintitis fhéindheimhnithe) bunaithe go heisiach ar bhallraíocht an eintitis sin sa chreat faoi seach. Sa chás go bhfuilimid nó ceann dár ngrúpa-eintitis mar bhall de chreat den sórt sin, tá gach aistriú chugainn nó chuig ár ngrúpa eintiteas bunaithe go heisiach ar bhallraíocht na n-eintiteas sa chreat sin.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

Is féidir le haon ábhar sonraí cóip de na creataí a fháil uainn. Ina theannta sin, tá na creataí ar fáil freisin in Iris Oifigiúil an Aontais Eorpaigh nó sna hábhair dhlíthiúla a foilsíodh nó ar shuíomhanna gréasáin na n-údarás maoirseachta nó na n-údarás inniúil nó na n-institiúidí inniúla eile.

## F. Tréimhse stórála na sonraí pearsanta, nó murarb indéanta sin, na critéir a úsáidtear chun an tréimhse sin a chinneadh (Airteagal 13(2) lit. a GDPR)

Is é 6 mhí an ré stórála sonraí pearsanta iarratasóirí. Maidir le sonraí fostaithe tá feidhm ag an tréimhse choinneála reachtúil faoi seach. Tar éis don tréimhse sin dul in éag, scriostar na sonraí comhfhreagracha go rialta, fad nach bhfuil gá leo a thuilleadh chun an conradh a chomhlíonadh nó chun conradh a thionscnamh.

## G. Is ann don cheart rochtain ar shonraí pearsanta a bhaineann leis ábhar sonraí agus go ndéanfaí ceartú nó léirscriosadh na sonraí sin, a iarraidh ar an rialaitheoir, nó srianadh ar phróiseáil maidir leis an ábhar sonraí agus is ann don cheart agóid a dhéanamh i gcoinne na próiseála chomh maith leis an gceart chun iniomparthacht sonraí (Airteagal 13(2) lit. b. GDPR)

Tá na cearta seo a leanas ag gach ábhar sonraí:

***Ceart rochtana***

Tá sé de cheart ag gach ábhar sonraí rochtain a fháil ar na sonraí pearsanta a bhaineann leis nó léi. Síneann an ceart rochtana chuig na sonraí go léir a phróiseálann muid. Is féidir an ceart a fheidhmiú go héasca agus ag eatraimh réasúnacha, chun a bheith feasach ar dhlíthiúlacht na próiseála agus chun a fhíorú (Aithris 63 GDPR). Eascraíonn an ceart seo as Art. 15 GDPR. Féadfaidh an t-ábhar sonraí teagmháil a dhéanamh linn chun an ceart rochtana a fheidhmiú.

***Ceart chun ceartúcháin***

De réir Airteagal 16 Pianbhreith 1 GDPR tá an ceart ag an ábhar sonraí ceartú sonraí pearsanta míchruinn a bhaineann leis nó léi a fháil ón rialaitheoir gan mhoill mhíchuí. Ina theannta sin, foráiltear le hAirteagal 16 Pianbhreith 2 GDPR go bhfuil an t-ábhar sonraí i dteideal, ag cur críocha na próiseála san áireamh, sonraí pearsanta neamhiomlána a bheith comhlánaithe, lena n-áirítear trí bhíthin ráiteas forlíontach a sholáthar. Féadfaidh an t-ábhar sonraí teagmháil a dhéanamh linn chun an ceart ceartúcháin a fheidhmiú.

***An ceart chun scriosta (ceart chun dearmad a dhéanamh)***

Ina theannta sin, tá daoine is ábhar do na sonraí i dteideal ceart scriosta agus chun dearmad a dhéanamh orthu faoi Airteagal 17 GDPR. Is féidir an ceart seo a fheidhmiú freisin trí theagmháil a dhéanamh linn. Ag an bpointe seo, áfach, ba mhaith linn a chur in iúl nach bhfuil feidhm ag an gceart seo a mhéid is gá an phróiseáil chun oibleagáid dhlíthiúil a bhfuil ár gcuideachta faoina réir a chomhlíonadh, Airteagal 17(3)


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

lit. b GDPR. Ciallaíonn sé seo nach féidir linn iarratas a scriosadh a cheadú ach amháin tar éis don tréimhse choinneála reachtúil dul in éag.

***An ceart chun próiseáil a shrianadh***

De réir Airteagal 18 GDPR tá aon ábhar sonraí i dteideal srianta próiseála. Féadfar srianadh ar phróiseáil a éileamh má tá ceann de na coinníollacha atá leagtha amach in Airteagal 18(1) lit. ad go bhfuil an GDPR comhlíonta. Féadfaidh an t-ábhar sonraí teagmháil a dhéanamh linn chun an ceart chun srianadh ar phróiseáil a fheidhmiú.

***Ceart agóid a dhéanamh***

Ina theannta sin, Art. 21 Ráthaíonn GDPR an ceart agóide. Féadfaidh an t-ábhar sonraí teagmháil a dhéanamh linn chun an ceart agóide a fheidhmiú.

***Ceart chun iniomparthacht sonraí***

Ealaín. Tugann 20 GDPR an ceart chun iniomparthacht sonraí don duine is ábhar do na sonraí. Faoin bhforáil seo, tá an duine is ábhar do na sonraí faoi na coinníollacha atá leagtha síos in Airteagal 20(1) lit. a agus b GDPR an ceart chun na sonraí pearsanta a bhaineann leis nó léi, a sholáthair sé nó sí do rialaitheoir, a fháil i bhformáid struchtúrtha, a úsáidtear go coitianta agus atá inléite ag meaisín agus an ceart chun na sonraí sin a tharchur chuig rialaitheoir eile gan bhac. ón rialaitheoir ar soláthraíodh na sonraí pearsanta dó. Féadfaidh an t-ábhar sonraí teagmháil a dhéanamh linn chun an ceart chun iniomparthacht sonraí a fheidhmiú.

## H. I gcás ina bhfuil an phróiseáil bunaithe ar phointe (a) d'Airteagal 6(1) nó ar phointe (a) d'Airteagal 9(2), beidh sé de cheart an toiliú a tharraingt siar tráth ar bith, gan difear a dhéanamh do dhlíthiúlacht na próiseála atá bunaithe ar an toiliú sin a fháil roimh an tarraingt siar a dhéanamh (Airteagal 13(2) lit. c GDPR)

Má tá próiseáil sonraí pearsanta bunaithe ar Airteagal 6(1) lit. GDPR, is é sin an cás, má tá toiliú tugtha ag an duine is ábhar do na sonraí le próiseáil sonraí pearsanta chun críoch sonrach amháin nó níos mó nó an bhfuil sé bunaithe ar Airteagal 9(2) lit. GDPR, a rialaíonn toiliú sainráite le próiseáil catagóirí speisialta sonraí pearsanta, tá sé de cheart ag an ábhar sonraí de réir Airteagal 7(3) Pianbhreith 1 GDPR a thoiliú nó a toiliú a tharraingt siar tráth ar bith.

Ní dhéanfaidh toiliú a tharraingt siar difear do dhlíthiúlacht na próiseála atá bunaithe ar thoiliú roimh é a tharraingt siar, Airteagal 7(3) Pianbhreith 2 GDPR. Beidh sé chomh héasca tarraingt siar agus toiliú a thabhairt, Airteagal 7(3) Pianbhreith 4 GDPR. Dá bhrí sin, is féidir i gcónaí an toiliú a tharraingt siar ar an mbealach céanna agus a tugadh an toiliú nó ar aon bhealach eile, a mheasann an t-ábhar sonraí a bheith níos simplí. I sochaí faisnéise an lae inniu, is dócha gurb é an bealach is simplí toiliú a tharraingt siar ná ríomhphost simplí. Más mian leis an ábhar sonraí an toiliú a tugadh dúinn a tharraingt siar, is leor ríomhphost simplí a chur chugainn. Mar mhalairt air sin, féadfaidh an t-ábhar sonraí bealach ar bith eile a roghnú chun a toiliú a tharraingt siar a chur in iúl dúinn.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## I. An ceart gearán a thaisceadh le húdarás maoirseachta (Airteagal 13(2) lit. d, 77(1) GDPR)

Mar an rialaitheoir, tá oibleagáid orainn fógra a thabhairt don ábhar sonraí maidir leis an gceart chun gearán a dhéanamh le húdarás maoirseachta, Airteagal 13(2) lit. d GDPR. Tá an ceart chun gearán a dhéanamh le húdarás maoirseachta arna rialú ag Airteagal 77(1) GDPR. De réir na forála seo, gan dochar d'aon leigheas riaracháin nó breithiúnach eile, beidh an ceart ag gach duine is ábhar do na sonraí gearán a dhéanamh le húdarás maoirseachta, go háirithe sa Bhallstát ina bhfuil gnáthchónaí, áit oibre nó áit oibre aige nó aici. an sárú líomhnaithe má mheasann an duine is ábhar do na sonraí go sáraíonn próiseáil sonraí pearsanta a bhaineann leis nó léi an Rialachán Ginearálta maidir le Cosaint Sonraí. Ní raibh an ceart chun gearán a dhéanamh le húdarás maoirseachta teoranta ach amháin ag dlí an Aontais sa chaoi is nach bhféadfar é a fheidhmiú ach amháin os comhair údaráis mhaoirseachta aonair (Aithris 141 Pianbhreith 1 GDPR). Tá an riail seo beartaithe chun gearáin dhúbailte ón ábhar sonraí céanna a sheachaint san ábhar céanna. Más mian le duine is ábhar do na sonraí gearán a dhéanamh fúinn, d'iarramar mar sin teagmháil a dhéanamh le húdarás maoirseachta amháin.

## J. An ceanglas reachtach nó conarthach é an ceanglas sonraí pearsanta a sholáthar, nó an ceanglas é ar gá é le go ndéanfaí i gconradh, agus an bhfuil oibleagáid ar an ábhar sonraí na sonraí pearsanta sin a sholáthar mar aon leis na hiarmhairtí a d'fhéadfadh a bheith ann i gcás nár soláthraíodh na sonraí sin; agus sin (Airteagal 13(2) lit. e GDPR)

Soiléirímid go bhfuil soláthar sonraí pearsanta riachtanach go páirteach de réir an dlí ( m.sh. rialacháin chánach) nó go bhféadfadh sé tarlú freisin ó fhorálacha conartha (m.sh. faisnéis ar an gcomhpháirtí conarthach).

Uaireanta b'fhéidir go mbeadh sé riachtanach conradh a thabhairt i gcrích go soláthraíonn an damhna sonraí sonraí pearsanta dúinn, nach mór dúinn a phróiseáil ina dhiaidh sin. Tá oibleagáid ar an ábhar sonraí, mar shampla, sonraí pearsanta a sholáthar dúinn nuair a shíníonn ár gcuideachta conradh leis nó léi. Bheadh sé mar thoradh ar neamhsholáthar na sonraí pearsanta nach bhféadfaí an conradh leis an ábhar sonraí a thabhairt i gcrích.

Sula gcuireann an t-ábhar sonraí sonraí pearsanta ar fáil, ní mór don ábhar sonraí teagmháil a dhéanamh linn. Soiléirímid don duine is ábhar do na sonraí an bhfuil gá le soláthar na sonraí pearsanta de réir an dlí nó an chonartha nó an bhfuil gá leis chun an conradh a thabhairt i gcrích, an bhfuil oibleagáid ann na sonraí pearsanta a sholáthar agus na hiarmhairtí a bhaineann le neamhsholáthar na sonraí pearsanta.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

### K. Is ann do chinnteoireacht uathoibrithe, lena n-áirítear próifíliú, dá dtagraítear in Airteagal 22(1) agus (4) agus, sna cásanna sin ar a laghad, d'fhaisnéis fhónta faoin loighic a bheidh i gceist, chomh maith le suntasacht na próiseála sin agus na hiarmhairtí a mheastar a bheadh aici ar an ábhar sonraí (Airteagal 13(2) lit. f GDPR)

Mar chuideachta fhreagrach, de ghnáth ní úsáidimid cinnteoireacht nó próifíliú uathoibrithe. Más rud é, i gcásanna eisceachtúla, go ndéanaimid cinnteoireacht nó próifíliú uathoibrithe, cuirfimid an t-ábhar sonraí ar an eolas go leithleach nó trí fho-alt inár mbeartas príobháideachta (ar ár suíomh Gréasáin). Sa chás seo, tá feidhm ag an méid seo a leanas:

Féadfaidh cinnteoireacht uathoibrithe - lena n-áirítear próifíliú - tarlú (1) má tá sé seo riachtanach chun conradh a dhéanamh, nó chun conradh a chomhlíonadh idir an duine is ábhar do na sonraí agus sinne, nó (2) má údaraítear é seo le dlí an Aontais nó an Bhallstáit lena mbaineann muid. atá faoina réir agus a leagann síos freisin bearta oiriúnacha chun cearta agus saoirsí agus leasanna dlisteanacha an duine is ábhar do na sonraí a chosaint; nó (3) tá sé seo bunaithe ar thoiliú sainráite an ábhair sonraí.

Sna cásanna dá dtagraítear in Airteagal 22(2)(a) agus (c) den GDPR, cuirfimid bearta oiriúnacha i bhfeidhm chun cearta agus saoirsí agus leasanna dlisteanacha an duine is ábhar do na sonraí a chosaint. Sna cásanna seo, tá sé de cheart agat idirghabháil dhaonna a fháil ó thaobh an rialaitheora, do dhearcadh a chur in iúl agus cur in aghaidh an chinnidh.

Tá faisnéis bhríoch faoin loighic atá i gceist, chomh maith leis an tábhacht agus na hiarmhairtí a shamhlaítear lena leithéid de phróiseáil don ábhar sonraí leagtha amach inár mbeartas príobháideachta.

## II. An fhaisnéis a bheidh le soláthar i gcás nár bailíodh na sonraí ón ábhar sonraí (Airteagal 14 GDPR)

### A. Céannacht agus sonraí teagmhála an rialaitheora agus, i gcás inarb infheidhme, céannacht agus sonraí teagmhála ionadaí an rialaitheora (Airteagal 14(1) lit. a GDPR)

Féach thuas

### B. Sonraí teagmhála an oifigigh cosanta sonraí, más ann dó, más infheidhme (Airteagal 14(1) lit. b GDPR)

Féach thuas


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## C. Críocha na próiseála dá bhfuil na sonraí pearsanta beartaithe chomh maith leis an mbunús dlí don phróiseáil (Airteagal 14(1) lit. c GDPR)

Maidir le sonraí an iarratasóra nár bailíodh ón ábhar sonraí, is é cuspóir na próiseála sonraí scrúdú a dhéanamh ar an iarratas le linn an phróisis earcaíochta. Chun na críche sin, féadfaimid sonraí nár bailíodh uait a phróiseáil. Bunaithe ar na sonraí a próiseáladh le linn an phróisis earcaíochta, seiceálfaimid an dtugtar cuireadh duit chuig agallamh poist (cuid den phróiseas roghnóireachta). Má tá tú fostaithe againn, déanfar sonraí an iarratasóra go huathoibríoch a thiontú go sonraí fostaithe. Maidir le sonraí fostaithe, is é cuspóir na próiseála sonraí feidhmíocht an chonartha fostaíochta nó comhlíonadh forálacha dlí eile is infheidhme maidir leis an gcaidreamh fostaíochta. Stóráiltear sonraí fostaithe tar éis foirceannadh an chaidrimh fostaíochta chun tréimhsí coinneála dlíthiúla a chomhlíonadh.

Is é Airteagal 6(1) lit an bunús dlí le próiseáil sonraí. b agus f GDPR, Airteagal 9(2) lit. b agus h GDPR, Airteagal 88(1) GDPR agus reachtaíocht náisiúnta, amhail don Ghearmáin Alt 26 BDSG (An tAcht um Chosaint Sonraí Chónaidhme).

## D. Catagóirí na sonraí pearsanta lena mbaineann (Airteagal 14(1) lit. d GDPR)

Sonraí an iarratasóra

Sonraí fostaithe

## E. Faighteoirí nó catagóirí fhaighteoirí na sonraí pearsanta, más ann dóibh (Airteagal 14(1) lit. e GDPR)

Údaráis phoiblí

Comhlachtaí seachtracha

Tuilleadh comhlachtaí seachtracha

Próiseáil inmheánach

Próiseáil inghrúpa

Comhlachtaí eile

Foilsítear liosta dár bpróiseálaithe agus dár bhfaighteoirí sonraí i dtríú tíortha agus, más infheidhme, eagraíochtaí idirnáisiúnta ar ár suíomh Gréasáin nó is féidir é a iarraidh orainn saor in aisce. Déan teagmháil lenár n-oifigeach cosanta sonraí le do thoil chun an liosta seo a iarraidh.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## F. I gcás inarb infheidhme, go bhfuil sé beartaithe ag an rialaitheoir sonraí pearsanta a aistriú chuig faighteoir i dtríú tír nó in eagraíocht idirnáisiúnta agus cibé arb ann nó nach ann do chinneadh leordhóthanachta, nó i gcás na n-aistrithe dá dtagraítear in Airteagal 46 nó in Airteagal 47, nó sa dara fomhír d'Airteagal 49(1), tagairt do na coimircí iomchuí nó oiriúnacha agus na bealaí chun cóip díobh a fháil nó cá bhfuil siad ar fáil (Airteagal 14(1) lit. f, 46(1), 46(2) lit. c GDPR)

Féadfaidh gach cuideachta agus brainse atá mar chuid dár ngrúpa (dá ngairtear “grúpchuideachtaí” anseo feasta) a bhfuil a n-áit ghnó nó oifig i dtríú tír bheith ina mbaill d’fhaighteoirí sonraí pearsanta. Is féidir liosta de na cuideachtaí grúpa nó na faighteoirí go léir a iarraidh uainn.

De réir Airteagal 46(1) GDPR ní fhéadfaidh rialaitheoir nó próiseálaí sonraí pearsanta a aistriú chuig tríú tír ach amháin má tá coimircí iomchuí curtha ar fáil ag an rialaitheoir nó ag an bpróiseálaí, agus ar an gcoinníoll go bhfuil cearta infhorghníomhaithe damhna sonraí agus leigheasanna dlí éifeachtacha ar fáil do dhaoine is ábhar do na sonraí. Féadfar coimircí iomchuí a sholáthar gan aon údarú sonrach a éileamh ó údarás maoirseachta trí bhíthin clásail chaighdeánacha um chosaint sonraí, Airteagal 46(2) lit. c GDPR.

Comhaontaítear clásail chaighdeánacha chonarthacha an Aontais Eorpaigh nó cosaintí iomchuí eile le gach faighteoir ó thríú tíortha roimh an gcéad tarchur sonraí pearsanta. Dá bhrí sin, áirithítear go ráthaítear cosaintí iomchuí, cearta infhorghníomhaithe ábhar sonraí agus leigheasanna éifeachtacha dlí do dhaoine is ábhar do na sonraí. Is féidir le gach ábhar sonraí cóip de na clásail chaighdeánacha chonarthacha a fháil uainn. Tá na clásail chaighdeánacha chonarthacha ar fáil freisin in Iris Oifigiúil an Aontais Eorpaigh.

Tugann Airteagal 45(3) den Rialachán Ginearálta um Chosaint Sonraí (GDPR) an chumhacht don Choimisiún Eorpach a chinneadh, trí bhíthin gnímh cur chun feidhme, go n-áirithíonn tír nach bhfuil san AE leibhéal leordhóthanach cosanta. Ciallaíonn sé seo leibhéal cosanta do shonraí pearsanta atá comhionann go bunúsach leis an leibhéal cosanta laistigh den AE. Is é éifeacht na gcinntí leordhóthanachta gur féidir le sonraí pearsanta sreabhadh gan bhac ón AE (agus ón Iorua, ó Lichtinstéin agus ón Íoslainn) chuig tríú tír gan a thuilleadh constaicí. Tá rialacha comhchosúla ann don Ríocht Aontaithe, don Eilvéis agus do thíortha áirithe eile.

I gcás inar chinn an Coimisiún Eorpach nó rialtas tíre eile go n-áirithíonn tríú tír leibhéal leordhóthanach cosanta, agus go bhfuil Creat bailí i bhfeidhm (m.sh. EU-U.S. Data Privacy Framework, Swiss-U.S. Data Privacy Framework, UK Extension to the EU-U.S. Data Privacy Framework), tá gach aistriú a dhéanaimid chuig comhaltaí creata den sórt sin (m.sh. eintitis fhéindheimhnithe) bunaithe go heisiach ar bhallraíocht an eintitis sin sa chreat faoi seach. Sa chás go bhfuilimid nó ceann dár ngrúpa-eintitis mar bhall de chreat den sórt sin, tá gach aistriú chugainn nó chuig ár ngrúpa eintiteas bunaithe go heisiach ar bhallraíocht na n-eintiteas sa chreat sin.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

Is féidir le haon ábhar sonraí cóip de na creataí a fháil uainn. Ina theannta sin, tá na creataí ar fáil freisin in Iris Oifigiúil an Aontais Eorpaigh nó sna hábhair dhlíthiúla a foilsíodh nó ar shuíomhanna gréasáin na n-údarás maoirseachta nó na n-údarás inniúil nó na n-institiúidí inniúla eile.

## G. Tréimhse stórála na sonraí pearsanta, nó murarb indéanta sin, na critéir a úsáidtear chun an tréimhse sin a chinneadh (Airteagal 14(2) lit. a GDPR).

Is é 6 mhí an ré stórála sonraí pearsanta iarratasóirí. Maidir le sonraí fostaithe tá feidhm ag an tréimhse choinneála reachtúil faoi seach. Tar éis don tréimhse sin dul in éag, scriostar na sonraí comhfhreagracha go rialta, fad nach bhfuil gá leo a thuilleadh chun an conradh a chomhlíonadh nó chun conradh a thionscnamh.

## H. I gcás ina bhfuil an phróiseáil bunaithe ar phointe (f) d'Airteagal 6(1), na leasanna dlisteanacha atá á saothrú ag an rialaitheoir nó ag triú páirtí (Airteagal 14(2) lit. b GDPR)

De réir Airteagal 6(1) lit. f GDPR, ní bheidh an phróiseáil dleathach ach amháin má tá gá leis an bpróiseáil chun críocha leasanna dlisteanacha arna saothrú ag an rialaitheoir nó ag tríú páirtí, ach amháin i gcás ina sáraítear leasanna den sórt sin ag leasanna nó cearta bunúsacha agus saoirsí an ábhair sonraí a éilíonn cosaint. de shonraí pearsanta. De réir Aithris 47 Pianbhreith 2 GDPR d'fhéadfadh leas dlisteanach a bheith ann i gcás ina bhfuil gaol ábhartha agus iomchuí idir an duine is ábhar do na sonraí agus an rialaitheoir, m.sh. i gcásanna inar cliant de chuid an rialaitheora an t-ábhar sonraí. I ngach cás ina bpróiseálann ár gcuideachta sonraí an iarratasóra bunaithe ar Airteagal 6(1) lit. f GDPR, is é ár leas dlisteanach pearsanra agus daoine gairmiúla oiriúnacha a fhostú.

## I. Is ann don cheart rochtain ar shonraí pearsanta a bhaineann leis an ábhair sonraí agus ceartú nó léirscriosadh na sonraí pearsanta sin, a iarraidh ar an rialaitheoir, nó srianadh ar phróiseáil maidir leis an ábhar sonraí agus is ann don cheart agóid a dhéanamh i gcoinne na próiseála chomh maith leis an gceart chun iniomparthacht sonra (Airteagal 14(2) lit. c. GDPR)

Tá na cearta seo a leanas ag gach ábhar sonraí:

***Ceart rochtana***

Tá sé de cheart ag gach ábhar sonraí rochtain a fháil ar na sonraí pearsanta a bhaineann leis nó léi. Síneann an ceart rochtana chuig na sonraí go léir a phróiseálann muid. Is féidir an ceart a fheidhmiú go héasca agus ag eatraimh réasúnacha, chun a bheith feasach ar dhlíthiúlacht na próiseála agus chun a fhíorú (Aithris 63 GDPR). Eascraíonn an ceart seo as Art. 15 GDPR. Féadfaidh an t-ábhar sonraí teagmháil a dhéanamh linn chun an ceart rochtana a fheidhmiú.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

***Ceart chun ceartúcháin***

De réir Airteagal 16 Pianbhreith 1 GDPR tá an ceart ag an ábhar sonraí ceartú sonraí pearsanta míchruinn a bhaineann leis nó léi a fháil ón rialaitheoir gan mhoill mhíchuí. Ina theannta sin, foráiltear le hAirteagal 16 Pianbhreith 2 GDPR go bhfuil an t-ábhar sonraí i dteideal, ag cur críocha na próiseála san áireamh, sonraí pearsanta neamhiomlána a bheith comhlánaithe, lena n-áirítear trí bhíthin ráiteas forlíontach a sholáthar. Féadfaidh an t-ábhar sonraí teagmháil a dhéanamh linn chun an ceart ceartúcháin a fheidhmiú.

***An ceart chun scriosta (an ceart chun dearmad a dhéanamh)***

Ina theannta sin, tá daoine is ábhar do na sonraí i dteideal ceart scriosta agus chun dearmad a dhéanamh orthu faoi Airteagal 17 GDPR. Is féidir an ceart seo a fheidhmiú freisin trí theagmháil a dhéanamh linn. Ag an bpointe seo, áfach, ba mhaith linn a chur in iúl nach bhfuil feidhm ag an gceart seo a mhéid is gá an phróiseáil chun oibleagáid dhlíthiúil a bhfuil ár gcuideachta faoina réir a chomhlíonadh, Airteagal 17(3) lit. b GDPR. Ciallaíonn sé seo nach féidir linn iarratas a scriosadh a cheadú ach amháin tar éis don tréimhse choinneála reachtúil dul in éag.

***An ceart chun próiseáil a shrianadh***

De réir Airteagal 18 GDPR tá aon ábhar sonraí i dteideal srian a chur ar phróiseáil. Féadfar srianadh ar phróiseáil a éileamh má tá ceann de na coinníollacha atá leagtha amach in Airteagal 18(1) lit. ad go bhfuil an GDPR comhlíonta. Féadfaidh an t-ábhar sonraí teagmháil a dhéanamh linn chun an ceart chun srianadh ar phróiseáil a fheidhmiú.

***Ceart agóid a dhéanamh***

Ina theannta sin, Art. 21 Ráthaíonn GDPR an ceart agóide. Féadfaidh an t-ábhar sonraí teagmháil a dhéanamh linn chun an ceart agóide a fheidhmiú.

***Ceart chun iniomparthacht sonraí***

Ealaín. Tugann 20 GDPR an ceart chun iniomparthacht sonraí don duine is ábhar do na sonraí. De réir na forála seo tá an duine is ábhar do na sonraí faoi na coinníollacha atá leagtha síos in Airteagal 20(1) lit. a agus b GDPR an ceart chun na sonraí pearsanta a bhaineann leis nó léi, a sholáthair sé nó sí do rialaitheoir, a fháil i bhformáid struchtúrtha, a úsáidtear go coitianta agus atá inléite ag meaisín agus an ceart chun na sonraí sin a tharchur chuig rialaitheoir eile gan bhac. ón rialaitheoir ar soláthraíodh na sonraí pearsanta dó. Féadfaidh an t-ábhar sonraí teagmháil a dhéanamh linn chun an ceart chun iniomparthacht sonraí a fheidhmiú.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## J. I gcás ina bhfuil an phróiseáil bunaithe ar phointe (a) d'Airteagal 6(1) nó ar phointe (a) d'Airteagal 9(2), beidh sé de cheart an toiliú a tharraingt siar tráth ar bith, gan difear a dhéanamh do dhlíthiúlacht na próiseála atá bunaithe ar an toiliú sin a fháil roimh an tarraingt siar a dhéanamh (Airteagal 14(2) lit. d GDPR)

Má tá próiseáil sonraí pearsanta bunaithe ar Airteagal 6(1) lit. GDPR, is é sin an cás, má tá toiliú tugtha ag an duine is ábhar do na sonraí le próiseáil sonraí pearsanta chun críoch sonrach amháin nó níos mó nó an bhfuil sé bunaithe ar Airteagal 9(2) lit. GDPR, a rialaíonn toiliú sainráite le próiseáil catagóirí speisialta sonraí pearsanta, tá sé de cheart ag an ábhar sonraí de réir Airteagal 7(3) Pianbhreith 1 GDPR a thoiliú nó a toiliú a tharraingt siar tráth ar bith.

Ní dhéanfaidh toiliú a tharraingt siar difear do dhlíthiúlacht na próiseála atá bunaithe ar thoiliú roimh é a tharraingt siar, Airteagal 7(3) Pianbhreith 2 GDPR. Beidh sé chomh héasca tarraingt siar agus toiliú a thabhairt, Airteagal 7(3) Pianbhreith 4 GDPR. Dá bhrí sin, is féidir i gcónaí an toiliú a tharraingt siar ar an mbealach céanna agus a tugadh an toiliú nó ar aon bhealach eile, a mheasann an t-ábhar sonraí a bheith níos simplí. I sochaí faisnéise an lae inniu, is dócha gurb é an bealach is simplí toiliú a tharraingt siar ná ríomhphost simplí. Más mian leis an ábhar sonraí an toiliú a tugadh dúinn a tharraingt siar, is leor ríomhphost simplí a chur chugainn. Mar mhalairt air sin, féadfaidh an t-ábhar sonraí bealach ar bith eile a roghnú chun a toiliú a tharraingt siar a chur in iúl dúinn.

## K. An ceart gearán a thaisceadh le húdarás maoirseachta (Airteagal 14(2) lit. e, 77(1) GDPR)

Mar an rialaitheoir, tá oibleagáid orainn fógra a thabhairt don ábhar sonraí maidir leis an gceart chun gearán a dhéanamh le húdarás maoirseachta, Airteagal 14(2) lit. agus GDPR. Tá an ceart chun gearán a dhéanamh le húdarás maoirseachta arna rialú ag Airteagal 77(1) GDPR. De réir na forála seo, gan dochar d'aon leigheas riaracháin nó breithiúnach eile, beidh an ceart ag gach duine is ábhar do na sonraí gearán a dhéanamh le húdarás maoirseachta, go háirithe sa Bhallstát ina bhfuil gnáthchónaí, áit oibre nó áit oibre aige nó aici. an sárú líomhnaithe má mheasann an duine is ábhar do na sonraí go sáraíonn próiseáil sonraí pearsanta a bhaineann leis nó léi an Rialachán Ginearálta maidir le Cosaint Sonraí. Ní raibh an ceart chun gearán a dhéanamh le húdarás maoirseachta teoranta ach amháin ag dlí an Aontais sa chaoi is nach bhféadfar é a fheidhmiú ach amháin os comhair údaráis mhaoirseachta aonair (Aithris 141 Pianbhreith 1 GDPR). Tá an riail seo beartaithe chun gearáin dhúbailte ón ábhar sonraí céanna a sheachaint san ábhar céanna. Más mian le duine is ábhar do na sonraí gearán a dhéanamh fúinn, d'iarramar mar sin teagmháil a dhéanamh le húdarás maoirseachta amháin.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## L. An fhoinse as ar tháinig na sonraí pearsanta, agus más infheidhme, ar tháinig na sonraí as foinsí a bhfuil rochtain ag an bpobal orthu; agus (Airteagal 14(2) lit. f GDPR)

I bprionsabal, bailítear sonraí pearsanta go díreach ón ábhar sonraí nó i gcomhar le húdarás ( eg sonraí a aisghabháil ó chlár oifigiúil). Tá sonraí eile ar ábhair sonraí díorthaithe ó aistrithe cuideachtaí grúpa. I gcomhthéacs na faisnéise ginearálta seo, tá sé dodhéanta na foinsí beachta as a dtáinig sonraí pearsanta a ainmniú nó bheadh iarracht dhíréireach de réir bhrí Airt i gceist leis. 14(5) lit. b GDPR. I bprionsabal, ní bhailímid sonraí pearsanta ó fhoinsí atá inrochtana go poiblí.

Is féidir le haon ábhar sonraí teagmháil a dhéanamh linn am ar bith chun faisnéis níos mionsonraithe a fháil faoi fhoinsí cruinne na sonraí pearsanta a bhaineann leis nó léi. I gcás nach féidir tionscnamh na sonraí pearsanta a sholáthar don ábhar sonraí toisc gur úsáideadh foinsí éagsúla, ba cheart faisnéis ghinearálta a sholáthar (Aithris 61 Abairt 4 GDPR).

## M. Is ann do chinnteoireacht uathoibrithe, lena n-áirítear próifíliú dá dtagraítear in Airteagal 22(1) agus (4) agus sna cásanna sin ar a laghad, d'fhaisnéis a bhaineann leis an loighic a bheidh i gceist, chomh maith le suntasacht na próiseála sin agus na hiarmhairtí a mheastar a bheadh aici ar an ábhar sonraí (Airteagal 14(2) lit. g GDPR)

Mar chuideachta fhreagrach, de ghnáth ní úsáidimid cinnteoireacht nó próifíliú uathoibrithe. Más rud é, i gcásanna eisceachtúla, go ndéanaimid cinnteoireacht nó próifíliú uathoibrithe, cuirfimid an t-ábhar sonraí ar an eolas go leithleach nó trí fho-alt inár mbeartas príobháideachta (ar ár suíomh Gréasáin). Sa chás seo, tá feidhm ag an méid seo a leanas:

Féadfaidh cinnteoireacht uathoibrithe - lena n-áirítear próifíliú - tarlú (1) má tá sé seo riachtanach chun conradh a dhéanamh, nó chun conradh a chomhlíonadh idir an duine is ábhar do na sonraí agus sinne, nó (2) má údaraítear é seo le dlí an Aontais nó an Bhallstáit lena mbaineann muid. atá faoina réir agus a leagann síos freisin bearta oiriúnacha chun cearta agus saoirsí agus leasanna dlisteanacha an duine is ábhar do na sonraí a chosaint; nó (3) tá sé seo bunaithe ar thoiliú sainráite an ábhair sonraí.

Sna cásanna dá dtagraítear in Airteagal 22(2)(a) agus (c) den GDPR, cuirfimid bearta oiriúnacha i bhfeidhm chun cearta agus saoirsí agus leasanna dlisteanacha an duine is ábhar do na sonraí a chosaint. Sna cásanna seo, tá sé de cheart agat idirghabháil dhaonna a fháil ó thaobh an rialaitheora, do dhearcadh a chur in iúl agus cur in aghaidh an chinnidh.

Tá faisnéis bhríoch faoin loighic atá i gceist, chomh maith leis an tábhacht agus na hiarmhairtí a shamhlaítear lena leithéid de phróiseáil don ábhar sonraí leagtha amach inár mbeartas príobháideachta.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## III. EU-U.S. Data Privacy Framework (EU-U.S. DPF), UK Extension to the EU-U.S. DPF, Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF)

Má tá ár n-eagraíocht ina ball deimhnithe de EU-U.S. Data Privacy Framework (EU-U.S. DPF) agus/nó UK Extension to the EU-U.S. DPF agus/nó Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF), tá na nithe seo a leanas i bhfeidhm:

Cloíonn muid leis an EU-U.S. Data Privacy Framework (EU-U.S. DPF) agus an UK Extension to the EU-U.S. DPF chomh maith leis an Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF), mar atá leagtha síos ag an U.S. Department of Commerce. Tá ár gcuideachta tar éis a dhearbhú leis an Roinn Trádála na Stát Aontaithe go gcloíonn sí leis na EU-U.S. Data Privacy Framework Principles (EU-U.S. DPF Principles) maidir le próiseáil sonraí pearsanta a fhaigheann sí ón Aontas Eorpach agus an Ríocht Aontaithe de réir EU-U.S. DPF agus an UK Extension to the EU-U.S. DPF. Tá ár gcuideachta tar éis a dhearbhú leis an Roinn Trádála na Stát Aontaithe go gcloíonn sí leis na Swiss-U.S. Data Privacy Framework Principles (Swiss-U.S. DPF Principles) maidir le próiseáil sonraí pearsanta a fhaigheann sí ón Eilvéis de réir Swiss-U.S. DPF. I gcás coimhlint idir forálacha ár bpolasaí príobháideachta agus na EU-U.S. DPF Principles agus/nó na Swiss-U.S. DPF Principles, tá na Principles cinntitheach.

Chun tuilleadh eolais a fháil faoin gclár Data Privacy Framework (DPF) agus chun ár ndeimhniú a fheiceáil, tabhair cuairt ar https://www.dataprivacyframework.gov/.

Luafar na haonaid nó na fochuideachtaí eile de chuid na Stát Aontaithe de chuid ár gcuideachta a chloíonn freisin leis na EU-U.S. DPF Principals, lena n-áirítear an UK Extension to the EU-U.S. DPF agus na Swiss-U.S. DPF Principals, más ann dóibh, inár bpolasaí príobháideachta.

De réir an EU-U.S. DPF agus an UK Extension to the EU-U.S. DPF chomh maith leis an Swiss-U.S. DPF, geallann ár gcuideachta comhoibriú leis an bpainéal arna bhunú ag údaráis cosanta sonraí an AE agus an Information Commissioner's Office (ICO) na Breataine chomh maith leis an gCoimisinéir Feidearálach Cosanta Sonraí agus Faisnéise (EDÖB) na hEilvéise agus comhairle an phainéil maidir le gearáin neamhchinnte faoi ár láimhseáil sonraí pearsanta a fhaighimid de réir an EU-U.S. DPF agus an UK Extension to the EU-U.S. DPF agus an Swiss-U.S. DPF a leanúint.

Cuirimid na daoine lena mbaineann ar an eolas faoi na húdaráis cosanta sonraí Eorpacha ábhartha atá freagrach as gearáin a bhaineann le láimhseáil sonraí pearsanta ár n-eagraíochta a phróiseáil, ag barr an doiciméid trédhearcachta seo agus go dtugann muid leigheas dlíthiúil cuí agus saor in aisce do na daoine lena mbaineann.

Cuirimid na daoine lena mbaineann ar an eolas go bhfuil ár gcuideachta faoi réir na gcumhachtaí imscrúdaithe agus forfheidhmithe ag an Federal Trade Commission (FTC).

Tá deis ag daoine lena mbaineann, faoi choinníollacha áirithe, dul i muinín eadrána cheangailteacha. Tá ár n-eagraíocht faoi dhliteanas éilimh a réiteach agus na coinníollacha a leagtar amach in Iarscríbhinn I


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

de na DPF-Principals a chomhlíonadh má tá éileamh eadrána cheangailteacha curtha isteach ag an duine lena mbaineann trí chur in iúl dár n-eagraíocht agus na nósanna imeachta agus na coinníollacha atá leagtha amach in Iarscríbhinn I de na Principals a chomhlíonadh.

Cuirimid na daoine lena mbaineann ar an eolas faoin dliteanas atá ar ár n-eagraíocht i gcás go ndéantar sonraí pearsanta a aistriú chuig tríú páirtithe.

Maidir le ceisteanna ó dhaoine lena mbaineann nó ó údaráis maoirseachta sonraí, tá ár n-ionadaithe áitiúla luaite thuas sa doiciméad trédhearcachta seo.

Cuirimid an rogha ar fáil duit (Opt-out) maidir le cibé ar cheart do shonraí pearsanta (i) a bheith aistrithe chuig tríú páirtithe nó (ii) a úsáid chun críche a bhíonn go mór difriúil ó na críche/críocha ar bhailigh siad iad ar dtús nó ar ceadaíodh níos déanaí duit. Is é an mheicníocht shoiléir, shoiléir agus inrochtana go héasca chun do rogha a fheidhmiú ná teagmháil a dhéanamh lenár n-oifigeach cosanta sonraí (DSB) trí ríomhphost. Níl aon rogha agat agus níl orainn é sin a dhéanamh más rud é go ndéantar na sonraí a aistriú chuig tríú páirtí a ghníomhaíonn mar ghníomhaire nó próiseálaí thar ár gceann agus de réir ár dtreoracha. Mar sin féin, déanaimid conradh i gcónaí le gníomhaire nó próiseálaí den sórt sin.

Maidir le sonraí íogaire (i.e. sonraí pearsanta a chuimsíonn faisnéis faoi staid sláinte, bunús ciníoch nó eitneach, tuairimí polaitiúla, creideamh reiligiúnach nó fealsúnachta, ballraíocht in aontas ceardchumann nó faisnéis faoi shaol gnéasach an duine lena mbaineann) faighimid do thoiliú sainráite (Opt-in) nuair a dhéantar na sonraí sin (i) a aistriú chuig tríú páirtithe nó (ii) a úsáid chun críche difriúil ná an ceann ar bailíodh iad ar dtús nó an ceann ar thug tú do thoiliú níos déanaí dó trí do rogha Opt-in a roghnú. Ina theannta sin, déileálfaimid le gach sonra pearsanta a fhaighimid ó thríú páirtithe mar íogair má dhéanann an tríú páirtí iad a aithint agus a láimhseáil mar íogair.

Cuirimid in iúl duit faoin riachtanas sonraí pearsanta a nochtadh mar fhreagairt ar iarratais dhlíthiúla ó údaráis, lena n-áirítear comhlíonadh riachtanais slándála náisiúnta nó forfheidhmithe dlí.

Nuair a aistrímid sonraí pearsanta chuig tríú páirtí a ghníomhaíonn mar rialaitheoir, cloímid leis na Principals fógra agus rogha. Ina theannta sin, déanaimid conradh leis an tríú páirtí atá freagrach as an bpróiseáil, a fhorálann go ndéantar na sonraí sin a phróiseáil ach amháin chun críocha teoranta agus sonracha de réir do thoilithe agus go gcaithfidh an faighteoir an leibhéal céanna cosanta a chur ar fáil leis na Principals an DPF agus cuir in iúl dúinn má chinneann sé nach féidir leis an oibleagáid sin a chomhlíonadh a thuilleadh. Foráiltear sa chonradh go gcaithfidh an tríú páirtí, atá freagrach, an phróiseáil a stopadh nó bearta cuí agus iomchuí eile a dhéanamh chun an cás a leigheas má dhéantar a leithéid de chinneadh.

Nuair a aistrímid sonraí pearsanta chuig tríú páirtí a ghníomhaíonn mar ghníomhaire nó próiseálaí, (i) ní dhéanaimid na sonraí sin a aistriú ach amháin chun críocha teoranta agus sonracha; (ii) cinntímid go bhfuil ar an ngníomhaire nó ar an bpróiseálaí an leibhéal céanna cosanta sonraí a chur ar fáil ar a laghad agus a éilíonn na DPF-Principals; (iii) glacaimid bearta cuí agus iomchuí chun a chinntiú go bpróiseálann an gníomhaire nó an próiseálaí na sonraí pearsanta a aistríodh i ndáiríre ar bhealach atá i gcomhréir


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

lenár n-oibleagáidí de réir na DPF-Principals; (iv) éilímid ar an ngníomhaire nó ar an bpróiseálaí ár n-eagraíocht a chur ar an eolas má chinneann sé nach féidir leis an leibhéal céanna cosanta a thuilleadh a chur ar fáil, mar a fhoráiltear i na DPF-Principals; (v) tar éis fógra den sórt sin, lena n-áirítear faoi (iv), glacaimid bearta cuí agus iomchuí chun an phróiseáil neamhúdaraithe a stopadh agus chun an cás a leigheas; agus (vi) cuirimid ar fáil don DPF Department, ar iarratas, achoimre nó sampla ionadaíoch de na forálacha ábhartha cosanta sonraí ó ár gconradh leis an ngníomhaire seo.

De réir an EU-U.S. DPF agus/nó an UK Extension to the EU-U.S. DPF agus/nó an Swiss-U.S. DPF, geallann ár n-eagraíocht comhoibriú leis an bpainéal arna bhunú ag údaráis cosanta sonraí an AE agus an Information Commissioner's Office (ICO) na Breataine nó an Coimisinéir Feidearálach Cosanta Sonraí agus Faisnéise (EDÖB) na hEilvéise agus cloí lena gcomhairle maidir le gearáin neamhchinnte faoi láimhseáil sonraí pearsanta a fhaighimid maidir le caidreamh fostaíochta de réir an EU-U.S. DPF agus an UK Extension to the EU-U.S. DPF agus an Swiss-U.S. DPF.

Tá gach ábhar sonraí atá san Aontas Eorpach (AE), sa Limistéar Eorpach Eacnamaíoch (LEE) nó sa Ríocht Aontaithe go sealadach, nó a bhfuil a sainchónaí nó a ngnáthchónaí ann, i dteideal na gceart agus na cearta damhna sonraí atá foilsithe inár Doiciméad Trédhearcachta, a eascraíonn freisin ó Airteagail 15 go 22 GDPR, lena n-áirítear an ceart chun rochtain a fháil ar shonraí pearsanta. Tá an fhaisnéis seo curtha ar fáil againn i dteangacha uile an AE agus LEE. Baineann an leagan Béarla leis an Ríocht Aontaithe.

Tá gach ábhar sonraí a bhfuil cónaí orthu go sealadach san Eilvéis nó a bhfuil a sainchónaí nó a ngnáthchónaí ann i dteideal na gceart agus na cearta damhna sonraí faoi Acht um Chosaint Sonraí na hEilvéise (DPA) agus faoi Rialachán na hEilvéise um Chosaint Sonraí (DPR) a fhoilsítear inár dTrédhearcacht. Doiciméad, lena n-áirítear an ceart chun rochtain a fháil ar shonraí pearsanta. Tá an fhaisnéis seo curtha ar fáil againn i dtrí theanga oifigiúla na hEilvéise (Gearmáinis, Iodáilis agus Fraincis).


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

# FINNISH: Tietoa henkilötietojen käsittelystä (tietosuoja-asetuksen 13 ja 14 artikla)

Hyvä herra tai rouva,

Jokaisen sellaisen henkilön henkilötiedot, joka on sopimussuhteessa, esisopimussuhteessa tai muussa suhteessa yritykseemme, ansaitsevat erityistä suojaa. Tavoitteenamme on pitää tietosuojan taso korkealla tasolla. Siksi kehitämme rutiininomaisesti tietosuoja- ja tietoturvakonseptejamme.

Noudatamme luonnollisesti tietosuojaa koskevia lakisääteisiä säännöksiä. Yleisen tietosuoja-asetuksen 13 ja 14 artiklan mukaan rekisterinpitäjät täyttävät henkilötietoja kerätessään tietyt tietovaatimukset. Tämä asiakirja täyttää nämä velvoitteet.

Oikeudellisten säännösten terminologia on monimutkaista. Valitettavasti tätä asiakirjaa laadittaessa ei ole voitu luopua oikeudellisten termien käytöstä. Siksi haluamme huomauttaa, että olette aina tervetulleita ottamaan meihin yhteyttä kaikissa tätä asiakirjaa, käytettyjä termejä tai muotoiluja koskevissa kysymyksissä.

## I. Toimitettavat tiedot, kun henkilötietoja kerätään rekisteröidyltä (yleinen tietosuoja-asetus, 13 artikla).

### A. Rekisterinpitäjän ja tapauksen mukaan tämän mahdollisen edustajan identiteetti ja yhteystiedot (yleisen tietosuoja-asetuksen 13 artiklan 1 ktohdan a alakoha).

Katso edellä.

### B. Tapauksen mukaan tietosuojavastaavan yhteystiedot (yleisen tietosuoja-asetuksen 13 artiklan 1 kohdan b alakohta).

Katso edellä.

### C. Henkilötietojen käsittelyn tarkoitukset sekä käsittelyn oikeusperuste (yleinen tietosuoja-asetus, 13 artiklan 1 kohdan c alakohta).

Henkilötietojen käsittelyn tarkoituksena on kaikkien sellaisten toimintojen käsittely, jotka koskevat rekisterinpitäjää, asiakkaita, potentiaalisia asiakkaita, liikekumppaneita tai muita sopimussuhteita tai


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

sopimusta edeltäviä suhteita mainittujen ryhmien välillä (laajassa merkityksessä) tai rekisterinpitäjän oikeudellisia velvoitteita.

Art. 6(1) lit. a GDPR toimii oikeusperustana käsittelytoimille, joita varten saamme suostumuksen tiettyä käsittelytarkoitusta varten. Jos henkilötietojen käsittely on tarpeen sellaisen sopimuksen täyttämiseksi, jossa rekisteröity on osapuolena, kuten esimerkiksi silloin, kun käsittelytoimet ovat tarpeen tavaroiden toimittamiseksi tai muun palvelun tarjoamiseksi, käsittely perustuu yleisen tietosuoja-asetuksen 6 artiklan 1 kohdan b alakohtaan. Sama koskee sellaisia käsittelytoimia, jotka ovat välttämättömiä sopimusta edeltävien toimenpiteiden toteuttamiseksi, esimerkiksi kun kyseessä ovat tuotteitamme tai palveluitamme koskevat tiedustelut. Jos yritykseemme kohdistuu lakisääteinen velvoite, joka edellyttää henkilötietojen käsittelyä, esimerkiksi verovelvoitteiden täyttämiseksi, käsittely perustuu GDPR art. 6(1) lit. c GDPR.

Harvinaisissa tapauksissa henkilötietojen käsittely voi olla tarpeen rekisteröidyn tai toisen luonnollisen henkilön elintärkeiden etujen suojaamiseksi. Näin olisi esimerkiksi silloin, jos kävijä loukkaantuisi yrityksessämme ja hänen nimensä, ikänsä, sairausvakuutustietonsa tai muut elintärkeät tiedot olisi välitettävä lääkärille, sairaalalle tai muulle kolmannelle osapuolelle. Tällöin käsittely perustuisi art. 6(1) lit. d GDPR.

Jos käsittely on tarpeen yleistä etua koskevan tehtävän suorittamiseksi tai rekisterinpitäjälle kuuluvan julkisen vallan käyttämiseksi, oikeusperustana on tietosuojalainsäädännön art. 6(1) lit. e GDPR.

Käsittelytoimet voivat perustua myös yleisen tietosuoja-asetuksen 6 artiklan 1 kohdan f alakohtaan. Tätä oikeusperustaa käytetään käsittelytoimiin, jotka eivät kuulu minkään edellä mainitun oikeusperusteen piiriin, jos käsittely on tarpeen yrityksemme tai kolmannen osapuolen oikeutettujen etujen vuoksi, paitsi jos rekisteröidyn edut tai perusoikeudet ja -vapaudet, jotka edellyttävät henkilötietojen suojaa, syrjäyttävät nämä edut. Tällaiset käsittelytoimet ovat erityisen sallittuja, koska eurooppalainen lainsäätäjä on nimenomaisesti maininnut ne. Hän katsoi, että oikeutettua etua voidaan olettaa olevan, jos rekisteröity on rekisterinpitäjän asiakas (yleinen tietosuoja-asetuksen johdanto-osan 47 kappaleen 2 virke).

## D. Rekisterinpitäjän tai kolmannen osapuolen oikeutetut edut, jos käsittely perustuu 6 artiklan 1 kohdan f alakohtaan (yleisen tietosuoja-asetuksen 13 artiklan 1 kohdan d alakohta).

Jos henkilötietojen käsittely perustuu yleisen tietosuoja-asetuksen 6 artiklan 1 kohdan f alakohtaan, oikeutettu etumme on harjoittaa liiketoimintaamme kaikkien työntekijöidemme ja osakkeenomistajien hyvinvoinnin hyväksi.

## E. Henkilötietojen vastaanottajat tai vastaanottajaryhmät (yleisen tietosuoja-asetuksen 13 artiklan 1 kohdan e alakohta)


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

Julkiset viranomaiset

Ulkoiset elimet

Muut ulkoiset elimet

Sisäinen käsittely

Ryhmän sisäinen käsittely

Muut elimet

Luettelo kolmansissa maissa toimivista henkilötietojen käsittelijöistä ja vastaanottajista sekä tarvittaessa kansainvälisistä organisaatioista julkaistaan verkkosivustollamme tai sitä voi pyytää meiltä maksutta. Ota yhteyttä tietosuojavastaavaamme pyytääksesi tätä luetteloa.

## F. Tapauksen mukaan tieto siitä, että rekisterinpitäjä aikoo siirtää henkilötietoja kolmanteen maahan tai kansainväliselle järjestölle, ja tieto tietosuojan riittävyyttä koskevan komission päätöksen olemassaolosta tai puuttumisesta, tai jos kyseessä on 46 tai 47 artiklassa tai 49 artiklan 1 kohdan toisessa alakohdassa tarkoitettu siirto, tieto sopivista tai asianmukaisista suojatoimista ja siitä, miten niistä saa jäljennöksen tai minne ne on asetettu saataville (yleisen tietosuoja-asetuksen 13 artiklan 1 kohdan f alakohta, 46 artiklan 1 kohta, 46 artiklan 2 kohdan c alakohta).

Kaikki konserniimme kuuluvat yritykset ja sivuliikkeet (jäljempänä "konserniyritykset"), joilla on toimipaikka tai toimisto kolmannessa maassa, voivat kuulua henkilötietojen vastaanottajiin. Luettelon kaikista konserniyhtiöistä tai vastaanottajista voi pyytää meiltä.

Yleisen tietosuoja-asetuksen 46 artiklan 1 kohdan mukaan rekisterinpitäjä tai henkilötietojen käsittelijä voi siirtää henkilötietoja kolmanteen maahan vain, jos rekisterinpitäjä tai henkilötietojen käsittelijä on toteuttanut asianmukaiset suojatoimet, ja sillä edellytyksellä, että rekisteröidyillä on käytettävissään täytäntöönpanokelpoiset rekisteröidyn oikeudet ja tehokkaat oikeussuojakeinot. Asianmukaiset takeet voidaan antaa ilman valvontaviranomaisen erityistä lupaa vakiosopimuslausekkeilla, yleisen tietosuoja-asetuksen 46 artiklan 2 kohdan c alakohta.

Kaikkien kolmansista maista tulevien vastaanottajien kanssa sovitaan Euroopan unionin vakiosopimuslausekkeista tai muista asianmukaisista suojatoimista ennen ensimmäistä henkilötietojen siirtoa. Näin varmistetaan, että rekisteröidyille taataan asianmukaiset suojatoimet, täytäntöönpanokelpoiset rekisteröidyn oikeudet ja tehokkaat oikeussuojakeinot. Jokainen rekisteröity voi saada meiltä kopion vakiosopimuslausekkeista. Vakiosopimuslausekkeet ovat saatavilla myös Euroopan unionin virallisessa lehdessä.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

Yleisen tietosuoja-asetuksen 45 artiklan 3 kohdassa annetaan Euroopan komissiolle valtuudet päättää täytäntöönpanosäädöksellä, että jokin EU:n ulkopuolinen maa takaa riittävän tietosuojan tason. Tämä tarkoittaa henkilötietojen suojan tasoa, joka vastaa olennaisilta osin EU:n suojan tasoa. Riittävyyspäätösten seurauksena henkilötiedot voivat liikkua vapaasti EU:sta (ja Norjasta, Liechtensteinista ja Islannista) kolmanteen maahan ilman lisäesteitä. Samanlaisia sääntöjä sovelletaan Yhdistyneeseen kuningaskuntaan, Sveitsiin ja joihinkin muihin maihin.

Jos Euroopan komissio tai jonkin muun maan hallitus on päättänyt, että kolmas maa takaa riittävän tietosuojan tason, ja jos käytössä on voimassa oleva kehys (esim. EU-U.S. Data Privacy Framework, Swiss-U.S. Data Privacy Framework, UK Extension to the EU-U.S. Data Privacy Framework), kaikki siirtomme tällaisten kehysten jäsenille (esim. itse sertifioiduille yksiköille) perustuvat yksinomaan kyseisen yksikön jäsenyyteen kyseisessä kehyksessä. Jos me tai jokin konserniyhteisöistämme on tällaisen kehyksen jäsen, kaikki siirrot meille tai konserniyhteisöllemme perustuvat yksinomaan kyseisen yhteisön jäsenyyteen kyseisessä kehyksessä.

Is féidir le haon ábhar sonraí cóip de na creataí a fháil uainn. Ina theannta sin, tá na creataí ar fáil freisin in Iris Oifigiúil an Aontais Eorpaigh nó sna hábhair dhlíthiúla a foilsíodh nó ar shuíomhanna gréasáin na n-údarás maoirseachta nó na n-údarás inniúil nó na na n-institiúidí inniúla eile.

## G. Henkilötietojen säilytysaika tai jos se ei ole mahdollista, tämän ajan määrittämiskriteerit (yleisen tietosuoja-asetuksen 13 artiklan 2 kohdan a alakohta).

Henkilötietojen säilytysaika määritetään lakisääteisen säilytysajan perusteella. Kyseisen ajanjakson päätyttyä vastaavat tiedot poistetaan rutiininomaisesti, kunhan ne eivät enää ole tarpeen sopimuksen täyttämiseksi tai sopimuksen aloittamiseksi.

Jos lakisääteistä säilytysaikaa ei ole, perusteena on sopimusperusteinen tai sisäinen säilytysaika.

## H. Rekisteröidyn oikeus pyytää rekisterinpitäjältä pääsy häntä itseään koskeviin henkilötietoihin sekä oikeus pyytää kyseisten tietojen oikaisemista tai poistamista taikka käsittelyn rajoittamista tai vastustaa käsittelyä sekä oikeutta siirtää tiedot järjestelmästä toiseen (yleinen tietosuoja-asetus, 13 artiklan 2 kohdan b alakohta).

Kaikilla rekisteröidyillä on seuraavat oikeudet:

***Oikeus tutustua***

Jokaisella rekisteröidyllä on oikeus tutustua itseään koskeviin henkilötietoihin. Oikeus tutustua tietoihin koskee kaikkia käsittelemiämme tietoja. Oikeutta voidaan käyttää helposti ja kohtuullisin väliajoin, jotta voidaan olla tietoisia käsittelyn laillisuudesta ja tarkistaa se (yleisen tietosuoja-asetuksen johdanto-osan


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

63 kappale). Tämä oikeus perustuu art. 15 GDPR. Rekisteröity voi ottaa meihin yhteyttä käyttäessään oikeuttaan tutustua tietoihin.

***Oikeus oikaisuun***

Yleisen tietosuoja-asetuksen 16 artiklan 1 lauseen mukaan rekisteröidyllä on oikeus saada rekisterinpitäjältä ilman aiheetonta viivytystä oikaistua häntä koskevat virheelliset henkilötiedot. Lisäksi yleisen tietosuoja-asetuksen 16 artiklan 2 lauseen mukaan rekisteröidyllä on oikeus saada puutteelliset henkilötiedot täydennettyä ottaen huomioon käsittelyn tarkoitukset, myös antamalla täydentävä ilmoitus. Rekisteröity voi ottaa meihin yhteyttä käyttäessään oikeuttaan tietojen oikaisemiseen.

***Oikeus tietojen poistamiseen (oikeus tulla unohdetuksi)***

Lisäksi rekisteröidyillä on oikeus tietojen poistamiseen ja unohtamiseen tietosuojakäytäntöä koskevan asetuksen (EY) N:o 2100/94 artiklan mukaisesti. 17 YLEISEN TIETOSUOJA-ASETUKSEN MUKAISESTI. Tätä oikeutta voi myös käyttää ottamalla meihin yhteyttä. Tässä vaiheessa haluamme kuitenkin huomauttaa, että tätä oikeutta ei sovelleta, jos käsittely on tarpeen sellaisen oikeudellisen velvoitteen täyttämiseksi, joka koskee yritystämme, yleisen tietosuoja-asetuksen 17 artiklan 3 kohdan b alakohta. Tämä tarkoittaa, että voimme hyväksyä poistopyynnön vasta lakisääteisen säilytysajan päätyttyä.

***Oikeus käsittelyn rajoittamiseen***

Yleisen tietosuoja-asetuksen 18 artiklan mukaan jokaisella rekisteröidyllä on oikeus käsittelyn rajoittamiseen. Käsittelyn rajoittamista voidaan vaatia, jos jokin yleisen tietosuoja-asetuksen 18 artiklan 1 kohdan a-d alakohdassa säädetyistä edellytyksistä täyttyy. Rekisteröity voi ottaa meihin yhteyttä voidakseen käyttää oikeuttaan käsittelyn rajoittamiseen.

***Oikeus vastustaa***

Lisäksi art. 21 GDPR takaa oikeuden vastustaa. Rekisteröity voi ottaa meihin yhteyttä voidakseen käyttää vastustamisoikeuttaan.

***Oikeus tietojen siirrettävyyteen***

Art. 20 GDPR antaa rekisteröidylle oikeuden tietojen siirrettävyyteen. Tämän säännöksen mukaan rekisteröidyllä on yleisen tietosuoja-asetuksen 20 artiklan 1 kohdan a ja b alakohdassa säädetyin edellytyksin oikeus saada itseään koskevat henkilötiedot, jotka hän on toimittanut rekisterinpitäjälle, jäsennellyssä, yleisesti käytetyssä ja koneellisesti luettavassa muodossa, ja oikeus siirtää nämä tiedot toiselle rekisterinpitäjälle ilman, että rekisterinpitäjä, jolle henkilötiedot on toimitettu, estää häntä toimittamasta niitä. Rekisteröity voi ottaa meihin yhteyttä voidakseen käyttää oikeuttaan tietojen siirtämiseen.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## I. Oikeus peruuttaa suostumus milloin tahansa tämän vaikuttamatta suostumuksen perusteella ennen sen peruuttamista suoritetun käsittelyn lainmukaisuuteen, jos käsittely perustuu 6 artiklan 1 kohdan a alakohtaan tai 9 artiklan 2 kohdan a alakohtaan (yleisen tietosuoja-asetuksen 13 artiklan 2 kohdan c alakohta).

Jos henkilötietojen käsittely perustuu art. 6 artiklan 1 kohdan a alakohtaan, mikä on tilanne, jos rekisteröity on antanut suostumuksensa henkilötietojen käsittelyyn yhtä tai useampaa erityistä tarkoitusta varten, tai jos se perustuu yleisen tietosuoja-asetuksen 9 artiklan 2 kohdan a alakohtaan, jossa säädetään nimenomaisesta suostumuksesta erityisiin henkilötietoryhmiin kuuluvien tietojen käsittelyyn, rekisteröidyllä on yleisen tietosuoja-asetuksen 7 artiklan 3 kohdan 1 virkkeen mukaisesti oikeus peruuttaa suostumuksensa milloin tahansa.

Suostumuksen peruuttaminen ei vaikuta suostumukseen ennen sen peruuttamista perustuvan käsittelyn laillisuuteen, tietosuoja-asetuksen 7 artiklan 3 kohdan 2 lause. Suostumuksen peruuttamisen on oltava yhtä helppoa kuin suostumuksen antamisen, ks. 7(3) lause 4 yleinen tietosuoja-asetus. Näin ollen suostumus voidaan aina peruuttaa samalla tavalla kuin suostumus on annettu tai muulla tavalla, jota rekisteröity pitää yksinkertaisempana. Nykyisessä tietoyhteiskunnassa yksinkertaisin tapa peruuttaa suostumus on todennäköisesti pelkkä sähköposti. Jos rekisteröity haluaa peruuttaa meille antamansa suostumuksen, pelkkä sähköpostiviesti meille riittää. Vaihtoehtoisesti rekisteröity voi valita minkä tahansa muun tavan ilmoittaa meille suostumuksensa peruuttamisesta.

## J. Oikeus tehdä valitus valvontaviranomaiselle (tietosuoja-asetuksen 13 artiklan 2 kohdan d alakohta ja 77 artiklan 1 kohta)

Rekisterinpitäjänä olemme velvollisia ilmoittamaan rekisteröidylle oikeudesta tehdä valitus valvontaviranomaiselle yleisen tietosuoja-asetuksen 13 artiklan 2 kohdan d alakohdan mukaisesti. Oikeudesta tehdä valitus valvontaviranomaiselle säädetään yleisen tietosuoja-asetuksen 77 artiklan 1 kohdassa. Tämän säännöksen mukaan jokaisella rekisteröidyllä on oikeus tehdä valitus valvontaviranomaiselle erityisesti siinä jäsenvaltiossa, jossa hänen vakinainen asuinpaikkansa, työpaikkansa tai paikka, jossa väitetty rikkominen tapahtuu, jos rekisteröity katsoo, että häntä koskevien henkilötietojen käsittelyssä rikotaan yleistä tietosuoja-asetusta, sanotun kuitenkaan rajoittamatta muita hallinnollisia tai oikeudellisia muutoksenhakukeinoja. Oikeus tehdä valitus valvontaviranomaiselle rajoitettiin unionin lainsäädännössä vain siten, että sitä voidaan käyttää vain yhden valvontaviranomaisen edessä (yleisen tietosuoja-asetuksen johdanto-osan 141 kappaleen 1 virke). Tämän säännön tarkoituksena on välttää saman rekisteröidyn tekemät kaksinkertaiset valitukset samasta asiasta. Jos rekisteröity haluaa tehdä meihin kohdistuvan valituksen, pyydämme häntä ottamaan yhteyttä vain yhteen valvontaviranomaiseen.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## K. Onko henkilötietojen antaminen lakisääteinen tai sopimukseen perustuva vaatimus taikka sopimuksen tekemisen edellyttämä vaatimus sekä onko rekisteröidyn pakko toimittaa henkilötiedot ja tällaisten tietojen antamatta jättämisen mahdolliset seuraukset (yleisen tietosuoja-asetuksen 13 artiklan 2 kohdan e alakohta).

Selvennämme, että henkilötietojen toimittamista vaaditaan osittain laissa (esim. verosäännökset) tai se voi johtua myös sopimusmääräyksistä (esim. tiedot sopimuskumppanista).

Joskus sopimuksen tekeminen voi edellyttää, että rekisteröity antaa meille henkilötietoja, joita meidän on myöhemmin käsiteltävä. Rekisteröity on esimerkiksi velvollinen antamaan meille henkilötietoja, kun yrityksemme tekee sopimuksen hänen kanssaan. Henkilötietojen toimittamatta jättäminen johtaisi siihen, että sopimusta rekisteröidyn kanssa ei voitaisi tehdä.

Ennen kuin rekisteröity toimittaa henkilötietoja, hänen on otettava meihin yhteyttä. Selvitämme rekisteröidylle, vaaditaanko henkilötietojen toimittamista lain tai sopimuksen nojalla tai onko se tarpeen sopimuksen tekemistä varten, onko henkilötietojen toimittaminen pakollista ja mitä seurauksia on henkilötietojen toimittamatta jättämisestä.

## L. Automaattisen päätöksenteon, muun muassa 22 artiklan 1 ja 4 kohdassa tarkoitetun profiloinnin olemassaolo, sekä ainakin näissä tapauksissa merkitykselliset tiedot käsittelyyn liittyvästä logiikasta samoin kuin kyseisen käsittelyn merkittävyys ja mahdolliset seuraukset rekisteröidylle (yleisen tietosuoja-asetuksen 13 artiklan 2 kohdan f alakohta).

Vastuullisena yrityksenä emme yleensä käytä automaattista päätöksentekoa tai profilointia. Jos poikkeustapauksissa käytämme automaattista päätöksentekoa tai profilointia, ilmoitamme siitä rekisteröidylle joko erikseen tai tietosuojaselosteemme (verkkosivuillamme) alajakson kautta. Tällöin sovelletaan seuraavaa:

Automaattinen päätöksenteko - mukaan lukien profilointi - voi tapahtua, jos (1) se on tarpeen rekisteröidyn ja meidän välisen sopimuksen tekemistä tai täytäntöönpanoa varten, tai (2) se on sallittua unionin tai jäsenvaltion lainsäädännön nojalla, jota me noudatamme ja jossa säädetään myös asianmukaisista toimenpiteistä rekisteröidyn oikeuksien ja vapauksien sekä oikeutettujen etujen suojaamiseksi; tai (3) se perustuu rekisteröidyn nimenomaiseen suostumukseen.

Yleisen tietosuoja-asetuksen 22 artiklan 2 kohdan a ja c alakohdassa tarkoitetuissa tapauksissa meidän on toteutettava asianmukaiset toimenpiteet rekisteröidyn oikeuksien ja vapauksien sekä oikeutettujen etujen turvaamiseksi. Näissä tapauksissa sinulla on oikeus saada rekisterinpitäjältä inhimillinen puuttuminen asiaan, ilmaista näkemyksesi ja riitauttaa päätös.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

Tietosuojaselosteessamme annetaan merkitykselliset tiedot kyseisestä logiikasta sekä tällaisen käsittelyn merkityksestä ja suunnitelluista seurauksista rekisteröidylle.

## II. Toimitettavat henkilötiedot, kun tietoja ei ole saatu rekisteröidyltä (yleinen tietosuoja-asetus 14 artikla).

### A. Rekisterinpitäjän ja tämän mahdollisen edustajan identiteetti ja yhteystiedot (yleisen tietosuoja-asetuksen 14 artiklan 1 kohdan a alakohta).

Katso edellä.

### B. Tapauksen mukaan mahdollisen tietosuojavastaavan yhteystiedot (yleisen tietosuoja-asetuksen 14 artiklan 1 kohdan b alakohta).

Katso edellä.

### C. Henkilötietojen käsittelyn tarkoitukset sekä käsittelyn oikeusperuste (yleinen tietosuoja-asetus, 14 artiklan 1 kohdan c alakohta).

Henkilötietojen käsittelyn tarkoituksena on kaikkien sellaisten toimintojen käsittely, jotka koskevat rekisterinpitäjää, asiakkaita, potentiaalisia asiakkaita, liikekumppaneita tai muita sopimussuhteita tai sopimuksia edeltäviä suhteita mainittujen ryhmien välillä (laajassa merkityksessä) tai rekisterinpitäjän oikeudellisia velvoitteita.

Jos henkilötietojen käsittely on tarpeen sellaisen sopimuksen täyttämiseksi, jonka osapuoli rekisteröity on, kuten esimerkiksi silloin, kun käsittelytoimet ovat tarpeen tavaroiden toimittamiseksi tai muun palvelun tarjoamiseksi, käsittely perustuu yleisen tietosuoja-asetuksen 6 artiklan 1 kohdan b alakohtaan. Sama koskee sellaisia käsittelytoimia, jotka ovat välttämättömiä sopimusta edeltävien toimenpiteiden suorittamiseksi, esimerkiksi kun kyseessä ovat tuotteitamme tai palveluitamme koskevat kyselyt. Jos yritykseemme kohdistuu lakisääteinen velvoite, joka edellyttää henkilötietojen käsittelyä, esimerkiksi verovelvoitteiden täyttämiseksi, käsittely perustuu GDPR art. 6(1) lit. c GDPR.

Harvinaisissa tapauksissa henkilötietojen käsittely voi olla tarpeen rekisteröidyn tai toisen luonnollisen henkilön elintärkeiden etujen suojaamiseksi. Näin olisi esimerkiksi silloin, jos kävijä loukkaantuisi yrityksessämme ja hänen nimensä, ikänsä, sairausvakuutustietonsa tai muut elintärkeät tiedot olisi välitettävä lääkärille, sairaalalle tai muulle kolmannelle osapuolelle. Tällöin käsittely perustuisi art. 6(1) lit. d GDPR.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

Jos käsittely on tarpeen yleistä etua koskevan tehtävän suorittamiseksi tai rekisterinpitäjälle kuuluvan julkisen vallan käyttämiseksi, oikeusperustana on tietosuojalainsäädännön art. 6(1) lit. e GDPR.

Käsittelytoimet voivat perustua myös yleisen tietosuoja-asetuksen 6 artiklan 1 kohdan f alakohtaan. Tätä oikeusperustaa käytetään käsittelytoimiin, jotka eivät kuulu minkään edellä mainitun oikeusperusteen piiriin, jos käsittely on tarpeen yrityksemme tai kolmannen osapuolen oikeutettujen etujen toteuttamiseksi, paitsi jos rekisteröidyn edut tai perusoikeudet ja -vapaudet, jotka edellyttävät henkilötietojen suojaa, syrjäyttävät nämä edut. Tällaiset käsittelytoimet ovat erityisen sallittuja, koska eurooppalainen lainsäätäjä on nimenomaisesti maininnut ne. Hän katsoi, että oikeutettua etua voidaan olettaa olevan, jos rekisteröity on rekisterinpitäjän asiakas (yleinen tietosuoja-asetuksen johdanto-osan 47 kappaleen 2 virke).

## D. Kyseessä olevat henkilötietoryhmät (yleisen tietosuoja-asetuksen 14 artiklan 1 kohdan d alakohta)

Asiakastiedot

Potentiaalisten asiakkaiden tiedot

Työntekijöiden tiedot

Toimittajien tiedot

## E. Mahdolliset henkilötietojen vastaanottajat tai vastaanottajaryhmät (yleisen tietosuoja-asetuksen 14 artiklan 1 kohdan e alakohta)

Julkiset viranomaiset

Ulkoiset elimet

Muut ulkoiset elimet

Sisäinen käsittely

Ryhmän sisäinen käsittely

Muut elimet

Luettelo kolmansissa maissa toimivista henkilötietojen käsittelijöistä ja vastaanottajista sekä tarvittaessa kansainvälisistä organisaatioista julkaistaan verkkosivustollamme tai sitä voi pyytää meiltä maksutta. Ota yhteyttä tietosuojavastaavaamme pyytääksesi tätä luetteloa.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## F. Tarvittaessa tieto siitä, että rekisterinpitäjä aikoo siirtää henkilötietoja kolmannessa maassa olevalle vastaanottajalle tai kansainväliselle järjestölle, ja tieto tietosuojan riittävyyttä koskevan komission päätöksen olemassaolosta tai puuttumisesta, tai jos kyseessä on 46 tai 47 artiklassa tai 49 artiklan 1 kohdan toisessa alakohdassa tarkoitettu siirto, tieto sopivista tai asianmukaisista suojatoimista ja siitä, miten niistä saa jäljennöksen tai minne ne on asetettu saataville (yleisen tietosuoja-asetuksen 14 artiklan 1 kohdan f alakohta, 46 artiklan 1 kohta, 46 artiklan 2 kohdan c alakohta).

Kaikki konserniimme kuuluvat yritykset ja sivuliikkeet (jäljempänä "konserniyritykset"), joilla on toimipaikka tai toimisto kolmannessa maassa, voivat kuulua henkilötietojen vastaanottajiin. Luettelon kaikista konserniyhtiöistä voi pyytää meiltä.

Yleisen tietosuoja-asetuksen 46 artiklan 1 kohdan mukaan rekisterinpitäjä tai henkilötietojen käsittelijä voi siirtää henkilötietoja kolmanteen maahan vain, jos rekisterinpitäjä tai henkilötietojen käsittelijä on toteuttanut asianmukaiset suojatoimet, ja sillä edellytyksellä, että rekisteröidyillä on käytettävissään täytäntöönpanokelpoiset rekisteröidyn oikeudet ja tehokkaat oikeussuojakeinot. Asianmukaiset takeet voidaan antaa ilman valvontaviranomaisen erityistä lupaa vakiomuotoisilla tietosuojalausekkeilla, yleisen tietosuoja-asetuksen 46 artiklan 2 kohdan c alakohta.

Kaikkien kolmansista maista tulevien vastaanottajien kanssa sovitaan Euroopan unionin vakiosopimuslausekkeista tai muista asianmukaisista suojatoimista ennen ensimmäistä henkilötietojen siirtoa. Näin varmistetaan, että rekisteröidyille taataan asianmukaiset suojatoimet, täytäntöönpanokelpoiset rekisteröidyn oikeudet ja tehokkaat oikeussuojakeinot. Jokainen rekisteröity voi saada meiltä kopion vakiosopimuslausekkeista. Vakiosopimuslausekkeet ovat saatavilla myös Euroopan unionin virallisessa lehdessä.

Yleisen tietosuoja-asetuksen 45 artiklan 3 kohdassa annetaan Euroopan komissiolle valtuudet päättää täytäntöönpanosäädöksellä, että jokin EU:n ulkopuolinen maa takaa riittävän tietosuojan tason. Tämä tarkoittaa henkilötietojen suojan tasoa, joka vastaa olennaisilta osin EU:n suojan tasoa. Riittävyyspäätösten seurauksena henkilötiedot voivat liikkua vapaasti EU:sta (ja Norjasta, Liechtensteinista ja Islannista) kolmanteen maahan ilman lisäesteitä. Samanlaisia sääntöjä sovelletaan Yhdistyneeseen kuningaskuntaan, Sveitsiin ja joihinkin muihin maihin.

Jos Euroopan komissio tai jonkin muun maan hallitus on päättänyt, että kolmas maa takaa riittävän tietosuojan tason, ja jos käytössä on voimassa oleva kehys (esim. EU-U.S. Data Privacy Framework, Swiss-U.S. Data Privacy Framework, UK Extension to the EU-U.S. Data Privacy Framework), kaikki siirtomme tällaisten kehysten jäsenille (esim. itse sertifioiduille yksiköille) perustuvat yksinomaan kyseisen yksikön jäsenyyteen kyseisessä kehyksessä. Jos me tai jokin konserniyhteisöistämme on


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

tällaisen kehyksen jäsen, kaikki siirrot meille tai konserniyhteisöllemme perustuvat yksinomaan kyseisen yhteisön jäsenyyteen kyseisessä kehyksessä.

Is féidir le haon ábhar sonraí cóip de na creataí a fháil uainn. Ina theannta sin, tá na creataí ar fáil freisin in Iris Oifigiúil an Aontais Eorpaigh nó sna hábhair dhlíthiúla a foilsíodh nó ar shuíomhanna gréasáin na n-údarás maoirseachta nó na n-údarás inniúil nó na na n-institiúidí inniúla eile.

## G. Henkilötietojen säilytysaika tai jos se ei ole mahdollista, tämän ajan määrittämiskriteerit (yleinen tietosuoja-asetus 14 artiklan 2 kohdan a alakohta).

Henkilötietojen säilytysaika määritetään lakisääteisen säilytysajan perusteella. Kyseisen ajanjakson päätyttyä vastaavat tiedot poistetaan rutiininomaisesti, kunhan ne eivät enää ole tarpeen sopimuksen täyttämiseksi tai sopimuksen aloittamiseksi.

Jos lakisääteistä säilytysaikaa ei ole, perusteena on sopimusperusteinen tai sisäinen säilytysaika.

## H. Rekisterinpitäjän tai kolmannen osapuolen oikeutetut edut, jos käsittely perustuu 6 artiklan 1 kohdan f alakohtaan (yleisen tietosuoja-asetuksen 14 artiklan 2 kohdan b alakohta).

Yleisen tietosuoja-asetuksen 6 artiklan 1 kohdan f alakohdan mukaan käsittely on laillista ainoastaan, jos käsittely on tarpeen rekisterinpitäjän tai kolmannen osapuolen oikeutettujen etujen toteuttamiseksi, paitsi jos rekisteröidyn edut tai perusoikeudet ja -vapaudet, jotka edellyttävät henkilötietojen suojaa, syrjäyttävät nämä edut. Yleisen tietosuoja-asetuksen johdanto-osan 47 kappaleen 2 virkkeen mukaan oikeutettu etu voi olla olemassa, jos rekisteröidyn ja rekisterinpitäjän välillä on merkityksellinen ja asianmukainen suhde, esimerkiksi tilanteissa, joissa rekisteröity on rekisterinpitäjän asiakas. Kaikissa tapauksissa, joissa yrityksemme käsittelee henkilötietoja yleisen tietosuoja-asetuksen 6 artiklan 1 kohdan f alakohdan perusteella, oikeutettu etumme on liiketoimintamme harjoittaminen kaikkien työntekijöidemme ja osakkeenomistajien hyvinvoinnin hyväksi.

## I. Rekisteröidyn oikeus pyytää rekisterinpitäjältä pääsy häntä itseään koskeviin henkilötietoihin sekä oikeus pyytää kyseisten tietojen oikaisemista tai poistamista taikka käsittelyn rajoittamista ja vastustaa käsittelyä sekä oikeutta siirtää tiedot järjestelmästä toiseen (yleisen tietosuoja-asetuksen 14 artiklan 2 kohdan c alakohta).

Kaikilla rekisteröidyillä on seuraavat oikeudet:


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

***Oikeus tutustua***

Jokaisella rekisteröidyllä on oikeus tutustua itseään koskeviin henkilötietoihin. Oikeus tutustua tietoihin koskee kaikkia käsittelemiämme tietoja. Oikeutta voidaan käyttää helposti ja kohtuullisin väliajoin, jotta voidaan olla tietoisia käsittelyn laillisuudesta ja tarkistaa se (yleisen tietosuoja-asetuksen johdanto-osan 63 kappale). Tämä oikeus perustuu art. 15 GDPR. Rekisteröity voi ottaa meihin yhteyttä käyttäessään oikeuttaan tutustua tietoihin.

***Oikeus oikaisuun***

Yleisen tietosuoja-asetuksen 16 artiklan 1 lauseen mukaan rekisteröidyllä on oikeus saada rekisterinpitäjältä ilman aiheetonta viivytystä oikaistua häntä koskevat virheelliset henkilötiedot. Lisäksi yleisen tietosuoja-asetuksen 16 artiklan 2 lauseen mukaan rekisteröidyllä on oikeus saada puutteelliset henkilötiedot täydennettyä ottaen huomioon käsittelyn tarkoitukset, myös antamalla täydentävä ilmoitus. Rekisteröity voi ottaa meihin yhteyttä käyttäessään oikeuttaan tietojen oikaisemiseen.

***Oikeus tietojen poistamiseen (oikeus tulla unohdetuksi)***

Lisäksi rekisteröidyillä on oikeus tietojen poistamiseen ja unohtamiseen tietosuojakäytäntöä koskevan asetuksen (EY) N:o 2100/94 artiklan mukaisesti. 17 YLEISEN TIETOSUOJA-ASETUKSEN MUKAISESTI. Tätä oikeutta voi myös käyttää ottamalla meihin yhteyttä. Tässä vaiheessa haluamme kuitenkin huomauttaa, että tätä oikeutta ei sovelleta, jos käsittely on tarpeen sellaisen oikeudellisen velvoitteen täyttämiseksi, joka koskee yritystämme, yleisen tietosuoja-asetuksen 17 artiklan 3 kohdan b alakohta. Tämä tarkoittaa, että voimme hyväksyä poistopyynnön vasta lakisääteisen säilytysajan päätyttyä.

***Oikeus käsittelyn rajoittamiseen***

Yleisen tietosuoja-asetuksen 18 artiklan mukaan jokaisella rekisteröidyllä on oikeus käsittelyn rajoittamiseen. Käsittelyn rajoittamista voidaan vaatia, jos jokin yleisen tietosuoja-asetuksen 18 artiklan 1 kohdan a-d alakohdassa säädetyistä edellytyksistä täyttyy. Rekisteröity voi ottaa meihin yhteyttä voidakseen käyttää oikeuttaan käsittelyn rajoittamiseen.

***Oikeus vastustaa***

Lisäksi art. 21 GDPR takaa oikeuden vastustaa. Rekisteröity voi ottaa meihin yhteyttä voidakseen käyttää vastustamisoikeuttaan.

***Oikeus tietojen siirrettävyyteen***

Art. 20 GDPR antaa rekisteröidylle oikeuden tietojen siirrettävyyteen. Tämän säännöksen mukaan rekisteröidyllä on yleisen tietosuoja-asetuksen 20 artiklan 1 kohdan a ja b alakohdassa säädetyin edellytyksin oikeus saada itseään koskevat henkilötiedot, jotka hän on toimittanut rekisterinpitäjälle, jäsennellyssä, yleisesti käytetyssä ja koneellisesti luettavassa muodossa, ja oikeus siirtää nämä tiedot toiselle rekisterinpitäjälle ilman, että rekisterinpitäjä, jolle henkilötiedot on toimitettu, estää häntä toimittamasta niitä. Rekisteröity voi ottaa meihin yhteyttä voidakseen käyttää oikeuttaan tietojen siirtämiseen.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## J. Oikeus peruuttaa suostumus milloin tahansa ilman, että tämä vaikuttaa suostumukseen perustuvan käsittelyn laillisuuteen ennen sen peruuttamista, kun käsittely perustuu yleisen tietosuoja-asetuksen 6 artiklan 1 kohdan a alakohtaan tai 9 artiklan 2 kohdan a alakohtaan (yleisen tietosuoja-asetuksen 14 artiklan 2 kohdan d alakohta).

Jos henkilötietojen käsittely perustuu art. 6 artiklan 1 kohdan a alakohtaan, mikä on tilanne, jos rekisteröity on antanut suostumuksensa henkilötietojen käsittelyyn yhtä tai useampaa erityistä tarkoitusta varten, tai jos se perustuu yleisen tietosuoja-asetuksen 9 artiklan 2 kohdan a alakohtaan, jossa säädetään nimenomaisesta suostumuksesta erityisiin henkilötietoryhmiin kuuluvien tietojen käsittelyyn, rekisteröidyllä on yleisen tietosuoja-asetuksen 7 artiklan 3 kohdan 1 virkkeen mukaisesti oikeus peruuttaa suostumuksensa milloin tahansa.

Suostumuksen peruuttaminen ei vaikuta suostumukseen ennen sen peruuttamista perustuvan käsittelyn laillisuuteen, tietosuoja-asetuksen 7 artiklan 3 kohdan 2 lause. Suostumuksen peruuttamisen on oltava yhtä helppoa kuin suostumuksen antamisen, ks. 7(3) lause 4 yleinen tietosuoja-asetus. Näin ollen suostumus voidaan aina peruuttaa samalla tavalla kuin suostumus on annettu tai muulla tavalla, jota rekisteröity pitää yksinkertaisempana. Nykyisessä tietoyhteiskunnassa yksinkertaisin tapa peruuttaa suostumus on todennäköisesti pelkkä sähköposti. Jos rekisteröity haluaa peruuttaa meille antamansa suostumuksen, pelkkä sähköpostiviesti meille riittää. Vaihtoehtoisesti rekisteröity voi valita minkä tahansa muun tavan ilmoittaa meille suostumuksensa peruuttamisesta.

## K. Oikeus tehdä valitus valvontaviranomaiselle (tietosuoja-asetuksen 14 artiklan 2 kohdan e alakohta ja 77 artiklan 1 kohta).

Rekisterinpitäjänä olemme velvollisia ilmoittamaan rekisteröidylle oikeudesta tehdä valitus valvontaviranomaiselle yleisen tietosuoja-asetuksen 14 artiklan 2 kohdan e alakohdan mukaisesti. Oikeudesta tehdä valitus valvontaviranomaiselle säädetään yleisen tietosuoja-asetuksen 77 artiklan 1 kohdassa. Tämän säännöksen mukaan jokaisella rekisteröidyllä on oikeus tehdä valitus valvontaviranomaiselle erityisesti siinä jäsenvaltiossa, jossa hänen vakinainen asuinpaikkansa, työpaikkansa tai paikka, jossa väitetty rikkominen tapahtuu, jos rekisteröity katsoo, että häntä koskevien henkilötietojen käsittelyssä rikotaan yleistä tietosuoja-asetusta, sanotun kuitenkaan rajoittamatta muita hallinnollisia tai oikeudellisia muutoksenhakukeinoja. Oikeus tehdä valitus valvontaviranomaiselle rajoitettiin unionin lainsäädännössä vain siten, että sitä voidaan käyttää vain yhden valvontaviranomaisen edessä (yleinen tietosuoja-asetus, johdanto-osan 141 kappale, 1 virke). Tämän säännön tarkoituksena on välttää saman rekisteröidyn tekemät kaksinkertaiset valitukset samasta asiasta. Jos rekisteröity haluaa tehdä meihin kohdistuvan valituksen, pyydämme häntä ottamaan yhteyttä vain yhteen valvontaviranomaiseen.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## L. Mistä henkilötiedot on saatu sekä tarvittaessa se, onko tiedot saatu yleisesti saatavilla olevista lähteistä (yleinen tietosuoja-asetus, 14 artiklan 2 kohdan f alakohta).

Periaatteessa henkilötiedot kerätään suoraan rekisteröidyltä itseltään tai yhteistyössä viranomaisen kanssa (esim. tietojen haku virallisesta rekisteristä). Muut rekisteröityjä koskevat tiedot saadaan konserniyhtiöiden tiedonsiirroista. Näiden yleisten tietojen yhteydessä henkilötietojen tarkkojen lähteiden mainitseminen on joko mahdotonta tai aiheuttaisi suhteettoman suurta vaivaa henkilötietojen siirtojen yhteydessä. 14(5) lit. b yleisen tietosuoja-asetuksen mukaisesti. Periaatteessa emme kerää henkilötietoja julkisista lähteistä.

Rekisteröity voi milloin tahansa ottaa meihin yhteyttä saadakseen tarkempia tietoja häntä koskevien henkilötietojen tarkoista lähteistä. Jos rekisteröidylle ei voida ilmoittaa henkilötietojen alkuperää, koska on käytetty eri lähteitä, on annettava yleistietoja (tietosuoja-asetuksen johdanto-osan 61 kappaleen 4 lause).

## M. Automaattisen päätöksenteon, muun muassa 22 artiklan 1 ja 4 kohdassa tarkoitetun profiloinnin olemassaolo, sekä ainakin näissä tapauksissa merkitykselliset tiedot käsittelyyn liittyvästä logiikasta samoin kuin kyseisen käsittelyn merkittävyys ja mahdolliset seuraukset rekisteröidylle (yleisen tietosuoja-asetuksen 14 artiklan 2 kohdan g alakohta).

Vastuullisena yrityksenä emme yleensä käytä automaattista päätöksentekoa tai profilointia. Jos poikkeustapauksissa käytämme automaattista päätöksentekoa tai profilointia, ilmoitamme siitä rekisteröidylle joko erikseen tai tietosuojaselosteemme (verkkosivuillamme) alajakson kautta. Tällöin sovelletaan seuraavaa:

Automaattinen päätöksenteko - mukaan lukien profilointi - voi tapahtua, jos (1) se on tarpeen rekisteröidyn ja meidän välisen sopimuksen tekemistä tai täytäntöönpanoa varten, tai (2) se on sallittua unionin tai jäsenvaltion lainsäädännön nojalla, jota me noudatamme ja jossa säädetään myös asianmukaisista toimenpiteistä rekisteröidyn oikeuksien ja vapauksien sekä oikeutettujen etujen suojaamiseksi; tai (3) se perustuu rekisteröidyn nimenomaiseen suostumukseen.

Yleisen tietosuoja-asetuksen 22 artiklan 2 kohdan a ja c alakohdassa tarkoitetuissa tapauksissa meidän on toteutettava asianmukaiset toimenpiteet rekisteröidyn oikeuksien ja vapauksien sekä oikeutettujen etujen turvaamiseksi. Näissä tapauksissa sinulla on oikeus saada rekisterinpitäjältä inhimillinen puuttuminen asiaan, ilmaista näkemyksesi ja riitauttaa päätös.

Tietosuojaselosteessamme annetaan merkitykselliset tiedot kyseisestä logiikasta sekä tällaisen käsittelyn merkityksestä ja suunnitelluista seurauksista rekisteröidylle.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## III. EU-U.S. Data Privacy Framework (EU-U.S. DPF), UK Extension to the EU-U.S. DPF, Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF)

Jos organisaatiomme on sertifioitu jäsen EU-U.S. Data Privacy Framework (EU-U.S. DPF) ja/tai UK Extension to the EU-U.S. DPF ja/tai Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF), sovelletaan seuraavaa:

Noudatamme EU-U.S. Data Privacy Framework (EU-U.S. DPF) ja UK Extension to the EU-U.S. DPF sekä Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF) sääntöjä, kuten U.S. Department of Commerce on määrittänyt. Yrityksemme on vahvistanut Yhdysvaltain kauppaministeriölle, että se noudattaa EU-U.S. Data Privacy Framework Principles (EU-U.S. DPF Principles) henkilötietojen käsittelyssä, jotka se saa Euroopan unionista ja Yhdistyneestä kuningaskunnasta EU-U.S. DPF ja UK Extension to the EU-U.S. DPF mukaisesti. Yrityksemme on vahvistanut Yhdysvaltain kauppaministeriölle, että se noudattaa Swiss-U.S. Data Privacy Framework Principles (Swiss-U.S. DPF Principles) henkilötietojen käsittelyssä, jotka se saa Sveitsistä Swiss-U.S. DPF mukaisesti. Jos yksityisyydensuojakäytäntömme ja EU-U.S. DPF Principles ja/tai Swiss-U.S. DPF Principles välillä on ristiriitoja, Principles ovat määräääviä.

Lisätietoja Data Privacy Framework (DPF) -ohjelmasta ja sertifiointimme tarkastelusta on saatavilla osoitteessa https://www.dataprivacyframework.gov/.

Muut Yhdysvaltojen yksikkömme tai tytäryhtiömme, jotka myös noudattavat EU-U.S. DPF Principals, mukaan lukien UK Extension to the EU-U.S. DPF ja Swiss-U.S. DPF Principals, mainitaan yksityisyydensuojakäytännössämme, jos niitä on.

EU-U.S. DPF ja UK Extension to the EU-U.S. DPF sekä Swiss-U.S. DPF mukaisesti yrityksemme sitoutuu tekemään yhteistyötä EU tietosuojaviranomaisten ja Yhdistyneen kuningaskunnan Information Commissioner's Office (ICO) sekä Sveitsin liittovaltion tietosuojavaltuutetun (EDÖB) perustaman paneelin kanssa ja noudattamaan heidän neuvojaan ratkaisemattomista valituksista koskien henkilötietojen käsittelyämme, jotka saamme EU-U.S. DPF, UK Extension to the EU-U.S. DPF ja Swiss-U.S. DPF mukaisesti.

Informoimme asianomaisia henkilöitä asianomaisista Euroopan tietosuojaviranomaisista, jotka ovat vastuussa valitusten käsittelystä organisaatiomme henkilötietojen käsittelystä, tämän läpinäkyvyysasiakirjan yläosassa ja siitä, että tarjoamme asianomaisille henkilöille asianmukaisen ja maksuttoman oikeussuojan.

Informoimme kaikkia asianomaisia henkilöitä siitä, että yrityksemme on Federal Trade Commissionin (FTC) tutkinta- ja täytäntöönpanovaltuuksien alainen.

Asianomaisilla henkilöillä on tietyin edellytyksin mahdollisuus käyttää sitovaa välimiesmenettelyä. Organisaatiomme on sitoutunut ratkaisemaan vaatimuksia ja noudattamaan DPF-Principalsin liitteessä I


© All rights reserved by Heiko Maniero.

esitettyjä ehtoja, jos asianomainen henkilö on pyytänyt sitovaa välimiesmenettelyä ilmoittamalla siitä organisaatiollemme ja noudattamalla liitteessä I esitettyjä menettelyjä ja ehtoja.

Informoimme täten kaikkia asianomaisia henkilöitä organisaatiomme vastuusta henkilötietojen siirrossa kolmansille osapuolille.

Asianomaisten henkilöiden tai tietosuojaviranomaisten kysymyksiin olemme nimenneet tässä läpinäkyvyysasiakirjassa mainitut paikalliset edustajat.

Tarjoamme sinulle mahdollisuuden valita (Opt-out), siirretäänkö henkilötietosi (i) kolmansille osapuolille vai (ii) käytetäänkö niitä olennaisesti eri tarkoitukseen kuin mihin ne alun perin kerättiin tai johon olet myöhemmin antanut suostumuksesi. Selkeä, näkyvä ja helposti saatavilla oleva mekanismi valinnan käyttämiseksi on ottaa yhteyttä tietosuojavastaavaamme (DSB) sähköpostitse. Sinulla ei ole valintamahdollisuutta, eikä meidän tarvitse tehdä niin, jos tiedot siirretään kolmannelle osapuolelle, joka toimii agenttina tai käsittelijänä meidän nimissämme ja ohjeidemme mukaisesti. Solmimme kuitenkin aina sopimuksen tällaisen agentin tai käsittelijän kanssa.

Herkkiä tietoja (ts. henkilötietoja, jotka sisältävät tietoja terveydentilasta, rodullisesta tai etnisestä alkuperästä, poliittisista mielipiteistä, uskonnollisista tai filosofisista uskomuksista, ammattiliiton jäsenyydestä tai asianomaisen henkilön seksuaalielämästä) varten hankimme nimenomaisen suostumuksesi (Opt-in), kun nämä tiedot (i) siirretään kolmansille osapuolille tai (ii) käytetään muuhun tarkoitukseen kuin mihin ne alun perin kerättiin tai mihin olet myöhemmin antanut suostumuksesi valitsemalla Opt-in. Lisäksi käsittelemme kaikkia kolmansilta osapuolilta saamamme henkilötietoja herkkinä, jos kolmas osapuoli tunnistaa ja käsittelee niitä herkkinä.

Informoimme sinua täten vaatimuksesta luovuttaa henkilötietoja vastauksena viranomaisten laillisiin pyyntöihin, mukaan lukien kansallisen turvallisuuden tai lainvalvonnan vaatimusten noudattaminen.

Henkilötietoja siirrettäessä kolmannelle osapuolelle, joka toimii rekisterinpitäjänä, noudatamme ilmoitus- ja valintaperiaatteita. Lisäksi solmimme kolmannen osapuolen kanssa, joka vastaa käsittelystä, sopimuksen, jossa määrätään, että näitä tietoja saa käsitellä vain rajoitettuihin ja määriteltyihin tarkoituksiin suostumuksesi mukaisesti ja että vastaanottajan on tarjottava sama suojaustaso kuin DPF Principles ja ilmoitettava meille, jos se toteaa, ettei se enää pysty täyttämään tätä velvoitetta. Sopimuksessa määrätään, että kolmas osapuoli, joka on rekisterinpitäjä, lopettaa käsittelyn tai ryhtyy muihin asianmukaisiin ja sopiviin toimenpiteisiin tilanteen korjaamiseksi, jos tällainen toteamus tehdään.

Henkilötietoja siirrettäessä kolmannelle osapuolelle, joka toimii agenttina tai käsittelijänä, (i) siirrämme nämä tiedot vain rajoitettuihin ja määriteltyihin tarkoituksiin; (ii) varmistamme, että agentin tai käsittelijän on tarjottava vähintään sama tietosuojan taso, jota DPF Principles edellyttää; (iii) ryhdymme asianmukaisiin ja sopiviin toimenpiteisiin varmistaaksemme, että agentti tai käsittelijä todella käsittelee siirrettyjä henkilötietoja tavalla, joka vastaa velvoitteitamme DPF Principles mukaisesti; (iv) vaadimme, että agentti tai käsittelijä ilmoittaa organisaatiollemme, jos se toteaa, ettei se enää pysty täyttämään velvoitetta tarjota sama suojaustaso, jota DPF Principles edellyttää; (v) tällaisen ilmoituksen jälkeen,


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

myös (iv) mukaisesti, ryhdymme asianmukaisiin ja sopiviin toimenpiteisiin luvattoman käsittelyn lopettamiseksi ja tilanteen korjaamiseksi; ja (vi) toimitamme DPF Department pyynnöstä yhteenvedon tai edustavan näytteen asianmukaisista tietosuojasäännöksistä sopimuksestamme tämän agentin kanssa.

EU-U.S. DPF ja/tai UK Extension to the EU-U.S. DPF ja/tai Swiss-U.S. DPF mukaisesti organisaatiomme sitoutuu tekemään yhteistyötä EU tietosuojaviranomaisten ja Yhdistyneen kuningaskunnan Information Commissioner's Office (ICO) tai Sveitsin liittovaltion tietosuojavaltuutetun (EDÖB) perustaman paneelin kanssa ja noudattamaan heidän neuvojaan ratkaisemattomista valituksista koskien työsuhteen yhteydessä saamiemme henkilötietojen käsittelyä EU-U.S. DPF ja UK Extension to the EU-U.S. DPF ja Swiss-U.S. DPF mukaisesti.

Kaikilla rekisteröidyillä, jotka oleskelevat tilapäisesti Euroopan unionissa (EU), Euroopan talousalueella (ETA) tai Yhdistyneessä kuningaskunnassa tai joilla on siellä kotipaikka tai vakinainen asuinpaikka, on oikeus avoimuusasiakirjassamme julkaistuihin oikeuksiin ja rekisteröidyn oikeuksiin, jotka johtuvat myös yleisen tietosuoja-asetuksen 15-22 artiklasta, mukaan lukien oikeus tutustua henkilötietoihin. Olemme asettaneet nämä tiedot saataville kaikilla EU- ja ETA-kielillä. Englanninkielinen versio koskee Yhdistynyttä kuningaskuntaa.

Kaikilla rekisteröidyillä, jotka asuvat tilapäisesti Sveitsissä tai joiden kotipaikka tai asuinpaikka on Sveitsissä, on oikeus Sveitsin tietosuojalain (DPA) ja Sveitsin tietosuoja-asetuksen (DPR) mukaisiin oikeuksiin ja rekisteröidyn oikeuksiin, jotka on julkaistu avoimuusasiakirjassamme, mukaan lukien oikeus tutustua henkilötietoihin. Olemme toimittaneet nämä tiedot Sveitsin kolmella virallisella kielellä (saksa, italia ja ranska).


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

# FINNISH: Tietoa työntekijöiden ja hakijoiden henkilötietojen käsittelystä (tietosuoja-asetuksen 13 ja 14 artikla).

Hyvä herra tai rouva,

Työntekijöiden ja hakijoiden henkilötiedot ansaitsevat erityistä suojaa. Tavoitteenamme on pitää tietosuojan taso korkealla tasolla. Siksi kehitämme rutiininomaisesti tietosuoja- ja tietoturvakonseptejamme.

Noudatamme luonnollisesti tietosuojaa koskevia lakisääteisiä säännöksiä. Yleisen tietosuoja-asetuksen 13 ja 14 artiklan mukaan rekisterinpitäjät täyttävät henkilötietoja käsitellessään tietyt tietovaatimukset. Tämä asiakirja täyttää nämä velvoitteet.

Oikeudellisen sääntelyn terminologia on monimutkaista. Valitettavasti tätä asiakirjaa laadittaessa ei ole voitu luopua oikeudellisten termien käytöstä. Siksi haluamme huomauttaa, että olette aina tervetulleita ottamaan meihin yhteyttä kaikissa tätä asiakirjaa, käytettyjä termejä tai muotoiluja koskevissa kysymyksissä.

## I. Toimitettavat tiedot, kun henkilötietoja kerätään rekisteröidyltä (yleinen tietosuoja-asetus, 13 artikla).

### A. Rekisterinpitäjän ja tapauksen mukaan tämän mahdollisen edustajan identiteetti ja yhteystiedot (yleisen tietosuoja-asetuksen 13 artiklan 1 kohdan a alakohta).

Katso edellä.

### B. Tapauksen mukaan tietosuojavastaavan yhteystiedot (yleisen tietosuoja-asetuksen 13 artiklan 1 kohdan b alakohta).

Katso edellä.

### C. Henkilötietojen käsittelyn tarkoitukset sekä käsittelyn oikeusperuste (yleinen tietosuoja-asetus, 13 artiklan 1 kohdan c alakohta).

Hakijoiden tietojen käsittelyn tarkoituksena on hakemuksen tutkiminen rekrytointiprosessin aikana. Tätä tarkoitusta varten käsittelemme kaikkia antamiasi tietoja. Rekrytointiprosessin aikana toimitettujen tietojen perusteella tarkistamme, kutsutaanko sinut työhaastatteluun (osa valintaprosessia). Yleisesti


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

sopivien hakijoiden kohdalla, erityisesti työhaastattelun yhteydessä, käsittelemme tiettyjä muita antamiasi henkilötietoja, jotka ovat olennaisia valintapäätöksen kannalta. Jos sinut palkataan meille, hakijan tiedot muuttuvat automaattisesti työntekijän tiedoiksi. Osana rekrytointiprosessia käsittelemme muita henkilötietojasi, joita pyydämme sinulta ja joita tarvitaan sopimuksen käynnistämiseksi tai täyttämiseksi (kuten henkilötunnuksia tai veronumeroita). Työntekijän tietojen osalta tietojenkäsittelyn tarkoituksena on työsopimuksen täyttäminen tai muiden työsuhteeseen sovellettavien oikeudellisten säännösten noudattaminen (esim. verolainsäädäntö) sekä henkilötietojesi käyttäminen kanssasi tehdyn työsopimuksen toteuttamiseksi (esim. nimesi ja yhteystietojesi julkaiseminen yrityksessä tai asiakkaille). Työntekijän tietoja säilytetään työsuhteen päättymisen jälkeen lakisääteisten säilytysaikojen noudattamiseksi.

Tietojenkäsittelyn oikeusperustana ovat yleisen tietosuoja-asetuksen 6 artiklan 1 kohdan b alakohta, yleisen tietosuoja-asetuksen 9 artiklan 2 kohdan b ja h alakohta, yleisen tietosuoja-asetuksen 88 artiklan 1 kohta ja kansallinen lainsäädäntö, kuten Saksan osalta BDSG:n 26 §.

## D. Henkilötietojen vastaanottajat tai vastaanottajaryhmät (yleisen tietosuoja-asetuksen 13 artiklan 1 kohdan e alakohta)

Julkiset viranomaiset

Ulkoiset elimet

Muut ulkoiset elimet

Sisäinen käsittely

Ryhmän sisäinen käsittely

Muut elimet

Luettelo kolmansissa maissa toimivista henkilötietojen käsittelijöistä ja vastaanottajista sekä tarvittaessa kansainvälisistä organisaatioista julkaistaan verkkosivustollamme tai sitä voi pyytää meiltä maksutta. Ota yhteyttä tietosuojavastaavaamme pyytääksesi tätä luetteloa.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## E. Tapauksen mukaan tieto siitä, että rekisterinpitäjä aikoo siirtää henkilötietoja kolmanteen maahan tai kansainväliselle järjestölle, ja tieto tietosuojan riittävyyttä koskevan komission päätöksen olemassaolosta tai puuttumisesta, tai jos kyseessä on 46 tai 47 artiklassa tai 49 artiklan 1 kohdan toisessa alakohdassa tarkoitettu siirto, tieto sopivista tai asianmukaisista suojatoimista ja siitä, miten niistä saa jäljennöksen tai minne ne on asetettu saataville (yleisen tietosuoja-asetuksen 13 artiklan 1 kohdan f alakohta, 46 artiklan 1 kohta, 46 artiklan 2 kohdan c alakohta).

Kaikki konserniimme kuuluvat yritykset ja sivuliikkeet (jäljempänä "konserniyritykset"), joilla on toimipaikka tai toimisto kolmannessa maassa, voivat kuulua henkilötietojen vastaanottajiin. Luettelon kaikista konserniyhtiöistä tai vastaanottajista voi pyytää meiltä.

Yleisen tietosuoja-asetuksen 46 artiklan 1 kohdan mukaan rekisterinpitäjä tai henkilötietojen käsittelijä voi siirtää henkilötietoja kolmanteen maahan vain, jos rekisterinpitäjä tai henkilötietojen käsittelijä on toteuttanut asianmukaiset suojatoimet, ja sillä edellytyksellä, että rekisteröidyillä on käytettävissään täytäntöönpanokelpoiset rekisteröidyn oikeudet ja tehokkaat oikeussuojakeinot. Asianmukaiset takeet voidaan antaa ilman valvontaviranomaisen erityistä lupaa vakiosopimuslausekkeilla, yleisen tietosuoja-asetuksen 46 artiklan 2 kohdan c alakohta.

Kaikkien kolmansista maista tulevien vastaanottajien kanssa sovitaan Euroopan unionin vakiosopimuslausekkeista tai muista asianmukaisista suojatoimista ennen ensimmäistä henkilötietojen siirtoa. Näin varmistetaan, että rekisteröidyille taataan asianmukaiset suojatoimet, täytäntöönpanokelpoiset rekisteröidyn oikeudet ja tehokkaat oikeussuojakeinot. Jokainen rekisteröity voi saada meiltä kopion vakiosopimuslausekkeista. Vakiosopimuslausekkeet ovat saatavilla myös Euroopan unionin virallisessa lehdessä.

Yleisen tietosuoja-asetuksen 45 artiklan 3 kohdassa annetaan Euroopan komissiolle valtuudet päättää täytäntöönpanosäädöksellä, että jokin EU:n ulkopuolinen maa takaa riittävän tietosuojan tason. Tämä tarkoittaa henkilötietojen suojan tasoa, joka vastaa olennaisilta osin EU:n suojan tasoa. Riittävyyspäätösten seurauksena henkilötiedot voivat liikkua vapaasti EU:sta (ja Norjasta, Liechtensteinista ja Islannista) kolmanteen maahan ilman lisäesteitä. Samanlaisia sääntöjä sovelletaan Yhdistyneeseen kuningaskuntaan, Sveitsiin ja joihinkin muihin maihin.

Jos Euroopan komissio tai jonkin muun maan hallitus on päättänyt, että kolmas maa takaa riittävän tietosuojan tason, ja jos käytössä on voimassa oleva kehys (esim. EU-U.S. Data Privacy Framework, Swiss-U.S. Data Privacy Framework, UK Extension to the EU-U.S. Data Privacy Framework), kaikki siirtomme tällaisten kehysten jäsenille (esim. itse sertifioiduille yksiköille) perustuvat yksinomaan kyseisen yksikön jäsenyyteen kyseisessä kehyksessä. Jos me tai jokin konserniyhteisöistämme on tällaisen kehyksen jäsen, kaikki siirrot meille tai konserniyhteisöllemme perustuvat yksinomaan kyseisen yhteisön jäsenyyteen kyseisessä kehyksessä.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

Is féidir le haon ábhar sonraí cóip de na creataí a fháil uainn. Ina theannta sin, tá na creataí ar fáil freisin in Iris Oifigiúil an Aontais Eorpaigh nó sna hábhair dhlíthiúla a foilsíodh nó ar shuíomhanna gréasáin na n-údarás maoirseachta nó na n-údarás inniúil nó na na n-institiúidí inniúla eile.

## F. Henkilötietojen säilytysaika tai jos se ei ole mahdollista, tämän ajan määrittämiskriteerit (yleisen tietosuoja-asetuksen 13 artiklan 2 kohdan a alakohta).

Hakijoiden henkilötietoja säilytetään 6 kuukautta. Työntekijöiden tietoihin sovelletaan vastaavaa lakisääteistä säilytysaikaa. Tämän ajanjakson päätyttyä vastaavat tiedot poistetaan rutiininomaisesti, kunhan ne eivät enää ole tarpeen sopimuksen täyttämiseksi tai sopimuksen aloittamiseksi.

## G. Rekisteröidyn oikeus pyytää rekisterinpitäjältä pääsy häntä itseään koskeviin henkilötietoihin sekä oikeus pyytää kyseisten tietojen oikaisemista tai poistamista taikka käsittelyn rajoittamista tai vastustaa käsittelyä sekä oikeutta siirtää tiedot järjestelmästä toiseen (yleinen tietosuoja-asetus, 13 artiklan 2 kohdan b alakohta).

Kaikilla rekisteröidyillä on seuraavat oikeudet:

***Oikeus tutustua***

Jokaisella rekisteröidyllä on oikeus tutustua itseään koskeviin henkilötietoihin. Oikeus tutustua tietoihin koskee kaikkia käsittelemiämme tietoja. Oikeutta voidaan käyttää helposti ja kohtuullisin väliajoin, jotta voidaan olla tietoisia käsittelyn laillisuudesta ja tarkistaa se (yleisen tietosuoja-asetuksen johdanto-osan 63 kappale). Tämä oikeus perustuu art. 15 GDPR. Rekisteröity voi ottaa meihin yhteyttä käyttäessään oikeuttaan tutustua tietoihin.

***Oikeus oikaisuun***

Yleisen tietosuoja-asetuksen 16 artiklan 1 lauseen mukaan rekisteröidyllä on oikeus saada rekisterinpitäjältä ilman aiheetonta viivytystä oikaistua häntä koskevat virheelliset henkilötiedot. Lisäksi yleisen tietosuoja-asetuksen 16 artiklan 2 lauseen mukaan rekisteröidyllä on oikeus saada puutteelliset henkilötiedot täydennettyä ottaen huomioon käsittelyn tarkoitukset, myös antamalla täydentävä ilmoitus. Rekisteröity voi ottaa meihin yhteyttä käyttäessään oikeuttaan tietojen oikaisemiseen.

***Oikeus tietojen poistamiseen (oikeus tulla unohdetuksi)***

Lisäksi rekisteröidyillä on oikeus tietojen poistamiseen ja unohtamiseen tietosuojakäytäntöä koskevan asetuksen (EY) N:o 2100/94 artiklan mukaisesti. 17 YLEISEN TIETOSUOJA-ASETUKSEN MUKAISESTI. Tätä oikeutta voi myös käyttää ottamalla meihin yhteyttä. Tässä vaiheessa haluamme kuitenkin huomauttaa, että tätä oikeutta ei sovelleta, jos käsittely on tarpeen sellaisen oikeudellisen velvoitteen täyttämiseksi, joka koskee yritystämme, yleisen tietosuoja-asetuksen 17 artiklan 3 kohdan b alakohta. Tämä tarkoittaa, että voimme hyväksyä poistopyynnön vasta lakisääteisen säilytysajan päätyttyä.


© All rights reserved by Heiko Maniero.

***Oikeus käsittelyn rajoittamiseen***

Yleisen tietosuoja-asetuksen 18 artiklan mukaan jokaisella rekisteröidyllä on oikeus käsittelyn rajoittamiseen. Käsittelyn rajoittamista voidaan vaatia, jos jokin yleisen tietosuoja-asetuksen 18 artiklan 1 kohdan a-d alakohdassa säädetyistä edellytyksistä täyttyy. Rekisteröity voi ottaa meihin yhteyttä käyttäessään oikeuttaan käsittelyn rajoittamiseen.

***Oikeus vastustaa***

Lisäksi art. 21 GDPR takaa oikeuden vastustaa. Rekisteröity voi ottaa meihin yhteyttä voidakseen käyttää vastustamisoikeuttaan.

***Oikeus tietojen siirrettävyyteen***

Art. 20 GDPR antaa rekisteröidylle oikeuden tietojen siirrettävyyteen. Tämän säännöksen mukaan rekisteröidyllä on yleisen tietosuoja-asetuksen 20 artiklan 1 kohdan a ja b alakohdassa säädetyin edellytyksin oikeus saada itseään koskevat henkilötiedot, jotka hän on toimittanut rekisterinpitäjälle, jäsennellyssä, yleisesti käytetyssä ja koneellisesti luettavassa muodossa, ja oikeus siirtää nämä tiedot toiselle rekisterinpitäjälle ilman, että rekisterinpitäjä, jolle henkilötiedot on toimitettu, estää häntä toimittamasta niitä. Rekisteröity voi ottaa meihin yhteyttä voidakseen käyttää oikeuttaan tietojen siirtämiseen.

## H. Oikeus peruuttaa suostumus milloin tahansa tämän vaikuttamatta suostumuksen perusteella ennen sen peruuttamista suoritetun käsittelyn lainmukaisuuteen, jos käsittely perustuu 6 artiklan 1 kohdan a alakohtaan tai 9 artiklan 2 kohdan a alakohtaan (yleisen tietosuoja-asetuksen 13 artiklan 2 kohdan c alakohta).

Jos henkilötietojen käsittely perustuu art. 6 artiklan 1 kohdan a alakohtaan, mikä on tilanne, jos rekisteröity on antanut suostumuksensa henkilötietojen käsittelyyn yhtä tai useampaa erityistä tarkoitusta varten, tai jos se perustuu yleisen tietosuoja-asetuksen 9 artiklan 2 kohdan a alakohtaan, jossa säädetään nimenomaisesta suostumuksesta erityisiin henkilötietoryhmiin kuuluvien tietojen käsittelyyn, rekisteröidyllä on yleisen tietosuoja-asetuksen 7 artiklan 3 kohdan 1 virkkeen mukaisesti oikeus peruuttaa suostumuksensa milloin tahansa.

Suostumuksen peruuttaminen ei vaikuta suostumukseen ennen sen peruuttamista perustuvan käsittelyn laillisuuteen, tietosuoja-asetuksen 7 artiklan 3 kohdan 2 lause. Suostumuksen peruuttamisen on oltava yhtä helppoa kuin suostumuksen antamisen, ks. 7(3) lause 4 yleinen tietosuoja-asetus. Näin ollen suostumus voidaan aina peruuttaa samalla tavalla kuin suostumus on annettu tai muulla tavalla, jota rekisteröity pitää yksinkertaisempana. Nykyisessä tietoyhteiskunnassa yksinkertaisin tapa peruuttaa suostumus on todennäköisesti pelkkä sähköposti. Jos rekisteröity haluaa peruuttaa meille antamansa suostumuksen, pelkkä sähköpostiviesti meille riittää. Vaihtoehtoisesti rekisteröity voi valita minkä tahansa muun tavan ilmoittaa meille suostumuksensa peruuttamisesta.


© All rights reserved by Heiko Maniero.

## I. Oikeus tehdä valitus valvontaviranomaiselle (tietosuoja-asetuksen 13 artiklan 2 kohdan d alakohta ja 77 artiklan 1 kohta).

Rekisterinpitäjänä olemme velvollisia ilmoittamaan rekisteröidylle oikeudesta tehdä valitus valvontaviranomaiselle yleisen tietosuoja-asetuksen 13 artiklan 2 kohdan d alakohdan mukaisesti. Oikeudesta tehdä valitus valvontaviranomaiselle säädetään yleisen tietosuoja-asetuksen 77 artiklan 1 kohdassa. Tämän säännöksen mukaan jokaisella rekisteröidyllä on oikeus tehdä valitus valvontaviranomaiselle erityisesti siinä jäsenvaltiossa, jossa hänen vakinainen asuinpaikkansa, työpaikkansa tai paikka, jossa väitetty rikkominen tapahtuu, jos rekisteröity katsoo, että häntä koskevien henkilötietojen käsittelyssä rikotaan yleistä tietosuoja-asetusta, sanotun kuitenkaan rajoittamatta muita hallinnollisia tai oikeudellisia muutoksenhakukeinoja. Oikeus tehdä valitus valvontaviranomaiselle rajoitettiin unionin lainsäädännössä vain siten, että sitä voidaan käyttää vain yhden valvontaviranomaisen edessä (yleinen tietosuoja-asetus, johdanto-osan 141 kappale, 1 virke). Tämän säännön tarkoituksena on välttää saman rekisteröidyn tekemät kaksinkertaiset valitukset samasta asiasta. Jos rekisteröity haluaa tehdä meihin kohdistuvan valituksen, pyydämme häntä ottamaan yhteyttä vain yhteen valvontaviranomaiseen.

## J. Onko henkilötietojen antaminen lakisääteinen tai sopimukseen perustuva vaatimus taikka sopimuksen tekemisen edellyttämä vaatimus sekä onko rekisteröidyn pakko toimittaa henkilötiedot ja tällaisten tietojen antamatta jättämisen mahdolliset seuraukset (yleisen tietosuoja-asetuksen 13 artiklan 2 kohdan e alakohta).

Selvennämme, että henkilötietojen toimittamista vaaditaan osittain laissa (esim. verosäännökset) tai se voi johtua myös sopimusmääräyksistä (esim. tiedot sopimuskumppanista).

Joskus sopimuksen tekeminen voi edellyttää, että rekisteröity antaa meille henkilötietoja, joita meidän on myöhemmin käsiteltävä. Rekisteröity on esimerkiksi velvollinen antamaan meille henkilötietoja, kun yrityksemme tekee sopimuksen hänen kanssaan. Henkilötietojen toimittamatta jättäminen johtaisi siihen, että sopimusta rekisteröidyn kanssa ei voitaisi tehdä.

Ennen kuin rekisteröity toimittaa henkilötietoja, hänen on otettava meihin yhteyttä. Selvitämme rekisteröidylle, vaaditaanko henkilötietojen toimittamista lain tai sopimuksen nojalla tai onko se tarpeen sopimuksen tekemistä varten, onko henkilötietojen toimittaminen pakollista ja mitä seurauksia on henkilötietojen toimittamatta jättämisestä.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

### K. Automaattisen päätöksenteon, muun muassa 22 artiklan 1 ja 4 kohdassa tarkoitetun profiloinnin olemassaolo, sekä ainakin näissä tapauksissa merkitykselliset tiedot käsittelyyn liittyvästä logiikasta samoin kuin kyseisen käsittelyn merkittävyys ja mahdolliset seuraukset rekisteröidylle (yleisen tietosuoja-asetuksen 13 artiklan 2 kohdan f alakohta).

Vastuullisena yrityksenä emme yleensä käytä automaattista päätöksentekoa tai profilointia. Jos poikkeustapauksissa käytämme automaattista päätöksentekoa tai profilointia, ilmoitamme siitä rekisteröidylle joko erikseen tai tietosuojaselosteemme (verkkosivuillamme) alajakson kautta. Tällöin sovelletaan seuraavaa:

Automaattinen päätöksenteko - mukaan lukien profilointi - voi tapahtua, jos (1) se on tarpeen rekisteröidyn ja meidän välisen sopimuksen tekemistä tai täytäntöönpanoa varten, tai (2) se on sallittua unionin tai jäsenvaltion lainsäädännön nojalla, jota me noudatamme ja jossa säädetään myös asianmukaisista toimenpiteistä rekisteröidyn oikeuksien ja vapauksien sekä oikeutettujen etujen suojaamiseksi; tai (3) se perustuu rekisteröidyn nimenomaiseen suostumukseen.

Yleisen tietosuoja-asetuksen 22 artiklan 2 kohdan a ja c alakohdassa tarkoitetuissa tapauksissa meidän on toteutettava asianmukaiset toimenpiteet rekisteröidyn oikeuksien ja vapauksien sekä oikeutettujen etujen turvaamiseksi. Näissä tapauksissa sinulla on oikeus saada rekisterinpitäjältä inhimillinen puuttuminen asiaan, ilmaista näkemyksesi ja riitauttaa päätös.

Tietosuojaselosteessamme annetaan merkitykselliset tiedot kyseisestä logiikasta sekä tällaisen käsittelyn merkityksestä ja suunnitelluista seurauksista rekisteröidylle.

## II. Toimitettavat henkilötiedot, kun tietoja ei ole saatu rekisteröidyltä (yleinen tietosuoja-asetus 14 artikla).

### A. Rekisterinpitäjän ja tämän mahdollisen edustajan identiteetti ja yhteystiedot (yleisen tietosuoja-asetuksen 14 artiklan 1 kohdan a alakohta).

Katso edellä.

### B. Tapauksen mukaan mahdollisen tietosuojavastaavan yhteystiedot (yleisen tietosuoja-asetuksen 14 artiklan 1 kohdan b alakohta).

Katso edellä.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## C. Henkilötietojen käsittelyn tarkoitukset sekä käsittelyn oikeusperuste (yleinen tietosuoja-asetus, 14 artiklan 1 kohdan c alakohta).

Niiden hakijatietojen osalta, joita ei ole kerätty rekisteröidyltä itseltään, tietojenkäsittelyn tarkoituksena on hakemuksen tutkiminen rekrytointiprosessin aikana. Tätä tarkoitusta varten voimme käsitellä tietoja, joita ei ole kerätty hakijalta. Rekrytointiprosessin aikana käsiteltyjen tietojen perusteella tarkistamme, kutsutaanko sinut työhaastatteluun (osa valintaprosessia). Jos sinut palkataan meille, hakijan tiedot muuttuvat automaattisesti työntekijän tiedoiksi. Työntekijätietojen osalta tietojenkäsittelyn tarkoitus on työsopimuksen täyttäminen tai muiden työsuhteeseen sovellettavien oikeudellisten säännösten noudattaminen. Työntekijätietoja säilytetään työsuhteen päättymisen jälkeen lakisääteisten säilytysaikojen noudattamiseksi.

Tietojenkäsittelyn oikeusperustana ovat yleisen tietosuoja-asetuksen 6 artiklan 1 kohdan b ja f alakohta, yleisen tietosuoja-asetuksen 9 artiklan 2 kohdan b ja h alakohta, yleisen tietosuoja-asetuksen 88 artiklan 1 kohta ja kansallinen lainsäädäntö, kuten Saksan osalta BDSG:n 26 § (liittovaltion tietosuojalaki).

## D. Kyseessä olevat henkilötietoryhmät (yleisen tietosuoja-asetuksen 14 artiklan 1 kohdan d alakohta)

Hakijan tiedot

Työntekijöiden tiedot

## E. Mahdolliset henkilötietojen vastaanottajat tai vastaanottajaryhmät (yleisen tietosuoja-asetuksen 14 artiklan 1 kohdan e alakohta)

Julkiset viranomaiset

Ulkoiset elimet

Muut ulkoiset elimet

Sisäinen käsittely

Ryhmän sisäinen käsittely

Muut elimet


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

Luettelo kolmansissa maissa toimivista henkilötietojen käsittelijöistä ja vastaanottajista sekä tarvittaessa kansainvälisistä organisaatioista julkaistaan verkkosivustollamme tai sitä voi pyytää meiltä maksutta. Ota yhteyttä tietosuojavastaavaamme pyytääksesi tätä luetteloa.

## F. Tarvittaessa tieto siitä, että rekisterinpitäjä aikoo siirtää henkilötietoja kolmannessa maassa olevalle vastaanottajalle tai kansainväliselle järjestölle, ja tieto tietosuojan riittävyyttä koskevan komission päätöksen olemassaolosta tai puuttumisesta, tai jos kyseessä on 46 tai 47 artiklassa tai 49 artiklan 1 kohdan toisessa alakohdassa tarkoitettu siirto, tieto sopivista tai asianmukaisista suojatoimista ja siitä, miten niistä saa jäljennöksen tai minne ne on asetettu saataville (yleisen tietosuoja-asetuksen 14 artiklan 1 kohdan f alakohta, 46 artiklan 1 kohta, 46 artiklan 2 kohdan c alakohta).

Kaikki konserniimme kuuluvat yritykset ja sivuliikkeet (jäljempänä "konserniyritykset"), joilla on toimipaikka tai toimisto kolmannessa maassa, voivat kuulua henkilötietojen vastaanottajiin. Luettelon kaikista konserniyhtiöistä tai vastaanottajista voi pyytää meiltä.

Yleisen tietosuoja-asetuksen 46 artiklan 1 kohdan mukaan rekisterinpitäjä tai henkilötietojen käsittelijä voi siirtää henkilötietoja kolmanteen maahan vain, jos rekisterinpitäjä tai henkilötietojen käsittelijä on toteuttanut asianmukaiset suojatoimet, ja sillä edellytyksellä, että rekisteröidyillä on käytettävissään täytäntöönpanokelpoiset rekisteröidyn oikeudet ja tehokkaat oikeussuojakeinot. Asianmukaiset takeet voidaan antaa ilman valvontaviranomaisen erityistä lupaa vakiomuotoisilla tietosuojalausekkeilla, yleisen tietosuoja-asetuksen 46 artiklan 2 kohdan c alakohta.

Kaikkien kolmansista maista tulevien vastaanottajien kanssa sovitaan Euroopan unionin vakiosopimuslausekkeista tai muista asianmukaisista suojatoimista ennen ensimmäistä henkilötietojen siirtoa. Näin varmistetaan, että rekisteröidyille taataan asianmukaiset suojatoimet, täytäntöönpanokelpoiset rekisteröidyn oikeudet ja tehokkaat oikeussuojakeinot. Jokainen rekisteröity voi saada meiltä kopion vakiosopimuslausekkeista. Vakiosopimuslausekkeet ovat saatavilla myös Euroopan unionin virallisessa lehdessä.

Yleisen tietosuoja-asetuksen 45 artiklan 3 kohdassa annetaan Euroopan komissiolle valtuudet päättää täytäntöönpanosäädöksellä, että jokin EU:n ulkopuolinen maa takaa riittävän tietosuojan tason. Tämä tarkoittaa henkilötietojen suojan tasoa, joka vastaa olennaisilta osin EU:n suojan tasoa. Riittävyyspäätösten seurauksena henkilötiedot voivat liikkua vapaasti EU:sta (ja Norjasta, Liechtensteinista ja Islannista) kolmanteen maahan ilman lisäesteitä. Samanlaisia sääntöjä sovelletaan Yhdistyneeseen kuningaskuntaan, Sveitsiin ja joihinkin muihin maihin.

Jos Euroopan komissio tai jonkin muun maan hallitus on päättänyt, että kolmas maa takaa riittävän tietosuojan tason, ja jos käytössä on voimassa oleva kehys (esim. EU-U.S. Data Privacy Framework,


© All rights reserved by Heiko Maniero.

Swiss-U.S. Data Privacy Framework, UK Extension to the EU-U.S. Data Privacy Framework), kaikki siirtomme tällaisten kehysten jäsenille (esim. itse sertifioiduille yksiköille) perustuvat yksinomaan kyseisen yksikön jäsenyyteen kyseisessä kehyksessä. Jos me tai jokin konserniyhteisöistämme on tällaisen kehyksen jäsen, kaikki siirrot meille tai konserniyhteisöllemme perustuvat yksinomaan kyseisen yhteisön jäsenyyteen kyseisessä kehyksessä.

Is féidir le haon ábhar sonraí cóip de na creataí a fháil uainn. Ina theannta sin, tá na creataí ar fáil freisin in Iris Oifigiúil an Aontais Eorpaigh nó sna hábhair dhlíthiúla a foilsíodh nó ar shuíomhanna gréasáin na n-údarás maoirseachta nó na n-údarás inniúil nó na na n-institiúidí inniúla eile.

## G. Henkilötietojen säilytysaika tai jos se ei ole mahdollista, tämän ajan määrittämiskriteerit (yleinen tietosuoja-asetus 14 artiklan 2 kohdan a alakohta).

Hakijoiden henkilötietoja säilytetään 6 kuukautta. Työntekijöiden tietoihin sovelletaan vastaavaa lakisääteistä säilytysaikaa. Tämän ajanjakson päätyttyä vastaavat tiedot poistetaan rutiininomaisesti, kunhan ne eivät enää ole tarpeen sopimuksen täyttämiseksi tai sopimuksen aloittamiseksi.

## H. Rekisterinpitäjän tai kolmannen osapuolen oikeutetut edut, jos käsittely perustuu 6 artiklan 1 kohdan f alakohtaan (yleisen tietosuoja-asetuksen 14 artiklan 2 kohdan b alakohta).

Yleisen tietosuoja-asetuksen 6 artiklan 1 kohdan f alakohdan mukaan käsittely on laillista ainoastaan, jos käsittely on tarpeen rekisterinpitäjän tai kolmannen osapuolen oikeutettujen etujen toteuttamiseksi, paitsi jos rekisteröidyn edut tai perusoikeudet ja -vapaudet, jotka edellyttävät henkilötietojen suojaa, syrjäyttävät nämä edut. Yleisen tietosuoja-asetuksen johdanto-osan 47 kappaleen 2 virkkeen mukaan oikeutettu etu voi olla olemassa, jos rekisteröidyn ja rekisterinpitäjän välillä on merkityksellinen ja asianmukainen suhde, esimerkiksi tilanteissa, joissa rekisteröity on rekisterinpitäjän asiakas. Kaikissa tapauksissa, joissa yrityksemme käsittelee hakijoiden tietoja yleisen tietosuoja-asetuksen 6 artiklan 1 kohdan f alakohdan perusteella, oikeutettu etumme on sopivan henkilöstön ja ammattilaisten palkkaaminen.

## I. Rekisteröidyn oikeus pyytää rekisterinpitäjältä pääsy häntä itseään koskeviin henkilötietoihin sekä oikeus pyytää kyseisten tietojen oikaisemista tai poistamista taikka käsittelyn rajoittamista ja vastustaa käsittelyä sekä oikeutta siirtää tiedot järjestelmästä toiseen (yleisen tietosuoja-asetuksen 14 artiklan 2 kohdan c alakohta).

Kaikilla rekisteröidyillä on seuraavat oikeudet:


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

***Oikeus tutustua***

Jokaisella rekisteröidyllä on oikeus tutustua itseään koskeviin henkilötietoihin. Oikeus tutustua tietoihin koskee kaikkia käsittelemiämme tietoja. Oikeutta voidaan käyttää helposti ja kohtuullisin väliajoin, jotta voidaan olla tietoisia käsittelyn laillisuudesta ja tarkistaa se (yleisen tietosuoja-asetuksen johdanto-osan 63 kappale). Tämä oikeus perustuu art. 15 GDPR. Rekisteröity voi ottaa meihin yhteyttä käyttäessään oikeuttaan tutustua tietoihin.

***Oikeus oikaisuun***

Yleisen tietosuoja-asetuksen 16 artiklan 1 lauseen mukaan rekisteröidyllä on oikeus saada rekisterinpitäjältä ilman aiheetonta viivytystä oikaistua häntä koskevat virheelliset henkilötiedot. Lisäksi yleisen tietosuoja-asetuksen 16 artiklan 2 lauseen mukaan rekisteröidyllä on oikeus saada puutteelliset henkilötiedot täydennettyä ottaen huomioon käsittelyn tarkoitukset, myös antamalla täydentävä ilmoitus. Rekisteröity voi ottaa meihin yhteyttä käyttäessään oikeuttaan tietojen oikaisemiseen.

***Oikeus tietojen poistamiseen (oikeus tulla unohdetuksi)***

Lisäksi rekisteröidyillä on oikeus tietojen poistamiseen ja unohtamiseen tietosuojakäytäntöä koskevan asetuksen (EY) N:o 2100/94 artiklan mukaisesti. 17 YLEISEN TIETOSUOJA-ASETUKSEN MUKAISESTI. Tätä oikeutta voi myös käyttää ottamalla meihin yhteyttä. Tässä vaiheessa haluamme kuitenkin huomauttaa, että tätä oikeutta ei sovelleta, jos käsittely on tarpeen sellaisen oikeudellisen velvoitteen täyttämiseksi, joka koskee yritystämme, yleisen tietosuoja-asetuksen 17 artiklan 3 kohdan b alakohta. Tämä tarkoittaa, että voimme hyväksyä poistopyynnön vasta lakisääteisen säilytysajan päätyttyä.

***Oikeus käsittelyn rajoittamiseen***

Yleisen tietosuoja-asetuksen 18 artiklan mukaan jokaisella rekisteröidyllä on oikeus käsittelyn rajoittamiseen. Käsittelyn rajoittamista voidaan vaatia, jos jokin yleisen tietosuoja-asetuksen 18 artiklan 1 kohdan a-d alakohdassa säädetyistä edellytyksistä täyttyy. Rekisteröity voi ottaa meihin yhteyttä voidakseen käyttää oikeuttaan käsittelyn rajoittamiseen.

***Oikeus vastustaa***

Lisäksi art. 21 GDPR takaa oikeuden vastustaa. Rekisteröity voi ottaa meihin yhteyttä voidakseen käyttää vastustamisoikeuttaan.

***Oikeus tietojen siirrettävyyteen***

Art. 20 GDPR antaa rekisteröidylle oikeuden tietojen siirrettävyyteen. Tämän säännöksen mukaan rekisteröidyllä on yleisen tietosuoja-asetuksen 20 artiklan 1 kohdan a ja b alakohdassa säädetyin edellytyksin oikeus saada itseään koskevat henkilötiedot, jotka hän on toimittanut rekisterinpitäjälle, jäsennellyssä, yleisesti käytetyssä ja koneellisesti luettavassa muodossa, ja oikeus siirtää nämä tiedot toiselle rekisterinpitäjälle ilman, että rekisterinpitäjä, jolle henkilötiedot on toimitettu, estää häntä toimittamasta niitä. Rekisteröity voi ottaa meihin yhteyttä voidakseen käyttää oikeuttaan tietojen siirtämiseen.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## J. Oikeus peruuttaa suostumus milloin tahansa ilman, että tämä vaikuttaa suostumukseen perustuvan käsittelyn laillisuuteen ennen sen peruuttamista, kun käsittely perustuu yleisen tietosuoja-asetuksen 6 artiklan 1 kohdan a alakohtaan tai 9 artiklan 2 kohdan a alakohtaan (yleisen tietosuoja-asetuksen 14 artiklan 2 kohdan d alakohta).

Jos henkilötietojen käsittely perustuu art. 6 artiklan 1 kohdan a alakohtaan, mikä on tilanne, jos rekisteröity on antanut suostumuksensa henkilötietojen käsittelyyn yhtä tai useampaa erityistä tarkoitusta varten, tai jos se perustuu yleisen tietosuoja-asetuksen 9 artiklan 2 kohdan a alakohtaan, jossa säädetään nimenomaisesta suostumuksesta erityisiin henkilötietoryhmiin kuuluvien tietojen käsittelyyn, rekisteröidyllä on yleisen tietosuoja-asetuksen 7 artiklan 3 kohdan 1 virkkeen mukaisesti oikeus peruuttaa suostumuksensa milloin tahansa.

Suostumuksen peruuttaminen ei vaikuta suostumukseen ennen sen peruuttamista perustuvan käsittelyn laillisuuteen, tietosuoja-asetuksen 7 artiklan 3 kohdan 2 lause. Suostumuksen peruuttamisen on oltava yhtä helppoa kuin suostumuksen antamisen, ks. 7(3) lause 4 yleinen tietosuoja-asetus. Näin ollen suostumus voidaan aina peruuttaa samalla tavalla kuin suostumus on annettu tai muulla tavalla, jota rekisteröity pitää yksinkertaisempana. Nykyisessä tietoyhteiskunnassa yksinkertaisin tapa peruuttaa suostumus on luultavasti pelkkä sähköposti. Jos rekisteröity haluaa peruuttaa meille antamansa suostumuksen, pelkkä sähköpostiviesti meille riittää. Vaihtoehtoisesti rekisteröity voi valita minkä tahansa muun tavan ilmoittaa meille suostumuksensa peruuttamisesta.

## K. Oikeus tehdä valitus valvontaviranomaiselle (tietosuoja-asetuksen 14 artiklan 2 kohdan e alakohta ja 77 artiklan 1 kohta).

Rekisterinpitäjänä olemme velvollisia ilmoittamaan rekisteröidylle oikeudesta tehdä valitus valvontaviranomaiselle yleisen tietosuoja-asetuksen 14 artiklan 2 kohdan e alakohdan mukaisesti. Oikeudesta tehdä valitus valvontaviranomaiselle säädetään yleisen tietosuoja-asetuksen 77 artiklan 1 kohdassa. Tämän säännöksen mukaan jokaisella rekisteröidyllä on oikeus tehdä valitus valvontaviranomaiselle erityisesti siinä jäsenvaltiossa, jossa hänen vakinainen asuinpaikkansa, työpaikkansa tai paikka, jossa väitetty rikkominen tapahtuu, jos rekisteröity katsoo, että häntä koskevien henkilötietojen käsittelyssä rikotaan yleistä tietosuoja-asetusta, sanotun kuitenkaan rajoittamatta muita hallinnollisia tai oikeudellisia muutoksenhakukeinoja. Oikeus tehdä valitus valvontaviranomaiselle rajoitettiin unionin lainsäädännössä vain siten, että sitä voidaan käyttää vain yhden valvontaviranomaisen edessä (yleisen tietosuoja-asetuksen johdanto-osan 141 kappaleen 1 virke). Tämän säännön tarkoituksena on välttää saman rekisteröidyn tekemät kaksinkertaiset valitukset samasta asiasta. Jos rekisteröity haluaa tehdä meihin kohdistuvan valituksen, pyydämme häntä ottamaan yhteyttä vain yhteen valvontaviranomaiseen.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## L. Mistä henkilötiedot on saatu sekä tarvittaessa se, onko tiedot saatu yleisesti saatavilla olevista lähteistä (yleinen tietosuoja-asetus, 14 artiklan 2 kohdan f alakohta).

Periaatteessa henkilötiedot kerätään suoraan rekisteröidyltä itseltään tai yhteistyössä viranomaisen kanssa (esim. tietojen haku virallisesta rekisteristä). Muut rekisteröityjä koskevat tiedot saadaan konserniyhtiöiden tiedonsiirroista. Näiden yleisten tietojen yhteydessä henkilötietojen tarkkojen lähteiden mainitseminen on joko mahdotonta tai aiheuttaisi suhteettoman suurta vaivaa henkilötietojen siirtojen yhteydessä. 14(5) lit. b yleisen tietosuoja-asetuksen mukaisesti. Periaatteessa emme kerää henkilötietoja julkisista lähteistä.

Rekisteröity voi milloin tahansa ottaa meihin yhteyttä saadakseen tarkempia tietoja häntä koskevien henkilötietojen tarkoista lähteistä. Jos rekisteröidylle ei voida ilmoittaa henkilötietojen alkuperää, koska on käytetty eri lähteitä, olisi annettava yleistietoja (tietosuoja-asetuksen johdanto-osan 61 kappaleen 4 lause).

## M. Automaattisen päätöksenteon, muun muassa 22 artiklan 1 ja 4 kohdassa tarkoitetun profiloinnin olemassaolo, sekä ainakin näissä tapauksissa merkitykselliset tiedot käsittelyyn liittyvästä logiikasta samoin kuin kyseisen käsittelyn merkittävyys ja mahdolliset seuraukset rekisteröidylle (yleisen tietosuoja-asetuksen 14 artiklan 2 kohdan g alakohta).

Vastuullisena yrityksenä emme yleensä käytä automaattista päätöksentekoa tai profilointia. Jos poikkeustapauksissa käytämme automaattista päätöksentekoa tai profilointia, ilmoitamme siitä rekisteröidylle joko erikseen tai tietosuojaselosteemme (verkkosivuillamme) alajakson kautta. Tällöin sovelletaan seuraavaa:

Automaattinen päätöksenteko - mukaan lukien profilointi - voi tapahtua, jos (1) se on tarpeen rekisteröidyn ja meidän välisen sopimuksen tekemistä tai täytäntöönpanoa varten, tai (2) se on sallittua unionin tai jäsenvaltion lainsäädännön nojalla, jota me noudatamme ja jossa säädetään myös asianmukaisista toimenpiteistä rekisteröidyn oikeuksien ja vapauksien sekä oikeutettujen etujen suojaamiseksi; tai (3) se perustuu rekisteröidyn nimenomaiseen suostumukseen.

Yleisen tietosuoja-asetuksen 22 artiklan 2 kohdan a ja c alakohdassa tarkoitetuissa tapauksissa meidän on toteutettava asianmukaiset toimenpiteet rekisteröidyn oikeuksien ja vapauksien sekä oikeutettujen etujen turvaamiseksi. Näissä tapauksissa sinulla on oikeus saada rekisterinpitäjältä inhimillinen puuttuminen asiaan, ilmaista näkemyksesi ja riitauttaa päätös.

Tietosuojaselosteessamme annetaan merkitykselliset tiedot kyseisestä logiikasta sekä tällaisen käsittelyn merkityksestä ja suunnitelluista seurauksista rekisteröidylle.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## III. EU-U.S. Data Privacy Framework (EU-U.S. DPF), UK Extension to the EU-U.S. DPF, Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF)

Jos organisaatiomme on sertifioitu jäsen EU-U.S. Data Privacy Framework (EU-U.S. DPF) ja/tai UK Extension to the EU-U.S. DPF ja/tai Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF), sovelletaan seuraavaa:

Noudatamme EU-U.S. Data Privacy Framework (EU-U.S. DPF) ja UK Extension to the EU-U.S. DPF sekä Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF) sääntöjä, kuten U.S. Department of Commerce on määrittänyt. Yrityksemme on vahvistanut Yhdysvaltain kauppaministeriölle, että se noudattaa EU-U.S. Data Privacy Framework Principles (EU-U.S. DPF Principles) henkilötietojen käsittelyssä, jotka se saa Euroopan unionista ja Yhdistyneestä kuningaskunnasta EU-U.S. DPF ja UK Extension to the EU-U.S. DPF mukaisesti. Yrityksemme on vahvistanut Yhdysvaltain kauppaministeriölle, että se noudattaa Swiss-U.S. Data Privacy Framework Principles (Swiss-U.S. DPF Principles) henkilötietojen käsittelyssä, jotka se saa Sveitsistä Swiss-U.S. DPF mukaisesti. Jos yksityisyydensuojakäytäntömme ja EU-U.S. DPF Principles ja/tai Swiss-U.S. DPF Principles välillä on ristiriitoja, Principles ovat määräääviä.

Lisätietoja Data Privacy Framework (DPF) -ohjelmasta ja sertifiointimme tarkastelusta on saatavilla osoitteessa https://www.dataprivacyframework.gov/.

Muut Yhdysvaltojen yksikkömme tai tytäryhtiömme, jotka myös noudattavat EU-U.S. DPF Principals, mukaan lukien UK Extension to the EU-U.S. DPF ja Swiss-U.S. DPF Principals, mainitaan yksityisyydensuojakäytännössämme, jos niitä on.

EU-U.S. DPF ja UK Extension to the EU-U.S. DPF sekä Swiss-U.S. DPF mukaisesti yrityksemme sitoutuu tekemään yhteistyötä EU tietosuojaviranomaisten ja Yhdistyneen kuningaskunnan Information Commissioner's Office (ICO) sekä Sveitsin liittovaltion tietosuojavaltuutetun (EDÖB) perustaman paneelin kanssa ja noudattamaan heidän neuvojaan ratkaisemattomista valituksista koskien henkilötietojen käsittelyämme, jotka saamme EU-U.S. DPF, UK Extension to the EU-U.S. DPF ja Swiss-U.S. DPF mukaisesti.

Informoimme asianomaisia henkilöitä asianomaisista Euroopan tietosuojaviranomaisista, jotka ovat vastuussa valitusten käsittelystä organisaatiomme henkilötietojen käsittelystä, tämän läpinäkyvyysasiakirjan yläosassa ja siitä, että tarjoamme asianomaisille henkilöille asianmukaisen ja maksuttoman oikeussuojan.

Informoimme kaikkia asianomaisia henkilöitä siitä, että yrityksemme on Federal Trade Commissionin (FTC) tutkinta- ja täytäntöönpanovaltuuksien alainen.

Asianomaisilla henkilöillä on tietyin edellytyksin mahdollisuus käyttää sitovaa välimiesmenettelyä. Organisaatiomme on sitoutunut ratkaisemaan vaatimuksia ja noudattamaan DPF-Principalsin liitteessä I


© All rights reserved by Heiko Maniero.

esitettyjä ehtoja, jos asianomainen henkilö on pyytänyt sitovaa välimiesmenettelyä ilmoittamalla siitä organisaatiollemme ja noudattamalla liitteessä I esitettyjä menettelyjä ja ehtoja.

Informoimme täten kaikkia asianomaisia henkilöitä organisaatiomme vastuusta henkilötietojen siirrossa kolmansille osapuolille.

Asianomaisten henkilöiden tai tietosuojaviranomaisten kysymyksiin olemme nimenneet tässä läpinäkyvyysasiakirjassa mainitut paikalliset edustajat.

Tarjoamme sinulle mahdollisuuden valita (Opt-out), siirretäänkö henkilötietosi (i) kolmansille osapuolille vai (ii) käytetäänkö niitä olennaisesti eri tarkoitukseen kuin mihin ne alun perin kerättiin tai johon olet myöhemmin antanut suostumuksesi. Selkeä, näkyvä ja helposti saatavilla oleva mekanismi valinnan käyttämiseksi on ottaa yhteyttä tietosuojavastaavaamme (DSB) sähköpostitse. Sinulla ei ole valintamahdollisuutta, eikä meidän tarvitse tehdä niin, jos tiedot siirretään kolmannelle osapuolelle, joka toimii agenttina tai käsittelijänä meidän nimissämme ja ohjeidemme mukaisesti. Solmimme kuitenkin aina sopimuksen tällaisen agentin tai käsittelijän kanssa.

Herkkiä tietoja (ts. henkilötietoja, jotka sisältävät tietoja terveydentilasta, rodullisesta tai etnisestä alkuperästä, poliittisista mielipiteistä, uskonnollisista tai filosofisista uskomuksista, ammattiliiton jäsenyydestä tai asianomaisen henkilön seksuaalielämästä) varten hankimme nimenomaisen suostumuksesi (Opt-in), kun nämä tiedot (i) siirretään kolmansille osapuolille tai (ii) käytetään muuhun tarkoitukseen kuin mihin ne alun perin kerättiin tai mihin olet myöhemmin antanut suostumuksesi valitsemalla Opt-in. Lisäksi käsittelemme kaikkia kolmansilta osapuolilta saamamme henkilötietoja herkkinä, jos kolmas osapuoli tunnistaa ja käsittelee niitä herkkinä.

Informoimme sinua täten vaatimuksesta luovuttaa henkilötietoja vastauksena viranomaisten laillisiin pyyntöihin, mukaan lukien kansallisen turvallisuuden tai lainvalvonnan vaatimusten noudattaminen.

Henkilötietoja siirrettäessä kolmannelle osapuolelle, joka toimii rekisterinpitäjänä, noudatamme ilmoitus- ja valintaperiaatteita. Lisäksi solmimme kolmannen osapuolen kanssa, joka vastaa käsittelystä, sopimuksen, jossa määrätään, että näitä tietoja saa käsitellä vain rajoitettuihin ja määriteltyihin tarkoituksiin suostumuksesi mukaisesti ja että vastaanottajan on tarjottava sama suojaustaso kuin DPF Principles ja ilmoitettava meille, jos se toteaa, ettei se enää pysty täyttämään tätä velvoitetta. Sopimuksessa määrätään, että kolmas osapuoli, joka on rekisterinpitäjä, lopettaa käsittelyn tai ryhtyy muihin asianmukaisiin ja sopiviin toimenpiteisiin tilanteen korjaamiseksi, jos tällainen toteamus tehdään.

Henkilötietoja siirrettäessä kolmannelle osapuolelle, joka toimii agenttina tai käsittelijänä, (i) siirrämme nämä tiedot vain rajoitettuihin ja määriteltyihin tarkoituksiin; (ii) varmistamme, että agentin tai käsittelijän on tarjottava vähintään sama tietosuojan taso, jota DPF Principles edellyttää; (iii) ryhdymme asianmukaisiin ja sopiviin toimenpiteisiin varmistaaksemme, että agentti tai käsittelijä todella käsittelee siirrettyjä henkilötietoja tavalla, joka vastaa velvoitteitamme DPF Principles mukaisesti; (iv) vaadimme, että agentti tai käsittelijä ilmoittaa organisaatiollemme, jos se toteaa, ettei se enää pysty täyttämään velvoitetta tarjota sama suojaustaso, jota DPF Principles edellyttää; (v) tällaisen ilmoituksen jälkeen,


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

myös (iv) mukaisesti, ryhdymme asianmukaisiin ja sopiviin toimenpiteisiin luvattoman käsittelyn lopettamiseksi ja tilanteen korjaamiseksi; ja (vi) toimitamme DPF Department pyynnöstä yhteenvedon tai edustavan näytteen asianmukaisista tietosuojasäännöksistä sopimuksestamme tämän agentin kanssa.

EU-U.S. DPF ja/tai UK Extension to the EU-U.S. DPF ja/tai Swiss-U.S. DPF mukaisesti organisaatiomme sitoutuu tekemään yhteistyötä EU tietosuojaviranomaisten ja Yhdistyneen kuningaskunnan Information Commissioner's Office (ICO) tai Sveitsin liittovaltion tietosuojavaltuutetun (EDÖB) perustaman paneelin kanssa ja noudattamaan heidän neuvojaan ratkaisemattomista valituksista koskien työsuhteen yhteydessä saamiemme henkilötietojen käsittelyä EU-U.S. DPF ja UK Extension to the EU-U.S. DPF ja Swiss-U.S. DPF mukaisesti.

Kaikilla rekisteröidyillä, jotka oleskelevat tilapäisesti Euroopan unionissa (EU), Euroopan talousalueella (ETA) tai Yhdistyneessä kuningaskunnassa tai joilla on siellä kotipaikka tai vakinainen asuinpaikka, on oikeus avoimuusasiakirjassamme julkaistuihin oikeuksiin ja rekisteröidyn oikeuksiin, jotka johtuvat myös yleisen tietosuoja-asetuksen 15-22 artiklasta, mukaan lukien oikeus tutustua henkilötietoihin. Olemme asettaneet nämä tiedot saataville kaikilla EU- ja ETA-kielillä. Englanninkielinen versio koskee Yhdistynyttä kuningaskuntaa.

Kaikilla rekisteröidyillä, jotka asuvat tilapäisesti Sveitsissä tai joiden kotipaikka tai asuinpaikka on Sveitsissä, on oikeus Sveitsin tietosuojalain (DPA) ja Sveitsin tietosuoja-asetuksen (DPR) mukaisiin oikeuksiin ja rekisteröidyn oikeuksiin, jotka on julkaistu avoimuusasiakirjassamme, mukaan lukien oikeus tutustua henkilötietoihin. Olemme toimittaneet nämä tiedot Sveitsin kolmella virallisella kielellä (saksa, italia ja ranska).


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

# DANISH: Oplysninger om behandling af personoplysninger (Artikel 13, 14 GDPR)

Kære Herre eller frue,

Personoplysningerne om enhver person, der er i et kontraktligt, præ-kontraktuelt eller andet forhold til vores virksomhed, fortjener særlig beskyttelse. Vores mål er at holde vores databeskyttelsesniveau på en høj standard. Derfor udvikler vi rutinemæssigt vores databeskyttelses- og datasikkerhedskoncepter.

Vi overholder naturligvis de lovbestemte bestemmelser om databeskyttelse. I henhold til artikel 13, 14 GDPR opfylder registeransvarlige specifikke informationskrav, når de indsamler personoplysninger. Dette dokument opfylder disse forpligtelser.

Terminologien for lovbestemmelser er kompliceret. Desværre kunne brugen af juridiske udtryk ikke undværes ved udarbejdelsen af dette dokument. Derfor vil vi gerne gøre opmærksom på, at du altid er velkommen til at kontakte os for alle spørgsmål vedrørende dette dokument, de anvendte udtryk eller formuleringer.

## I. Oplysningspligt ved indsamling af personoplysninger hos den registrerede (artikel 13 GDPR)

### A. Identitet på og kontaktoplysninger for den dataansvarlige og dennes eventuelle repræsentant (artikel 13, stk. 1, litra a GDPR)

Se ovenfor

### B. Kontaktoplysninger for en eventuel databeskyttelsesrådgiver (artikel 1 3, stk. 1, litra b GDPR)

Se ovenfor

### C. Formålene med den behandling, som personoplysningerne skal bruges til, og retsgrundlaget for behandlingen (artikel 13, stk. 1, litra c GDPR)

Formålet med behandlingen af personoplysninger er håndteringen af alle operationer, der vedrører den dataansvarlige, kunder, potentielle kunder, samarbejdspartnere eller andre kontraktlige eller


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

præKontraktuelle relationer mellem de nævnte grupper (i bredeste forstand) eller juridiske forpligtelser for den dataansvarlige.

Kunst. 6, stk. 1 lit. en GDPR fungerer som det juridiske grundlag for behandlingsoperationer, som vi indhenter samtykke til til et bestemt behandlingsformål. Hvis behandlingen af personoplysninger er nødvendig for opfyldelse af en kontrakt, som den registrerede er part i, som det f.eks. er tilfældet, når behandlinger er nødvendige for levering af varer eller for at yde en anden tjenesteydelse, er behandlingen baseret på artikel 6, stk. b GDPR. Det samme gælder sådanne behandlinger, som er nødvendige for at udføre præKontraktuelle foranstaltninger, for eksempel i tilfælde af forespørgsler vedrørende vores produkter eller tjenester. Er vores virksomhed underlagt en juridisk forpligtelse, hvorved behandling af personoplysninger er påkrævet, såsom for opfyldelse af skatteforpligtelser, er behandlingen baseret på art. 6, stk. 1 lit. c GDPR.

I sjældne tilfælde kan behandling af personoplysninger være nødvendig for at beskytte den registreredes eller en anden fysisk persons vitale interesser. Dette vil for eksempel være tilfældet, hvis en besøgende kom til skade i vores virksomhed, og hans navn, alder, sygesikringsdata eller andre vitale oplysninger skulle videregives til en læge, hospital eller anden tredjepart. Så ville behandlingen være baseret på art. 6, stk. 1 lit. d GDPR.

Hvis behandlingen er nødvendig for at udføre en opgave i samfundets interesse eller som henhører under offentlig myndighedsudøvelse, som den dataansvarlige har fået pålagt, er retsgrundlaget artikel. 6(1) lit. e i GDPR.

Endelig kunne behandlinger baseres på artikel 6, stk. 1, litra. f GDPR. Dette retsgrundlag bruges til behandlinger, der ikke er omfattet af nogen af de ovennævnte juridiske grunde, hvis behandlingen er nødvendig af hensyn til de legitime interesser, der forfølges af vores virksomhed eller af en tredjepart, undtagen hvor sådanne interesser tilsidesættes af interesserne eller den registreredes grundlæggende rettigheder og friheder, som kræver beskyttelse af personoplysninger. Sådanne behandlinger er særligt tilladte, fordi de er blevet specifikt nævnt af den europæiske lovgiver. Han mente, at en legitim interesse kunne antages, hvis den registrerede er klient hos den dataansvarlige (betragtning 47, sætning 2 GDPR).

## D. De legitime interesser, som forfølges af den dataansvarlige eller en tredjemand, hvis behandlingen er baseret på artikel 6, stk. 1, litra f (artikel 13, stk. 1, litra d GDPR)

Hvor behandlingen af personoplysninger er baseret på artikel 6, stk. f GDPR er vores legitime interesse at udføre vores forretning til fordel for alle vores medarbejderes og aktionærers velbefindende.

## E. Eventuelle modtagere eller kategorier af modtagere af personoplysningerne (artikel 13, stk. 1, litra e GDPR)


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

Offentlige myndigheder

Eksterne organer

Yderligere eksterne organer

Intern behandling

Intragruppebehandling

Andre kroppe

En liste over vores databehandlere og datamodtagere i tredjelande og, hvis relevant, internationale organisationer er enten offentliggjort på vores hjemmeside eller kan rekvireres gratis fra os. Kontakt venligst vores databeskyttelsesansvarlige for at anmode om denne liste.

## F. Hvor det er relevant, at den dataansvarlige agter at overføre personoplysninger til et tredjeland eller en international organisation, og om hvorvidt Kommissionen har truffet afgørelse om tilstrækkeligheden af beskyttelsesniveauet, eller i tilfælde af overførsler i henhold til artikel 46 eller 47 eller artikel 49, stk. 1, andet afsnit, litra h), henvisning til de fornødne eller passende garantier, og hvordan der kan fås en kopi heraf, eller hvor de er blevet gjort tilgængelige (artikel 13, stk. 1, litra f, 46, stk. 1, 46, stk. c GDPR)

Alle virksomheder og filialer, der er en del af vores koncern (herefter benævnt "koncernselskaber"), der har deres forretningssted eller kontor i et tredjeland, kan tilhøre modtagerne af personoplysninger. En liste over alle koncernselskaber eller modtagere kan rekvireres hos os.

I henhold til artikel 46, stk. 1, GDPR, må en dataansvarlig eller databehandler kun overføre personoplysninger til et tredjeland, hvis den dataansvarlige eller databehandleren har ydet passende garantier, og på betingelse af, at håndhævede registrerede rettigheder og effektive retsmidler er tilgængelige for de registrerede. Der kan ydes passende garantier uden at kræve nogen særlig tilladelse fra en tilsynsmyndighed ved hjælp af standardkontraktbestemmelser, artikel 46, stk. 2, litra. c GDPR.

Den Europæiske Unions standardkontraktklausuler eller andre passende sikkerhedsforanstaltninger aftales med alle modtagere fra tredjelande før den første overførsel af personoplysninger. Som følge heraf sikres det, at passende sikkerhedsforanstaltninger, håndhævbare registreredes rettigheder og effektive retsmidler for de registrerede er garanteret. Alle registrerede kan få en kopi af standardkontraktbestemmelserne fra os. Standardkontraktbestemmelserne er også tilgængelige i Den Europæiske Unions Tidende.

Artikel 45, stk. 3, i GDPR giver Europa-Kommissionen beføjelse til ved hjælp af en gennemførelsesretsakt at beslutte, at et tredjeland sikrer et tilstrækkeligt databeskyttelsesniveau. Det betyder et niveau for


© All rights reserved by Heiko Maniero.

beskyttelse af personoplysninger, der i det væsentlige svarer til beskyttelsesniveauet i EU. Som følge af afgørelser om tilstrækkeligheden af beskyttelsesniveauet kan persondata frit flyttes fra EU (og Norge, Liechtenstein og Island) til et tredjeland uden yderligere hindringer. Lignende regler gælder for Storbritannien, Schweiz og nogle andre lande.

Hvor Europa-Kommissionen eller regeringen i et andet land har fastslået, at et tredjeland sikrer et tilstrækkeligt databeskyttelsesniveau, og hvor der findes en eksisterende ramme (f.eks. EU-U.S. Data Privacy Framework, Swiss-U.S. Data Privacy Framework, UK Extension to the EU-U.S. Data Privacy Framework), vil alle overførsler, vi foretager til medlemmer af sådanne rammer (f.eks. selvcertificerede enheder), udelukkende være baseret på enhedens medlemskab af den pågældende ramme. Hvis vi eller en af vores koncernenheder er medlem af en sådan ramme, vil alle overførsler til os eller vores koncernenhed udelukkende være baseret på den pågældende enheds medlemskab af denne ramme.

Is féidir le haon ábhar sonraí cóip de na creataí a fháil uainn. Ina theannta sin, tá na creataí ar fáil freisin in Iris Oifigiúil an Aontais Eorpaigh nó sna hábhair dhlíthiúla a foilsíodh nó ar shuíomhanna gréasáin na n-údarás maoirseachta nó na n-údarás inniúil nó na n-institiúidí inniúla eile.

## G. Det tidsrum, hvor personoplysningerne vil blive opbevaret, eller hvis dette ikke er muligt, de kriterier, der anvendes til at fastlægge dette tidsrum (artikel 13, stk. 2, litra a GDPR)

Kriterierne, der bruges til at bestemme perioden for opbevaring af personoplysninger, er den respektive lovpligtige opbevaringsperiode. Efter udløbet af denne periode slettes de tilsvarende data rutinemæssigt, så længe det ikke længere er nødvendigt for opfyldelse af kontrakten eller iværksættelse af en kontrakt.

Hvis der ikke er nogen lovbestemt opbevaringsperiode, er kriteriet den kontraktlige eller interne opbevaringsperiode.

## H. Retten til at anmode den dataansvarlige om indsigt i og berigtigelse eller sletning af personoplysninger eller begrænsning af behandling vedrørende den registrerede eller til at gøre indsigelse mod behandling samt retten til dataportabilitet (artikel 13, stk. 2, litra b) GDPR)

Alle registrerede har følgende rettigheder:

***Ret til adgang***

Hver registreret har ret til at få adgang til de personoplysninger, der vedrører ham eller hende. Retten til indsigt omfatter alle data, der behandles af os. Retten kan udøves let og med rimelige intervaller for at være opmærksom på og verificere lovligheden af behandlingen (betragtning 63 GDPR). Denne ret følger af art. 15 GDPR. Den registrerede kan kontakte os for at udøve retten til indsigt.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

***Ret til berigtigelse***

I henhold til artikel 16, punktum 1 GDPR, har den registrerede ret til uden unødig forsinkelse at få berigtiget unøjagtige personoplysninger om ham eller hende fra den dataansvarlige. Desuden bestemmer artikel 16 sætning 2 GDPR, at den registrerede under hensyntagen til formålene med behandlingen har ret til at få ufuldstændige personoplysninger udfyldt, herunder ved at afgive en supplerende erklæring. Den registrerede kan kontakte os for at udøve retten til berigtigelse.

***Ret til sletning (retten til at blive glemt)***

Derudover har registrerede ret til en ret til sletning og til at blive glemt i henhold til art. 17 GDPR. Denne ret kan også udøves ved at kontakte os. På dette tidspunkt vil vi dog gerne gøre opmærksom på, at denne ret ikke gælder i det omfang, behandlingen er nødvendig for at opfylde en retlig forpligtelse, som vores virksomhed er underlagt, § 17, stk. b GDPR. Det betyder, at vi først kan godkende en ansøgning om sletning efter udløbet af den lovpligtige opbevaringsperiode.

***Ret til begrænsning af behandlingen***

I henhold til artikel 18 GDPR har enhver registreret ret til en begrænsning af behandlingen. Begrænsning af behandlingen kan kræves, hvis en af betingelserne i artikel 18, stk. ad GDPR er opfyldt. Den registrerede kan kontakte os for at udøve retten til begrænsning af behandlingen.

***Ret til at gøre indsigelse***

Endvidere er art. 21 GDPR garanterer retten til at gøre indsigelse. Den registrerede kan kontakte os for at udøve retten til at gøre indsigelse.

***Ret til dataportabilitet***

Kunst. 20 GDPR giver den registrerede ret til dataportabilitet. Efter denne bestemmelse har den registrerede under de betingelser, der er fastsat i artikel 20, stk. a og b GDPR retten til at modtage de personoplysninger om ham eller hende, som han eller hun har givet til en dataansvarlig, i et struktureret, almindeligt anvendt og maskinlæsbart format og har ret til at overføre disse data til en anden dataansvarlig uden hindring fra den dataansvarlige, som personoplysningerne er givet til. Den registrerede kan kontakte os for at udøve retten til dataportabilitet.

## I. Når behandling er baseret på artikel 6, stk. 1, litra a), eller artikel 9, stk. 2, litra a), retten til at trække samtykke tilbage på ethvert tidspunkt, uden at dette berører lovligheden af behandling, der er baseret på samtykke, inden tilbagetrækning heraf (Artikel 13, stk. 2, litra c GDPR)

Hvis behandlingen af personoplysninger er baseret på art. 6, stk. 1 lit. en GDPR, hvilket er tilfældet, hvis den registrerede har givet samtykke til behandling af personoplysninger til et eller flere specifikke formål eller er baseret på artikel 9, stk. en GDPR, som regulerer det udtrykkelige samtykke til behandling af særlige kategorier af personoplysninger, har den registrerede i henhold til artikel 7, stk. 3, punktum 1 GDPR ret til at trække sit samtykke tilbage til enhver tid.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

Tilbagetrækning af samtykke påvirker ikke lovligheden af behandling baseret på samtykke før tilbagetrækningen, artikel 7, stk. 3, punktum 2 GDPR. Det skal være lige så nemt at trække tilbage som at give samtykke, art. 7, stk. 3, punktum 4 GDPR. Derfor kan tilbagekaldelse af samtykke altid ske på samme måde, som der er givet samtykke, eller på anden måde, der af den registrerede anses for at være enklere. I dagens informationssamfund er nok den enkleste måde at trække samtykke tilbage på en simpel e-mail. Hvis den registrerede ønsker at trække sit samtykke, der er givet til os, tilbage, er en simpel e-mail til os tilstrækkelig. Alternativt kan den registrerede vælge en hvilken som helst anden måde at kommunikere sin tilbagetrækning af samtykke til os på.

## J. Retten til at indgive en klage til en tilsynsmyndighed (Artikel 13, stk. 2, litra d, 77, stk. 1, GDPR)

Som dataansvarlig er vi forpligtet til at underrette den registrerede om retten til at indgive en klage til en tilsynsmyndighed, artikel 13, stk. d GDPR. Retten til at indgive en klage til en tilsynsmyndighed er reguleret af artikel 77, stk. 1, GDPR. I henhold til denne bestemmelse har enhver registreret ret til at indgive en klage til en tilsynsmyndighed, især i den medlemsstat, hvor vedkommendes sædvanlige opholdssted, arbejdssted eller sted, uden at det berører andre administrative eller retslige retsmidler. den påståede krænkelse, hvis den registrerede mener, at behandlingen af personoplysninger vedrørende ham eller hende er i strid med den generelle databeskyttelsesforordning. Retten til at indgive en klage til en tilsynsmyndighed var kun begrænset af unionsretten på en sådan måde, at den kun kan udøves over for en enkelt tilsynsmyndighed (betragtning 141, sætning 1 GDPR). Denne regel har til formål at undgå dobbeltklager fra samme registrerede i samme sag. Hvis en registreret ønsker at indgive en klage over os, har vi derfor bedt om kun at kontakte en enkelt tilsynsmyndighed.

## K. Om meddelelse af personoplysninger er lovpligtigt eller et krav i henhold til en kontrakt eller et krav, der skal være opfyldt for at indgå en kontrakt, samt om den registrerede har pligt til at give personoplysningerne og de eventuelle konsekvenser af ikke at give sådanne oplysninger (Art. 13(2) lit. e GDPR)

Vi præciserer, at leveringen af personoplysninger delvist er lovpligtig (f.eks. skatteregler) eller også kan følge af kontraktlige bestemmelser (f.eks. oplysninger om den kontraktlige partner).

Nogle gange kan det være nødvendigt at indgå en kontrakt om, at den registrerede giver os personoplysninger, som efterfølgende skal behandles af os. Den registrerede er for eksempel forpligtet til at give os personoplysninger, når vores virksomhed underskriver en kontrakt med ham eller hende. Manglende udlevering af personoplysningerne ville have den konsekvens, at kontrakten med den registrerede ikke kunne indgås.

Inden personoplysninger afgives af den registrerede, skal den registrerede kontakte os. Vi afklarer over for den registrerede, om leveringen af personoplysningerne er påkrævet ved lov eller kontrakt eller er


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

nødvendig for indgåelse af kontrakten, om der er en forpligtelse til at udlevere personoplysningerne og konsekvenserne af manglende levering af personoplysningerne. data.

### L. Forekomsten af automatiske afgørelser, herunder profilering, som omhandlet i artikel 22, stk. 1 og 4, og i disse tilfælde som minimum meningsfulde oplysninger om logikken heri samt betydningen og de forventede konsekvenser af en sådan behandling for den registrerede (artikel 13, stk. 2, litra f GDPR)

Som en ansvarlig virksomhed bruger vi normalt ikke automatiseret beslutningstagning eller profilering. Hvis vi i undtagelsestilfælde udfører automatiseret beslutningstagning eller profilering, informerer vi den registrerede enten separat eller via et underafsnit i vores privatlivspolitik (på vores hjemmeside). I dette tilfælde gælder følgende:

Automatiseret beslutningstagning - herunder profilering - kan forekomme, hvis (1) dette er nødvendigt for at indgå eller opfylde en kontrakt mellem den registrerede og os, eller (2) dette er tilladt i henhold til EU-lovgivning eller medlemsstatslovgivning, som vi er underlagt, og som også fastlægger passende foranstaltninger til at beskytte den registreredes rettigheder og friheder og legitime interesser; eller (3) dette er baseret på den registreredes udtrykkelige samtykke.

I de tilfælde, der henvises til i artikel 22, stk. 2, litra a) og c), i GDPR, skal vi gennemføre passende foranstaltninger for at beskytte den registreredes rettigheder og friheder og legitime interesser. I disse tilfælde har du ret til at opnå menneskelig indgriben fra den dataansvarliges side, til at udtrykke dit synspunkt og til at anfægte beslutningen.

Betydningsfulde oplysninger om den involverede logik samt betydningen og de forventede konsekvenser af en sådan behandling for den registrerede er beskrevet i vores privatlivspolitik.

## II. Oplysningspligt, hvis personoplysninger ikke er indsamlet hos den registrerede (artikel 14 GDPR)

### A. Identitet på og kontaktoplysninger for den dataansvarlige og dennes eventuelle repræsentant (artikel 14, stk. 1, litra a GDPR)

Se ovenfor


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## B. Kontaktoplysninger for en eventuel databeskyttelsesrådgiver (artikel 14, stk. 1, litra b GDPR)

Se ovenfor

## C. Formålene med den behandling, som personoplysningerne skal bruges til, samt retsgrundlaget for behandlingen (artikel 14, stk. 1, litra c GDPR)

Formålet med behandlingen af personoplysninger er håndteringen af alle operationer, der vedrører den dataansvarlige, kunder, potentielle kunder, samarbejdspartnere eller andre kontraktlige eller prækontraktuelle relationer mellem de nævnte grupper (i bredeste forstand) eller juridiske forpligtelser for den dataansvarlige.

Hvis behandlingen af personoplysninger er nødvendig for opfyldelse af en kontrakt, som den registrerede er part i, som det f.eks. er tilfældet, når behandlinger er nødvendige for levering af varer eller for at yde en anden tjenesteydelse, er behandlingen baseret på artikel 6, stk. b GDPR. Det samme gælder sådanne behandlinger, som er nødvendige for at udføre prækontraktuelle foranstaltninger, for eksempel i tilfælde af forespørgsler vedrørende vores produkter eller tjenester. Er vores virksomhed underlagt en juridisk forpligtelse, hvorved behandling af personoplysninger er påkrævet, såsom for opfyldelse af skatteforpligtelser, er behandlingen baseret på art. 6, stk. 1 lit. c GDPR.

I sjældne tilfælde kan behandling af personoplysninger være nødvendig for at beskytte den registreredes eller en anden fysisk persons vitale interesser. Dette vil for eksempel være tilfældet, hvis en besøgende kom til skade i vores virksomhed, og hans navn, alder, sygesikringsdata eller andre vitale oplysninger skulle videregives til en læge, hospital eller anden tredjepart. Så ville behandlingen være baseret på art. 6, stk. 1 lit. d GDPR.

Hvis behandlingen er nødvendig for at udføre en opgave i samfundets interesse eller som henhører under offentlig myndighedsudøvelse, som den dataansvarlige har fået pålagt, er retsgrundlaget artikel. 6(1) lit. e i GDPR.

Endelig kunne behandlinger baseres på artikel 6, stk. 1, litra. f GDPR. Dette retsgrundlag bruges til behandlinger, der ikke er omfattet af nogen af de ovennævnte juridiske grunde, hvis behandlingen er nødvendig af hensyn til de legitime interesser, der forfølges af vores virksomhed eller af en tredjepart, undtagen hvor sådanne interesser tilsidesættes af interesserne eller den registreredes grundlæggende rettigheder og friheder, som kræver beskyttelse af personoplysninger. Sådanne behandlinger er særligt tilladte, fordi de er blevet specifikt nævnt af den europæiske lovgiver. Han mente, at en legitim interesse kunne antages, hvis den registrerede er klient hos den dataansvarlige (betragtning 47, sætning 2 GDPR).

## D. De berørte kategorier af personoplysninger (artikel 14, stk. 1, litra d GDPR)


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

Kundedata

Data om potentielle kunder

Data om medarbejdere

Data fra leverandører

## E. Eventuelle modtagere eller kategorier af modtagere af personoplysningerne (artikel 14, stk. 1, litra e GDPR)

Offentlige myndigheder

Eksterne organer

Yderligere eksterne organer

Intern behandling

Intragruppebehandling

Andre kroppe

En liste over vores databehandlere og datamodtagere i tredjelande og, hvis relevant, internationale organisationer er enten offentliggjort på vores hjemmeside eller kan rekvireres gratis fra os. Kontakt venligst vores databeskyttelsesansvarlige for at anmode om denne liste.

## F. Hvor det er relevant, at den dataansvarlige agter at overføre personoplysninger til en modtager i et tredjeland eller en international organisation, og om hvorvidt Kommissionen har truffet afgørelse om tilstrækkeligheden af beskyttelsesniveauet, eller i tilfælde af overførsler i henhold til artikel 46 eller 47 eller artikel 49, stk. 1, andet afsnit, litra h), henvisning til de fornødne eller passende garantier, og hvordan der kan fås en kopi heraf, eller hvor de er blevet gjort tilgængelige (artikel 14, stk. 1, litra f, 46, stk. 1, 46, stk. c GDPR)

Alle virksomheder og filialer, der er en del af vores koncern (herefter benævnt "koncernselskaber"), der har deres forretningssted eller kontor i et tredjeland, kan tilhøre modtagerne af personoplysninger. En liste over alle koncernselskaber kan rekvireres hos os.

I henhold til artikel 46, stk. 1, GDPR, må en dataansvarlig eller databehandler kun overføre personoplysninger til et tredjeland, hvis den dataansvarlige eller databehandleren har ydet passende


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

garantier, og på betingelse af, at håndhævede registrerede rettigheder og effektive retsmidler er tilgængelige for de registrerede. Der kan ydes passende sikkerhedsforanstaltninger uden at kræve nogen specifik tilladelse fra en tilsynsmyndighed ved hjælp af standarddatabeskyttelsesklausuler, artikel 46, stk. c GDPR.

Den Europæiske Unions standardkontraktklausuler eller andre passende sikkerhedsforanstaltninger aftales med alle modtagere fra tredjelande før den første overførsel af personoplysninger. Som følge heraf sikres det, at passende sikkerhedsforanstaltninger, håndhævbare registreredes rettigheder og effektive retsmidler for de registrerede er garanteret. Alle registrerede kan få en kopi af standardkontraktbestemmelserne fra os. Standardkontraktbestemmelserne er også tilgængelige i Den Europæiske Unions Tidende.

Artikel 45, stk. 3, i GDPR giver Europa-Kommissionen beføjelse til ved hjælp af en gennemførelsesretsakt at beslutte, at et tredjeland sikrer et tilstrækkeligt databeskyttelsesniveau. Det betyder et niveau for beskyttelse af personoplysninger, der i det væsentlige svarer til beskyttelsesniveauet i EU. Som følge af afgørelser om tilstrækkeligheden af beskyttelsesniveauet kan persondata frit flyttes fra EU (og Norge, Liechtenstein og Island) til et tredjeland uden yderligere hindringer. Lignende regler gælder for Storbritannien, Schweiz og nogle andre lande.

Hvor Europa-Kommissionen eller regeringen i et andet land har fastslået, at et tredjeland sikrer et tilstrækkeligt databeskyttelsesniveau, og hvor der findes en eksisterende ramme (f.eks. EU-U.S. Data Privacy Framework, Swiss-U.S. Data Privacy Framework, UK Extension to the EU-U.S. Data Privacy Framework), vil alle overførsler, vi foretager til medlemmer af sådanne rammer (f.eks. selvcertificerede enheder), udelukkende være baseret på enhedens medlemskab af den pågældende ramme. Hvis vi eller en af vores koncernenheder er medlem af en sådan ramme, vil alle overførsler til os eller vores koncernenhed udelukkende være baseret på den pågældende enheds medlemskab af denne ramme.

Is féidir le haon ábhar sonraí cóip de na creataí a fháil uainn. Ina theannta sin, tá na creataí ar fáil freisin in Iris Oifigiúil an Aontais Eorpaigh nó sna hábhair dhlíthiúla a foilsíodh nó ar shuíomhanna gréasáin na n-údarás maoirseachta nó na n-údarás inniúil nó na n-institiúidí inniúla eile.

## G. Det tidsrum, hvor personoplysningerne vil blive opbevaret, eller hvis dette ikke er muligt, de kriterier, der anvendes til at fastlægge dette tidsrum (artikel 14, stk. 2, litra a GDPR)

Kriterierne, der bruges til at bestemme perioden for opbevaring af personoplysninger, er den respektive lovpligtige opbevaringsperiode. Efter udløbet af denne periode slettes de tilsvarende data rutinemæssigt, så længe det ikke længere er nødvendigt for opfyldelse af kontrakten eller iværksættelse af en kontrakt.

Hvis der ikke er nogen lovbestemt opbevaringsperiode, er kriteriet den kontraktlige eller interne opbevaringsperiode.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## H. De legitime interesser, som forfølges af den dataansvarlige eller en tredjemand, hvis behandlingen er baseret på artikel 6, stk. 1, litra f) (Art. 14(2) lit. b GDPR)

I henhold til artikel 6, stk. f GDPR er behandlingen kun lovlig, hvis behandlingen er nødvendig af hensyn til legitime interesser, der forfølges af den dataansvarlige eller af en tredjepart, undtagen hvor sådanne interesser tilsidesættes af den registreredes interesser eller grundlæggende rettigheder og friheder, som kræver beskyttelse af personlige data. Ifølge betragtning 47, punktum 2 GDPR, kunne der eksistere en legitim interesse, hvor der er et relevant og passende forhold mellem den registrerede og den dataansvarlige, fx i situationer, hvor den registrerede er klient hos den dataansvarlige. I alle tilfælde, hvor vores virksomhed behandler personoplysninger baseret på artikel 6, stk. f GDPR er vores legitime interesse i at udføre vores forretning til fordel for alle vores medarbejderes og aktionærers velbefindende.

## I. Retten til at anmode den dataansvarlige om indsigt i og berigtigelse eller sletning af personoplysninger eller begrænsning af behandling vedrørende den registrerede og til at gøre indsigelse mod behandling samt retten til dataportabilitet (artikel 14, stk. 2, litra c). GDPR)

Alle registrerede har følgende rettigheder:

***Ret til adgang***

Hver registreret har ret til at få adgang til de personoplysninger, der vedrører ham eller hende. Retten til indsigt omfatter alle data, der behandles af os. Retten kan udøves let og med rimelige intervaller for at være opmærksom på og verificere lovligheden af behandlingen (betragtning 63 GDPR). Denne ret følger af art. 15 GDPR. Den registrerede kan kontakte os for at udøve retten til indsigt.

***Ret til berigtigelse***

I henhold til artikel 16, punktum 1 GDPR, har den registrerede ret til uden unødig forsinkelse at få berigtiget unøjagtige personoplysninger om ham eller hende fra den dataansvarlige. Desuden bestemmer artikel 16 sætning 2 GDPR, at den registrerede under hensyntagen til formålene med behandlingen har ret til at få ufuldstændige personoplysninger udfyldt, herunder ved at afgive en supplerende erklæring. Den registrerede kan kontakte os for at udøve retten til berigtigelse.

***Ret til sletning (retten til at blive glemt)***

Derudover har registrerede ret til en ret til sletning og til at blive glemt i henhold til art. 17 GDPR. Denne ret kan også udøves ved at kontakte os. På dette tidspunkt vil vi dog gerne gøre opmærksom på, at denne ret ikke gælder i det omfang, behandlingen er nødvendig for at opfylde en retlig forpligtelse, som vores virksomhed er underlagt, § 17, stk. b GDPR. Det betyder, at vi først kan godkende en ansøgning om sletning efter udløbet af den lovpligtige opbevaringsperiode.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

***Ret til begrænsning af behandlingen***

I henhold til artikel 18 GDPR har enhver registreret ret til begrænsning af behandlingen. Begrænsning af behandlingen kan kræves, hvis en af betingelserne i artikel 18, stk. ad GDPR er opfyldt. Den registrerede kan kontakte os for at udøve retten til begrænsning af behandlingen.

***Ret til at gøre indsigelse***

Endvidere er art. 21 GDPR garanterer retten til at gøre indsigelse. Den registrerede kan kontakte os for at udøve retten til at gøre indsigelse.

***Ret til dataportabilitet***

Kunst. 20 GDPR giver den registrerede ret til dataportabilitet. I henhold til denne bestemmelse har den registrerede under de betingelser, der er fastsat i artikel 20, stk. a og b GDPR retten til at modtage de personoplysninger om ham eller hende, som han eller hun har givet til en dataansvarlig, i et struktureret, almindeligt anvendt og maskinlæsbart format og har ret til at overføre disse data til en anden dataansvarlig uden hindring fra den dataansvarlige, som personoplysningerne er givet til. Den registrerede kan kontakte os for at udøve retten til dataportabilitet.

## J. Når behandling er baseret på artikel 6, stk. 1, litra a), eller artikel 9, stk. 2, litra a), retten til at trække samtykke tilbage på ethvert tidspunkt, uden at dette berører lovligheden af behandling, der er baseret på samtykke, inden tilbagetrækning heraf (Art. 14(2) lit. d GDPR)

Hvis behandlingen af personoplysninger er baseret på art. 6, stk. 1 lit. en GDPR, hvilket er tilfældet, hvis den registrerede har givet samtykke til behandling af personoplysninger til et eller flere specifikke formål eller er baseret på artikel 9, stk. en GDPR, som regulerer det udtrykkelige samtykke til behandling af særlige kategorier af personoplysninger, har den registrerede i henhold til artikel 7, stk. 3, punktum 1 GDPR ret til at trække sit samtykke tilbage til enhver tid.

Tilbagetrækning af samtykke påvirker ikke lovligheden af behandling baseret på samtykke før tilbagetrækningen, artikel 7, stk. 3, punktum 2 GDPR. Det skal være lige så nemt at trække tilbage som at give samtykke, art. 7, stk. 3, punktum 4 GDPR. Derfor kan tilbagekaldelse af samtykke altid ske på samme måde, som der er givet samtykke, eller på anden måde, der af den registrerede anses for at være enklere. I dagens informationssamfund er nok den enkleste måde at trække samtykke tilbage på en simpel e-mail. Hvis den registrerede ønsker at trække sit samtykke, der er givet til os, tilbage, er en simpel e-mail til os tilstrækkelig. Alternativt kan den registrerede vælge en hvilken som helst anden måde at kommunikere sin tilbagetrækning af samtykke til os på.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## K. Retten til at indgive en klage til en tilsynsmyndighed (Artikel 14, stk. 2, lit. e, 77, stk. 1, GDPR)

Som dataansvarlig er vi forpligtet til at underrette den registrerede om retten til at indgive en klage til en tilsynsmyndighed, artikel 14, stk. e GDPR. Retten til at indgive en klage til en tilsynsmyndighed er reguleret af artikel 77, stk. 1, GDPR. I henhold til denne bestemmelse har enhver registreret ret til at indgive en klage til en tilsynsmyndighed, især i den medlemsstat, hvor vedkommendes sædvanlige opholdssted, arbejdssted eller sted, uden at det berører andre administrative eller retslige retsmidler. den påståede krænkelse, hvis den registrerede mener, at behandlingen af personoplysninger vedrørende ham eller hende er i strid med den generelle databeskyttelsesforordning. Retten til at indgive en klage til en tilsynsmyndighed var kun begrænset af unionsretten på en sådan måde, at den kun kan udøves over for en enkelt tilsynsmyndighed (betragtning 141, sætning 1 GDPR). Denne regel har til formål at undgå dobbeltklager fra samme registrerede i samme sag. Hvis en registreret ønsker at indgive en klage over os, har vi derfor bedt om kun at kontakte en enkelt tilsynsmyndighed.

## L. Hvilken kilde personoplysningerne hidrører fra, og eventuelt hvorvidt de stammer fra offentligt tilgængelige kilder (artikel 14, stk. 2, litra f GDPR)

I princippet indsamles personoplysninger direkte fra den registrerede eller i samarbejde med en myndighed (f.eks. indhentning af data fra et officielt register). Andre data om registrerede er afledt af overdragelser af koncernselskaber. I forbindelse med denne generelle information er navngivningen af de nøjagtige kilder, hvorfra personoplysningerne stammer, enten umuligt eller ville involvere en uforholdsmæssig indsats i henhold til art. 14(5) lit. b GDPR. I princippet indsamler vi ikke personoplysninger fra offentligt tilgængelige kilder.

Enhver registreret person kan til enhver tid kontakte os for at få mere detaljeret information om de nøjagtige kilder til de personoplysninger, der vedrører ham eller hende. Hvor oprindelsen af personoplysningerne ikke kan gives til den registrerede, fordi forskellige kilder er blevet brugt, bør der gives generel information (betragtning 61, sætning 4 GDPR).

## M. Forekomsten af automatiske afgørelser, herunder profilering, som omhandlet i artikel 22, stk. 1 og 4, og i disse tilfælde som minimum meningsfulde oplysninger om logikken heri samt betydningen og de forventede konsekvenser af en sådan behandling for den registrerede (artikel 14, stk. 2, litra g GDPR)

Som en ansvarlig virksomhed bruger vi normalt ikke automatiseret beslutningstagning eller profilering. Hvis vi i undtagelsestilfælde udfører automatiseret beslutningstagning eller profilering, informerer vi den registrerede enten separat eller via et underafsnit i vores privatlivspolitik (på vores hjemmeside). I dette tilfælde gælder følgende:


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

Automatiseret beslutningstagning - herunder profilering - kan forekomme, hvis (1) dette er nødvendigt for at indgå eller opfylde en kontrakt mellem den registrerede og os, eller (2) dette er tilladt i henhold til EU-lovgivning eller medlemsstatslovgivning, som vi er underlagt, og som også fastlægger passende foranstaltninger til at beskytte den registreredes rettigheder og friheder og legitime interesser; eller (3) dette er baseret på den registreredes udtrykkelige samtykke.

I de tilfælde, der henvises til i artikel 22, stk. 2, litra a) og c), i GDPR, skal vi gennemføre passende foranstaltninger for at beskytte den registreredes rettigheder og friheder og legitime interesser. I disse tilfælde har du ret til at opnå menneskelig indgriben fra den dataansvarliges side, til at udtrykke dit synspunkt og til at anfægte beslutningen.

Betydningsfulde oplysninger om den involverede logik samt betydningen og de forventede konsekvenser af en sådan behandling for den registrerede er beskrevet i vores privatlivspolitik.

## III. EU-U.S. Data Privacy Framework (EU-U.S. DPF), UK Extension to the EU-U.S. DPF, Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF)

Hvis vores organisation er et certificeret medlem af EU-U.S. Data Privacy Framework (EU-U.S. DPF) og/eller UK Extension to the EU-U.S. DPF og/eller Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF), gælder følgende:

Vi overholder EU-U.S. Data Privacy Framework (EU-U.S. DPF) og UK Extension to the EU-U.S. DPF samt Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF), som fastsat af U.S. Department of Commerce. Vores virksomhed har bekræftet over for det amerikanske handelsministerium, at den overholder EU-U.S. Data Privacy Framework Principles (EU-U.S. DPF Principles) med hensyn til behandling af personoplysninger, som den modtager fra Den Europæiske Union og Det Forenede Kongerige i henhold til EU-U.S. DPF og UK Extension to the EU-U.S. DPF. Vores virksomhed har bekræftet over for det amerikanske handelsministerium, at den overholder Swiss-U.S. Data Privacy Framework Principles (Swiss-U.S. DPF Principles) med hensyn til behandling af personoplysninger, som den modtager fra Schweiz i henhold til Swiss-U.S. DPF. I tilfælde af uoverensstemmelse mellem bestemmelserne i vores privatlivspolitik og EU-U.S. DPF Principles og/eller Swiss-U.S. DPF Principles, er Principles afgørende.

For at få mere at vide om Data Privacy Framework (DPF) programmet og for at se vores certificering, besøg venligst https://www.dataprivacyframework.gov/.

De øvrige amerikanske enheder eller datterselskaber i vores virksomhed, der også overholder EU-U.S. DPF Principals, herunder UK Extension to the EU-U.S. DPF og Swiss-U.S. DPF Principals, hvis de findes, er nævnt i vores privatlivspolitik.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

I overensstemmelse med EU-U.S. DPF og UK Extension to the EU-U.S. DPF samt Swiss-U.S. DPF forpligter vores virksomhed sig til at samarbejde med det panel, der er oprettet af EU's databeskyttelsesmyndigheder og Det Forenede Kongeriges Information Commissioner's Office (ICO) samt den schweiziske føderale databeskyttelses- og informationskommissær (EDÖB), og følge deres råd vedrørende uløste klager over vores håndtering af personoplysninger, som vi modtager i henhold til EU-U.S. DPF og UK Extension to the EU-U.S. DPF samt Swiss-U.S. DPF.

Vi informerer de berørte personer om de relevante europæiske databeskyttelsesmyndigheder, der er ansvarlige for behandlingen af klager over vores organisations håndtering af personoplysninger, i den øverste del af dette gennemsigtighedsdokument og om, at vi tilbyder de berørte personer en passende og gratis retsmidler.

Vi informerer alle berørte personer om, at vores virksomhed er underlagt Federal Trade Commissions (FTC) undersøgelses- og håndhævelsesbeføjelser.

Berørte personer har under visse forudsætninger mulighed for at benytte bindende voldgift. Vores organisation er forpligtet til at bilægge krav og overholde betingelserne i bilag I til DPF-Principals, forudsat at den berørte person har anmodet om bindende voldgift ved at underrette vores organisation og har fulgt procedurerne og betingelserne i bilag I til Principals.

Vi informerer hermed alle berørte personer om vores organisations ansvar i tilfælde af videregivelse af personoplysninger til tredjepart.

For spørgsmål fra berørte personer eller datatilsynsmyndigheder har vi udpeget de lokale repræsentanter, der er nævnt ovenfor i dette gennemsigtighedsdokument.

Vi giver dig mulighed for at vælge (Opt-out), om dine personoplysninger (i) skal videregives til tredjepart eller (ii) bruges til et formål, der væsentligt adskiller sig fra det/de formål, som de oprindeligt blev indsamlet til eller senere blev godkendt af dig. Den klare, synlige og let tilgængelige mekanisme til at udøve dit valg består i at kontakte vores databeskyttelsesansvarlige (DSB) via e-mail. Du har ikke mulighed for at vælge, og vi er heller ikke forpligtet til det, hvis oplysningerne videregives til en tredjepart, der fungerer som agent eller databehandler på vores vegne og efter vores anvisninger. Vi indgår dog altid en aftale med en sådan agent eller databehandler.

For følsomme oplysninger (dvs. personoplysninger, der indeholder oplysninger om helbredstilstand, race eller etnisk oprindelse, politiske holdninger, religiøse eller filosofiske overbevisninger, fagforeningsmedlemskab eller oplysninger om den pågældende persons seksualliv) indhenter vi dit udtrykkelige samtykke (Opt-in), når disse oplysninger (i) videregives til tredjepart eller (ii) bruges til et andet formål end det, som de oprindeligt blev indsamlet til, eller som du senere har givet samtykke til ved at vælge Opt-in. Desuden behandler vi alle personoplysninger, som vi modtager fra tredjepart, som følsomme, hvis tredjeparten identificerer og behandler dem som følsomme.

Vi informerer dig hermed om kravet om at videregive personoplysninger som reaktion på lovlige anmodninger fra myndigheder, herunder opfyldelse af krav om national sikkerhed eller retshåndhævelse.


© All rights reserved by Heiko Maniero.

Ved videregivelse af personoplysninger til en tredjepart, der fungerer som dataansvarlig, overholder vi Principals om meddelelse og valg. Derudover indgår vi en aftale med tredjeparten, der er ansvarlig for behandlingen, som fastsætter, at disse oplysninger kun må behandles til begrænsede og specificerede formål i overensstemmelse med dit samtykke, og at modtageren skal tilbyde det samme beskyttelsesniveau som DPF Principals og underrette os, hvis det konstaterer, at det ikke længere kan opfylde denne forpligtelse. Aftalen fastsætter, at tredjeparten, der er ansvarlig, skal stoppe behandlingen eller træffe andre passende og rimelige foranstaltninger for at afhjælpe situationen, hvis en sådan konstatering foretages.

Ved videregivelse af personoplysninger til en tredjepart, der fungerer som agent eller databehandler, (i) videregiver vi kun disse oplysninger til begrænsede og specificerede formål; (ii) sikrer vi, at agenten eller databehandleren er forpligtet til at tilbyde mindst samme niveau af databeskyttelse, som DPF-Principals kræver; (iii) træffer vi passende og rimelige foranstaltninger for at sikre, at agenten eller databehandleren faktisk behandler de videregivne personoplysninger på en måde, der er i overensstemmelse med vores forpligtelser i henhold til DPF-Principals; (iv) kræver vi, at agenten eller databehandleren underretter vores organisation, hvis det konstaterer, at det ikke længere kan opfylde forpligtelsen til at tilbyde samme beskyttelsesniveau, som DPF-Principals kræver; (v) efter en sådan underretning, også i henhold til (iv), træffer vi passende og rimelige foranstaltninger for at stoppe uautoriseret behandling og afhjælpe situationen; og (vi) giver vi DPF Department efter anmodning et resumé eller et repræsentativt eksempel på de relevante databeskyttelsesbestemmelser fra vores aftale med denne agent.

I overensstemmelse med EU-U.S. DPF og/eller UK Extension to the EU-U.S. DPF og/eller Swiss-U.S. DPF forpligter vores organisation sig til at samarbejde med det panel, der er oprettet af EU's databeskyttelsesmyndigheder og Det Forenede Kongeriges Information Commissioner's Office (ICO) eller den schweiziske føderale databeskyttelses- og informationskommissær (EDÖB) og følge deres råd vedrørende uløste klager over vores håndtering af personoplysninger, som vi modtager i forbindelse med ansættelsesforhold i henhold til EU-U.S. DPF og UK Extension to the EU-U.S. DPF og Swiss-U.S. DPF.

Alle registrerede, der midlertidigt befinder sig i Den Europæiske Union (EU), Det Europæiske Økonomiske Samarbejdsområde (EØS) eller Det Forenede Kongerige, eller som har deres bopæl eller sædvanlige opholdssted der, har ret til de rettigheder og registreredes rettigheder, der er offentliggjort i vores gennemsigtighedsdokument, og som også følger af artikel 15 til 22 i GDPR, herunder retten til at få adgang til personoplysninger. Vi har gjort disse oplysninger tilgængelige på alle EU- og EØS-sprog. Den engelsksprogede version gælder for Storbritannien.

Alle registrerede, der er midlertidigt bosiddende i Schweiz eller har deres bopæl eller sædvanlige opholdssted der, har ret til de rettigheder og den registreredes rettigheder i henhold til den schweiziske databeskyttelseslov (DPA) og den schweiziske databeskyttelsesforordning (DPR), som er offentliggjort i vores gennemsigtighedsdokument, herunder retten til at få adgang til personlige data. Vi har stillet disse oplysninger til rådighed på de tre officielle sprog i Schweiz (tysk, italiensk og fransk).


© All rights reserved by Heiko Maniero.

# DANISH: Information om behandling af personoplysninger for medarbejdere og ansøgere (Artikel 13, 14 GDPR)

Kære Herre eller frue,

Personlige data om medarbejdere og ansøgere fortjener særlig beskyttelse. Vores mål er at holde vores databeskyttelsesniveau på en høj standard. Derfor udvikler vi rutinemæssigt vores databeskyttelses- og datasikkerhedskoncepter.

Vi overholder naturligvis de lovbestemte bestemmelser om databeskyttelse. I henhold til artikel 13, 14 GDPR opfylder registeransvarlige specifikke informationskrav, når de behandler personoplysninger. Dette dokument opfylder disse forpligtelser.

Terminologien for juridisk regulering er kompliceret. Desværre kunne brugen af juridiske udtryk ikke undværes ved udarbejdelsen af dette dokument. Derfor vil vi gerne gøre opmærksom på, at du altid er velkommen til at kontakte os for alle spørgsmål vedrørende dette dokument, de anvendte udtryk eller formuleringer.

## I. Oplysningspligt ved indsamling af personoplysninger hos den registrerede (artikel 13 GDPR)

### A. Identitet på og kontaktoplysninger for den dataansvarlige og dennes eventuelle repræsentant (artikel 13, stk. 1, litra a GDPR)

Se ovenfor

### B. Kontaktoplysninger for en eventuel databeskyttelsesrådgiver (artikel 13, stk. 1, litra b GDPR)

Se ovenfor

### C. Formålene med den behandling, som personoplysningerne skal bruges til, og retsgrundlaget for behandlingen (artikel 13, stk. 1, litra c GDPR)

For ansøgers data er formålet med databehandlingen at gennemføre en undersøgelse af ansøgningen under rekrutteringsprocessen. Til dette formål behandler vi alle data, som du har givet. På baggrund af de data, der er afgivet under rekrutteringsprocessen, tjekker vi, om du bliver inviteret til en jobsamtale


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

(en del af udvælgelsesprocessen). I tilfælde af generelt egnede kandidater, især i forbindelse med jobsamtalen, behandler vi visse andre personoplysninger, som du har oplyst, hvilket er afgørende for vores valgbeslutning. Hvis du bliver ansat af os, ændres ansøgerens data automatisk til medarbejderdata. Som en del af rekrutteringsprocessen vil vi behandle andre personoplysninger om dig, som vi anmoder om fra dig, og som er nødvendige for at påbegynde eller opfylde din kontrakt (såsom personlige identifikationsnumre eller skattenumre). For medarbejderdata er formålet med databehandling udførelsen af ansættelseskontrakten eller overholdelse af andre lovbestemmelser gældende for ansættelsesforholdet (f.eks. skattelovgivning) samt brugen af dine personoplysninger til at udføre den ansættelseskontrakt, der er indgået med dig (f.eks. offentliggørelse af dit navn og kontaktoplysningerne i virksomheden eller til kunder). Medarbejderdata opbevares efter ansættelsesforholdets ophør for at opfylde lovmæssige opbevaringsperioder.

Retsgrundlaget for databehandling er artikel 6, stk. b GDPR, artikel 9, stk. 2, lit. b og h GDPR, artikel 88 (1) GDPR og national lovgivning, såsom for Tysklands § 26 BDSG (Federal Data Protection Act).

## D. Eventuelle modtagere eller kategorier af modtagere af personoplysningerne (artikel 13, stk. 1, litra e GDPR)

Offentlige myndigheder

Eksterne organer

Yderligere eksterne organer

Intern behandling

Intragruppebehandling

Andre kroppe

En liste over vores databehandlere og datamodtagere i tredjelande og, hvis relevant, internationale organisationer er enten offentliggjort på vores hjemmeside eller kan rekvireres gratis fra os. Kontakt venligst vores databeskyttelsesansvarlige for at anmode om denne liste.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## E. Hvor det er relevant, at den dataansvarlige agter at overføre personoplysninger til et tredjeland eller en international organisation, og om hvorvidt Kommissionen har truffet afgørelse om tilstrækkeligheden af beskyttelsesniveauet, eller i tilfælde af overførsler i henhold til artikel 46 eller 47 eller artikel 49, stk. 1, andet afsnit, litra h), henvisning til de fornødne eller passende garantier, og hvordan der kan fås en kopi heraf, eller hvor de er blevet gjort tilgængelige (artikel 13, stk. 1, litra f, 46, stk. 1, 46, stk. c GDPR)

Alle virksomheder og filialer, der er en del af vores koncern (herefter benævnt "koncernselskaber"), der har deres forretningssted eller kontor i et tredjeland, kan tilhøre modtagerne af personoplysninger. En liste over alle koncernselskaber eller modtagere kan rekvireres hos os.

I henhold til artikel 46, stk. 1, GDPR, må en dataansvarlig eller databehandler kun overføre personoplysninger til et tredjeland, hvis den dataansvarlige eller databehandleren har ydet passende garantier, og på betingelse af, at håndhævede registrerede rettigheder og effektive retsmidler er tilgængelige for de registrerede. Der kan ydes passende garantier uden at kræve nogen særlig tilladelse fra en tilsynsmyndighed ved hjælp af standardkontraktbestemmelser, artikel 46, stk. 2, litra. c GDPR.

Den Europæiske Unions standardkontraktklausuler eller andre passende sikkerhedsforanstaltninger aftales med alle modtagere fra tredjelande før den første overførsel af personoplysninger. Som følge heraf sikres det, at passende sikkerhedsforanstaltninger, håndhævbare registreredes rettigheder og effektive retsmidler for de registrerede er garanteret. Alle registrerede kan få en kopi af standardkontraktbestemmelserne fra os. Standardkontraktbestemmelserne er også tilgængelige i Den Europæiske Unions Tidende.

Artikel 45, stk. 3, i GDPR giver Europa-Kommissionen beføjelse til ved hjælp af en gennemførelsesretsakt at beslutte, at et tredjeland sikrer et tilstrækkeligt databeskyttelsesniveau. Det betyder et niveau for beskyttelse af personoplysninger, der i det væsentlige svarer til beskyttelsesniveauet i EU. Som følge af afgørelser om tilstrækkeligheden af beskyttelsesniveauet kan persondata frit flyttes fra EU (og Norge, Liechtenstein og Island) til et tredjeland uden yderligere hindringer. Lignende regler gælder for Storbritannien, Schweiz og nogle andre lande.

Hvor Europa-Kommissionen eller regeringen i et andet land har fastslået, at et tredjeland sikrer et tilstrækkeligt databeskyttelsesniveau, og hvor der findes en eksisterende ramme (f.eks. EU-U.S. Data Privacy Framework, Swiss-U.S. Data Privacy Framework, UK Extension to the EU-U.S. Data Privacy Framework), vil alle overførsler, vi foretager til medlemmer af sådanne rammer (f.eks. selvcertificerede enheder), udelukkende være baseret på enhedens medlemskab af den pågældende ramme. Hvis vi eller en af vores koncernenheder er medlem af en sådan ramme, vil alle overførsler til os eller vores koncernenhed udelukkende være baseret på den pågældende enheds medlemskab af denne ramme.


© All rights reserved by Heiko Maniero.

Is féidir le haon ábhar sonraí cóip de na creataí a fháil uainn. Ina theannta sin, tá na creataí ar fáil freisin in Iris Oifigiúil an Aontais Eorpaigh nó sna hábhair dhlíthiúla a foilsíodh nó ar shuíomhanna gréasáin na n-údarás maoirseachta nó na n-údarás inniúil nó na n-institiúidí inniúla eile.

## F. Det tidsrum, hvor personoplysningerne vil blive opbevaret, eller hvis dette ikke er muligt, de kriterier, der anvendes til at fastlægge dette tidsrum (artikel 13, stk. 2, litra a GDPR)

Varigheden af opbevaring af personoplysninger om ansøgere er 6 måneder. For medarbejderdata gælder den respektive lovpligtige opbevaringsperiode. Efter udløbet af denne periode slettes de tilsvarende data rutinemæssigt, så længe det ikke længere er nødvendigt for opfyldelse af kontrakten eller iværksættelse af en kontrakt.

## G. Retten til at anmode den dataansvarlige om indsigt i og berigtigelse eller sletning af personoplysninger eller begrænsning af behandling vedrørende den registrerede eller til at gøre indsigelse mod behandling samt retten til dataportabilitet (artikel 13, stk. 2, litra b) GDPR)

Alle registrerede har følgende rettigheder:

***Ret til adgang***

Hver registreret har ret til at få adgang til de personoplysninger, der vedrører ham eller hende. Retten til indsigt omfatter alle data, der behandles af os. Retten kan udøves let og med rimelige intervaller for at være opmærksom på og verificere lovligheden af behandlingen (betragtning 63 GDPR). Denne ret følger af art. 15 GDPR. Den registrerede kan kontakte os for at udøve retten til indsigt.

***Ret til berigtigelse***

I henhold til artikel 16, punktum 1 GDPR, har den registrerede ret til uden unødig forsinkelse at få berigtiget unøjagtige personoplysninger om ham eller hende fra den dataansvarlige. Desuden bestemmer artikel 16 sætning 2 GDPR, at den registrerede under hensyntagen til formålene med behandlingen har ret til at få ufuldstændige personoplysninger udfyldt, herunder ved at afgive en supplerende erklæring. Den registrerede kan kontakte os for at udøve retten til berigtigelse.

***Ret til sletning (retten til at blive glemt)***

Derudover har registrerede ret til en ret til sletning og til at blive glemt i henhold til art. 17 GDPR. Denne ret kan også udøves ved at kontakte os. På dette tidspunkt vil vi dog gerne gøre opmærksom på, at denne ret ikke gælder i det omfang, behandlingen er nødvendig for at opfylde en retlig forpligtelse, som vores virksomhed er underlagt, § 17, stk. b GDPR. Det betyder, at vi først kan godkende en ansøgning om sletning efter udløbet af den lovpligtige opbevaringsperiode.


© All rights reserved by Heiko Maniero.

***Ret til begrænsning af behandlingen***

I henhold til artikel 18 GDPR har enhver registreret ret til en begrænsning af behandlingen. Begrænsning af behandlingen kan kræves, hvis en af betingelserne i artikel 18, stk. ad GDPR er opfyldt. Den registrerede kan kontakte os for at udøve retten til begrænsning af behandlingen.

***Ret til at gøre indsigelse***

Endvidere er art. 21 GDPR garanterer retten til at gøre indsigelse. Den registrerede kan kontakte os for at udøve retten til at gøre indsigelse.

***Ret til dataportabilitet***

Kunst. 20 GDPR giver den registrerede ret til dataportabilitet. Efter denne bestemmelse har den registrerede under de betingelser, der er fastsat i artikel 20, stk. a og b GDPR retten til at modtage de personoplysninger om ham eller hende, som han eller hun har givet til en dataansvarlig, i et struktureret, almindeligt anvendt og maskinlæsbart format og har ret til at overføre disse data til en anden dataansvarlig uden hindring fra den dataansvarlige, som personoplysningerne er givet til. Den registrerede kan kontakte os for at udøve retten til dataportabilitet.

## H. Når behandling er baseret på artikel 6, stk. 1, litra a), eller artikel 9, stk. 2, litra a), retten til at trække samtykke tilbage på ethvert tidspunkt, uden at dette berører lovligheden af behandling, der er baseret på samtykke, inden tilbagetrækning heraf (Artikel 13, stk. 2, litra c GDPR)

Hvis behandlingen af personoplysninger er baseret på art. 6, stk. 1 lit. en GDPR, hvilket er tilfældet, hvis den registrerede har givet samtykke til behandling af personoplysninger til et eller flere specifikke formål eller er baseret på artikel 9, stk. en GDPR, som regulerer det udtrykkelige samtykke til behandling af særlige kategorier af personoplysninger, har den registrerede i henhold til artikel 7, stk. 3, punktum 1 GDPR ret til at trække sit samtykke tilbage til enhver tid.

Tilbagetrækning af samtykke påvirker ikke lovligheden af behandling baseret på samtykke før tilbagetrækningen, artikel 7, stk. 3, punktum 2 GDPR. Det skal være lige så nemt at trække tilbage som at give samtykke, art. 7, stk. 3, punktum 4 GDPR. Derfor kan tilbagekaldelse af samtykke altid ske på samme måde, som der er givet samtykke, eller på anden måde, der af den registrerede anses for at være enklere. I dagens informationssamfund er nok den enkleste måde at trække samtykke tilbage på en simpel e-mail. Hvis den registrerede ønsker at trække sit samtykke, der er givet til os, tilbage, er en simpel e-mail til os tilstrækkelig. Alternativt kan den registrerede vælge en hvilken som helst anden måde at kommunikere sin tilbagetrækning af samtykke til os på.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## I. Retten til at indgive en klage til en tilsynsmyndighed (Artikel 13, stk. 2, litra d, 77, stk. 1, GDPR)

Som dataansvarlig er vi forpligtet til at underrette den registrerede om retten til at indgive en klage til en tilsynsmyndighed, artikel 13, stk. d GDPR. Retten til at indgive en klage til en tilsynsmyndighed er reguleret af artikel 77, stk. 1, GDPR. I henhold til denne bestemmelse har enhver registreret ret til at indgive en klage til en tilsynsmyndighed, især i den medlemsstat, hvor vedkommendes sædvanlige opholdssted, arbejdssted eller sted, uden at det berører andre administrative eller retslige retsmidler. den påståede krænkelse, hvis den registrerede mener, at behandlingen af personoplysninger vedrørende ham eller hende er i strid med den generelle databeskyttelsesforordning. Retten til at indgive en klage til en tilsynsmyndighed var kun begrænset af unionsretten på en sådan måde, at den kun kan udøves over for en enkelt tilsynsmyndighed (betragtning 141, sætning 1 GDPR). Denne regel har til formål at undgå dobbeltklager fra samme registrerede i samme sag. Hvis en registreret ønsker at indgive en klage over os, har vi derfor bedt om kun at kontakte en enkelt tilsynsmyndighed.

## J. Om meddelelse af personoplysninger er lovpligtigt eller et krav i henhold til en kontrakt eller et krav, der skal være opfyldt for at indgå en kontrakt, samt om den registrerede har pligt til at give personoplysningerne og de eventuelle konsekvenser af ikke at give sådanne oplysninger (Art. 13(2) lit. e GDPR)

Vi præciserer, at leveringen af personoplysninger delvist er lovpligtig (f.eks. skatteregler) eller også kan følge af kontraktlige bestemmelser (f.eks. oplysninger om den kontraktlige partner).

Nogle gange kan det være nødvendigt at indgå en kontrakt om, at den registrerede giver os personoplysninger, som efterfølgende skal behandles af os. Den registrerede er for eksempel forpligtet til at give os personoplysninger, når vores virksomhed underskriver en kontrakt med ham eller hende. Manglende udlevering af personoplysningerne ville have den konsekvens, at kontrakten med den registrerede ikke kunne indgås.

Inden personoplysninger afgives af den registrerede, skal den registrerede kontakte os. Vi afklarer over for den registrerede, om udleveringen af personoplysningerne er påkrævet ved lov eller kontrakt eller er nødvendig for indgåelse af kontrakten, om der er en forpligtelse til at udlevere personoplysningerne og konsekvenserne af manglende udlevering af personoplysningerne.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

### K. Forekomsten af automatiske afgørelser, herunder profilering, som omhandlet i artikel 22, stk. 1 og 4, og i disse tilfælde som minimum meningsfulde oplysninger om logikken heri samt betydningen og de forventede konsekvenser af en sådan behandling for den registrerede (artikel 13, stk. 2, litra f GDPR)

Som en ansvarlig virksomhed bruger vi normalt ikke automatiseret beslutningstagning eller profilering. Hvis vi i undtagelsestilfælde udfører automatiseret beslutningstagning eller profilering, informerer vi den registrerede enten separat eller via et underafsnit i vores privatlivspolitik (på vores hjemmeside). I dette tilfælde gælder følgende:

Automatiseret beslutningstagning - herunder profilering - kan forekomme, hvis (1) dette er nødvendigt for at indgå eller opfylde en kontrakt mellem den registrerede og os, eller (2) dette er tilladt i henhold til EU-lovgivning eller medlemsstatslovgivning, som vi er underlagt, og som også fastlægger passende foranstaltninger til at beskytte den registreredes rettigheder og friheder og legitime interesser; eller (3) dette er baseret på den registreredes udtrykkelige samtykke.

I de tilfælde, der henvises til i artikel 22, stk. 2, litra a) og c), i GDPR, skal vi gennemføre passende foranstaltninger for at beskytte den registreredes rettigheder og friheder og legitime interesser. I disse tilfælde har du ret til at opnå menneskelig indgriben fra den dataansvarliges side, til at udtrykke dit synspunkt og til at anfægte beslutningen.

Betydningsfulde oplysninger om den involverede logik samt betydningen og de forventede konsekvenser af en sådan behandling for den registrerede er beskrevet i vores privatlivspolitik.

## II. Oplysningspligt, hvis personoplysninger ikke er indsamlet hos den registrerede (artikel 14 GDPR)

### A. Identitet på og kontaktoplysninger for den dataansvarlige og dennes eventuelle repræsentant (artikel 14, stk. 1, litra a GDPR)

Se ovenfor

### B. Kontaktoplysninger for en eventuel databeskyttelsesrådgiver (artikel 14, stk. 1, litra b GDPR)

Se ovenfor


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## C. Formålene med den behandling, som personoplysningerne skal bruges til, samt retsgrundlaget for behandlingen (artikel 14, stk. 1, litra c GDPR)

For ansøgers data, der ikke er indsamlet fra den registrerede, er formålet med databehandlingen at gennemføre en undersøgelse af ansøgningen under rekrutteringsprocessen. Til dette formål kan vi behandle data, der ikke er indsamlet fra dig. På baggrund af de data, der behandles under rekrutteringsprocessen, tjekker vi, om du bliver inviteret til en jobsamtale (en del af udvælgelsesprocessen). Hvis du bliver ansat af os, konverteres ansøgerens data automatisk til medarbejderdata. For medarbejderdata er formålet med databehandling udførelsen af ansættelseskontrakten eller overholdelse af andre lovbestemmelser, der gælder for ansættelsesforholdet. Medarbejderdata opbevares efter ansættelsesforholdets ophør for at opfylde lovmæssige opbevaringsperioder.

Retsgrundlaget for databehandling er artikel 6, stk. b og f GDPR, artikel 9, stk. 2, lit. b og h GDPR, artikel 88 (1) GDPR og national lovgivning, såsom for Tysklands § 26 BDSG (Federal Data Protection Act).

## D. De berørte kategorier af personoplysninger (artikel 14, stk. 1, litra d GDPR)

Ansøgers data

Medarbejderdata

## E. Eventuelle modtagere eller kategorier af modtagere af personoplysningerne (artikel 14, stk. 1, litra e GDPR)

Offentlige myndigheder

Eksterne organer

Yderligere eksterne organer

Intern behandling

Intragruppebehandling

Andre kroppe

En liste over vores databehandlere og datamodtagere i tredjelande og, hvis relevant, internationale organisationer er enten offentliggjort på vores hjemmeside eller kan rekvireres gratis fra os. Kontakt venligst vores databeskyttelsesansvarlige for at anmode om denne liste.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## F. Hvor det er relevant, at den dataansvarlige agter at overføre personoplysninger til en modtager i et tredjeland eller en international organisation, og om hvorvidt Kommissionen har truffet afgørelse om tilstrækkeligheden af beskyttelsesniveauet, eller i tilfælde af overførsler i henhold til artikel 46 eller 47 eller artikel 49, stk. 1, andet afsnit, litra h), henvisning til de fornødne eller passende garantier, og hvordan der kan fås en kopi heraf, eller hvor de er blevet gjort tilgængelige (artikel 14, stk. 1, litra f, 46, stk. 1, 46, stk. c GDPR)

Alle virksomheder og filialer, der er en del af vores koncern (herefter benævnt "koncernselskaber"), der har deres forretningssted eller kontor i et tredjeland, kan tilhøre modtagerne af personoplysninger. En liste over alle koncernselskaber eller modtagere kan rekvireres hos os.

I henhold til artikel 46, stk. 1, GDPR, må en dataansvarlig eller databehandler kun overføre personoplysninger til et tredjeland, hvis den dataansvarlige eller databehandleren har ydet passende garantier, og på betingelse af, at håndhævede registrerede rettigheder og effektive retsmidler er tilgængelige for de registrerede. Der kan ydes passende sikkerhedsforanstaltninger uden at kræve nogen specifik tilladelse fra en tilsynsmyndighed ved hjælp af standarddatabeskyttelsesklausuler, artikel 46, stk. c GDPR.

Den Europæiske Unions standardkontraktklausuler eller andre passende sikkerhedsforanstaltninger aftales med alle modtagere fra tredjelande før den første overførsel af personoplysninger. Som følge heraf sikres det, at passende sikkerhedsforanstaltninger, håndhævbare registreredes rettigheder og effektive retsmidler for de registrerede er garanteret. Alle registrerede kan få en kopi af standardkontraktbestemmelserne fra os. Standardkontraktbestemmelserne er også tilgængelige i Den Europæiske Unions Tidende.

Artikel 45, stk. 3, i GDPR giver Europa-Kommissionen beføjelse til ved hjælp af en gennemførelsesretsakt at beslutte, at et tredjeland sikrer et tilstrækkeligt databeskyttelsesniveau. Det betyder et niveau for beskyttelse af personoplysninger, der i det væsentlige svarer til beskyttelsesniveauet i EU. Som følge af afgørelser om tilstrækkeligheden af beskyttelsesniveauet kan persondata frit flyttes fra EU (og Norge, Liechtenstein og Island) til et tredjeland uden yderligere hindringer. Lignende regler gælder for Storbritannien, Schweiz og nogle andre lande.

Hvor Europa-Kommissionen eller regeringen i et andet land har fastslået, at et tredjeland sikrer et tilstrækkeligt databeskyttelsesniveau, og hvor der findes en eksisterende ramme (f.eks. EU-U.S. Data Privacy Framework, Swiss-U.S. Data Privacy Framework, UK Extension to the EU-U.S. Data Privacy Framework), vil alle overførsler, vi foretager til medlemmer af sådanne rammer (f.eks. selvcertificerede enheder), udelukkende være baseret på enhedens medlemskab af den pågældende ramme. Hvis vi eller en af vores koncernenheder er medlem af en sådan ramme, vil alle overførsler til os eller vores koncernenhed udelukkende være baseret på den pågældende enheds medlemskab af denne ramme.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

Is féidir le haon ábhar sonraí cóip de na creataí a fháil uainn. Ina theannta sin, tá na creataí ar fáil freisin in Iris Oifigiúil an Aontais Eorpaigh nó sna hábhair dhlíthiúla a foilsíodh nó ar shuíomhanna gréasáin na n-údarás maoirseachta nó na n-údarás inniúil nó na n-institiúidí inniúla eile.

## G. Det tidsrum, hvor personoplysningerne vil blive opbevaret, eller hvis dette ikke er muligt, de kriterier, der anvendes til at fastlægge dette tidsrum (artikel 14, stk. 2, litra a GDPR)

Varigheden af opbevaring af personoplysninger om ansøgere er 6 måneder. For medarbejderdata gælder den respektive lovpligtige opbevaringsperiode. Efter udløbet af denne periode slettes de tilsvarende data rutinemæssigt, så længe det ikke længere er nødvendigt for opfyldelse af kontrakten eller iværksættelse af en kontrakt.

## H. De legitime interesser, som forfølges af den dataansvarlige eller en tredjemand, hvis behandlingen er baseret på artikel 6, stk. 1, litra f) (Art. 14(2) lit. b GDPR)

I henhold til artikel 6, stk. f GDPR er behandlingen kun lovlig, hvis behandlingen er nødvendig af hensyn til legitime interesser, der forfølges af den dataansvarlige eller af en tredjepart, undtagen hvor sådanne interesser tilsidesættes af den registreredes interesser eller grundlæggende rettigheder og friheder, som kræver beskyttelse af personlige data. Ifølge betragtning 47, punktum 2 GDPR, kunne der eksistere en legitim interesse, hvor der er et relevant og passende forhold mellem den registrerede og den dataansvarlige, fx i situationer, hvor den registrerede er klient hos den dataansvarlige. I alle tilfælde, hvor vores virksomhed behandler ansøgers data baseret på artikel 6, stk. f GDPR er vores legitime interesse ansættelse af egnet personale og fagfolk.

## I. Retten til at anmode den dataansvarlige om indsigt i og berigtigelse eller sletning af personoplysninger eller begrænsning af behandling vedrørende den registrerede og til at gøre indsigelse mod behandling samt retten til dataportabilitet (artikel 14, stk. 2, litra c). GDPR)

Alle registrerede har følgende rettigheder:

***Ret til adgang***

Hver registreret har ret til at få adgang til de personoplysninger, der vedrører ham eller hende. Retten til indsigt omfatter alle data, der behandles af os. Retten kan udøves let og med rimelige intervaller for at være opmærksom på og verificere lovligheden af behandlingen (betragtning 63 GDPR). Denne ret følger af art. 15 GDPR. Den registrerede kan kontakte os for at udøve retten til indsigt.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

***Ret til berigtigelse***

I henhold til artikel 16, punktum 1 GDPR, har den registrerede ret til uden unødig forsinkelse at få berigtiget unøjagtige personoplysninger om ham eller hende fra den dataansvarlige. Desuden bestemmer artikel 16 sætning 2 GDPR, at den registrerede under hensyntagen til formålene med behandlingen har ret til at få ufuldstændige personoplysninger udfyldt, herunder ved at afgive en supplerende erklæring. Den registrerede kan kontakte os for at udøve retten til berigtigelse.

***Ret til sletning (retten til at blive glemt)***

Derudover har registrerede ret til en ret til sletning og til at blive glemt i henhold til art. 17 GDPR. Denne ret kan også udøves ved at kontakte os. På dette tidspunkt vil vi dog gerne gøre opmærksom på, at denne ret ikke gælder i det omfang, behandlingen er nødvendig for at opfylde en retlig forpligtelse, som vores virksomhed er underlagt, § 17, stk. b GDPR. Det betyder, at vi først kan godkende en ansøgning om sletning efter udløbet af den lovpligtige opbevaringsperiode.

***Ret til begrænsning af behandlingen***

I henhold til artikel 18 GDPR har enhver registreret ret til begrænsning af behandlingen. Begrænsning af behandlingen kan kræves, hvis en af betingelserne i artikel 18, stk. ad GDPR er opfyldt. Den registrerede kan kontakte os for at udøve retten til begrænsning af behandlingen.

***Ret til at gøre indsigelse***

Endvidere er art. 21 GDPR garanterer retten til at gøre indsigelse. Den registrerede kan kontakte os for at udøve retten til at gøre indsigelse.

***Ret til dataportabilitet***

Kunst. 20 GDPR giver den registrerede ret til dataportabilitet. I henhold til denne bestemmelse har den registrerede under de betingelser, der er fastsat i artikel 20, stk. a og b GDPR retten til at modtage de personoplysninger om ham eller hende, som han eller hun har givet til en dataansvarlig, i et struktureret, almindeligt anvendt og maskinlæsbart format og har ret til at overføre disse data til en anden dataansvarlig uden hindring fra den dataansvarlige, som personoplysningerne er givet til. Den registrerede kan kontakte os for at udøve retten til dataportabilitet.

## J. Når behandling er baseret på artikel 6, stk. 1, litra a), eller artikel 9, stk. 2, litra a), retten til at trække samtykke tilbage på ethvert tidspunkt, uden at dette berører lovligheden af behandling, der er baseret på samtykke, inden tilbagetrækning heraf (Art. 14(2) lit. d GDPR)

Hvis behandlingen af personoplysninger er baseret på art. 6, stk. 1 lit. en GDPR, hvilket er tilfældet, hvis den registrerede har givet samtykke til behandling af personoplysninger til et eller flere specifikke formål eller er baseret på artikel 9, stk. en GDPR, som regulerer det udtrykkelige samtykke til behandling af særlige kategorier af personoplysninger, har den registrerede i henhold til artikel 7, stk. 3, punktum 1 GDPR ret til at trække sit samtykke tilbage til enhver tid.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

Tilbagetrækning af samtykke påvirker ikke lovligheden af behandling baseret på samtykke før tilbagetrækningen, artikel 7, stk. 3, punktum 2 GDPR. Det skal være lige så nemt at trække tilbage som at give samtykke, art. 7, stk. 3, punktum 4 GDPR. Derfor kan tilbagekaldelse af samtykke altid ske på samme måde, som der er givet samtykke, eller på anden måde, der af den registrerede anses for at være enklere. I dagens informationssamfund er nok den enkleste måde at trække samtykke tilbage på en simpel e-mail. Hvis den registrerede ønsker at trække sit samtykke, der er givet til os, tilbage, er en simpel e-mail til os tilstrækkelig. Alternativt kan den registrerede vælge en hvilken som helst anden måde at kommunikere sin tilbagetrækning af samtykke til os på.

## K. Retten til at indgive en klage til en tilsynsmyndighed (Artikel 14, stk. 2, lit. e, 77, stk. 1, GDPR)

Som dataansvarlig er vi forpligtet til at underrette den registrerede om retten til at indgive en klage til en tilsynsmyndighed, artikel 14, stk. e GDPR. Retten til at indgive en klage til en tilsynsmyndighed er reguleret af artikel 77, stk. 1, GDPR. I henhold til denne bestemmelse har enhver registreret ret til at indgive en klage til en tilsynsmyndighed, især i den medlemsstat, hvor vedkommendes sædvanlige opholdssted, arbejdssted eller sted, uden at det berører andre administrative eller retslige retsmidler. den påståede krænkelse, hvis den registrerede mener, at behandlingen af personoplysninger vedrørende ham eller hende er i strid med den generelle databeskyttelsesforordning. Retten til at indgive en klage til en tilsynsmyndighed var kun begrænset af unionsretten på en sådan måde, at den kun kan udøves over for en enkelt tilsynsmyndighed (betragtning 141, sætning 1 GDPR). Denne regel har til formål at undgå dobbeltklager fra samme registrerede i samme sag. Hvis en registreret ønsker at indgive en klage over os, har vi derfor bedt om kun at kontakte en enkelt tilsynsmyndighed.

## L. Hvilken kilde personoplysningerne hidrører fra, og eventuelt hvorvidt de stammer fra offentligt tilgængelige kilder (artikel 14, stk. 2, litra f GDPR)

I princippet indsamles personoplysninger direkte fra den registrerede eller i samarbejde med en myndighed (f.eks. indhentning af data fra et officielt register). Andre data om registrerede er afledt af overdragelser af koncernselskaber. I forbindelse med denne generelle information er navngivningen af de nøjagtige kilder, hvorfra personoplysningerne stammer, enten umuligt eller ville involvere en uforholdsmæssig indsats i henhold til art. 14(5) lit. b GDPR. I princippet indsamler vi ikke personoplysninger fra offentligt tilgængelige kilder.

Enhver registreret person kan til enhver tid kontakte os for at få mere detaljeret information om de nøjagtige kilder til de personoplysninger, der vedrører ham eller hende. Hvor oprindelsen af personoplysningerne ikke kan gives til den registrerede, fordi forskellige kilder er blevet brugt, bør der gives generel information (betragtning 61, sætning 4 GDPR).


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

### M. Forekomsten af automatiske afgørelser, herunder profilering, som omhandlet i artikel 22, stk. 1 og 4, og i disse tilfælde som minimum meningsfulde oplysninger om logikken heri samt betydningen og de forventede konsekvenser af en sådan behandling for den registrerede (artikel 14, stk. 2, litra g GDPR)

Som en ansvarlig virksomhed bruger vi normalt ikke automatiseret beslutningstagning eller profilering. Hvis vi i undtagelsestilfælde udfører automatiseret beslutningstagning eller profilering, informerer vi den registrerede enten separat eller via et underafsnit i vores privatlivspolitik (på vores hjemmeside). I dette tilfælde gælder følgende:

Automatiseret beslutningstagning - herunder profilering - kan forekomme, hvis (1) dette er nødvendigt for at indgå eller opfylde en kontrakt mellem den registrerede og os, eller (2) dette er tilladt i henhold til EU-lovgivning eller medlemsstatslovgivning, som vi er underlagt, og som også fastlægger passende foranstaltninger til at beskytte den registreredes rettigheder og friheder og legitime interesser; eller (3) dette er baseret på den registreredes udtrykkelige samtykke.

I de tilfælde, der henvises til i artikel 22, stk. 2, litra a) og c), i GDPR, skal vi gennemføre passende foranstaltninger for at beskytte den registreredes rettigheder og friheder og legitime interesser. I disse tilfælde har du ret til at opnå menneskelig indgriben fra den dataansvarliges side, til at udtrykke dit synspunkt og til at anfægte beslutningen.

Betydningsfulde oplysninger om den involverede logik samt betydningen og de forventede konsekvenser af en sådan behandling for den registrerede er beskrevet i vores privatlivspolitik.

## III. EU-U.S. Data Privacy Framework (EU-U.S. DPF), UK Extension to the EU-U.S. DPF, Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF)

Hvis vores organisation er et certificeret medlem af EU-U.S. Data Privacy Framework (EU-U.S. DPF) og/eller UK Extension to the EU-U.S. DPF og/eller Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF), gælder følgende:

Vi overholder EU-U.S. Data Privacy Framework (EU-U.S. DPF) og UK Extension to the EU-U.S. DPF samt Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF), som fastsat af U.S. Department of Commerce. Vores virksomhed har bekræftet over for det amerikanske handelsministerium, at den overholder EU-U.S. Data Privacy Framework Principles (EU-U.S. DPF Principles) med hensyn til behandling af personoplysninger, som den modtager fra Den Europæiske Union og Det Forenede Kongerige i henhold til EU-U.S. DPF og UK Extension to the EU-U.S. DPF. Vores virksomhed har bekræftet over for det amerikanske handelsministerium, at den overholder Swiss-U.S. Data Privacy Framework Principles (Swiss-U.S. DPF Principles) med hensyn til behandling af personoplysninger, som den modtager fra Schweiz i henhold til Swiss-U.S. DPF. I tilfælde af uoverensstemmelse mellem


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

bestemmelserne i vores privatlivspolitik og EU-U.S. DPF Principles og/eller Swiss-U.S. DPF Principles, er Principles afgørende.

For at få mere at vide om Data Privacy Framework (DPF) programmet og for at se vores certificering, besøg venligst https://www.dataprivacyframework.gov/.

De øvrige amerikanske enheder eller datterselskaber i vores virksomhed, der også overholder EU-U.S. DPF Principals, herunder UK Extension to the EU-U.S. DPF og Swiss-U.S. DPF Principals, hvis de findes, er nævnt i vores privatlivspolitik.

I overensstemmelse med EU-U.S. DPF og UK Extension to the EU-U.S. DPF samt Swiss-U.S. DPF forpligter vores virksomhed sig til at samarbejde med det panel, der er oprettet af EU's databeskyttelsesmyndigheder og Det Forenede Kongeriges Information Commissioner's Office (ICO) samt den schweiziske føderale databeskyttelses- og informationskommissær (EDÖB), og følge deres råd vedrørende uløste klager over vores håndtering af personoplysninger, som vi modtager i henhold til EU-U.S. DPF og UK Extension to the EU-U.S. DPF samt Swiss-U.S. DPF.

Vi informerer de berørte personer om de relevante europæiske databeskyttelsesmyndigheder, der er ansvarlige for behandlingen af klager over vores organisations håndtering af personoplysninger, i den øverste del af dette gennemsigtighedsdokument og om, at vi tilbyder de berørte personer en passende og gratis retsmidler.

Vi informerer alle berørte personer om, at vores virksomhed er underlagt Federal Trade Commissions (FTC) undersøgelses- og håndhævelsesbeføjelser.

Berørte personer har under visse forudsætninger mulighed for at benytte bindende voldgift. Vores organisation er forpligtet til at bilægge krav og overholde betingelserne i bilag I til DPF-Principals, forudsat at den berørte person har anmodet om bindende voldgift ved at underrette vores organisation og har fulgt procedurerne og betingelserne i bilag I til Principals.

Vi informerer hermed alle berørte personer om vores organisations ansvar i tilfælde af videregivelse af personoplysninger til tredjepart.

For spørgsmål fra berørte personer eller datatilsynsmyndigheder har vi udpeget de lokale repræsentanter, der er nævnt ovenfor i dette gennemsigtighedsdokument.

Vi giver dig mulighed for at vælge (Opt-out), om dine personoplysninger (i) skal videregives til tredjepart eller (ii) bruges til et formål, der væsentligt adskiller sig fra det/de formål, som de oprindeligt blev indsamlet til eller senere blev godkendt af dig. Den klare, synlige og let tilgængelige mekanisme til at udøve dit valg består i at kontakte vores databeskyttelsesansvarlige (DSB) via e-mail. Du har ikke mulighed for at vælge, og vi er heller ikke forpligtet til det, hvis oplysningerne videregives til en tredjepart, der fungerer som agent eller databehandler på vores vegne og efter vores anvisninger. Vi indgår dog altid en aftale med en sådan agent eller databehandler.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

For følsomme oplysninger (dvs. personoplysninger, der indeholder oplysninger om helbredstilstand, race eller etnisk oprindelse, politiske holdninger, religiøse eller filosofiske overbevisninger, fagforeningsmedlemskab eller oplysninger om den pågældende persons seksualliv) indhenter vi dit udtrykkelige samtykke (Opt-in), når disse oplysninger (i) videregives til tredjepart eller (ii) bruges til et andet formål end det, som de oprindeligt blev indsamlet til, eller som du senere har givet samtykke til ved at vælge Opt-in. Desuden behandler vi alle personoplysninger, som vi modtager fra tredjepart, som følsomme, hvis tredjeparten identificerer og behandler dem som følsomme.

Vi informerer dig hermed om kravet om at videregive personoplysninger som reaktion på lovlige anmodninger fra myndigheder, herunder opfyldelse af krav om national sikkerhed eller retshåndhævelse.

Ved videregivelse af personoplysninger til en tredjepart, der fungerer som dataansvarlig, overholder vi Principals om meddelelse og valg. Derudover indgår vi en aftale med tredjeparten, der er ansvarlig for behandlingen, som fastsætter, at disse oplysninger kun må behandles til begrænsede og specificerede formål i overensstemmelse med dit samtykke, og at modtageren skal tilbyde det samme beskyttelsesniveau som DPF Principals og underrette os, hvis det konstaterer, at det ikke længere kan opfylde denne forpligtelse. Aftalen fastsætter, at tredjeparten, der er ansvarlig, skal stoppe behandlingen eller træffe andre passende og rimelige foranstaltninger for at afhjælpe situationen, hvis en sådan konstatering foretages.

Ved videregivelse af personoplysninger til en tredjepart, der fungerer som agent eller databehandler, (i) videregiver vi kun disse oplysninger til begrænsede og specificerede formål; (ii) sikrer vi, at agenten eller databehandleren er forpligtet til at tilbyde mindst samme niveau af databeskyttelse, som DPF-Principals kræver; (iii) træffer vi passende og rimelige foranstaltninger for at sikre, at agenten eller databehandleren faktisk behandler de videregivne personoplysninger på en måde, der er i overensstemmelse med vores forpligtelser i henhold til DPF-Principals; (iv) kræver vi, at agenten eller databehandleren underretter vores organisation, hvis det konstaterer, at det ikke længere kan opfylde forpligtelsen til at tilbyde samme beskyttelsesniveau, som DPF-Principals kræver; (v) efter en sådan underretning, også i henhold til (iv), træffer vi passende og rimelige foranstaltninger for at stoppe uautoriseret behandling og afhjælpe situationen; og (vi) giver vi DPF Department efter anmodning et resumé eller et repræsentativt eksempel på de relevante databeskyttelsesbestemmelser fra vores aftale med denne agent.

I overensstemmelse med EU-U.S. DPF og/eller UK Extension to the EU-U.S. DPF og/eller Swiss-U.S. DPF forpligter vores organisation sig til at samarbejde med det panel, der er oprettet af EU's databeskyttelsesmyndigheder og Det Forenede Kongeriges Information Commissioner's Office (ICO) eller den schweiziske føderale databeskyttelses- og informationskommissær (EDÖB) og følge deres råd vedrørende uløste klager over vores håndtering af personoplysninger, som vi modtager i forbindelse med ansættelsesforhold i henhold til EU-U.S. DPF og UK Extension to the EU-U.S. DPF og Swiss-U.S. DPF.

Alle registrerede, der midlertidigt befinder sig i Den Europæiske Union (EU), Det Europæiske Økonomiske Samarbejdsområde (EØS) eller Det Forenede Kongerige, eller som har deres bopæl eller sædvanlige opholdssted der, har ret til de rettigheder og registreredes rettigheder, der er offentliggjort i


© All rights reserved by Heiko Maniero.

vores gennemsigtighedsdokument, og som også følger af artikel 15 til 22 i GDPR, herunder retten til at få adgang til personoplysninger. Vi har gjort disse oplysninger tilgængelige på alle EU- og EØS-sprog. Den engelsksprogede version gælder for Storbritannien.

Alle registrerede, der er midlertidigt bosiddende i Schweiz eller har deres bopæl eller sædvanlige opholdssted der, har ret til de rettigheder og den registreredes rettigheder i henhold til den schweiziske databeskyttelseslov (DPA) og den schweiziske databeskyttelsesforordning (DPR), som er offentliggjort i vores gennemsigtighedsdokument, herunder retten til at få adgang til personlige data. Vi har stillet disse oplysninger til rådighed på de tre officielle sprog i Schweiz (tysk, italiensk og fransk).


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

# NORWEGIAN: Informasjon om behandling av personopplysninger (artikkel 13 og 14 i GDPR)

Kjære frue eller herre,

Personopplysningene til hver enkelt person som står i et kontraktsforhold, et forhold før kontraktsinngåelse eller et annet forhold til selskapet vårt, fortjener spesiell beskyttelse. Vi har som mål å holde et høyt nivå når det gjelder personvern. Derfor jobber vi kontinuerlig med å utvikle konseptene våre for personvern og datasikkerhet.

Vi overholder selvfølgelig de lovbestemte bestemmelsene om personvern. I henhold til artikkel 13, 14 i personvernforordningen skal behandlingsansvarlige oppfylle spesifikke informasjonskrav når de samler inn personopplysninger. Dette dokumentet oppfyller disse forpliktelsene.

Terminologien i juridiske forskrifter er komplisert. Dessverre var det ikke mulig å unngå bruk av juridiske termer i forbindelse med utarbeidelsen av dette dokumentet. Vi gjør derfor oppmerksom på at du alltid er velkommen til å kontakte oss hvis du har spørsmål om dette dokumentet, de brukte begrepene eller formuleringene.

## I. Overholdelse av informasjonskravene når personopplysninger samles inn fra den registrerte (artikkel 13 i GDPR)

### A. Identitet og kontaktinformasjon til den behandlingsansvarlige (artikkel 13(1) lit. a GDPR)

Se ovenfor

### B. Kontaktinformasjon til personvernombudet (artikkel 13(1) bokstav b i GDPR)

Se ovenfor

### C. Formålene med behandlingen som personopplysningene er ment for, samt det rettslige grunnlaget for behandlingen (artikkel 13(1) bokstav c GDPR)

Formålet med behandlingen av personopplysninger er å håndtere alle operasjoner som gjelder den behandlingsansvarlige, kunder, potensielle kunder, forretningspartnere eller andre kontraktsmessige eller prekontraktsmessige forhold mellom de nevnte gruppene (i videste forstand) eller juridiske forpliktelser for den behandlingsansvarlige.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

Art. 6(1) lit. a GDPR tjener som rettslig grunnlag for behandlingsoperasjoner der vi innhenter samtykke for et spesifikt behandlingsformål. Hvis behandlingen av personopplysninger er nødvendig for å oppfylle en kontrakt som den registrerte er part i, som for eksempel når behandlingen er nødvendig for å levere varer eller andre tjenester, er behandlingen basert på artikkel 6(1) bokstav b i GDPR. Det samme gjelder for behandling som er nødvendig for å gjennomføre tiltak før kontraktsinngåelse, for eksempel ved forespørsler om våre produkter eller tjenester. Hvis selskapet vårt er underlagt en rettslig forpliktelse som krever behandling av personopplysninger, for eksempel for å oppfylle skatteforpliktelser, er behandlingen basert på art. 6(1) bokstav c i GDPR.

I sjeldne tilfeller kan behandling av personopplysninger være nødvendig for å beskytte den registrertes eller en annen fysisk persons vitale interesser. Dette kan f.eks. være tilfelle hvis en besøkende blir skadet hos oss og navn, alder, helseforsikringsopplysninger eller annen viktig informasjon må gis videre til lege, sykehus eller annen tredjepart. I så fall vil behandlingen være basert på art. 6(1) bokstav d i GDPR.

Når behandlingen er nødvendig for å utføre en oppgave i allmennhetens interesse eller som ledd i offentlig myndighetsutøvelse som den behandlingsansvarlige er pålagt, er det rettslige grunnlaget art. 6(1) bokstav e i GDPR.

Endelig kan behandlingen være basert på artikkel 6(1) lit. f i GDPR. Dette rettslige grunnlaget brukes for behandling som ikke dekkes av noen av de ovennevnte rettslige grunnlagene, hvis behandlingen er nødvendig for å ivareta selskapets eller en tredjeparts berettigede interesser, med mindre den registrertes interesser eller grunnleggende rettigheter og friheter, som krever beskyttelse av personopplysninger, går foran. Slike behandlinger er spesielt tillatt fordi de er spesifikt nevnt av den europeiske lovgiveren. Han mente at en berettiget interesse kan antas å foreligge dersom den registrerte er kunde av den behandlingsansvarlige (betraktning 47, 2. setning i GDPR).

## D. Når behandlingen er basert på artikkel 6(1) lit. f GDPR, er det den behandlingsansvarliges eller en tredjeparts berettigede interesser som forfølges (artikkel 13(1) lit. d GDPR)

Når behandlingen av personopplysninger er basert på artikkel 6(1) lit. f i GDPR, er vår berettigede interesse å drive virksomheten vår til beste for alle våre ansatte og aksjonærer.

## E. Kategorier av mottakere av personopplysninger (artikkel 13(1) lit. e GDPR)

Offentlige myndigheter

Eksterne organer

Andre eksterne organer


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

Intern behandling

Konsernintern behandling

Andre organer

En liste over våre databehandlere og datamottakere i tredjeland og, hvis aktuelt, internasjonale organisasjoner, er enten publisert på nettstedet vårt eller kan bestilles gratis fra oss. Ta kontakt med vårt personvernombud for å be om denne listen.

## F. mottakere i et tredjeland og hensiktsmessige eller egnede garantier og hvordan man kan få en kopi av dem eller hvor de er gjort tilgjengelige (artikkel 13(1) bokstav f, 46(1), 46(2) bokstav c GDPR)

Alle selskaper og filialer som er en del av konsernet vårt (heretter kalt "konsernselskaper") og som har forretningssted eller kontor i et tredjeland, kan være mottakere av personopplysninger. En liste over alle konsernselskaper eller mottakere kan fås ved henvendelse til oss.

I henhold til artikkel 46 nr. 1 i personvernforordningen kan en behandlingsansvarlig eller databehandler bare overføre personopplysninger til et tredjeland dersom den behandlingsansvarlige eller databehandleren har gitt egnede garantier, og på betingelse av at det finnes håndhevbare rettigheter og effektive rettsmidler for de registrerte. Passende garantier kan gis uten at det kreves noen spesifikk tillatelse fra en tilsynsmyndighet ved hjelp av standardkontraktsklausuler, jf. artikkel 46 nr. 2 bokstav c i personvernforordningen.

EUs standardkontraktsklausuler eller andre egnede garantier avtales med alle mottakere fra tredjeland før den første overføringen av personopplysninger. På denne måten sikres det at de registrerte er garantert passende garantier, håndhevbare rettigheter og effektive rettsmidler. Alle registrerte kan få en kopi av standardkontraktsbestemmelsene fra oss. Standardkontraktsbestemmelsene er også tilgjengelige i Den europeiske unions tidende.

Artikkel 45(3) i personvernforordningen (GDPR) gir EU-kommisjonen myndighet til å beslutte, ved hjelp av en gjennomføringsrettsakt, at et land utenfor EU sikrer et tilstrekkelig beskyttelsesnivå. Dette innebærer et beskyttelsesnivå for personopplysninger som i hovedsak tilsvarer beskyttelsesnivået i EU. Beslutninger om adekvat beskyttelsesnivå innebærer at personopplysninger kan flyte fritt fra EU (og Norge, Liechtenstein og Island) til et tredjeland uten ytterligere hindringer. Lignende regler gjelder for Storbritannia, Sveits og enkelte andre land.

Der EU-kommisjonen eller myndighetene i et annet land har bestemt at et tredjeland sikrer et tilstrekkelig beskyttelsesnivå, og et gyldig rammeverk er på plass (f.eks. EU-U.S. Data Privacy Framework, Swiss-U.S. Data Privacy Framework, UK Extension to the EU-U.S. Data Privacy Framework), er alle overføringer fra oss til medlemmene av slike rammeverk (f.eks. selvsertifiserte enheter) utelukkende


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

basert på enhetens medlemskap i det respektive rammeverket. Når vi eller en av våre konsernenheter er medlem av et slikt rammeverk, er alle overføringer til oss eller vår konsernenhet utelukkende basert på enhetens medlemskap i et slikt rammeverk.

Alle registrerte kan få en kopi av rammeverkene fra oss. I tillegg er rammeverkene også tilgjengelige i Den europeiske unions tidende eller i publisert juridisk materiale eller på nettsidene til tilsynsmyndigheter eller andre kompetente myndigheter eller institusjoner.

## G. Perioden personopplysningene skal lagres, eller hvis dette ikke er mulig, kriteriene som brukes for å fastsette denne perioden (artikkel 13(2) lit. a GDPR)

Kriteriene som brukes for å bestemme lagringsperioden for personopplysninger, er den respektive lovbestemte oppbevaringsperioden. Etter utløpet av denne perioden slettes de aktuelle opplysningene rutinemessig, så lenge de ikke lenger er nødvendige for å oppfylle kontrakten eller innlede en kontrakt.

Hvis det ikke finnes noen lovbestemt oppbevaringsperiode, er kriteriet den kontraktsfestede eller interne oppbevaringsperioden.

## H. Eksistensen av retten til å be den behandlingsansvarlige om innsyn i og retting eller sletting av personopplysninger eller begrensning av behandling som gjelder den registrerte, eller til å protestere mot behandling, samt retten til dataportabilitet (artikkel 13(2) bokstav b GDPR)

Alle registrerte har følgende rettigheter:

***Rett til tilgang***

Alle registrerte har rett til innsyn i personopplysningene som gjelder dem. Retten til innsyn omfatter alle opplysninger som behandles av oss. Retten kan utøves på en enkel måte og med rimelige mellomrom for å få kjennskap til og verifisere om behandlingen er lovlig (betraktning 63 i GDPR). Denne retten følger av art. 15 I PERSONVERNFORORDNINGEN. Den registrerte kan kontakte oss for å utøve retten til innsyn.

***Rett til retting***

I henhold til artikkel 16 nr. 1 i personvernforordningen har den registrerte rett til å få uriktige personopplysninger om seg selv rettet av den behandlingsansvarlige uten ugrunnet opphold. I henhold til artikkel 16 nr. 2 i personvernforordningen har den registrerte dessuten rett til å få ufullstendige personopplysninger komplettert, blant annet ved å gi en tilleggserklæring, idet det tas hensyn til formålet med behandlingen. Den registrerte kan kontakte oss for å utøve retten til retting.


© All rights reserved by Heiko Maniero.

***Rett til sletting (rett til å bli glemt)***

I tillegg har de registrerte rett til sletting og til å bli glemt i henhold til Art. 17 I PERSONVERNFORORDNINGEN. Denne retten kan også utøves ved å kontakte oss. Vi gjør imidlertid oppmerksom på at denne retten ikke gjelder i den grad behandlingen er nødvendig for å oppfylle en rettslig forpliktelse som selskapet vårt er underlagt, jf. artikkel 17 nr. 3 bokstav b i GDPR. Dette betyr at vi først kan godkjenne en søknad om sletting etter utløpet av den lovbestemte oppbevaringsperioden.

***Rett til begrensning av behandling***

I henhold til artikkel 18 i GDPR har enhver registrert rett til begrensning av behandlingen. Begrensning av behandlingen kan kreves dersom ett av vilkårene i artikkel 18 nr. 1 bokstav a-d i GDPR er oppfylt. Den registrerte kan kontakte oss for å utøve retten til begrensning av behandlingen.

***Rett til å komme med innsigelser***

Videre gir art. 21 i personvernforordningen retten til å protestere. Den registrerte kan kontakte oss for å utøve retten til å protestere.

***Rett til dataportabilitet***

Art. 20 i GDPR gir den registrerte rett til dataportabilitet. I henhold til denne bestemmelsen har den registrerte, på de vilkår som er fastsatt i artikkel 20 nr. 1 bokstav a og b i GDPR, rett til å motta personopplysninger om seg selv som vedkommende har gitt til en behandlingsansvarlig, i et strukturert, alminnelig anvendt og maskinlesbart format, og har rett til å overføre disse opplysningene til en annen behandlingsansvarlig uten hindring fra den behandlingsansvarlige som personopplysningene er gitt til. Den registrerte kan kontakte oss for å utøve retten til dataportabilitet.

## I. Retten til å trekke tilbake samtykket når som helst, uten at det påvirker lovligheten av behandling basert på samtykke før det ble trukket tilbake, dersom behandlingen er basert på GDPR artikkel 6(1) bokstav a eller GDPR artikkel 9(2) bokstav a (GDPR artikkel 13(2) bokstav c).

Hvis behandlingen av personopplysninger er basert på art. 6(1) lit. a GDPR, noe som er tilfellet hvis den registrerte har gitt samtykke til behandling av personopplysninger for ett eller flere spesifikke formål, eller hvis den er basert på artikkel 9(2) lit. a GDPR, som regulerer eksplisitt samtykke til behandling av særlige kategorier av personopplysninger, har den registrerte i henhold til artikkel 7(3) setning 1 GDPR rett til å trekke tilbake sitt samtykke når som helst.

Tilbaketrekking av samtykke skal ikke påvirke lovligheten av behandling basert på samtykke før det ble trukket tilbake, personvernforordningen artikkel 7 nr. 3, 2. punktum. Det skal være like enkelt å trekke tilbake et samtykke som å gi det, art. 7(3) fjerde punktum i GDPR. Tilbaketrekking av samtykke kan derfor alltid skje på samme måte som samtykket ble gitt, eller på en annen måte som den registrerte anser som enklere. I dagens informasjonssamfunn er sannsynligvis den enkleste måten å trekke tilbake et samtykke på en enkel e-post. Hvis den registrerte ønsker å trekke tilbake samtykket han eller hun har gitt oss, er


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

det tilstrekkelig med en enkel e-post til oss. Alternativt kan den registrerte velge en annen måte å kommunisere sin tilbaketrekking av samtykke til oss på.

## J. Rett til å klage til en tilsynsmyndighet (artikkel 13(2) bokstav d, 77(1) GDPR)

Som behandlingsansvarlig er vi forpliktet til å informere den registrerte om retten til å klage til en tilsynsmyndighet, jf. personvernforordningen artikkel 13 nr. 2 bokstav d. Retten til å klage til en tilsynsmyndighet er regulert i artikkel 77(1) i GDPR. I henhold til denne bestemmelsen skal enhver registrert ha rett til å klage til en tilsynsmyndighet, særlig i den medlemsstat der vedkommende har sitt vanlige bosted, sitt arbeidssted eller stedet for det påståtte bruddet, dersom den registrerte mener at behandlingen av personopplysninger om vedkommende er i strid med personvernforordningen, uten at dette berører andre administrative eller rettslige midler. Retten til å klage til en tilsynsmyndighet er i unionsretten begrenset slik at den bare kan utøves overfor én enkelt tilsynsmyndighet (betraktning 141 første setning i GDPR). Hensikten med denne regelen er å unngå at samme registrerte klager to ganger i samme sak. Hvis en registrert ønsker å klage på oss, blir vi derfor bedt om å henvende oss til én enkelt tilsynsmyndighet.

## K. Levering av personopplysninger som lov- eller avtalefestet krav; krav som er nødvendig for å inngå en avtale; den registrertes plikt til å levere personopplysningene; mulige konsekvenser av manglende levering av slike opplysninger (art. 13(2) lit. e GDPR)

Vi presiserer at utlevering av personopplysninger delvis er lovpålagt (f.eks. skatteregler) eller også kan følge av kontraktsbestemmelser (f.eks. informasjon om kontraktspartneren).

Noen ganger kan det være nødvendig for å inngå en avtale at den registrerte gir oss personopplysninger som vi deretter må behandle. Den registrerte er for eksempel forpliktet til å gi oss personopplysninger når selskapet vårt inngår en kontrakt med ham eller henne. Hvis vi ikke leverer personopplysningene, vil konsekvensen være at kontrakten med den registrerte ikke kan inngås.

Før personopplysninger oppgis av den registrerte, må den registrerte kontakte oss. Vi avklarer med den registrerte om utlevering av personopplysningene er påkrevd ved lov eller kontrakt eller er nødvendig for å inngå kontrakten, om det foreligger en forpliktelse til å utlevere personopplysningene og konsekvensene av ikke å utlevere personopplysningene.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

### L. Forekomst av automatiserte avgjørelser, herunder profilering, som nevnt i artikkel 22 nr. 1 og 4 i GDPR, og, i det minste i disse tilfellene, meningsfull informasjon om logikken som er involvert, samt betydningen og de forventede konsekvensene av slik behandling for den registrerte (artikkel 13 nr. 2 bokstav f i GDPR).

Som et ansvarlig selskap bruker vi vanligvis ikke automatiserte avgjørelser eller profilering. Hvis vi i unntakstilfeller bruker automatiserte avgjørelser eller profilering, vil vi informere den registrerte om dette, enten separat eller via et underkapittel i personvernerklæringen vår (på nettstedet vårt). I slike tilfeller gjelder følgende:

Automatiserte avgjørelser - inkludert profilering - kan forekomme hvis (1) dette er nødvendig for å inngå eller oppfylle en avtale mellom den registrerte og oss, eller (2) dette er tillatt i henhold til unionsretten eller medlemsstatenes nasjonale rett som vi er underlagt, og som også fastsetter egnede tiltak for å beskytte den registrertes rettigheter og friheter og berettigede interesser, eller (3) dette er basert på den registrertes uttrykkelige samtykke.

I de tilfellene som er nevnt i artikkel 22 nr. 2 bokstav a og c i personvernforordningen, skal vi iverksette egnede tiltak for å ivareta den registrertes rettigheter og friheter og berettigede interesser. I disse tilfellene har du rett til å be om menneskelig inngripen fra den behandlingsansvarliges side, til å uttrykke ditt synspunkt og til å bestride avgjørelsen.

Betydningsfull informasjon om den involverte logikken, samt betydningen og de forventede konsekvensene av slik behandling for den registrerte, er beskrevet i vår personvernerklæring.

## II. Overholdelse av informasjonskravene når personopplysninger ikke samles inn fra den registrerte (artikkel 14 i GDPR)

### A. Identitet og kontaktinformasjon for den behandlingsansvarlige (artikkel 14(1) bokstav a i GDPR).

Se ovenfor

### B. Kontaktinformasjon til personvernombudet (artikkel 14(1) bokstav b i GDPR)

Se ovenfor


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## C. Formålene med behandlingen av personopplysningene og det rettslige grunnlaget for behandlingen (artikkel 14(1) lit. c GDPR)

Formålet med behandlingen av personopplysninger er å håndtere alle operasjoner som gjelder den behandlingsansvarlige, kunder, potensielle kunder, forretningspartnere eller andre kontraktsmessige eller prekontraktsmessige forhold mellom de nevnte gruppene (i videste forstand) eller juridiske forpliktelser for den behandlingsansvarlige.

Hvis behandlingen av personopplysninger er nødvendig for å oppfylle en kontrakt som den registrerte er part i, for eksempel når behandlingen er nødvendig for å levere varer eller andre tjenester, er behandlingen basert på artikkel 6(1) bokstav b i GDPR. Det samme gjelder for behandling som er nødvendig for å gjennomføre tiltak før kontraktsinngåelse, for eksempel ved forespørsler om våre produkter eller tjenester. Hvis selskapet vårt er underlagt en rettslig forpliktelse som krever behandling av personopplysninger, for eksempel for å oppfylle skatteforpliktelser, er behandlingen basert på art. 6(1) bokstav c i GDPR.

I sjeldne tilfeller kan behandling av personopplysninger være nødvendig for å beskytte den registrertes eller en annen fysisk persons vitale interesser. Dette kan f.eks. være tilfelle hvis en besøkende blir skadet hos oss og navn, alder, helseforsikringsopplysninger eller annen viktig informasjon må gis videre til lege, sykehus eller annen tredjepart. I så fall vil behandlingen være basert på art. 6(1) bokstav d i GDPR.

Når behandlingen er nødvendig for å utføre en oppgave i allmennhetens interesse eller som ledd i offentlig myndighetsutøvelse som den behandlingsansvarlige er pålagt, er det rettslige grunnlaget art. 6(1) bokstav e i GDPR.

Endelig kan behandlingen være basert på artikkel 6(1) lit. f i GDPR. Dette rettslige grunnlaget brukes for behandling som ikke dekkes av noen av de ovennevnte rettslige grunnlagene, hvis behandlingen er nødvendig for å ivareta selskapets eller en tredjeparts berettigede interesser, med mindre den registrertes interesser eller grunnleggende rettigheter og friheter, som krever beskyttelse av personopplysninger, går foran. Slike behandlinger er spesielt tillatt fordi de er spesifikt nevnt av den europeiske lovgiveren. Han mente at en berettiget interesse kan antas å foreligge dersom den registrerte er kunde av den behandlingsansvarlige (GDPR, fortalepunkt 47, 2. setning).

## D. Kategorier av berørte personopplysninger (artikkel 14(1) lit. d GDPR)

Kundedata

Data om potensielle kunder

Data om ansatte

Data om leverandører


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## E. Kategorier av mottakere av personopplysninger (artikkel 14(1) lit. e GDPR)

Offentlige myndigheter

Eksterne organer

Andre eksterne organer

Intern behandling

Konsernintern behandling

Andre organer

En liste over våre databehandlere og datamottakere i tredjeland og, hvis aktuelt, internasjonale organisasjoner, er enten publisert på nettstedet vårt eller kan bestilles gratis fra oss. Ta kontakt med vårt personvernombud for å be om denne listen.

## F. mottakere i et tredjeland og hensiktsmessige eller egnede garantier og hvordan man kan få en kopi av dem eller hvor de er gjort tilgjengelige (artikkel 14(1) lit. f, 46(1), 46(2) lit. c GDPR).

Alle selskaper og filialer som er en del av konsernet vårt (heretter kalt "konsernselskaper") og som har forretningssted eller kontor i et tredjeland, kan være mottakere av personopplysninger. En liste over alle konsernselskapene kan fås ved henvendelse til oss.

I henhold til artikkel 46 nr. 1 i personvernforordningen kan en behandlingsansvarlig eller databehandler bare overføre personopplysninger til et tredjeland dersom den behandlingsansvarlige eller databehandleren har gitt egnede garantier, og på betingelse av at det finnes håndhevbare rettigheter og effektive rettsmidler for de registrerte. Passende garantier kan gis uten at det kreves noen spesifikk tillatelse fra en tilsynsmyndighet ved hjelp av standard personvernbestemmelser, jf. artikkel 46 nr. 2 bokstav c i GDPR.

EUs standardkontraktsklausuler eller andre egnede garantier avtales med alle mottakere fra tredjeland før den første overføringen av personopplysninger. På denne måten sikres det at de registrerte er garantert passende garantier, rettigheter som kan håndheves og effektive rettsmidler for de registrerte. Alle registrerte kan få en kopi av standardkontraktsbestemmelsene fra oss. Standardkontraktsbestemmelsene er også tilgjengelige i Den europeiske unions tidende.

Artikkel 45(3) i personvernforordningen (GDPR) gir EU-kommisjonen myndighet til å beslutte, ved hjelp av en gjennomføringsrettsakt, at et land utenfor EU sikrer et tilstrekkelig beskyttelsesnivå. Dette


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

innebærer et beskyttelsesnivå for personopplysninger som i hovedsak tilsvarer beskyttelsesnivået i EU. Beslutninger om adekvat beskyttelsesnivå innebærer at personopplysninger kan flyte fritt fra EU (og Norge, Liechtenstein og Island) til et tredjeland uten ytterligere hindringer. Lignende regler gjelder for Storbritannia, Sveits og enkelte andre land.

Der EU-kommisjonen eller myndighetene i et annet land har bestemt at et tredjeland sikrer et tilstrekkelig beskyttelsesnivå, og et gyldig rammeverk er på plass (f.eks. EU-U.S. Data Privacy Framework, Swiss-U.S. Data Privacy Framework, UK Extension to the EU-U.S. Data Privacy Framework), er alle overføringer fra oss til medlemmene av slike rammeverk (f.eks. selvsertifiserte enheter) utelukkende basert på enhetens medlemskap i det respektive rammeverket. Når vi eller en av våre konsernenheter er medlem av et slikt rammeverk, er alle overføringer til oss eller vår konsernenhet utelukkende basert på enhetens medlemskap i et slikt rammeverk.

Alle registrerte kan få en kopi av rammeverkene fra oss. I tillegg er rammeverkene også tilgjengelige i Den europeiske unions tidende eller i publisert juridisk materiale eller på nettsidene til tilsynsmyndigheter eller andre kompetente myndigheter eller institusjoner.

## G. Perioden personopplysningene skal lagres, eller hvis dette ikke er mulig, kriteriene som brukes for å fastsette denne perioden (artikkel 14(2) lit. a GDPR)

Kriteriene som brukes for å bestemme lagringsperioden for personopplysninger, er den respektive lovbestemte oppbevaringsperioden. Etter utløpet av denne perioden slettes de aktuelle opplysningene rutinemessig, så lenge de ikke lenger er nødvendige for å oppfylle kontrakten eller innlede en kontrakt.

Hvis det ikke finnes noen lovbestemt oppbevaringsperiode, er kriteriet den kontraktsfestede eller interne oppbevaringsperioden.

## H. Varsel om de berettigede interessene som forfølges av den behandlingsansvarlige eller en tredjepart dersom behandlingen er basert på artikkel 6(1) lit. f GDPR (art. 14(2) lit. b GDPR).

I henhold til artikkel 6 nr. 1 bokstav f i personvernforordningen skal behandling bare være lovlig dersom behandlingen er nødvendig for formål knyttet til berettigede interesser som forfølges av den behandlingsansvarlige eller en tredjepart, med mindre den registrertes interesser eller grunnleggende rettigheter og friheter, som krever vern av personopplysninger, går foran. I henhold til fortalepunkt 47, 2. setning i GDPR kan en berettiget interesse foreligge der det er et relevant og hensiktsmessig forhold mellom den registrerte og den behandlingsansvarlige, f.eks. i situasjoner der den registrerte er kunde hos den behandlingsansvarlige. I alle tilfeller der selskapet vårt behandler personopplysninger basert på artikkel 6(1) bokstav f i GDPR, er vår berettigede interesse å drive virksomheten vår til beste for alle våre ansatte og aksjonærer.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## I. Eksistensen av retten til å be den behandlingsansvarlige om innsyn i og retting eller sletting av personopplysninger eller begrensning av behandling som gjelder den registrerte, og til å protestere mot behandling samt retten til dataportabilitet (artikkel 14(2) bokstav c i GDPR)

Alle registrerte har følgende rettigheter:

***Rett til tilgang***

Alle registrerte har rett til innsyn i personopplysningene som gjelder dem. Retten til innsyn omfatter alle opplysninger som behandles av oss. Retten kan utøves på en enkel måte og med rimelige mellomrom for å få kjennskap til og verifisere om behandlingen er lovlig (betraktning 63 i GDPR). Denne retten følger av art. 15 I PERSONVERNFORORDNINGEN. Den registrerte kan kontakte oss for å utøve retten til innsyn.

***Rett til retting***

I henhold til artikkel 16 nr. 1 i personvernforordningen har den registrerte rett til å få uriktige personopplysninger om seg selv rettet av den behandlingsansvarlige uten ugrunnet opphold. I henhold til artikkel 16 nr. 2 i personvernforordningen har den registrerte dessuten rett til å få ufullstendige personopplysninger komplettert, blant annet ved å gi en tilleggserklæring, idet det tas hensyn til formålet med behandlingen. Den registrerte kan kontakte oss for å utøve retten til retting.

***Rett til sletting (rett til å bli glemt)***

I tillegg har de registrerte rett til sletting og til å bli glemt i henhold til Art. 17 I PERSONVERNFORORDNINGEN. Denne retten kan også utøves ved å kontakte oss. Vi gjør imidlertid oppmerksom på at denne retten ikke gjelder i den grad behandlingen er nødvendig for å oppfylle en rettslig forpliktelse som selskapet vårt er underlagt, jf. artikkel 17 nr. 3 bokstav b i GDPR. Dette betyr at vi først kan godkjenne en søknad om sletting etter utløpet av den lovbestemte oppbevaringsperioden.

***Rett til begrensning av behandling***

I henhold til artikkel 18 i GDPR har enhver registrert rett til begrensning av behandlingen. Begrensning av behandlingen kan kreves dersom ett av vilkårene i artikkel 18 nr. 1 bokstav a-d i GDPR er oppfylt. Den registrerte kan kontakte oss for å utøve retten til begrensning av behandlingen.

***Rett til å komme med innsigelser***

Videre gir art. 21 i personvernforordningen retten til å protestere. Den registrerte kan kontakte oss for å utøve retten til å protestere.

***Rett til dataportabilitet***

Art. 20 i GDPR gir den registrerte rett til dataportabilitet. I henhold til denne bestemmelsen har den registrerte, på de vilkår som er fastsatt i artikkel 20 nr. 1 bokstav a og b i GDPR, rett til å motta personopplysninger om seg selv som vedkommende har gitt til en behandlingsansvarlig, i et strukturert,


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

alminnelig anvendt og maskinlesbart format, og har rett til å overføre disse opplysningene til en annen behandlingsansvarlig uten hindring fra den behandlingsansvarlige som personopplysningene er gitt til. Den registrerte kan kontakte oss for å utøve retten til dataportabilitet.

## J. Retten til å trekke tilbake samtykket når som helst, uten at det påvirker lovligheten av behandling basert på samtykke før tilbaketrekking, når behandlingen er basert på artikkel 6(1) lit. a eller artikkel 9(2) lit. a GDPR (art. 14(2) lit. d GDPR).

Hvis behandlingen av personopplysninger er basert på art. 6(1) lit. a GDPR, noe som er tilfelle hvis den registrerte har gitt samtykke til behandling av personopplysninger for ett eller flere spesifikke formål, eller hvis den er basert på artikkel 9(2) lit. a GDPR, som regulerer eksplisitt samtykke til behandling av særlige kategorier av personopplysninger, har den registrerte i henhold til artikkel 7(3) setning 1 GDPR rett til å trekke tilbake sitt samtykke når som helst.

Tilbaketrekking av samtykke skal ikke påvirke lovligheten av behandling basert på samtykke før det ble trukket tilbake, personvernforordningen artikkel 7 nr. 3 annet punktum. Det skal være like enkelt å trekke tilbake som å gi samtykke, art. 7(3) fjerde punktum i GDPR. Tilbaketrekking av samtykke kan derfor alltid skje på samme måte som samtykket ble gitt, eller på en annen måte som den registrerte anser som enklere. I dagens informasjonssamfunn er sannsynligvis den enkleste måten å trekke tilbake et samtykke på en enkel e-post. Hvis den registrerte ønsker å trekke tilbake sitt samtykke til oss, er det tilstrekkelig med en enkel e-post til oss. Alternativt kan den registrerte velge en annen måte å kommunisere sin tilbaketrekking av samtykke til oss på.

## K. Rett til å klage til en tilsynsmyndighet (artikkel 14(2) lit. e, 77(1) GDPR)

Som behandlingsansvarlig er vi forpliktet til å informere den registrerte om retten til å klage til en tilsynsmyndighet, jf. personvernforordningen artikkel 14 nr. 2 bokstav e. Retten til å klage til en tilsynsmyndighet er regulert i artikkel 77(1) i GDPR. I henhold til denne bestemmelsen skal enhver registrert ha rett til å klage til en tilsynsmyndighet, særlig i den medlemsstat der vedkommende har sitt vanlige bosted, sitt arbeidssted eller stedet for det påståtte bruddet, dersom den registrerte mener at behandlingen av personopplysninger om vedkommende er i strid med personvernforordningen, uten at dette berører andre administrative eller rettslige midler. Retten til å klage til en tilsynsmyndighet er begrenset i unionsretten slik at den bare kan utøves overfor én enkelt tilsynsmyndighet (betraktning 141 første setning i GDPR). Hensikten med denne regelen er å unngå at samme registrerte klager to ganger i samme sak. Hvis en registrert ønsker å klage på oss, ber vi derfor om at vedkommende kun kontakter én tilsynsmyndighet.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## L. Hvor personopplysningene stammer fra, og eventuelt om de kommer fra offentlig tilgjengelige kilder (artikkel 14(2) lit. f GDPR)

I prinsippet innhentes personopplysninger direkte fra den registrerte eller i samarbeid med en myndighet (f.eks. innhenting av opplysninger fra et offentlig register). Andre opplysninger om de registrerte **stammer** fra overføringer fra konsernselskaper. I forbindelse med denne generelle informasjonen er det enten umulig å oppgi de nøyaktige kildene som personopplysningene stammer fra, eller det ville innebære en uforholdsmessig stor innsats i henhold til art. 14(5) lit. b GDPR. 14(5) bokstav b i GDPR. I prinsippet samler vi ikke inn personopplysninger fra offentlig tilgjengelige kilder.

Enhver registrert kan når som helst kontakte oss for å få mer detaljert informasjon om de nøyaktige kildene til personopplysningene om ham eller henne. Hvis det ikke er mulig å opplyse den registrerte om hvor personopplysningene stammer fra fordi det er brukt ulike kilder, bør det gis generell informasjon (betraktning 61, setning 4 i GDPR).

## M. Forekomst av automatiserte avgjørelser, herunder profilering, som nevnt i artikkel 22 nr. 1 og 4 i GDPR, og, i det minste i disse tilfellene, meningsfull informasjon om den involverte logikken, samt betydningen og de forventede konsekvensene av slik behandling for den registrerte (artikkel 14 nr. 2 bokstav g i GDPR).

Som et ansvarlig selskap bruker vi vanligvis ikke automatiserte avgjørelser eller profilering. Hvis vi i unntakstilfeller bruker automatiserte avgjørelser eller profilering, vil vi informere den registrerte om dette, enten separat eller via et underkapittel i personvernerklæringen vår (på nettstedet vårt). I slike tilfeller gjelder følgende:

Automatiserte avgjørelser - herunder profilering - kan forekomme hvis (1) dette er nødvendig for å inngå eller oppfylle en avtale mellom den registrerte og oss, eller (2) dette er tillatt i henhold til unionsretten eller medlemsstatenes nasjonale rett som vi er underlagt, og som også fastsetter egnede tiltak for å beskytte den registrertes rettigheter og friheter og berettigede interesser, eller (3) dette er basert på den registrertes uttrykkelige samtykke.

I de tilfellene som er nevnt i artikkel 22 nr. 2 bokstav a og c i personvernforordningen, skal vi iverksette egnede tiltak for å ivareta den registrertes rettigheter og friheter og berettigede interesser. I slike tilfeller har du rett til å be om menneskelig inngripen fra den behandlingsansvarliges side, til å uttrykke ditt synspunkt og til å bestride avgjørelsen.

Betydningsfull informasjon om den involverte logikken, samt betydningen og de forventede konsekvensene av slik behandling for den registrerte, er beskrevet i vår personvernerklæring.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## III. EU-U.S. Data Privacy Framework (EU-U.S. DPF), UK Extension to the EU-U.S. DPF, Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF)

Hvis vår organisasjon er et sertifisert medlem av EU-U.S. Data Privacy Framework (EU-U.S. DPF) og/eller UK Extension to the EU-U.S. DPF og/eller Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF), gjelder følgende:

Vi overholder EU-U.S. Data Privacy Framework (EU-U.S. DPF) og UK Extension to the EU-U.S. DPF samt Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF), som fastsatt av U.S. Department of Commerce. Vår virksomhet har bekreftet overfor det amerikanske handelsdepartementet at den overholder EU-U.S. Data Privacy Framework Principles (EU-U.S. DPF Principles) når det gjelder behandling av personopplysninger som den mottar fra Den europeiske union og Storbritannia i henhold til EU-U.S. DPF og UK Extension to the EU-U.S. DPF. Vår virksomhet har bekreftet overfor det amerikanske handelsdepartementet at den overholder Swiss-U.S. Data Privacy Framework Principles (Swiss-U.S. DPF Principles) når det gjelder behandling av personopplysninger som den mottar fra Sveits i henhold til Swiss-U.S. DPF. Ved motstrid mellom bestemmelsene i vår personvernerklæring og EU-U.S. DPF Principles og/eller Swiss-U.S. DPF Principles, vil Principles være avgjørende.

For å lære mer om Data Privacy Framework (DPF) programmet og for å se vår sertifisering, vennligst besøk https://www.dataprivacyframework.gov/.

De andre amerikanske enhetene eller datterselskapene i vår virksomhet som også overholder EU-U.S. DPF Principals, inkludert UK Extension to the EU-U.S. DPF og Swiss-U.S. DPF Principals, hvis noen, er nevnt i vår personvernerklæring.

I samsvar med EU-U.S. DPF og UK Extension to the EU-U.S. DPF samt Swiss-U.S. DPF, forplikter vår virksomhet seg til å samarbeide med det panelet som er opprettet av EUs databeskyttelsesmyndigheter og det britiske Information Commissioner's Office (ICO) samt den sveitsiske føderale databeskyttelses- og informasjonskommissæren (EDÖB), og følge deres råd angående uløste klager om vår håndtering av personopplysninger vi mottar i henhold til EU-U.S. DPF og UK Extension to the EU-U.S. DPF og Swiss-U.S. DPF.

Vi informerer de berørte personene om de relevante europeiske databeskyttelsesmyndighetene som er ansvarlige for behandling av klager om vår organisasjons håndtering av personopplysninger, øverst i dette gjennomsiktighetsdokumentet, og at vi tilbyr de berørte personene en passende og gratis rettsmiddel.

Vi informerer alle berørte personer om at vår virksomhet er underlagt Federal Trade Commission's (FTC) etterforsknings- og håndhevingsmyndighet.

Berørte personer har under visse betingelser muligheten til å benytte bindende voldgift. Vår organisasjon er forpliktet til å avgjøre krav og overholde betingelsene i vedlegg I til DPF-Principals, forutsatt at den


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

berørte personen har anmodet om bindende voldgift ved å varsle vår organisasjon og følge prosedyrene og betingelsene i vedlegg I til Principals.

Vi informerer herved alle berørte personer om vårt selskaps ansvar i tilfelle overføring av personopplysninger til tredjeparter.

For spørsmål fra berørte personer eller datatilsynsmyndigheter har vi utpekt de lokale representantene som er nevnt ovenfor i dette gjennomsiktighetsdokumentet.

Vi gir deg muligheten til å velge (Opt-out) om dine personopplysninger (i) skal overføres til tredjeparter eller (ii) brukes til et formål som er vesentlig forskjellig fra det/de formålet/formålene de opprinnelig ble samlet inn for eller senere godkjent av deg. Den tydelige, godt synlige og lett tilgjengelige mekanismen for å utøve ditt valg er å kontakte vår personvernansvarlige (DSB) via e-post. Du har ikke muligheten til å velge, og vi er heller ikke forpliktet til det, hvis opplysningene overføres til en tredjepart som fungerer som agent eller databehandler på våre vegne og i henhold til våre instruksjoner. Vi inngår imidlertid alltid en avtale med en slik agent eller databehandler.

For sensitive data (dvs. personopplysninger som inneholder informasjon om helsetilstand, rase eller etnisk opprinnelse, politiske meninger, religiøse eller filosofiske overbevisninger, medlemskap i fagforening eller opplysninger om den aktuelle personens seksualliv) innhenter vi ditt uttrykkelige samtykke (Opt-in) når disse opplysningene (i) overføres til tredjeparter eller (ii) brukes til et annet formål enn det de opprinnelig ble samlet inn for eller som du senere har gitt ditt samtykke til ved å velge Opt-in. Videre behandler vi alle personopplysninger vi mottar fra tredjeparter som sensitive hvis tredjeparten identifiserer og behandler dem som sensitive.

Vi informerer deg herved om kravet om å avsløre personopplysninger som svar på lovlige forespørsler fra myndigheter, inkludert for å oppfylle krav til nasjonal sikkerhet eller rettshåndhevelse.

Ved overføring av personopplysninger til en tredjepart som fungerer som behandlingsansvarlig, overholder vi Principals for varsling og valg. I tillegg inngår vi en avtale med tredjeparten som er ansvarlig for behandlingen, som fastsetter at disse opplysningene kun skal behandles for begrensede og spesifiserte formål i samsvar med ditt samtykke og at mottakeren skal gi samme beskyttelsesnivå som DPF Principles og varsle oss hvis de fastslår at de ikke lenger kan oppfylle denne forpliktelsen. Avtalen fastsetter at tredjeparten som er ansvarlig, skal stoppe behandlingen eller treffe andre passende og rimelige tiltak for å rette opp situasjonen hvis en slik fastsettelse gjøres.

Ved overføring av personopplysninger til en tredjepart som fungerer som agent eller databehandler, (i) overfører vi disse opplysningene kun for begrensede og spesifiserte formål; (ii) vi sørger for at agenten eller databehandleren er forpliktet til å tilby minst samme nivå av databeskyttelse som DPF-Principals krever; (iii) vi tar passende og rimelige tiltak for å sikre at agenten eller databehandleren faktisk behandler de overførte personopplysningene på en måte som er i samsvar med våre forpliktelser i henhold til DPF-Principals; (iv) vi krever at agenten eller databehandleren varsler vår organisasjon hvis de fastslår at de ikke lenger kan oppfylle forpliktelsen til å gi samme beskyttelsesnivå som DPF-Principals krever; (v) etter


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

en slik varsling, også i henhold til (iv), tar vi passende og rimelige tiltak for å stoppe uautorisert behandling og rette opp situasjonen; og (vi) vi gir DPF Department på forespørsel et sammendrag eller et representativt eksempel på de relevante databeskyttelsesbestemmelsene fra vår avtale med denne agenten.

I samsvar med EU-U.S. DPF og/eller UK Extension to the EU-U.S. DPF og/eller Swiss-U.S. DPF forplikter vår organisasjon seg til å samarbeide med det panelet som er opprettet av EUs databeskyttelsesmyndigheter og det britiske Information Commissioner's Office (ICO) eller den sveitsiske føderale databeskyttelses- og informasjonskommissæren (EDÖB) og følge deres råd angående uløste klager om vår håndtering av personopplysninger vi mottar i forbindelse med arbeidsforhold i henhold til EU-U.S. DPF og UK Extension to the EU-U.S. DPF og Swiss-U.S. DPF.

Alle registrerte som midlertidig oppholder seg i Den europeiske union (EU), Det europeiske økonomiske samarbeidsområdet (EØS) eller Storbritannia, eller som har sin bopel eller sitt vanlige oppholdssted der, har rett til de rettighetene og de registrerte rettighetene som er publisert i vårt åpenhetsdokument, og som også følger av artikkel 15 til 22 i GDPR, inkludert retten til innsyn i personopplysninger. Vi har gjort denne informasjonen tilgjengelig på alle EU- og EØS-språk. Den engelskspråklige versjonen gjelder for Storbritannia.

Alle registrerte som er midlertidig bosatt i Sveits eller har bosted eller vanlig oppholdssted der, har rett til de rettighetene som følger av den sveitsiske databeskyttelsesloven (DPA) og den sveitsiske databeskyttelsesforordningen (DPR), som er publisert i vårt åpenhetsdokument, inkludert retten til innsyn i personopplysninger. Vi har gitt denne informasjonen på de tre offisielle språkene i Sveits (tysk, italiensk og fransk).


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

# NORWEGIAN: Informasjon om behandling av personopplysninger for ansatte og søkere (artikkel 13 og 14 i GDPR)

Kjære frue eller herre,

Personopplysninger om ansatte og søkere fortjener spesiell beskyttelse. Vårt mål er å holde et høyt personvernnivå. Derfor utvikler vi kontinuerlig våre konsepter for databeskyttelse og datasikkerhet.

Vi overholder selvfølgelig de lovbestemte bestemmelsene om personvern. I henhold til artikkel 13, 14 i personvernforordningen skal behandlingsansvarlige oppfylle spesifikke informasjonskrav ved behandling av personopplysninger. Dette dokumentet oppfyller disse forpliktelsene.

Terminologien innen juridisk regulering er komplisert. Dessverre var det ikke mulig å unngå bruk av juridiske termer i forbindelse med utarbeidelsen av dette dokumentet. Vi gjør derfor oppmerksom på at du alltid er velkommen til å kontakte oss hvis du har spørsmål om dette dokumentet, termer eller formuleringer.

## I. Overholdelse av informasjonskravene når personopplysninger samles inn fra den registrerte (artikkel 13 i GDPR)

### A. Identitet og kontaktinformasjon til den behandlingsansvarlige (artikkel 13(1) lit. a GDPR)

Se ovenfor

### B. Kontaktinformasjon til personvernombudet (artikkel 13(1) lit. b GDPR)

Se ovenfor

### C. Formålene med behandlingen av personopplysningene og det rettslige grunnlaget for behandlingen (artikkel 13(1) lit. c GDPR)

Når det gjelder opplysninger om søkere, er formålet med databehandlingen å undersøke søknaden i løpet av rekrutteringsprosessen. Til dette formålet behandler vi alle opplysningene du har oppgitt. På grunnlag av opplysningene du har oppgitt i løpet av rekrutteringsprosessen, kontrollerer vi om du blir innkalt til et jobbintervju (en del av utvelgelsesprosessen). Når det gjelder generelt egnede kandidater,


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

særlig i forbindelse med jobbintervjuet, behandler vi visse andre personopplysninger som du har oppgitt, og som er avgjørende for vår utvelgelsesbeslutning. Hvis du blir ansatt hos oss, vil søkerdataene automatisk bli endret til ansattdata. Som en del av rekrutteringsprosessen vil vi behandle andre personopplysninger om deg som vi ber deg om, og som er nødvendige for å inngå eller oppfylle kontrakten din (for eksempel personnummer eller skattenummer). Når det gjelder opplysninger om ansatte, er formålet med databehandlingen å oppfylle arbeidsavtalen eller overholde andre lovbestemmelser som gjelder for ansettelsesforholdet (f.eks. skattelovgivningen), samt å bruke personopplysningene dine til å oppfylle arbeidsavtalen som er inngått med deg (f.eks. publisering av navnet ditt og kontaktinformasjonen din i selskapet eller til kunder). Opplysninger om ansatte lagres etter at arbeidsforholdet er avsluttet for å overholde lovbestemte oppbevaringsperioder.

Det rettslige grunnlaget for databehandlingen er artikkel 6(1) bokstav b i GDPR, artikkel 9(2) bokstav b og h i GDPR, artikkel 88(1) i GDPR og nasjonal lovgivning, som for Tysklands del § 26 BDSG (Federal Data Protection Act).

## D. Kategorier av mottakere av personopplysninger (artikkel 13(1) lit. e GDPR)

Offentlige myndigheter

Eksterne organer

Andre eksterne organer

Intern behandling

Konsernintern behandling

Andre organer

En liste over våre databehandlere og datamottakere i tredjeland og, hvis aktuelt, internasjonale organisasjoner, er enten publisert på nettstedet vårt eller kan bestilles gratis fra oss. Ta kontakt med vårt personvernombud for å be om denne listen.

## E. Mottakere i et tredjeland og hensiktsmessige eller egnede garantier og hvordan man kan få en kopi av dem eller hvor de er gjort tilgjengelige (artikkel 13(1) bokstav f, 46(1), 46(2) bokstav c GDPR).

Alle selskaper og filialer som er en del av konsernet vårt (heretter kalt "konsernselskaper") og som har forretningssted eller kontor i et tredjeland, kan være mottakere av personopplysninger. En liste over alle konsernselskaper eller mottakere kan fås ved henvendelse til oss.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

I henhold til artikkel 46 nr. 1 i personvernforordningen kan en behandlingsansvarlig eller databehandler bare overføre personopplysninger til et tredjeland dersom den behandlingsansvarlige eller databehandleren har gitt egnede garantier, og på betingelse av at det finnes håndhevbare rettigheter og effektive rettsmidler for de registrerte. Passende garantier kan gis uten at det kreves noen spesifikk tillatelse fra en tilsynsmyndighet ved hjelp av standardkontraktsklausuler, jf. artikkel 46 nr. 2 bokstav c i personvernforordningen.

EUs standardkontraktsklausuler eller andre egnede garantier avtales med alle mottakere fra tredjeland før den første overføringen av personopplysninger. På denne måten sikres det at de registrerte er garantert passende garantier, håndhevbare rettigheter og effektive rettsmidler. Alle registrerte kan få en kopi av standardkontraktsbestemmelsene fra oss. Standardkontraktsbestemmelsene er også tilgjengelige i Den europeiske unions tidende.

Artikkel 45(3) i personvernforordningen (GDPR) gir EU-kommisjonen myndighet til å beslutte, ved hjelp av en gjennomføringsrettsakt, at et land utenfor EU sikrer et tilstrekkelig beskyttelsesnivå. Dette innebærer et beskyttelsesnivå for personopplysninger som i hovedsak tilsvarer beskyttelsesnivået i EU. Beslutninger om adekvat beskyttelsesnivå innebærer at personopplysninger kan flyte fritt fra EU (og Norge, Liechtenstein og Island) til et tredjeland uten ytterligere hindringer. Lignende regler gjelder for Storbritannia, Sveits og enkelte andre land.

Der EU-kommisjonen eller myndighetene i et annet land har bestemt at et tredjeland sikrer et tilstrekkelig beskyttelsesnivå, og et gyldig rammeverk er på plass (f.eks. EU-U.S. Data Privacy Framework, Swiss-U.S. Data Privacy Framework, UK Extension to the EU-U.S. Data Privacy Framework), er alle overføringer fra oss til medlemmene av slike rammeverk (f.eks. selvsertifiserte enheter) utelukkende basert på enhetens medlemskap i det respektive rammeverket. Når vi eller en av våre konsernenheter er medlem av et slikt rammeverk, er alle overføringer til oss eller vår konsernenhet utelukkende basert på enhetens medlemskap i et slikt rammeverk.

Alle registrerte kan få en kopi av rammeverkene fra oss. I tillegg er rammeverkene også tilgjengelige i Den europeiske unions tidende eller i publisert juridisk materiale eller på nettsidene til tilsynsmyndigheter eller andre kompetente myndigheter eller institusjoner.

## F. Perioden personopplysningene skal lagres, eller hvis dette ikke er mulig, kriteriene som brukes for å fastsette denne perioden (artikkel 13(2) lit. a GDPR)

Oppbevaringsperioden for personopplysninger om søkere er 6 måneder. For opplysninger om ansatte gjelder den respektive lovbestemte oppbevaringsperioden. Etter utløpet av denne perioden slettes de aktuelle opplysningene rutinemessig så lenge de ikke lenger er nødvendige for å oppfylle kontrakten eller inngå en kontrakt.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## G. Eksistensen av retten til å be den behandlingsansvarlige om innsyn i og retting eller sletting av personopplysninger eller begrensning av behandling som gjelder den registrerte, eller til å protestere mot behandling, samt retten til dataportabilitet (artikkel 13(2) bokstav b GDPR)

Alle registrerte har følgende rettigheter:

***Rett til tilgang***

Alle registrerte har rett til innsyn i personopplysningene som gjelder dem. Retten til innsyn omfatter alle opplysninger som behandles av oss. Retten kan utøves på en enkel måte og med rimelige mellomrom for å få kjennskap til og verifisere om behandlingen er lovlig (betraktning 63 i GDPR). Denne retten følger av art. 15 I PERSONVERNFORORDNINGEN. Den registrerte kan kontakte oss for å utøve retten til innsyn.

***Rett til retting***

I henhold til artikkel 16 nr. 1 i personvernforordningen har den registrerte rett til å få uriktige personopplysninger om seg selv rettet av den behandlingsansvarlige uten ugrunnet opphold. I henhold til artikkel 16 nr. 2 i personvernforordningen har den registrerte dessuten rett til å få ufullstendige personopplysninger komplettert, blant annet ved å gi en tilleggserklæring, idet det tas hensyn til formålet med behandlingen. Den registrerte kan kontakte oss for å utøve retten til retting.

***Rett til sletting (rett til å bli glemt)***

I tillegg har de registrerte rett til sletting og til å bli glemt i henhold til Art. 17 I PERSONVERNFORORDNINGEN. Denne retten kan også utøves ved å kontakte oss. Vi gjør imidlertid oppmerksom på at denne retten ikke gjelder i den grad behandlingen er nødvendig for å oppfylle en rettslig forpliktelse som selskapet vårt er underlagt, jf. artikkel 17 nr. 3 bokstav b i GDPR. Dette betyr at vi først kan godkjenne en søknad om sletting etter utløpet av den lovbestemte oppbevaringsperioden.

***Rett til begrensning av behandling***

I henhold til artikkel 18 i GDPR har enhver registrert rett til begrensning av behandlingen. Begrensning av behandlingen kan kreves dersom ett av vilkårene i artikkel 18 nr. 1 bokstav a-d i GDPR er oppfylt. Den registrerte kan kontakte oss for å utøve retten til begrensning av behandlingen.

***Rett til å komme med innsigelser***

Videre gir art. 21 i personvernforordningen retten til å protestere. Den registrerte kan kontakte oss for å utøve retten til å protestere.

***Rett til dataportabilitet***

Art. 20 i GDPR gir den registrerte rett til dataportabilitet. I henhold til denne bestemmelsen har den registrerte, på de vilkår som er fastsatt i artikkel 20 nr. 1 bokstav a og b i GDPR, rett til å motta personopplysninger om seg selv som vedkommende har gitt til en behandlingsansvarlig, i et strukturert, alminnelig anvendt og maskinlesbart format, og har rett til å overføre disse opplysningene til en annen


© All rights reserved by Heiko Maniero.

behandlingsansvarlig uten hindring fra den behandlingsansvarlige som personopplysningene er gitt til. Den registrerte kan kontakte oss for å utøve retten til dataportabilitet.

## H. Retten til å trekke tilbake samtykket når som helst, uten at det påvirker lovligheten av behandling basert på samtykke før tilbaketrekking, når behandlingen er basert på artikkel 6(1) lit. a GDPR eller artikkel 9(2) lit. a GDPR (artikkel 13(2) lit. c GDPR).

Hvis behandlingen av personopplysninger er basert på art. 6(1) lit. a GDPR, noe som er tilfellet hvis den registrerte har gitt samtykke til behandling av personopplysninger for ett eller flere spesifikke formål, eller hvis den er basert på artikkel 9(2) lit. a GDPR, som regulerer uttrykkelig samtykke til behandling av særlige kategorier av personopplysninger, har den registrerte i henhold til artikkel 7(3) setning 1 GDPR rett til å trekke tilbake sitt samtykke når som helst.

Tilbaketrekking av samtykke skal ikke påvirke lovligheten av behandling basert på samtykke før det ble trukket tilbake, personvernforordningen artikkel 7 nr. 3 annet punktum. Det skal være like enkelt å trekke tilbake som å gi samtykke, art. 7(3) fjerde punktum i GDPR. Tilbaketrekking av samtykke kan derfor alltid skje på samme måte som samtykket ble gitt, eller på en annen måte som den registrerte anser som enklere. I dagens informasjonssamfunn er sannsynligvis den enkleste måten å trekke tilbake et samtykke på en enkel e-post. Hvis den registrerte ønsker å trekke tilbake samtykket han eller hun har gitt oss, er det tilstrekkelig med en enkel e-post til oss. Alternativt kan den registrerte velge en annen måte å kommunisere sin tilbaketrekking av samtykke til oss på.

## I. Rett til å klage til en tilsynsmyndighet (artikkel 13(2) bokstav d, 77(1) GDPR)

Som behandlingsansvarlig er vi forpliktet til å informere den registrerte om retten til å klage til en tilsynsmyndighet, jf. personvernforordningen artikkel 13 nr. 2 bokstav d. Retten til å klage til en tilsynsmyndighet er regulert i artikkel 77(1) i GDPR. I henhold til denne bestemmelsen skal enhver registrert, uten at det berører andre administrative eller rettslige midler, ha rett til å klage til en tilsynsmyndighet, særlig i den medlemsstaten der vedkommende har sitt vanlige bosted, sitt arbeidssted eller stedet for det påståtte bruddet, dersom den registrerte mener at behandlingen av personopplysninger om vedkommende er i strid med personvernforordningen. Retten til å klage til en tilsynsmyndighet er i unionsretten begrenset slik at den bare kan utøves overfor én enkelt tilsynsmyndighet (betraktning 141 første setning i GDPR). Hensikten med denne regelen er å unngå at samme registrerte klager to ganger i samme sak. Hvis en registrert ønsker å klage på oss, blir vi derfor bedt om å henvende oss til én enkelt tilsynsmyndighet.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## J. Levering av personopplysninger som et lov- eller avtalefestet krav; krav som er nødvendig for å inngå en avtale; den registrertes plikt til å levere personopplysningene; mulige konsekvenser av å unnlate å levere slike opplysninger (art. 13(2) lit. e GDPR)

Vi presiserer at utlevering av personopplysninger delvis er lovpålagt (f.eks. skatteregler) eller også kan følge av kontraktsbestemmelser (f.eks. informasjon om kontraktspartneren).

Noen ganger kan det være nødvendig for å inngå en avtale at den registrerte gir oss personopplysninger som vi deretter må behandle. Den registrerte er for eksempel forpliktet til å gi oss personopplysninger når selskapet vårt inngår en kontrakt med ham eller henne. Hvis vi ikke leverer personopplysningene, vil konsekvensen være at kontrakten med den registrerte ikke kan inngås.

Før personopplysninger oppgis av den registrerte, må den registrerte kontakte oss. Vi avklarer med den registrerte om utlevering av personopplysningene er påkrevd ved lov eller kontrakt eller er nødvendig for å inngå kontrakten, om det foreligger en forpliktelse til å utlevere personopplysningene og konsekvensene av ikke å utlevere personopplysningene.

## K. Eksistensen av automatiserte avgjørelser, herunder profilering, som nevnt i artikkel 22 nr. 1 og 4 i GDPR, og, i det minste i disse tilfellene, meningsfull informasjon om logikken som er involvert, samt betydningen og de forventede konsekvensene av slik behandling for den registrerte (artikkel 13 nr. 2 bokstav f i GDPR).

Som et ansvarlig selskap bruker vi vanligvis ikke automatiserte avgjørelser eller profilering. Hvis vi i unntakstilfeller bruker automatiserte avgjørelser eller profilering, vil vi informere den registrerte om dette, enten separat eller via et underavsnitt i personvernerklæringen vår (på nettstedet vårt). I slike tilfeller gjelder følgende:

Automatiserte avgjørelser - herunder profilering - kan forekomme hvis (1) dette er nødvendig for å inngå eller oppfylle en avtale mellom den registrerte og oss, eller (2) dette er tillatt i henhold til unionsretten eller medlemsstatenes nasjonale rett som vi er underlagt, og som også fastsetter egnede tiltak for å sikre den registrertes rettigheter og friheter og berettigede interesser, eller (3) dette er basert på den registrertes uttrykkelige samtykke.

I de tilfellene som er nevnt i artikkel 22 nr. 2 bokstav a og c i personvernforordningen, skal vi iverksette egnede tiltak for å ivareta den registrertes rettigheter og friheter og berettigede interesser. I disse tilfellene har du rett til å be om menneskelig inngripen fra den behandlingsansvarliges side, til å uttrykke ditt synspunkt og til å bestride avgjørelsen.

Betydningsfull informasjon om den involverte logikken, samt betydningen og de forventede konsekvensene av slik behandling for den registrerte, er beskrevet i vår personvernerklæring.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## II. Overholdelse av informasjonskravene når personopplysninger ikke samles inn fra den registrerte (artikkel 14 i GDPR)

### A. Identitet og kontaktinformasjon for den behandlingsansvarlige (artikkel 14(1) bokstav a i GDPR).

Se ovenfor

### B. Kontaktinformasjon til personvernombudet (artikkel 14(1) bokstav b i GDPR)

Se ovenfor

### C. Formålene med behandlingen av personopplysningene og det rettslige grunnlaget for behandlingen (artikkel 14(1) bokstav c i GDPR)

Når det gjelder opplysninger om søkere som ikke er innhentet fra den registrerte, er formålet med databehandlingen å undersøke søknaden i løpet av rekrutteringsprosessen. For dette formålet kan vi behandle opplysninger som ikke er innhentet fra deg. Basert på opplysningene som behandles under rekrutteringsprosessen, vil vi sjekke om du blir innkalt til et jobbintervju (en del av utvelgelsesprosessen). Hvis du blir ansatt hos oss, konverteres søkerdataene automatisk til ansattdata. Når det gjelder opplysninger om ansatte, er formålet med databehandlingen å oppfylle arbeidsavtalen eller overholde andre lovbestemmelser som gjelder for ansettelsesforholdet. Opplysninger om ansatte lagres etter at ansettelsesforholdet er avsluttet for å oppfylle lovbestemte oppbevaringsperioder.

Det rettslige grunnlaget for databehandlingen er artikkel 6(1) bokstav b og f i GDPR, artikkel 9(2) bokstav b og h i GDPR, artikkel 88(1) i GDPR og nasjonal lovgivning, for eksempel § 26 i BDSG (Bundesdatenschutzgesetz) i Tyskland.

### D. Kategorier av berørte personopplysninger (artikkel 14(1) lit. d GDPR)

Søkerens opplysninger

Data om ansatte

### E. Kategorier av mottakere av personopplysninger (artikkel 14(1) lit. e GDPR)


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

Offentlige myndigheter

Eksterne organer

Andre eksterne organer

Intern behandling

Konsernintern behandling

Andre organer

En liste over våre databehandlere og datamottakere i tredjeland og, hvis aktuelt, internasjonale organisasjoner, er enten publisert på nettstedet vårt eller kan bestilles gratis fra oss. Ta kontakt med vårt personvernombud for å be om denne listen.

## F. mottakere i et tredjeland og hensiktsmessige eller egnede garantier og hvordan man kan få en kopi av dem eller hvor de er gjort tilgjengelige (artikkel 14(1) lit. f, 46(1), 46(2) lit. c GDPR).

Alle selskaper og filialer som er en del av konsernet vårt (heretter kalt "konsernselskaper") og som har forretningssted eller kontor i et tredjeland, kan være mottakere av personopplysninger. En liste over alle konsernselskaper eller mottakere kan fås ved henvendelse til oss.

I henhold til artikkel 46 nr. 1 i personvernforordningen kan en behandlingsansvarlig eller databehandler bare overføre personopplysninger til et tredjeland dersom den behandlingsansvarlige eller databehandleren har gitt egnede garantier, og på betingelse av at det finnes håndhevbare rettigheter og effektive rettsmidler for de registrerte. Passende garantier kan gis uten at det kreves noen spesifikk tillatelse fra en tilsynsmyndighet ved hjelp av standard personvernbestemmelser, jf. artikkel 46 nr. 2 bokstav c i personvernforordningen.

EUs standardkontraktsklausuler eller andre egnede garantier avtales med alle mottakere fra tredjeland før den første overføringen av personopplysninger. På denne måten sikres det at de registrerte er garantert passende garantier, rettigheter som kan håndheves og effektive rettsmidler for de registrerte. Alle registrerte kan få en kopi av standardkontraktsbestemmelsene fra oss. Standardkontraktsbestemmelsene er også tilgjengelige i Den europeiske unions tidende.

Artikkel 45(3) i personvernforordningen (GDPR) gir EU-kommisjonen myndighet til å beslutte, ved hjelp av en gjennomføringsrettsakt, at et land utenfor EU sikrer et tilstrekkelig beskyttelsesnivå. Dette innebærer et beskyttelsesnivå for personopplysninger som i hovedsak tilsvarer beskyttelsesnivået i EU. Beslutninger om adekvat beskyttelsesnivå innebærer at personopplysninger kan flyte fritt fra EU (og Norge, Liechtenstein og Island) til et tredjeland uten ytterligere hindringer. Lignende regler gjelder for Storbritannia, Sveits og enkelte andre land.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

Der EU-kommisjonen eller myndighetene i et annet land har bestemt at et tredjeland sikrer et tilstrekkelig beskyttelsesnivå, og et gyldig rammeverk er på plass (f.eks. EU-U.S. Data Privacy Framework, Swiss-U.S. Data Privacy Framework, UK Extension to the EU-U.S. Data Privacy Framework), er alle overføringer fra oss til medlemmene av slike rammeverk (f.eks. selvsertifiserte enheter) utelukkende basert på enhetens medlemskap i det respektive rammeverket. Når vi eller en av våre konsernenheter er medlem av et slikt rammeverk, er alle overføringer til oss eller vår konsernenhet utelukkende basert på enhetens medlemskap i et slikt rammeverk.

Alle registrerte kan få en kopi av rammeverkene fra oss. I tillegg er rammeverkene også tilgjengelige i Den europeiske unions tidende eller i publisert juridisk materiale eller på nettsidene til tilsynsmyndigheter eller andre kompetente myndigheter eller institusjoner.

## G. Perioden personopplysningene skal lagres, eller hvis dette ikke er mulig, kriteriene som brukes for å fastsette denne perioden (artikkel 14(2) bokstav a i GDPR)

Oppbevaringsperioden for personopplysninger om søkere er 6 måneder. For opplysninger om ansatte gjelder den respektive lovbestemte oppbevaringsperioden. Etter utløpet av denne perioden slettes de aktuelle opplysningene rutinemessig, så lenge de ikke lenger er nødvendige for å oppfylle kontrakten eller innlede en kontrakt.

## H. Varsel om de berettigede interessene som forfølges av den behandlingsansvarlige eller en tredjepart dersom behandlingen er basert på artikkel 6(1) lit. f GDPR (art. 14(2) lit. b GDPR).

I henhold til artikkel 6 nr. 1 bokstav f i personvernforordningen skal behandling bare være lovlig dersom behandlingen er nødvendig for formål knyttet til berettigede interesser som forfølges av den behandlingsansvarlige eller en tredjepart, med mindre den registrertes interesser eller grunnleggende rettigheter og friheter, som krever vern av personopplysninger, går foran. I henhold til fortalepunkt 47, 2. setning i GDPR kan en berettiget interesse foreligge der det er et relevant og hensiktsmessig forhold mellom den registrerte og den behandlingsansvarlige, f.eks. i situasjoner der den registrerte er kunde av den behandlingsansvarlige. I alle tilfeller der selskapet vårt behandler opplysninger om søkere basert på artikkel 6(1) bokstav f i GDPR, er vår berettigede interesse å ansette egnet personell og fagpersoner.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## I. Eksistensen av retten til å be den behandlingsansvarlige om innsyn i og retting eller sletting av personopplysninger eller begrensning av behandling som gjelder den registrerte, og til å protestere mot behandling, samt retten til dataportabilitet (artikkel 14(2) bokstav c GDPR)

Alle registrerte har følgende rettigheter:

***Rett til tilgang***

Alle registrerte har rett til innsyn i personopplysningene som gjelder dem. Retten til innsyn omfatter alle opplysninger som behandles av oss. Retten kan utøves på en enkel måte og med rimelige mellomrom for å få kjennskap til og verifisere om behandlingen er lovlig (betraktning 63 i GDPR). Denne retten følger av art. 15 I PERSONVERNFORORDNINGEN. Den registrerte kan kontakte oss for å utøve retten til innsyn.

***Rett til retting***

I henhold til artikkel 16 nr. 1 i personvernforordningen har den registrerte rett til å få uriktige personopplysninger om seg selv rettet av den behandlingsansvarlige uten ugrunnet opphold. I henhold til artikkel 16 nr. 2 i personvernforordningen har den registrerte dessuten rett til å få ufullstendige personopplysninger komplettert, blant annet ved å gi en utfyllende redegjørelse, idet det tas hensyn til formålet med behandlingen. Den registrerte kan kontakte oss for å utøve retten til retting.

***Rett til sletting (rett til å bli glemt)***

I tillegg har de registrerte rett til sletting og til å bli glemt i henhold til Art. 17 I GDPR. Denne retten kan også utøves ved å kontakte oss. Vi gjør imidlertid oppmerksom på at denne retten ikke gjelder i den grad behandlingen er nødvendig for å oppfylle en rettslig forpliktelse som selskapet vårt er underlagt, jf. artikkel 17 nr. 3 bokstav b i GDPR. Dette betyr at vi først kan godkjenne en søknad om sletting etter utløpet av den lovbestemte oppbevaringsperioden.

***Rett til begrensning av behandling***

I henhold til artikkel 18 i GDPR har enhver registrert rett til begrensning av behandlingen. Begrensning av behandlingen kan kreves dersom ett av vilkårene i artikkel 18 nr. 1 bokstav a-d i GDPR er oppfylt. Den registrerte kan kontakte oss for å utøve retten til begrensning av behandlingen.

***Rett til å komme med innsigelser***

Videre gir art. 21 i personvernforordningen retten til å protestere. Den registrerte kan kontakte oss for å utøve retten til å protestere.

***Rett til dataportabilitet***

Art. 20 i GDPR gir den registrerte rett til dataportabilitet. I henhold til denne bestemmelsen har den registrerte, på de vilkår som er fastsatt i artikkel 20 nr. 1 bokstav a og b i GDPR, rett til å motta personopplysninger om seg selv som vedkommende har gitt til en behandlingsansvarlig, i et strukturert, alminnelig anvendt og maskinlesbart format, og har rett til å overføre disse opplysningene til en annen


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

behandlingsansvarlig uten hindring fra den behandlingsansvarlige som personopplysningene er gitt til. Den registrerte kan kontakte oss for å utøve retten til dataportabilitet.

## J. Retten til å trekke tilbake samtykket når som helst, uten at det påvirker lovligheten av behandling basert på samtykke før tilbaketrekking, når behandlingen er basert på artikkel 6(1) lit. a eller artikkel 9(2) lit. a GDPR (art. 14(2) lit. d GDPR).

Hvis behandlingen av personopplysninger er basert på art. 6(1) lit. a GDPR, noe som er tilfellet hvis den registrerte har gitt samtykke til behandling av personopplysninger for ett eller flere spesifikke formål, eller hvis den er basert på artikkel 9(2) lit. a GDPR, som regulerer eksplisitt samtykke til behandling av særlige kategorier av personopplysninger, har den registrerte i henhold til artikkel 7(3) setning 1 GDPR rett til å trekke tilbake sitt samtykke når som helst.

Tilbaketrekking av samtykke skal ikke påvirke lovligheten av behandling basert på samtykke før det ble trukket tilbake, personvernforordningen artikkel 7 nr. 3 annet punktum. Det skal være like enkelt å trekke tilbake som å gi samtykke, art. 7(3) fjerde punktum i GDPR. Tilbaketrekking av samtykke kan derfor alltid skje på samme måte som samtykket ble gitt, eller på en annen måte som den registrerte anser som enklere. I dagens informasjonssamfunn er sannsynligvis den enkleste måten å trekke tilbake et samtykke på en enkel e-post. Hvis den registrerte ønsker å trekke tilbake samtykket han eller hun har gitt oss, er det tilstrekkelig med en enkel e-post til oss. Alternativt kan den registrerte velge en annen måte å kommunisere sin tilbaketrekking av samtykke til oss på.

## K. Rett til å klage til en tilsynsmyndighet (art. 14(2) lit. e, 77(1) GDPR)

Som behandlingsansvarlig er vi forpliktet til å informere den registrerte om retten til å klage til en tilsynsmyndighet, jf. personvernforordningen artikkel 14 nr. 2 bokstav e. Retten til å klage til en tilsynsmyndighet er regulert i artikkel 77(1) i GDPR. I henhold til denne bestemmelsen skal enhver registrert, uten at det berører andre administrative eller rettslige midler, ha rett til å klage til en tilsynsmyndighet, særlig i den medlemsstaten der vedkommende har sitt vanlige bosted, sitt arbeidssted eller stedet for det påståtte bruddet, dersom den registrerte mener at behandlingen av personopplysninger om vedkommende er i strid med personvernforordningen. Retten til å klage til en tilsynsmyndighet er i unionsretten begrenset slik at den bare kan utøves overfor én enkelt tilsynsmyndighet (betraktning 141 første setning i GDPR). Hensikten med denne regelen er å unngå at samme registrerte klager to ganger i samme sak. Hvis en registrert ønsker å klage på oss, ber vi derfor om at vedkommende kun kontakter én tilsynsmyndighet.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## L. Kilden personopplysningene stammer fra, og eventuelt om de kommer fra offentlig tilgjengelige kilder (artikkel 14(2) lit. f GDPR)

I prinsippet innhentes personopplysninger direkte fra den registrerte eller i samarbeid med en myndighet (f.eks. innhenting av opplysninger fra et offentlig register). Andre opplysninger om de registrerte **stammer** fra overføringer fra konsernselskaper. I forbindelse med denne generelle informasjonen er det enten umulig å oppgi de nøyaktige kildene som personopplysningene stammer fra, eller det ville innebære en uforholdsmessig stor innsats i henhold til art. 14(5) lit. b GDPR. 14(5) bokstav b i GDPR. I prinsippet samler vi ikke inn personopplysninger fra offentlig tilgjengelige kilder.

Enhver registrert kan når som helst kontakte oss for å få mer detaljert informasjon om de nøyaktige kildene til personopplysningene om ham eller henne. Hvis det ikke er mulig å opplyse den registrerte om hvor personopplysningene stammer fra fordi det er brukt ulike kilder, bør det gis generell informasjon (betraktning 61, setning 4 i GDPR).

## M. Forekomst av automatiserte avgjørelser, herunder profilering, som nevnt i artikkel 22 nr. 1 og 4 i GDPR, og, i det minste i disse tilfellene, meningsfull informasjon om den involverte logikken, samt betydningen og de forventede konsekvensene av slik behandling for den registrerte (artikkel 14 nr. 2 bokstav g i GDPR).

Som et ansvarlig selskap bruker vi vanligvis ikke automatiserte avgjørelser eller profilering. Hvis vi i unntakstilfeller bruker automatiserte avgjørelser eller profilering, vil vi informere den registrerte om dette, enten separat eller via et underavsnitt i personvernerklæringen vår (på nettstedet vårt). I slike tilfeller gjelder følgende:

Automatiserte avgjørelser - inkludert profilering - kan forekomme hvis (1) dette er nødvendig for å inngå eller oppfylle en avtale mellom den registrerte og oss, eller (2) dette er tillatt i henhold til unionsretten eller medlemsstatenes nasjonale rett som vi er underlagt, og som også fastsetter egnede tiltak for å beskytte den registrertes rettigheter og friheter og berettigede interesser, eller (3) dette er basert på den registrertes uttrykkelige samtykke.

I de tilfellene som er nevnt i artikkel 22 nr. 2 bokstav a og c i personvernforordningen, skal vi iverksette egnede tiltak for å ivareta den registrertes rettigheter og friheter og berettigede interesser. I slike tilfeller har du rett til å be om menneskelig inngripen fra den behandlingsansvarliges side, til å uttrykke ditt synspunkt og til å bestride avgjørelsen.

Betydningsfull informasjon om den involverte logikken, samt betydningen og de forventede konsekvensene av slik behandling for den registrerte, er beskrevet i vår personvernerklæring.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## III. EU-U.S. Data Privacy Framework (EU-U.S. DPF), UK Extension to the EU-U.S. DPF, Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF)

Hvis vår organisasjon er et sertifisert medlem av EU-U.S. Data Privacy Framework (EU-U.S. DPF) og/eller UK Extension to the EU-U.S. DPF og/eller Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF), gjelder følgende:

Vi overholder EU-U.S. Data Privacy Framework (EU-U.S. DPF) og UK Extension to the EU-U.S. DPF samt Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF), som fastsatt av U.S. Department of Commerce. Vår virksomhet har bekreftet overfor det amerikanske handelsdepartementet at den overholder EU-U.S. Data Privacy Framework Principles (EU-U.S. DPF Principles) når det gjelder behandling av personopplysninger som den mottar fra Den europeiske union og Storbritannia i henhold til EU-U.S. DPF og UK Extension to the EU-U.S. DPF. Vår virksomhet har bekreftet overfor det amerikanske handelsdepartementet at den overholder Swiss-U.S. Data Privacy Framework Principles (Swiss-U.S. DPF Principles) når det gjelder behandling av personopplysninger som den mottar fra Sveits i henhold til Swiss-U.S. DPF. Ved motstrid mellom bestemmelsene i vår personvernerklæring og EU-U.S. DPF Principles og/eller Swiss-U.S. DPF Principles, vil Principles være avgjørende.

For å lære mer om Data Privacy Framework (DPF) programmet og for å se vår sertifisering, vennligst besøk https://www.dataprivacyframework.gov/.

De andre amerikanske enhetene eller datterselskapene i vår virksomhet som også overholder EU-U.S. DPF Principals, inkludert UK Extension to the EU-U.S. DPF og Swiss-U.S. DPF Principals, hvis noen, er nevnt i vår personvernerklæring.

I samsvar med EU-U.S. DPF og UK Extension to the EU-U.S. DPF samt Swiss-U.S. DPF, forplikter vår virksomhet seg til å samarbeide med det panelet som er opprettet av EUs databeskyttelsesmyndigheter og det britiske Information Commissioner's Office (ICO) samt den sveitsiske føderale databeskyttelses- og informasjonskommissæren (EDÖB), og følge deres råd angående uløste klager om vår håndtering av personopplysninger vi mottar i henhold til EU-U.S. DPF og UK Extension to the EU-U.S. DPF og Swiss-U.S. DPF.

Vi informerer de berørte personene om de relevante europeiske databeskyttelsesmyndighetene som er ansvarlige for behandling av klager om vår organisasjons håndtering av personopplysninger, øverst i dette gjennomsiktighetsdokumentet, og at vi tilbyr de berørte personene en passende og gratis rettsmiddel.

Vi informerer alle berørte personer om at vår virksomhet er underlagt Federal Trade Commission's (FTC) etterforsknings- og håndhevingsmyndighet.

Berørte personer har under visse betingelser muligheten til å benytte bindende voldgift. Vår organisasjon er forpliktet til å avgjøre krav og overholde betingelsene i vedlegg I til DPF-Principals, forutsatt at den


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

berørte personen har anmodet om bindende voldgift ved å varsle vår organisasjon og følge prosedyrene og betingelsene i vedlegg I til Principals.

Vi informerer herved alle berørte personer om vårt selskaps ansvar i tilfelle overføring av personopplysninger til tredjeparter.

For spørsmål fra berørte personer eller datatilsynsmyndigheter har vi utpekt de lokale representantene som er nevnt ovenfor i dette gjennomsiktighetsdokumentet.

Vi gir deg muligheten til å velge (Opt-out) om dine personopplysninger (i) skal overføres til tredjeparter eller (ii) brukes til et formål som er vesentlig forskjellig fra det/de formålet/formålene de opprinnelig ble samlet inn for eller senere godkjent av deg. Den tydelige, godt synlige og lett tilgjengelige mekanismen for å utøve ditt valg er å kontakte vår personvernansvarlige (DSB) via e-post. Du har ikke muligheten til å velge, og vi er heller ikke forpliktet til det, hvis opplysningene overføres til en tredjepart som fungerer som agent eller databehandler på våre vegne og i henhold til våre instruksjoner. Vi inngår imidlertid alltid en avtale med en slik agent eller databehandler.

For sensitive data (dvs. personopplysninger som inneholder informasjon om helsetilstand, rase eller etnisk opprinnelse, politiske meninger, religiøse eller filosofiske overbevisninger, medlemskap i fagforening eller opplysninger om den aktuelle personens seksualliv) innhenter vi ditt uttrykkelige samtykke (Opt-in) når disse opplysningene (i) overføres til tredjeparter eller (ii) brukes til et annet formål enn det de opprinnelig ble samlet inn for eller som du senere har gitt ditt samtykke til ved å velge Opt-in. Videre behandler vi alle personopplysninger vi mottar fra tredjeparter som sensitive hvis tredjeparten identifiserer og behandler dem som sensitive.

Vi informerer deg herved om kravet om å avsløre personopplysninger som svar på lovlige forespørsler fra myndigheter, inkludert for å oppfylle krav til nasjonal sikkerhet eller rettshåndhevelse.

Ved overføring av personopplysninger til en tredjepart som fungerer som behandlingsansvarlig, overholder vi Principals for varsling og valg. I tillegg inngår vi en avtale med tredjeparten som er ansvarlig for behandlingen, som fastsetter at disse opplysningene kun skal behandles for begrensede og spesifiserte formål i samsvar med ditt samtykke og at mottakeren skal gi samme beskyttelsesnivå som DPF Principles og varsle oss hvis de fastslår at de ikke lenger kan oppfylle denne forpliktelsen. Avtalen fastsetter at tredjeparten som er ansvarlig, skal stoppe behandlingen eller treffe andre passende og rimelige tiltak for å rette opp situasjonen hvis en slik fastsettelse gjøres.

Ved overføring av personopplysninger til en tredjepart som fungerer som agent eller databehandler, (i) overfører vi disse opplysningene kun for begrensede og spesifiserte formål; (ii) vi sørger for at agenten eller databehandleren er forpliktet til å tilby minst samme nivå av databeskyttelse som DPF-Principals krever; (iii) vi tar passende og rimelige tiltak for å sikre at agenten eller databehandleren faktisk behandler de overførte personopplysningene på en måte som er i samsvar med våre forpliktelser i henhold til DPF-Principals; (iv) vi krever at agenten eller databehandleren varsler vår organisasjon hvis de fastslår at de ikke lenger kan oppfylle forpliktelsen til å gi samme beskyttelsesnivå som DPF-Principals krever; (v) etter


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

en slik varsling, også i henhold til (iv), tar vi passende og rimelige tiltak for å stoppe uautorisert behandling og rette opp situasjonen; og (vi) vi gir DPF Department på forespørsel et sammendrag eller et representativt eksempel på de relevante databeskyttelsesbestemmelsene fra vår avtale med denne agenten.

I samsvar med EU-U.S. DPF og/eller UK Extension to the EU-U.S. DPF og/eller Swiss-U.S. DPF forplikter vår organisasjon seg til å samarbeide med det panelet som er opprettet av EUs databeskyttelsesmyndigheter og det britiske Information Commissioner's Office (ICO) eller den sveitsiske føderale databeskyttelses- og informasjonskommissæren (EDÖB) og følge deres råd angående uløste klager om vår håndtering av personopplysninger vi mottar i forbindelse med arbeidsforhold i henhold til EU-U.S. DPF og UK Extension to the EU-U.S. DPF og Swiss-U.S. DPF.

Alle registrerte som midlertidig oppholder seg i Den europeiske union (EU), Det europeiske økonomiske samarbeidsområdet (EØS) eller Storbritannia, eller som har sin bopel eller sitt vanlige oppholdssted der, har rett til de rettighetene og de registrerte rettighetene som er publisert i vårt åpenhetsdokument, og som også følger av artikkel 15 til 22 i GDPR, inkludert retten til innsyn i personopplysninger. Vi har gjort denne informasjonen tilgjengelig på alle EU- og EØS-språk. Den engelskspråklige versjonen gjelder for Storbritannia.

Alle registrerte som er midlertidig bosatt i Sveits eller har bosted eller vanlig oppholdssted der, har rett til de rettighetene som følger av den sveitsiske databeskyttelsesloven (DPA) og den sveitsiske databeskyttelsesforordningen (DPR), som er publisert i vårt åpenhetsdokument, inkludert retten til innsyn i personopplysninger. Vi har gitt denne informasjonen på de tre offisielle språkene i Sveits (tysk, italiensk og fransk).


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

# ICELANDIC: Upplýsingar um vinnslu persónuupplýsinga (13. gr., 14 GDPR)

Kæri herra eða frú,

Persónuupplýsingar hvers einstaklings sem er í samningsbundnu, forsamningsbundnu eða öðru sambandi við fyrirtækið okkar verðskulda sérstaka vernd. Markmið okkar er að halda gagnaverndarstigi okkar í háum gæðaflokki. Þess vegna erum við reglulega að þróa hugmyndir okkar um gagnavernd og gagnaöryggi.

Við förum að sjálfsögðu eftir ákvæðum laga um persónuvernd. Samkvæmt 13. grein, 14 GDPR uppfylla ábyrgðaraðilar sérstakar upplýsingakröfur við söfnun persónuupplýsinga. Þetta skjal uppfyllir þessar skyldur.

Hugtök lagareglugerða eru flókin. Því miður var ekki hægt að sleppa notkun lagalegra hugtaka við gerð þessa skjals. Þess vegna viljum við benda þér á að þér er alltaf velkomið að hafa samband við okkur fyrir allar spurningar varðandi þetta skjal, notuð hugtök eða samsetningar.

## I. Fylgni við upplýsingakröfur þegar persónuupplýsingum er safnað frá hinum skráða (13. gr. GDPR)

### A. Auðkenni og samskiptaupplýsingar ábyrgðaraðila (13. mgr. 13. gr. a GDPR)

Sjá fyrir ofan

### B. Samskiptaupplýsingar persónuverndarfulltrúa (1. gr. 3(1) lit. b GDPR)

Sjá fyrir ofan

### C. Tilgangur vinnslunnar sem persónuupplýsingarnar eru ætlaðar til sem og lagagrundvöllur vinnslunnar (13. gr. c GDPR)

Tilgangur vinnslu persónuupplýsinga er meðhöndlun allrar starfsemi sem varðar ábyrgðaraðila, viðskiptavini, væntanlega viðskiptavini, viðskiptafélaga eða önnur samningsbundin eða forsamningsbundin tengsl milli nefndra hópa (í víðasta skilningi) eða lagalegar skyldur ábyrgðaraðila. .

gr. 6(1) lit. GDPR þjónar sem lagagrundvöllur vinnsluaðgerða sem við fáum samþykki fyrir í ákveðnum vinnslutilgangi. Ef vinnsla persónuupplýsinga er nauðsynleg til að efna samnings sem hinn skráði er aðili


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

að, eins og td er tilvik þegar vinnsla er nauðsynleg vegna afhendingar vöru eða til að veita aðra þjónustu, er vinnslan nauðsynleg. byggt á 1. mgr. 6. gr. b GDPR. Sama á við um slíka vinnslu sem nauðsynleg er til að framkvæma ráðstafanir fyrir samningsgerð, td þegar um er að ræða fyrirspurnir um vörur okkar eða þjónustu. Er fyrirtæki okkar háð lagalegri skyldu þar sem vinnsla persónuupplýsinga er nauðsynleg, svo sem til að uppfylla skattskyldur, byggist vinnslan á 2. gr. 6(1) lit. c GDPR.

Í einstaka tilfellum getur vinnsla persónuupplýsinga verið nauðsynleg til að vernda brýna hagsmuni hins skráða eða annars einstaklings. Þetta væri til dæmis raunin ef gestur slasaðist í fyrirtæki okkar og nafn hans, aldur, sjúkratryggingagögn eða aðrar mikilvægar upplýsingar þyrfti að koma til læknis, sjúkrahúss eða annars þriðja aðila. Þá yrði vinnslan miðuð við 2. gr. 6(1) lit. d GDPR.

Þar sem vinnslan er nauðsynleg til að inna af hendi verkefni sem unnið er í þágu almannahagsmuna eða við beitingu opinbers valds sem ábyrgðaraðili hefur, er lagagrundvöllur 2. gr. 6(1) lit. e GDPR.

Loks mætti byggja vinnslu á 1. mgr. 6. gr. f GDPR. Þessi lagagrundvöllur er notaður til vinnsluaðgerða sem falla ekki undir neina af ofangreindum lagalegum forsendum, ef vinnslan er nauðsynleg í þágu lögmætra hagsmuna sem fyrirtæki okkar eða þriðji aðili hagsmuna að gæta, nema þar sem hagsmunir vegi þyngra. eða grundvallarréttindi og frelsi hins skráða sem krefjast verndar persónuupplýsinga. Slíkar vinnsluaðgerðir eru sérstaklega leyfilegar vegna þess að þær hafa verið sérstaklega tilgreindar af evrópska löggjafanum. Hann taldi að gera mætti ráð fyrir lögmætum hagsmunum ef hinn skráði væri skjólstæðingur ábyrgðaraðila (47. setning 2 GDPR).

## D. Þar sem vinnslan byggist á 1. mgr. 6. gr. f GDPR lögmætra hagsmuni sem ábyrgðaraðili eða þriðji aðili hefur fylgst með (13. gr. lit. d GDPR)

Þegar vinnsla persónuupplýsinga er byggð á 1. mgr. 6. gr. f GDPR lögmætir hagsmunir okkar eru að stunda viðskipti okkar í þágu velferðar allra starfsmanna okkar og hluthafa.

## E. Flokkar viðtakenda persónuupplýsinganna (13. mgr. 1. gr. e GDPR)

Opinberir aðilar

Ytri stofnanir

Frekari ytri aðilar

Innri vinnsla

Vinnsla innan hóps

Önnur lík


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

Listi yfir vinnsluaðila okkar og viðtakendur gagna í þriðju löndum og, ef við á, alþjóðlegum stofnunum er annað hvort birtur á vefsíðu okkar eða hægt er að biðja um það frá okkur án endurgjalds. Vinsamlegast hafðu samband við gagnaverndarfulltrúa okkar til að biðja um þennan lista.

## F. Viðtakendur í þriðja landi og viðeigandi eða viðeigandi öryggisráðstafanir og leiðir til að fá afrit af þeim eða þar sem þeir hafa verið aðgengilegir (13. gr. . c GDPR)

Öll fyrirtæki og útibú sem eru hluti af samstæðu okkar (hér eftir kölluð "samstæðufyrirtæki") sem hafa starfsstöð eða skrifstofu í þriðja landi geta tilheyrt viðtakendum persónuupplýsinga. Hægt er að óska eftir lista yfir öll samstæðufyrirtæki eða viðtakendur hjá okkur.

Samkvæmt 1. mgr. 46. gr. GDPR má ábyrgðaraðili eða vinnsluaðili einungis flytja persónuupplýsingar til þriðja lands ef ábyrgðaraðili eða vinnsluaðili hefur veitt viðeigandi verndarráðstafanir og að því tilskildu að aðfararhæf réttindi skráðra einstaklinga og skilvirk réttarúrræði fyrir skráða einstaklinga séu tiltæk. Heimilt er að veita viðeigandi verndarráðstafanir án þess að krefjast sérstakrar heimildar frá eftirlitsyfirvaldi með stöðluðum samningsákvæðum, 2. mgr. 46. gr. lit. c GDPR.

Samið er um staðlaða samningsákvæði Evrópusambandsins eða aðrar viðeigandi verndarráðstafanir við alla viðtakendur frá þriðju löndum fyrir fyrstu sendingu persónuupplýsinga. Þar af leiðandi er tryggt að viðeigandi verndarráðstafanir, framfylganleg réttindi skráðra einstaklinga og skilvirk réttarúrræði fyrir skráða einstaklinga séu tryggð. Sérhver skráður einstaklingur getur fengið afrit af stöðluðum samningsákvæðum frá okkur. Stöðluðu samningsákvæðin eru einnig fáanleg í Stjórnartíðindum Evrópusambandsins.

Grein 45(3) í almennu gagnaverndarreglugerðinni (GDPR) veitir framkvæmdastjórn Evrópusambandsins vald til að ákveða, með framkvæmdargerð, að ríki utan ESB tryggi fullnægjandi vernd. Þetta þýðir verndarstig fyrir persónuupplýsingar sem er í meginatriðum jafngilt verndarstigi innan ESB. Áhrif ákvarðana um fullnægjandi hæfi eru að persónuupplýsingar geta streymt óhindrað frá ESB (og Noregi, Liechtenstein og Íslandi) til þriðja lands án frekari hindrana. Svipaðar reglur gilda fyrir Bretland, Sviss og sum önnur lönd.

Þar sem framkvæmdastjórn Evrópusambandsins eða stjórnvöld annars lands ákváðu að þriðja land tryggi fullnægjandi vernd og gildur rammi er til staðar ( td gagnaverndarrammi ESB og Bandaríkjanna, gagnaverndarrammi Sviss og Bandaríkjanna, framlenging í Bretlandi við EU-US Data Privacy Framework), eru allar millifærslur af okkar hálfu til meðlima slíkra ramma (td sjálfvottaðra aðila) eingöngu byggðar á aðild þeirra aðila að viðkomandi ramma. Þar sem við eða einn úr hópnum okkar aðilar eru aðili að slíkum ramma, allar millifærslur til okkar eða hópeiningar okkar eru eingöngu byggðar á aðild aðila að slíkum ramma.

Allir skráðir einstaklingar geta fengið afrit af rammanum hjá okkur. Að auki eru rammana einnig aðgengileg í Stjórnartíðindum Evrópusambandsins eða í útgefnum lagagögnum eða á vefsíðum eftirlitsyfirvalda eða annarra lögbærra yfirvalda eða stofnana.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## G. Tímabil sem persónuupplýsingarnar verða geymdar í, eða ef það er ekki mögulegt, viðmiðin sem notuð eru til að ákvarða það tímabil (2. mgr. 13. gr. a GDPR)

Viðmiðin sem notuð eru til að ákvarða geymslutíma persónuupplýsinga er viðkomandi lögbundinn varðveislutími. Að þeim tíma liðnum er samsvarandi gögnum reglulega eytt, svo framarlega sem þau eru ekki lengur nauðsynleg til að uppfylla samninginn eða hefja samning.

Ef ekki er lögbundinn varðveislutími er viðmiðunin samningsbundinn eða innri varðveislutími.

## H. Til staðar er réttur til að krefja ábyrgðaraðila um aðgang að og leiðréttingu eða eyðingu persónuupplýsinga eða takmörkun á vinnslu varðandi hinn skráða eða til að andmæla vinnslu sem og réttur til gagnaflutnings (b-lið 2. mgr. 13. gr. GDPR)

Allir skráðir einstaklingar hafa eftirfarandi réttindi:

***Réttur til aðgangs***

Sérhver skráður einstaklingur á rétt á aðgangi að persónuupplýsingum um hann eða hana. Réttur til aðgangs nær til allra gagna sem við vinnum með. Rétturinn er hægt að nýta auðveldlega og með hæfilegu millibili, til þess að vera meðvitaður um og sannreyna lögmæti vinnslunnar (63. grein GDPR). Þessi réttur leiðir af 3. gr. 15 GDPR. Hinn skráði gæti haft samband við okkur til að nýta réttinn til aðgangs.

***Réttur til úrbóta***

Samkvæmt 16. grein 1. GDPR á hinn skráði rétt á að fá frá ábyrgðaraðila án ástæðulauss tafar leiðréttingu á ónákvæmum persónuupplýsingum um hann eða hana. Ennfremur kveður 16. gr. setning 2 GDPR á um að hinn skráði eigi rétt á, að teknu tilliti til tilgangs vinnslunnar, að fá ófullkomnar persónuupplýsingar fullnaðar, þar á meðal með því að leggja fram viðbótaryfirlýsingu. Hinn skráði getur haft samband við okkur til að nýta réttinn til úrbóta.

***Réttur til að eyða (réttur til að gleymast)***

Að auki eiga skráðir aðilar rétt á eyðingu og til að gleymast skv. 17 GDPR. Þennan rétt er einnig hægt að nýta með því að hafa samband við okkur. Á þessum tímapunkti viljum við þó benda á að þessi réttur á ekki við að svo miklu leyti sem vinnslan er nauðsynleg til að uppfylla lagaskyldu sem fyrirtæki okkar er háð, 3. mgr. 17. gr. lit. b GDPR. Þetta þýðir að við getum samþykkt umsókn um eyðingu aðeins eftir að lögbundinn varðveislutími er liðinn.

***Réttur til takmörkunar á vinnslu***

Samkvæmt 18. grein GDPR á hver skráður einstaklingur rétt á takmörkun á vinnslu. Heimilt er að krefjast takmörkunar á vinnslu ef eitthvert af skilyrðum 1. mgr. 18. gr. ad GDPR er uppfyllt. Hinn skráði gæti haft samband við okkur til að nýta réttinn til takmörkunar á vinnslu.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

***Réttur til andmæla***

Jafnframt er gr. 21 GDPR tryggir andmælarétt. Hinn skráði gæti haft samband við okkur til að nýta andmælaréttinn.

***Réttur til gagnaflutnings***

gr. 20 GDPR veitir hinum skráða rétt til gagnaflutnings. Samkvæmt þessu ákvæði hefur hinn skráði með þeim skilyrðum sem mælt er fyrir um í 1. mgr. 20. gr. a og b GDPR réttur til að fá persónuupplýsingar um hann eða hana, sem hann eða hún hefur látið ábyrgðaraðila í té, á skipulögðu, almennu og véllesanlegu sniði og hafa rétt til að senda þær gögn til annars ábyrgðaraðila án hindrunar. frá ábyrgðaraðilanum sem persónuupplýsingarnar hafa verið veittar til. Hinn skráði gæti haft samband við okkur til að nýta réttinn til gagnaflutnings.

## I. Réttur til að afturkalla samþykki hvenær sem er, án þess að hafa áhrif á lögmæti vinnslu sem byggist á samþykki fyrir afturköllun þess, þar sem vinnslan byggist á 1. mgr. 6. gr. lit. GDPR eða 2. mgr. 9. gr. a GDPR (2. mgr. 13. gr. c GDPR)

Sé vinnsla persónuupplýsinga byggð á 2. gr. 6(1) lit. GDPR, sem er tilfellið, ef hinn skráði hefur veitt samþykki fyrir vinnslu persónuupplýsinga í einum eða fleiri tilteknum tilgangi eða byggist hún á 2. mgr. 9. gr. GDPR, sem kveður á um skýrt samþykki fyrir vinnslu sérstakra flokka persónuupplýsinga, hefur hinn skráði samkvæmt 7. gr. 3. setningu 1 GDPR rétt til að afturkalla samþykki sitt hvenær sem er.

Afturköllun samþykkis hefur ekki áhrif á lögmæti vinnslu sem byggist á samþykki fyrir afturköllun þess, 3. mgr. 7. gr. 2. setning GDPR. Það skal vera jafn auðvelt að afturkalla og gefa samþykki, gr. 7(3) Málsgrein 4 GDPR. Afturköllun samþykkis getur því alltaf farið fram á sama hátt og samþykki hefur verið veitt eða á annan hátt sem hinn skráði telur einfaldari. Í upplýsingasamfélagi nútímans er líklega einfaldasta leiðin til að afturkalla samþykki einfaldur tölvupóstur. Ef hinn skráði vill afturkalla samþykki sitt sem okkur hefur verið veitt nægir einfaldur tölvupóstur til okkar. Að öðrum kosti getur hinn skráði valið hvaða aðra leið sem er til að koma samþykki sínu til baka til okkar.

## J. Réttur til að leggja fram kvörtun til eftirlitsyfirvalds (Gr. 13(2) lit. d, 77(1) GDPR)

Sem ábyrgðaraðili er okkur skylt að tilkynna hinum skráða um réttinn til að leggja fram kvörtun til eftirlitsyfirvalds, 2. mgr. 13. gr. lit. d GDPR. Réttur til að leggja fram kvörtun til eftirlitsyfirvalds er stjórnað af 1. mgr. 77. gr. GDPR. Samkvæmt þessu ákvæði, með fyrirvara um önnur stjórnsýslu- eða dómstólaúrræði, skal sérhver skráður einstaklingur hafa rétt til að leggja fram kvörtun til eftirlitsyfirvalds, einkum í því aðildarríki þar sem hann hefur venjulega búsetu, vinnustað eða starfsstað. meint brot telji hinn skráði að vinnsla persónuupplýsinga um hann brjóti í bága við almenna persónuverndarreglugerð. Réttur til að leggja fram kvörtun til eftirlitsyfirvalds var einungis takmarkaður af lögum sambandsins á þann hátt að hann er aðeins hægt að beita fyrir einu eftirlitsyfirvaldi (141. greinar setning 1 GDPR). Þessari reglu er ætlað að forðast tvöfaldar kvartanir sama skráðs einstaklings í sama máli. Ef skráður


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

einstaklingur vill leggja fram kvörtun vegna okkar, báðum við því um að hafa aðeins samband við eitt eftirlitsyfirvald.

## K. Veiting persónuupplýsinga sem lögbundin eða samningsbundin krafa; Krafa sem er nauðsynleg til að gera samning; Skylda hins skráða til að veita persónuupplýsingarnar; mögulegar afleiðingar þess að vanrækja slík gögn (2. gr. 13(2) lit. e GDPR)

Við skýrum að veiting persónuupplýsinga er að hluta til lögskyld ( td skattareglur) eða getur einnig stafað af samningsákvæðum (td upplýsingar um samningsaðilann).

Stundum getur verið nauðsynlegt að gera samning um að hinn skráði lætur okkur í té persónuupplýsingar sem við þurfum síðan að vinna úr. Hinum skráða er til dæmis skylt að láta okkur í té persónuupplýsingar þegar fyrirtæki okkar skrifar undir samning við hann eða hana. Vanskil persónuupplýsinga hefði þær afleiðingar að ekki væri hægt að gera samning við hinn skráða.

Áður en skráði einstaklingurinn veitir persónuupplýsingar þarf hann að hafa samband við okkur. Við skýrum fyrir hinum skráða hvort afhending persónuupplýsinganna sé áskilin samkvæmt lögum eða samningi eða sé nauðsynleg fyrir samningsgerð, hvort skylda sé til að veita persónuupplýsingarnar og afleiðingar þess að ekki sé veitt persónuupplýsingarnar. .

## L. Tilvist sjálfvirkrar ákvarðanatöku, þ.mt prófílgreiningar, sem um getur í 1. og 4. mgr. 22. gr. GDPR og, að minnsta kosti í þeim tilvikum, þýðingarmiklar upplýsingar um rökfræðina sem um er að ræða, svo og mikilvægi og fyrirhugaðar afleiðingar af slík vinnsla fyrir hinn skráða (2. mgr. 13. gr. f GDPR)

Sem ábyrgt fyrirtæki notum við venjulega ekki sjálfvirka ákvarðanatöku eða prófílgreiningu. Ef, í undantekningartilvikum, framkvæmum við sjálfvirka ákvarðanatöku eða prófílgreiningu munum við upplýsa hinn skráða annað hvort sérstaklega eða í gegnum undirkafla í persónuverndarstefnu okkar (á vefsíðu okkar). Í þessu tilviki á eftirfarandi við:

Sjálfvirk ákvarðanataka - þ.mt prófílgreining - getur átt sér stað ef (1) þetta er nauðsynlegt til að gera eða framkvæma samning milli hins skráða og okkar, eða (2) þetta er heimilað samkvæmt lögum sambandsins eða aðildarríkisins sem við eru háð og þar sem jafnframt er mælt fyrir um viðeigandi ráðstafanir til að standa vörð um réttindi og frelsi og lögmæta hagsmuni hins skráða; eða (3) þetta er byggt á skýru samþykki hins skráða.

Í þeim tilvikum sem um getur í a- og c-lið 22(2) (a) og (c) GDPR, munum við framkvæma viðeigandi ráðstafanir til að vernda réttindi og frelsi hins skráða og lögmæta hagsmuni. Í þessum tilvikum hefur þú


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

rétt á að fá mannleg afskipti af hálfu ábyrgðaraðila, til að koma sjónarmiðum þínum á framfæri og andmæla ákvörðuninni.

Merkingarríkar upplýsingar um rökfræðina sem um er að ræða, svo og mikilvægi og fyrirhugaðar afleiðingar slíkrar vinnslu fyrir hinn skráða, eru settar fram í persónuverndarstefnu okkar.

## II. Fylgni við upplýsingakröfur þegar persónuupplýsingum er ekki safnað frá hinum skráða (14. gr. GDPR)

### A. Auðkenni og samskiptaupplýsingar ábyrgðaraðila (14. mgr. 14. gr. a GDPR)

Sjá fyrir ofan

### B. Samskiptaupplýsingar persónuverndarfulltrúa (14. gr. b. GDPR)

Sjá fyrir ofan

### C. Tilgangur vinnslunnar sem persónuupplýsingarnar eru ætlaðar til sem og lagagrundvöllur vinnslunnar (14. gr. c GDPR)

Tilgangur vinnslu persónuupplýsinga er meðhöndlun allrar starfsemi sem varðar ábyrgðaraðila, viðskiptavini, væntanlega viðskiptavini, viðskiptafélaga eða önnur samningsbundin eða forsamningsbundin tengsl milli nefndra hópa (í víðasta skilningi) eða lagalegar skyldur ábyrgðaraðila. .

Ef vinnsla persónuupplýsinga er nauðsynleg til að efna samnings sem hinn skráði er aðili að, eins og td er tilvik þegar vinnsla er nauðsynleg vegna afhendingar vöru eða til að veita aðra þjónustu, er vinnslan nauðsynleg. byggt á 1. mgr. 6. gr. b GDPR. Sama á við um slíka vinnslu sem nauðsynleg er til að framkvæma ráðstafanir fyrir samningsgerð, td þegar um er að ræða fyrirspurnir um vörur okkar eða þjónustu. Er fyrirtæki okkar háð lagalegri skyldu þar sem vinnsla persónuupplýsinga er nauðsynleg, svo sem til að uppfylla skattskyldur, byggist vinnslan á 2. gr. 6(1) lit. c GDPR.

Í einstaka tilfellum getur vinnsla persónuupplýsinga verið nauðsynleg til að vernda brýna hagsmuni hins skráða eða annars einstaklings. Þetta væri til dæmis raunin ef gestur slasaðist í fyrirtæki okkar og nafn hans, aldur, sjúkratryggingagögn eða aðrar mikilvægar upplýsingar þyrfti að koma til læknis, sjúkrahúss eða annars þriðja aðila. Þá yrði vinnslan miðuð við 2. gr. 6(1) lit. d GDPR.

Þar sem vinnslan er nauðsynleg til að inna af hendi verkefni sem unnið er í þágu almannahagsmuna eða við beitingu opinbers valds sem ábyrgðaraðili hefur, er lagagrundvöllur 2. gr. 6(1) lit. e GDPR.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

Loks mætti byggja vinnslu á 1. mgr. 6. gr. f GDPR. Þessi lagagrundvöllur er notaður til vinnsluaðgerða sem falla ekki undir neina af ofangreindum lagalegum forsendum, ef vinnslan er nauðsynleg í þágu lögmætra hagsmuna sem fyrirtæki okkar eða þriðji aðili hagsmuna að gæta, nema þar sem hagsmunir vegi þyngra. eða grundvallarréttindi og frelsi hins skráða sem krefjast verndar persónuupplýsinga. Slíkar vinnsluaðgerðir eru sérstaklega leyfilegar vegna þess að þær hafa verið sérstaklega tilgreindar af evrópska löggjafanum. Hann taldi að gera mætti ráð fyrir lögmætum hagsmunum ef hinn skráði væri skjólstæðingur ábyrgðaraðila (47. setning 2 GDPR).

## D. Flokkar persónuupplýsinga sem málið varðar (14. gr. lit. d GDPR)

Gögn viðskiptavina

Gögn hugsanlegra viðskiptavina

Gögn starfsmanna

Gögn birgja

## E. Flokkar viðtakenda persónuupplýsinganna (14. gr. 14. gr. e GDPR)

Opinberir aðilar

Ytri stofnanir

Frekari ytri aðilar

Innri vinnsla

Vinnsla innan hóps

Önnur lík

Listi yfir vinnsluaðila okkar og viðtakendur gagna í þriðju löndum og, ef við á, alþjóðlegum stofnunum er annað hvort birtur á vefsíðu okkar eða hægt er að biðja um það frá okkur án endurgjalds. Vinsamlegast hafðu samband við gagnaverndarfulltrúa okkar til að biðja um þennan lista.


© All rights reserved by Heiko Maniero.

## F. Viðtakendur í þriðja landi og viðeigandi eða viðeigandi verndarráðstafanir og leiðir til að fá afrit af þeim eða þar sem þeir hafa verið aðgengilegir (14. gr. f., 1. mgr. . c GDPR)

Öll fyrirtæki og útibú sem eru hluti af samstæðu okkar (hér eftir kölluð "samstæðufyrirtæki") sem hafa starfsstöð eða skrifstofu í þriðja landi geta tilheyrt viðtakendum persónuupplýsinga. Hægt er að óska eftir lista yfir öll fyrirtæki samstæðunnar hjá okkur.

Samkvæmt 1. mgr. 46. gr. GDPR má ábyrgðaraðili eða vinnsluaðili einungis flytja persónuupplýsingar til þriðja lands ef ábyrgðaraðili eða vinnsluaðili hefur veitt viðeigandi verndarráðstafanir og að því tilskildu að aðfararhæf réttindi skráðra einstaklinga og skilvirk réttarúrræði fyrir skráða einstaklinga séu tiltæk. Veita má viðeigandi verndarráðstafanir án sérstakrar heimildar frá eftirlitsyfirvaldi með stöðluðum gagnaverndarákvæðum, 2. mgr. 46. gr. lit. c GDPR.

staðlaða samningsákvæði Evrópusambandsins eða aðrar viðeigandi verndarráðstafanir við alla viðtakendur frá þriðju löndum fyrir fyrstu sendingu persónuupplýsinga. Þar af leiðandi er tryggt að viðeigandi verndarráðstafanir, framfylganleg réttindi skráðra einstaklinga og skilvirk réttarúrræði fyrir skráða einstaklinga séu tryggð. Sérhver skráður einstaklingur getur fengið afrit af stöðluðum samningsákvæðum frá okkur. Stöðluðu samningsákvæðin eru einnig fáanleg í Stjórnartíðindum Evrópusambandsins.

Grein 45(3) í almennu gagnaverndarreglugerðinni (GDPR) veitir framkvæmdastjórn Evrópusambandsins vald til að ákveða, með framkvæmdargerð, að ríki utan ESB tryggi fullnægjandi vernd. Þetta þýðir verndarstig fyrir persónuupplýsingar sem er í meginatriðum jafngilt verndarstigi innan ESB. Áhrif ákvarðana um fullnægjandi hæfi eru að persónuupplýsingar geta streymt óhindrað frá ESB (og Noregi, Liechtenstein og Íslandi) til þriðja lands án frekari hindrana. Svipaðar reglur gilda fyrir Bretland, Sviss og sum önnur lönd.

Þar sem framkvæmdastjórn Evrópusambandsins eða stjórnvöld annars lands ákváðu að þriðja land tryggi fullnægjandi vernd og gildur rammi er til staðar ( td gagnaverndarrammi ESB og Bandaríkjanna, gagnaverndarrammi Sviss og Bandaríkjanna, framlenging í Bretlandi við EU-US Data Privacy Framework), eru allar millifærslur af okkar hálfu til meðlima slíkra ramma (td sjálfvottaðra aðila) eingöngu byggðar á aðild þeirra aðila að viðkomandi ramma. Þar sem við eða einn úr hópnum okkar aðilar eru aðili að slíkum ramma, allar millifærslur til okkar eða hópeiningar okkar eru eingöngu byggðar á aðild aðila að slíkum ramma.

Allir skráðir einstaklingar geta fengið afrit af rammanum hjá okkur. Að auki eru rammana einnig aðgengileg í Stjórnartíðindum Evrópusambandsins eða í útgefnum lagagögnum eða á vefsíðum eftirlitsyfirvalda eða annarra lögbærra yfirvalda eða stofnana.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## G. Tímabil sem persónuupplýsingarnar verða geymdar í, eða ef það er ekki mögulegt, viðmiðin sem notuð eru til að ákvarða það tímabil (2. mgr. 14. gr. a GDPR)

Viðmiðin sem notuð eru til að ákvarða geymslutíma persónuupplýsinga er viðkomandi lögbundinn varðveislutími. Að þeim tíma liðnum er samsvarandi gögnum reglulega eytt, svo framarlega sem þau eru ekki lengur nauðsynleg til að uppfylla samninginn eða hefja samning.

Ef ekki er lögbundinn varðveislutími er viðmiðunin samningsbundinn eða innri varðveislutími.

## H. Tilkynning um lögmæta hagsmuni sem ábyrgðaraðili eða þriðji aðili hefur fylgst með ef vinnslan byggist á 1. mgr. 6. gr. lit. f GDPR (Gr. 14(2) lit. b GDPR)

Samkvæmt 1. mgr. 6. gr. f GDPR skal vinnslan aðeins vera lögmæt ef vinnslan er nauðsynleg í þeim tilgangi að gæta lögmætra hagsmuna sem ábyrgðaraðili eða þriðji aðili hagsmunir að, nema hagsmunir eða grundvallarréttindi og frelsi hins skráða sem krefjast verndar vegi þyngra. af persónuupplýsingum. Samkvæmt ákvæði 47. setningu 2 GDPR gætu lögmætir hagsmunir verið fyrir hendi þar sem viðeigandi og viðeigandi tengsl eru á milli hins skráða og ábyrgðaraðilans, td í aðstæðum þar sem hinn skráði er viðskiptavinur ábyrgðaraðilans. Í öllum tilvikum þar sem fyrirtækið okkar vinnur persónuupplýsingar á grundvelli 1. mgr. 6. gr. f GDPR eru lögmætir hagsmunir okkar af því að stunda viðskipti okkar í þágu velferðar allra starfsmanna okkar og hluthafa.

## I. Til staðar er réttur til að óska eftir aðgangi að og leiðréttingu eða eyðingu persónuupplýsinga eða takmörkun á vinnslu varðandi hinn skráða og til að andmæla vinnslu frá ábyrgðaraðila sem og réttur til gagnaflutnings (c-liður 2. mgr. 14. gr. GDPR)

Allir skráðir einstaklingar hafa eftirfarandi réttindi:

***Réttur til aðgangs***

Sérhver skráður einstaklingur á rétt á aðgangi að persónuupplýsingum um hann eða hana. Réttur til aðgangs nær til allra gagna sem við vinnum með. Rétturinn er hægt að nýta auðveldlega og með hæfilegu millibili, til þess að vera meðvitaður um og sannreyna lögmæti vinnslunnar (63. grein GDPR). Þessi réttur leiðir af 3. gr. 15 GDPR. Hinn skráði gæti haft samband við okkur til að nýta réttinn til aðgangs.

***Réttur til úrbóta***

Samkvæmt 16. grein 1. GDPR á hinn skráði rétt á að fá frá ábyrgðaraðila án ástæðulauss tafar leiðréttingu á ónákvæmum persónuupplýsingum um hann eða hana. Ennfremur kveður 16. gr. setning 2 GDPR á um að hinn skráði eigi rétt á, að teknu tilliti til tilgangs vinnslunnar, að fá ófullkomnar persónuupplýsingar fullnaðar, þar á meðal með því að leggja fram viðbótaryfirlýsingu. Hinn skráði getur haft samband við okkur til að nýta réttinn til úrbóta.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

***Réttur til að eyða (réttur til að gleymast)***

Að auki eiga skráðir aðilar rétt á eyðingu og til að gleymast skv. 17 GDPR. Þennan rétt er einnig hægt að nýta með því að hafa samband við okkur. Á þessum tímapunkti viljum við þó benda á að þessi réttur á ekki við að svo miklu leyti sem vinnslan er nauðsynleg til að uppfylla lagaskyldu sem fyrirtæki okkar er háð, 3. mgr. 17. gr. lit. b GDPR. Þetta þýðir að við getum samþykkt umsókn um eyðingu aðeins eftir að lögbundinn varðveislutími er liðinn.

***Réttur til takmörkunar á vinnslu***

Samkvæmt 18. grein GDPR á hver skráður einstaklingur rétt á takmörkun á vinnslu. Heimilt er að krefjast takmörkunar á vinnslu ef eitthvert af skilyrðum 1. mgr. 18. gr. ad GDPR er uppfyllt. Hinn skráði gæti haft samband við okkur til að nýta réttinn til takmörkunar á vinnslu.

***Réttur til andmæla***

Jafnframt er gr. 21 GDPR tryggir andmælarétt. Hinn skráði gæti haft samband við okkur til að nýta andmælaréttinn.

***Réttur til gagnaflutnings***

gr. 20 GDPR veitir hinum skráða rétt til gagnaflutnings. Samkvæmt þessu ákvæði hefur hinn skráði með þeim skilyrðum sem mælt er fyrir um í 1. mgr. 20. gr. a og b GDPR réttur til að fá persónuupplýsingar um hann eða hana, sem hann eða hún hefur látið ábyrgðaraðila í té, á skipulögðu, almennu og véllesanlegu sniði og hafa rétt til að senda þær gögn til annars ábyrgðaraðila án hindrunar. frá ábyrgðaraðilanum sem persónuupplýsingarnar hafa verið veittar til. Hinn skráði gæti haft samband við okkur til að nýta réttinn til gagnaflutnings.

## J. Réttur til að afturkalla samþykki hvenær sem er, án þess að það hafi áhrif á lögmæti vinnslu sem byggist á samþykki fyrir afturköllun þess, þar sem vinnslan byggist á 1. mgr. 6. gr. lit. a eða 2. mgr. 9. gr. a GDPR (Gr. 14(2) lit. d GDPR)

Sé vinnsla persónuupplýsinga byggð á 2. gr. 6(1) lit. GDPR, sem er tilfellið, ef hinn skráði hefur veitt samþykki fyrir vinnslu persónuupplýsinga í einum eða fleiri tilteknum tilgangi eða byggist hún á 2. mgr. 9. gr. GDPR, sem kveður á um skýrt samþykki fyrir vinnslu sérstakra flokka persónuupplýsinga, hefur hinn skráði samkvæmt 7. gr. 3. setningu 1 GDPR rétt til að afturkalla samþykki sitt hvenær sem er.

Afturköllun samþykkis hefur ekki áhrif á lögmæti vinnslu sem byggist á samþykki fyrir afturköllun þess, 3. mgr. 7. gr. 2. setning GDPR. Það skal vera jafn auðvelt að afturkalla og gefa samþykki, gr. 7(3) Málsgrein 4 GDPR. Afturköllun samþykkis getur því alltaf farið fram á sama hátt og samþykki hefur verið veitt eða á annan hátt sem hinn skráði telur einfaldari. Í upplýsingasamfélagi nútímans er líklega einfaldasta leiðin til að afturkalla samþykki einfaldur tölvupóstur. Ef hinn skráði vill afturkalla samþykki sitt sem okkur hefur verið veitt nægir einfaldur tölvupóstur til okkar. Að öðrum kosti getur hinn skráði valið hvaða aðra leið sem er til að koma samþykki sínu til baka til okkar.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## K. Réttur til að leggja fram kvörtun til eftirlitsyfirvalds (2. mgr. 14. gr. e, 77(1) GDPR)

Sem ábyrgðaraðili er okkur skylt að tilkynna hinum skráða um réttinn til að leggja fram kvörtun til eftirlitsyfirvalds, 2. mgr. 14. gr. lit. e GDPR. Réttur til að leggja fram kvörtun til eftirlitsyfirvalds er stjórnað af 1. mgr. 77. gr. GDPR. Samkvæmt þessu ákvæði, með fyrirvara um önnur stjórnsýslu- eða dómstólaúrræði, skal sérhver skráður einstaklingur hafa rétt til að leggja fram kvörtun til eftirlitsyfirvalds, einkum í því aðildarríki þar sem hann hefur venjulega búsetu, vinnustað eða starfsstað. meint brot telji hinn skráði að vinnsla persónuupplýsinga um hann brjóti í bága við almenna persónuverndarreglugerð. Réttur til að leggja fram kvörtun til eftirlitsyfirvalds var einungis takmarkaður af lögum sambandsins á þann hátt að hann er aðeins hægt að beita fyrir einu eftirlitsyfirvaldi (141. greinar setning 1 GDPR). Þessari reglu er ætlað að forðast tvöfaldar kvartanir sama skráðs einstaklings í sama máli. Ef skráður einstaklingur vill leggja fram kvörtun vegna okkar, báðum við því um að hafa aðeins samband við eitt eftirlitsyfirvald.

## L. Uppruni persónuupplýsinganna, og ef við á, hvort þær komu frá opinberum aðgengilegum heimildum (2. mgr. 14. gr. f GDPR)

Í grundvallaratriðum er persónuupplýsingum safnað beint frá hinum skráða eða í samvinnu við yfirvald ( td öflun upplýsinga úr opinberri skrá). Aðrar upplýsingar um skráða einstaklinga eru stafar af millifærslum samstæðufélaga. Í samhengi við þessar almennu upplýsingar er nafngift á nákvæmum heimildum sem persónuupplýsingar eru upprunnar úr annaðhvort ómögulegt eða myndi fela í sér óhóflega fyrirhöfn í skilningi gr. 14(5) lit. b GDPR. Í grundvallaratriðum söfnum við ekki persónuupplýsingum frá opinberum aðgengilegum aðilum.

Allir skráðir einstaklingar geta haft samband við okkur hvenær sem er til að fá ítarlegri upplýsingar um nákvæmar heimildir persónuupplýsinga um hann eða hana. Ef ekki er hægt að veita hinum skráða uppruna persónuupplýsinganna vegna þess að ýmsar heimildir hafa verið notaðar, ætti að veita almennar upplýsingar (61. setning 4. GDPR).

## M. Tilvist sjálfvirkrar ákvarðanatöku, þ.mt prófílgreiningar, sem um getur í 1. og 4. mgr. 22. gr. GDPR og, að minnsta kosti í þeim tilvikum, þýðingarmiklar upplýsingar um rökfræðina sem um er að ræða, svo og mikilvægi og fyrirhugaðar afleiðingar af slík vinnsla fyrir hinn skráða (2. mgr. 14. gr. g GDPR)

Sem ábyrgt fyrirtæki notum við venjulega ekki sjálfvirka ákvarðanatöku eða prófílgreiningu. Ef, í undantekningartilvikum, framkvæmum við sjálfvirka ákvarðanatöku eða prófílgreiningu munum við upplýsa hinn skráða annað hvort sérstaklega eða í gegnum undirkafla í persónuverndarstefnu okkar (á vefsíðu okkar). Í þessu tilviki á eftirfarandi við:


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

Sjálfvirk ákvarðanataka - þ.mt prófílgreining - getur átt sér stað ef (1) þetta er nauðsynlegt til að gera eða framkvæma samning milli hins skráða og okkar, eða (2) þetta er heimilað samkvæmt lögum sambandsins eða aðildarríkisins sem við eru háð og þar sem jafnframt er mælt fyrir um viðeigandi ráðstafanir til að standa vörð um réttindi og frelsi og lögmæta hagsmuni hins skráða; eða (3) þetta er byggt á skýru samþykki hins skráða.

Í þeim tilvikum sem um getur í a- og c-lið 22(2) (a) og (c) GDPR, munum við framkvæma viðeigandi ráðstafanir til að vernda réttindi og frelsi hins skráða og lögmæta hagsmuni. Í þessum tilvikum hefur þú rétt á að fá mannleg afskipti af hálfu ábyrgðaraðila, til að koma sjónarmiðum þínum á framfæri og andmæla ákvörðuninni.

Merkingarríkar upplýsingar um rökfræðina sem um er að ræða, svo og mikilvægi og fyrirhugaðar afleiðingar slíkrar vinnslu fyrir hinn skráða, eru settar fram í persónuverndarstefnu okkar.

## III. EU-U.S. Data Privacy Framework (EU-U.S. DPF), UK Extension to the EU-U.S. DPF, Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF)

Ef stofnun okkar er vottaður aðili að EU-U.S. Data Privacy Framework (EU-U.S. DPF) og/eða UK Extension to the EU-U.S. DPF og/eða Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF) gildir eftirfarandi:

Við fylgjum EU-U.S. Data Privacy Framework (EU-U.S. DPF) og UK Extension to the EU-U.S. DPF sem og Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF), eins og það er sett af U.S. Department of Commerce. Fyrirtækið okkar hefur staðfest við bandarísku viðskiptaráðuneytið að það fylgi EU-U.S. Data Privacy Framework Principles (EU-U.S. DPF Principles) varðandi vinnslu persónuupplýsinga sem það fær frá Evrópusambandinu og Bretlandi samkvæmt EU-U.S. DPF og UK Extension to the EU-U.S. DPF. Fyrirtækið okkar hefur staðfest við bandarísku viðskiptaráðuneytið að það fylgi Swiss-U.S. Data Privacy Framework Principles (Swiss-U.S. DPF Principles) varðandi vinnslu persónuupplýsinga sem það fær frá Sviss samkvæmt Swiss-U.S. DPF. Ef árekstur er á milli ákvæða persónuverndarstefnu okkar og EU-U.S. DPF Principles og/eða Swiss-U.S. DPF Principles, eru Principles ráðandi.

Til að fá frekari upplýsingar um Data Privacy Framework (DPF) forritið og til að skoða vottun okkar, vinsamlegast heimsækið https://www.dataprivacyframework.gov/.

Aðrar bandarískar einingar eða dótturfélög fyrirtækisins okkar, sem einnig fylgja EU-U.S. DPF Principals, þar á meðal UK Extension to the EU-U.S. DPF og Swiss-U.S. DPF Principals, ef þau eru til, eru nefnd í persónuverndarstefnu okkar.

Í samræmi við EU-U.S. DPF og UK Extension to the EU-U.S. DPF sem og Swiss-U.S. DPF skuldbindur fyrirtækið okkar sig til að vinna með því ráðinu sem stofnað var af persónuverndaryfirvöldum ESB og


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

breska Information Commissioner's Office (ICO) sem og svissneska persónuverndarráðinu (EDÖB) og fylgja ráðleggingum þeirra varðandi óleystar kvartanir um meðhöndlun okkar á persónuupplýsingum sem við fáum samkvæmt EU-U.S. DPF og UK Extension to the EU-U.S. DPF og Swiss-U.S. DPF.

Við upplýsum viðkomandi einstaklinga um viðeigandi evrópsk persónuverndaryfirvöld sem eru ábyrg fyrir meðhöndlun kvartana um meðhöndlun fyrirtækisins okkar á persónuupplýsingum, í efri hluta þessa gagnsæisdokuments og um að við bjóðum viðkomandi einstaklingum upp á viðeigandi og ókeypis réttarúrræði.

Við upplýsum alla viðkomandi einstaklinga um að fyrirtækið okkar sé undir rannsóknar- og framkvæmdarvaldi Federal Trade Commission (FTC).

Viðkomandi einstaklingar hafa, við tilteknar aðstæður, möguleika á að nýta bindandi gerðardóm. Stofnun okkar er skuldbundin til að leysa kröfur og uppfylla skilyrðin í viðauka I við DPF-Principals, að því gefnu að viðkomandi einstaklingur hafi óskað eftir bindandi gerðardómi með því að tilkynna stofnun okkar og fylgja verklagi og skilyrðum í viðauka I við Principals.

Við upplýsum hér með alla viðkomandi einstaklinga um ábyrgð stofnunar okkar í tilfelli afhendingar persónuupplýsinga til þriðja aðila.

Fyrir spurningar frá viðkomandi einstaklingum eða persónuverndaryfirvöldum höfum við útnefnt þá staðbundnu fulltrúa sem nefndir eru í efri hluta þessa gagnsæisdokuments.

Við bjóðum þér að velja (Opt-out), hvort persónuupplýsingar þínar (i) séu afhentar þriðja aðila eða (ii) notaðar í tilgangi sem er verulega frábrugðinn þeim tilgangi/tilgangum sem þær voru upphaflega safnað fyrir eða síðar samþykktar af þér. Skýrt, vel sýnilegt og auðvelt aðgengilegt kerfi til að framkvæma val þitt felst í því að hafa samband við persónuverndarfulltrúa okkar (DSB) með tölvupósti. Þú hefur ekki möguleika á að velja, og við erum ekki heldur skuldbundin til þess, ef gögnin eru afhent þriðja aðila sem starfar sem umboðsmaður eða gagnavinnsluaðili í okkar umboði og samkvæmt fyrirmælum okkar. Við gerum þó alltaf samning við slíkan umboðsmann eða gagnavinnsluaðila.

Fyrir viðkvæmar upplýsingar (þ.e. persónuupplýsingar sem innihalda upplýsingar um heilsufar, kynþátt eða þjóðernisuppruna, pólitískar skoðanir, trúarlegar eða heimspekilegar skoðanir, aðild að verkalýðsfélagi eða upplýsingar um kynlíf viðkomandi einstaklings) fáum við þitt ótvíræða samþykki (Opt-in) þegar þessar upplýsingar (i) eru afhentar þriðja aðila eða (ii) eru notaðar í öðrum tilgangi en þeim sem þær voru upphaflega safnað fyrir eða sem þú síðar hefur samþykkt með því að velja Opt-in. Ennfremur meðhöndlum við allar persónuupplýsingar sem við fáum frá þriðja aðila sem viðkvæmar ef þriðji aðilinn auðkennir og meðhöndlar þær sem viðkvæmar.

Við upplýsum þig hér með um kröfu um að birta persónuupplýsingar sem svar við löglegum beiðnum frá yfirvöldum, þar á meðal til að uppfylla kröfur um þjóðaröryggi eða löggæslu.

Við afhendingu persónuupplýsinga til þriðja aðila, sem er ábyrgðaraðili, fylgjum við Principals um tilkynningu og val. Að auki gerum við samning við þriðja aðilann sem er ábyrgur fyrir vinnslunni, sem


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

kveður á um að þessar upplýsingar megi aðeins vinna í takmörkuðum og tilgreindum tilgangi í samræmi við þitt samþykki og að móttakandinn veiti sama verndarstig og Principals DPF og tilkynni okkur ef það kemst að því að það geti ekki lengur uppfyllt þessa skuldbindingu. Samningurinn kveður á um að þriðji aðilinn, sem er ábyrgur, hætti vinnslunni eða grípi til annarra viðeigandi og sanngjarnra ráðstafana til að bæta úr ástandinu ef slík ákvörðun er tekin.

Við afhendingu persónuupplýsinga til þriðja aðila, sem starfar sem umboðsmaður eða gagnavinnsluaðili, (i) afhendum við aðeins þessar upplýsingar í takmörkuðum og tilgreindum tilgangi; (ii) tryggjum við að umboðsmaðurinn eða gagnavinnsluaðilinn sé skuldbundinn til að veita a.m.k. sama verndarstig, eins og DPF-Principals krefst; (iii) grípum við til viðeigandi og sanngjarnra ráðstafana til að tryggja að umboðsmaðurinn eða gagnavinnsluaðilinn vinni raunverulega með afhentar persónuupplýsingar á þann hátt sem er í samræmi við okkar skuldbindingar samkvæmt DPF-Principals; (iv) krefjumst við að umboðsmaðurinn eða gagnavinnsluaðilinn tilkynni stofnun okkar ef það kemst að því að það getur ekki lengur uppfyllt skuldbindinguna um að veita sama verndarstig eins og DPF-Principals krefst; (v) eftir slíka tilkynningu, einnig samkvæmt (iv), grípum við til viðeigandi og sanngjarnra ráðstafana til að stöðva óheimila vinnslu og bæta úr ástandinu; og (vi) veitum við DPF Department eftir beiðni samantekt eða fulltrúa eintak af viðeigandi ákvæðum um persónuvernd í samningi okkar við þennan umboðsmann.

Í samræmi við EU-U.S. DPF og/eða UK Extension to the EU-U.S. DPF og/eða Swiss-U.S. DPF skuldbindur stofnun okkar sig til að vinna með því ráði sem stofnað var af EUs databeskyttelsesmyndigheter og britiske Information Commissioner's Office (ICO) eða sveitska persónuverndarráðinu (EDÖB) og fylgja ráðleggingum þeirra varðandi óleystar kvartanir um meðhöndlun okkar á persónuupplýsingum sem við fáum í tengslum við vinnusambönd samkvæmt EU-U.S. DPF og UK Extension to the EU-U.S. DPF og Swiss-U.S. DPF.

Allir skráðir einstaklingar sem eru tímabundið í Evrópusambandinu (ESB), Evrópska efnahagssvæðinu (EES) eða Bretlandi, eða hafa lögheimili eða fasta búsetu þar, eiga rétt á þeim réttindum og réttindum skráðra einstaklinga sem birt eru í okkar Gagnsæisskjal, sem einnig stafar af 15. til 22. gr. GDPR, þar á meðal réttinn til aðgangs að persónuupplýsingum. Við höfum gert þessar upplýsingar aðgengilegar á öllum tungumálum ESB og EES. Enska útgáfan á við um Bretland.

Allir skráðir einstaklingar sem eru tímabundið búsettir í Sviss eða hafa lögheimili eða fasta búsetu þar eiga rétt á réttindum og réttindum skráðra einstaklinga samkvæmt svissneskum gagnaverndarlögum (DPA) og svissnesku gagnaverndarreglugerðinni (DPR) sem eru birt í gagnsæi okkar Skjal, þar á meðal rétt til aðgangs að persónuupplýsingum. Við höfum veitt þessar upplýsingar á þremur opinberum tungumálum Sviss (þýsku, ítölsku og frönsku).


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

# ICELANDIC: Upplýsingar um vinnslu persónuupplýsinga fyrir starfsmenn og umsækjendur (13. gr., 14 GDPR)

Kæri herra eða frú,

Persónuupplýsingar starfsmanna og umsækjenda verðskulda sérstaka vernd. Markmið okkar er að halda gagnaverndarstigi okkar í háum gæðaflokki. Þess vegna erum við reglulega að þróa hugmyndir okkar um gagnavernd og gagnaöryggi.

Við förum að sjálfsögðu eftir ákvæðum laga um persónuvernd. Samkvæmt 13. grein, 14 GDPR uppfylla ábyrgðaraðilar sérstakar upplýsingakröfur við vinnslu persónuupplýsinga. Þetta skjal uppfyllir þessar skyldur.

Hugtök lagareglugerðar eru flókin. Því miður var ekki hægt að sleppa notkun lagalegra hugtaka við gerð þessa skjals. Þess vegna viljum við benda þér á að þér er alltaf velkomið að hafa samband við okkur fyrir allar spurningar varðandi þetta skjal, hugtökin sem notuð eru eða samsetningar.

## I. Fylgni við upplýsingakröfur þegar persónuupplýsingum er safnað frá hinum skráða (13. gr. GDPR)

### A. Auðkenni og samskiptaupplýsingar ábyrgðaraðila (13. mgr. 13. gr. a GDPR)

Sjá fyrir ofan

### B. Samskiptaupplýsingar gagnaverndarfulltrúa (13. mgr. 1. gr. b GDPR)

Sjá fyrir ofan

### C. Tilgangur vinnslunnar sem persónuupplýsingarnar eru ætlaðar til sem og lagagrundvöllur vinnslunnar (13. gr. c GDPR)

Fyrir gögn umsækjanda er tilgangur gagnavinnslu að framkvæma athugun á umsókn á meðan á ráðningarferlinu stendur. Í þessu skyni vinnum við öll gögn sem þú gefur upp. Á grundvelli gagna sem lögð voru fram í ráðningarferlinu munum við athuga hvort þér sé boðið í atvinnuviðtal (hluti af valferlinu). Ef um er að ræða almennt hæfa umsækjendur, sérstaklega í tengslum við atvinnuviðtalið, vinnum við með tilteknar aðrar persónuupplýsingar sem þú gefur upp, sem eru nauðsynlegar fyrir val okkar. Ef þú ert ráðinn til okkar munu gögn umsækjanda sjálfkrafa breytast í starfsmannagögn. Sem hluti af ráðningarferlinu munum við vinna úr öðrum persónuupplýsingum um þig sem við biðjum um frá þér og


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

eru nauðsynlegar til að hefja eða uppfylla samning þinn (svo sem persónunúmer eða skattanúmer). Að því er varðar starfsmannaupplýsingar er tilgangur gagnavinnslu framkvæmd ráðningarsamnings eða samræmi við önnur lagaákvæði sem gilda um ráðningarsambandið ( td skattalög) sem og notkun persónuupplýsinga þinna til að framkvæma ráðningarsamninginn sem gerður var við þig. (td birting nafns þíns og tengiliðaupplýsinga innan fyrirtækisins eða til viðskiptavina). Gögn starfsmanna eru geymd eftir að ráðningarsambandi lýkur til að uppfylla lagalega varðveislutíma.

Lagagrundvöllur gagnavinnslu er 1. mgr. 6. gr. b GDPR, 2. mgr. 9. gr. b og h GDPR, 88. gr. (1) GDPR og landslöggjöf, svo sem fyrir Þýskaland Section 26 BDSG (Alríkisgagnaverndarlög).

## D. Flokkar viðtakenda persónuupplýsinganna (13. mgr. 1. gr. e GDPR)

Opinberir aðilar

Ytri stofnanir

Frekari ytri aðilar

Innri vinnsla

Vinnsla innan hóps

Önnur lík

Listi yfir vinnsluaðila okkar og viðtakendur gagna í þriðju löndum og, ef við á, alþjóðlegum stofnunum er annað hvort birtur á vefsíðu okkar eða hægt er að biðja um það frá okkur án endurgjalds. Vinsamlegast hafðu samband við gagnaverndarfulltrúa okkar til að biðja um þennan lista.

## E. Viðtakendur í þriðja landi og viðeigandi eða viðeigandi öryggisráðstafanir og leiðir til að fá afrit af þeim eða þar sem þeir hafa verið aðgengilegir (13. gr. . c GDPR)

Öll fyrirtæki og útibú sem eru hluti af samstæðu okkar (hér eftir kölluð "samstæðufyrirtæki") sem hafa starfsstöð eða skrifstofu í þriðja landi geta tilheyrt viðtakendum persónuupplýsinga. Hægt er að óska eftir lista yfir öll samstæðufyrirtæki eða viðtakendur hjá okkur.

Samkvæmt 1. mgr. 46. gr. GDPR má ábyrgðaraðili eða vinnsluaðili einungis flytja persónuupplýsingar til þriðja lands ef ábyrgðaraðili eða vinnsluaðili hefur veitt viðeigandi verndarráðstafanir og að því tilskildu að aðfararhæf réttindi skráðra einstaklinga og skilvirk réttarúrræði fyrir skráða einstaklinga séu tiltæk. Heimilt er að veita viðeigandi verndarráðstafanir án þess að krefjast sérstakrar heimildar frá eftirlitsyfirvaldi með stöðluðum samningsákvæðum, 2. mgr. 46. gr. lit. c GDPR.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

Samið er um staðlaða samningsákvæði Evrópusambandsins eða aðrar viðeigandi verndarráðstafanir við alla viðtakendur frá þriðju löndum fyrir fyrstu sendingu persónuupplýsinga. Þar af leiðandi er tryggt að viðeigandi verndarráðstafanir, framfylganleg réttindi skráðra einstaklinga og skilvirk réttarúrræði fyrir skráða einstaklinga séu tryggð. Sérhver skráður einstaklingur getur fengið afrit af stöðluðum samningsákvæðum frá okkur. Stöðluðu samningsákvæðin eru einnig fáanleg í Stjórnartíðindum Evrópusambandsins.

Grein 45(3) í almennu gagnaverndarreglugerðinni (GDPR) veitir framkvæmdastjórn Evrópusambandsins vald til að ákveða, með framkvæmdargerð, að ríki utan ESB tryggi fullnægjandi vernd. Þetta þýðir verndarstig fyrir persónuupplýsingar sem er í meginatriðum jafngilt verndarstigi innan ESB. Áhrif ákvarðana um fullnægjandi hæfi eru að persónuupplýsingar geta streymt óhindrað frá ESB (og Noregi, Liechtenstein og Íslandi) til þriðja lands án frekari hindrana. Svipaðar reglur gilda fyrir Bretland, Sviss og sum önnur lönd.

Þar sem framkvæmdastjórn Evrópusambandsins eða stjórnvöld annars lands ákváðu að þriðja land tryggi fullnægjandi vernd og gildur rammi er til staðar ( td gagnaverndarrammi ESB og Bandaríkjanna, gagnaverndarrammi Sviss og Bandaríkjanna, framlenging í Bretlandi við EU-US Data Privacy Framework), eru allar millifærslur af okkar hálfu til meðlima slíkra ramma (td sjálfvottaðra aðila) eingöngu byggðar á aðild þeirra aðila að viðkomandi ramma. Þar sem við eða einn úr hópnum okkar aðilar eru aðili að slíkum ramma, allar millifærslur til okkar eða hópeiningar okkar eru eingöngu byggðar á aðild aðila að slíkum ramma.

Allir skráðir einstaklingar geta fengið afrit af rammanum hjá okkur. Að auki eru rammana einnig aðgengileg í Stjórnartíðindum Evrópusambandsins eða í útgefnum lagagögnum eða á vefsíðum eftirlitsyfirvalda eða annarra lögbærra yfirvalda eða stofnana.

## F. Tímabil sem persónuupplýsingarnar verða geymdar í, eða ef það er ekki mögulegt, viðmiðin sem notuð eru til að ákvarða það tímabil (2. mgr. 13. gr. a GDPR)

Lengd geymslu persónuupplýsinga umsækjenda er 6 mánuðir. Fyrir starfsmannagögn gildir viðkomandi lögbundinn varðveislutími. Að þeim tíma liðnum er samsvarandi gögnum reglulega eytt, svo framarlega sem þau eru ekki lengur nauðsynleg til að uppfylla samninginn eða hefja samning.

## G. Til staðar er réttur til að krefja ábyrgðaraðila um aðgang að og leiðréttingu eða eyðingu persónuupplýsinga eða takmörkun á vinnslu varðandi hinn skráða eða til að andmæla vinnslu sem og réttur til gagnaflutnings (b-lið 2. mgr. 13. gr. GDPR)

Allir skráðir einstaklingar hafa eftirfarandi réttindi:


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

***Réttur til aðgangs***

Sérhver skráður einstaklingur á rétt á aðgangi að persónuupplýsingum um hann eða hana. Réttur til aðgangs nær til allra gagna sem við vinnum með. Rétturinn er hægt að nýta auðveldlega og með hæfilegu millibili, til þess að vera meðvitaður um og sannreyna lögmæti vinnslunnar (63. grein GDPR). Þessi réttur leiðir af 3. gr. 15 GDPR. Hinn skráði gæti haft samband við okkur til að nýta réttinn til aðgangs.

***Réttur til úrbóta***

Samkvæmt 16. grein 1. GDPR á hinn skráði rétt á að fá frá ábyrgðaraðila án ástæðulauss tafar leiðréttingu á ónákvæmum persónuupplýsingum um hann eða hana. Ennfremur kveður 16. gr. setning 2 GDPR á um að hinn skráði eigi rétt á, að teknu tilliti til tilgangs vinnslunnar, að fá ófullkomnar persónuupplýsingar fullnaðar, þar á meðal með því að leggja fram viðbótaryfirlýsingu. Hinn skráði getur haft samband við okkur til að nýta réttinn til úrbóta.

***Réttur til að eyða (réttur til að gleymast)***

Að auki eiga skráðir aðilar rétt á eyðingu og til að gleymast skv. 17 GDPR. Þennan rétt er einnig hægt að nýta með því að hafa samband við okkur. Á þessum tímapunkti viljum við þó benda á að þessi réttur á ekki við að svo miklu leyti sem vinnslan er nauðsynleg til að uppfylla lagaskyldu sem fyrirtæki okkar er háð, 3. mgr. 17. gr. lit. b GDPR. Þetta þýðir að við getum samþykkt umsókn um eyðingu aðeins eftir að lögbundinn varðveislutími er liðinn.

***Réttur til takmörkunar á vinnslu***

Samkvæmt 18. grein GDPR á hver skráður einstaklingur rétt á takmörkun á vinnslu. Heimilt er að krefjast takmörkunar á vinnslu ef eitthvert af skilyrðum 1. mgr. 18. gr. ad GDPR er uppfyllt. Hinn skráði gæti haft samband við okkur til að nýta réttinn til takmörkunar á vinnslu.

***Réttur til andmæla***

Jafnframt er gr. 21 GDPR tryggir andmælarétt. Hinn skráði gæti haft samband við okkur til að nýta andmælaréttinn.

***Réttur til gagnaflutnings***

gr. 20 GDPR veitir hinum skráða rétt til gagnaflutnings. Samkvæmt þessu ákvæði hefur hinn skráði með þeim skilyrðum sem mælt er fyrir um í 1. mgr. 20. gr. a og b GDPR réttur til að fá persónuupplýsingar um hann eða hana, sem hann eða hún hefur látið ábyrgðaraðila í té, á skipulögðu, almennu og véllesanlegu sniði og hafa rétt til að senda þær gögn til annars ábyrgðaraðila án hindrunar. frá ábyrgðaraðilanum sem persónuupplýsingarnar hafa verið veittar til. Hinn skráði gæti haft samband við okkur til að nýta réttinn til gagnaflutnings.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## H. Réttur til að afturkalla samþykki hvenær sem er, án þess að hafa áhrif á lögmæti vinnslu sem byggist á samþykki fyrir afturköllun þess, þar sem vinnslan byggist á 1. mgr. 6. gr. lit. GDPR eða 2. mgr. 9. gr. a GDPR (2. mgr. 13. gr. c GDPR)

Sé vinnsla persónuupplýsinga byggð á 2. gr. 6(1) lit. GDPR, sem er tilfellið, ef hinn skráði hefur veitt samþykki fyrir vinnslu persónuupplýsinga í einum eða fleiri tilteknum tilgangi eða byggist hún á 2. mgr. 9. gr. GDPR, sem kveður á um skýrt samþykki fyrir vinnslu sérstakra flokka persónuupplýsinga , hefur hinn skráði samkvæmt 7. gr. 3. setningu 1 GDPR rétt til að afturkalla samþykki sitt hvenær sem er.

Afturköllun samþykkis hefur ekki áhrif á lögmæti vinnslu sem byggist á samþykki fyrir afturköllun þess, 3. mgr. 7. gr. 2. setning GDPR. Það skal vera jafn auðvelt að afturkalla og gefa samþykki, gr. 7(3) Málsgrein 4 GDPR. Afturköllun samþykkis getur því alltaf farið fram á sama hátt og samþykki hefur verið veitt eða á annan hátt sem hinn skráði telur einfaldari. Í upplýsingasamfélagi nútímans er líklega einfaldasta leiðin til að afturkalla samþykki einfaldur tölvupóstur. Ef hinn skráði vill afturkalla samþykki sitt sem okkur hefur verið veitt nægir einfaldur tölvupóstur til okkar. Að öðrum kosti getur hinn skráði valið hvaða aðra leið sem er til að koma samþykki sínu til baka til okkar.

## I. Réttur til að leggja fram kvörtun til eftirlitsyfirvalds (Gr. 13(2) lit. d, 77(1) GDPR)

Sem ábyrgðaraðili er okkur skylt að tilkynna hinum skráða um réttinn til að leggja fram kvörtun til eftirlitsyfirvalds, 2. mgr. 13. gr. lit. d GDPR. Réttur til að leggja fram kvörtun til eftirlitsyfirvalds er stjórnað af 1. mgr. 77. gr. GDPR. Samkvæmt þessu ákvæði, með fyrirvara um önnur stjórnsýslu- eða dómstólaúrræði, skal sérhver skráður einstaklingur hafa rétt til að leggja fram kvörtun til eftirlitsyfirvalds, einkum í því aðildarríki þar sem hann hefur venjulega búsetu, vinnustað eða starfsstað. meint brot telji hinn skráði að vinnsla persónuupplýsinga um hann brjóti í bága við almenna persónuverndarreglugerð. Réttur til að leggja fram kvörtun til eftirlitsyfirvalds var einungis takmarkaður af lögum sambandsins á þann hátt að hann er aðeins hægt að beita fyrir einu eftirlitsyfirvaldi (141. greinar setning 1 GDPR). Þessari reglu er ætlað að forðast tvöfaldar kvartanir sama skráðs einstaklings í sama máli. Ef skráður einstaklingur vill leggja fram kvörtun vegna okkar, báðum við því um að hafa aðeins samband við eitt eftirlitsyfirvald.

## J. Veiting persónuupplýsinga sem lögbundin eða samningsbundin krafa; Krafa sem er nauðsynleg til að gera samning; Skylda hins skráða til að veita persónuupplýsingarnar; mögulegar afleiðingar þess að vanrækja slík gögn (2. gr. 13(2) lit. e GDPR)

Við skýrum að veiting persónuupplýsinga er að hluta til lögskyld ( td skattareglur) eða getur einnig stafað af samningsákvæðum (td upplýsingar um samningsaðilann).


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

Stundum getur verið nauðsynlegt að gera samning um að hinn skráði lætur okkur í té persónuupplýsingar sem við þurfum síðan að vinna úr. Hinum skráða er til dæmis skylt að láta okkur í té persónuupplýsingar þegar fyrirtæki okkar skrifar undir samning við hann eða hana. Vanskil persónuupplýsinga hefði þær afleiðingar að ekki væri hægt að gera samning við hinn skráða.

Áður en skráði einstaklingurinn veitir persónuupplýsingar þarf hann að hafa samband við okkur. Við skýrum fyrir hinum skráða hvort afhending persónuupplýsinganna sé áskilin samkvæmt lögum eða samningi eða sé nauðsynleg fyrir samningsgerð, hvort skylda sé til að veita persónuupplýsingarnar og afleiðingar þess að ekki sé veitt persónuupplýsingarnar. .

### K. Tilvist sjálfvirkrar ákvarðanatöku, þ.mt prófílgreiningar, sem um getur í 1. og 4. mgr. 22. gr. GDPR og, að minnsta kosti í þeim tilvikum, þýðingarmiklar upplýsingar um rökfræðina sem um er að ræða, svo og mikilvægi og fyrirhugaðar afleiðingar af slík vinnsla fyrir hinn skráða (2. mgr. 13. gr. f GDPR)

Sem ábyrgt fyrirtæki notum við venjulega ekki sjálfvirka ákvarðanatöku eða prófílgreiningu. Ef, í undantekningartilvikum, framkvæmum við sjálfvirka ákvarðanatöku eða prófílgreiningu munum við upplýsa hinn skráða annað hvort sérstaklega eða í gegnum undirkafla í persónuverndarstefnu okkar (á vefsíðu okkar). Í þessu tilviki á eftirfarandi við:

Sjálfvirk ákvarðanataka - þ.mt prófílgreining - getur átt sér stað ef (1) þetta er nauðsynlegt til að gera eða framkvæma samning milli hins skráða og okkar, eða (2) þetta er heimilað samkvæmt lögum sambandsins eða aðildarríkisins sem við eru háð og þar sem jafnframt er mælt fyrir um viðeigandi ráðstafanir til að standa vörð um réttindi og frelsi og lögmæta hagsmuni hins skráða; eða (3) þetta er byggt á skýru samþykki hins skráða.

Í þeim tilvikum sem um getur í a- og c-lið 22(2) (a) og (c) GDPR, munum við framkvæma viðeigandi ráðstafanir til að vernda réttindi og frelsi hins skráða og lögmæta hagsmuni. Í þessum tilvikum hefur þú rétt á að fá mannleg afskipti af hálfu ábyrgðaraðila, til að koma sjónarmiðum þínum á framfæri og andmæla ákvörðuninni.

Merkingarríkar upplýsingar um rökfræðina sem um er að ræða, svo og mikilvægi og fyrirhugaðar afleiðingar slíkrar vinnslu fyrir hinn skráða, eru settar fram í persónuverndarstefnu okkar.

## II. Fylgni við upplýsingakröfur þegar persónuupplýsingum er ekki safnað frá hinum skráða (14. gr. GDPR)


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## A. Auðkenni og samskiptaupplýsingar ábyrgðaraðila (14. mgr. 14. gr. a GDPR)

Sjá fyrir ofan

## B. Samskiptaupplýsingar persónuverndarfulltrúa (14. gr. b. GDPR)

Sjá fyrir ofan

## C. Tilgangur vinnslunnar sem persónuupplýsingarnar eru ætlaðar til sem og lagagrundvöllur vinnslunnar (14. gr. c GDPR)

Fyrir gögn umsækjanda sem ekki er safnað frá hinum skráða er tilgangur gagnavinnslunnar að framkvæma athugun á umsókninni meðan á ráðningarferlinu stendur. Í þessum tilgangi kunnum við að vinna úr gögnum sem ekki er safnað frá þér. Á grundvelli þeirra gagna sem unnið er með í ráðningarferlinu munum við athuga hvort þér sé boðið í atvinnuviðtal (hluti af valferlinu). Ef þú ert ráðinn til okkar munu gögn umsækjanda sjálfkrafa breytast í starfsmannagögn. Að því er varðar starfsmannaupplýsingar er tilgangur gagnavinnslu efndir ráðningarsamnings eða að farið sé að öðrum lagaákvæðum sem gilda um ráðningarsambandið. Gögn starfsmanna eru geymd eftir að ráðningarsambandi lýkur til að uppfylla lagalega varðveislutíma.

Lagagrundvöllur gagnavinnslu er 1. mgr. 6. gr. b og f GDPR, 2. mgr. 9. gr. b og h GDPR, 88. gr. (1) GDPR og landslöggjöf, svo sem fyrir Þýskaland Section 26 BDSG (Alríkisgagnaverndarlög).

## D. Flokkar persónuupplýsinga sem málið varðar (14. gr. lit. d GDPR)

Gögn umsækjanda

Gögn starfsmanna

## E. Flokkar viðtakenda persónuupplýsinganna (14. gr. 14. gr. e GDPR)

Opinberir aðilar

Ytri stofnanir

Frekari ytri aðilar

Innri vinnsla


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

Vinnsla innan hóps

Önnur lík

Listi yfir vinnsluaðila okkar og viðtakendur gagna í þriðju löndum og, ef við á, alþjóðlegum stofnunum er annað hvort birtur á vefsíðu okkar eða hægt er að biðja um það frá okkur án endurgjalds. Vinsamlegast hafðu samband við gagnaverndarfulltrúa okkar til að biðja um þennan lista.

## F. Viðtakendur í þriðja landi og viðeigandi eða viðeigandi verndarráðstafanir og leiðir til að fá afrit af þeim eða þar sem þeir hafa verið aðgengilegir (14. gr. f., 1. mgr. . c GDPR)

Öll fyrirtæki og útibú sem eru hluti af samstæðu okkar (hér eftir kölluð "samstæðufyrirtæki") sem hafa starfsstöð eða skrifstofu í þriðja landi geta tilheyrt viðtakendum persónuupplýsinga. Hægt er að óska eftir lista yfir öll samstæðufyrirtæki eða viðtakendur hjá okkur.

Samkvæmt 1. mgr. 46. gr. GDPR má ábyrgðaraðili eða vinnsluaðili einungis flytja persónuupplýsingar til þriðja lands ef ábyrgðaraðili eða vinnsluaðili hefur veitt viðeigandi verndarráðstafanir og að því tilskildu að aðfararhæf réttindi skráðra einstaklinga og skilvirk réttarúrræði fyrir skráða einstaklinga séu tiltæk. Veita má viðeigandi verndarráðstafanir án sérstakrar heimildar frá eftirlitsyfirvaldi með stöðluðum gagnaverndarákvæðum, 2. mgr. 46. gr. lit. c GDPR.

staðlaða samningsákvæði Evrópusambandsins eða aðrar viðeigandi verndarráðstafanir við alla viðtakendur frá þriðju löndum fyrir fyrstu sendingu persónuupplýsinga. Þar af leiðandi er tryggt að viðeigandi verndarráðstafanir, framfylganleg réttindi skráðra einstaklinga og skilvirk réttarúrræði fyrir skráða einstaklinga séu tryggð. Sérhver skráður einstaklingur getur fengið afrit af stöðluðum samningsákvæðum frá okkur. Stöðluðu samningsákvæðin eru einnig fáanleg í Stjórnartíðindum Evrópusambandsins.

Grein 45(3) í almennu gagnaverndarreglugerðinni (GDPR) veitir framkvæmdastjórn Evrópusambandsins vald til að ákveða, með framkvæmdargerð, að ríki utan ESB tryggi fullnægjandi vernd. Þetta þýðir verndarstig fyrir persónuupplýsingar sem er í meginatriðum jafngilt verndarstigi innan ESB. Áhrif ákvarðana um fullnægjandi hæfi eru að persónuupplýsingar geta streymt óhindrað frá ESB (og Noregi, Liechtenstein og Íslandi) til þriðja lands án frekari hindrana. Svipaðar reglur gilda fyrir Bretland, Sviss og sum önnur lönd.

Þar sem framkvæmdastjórn Evrópusambandsins eða stjórnvöld annars lands ákváðu að þriðja land tryggi fullnægjandi vernd og gildur rammi er til staðar ( td gagnaverndarrammi ESB og Bandaríkjanna, gagnaverndarrammi Sviss og Bandaríkjanna, framlenging í Bretlandi við EU-US Data Privacy Framework), eru allar millifærslur af okkar hálfu til meðlima slíkra ramma (td sjálfvottaðra aðila) eingöngu byggðar á aðild þeirra aðila að viðkomandi ramma. Þar sem við eða einn úr hópnum okkar aðilar eru aðili


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

að slíkum ramma, allar millifærslur til okkar eða hópeiningar okkar eru eingöngu byggðar á aðild aðila að slíkum ramma.

Allir skráðir einstaklingar geta fengið afrit af rammanum hjá okkur. Að auki eru rammana einnig aðgengileg í Stjórnartíðindum Evrópusambandsins eða í útgefnum lagagögnum eða á vefsíðum eftirlitsyfirvalda eða annarra lögbærra yfirvalda eða stofnana.

## G. Tímabil sem persónuupplýsingarnar verða geymdar í, eða ef það er ekki mögulegt, viðmiðin sem notuð eru til að ákvarða það tímabil (2. mgr. 14. gr. a GDPR)

Lengd geymslu persónuupplýsinga umsækjenda er 6 mánuðir. Fyrir starfsmannagögn gildir viðkomandi lögbundinn varðveislutími. Að þeim tíma liðnum er samsvarandi gögnum reglulega eytt, svo framarlega sem þau eru ekki lengur nauðsynleg til að uppfylla samninginn eða hefja samning.

## H. Tilkynning um lögmæta hagsmuni sem ábyrgðaraðili eða þriðji aðili hefur fylgst með ef vinnslan byggist á 1. mgr. 6. gr. lit. f GDPR (Gr. 14(2) lit. b GDPR)

Samkvæmt 1. mgr. 6. gr. f GDPR skal vinnslan aðeins vera lögmæt ef vinnslan er nauðsynleg í þeim tilgangi að gæta lögmætra hagsmuna sem ábyrgðaraðili eða þriðji aðili hagsmunir að, nema hagsmunir eða grundvallarréttindi og frelsi hins skráða sem krefjast verndar vegi þyngra. af persónuupplýsingum. Samkvæmt ákvæði 47. setningu 2 GDPR gætu lögmætir hagsmunir verið fyrir hendi þar sem viðeigandi og viðeigandi tengsl eru á milli hins skráða og ábyrgðaraðilans, td í aðstæðum þar sem hinn skráði er viðskiptavinur ábyrgðaraðilans. Í öllum tilvikum þar sem fyrirtæki okkar vinnur gögn umsækjanda á grundvelli 1. mgr. 6. gr. f GDPR eru lögmætir hagsmunir okkar ráðning viðeigandi starfsfólks og fagfólks.

## I. Til staðar er réttur til að óska eftir aðgangi að og leiðréttingu eða eyðingu persónuupplýsinga eða takmörkun á vinnslu varðandi hinn skráða og til að andmæla vinnslu frá ábyrgðaraðila sem og réttur til gagnaflutnings (c-liður 2. mgr. 14. gr. GDPR)

Allir skráðir einstaklingar hafa eftirfarandi réttindi:

***Réttur til aðgangs***

Sérhver skráður einstaklingur á rétt á aðgangi að persónuupplýsingum um hann eða hana. Réttur til aðgangs nær til allra gagna sem við vinnum með. Rétturinn er hægt að nýta auðveldlega og með hæfilegu millibili, til þess að vera meðvitaður um og sannreyna lögmæti vinnslunnar (63. grein GDPR). Þessi réttur leiðir af 3. gr. 15 GDPR. Hinn skráði gæti haft samband við okkur til að nýta réttinn til aðgangs.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

***Réttur til úrbóta***

Samkvæmt 16. grein 1. GDPR á hinn skráði rétt á að fá frá ábyrgðaraðila án ástæðulauss tafar leiðréttingu á ónákvæmum persónuupplýsingum um hann eða hana. Ennfremur kveður 16. gr. setning 2 GDPR á um að hinn skráði eigi rétt á, að teknu tilliti til tilgangs vinnslunnar, að fá ófullkomnar persónuupplýsingar fullnaðar, þar á meðal með því að leggja fram viðbótaryfirlýsingu. Hinn skráði getur haft samband við okkur til að nýta réttinn til úrbóta.

***Réttur til að eyða (réttur til að gleymast)***

Að auki eiga skráðir aðilar rétt á eyðingu og til að gleymast skv. 17 GDPR. Þennan rétt er einnig hægt að nýta með því að hafa samband við okkur. Á þessum tímapunkti viljum við þó benda á að þessi réttur á ekki við að svo miklu leyti sem vinnslan er nauðsynleg til að uppfylla lagaskyldu sem fyrirtæki okkar er háð, 3. mgr. 17. gr. lit. b GDPR. Þetta þýðir að við getum samþykkt umsókn um eyðingu aðeins eftir að lögbundinn varðveislutími er liðinn.

***Réttur til takmörkunar á vinnslu***

Samkvæmt 18. grein GDPR á hver skráður einstaklingur rétt á takmörkun á vinnslu. Heimilt er að krefjast takmörkunar á vinnslu ef eitthvert af skilyrðum 1. mgr. 18. gr. ad GDPR er uppfyllt. Hinn skráði gæti haft samband við okkur til að nýta réttinn til takmörkunar á vinnslu.

***Réttur til andmæla***

Jafnframt er gr. 21 GDPR tryggir andmælarétt. Hinn skráði gæti haft samband við okkur til að nýta andmælaréttinn.

***Réttur til gagnaflutnings***

gr. 20 GDPR veitir hinum skráða rétt til gagnaflutnings. Samkvæmt þessu ákvæði hefur hinn skráði með þeim skilyrðum sem mælt er fyrir um í 1. mgr. 20. gr. a og b GDPR réttur til að fá persónuupplýsingar um hann eða hana, sem hann eða hún hefur látið ábyrgðaraðila í té, á skipulögðu, almennu og véllesanlegu sniði og hafa rétt til að senda þær gögn til annars ábyrgðaraðila án hindrunar. frá ábyrgðaraðilanum sem persónuupplýsingarnar hafa verið veittar til. Hinn skráði gæti haft samband við okkur til að nýta réttinn til gagnaflutnings.

## J. Réttur til að afturkalla samþykki hvenær sem er, án þess að það hafi áhrif á lögmæti vinnslu sem byggist á samþykki fyrir afturköllun þess, þar sem vinnslan byggist á 1. mgr. 6. gr. lit. a eða 2. mgr. 9. gr. a GDPR (Gr. 14(2) lit. d GDPR)

Sé vinnsla persónuupplýsinga byggð á 2. gr. 6(1) lit. GDPR, sem er tilfellið, ef hinn skráði hefur veitt samþykki fyrir vinnslu persónuupplýsinga í einum eða fleiri tilteknum tilgangi eða byggist hún á 2. mgr. 9. gr. GDPR, sem kveður á um skýrt samþykki fyrir vinnslu sérstakra flokka persónuupplýsinga, hefur hinn skráði samkvæmt 7. gr. 3. setningu 1 GDPR rétt til að afturkalla samþykki sitt hvenær sem er.

Afturköllun samþykkis hefur ekki áhrif á lögmæti vinnslu sem byggist á samþykki fyrir afturköllun þess, 3. mgr. 7. gr. 2. setning GDPR. Það skal vera jafn auðvelt að afturkalla og gefa samþykki, gr. 7(3) Málsgrein


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

4 GDPR. Afturköllun samþykkis getur því alltaf farið fram á sama hátt og samþykki hefur verið veitt eða á annan hátt sem hinn skráði telur einfaldari. Í upplýsingasamfélagi nútímans er líklega einfaldasta leiðin til að afturkalla samþykki einfaldur tölvupóstur. Ef hinn skráði vill afturkalla samþykki sitt sem okkur hefur verið veitt nægir einfaldur tölvupóstur til okkar. Að öðrum kosti getur hinn skráði valið hvaða aðra leið sem er til að koma samþykki sínu til baka til okkar.

## K. Réttur til að leggja fram kvörtun til eftirlitsyfirvalds (2. mgr. 14. gr. e, 77(1) GDPR)

Sem ábyrgðaraðili er okkur skylt að tilkynna hinum skráða um réttinn til að leggja fram kvörtun til eftirlitsyfirvalds, 2. mgr. 14. gr. lit. e GDPR. Réttur til að leggja fram kvörtun til eftirlitsyfirvalds er stjórnað af 1. mgr. 77. gr. GDPR. Samkvæmt þessu ákvæði, með fyrirvara um önnur stjórnsýslu- eða dómstólaúrræði, skal sérhver skráður einstaklingur hafa rétt til að leggja fram kvörtun til eftirlitsyfirvalds, einkum í því aðildarríki þar sem hann hefur venjulega búsetu, vinnustað eða starfsstað. meint brot telji hinn skráði að vinnsla persónuupplýsinga um hann brjóti í bága við almenna persónuverndarreglugerð. Réttur til að leggja fram kvörtun til eftirlitsyfirvalds var einungis takmarkaður af lögum sambandsins á þann hátt að hann er aðeins hægt að beita fyrir einu eftirlitsyfirvaldi (141. greinar setning 1 GDPR). Þessari reglu er ætlað að forðast tvöfaldar kvartanir sama skráðs einstaklings í sama máli. Ef skráður einstaklingur vill leggja fram kvörtun vegna okkar, báðum við því um að hafa aðeins samband við eitt eftirlitsyfirvald.

## L. Uppruni persónuupplýsinganna, og ef við á, hvort þær komu frá opinberum aðgengilegum heimildum (2. mgr. 14. gr. f GDPR)

Í grundvallaratriðum er persónuupplýsingum safnað beint frá hinum skráða eða í samvinnu við yfirvald ( td öflun upplýsinga úr opinberri skrá). Aðrar upplýsingar um skráða einstaklinga eru stafar af millifærslum samstæðufélaga. Í samhengi við þessar almennu upplýsingar er nafngift á nákvæmum heimildum sem persónuupplýsingar eru upprunnar úr annaðhvort ómögulegt eða myndi fela í sér óhóflega fyrirhöfn í skilningi gr. 14(5) lit. b GDPR. Í grundvallaratriðum söfnum við ekki persónuupplýsingum frá opinberum aðgengilegum aðilum.

Allir skráðir einstaklingar geta haft samband við okkur hvenær sem er til að fá ítarlegri upplýsingar um nákvæmar heimildir persónuupplýsinga um hann eða hana. Ef ekki er hægt að veita hinum skráða uppruna persónuupplýsinganna vegna þess að ýmsar heimildir hafa verið notaðar, ætti að veita almennar upplýsingar (61. setning 4. GDPR).


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## M. Tilvist sjálfvirkrar ákvarðanatöku, þ.mt prófílgreiningar, sem um getur í 1. og 4. mgr. 22. gr. GDPR og, að minnsta kosti í þeim tilvikum, þýðingarmiklar upplýsingar um rökfræðina sem um er að ræða, svo og mikilvægi og fyrirhugaðar afleiðingar af slík vinnsla fyrir hinn skráða (2. mgr. 14. gr. g GDPR)

Sem ábyrgt fyrirtæki notum við venjulega ekki sjálfvirka ákvarðanatöku eða prófílgreiningu. Ef, í undantekningartilvikum, framkvæmum við sjálfvirka ákvarðanatöku eða prófílgreiningu munum við upplýsa hinn skráða annað hvort sérstaklega eða í gegnum undirkafla í persónuverndarstefnu okkar (á vefsíðu okkar). Í þessu tilviki á eftirfarandi við:

Sjálfvirk ákvarðanataka - þ.mt prófílgreining - getur átt sér stað ef (1) þetta er nauðsynlegt til að gera eða framkvæma samning milli hins skráða og okkar, eða (2) þetta er heimilað samkvæmt lögum sambandsins eða aðildarríkisins sem við eru háð og þar sem jafnframt er mælt fyrir um viðeigandi ráðstafanir til að standa vörð um réttindi og frelsi og lögmæta hagsmuni hins skráða; eða (3) þetta er byggt á skýru samþykki hins skráða.

Í þeim tilvikum sem um getur í a- og c-lið 22(2) (a) og (c) GDPR, munum við framkvæma viðeigandi ráðstafanir til að vernda réttindi og frelsi hins skráða og lögmæta hagsmuni. Í þessum tilvikum hefur þú rétt á að fá mannleg afskipti af hálfu ábyrgðaraðila, til að koma sjónarmiðum þínum á framfæri og andmæla ákvörðuninni.

Merkingarríkar upplýsingar um rökfræðina sem um er að ræða, svo og mikilvægi og fyrirhugaðar afleiðingar slíkrar vinnslu fyrir hinn skráða, eru settar fram í persónuverndarstefnu okkar.

# III. EU-U.S. Data Privacy Framework (EU-U.S. DPF), UK Extension to the EU-U.S. DPF, Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF)

Ef stofnun okkar er vottaður aðili að EU-U.S. Data Privacy Framework (EU-U.S. DPF) og/eða UK Extension to the EU-U.S. DPF og/eða Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF) gildir eftirfarandi:

Við fylgjum EU-U.S. Data Privacy Framework (EU-U.S. DPF) og UK Extension to the EU-U.S. DPF sem og Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF), eins og það er sett af U.S. Department of Commerce. Fyrirtækið okkar hefur staðfest við bandarísk viðskiptaráðuneytið að það fylgi EU-U.S. Data Privacy Framework Principles (EU-U.S. DPF Principles) varðandi vinnslu persónuupplýsinga sem það fær frá Evrópusambandinu og Bretlandi samkvæmt EU-U.S. DPF og UK Extension to the EU-U.S. DPF. Fyrirtækið okkar hefur staðfest við bandarísk viðskiptaráðuneytið að það fylgi Swiss-U.S. Data Privacy Framework Principles (Swiss-U.S. DPF Principles) varðandi vinnslu persónuupplýsinga sem það fær frá Sviss samkvæmt Swiss-U.S. DPF. Ef árekstur er á milli ákvæða persónuverndarstefnu okkar og EU-U.S. DPF Principles og/eða Swiss-U.S. DPF Principles, eru Principles ráðandi.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

Til að fá frekari upplýsingar um Data Privacy Framework (DPF) forritið og til að skoða vottun okkar, vinsamlegast heimsækið https://www.dataprivacyframework.gov/.

Aðrar bandarískar einingar eða dótturfélög fyrirtækisins okkar, sem einnig fylgja EU-U.S. DPF Principals, þar á meðal UK Extension to the EU-U.S. DPF og Swiss-U.S. DPF Principals, ef þau eru til, eru nefnd í persónuverndarstefnu okkar.

Í samræmi við EU-U.S. DPF og UK Extension to the EU-U.S. DPF sem og Swiss-U.S. DPF skuldbindur fyrirtækið okkar sig til að vinna með því ráðinu sem stofnað var af persónuverndaryfirvöldum ESB og breska Information Commissioner's Office (ICO) sem og svissneska persónuverndarráðinu (EDÖB) og fylgja ráðleggingum þeirra varðandi óleystar kvartanir um meðhöndlun okkar á persónuupplýsingum sem við fáum samkvæmt EU-U.S. DPF og UK Extension to the EU-U.S. DPF og Swiss-U.S. DPF.

Við upplýsum viðkomandi einstaklinga um viðeigandi evrópsk persónuverndaryfirvöld sem eru ábyrg fyrir meðhöndlun kvartana um meðhöndlun fyrirtækisins okkar á persónuupplýsingum, í efri hluta þessa gagnsæisdokuments og um að við bjóðum viðkomandi einstaklingum upp á viðeigandi og ókeypis réttarúrræði.

Við upplýsum alla viðkomandi einstaklinga um að fyrirtækið okkar sé undir rannsóknar- og framkvæmdarvaldi Federal Trade Commission (FTC).

Viðkomandi einstaklingar hafa, við tilteknar aðstæður, möguleika á að nýta bindandi gerðardóm. Stofnun okkar er skuldbundin til að leysa kröfur og uppfylla skilyrðin í viðauka I við DPF-Principals, að því gefnu að viðkomandi einstaklingur hafi óskað eftir bindandi gerðardómi með því að tilkynna stofnun okkar og fylgja verklagi og skilyrðum í viðauka I við Principals.

Við upplýsum hér með alla viðkomandi einstaklinga um ábyrgð stofnunar okkar í tilfelli afhendingar persónuupplýsinga til þriðja aðila.

Fyrir spurningar frá viðkomandi einstaklingum eða persónuverndaryfirvöldum höfum við útnefnt þá staðbundnu fulltrúa sem nefndir eru í efri hluta þessa gagnsæisdokuments.

Við bjóðum þér að velja (Opt-out), hvort persónuupplýsingar þínar (i) séu afhentar þriðja aðila eða (ii) notaðar í tilgangi sem er verulega frábrugðinn þeim tilgangi/tilgangum sem þær voru upphaflega safnað fyrir eða síðar samþykktar af þér. Skýrt, vel sýnilegt og auðvelt aðgengilegt kerfi til að framkvæma val þitt felst í því að hafa samband við persónuverndarfulltrúa okkar (DSB) með tölvupósti. Þú hefur ekki möguleika á að velja, og við erum ekki heldur skuldbundin til þess, ef gögnin eru afhent þriðja aðila sem starfar sem umboðsmaður eða gagnavinnsluaðili í okkar umboði og samkvæmt fyrirmælum okkar. Við gerum þó alltaf samning við slíkan umboðsmann eða gagnavinnsluaðila.

Fyrir viðkvæmar upplýsingar (þ.e. persónuupplýsingar sem innihalda upplýsingar um heilsufar, kynþátt eða þjóðernisuppruna, pólitískar skoðanir, trúarlegar eða heimspekilegar skoðanir, aðild að verkalýðsfélagi eða upplýsingar um kynlíf viðkomandi einstaklings) fáum við þitt ótvíræða samþykki (Opt-in) þegar þessar upplýsingar (i) eru afhentar þriðja aðila eða (ii) eru notaðar í öðrum tilgangi en þeim sem


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

þær voru upphaflega safnað fyrir eða sem þú síðar hefur samþykkt með því að velja Opt-in. Ennfremur meðhöndlum við allar persónuupplýsingar sem við fáum frá þriðja aðila sem viðkvæmar ef þriðji aðilinn auðkennir og meðhöndlar þær sem viðkvæmar.

Við upplýsum þig hér með um kröfu um að birta persónuupplýsingar sem svar við löglegum beiðnum frá yfirvöldum, þar á meðal til að uppfylla kröfur um þjóðaröryggi eða löggæslu.

Við afhendingu persónuupplýsinga til þriðja aðila, sem er ábyrgðaraðili, fylgjum við Principals um tilkynningu og val. Að auki gerum við samning við þriðja aðilann sem er ábyrgur fyrir vinnslunni, sem kveður á um að þessar upplýsingar megi aðeins vinna í takmörkuðum og tilgreindum tilgangi í samræmi við þitt samþykki og að móttakandinn veiti sama verndarstig og Principals DPF og tilkynni okkur ef það kemst að því að það geti ekki lengur uppfyllt þessa skuldbindingu. Samningurinn kveður á um að þriðji aðilinn, sem er ábyrgur, hætti vinnslunni eða grípi til annarra viðeigandi og sanngjarnra ráðstafana til að bæta úr ástandinu ef slík ákvörðun er tekin.

Við afhendingu persónuupplýsinga til þriðja aðila, sem starfar sem umboðsmaður eða gagnavinnsluaðili, (i) afhendum við aðeins þessar upplýsingar í takmörkuðum og tilgreindum tilgangi; (ii) tryggjum við að umboðsmaðurinn eða gagnavinnsluaðilinn sé skuldbundinn til að veita a.m.k. sama verndarstig, eins og DPF-Principals krefst; (iii) grípum við til viðeigandi og sanngjarnra ráðstafana til að tryggja að umboðsmaðurinn eða gagnavinnsluaðilinn vinni raunverulega með afhentar persónuupplýsingar á þann hátt sem er í samræmi við okkar skuldbindingar samkvæmt DPF-Principals; (iv) krefjumst við að umboðsmaðurinn eða gagnavinnsluaðilinn tilkynni stofnun okkar ef það kemst að því að það getur ekki lengur uppfyllt skuldbindinguna um að veita sama verndarstig eins og DPF-Principals krefst; (v) eftir slíka tilkynningu, einnig samkvæmt (iv), grípum við til viðeigandi og sanngjarnra ráðstafana til að stöðva óheimila vinnslu og bæta úr ástandinu; og (vi) veitum við DPF Department eftir beiðni samantekt eða fulltrúa eintak af viðeigandi ákvæðum um persónuvernd í samningi okkar við þennan umboðsmann.

Í samræmi við EU-U.S. DPF og/eða UK Extension to the EU-U.S. DPF og/eða Swiss-U.S. DPF skuldbindur stofnun okkar sig til að vinna með því ráði sem stofnað var af EUs databeskyttelsesmyndigheter og britiske Information Commissioner's Office (ICO) eða sveitska persónuverndarráðinu (EDÖB) og fylgja ráðleggingum þeirra varðandi óleystar kvartanir um meðhöndlun okkar á persónuupplýsingum sem við fáum í tengslum við vinnusambönd samkvæmt EU-U.S. DPF og UK Extension to the EU-U.S. DPF og Swiss-U.S. DPF.

Allir skráðir einstaklingar sem eru tímabundið í Evrópusambandinu (ESB), Evrópska efnahagssvæðinu (EES) eða Bretlandi, eða hafa lögheimili eða fasta búsetu þar, eiga rétt á þeim réttindum og réttindum skráðra einstaklinga sem birt eru í okkar Gagnsæisskjal, sem einnig stafar af 15. til 22. gr. GDPR, þar á meðal réttinn til aðgangs að persónuupplýsingum. Við höfum gert þessar upplýsingar aðgengilegar á öllum tungumálum ESB og EES. Enska útgáfan á við um Bretland.

Allir skráðir einstaklingar sem eru tímabundið búsettir í Sviss eða hafa lögheimili eða fasta búsetu þar eiga rétt á réttindum og réttindum skráðra einstaklinga samkvæmt svissneskum gagnaverndarlögum (DPA) og svissnesku gagnaverndarreglugerðinni (DPR) sem eru birt í gagnsæi okkar Skjal, þar á meðal


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

rétt til aðgangs að persónuupplýsingum. Við höfum veitt þessar upplýsingar á þremur opinberum tungumálum Sviss (þýsku, ítölsku og frönsku).


Powered by ICB International Certification Body.
Document Owner: Heiko Maniero.
Information Contained: Business Data
© All rights reserved by Heiko Maniero.
Approved by: Heiko Maniero, Ulrich Baumann.
Date: 2026-10-27

# ENGLISH: California-Specific Description of Consumers' Privacy Rights (CCPA/CPRA)

Dear Sir or Madam,

The protection of Personal Information and the Security and Integrity of our IT infrastructure are very important to our Business.

Of course, our Business (in the following "we," "us," "our," or "Business") is in full compliance with all obligations imposed by the California Consumer Privacy Act of 2018 (CCPA), as amended or superseded from time to time, including, but not limited to, the California Privacy Rights Act of 2020 (CPRA). According to CCPA, a Business that Controls the Collection of a Consumer's Personal Information shall, at or before the point of Collection, inform the Consumer (in the following "you," or "your") of certain aspects of its processing activities. This publication was drafted to fulfill these obligations.

The terminology of legal regulations is complicated. Unfortunately, the use of legal terms could not be dispensed with in the preparation of this publication. Therefore, we would like to point out that you are always welcome to contact us for all questions concerning this publication, used terms or formulations.

**Data Protection Legislation** means CCPA and CPRA as well as any regulation adopted, published, administered, implemented, or enforced by the California Privacy Protection Agency or by the Attorney General to further the Purposes of CCPA and/or CPRA, and any related case-law.

In this publication and in CCPA related written or verbal communication the terms **Advertising and Marketing, Aggregate Consumer Information, Biometric Information, Business, Business Associate, Business Controller Information, Business Purpose, Collected, Collection, Collects, Commercial Credit Reporting Agency, Commercial Purposes, Common Branding, Consent, Consumer, Consumer Privacy Fund, Contractor, Control, Controlled, Covered Person, Cross-Context Behavioral Advertising, Dark Pattern, Deidentified, Designated Methods For Submitting Requests, Device, Director, Family, Fraudulent Concealment, Health Care Operations, Homepage, Household, Identifiable Private Information, Independent Contractor, Individually Identifiable Health Information, Infer, Inference, Intentionally Interacts, Management Employee, Medical Information, NonPersonalized Advertising, Officer, Owner, Ownership Information, Patient Information, Payment, Person, Personal Information, Precise Geolocation, Processing, Profiling, Protected Health Information, Provider Of Health Care, Pseudonymization, Pseudonymize, Publicly Available, Reidentify, Research, Right To Opt-Out, Sale, Security and Integrity, Sell, Selling, Sensitive Personal Information, Service, Services, Share, Shared, Sharing, Sold, Specific Pieces Of Information, Specific Pieces Of Information Obtained From The Consumer, Third Party, Treatment, Unique Identifier, Unique Personal Identifier, Vehicle Information, Verifiable Consumer Request, Vessel Dealer, Vessel Information** and **all other terms defined** by or under Data Protection Legislation shall have the meanings given to them by Data Protection Legislation.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

**Consumer Data** has the meaning given by Data Protection Legislation.

**Customer Data** means data about customers of the Business, including, but not limited to, contact information such as phone numbers and email addresses, contact history, billing information as well as all other data and shall include Personal Information that is collected by the Business about a natural person in the course of the natural person acting as an employee of, owner of, director of, officer of, medical staff member of, or independent contractor of, the customer to the extent that the natural person's personal information is collected and used by the Business solely within the context of the natural person's role or former role as an employee of, owner of, director of, officer of, medical staff member of, or an independent contractor of, the customer.

**Data Of Potential Customers** means data about potential customers of the Business, including, but not limited to, contact information such as phone numbers and email addresses, contact history as well as all other data and shall include Personal Information that is collected by the Business about a natural person in the course of the natural person acting as an employee of, owner of, director of, officer of, medical staff member of, or independent contractor of, the potential customer to the extent that the natural person's personal information is collected and used by the Business solely within the context of the natural person's role or former role as an employee of, owner of, director of, officer of, medical staff member of, or an independent contractor of, the potential customer.

**Data Of Suppliers** means data about suppliers, Service Providers and Contractors of the Business, including, but not limited to, contact information such as phone numbers and email addresses, contact history, delivery or service history as well as all other data and shall include Personal Information that is collected by the Business about a natural person in the course of the natural person acting as an employee of, owner of, director of, officer of, medical staff member of, or independent contractor of, the supplier to the extent that the natural person's personal information is collected and used by the Business solely within the context of the natural person's role or former role as an employee of, owner of, director of, officer of, medical staff member of, or an independent contractor of, the supplier.

**Data Of Employees** means Personal Information that is collected by the Business about a natural person in the course of the natural person acting as a job applicant to, an employee of, owner of, director of, officer of, medical staff member of, the Business to the extent that the natural person's personal information is collected and used by the Business solely within the context of the natural person's role or former role as a job applicant to, an employee of, owner of, director of, officer of, or medical staff member of, the Business.

**Employer Of The Consumer** means any company, corporation or other body corporate, partnership, sole proprietorship, nonprofit, or government agency wherever and however incorporated or established that a natural person is acting for or on behalf, including, an employee of, owner of, director of, officer of, medical staff member of, or independent contractor of, that organisation.

**Personal Information** shall include **Sensitive Personal Information**, where required and/ or indicated.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

# I. General Information about the Business and the Privacy Officer

## A. Identity and the contact details of the Business

See above

## B. Contact details of the Privacy Officer

See above

# II. General Duties of Businesses that Collect Personal Information (1798.100 CCPA)

## A. Categories of Personal Information to be Collected (1798.100 (a) (1) CCPA):

The General Categories of Personal Information to be Collected are Consumer Data, Customer Data, Data Of Potential Customers, Data Of Employees, and Data Of Suppliers. Under these General Categories we are going to collect, subject to the information we obtain from you directly, or that our Service Providers and/or Contractors obtained from you for a Business Purpose on behalf of us, or that we Collect from Publicly Available sources, Third Parties, Service Providers and/or Contractors, the following Categories of Personal Information:

1. Advertising and Marketing (in Categories: Consumer Data, Customer Data, Data Of Potential Customers, Data Of Suppliers),
2. Cross-Context Behavioral Advertising (in Categories: Consumer Data, Customer Data, Data Of Potential Customers, Data Of Suppliers),
3. Aggregate Consumer Information (in Categories: Consumer Data, Customer Data, Data Of Potential Customers, Data Of Employees, Data Of Suppliers),
4. Biometric Information (in Category: Data Of Employees, e.g., fingerprints and face ID for access Control, entry Control and other security Purposes),
5. Personal Information, such as a real name, alias, postal address, Unique Personal Identifier, online identifier, Internet Protocol address, email address, account name, social security number, driver's license number, passport number, or other similar identifiers (in Categories: Consumer Data, Customer Data, Data Of Potential Customers, Data Of Employees, Data Of Suppliers),
6. commercial information, including records of Personal property, products or Services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies (in Categories: Consumer Data, Customer Data, Data Of Potential Customers, Data Of Suppliers),
7. internet or other electronic network activity information, including, but not limited to, browsing history, search history, and information regarding a Consumer's interaction with an internet


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

website application, or advertisement (in Categories: Consumer Data, Customer Data, Data Of Potential Customers, Data Of Employees, Data Of Suppliers),

8. geolocation data (in Categories: Consumer Data, Customer Data, Data Of Potential Customers, Data Of Employees, Data Of Suppliers),
9. audio, electronic, visual, thermal, olfactory, or similar information (in Categories: Consumer Data, Customer Data, Data Of Potential Customers, Data Of Employees, Data Of Suppliers),
10. professional or employment-related information (in Category: Data Of Employees),
11. education information, defined as information that is not Publicly Available Personally identifiable information as defined in the Family Educational Rights and Privacy Act (20 U.S.C. Sec. 1232g; 34 C.F.R. Part 99) (in Category: Data Of Employees), and
12. inferences drawn from any of the information identified to create a profile about a Consumer reflecting the Consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes (in Categories: Consumer Data, Customer Data, Data Of Potential Customers, Data Of Employees, Data Of Suppliers).

## B. Purposes for which the Categories of Personal Information are Collected or Used (1798.100 (a) (1) CCPA):

The Purpose of Processing of Personal Information is the handling of all operations which concern the Business, Consumers, customers, prospective customers, business partners or other contractual or pre-contractual relations between the named groups (in the broadest sense) or legal obligations of the Business.

Where we Collect Consent of the Consumer, the Purpose is mentioned in the Consent language. Where Processing of Personal Information is necessary for the performance of a contract, as is the case, for example, when Processing operations are necessary for the supply of goods or to provide any other Service, the Purpose is the performance of such contract. Where Processing operations are necessary for carrying out pre-contractual measures, for example in the case of inquiries concerning our products or services, the Purpose is carrying out pre-contractual measures. Where we are subject to a legal obligation by which Processing of Personal Information is required, such as for the fulfillment of tax obligations, Purpose is to comply with such obligations.

Where Processing of Personal Information is necessary to protect the vital interests of the Consumer or of another natural Person, Purpose is the protection of these vital interests. This would be the case, for example, if a Consumer was injured on our premises and his/her name, age, health insurance data or other vital information would have to be passed on to a doctor, hospital or other Third Party.

Where Processing is necessary for the Purposes of the legitimate interests pursued by our company or by a Third Party, that legitimate interest is the Purpose.

## C. Whether that information is Sold or Shared (1798.100 (a) (1) CCPA):

We do not Sell your Personal Information. However, we might Share Personal Information for Cross-Context Behavioral Advertising, whether or not for monetary or other valuable consideration, including


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

transactions between us and a Third Party for Cross-Context Behavioral Advertising for the benefit of our Business in which no money is exchanged (e.g., when you visit our website, and your IP address is Shared with Third Parties for analytics, advertising, re-marketing purposes etc.).

## D. Notice Requirement (1798.100 (a) (1) CCPA))

We do not Collect additional Categories of Personal Information or use Personal Information Collected for additional Purposes that are incompatible with the disclosed Purpose for which the Personal Information was Collected without providing the Consumer with notice consistent with section 1798.100 (a) (1) CCPA.

## E. Categories of Sensitive Personal Information to be Collected (1798.100 (a) (2) CCPA)

The General Categories of Personal Information to be Collected are Consumer Data, Customer Data, Data Of Potential Customers, Data Of Employees, and Data Of Suppliers. These General Categories may include Sensitive Personal Information. Under these General Categories we may Process, subject to the information we obtain from you directly on a voluntary and informed basis, or that our Service Providers and/or Contractors obtained from you for a Business Purpose on behalf of us on a voluntary and informed basis, or that we Collected from Publicly Available sources, Third Parties, Service Providers and/or Contractors, the following Categories of Sensitive Personal Information about you:

a. social security, driver's license, state identification card, or passport number (in Categories: Consumer Data, Customer Data, Data Of Potential Customers, Data Of Employees, Data Of Suppliers),
b. account log-in, financial account, debit card, or credit card number in combination with any required security or access code, password, or credentials allowing access to an account (in Categories: Consumer Data, Customer Data, Data Of Potential Customers, Data Of Employees, Data Of Suppliers),
c. a Precise Geolocation (in Categories: Consumer Data, Customer Data, Data Of Potential Customers, Data Of Employees, Data Of Suppliers),
d. racial or ethnic origin, religious or philosophical beliefs, or union membership (in Category: Data Of Employees),
e. contents of mail, email, and text messages (in Categories: Consumer Data, Customer Data, Data Of Potential Customers, Data Of Employees, Data Of Suppliers),
f. genetic data (in Categories: Consumer Data, Customer Data),
g. Biometric Information (in Category: Data Of Employees, e.g., fingerprints and face ID for access Control, entry Control and other security Purposes), and
h. Personal Information concerning health (in Categories: Consumer Data, Customer Data, Data Of Employees).

## F. The Purposes for which the Categories of Sensitive Personal Information are Collected or used (1798.100 (a) (2) CCPA)


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

Purpose of Collection of your Sensitive Personal Information is to perform our Services or provide our goods, if such are reasonably expected by an average Consumer who requests those goods or Services, and if you requested these goods or Services from us, or to perform the Services set forth in paragraphs (2), (4), (5), and (8) of subdivision (e) of Section 1798.140 CCPA, and as authorized by regulations adopted pursuant to subparagraph (C) of paragraph (19) of subdivision (a) of Section 1798.185 CCPA.

### G. Whether that Sensitive Personal Information is Sold or Shared (1798.100 (a) (2) CCPA)

We do not Sell or Share Sensitive Personal Information.

### H. Notice Requirement (1798.100 (a) (2) CCPA)

We will not Collect additional Categories of Sensitive Personal Information or use Sensitive Personal Information Collected for additional Purposes that are incompatible with the disclosed Purpose for which the Sensitive Personal Information was Collected without providing the Consumer with notice consistent with Section 1798.100 (a) (2) CCPA.

### I. Criteria used to determine the length of time of retainment of Personal Information and Sensitive Personal Information (1798.100 (a) (3) CCPA)

The criteria used to determine the length of time we intend to retain each Category of Personal Information, including Sensitive Personal Information, is the respective statutory retention period or the company related retention period. After expiration of that period, the corresponding data is routinely deleted, as long as it is no longer necessary for the fulfillment of a contract or the initiation of a contract. We do not retain a Consumer's Personal Information or Sensitive Personal Information for each disclosed Purpose for which the Personal Information was Collected for longer than is reasonably necessary for the disclosed Purpose.

## III. Consumers' Right to Delete Personal Information (1798.105 CCPA)

As a Consumer you have the right to request that we delete any Personal Information about you which we Collected from you. We hereby disclose, pursuant to Section 1798.130 CCPA, your right to request the deletion of your Personal Information.

Where we receive a Verifiable Consumer Request to delete your Personal Information pursuant to subdivision (a) of Section 1798.105 CCPA we will delete your Personal Information from our records, notify any Service Providers or Contractors to delete your Personal Information from their records, and notify all Third Parties to whom we Sold or Shared the Personal Information to delete your Personal Information unless this proves impossible or involves disproportionate effort.

After you submitted a deletion request to us, we may maintain a confidential record of your deletion request solely for the Purpose of preventing your Personal Information from being Sold, for compliance with laws or for other Purposes, solely to the extent permissible under CCPA.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

Please feel free to contact us to exercise your rights.

## IV. Consumers' Right to Correct Inaccurate Personal Information (1798.106 CCPA)

As a Consumer you have the right to request from us, if we maintain inaccurate Personal Information about you, to correct that inaccurate Personal Information, taking into account the nature of the Personal Information and the Purposes of the Processing of the Personal Information. We hereby disclose, pursuant to Section 1798.130 CCPA, your right to request correction of inaccurate Personal Information.

If we receive a Verifiable Consumer Request to correct inaccurate Personal Information, we will use commercially reasonable efforts to correct the inaccurate Personal Information as directed by you, pursuant to Section 1798.130 CCPA and regulations adopted pursuant to paragraph (8) of subdivision (a) of Section 1798.185 CCPA.

Please feel free to contact us to exercise your rights.

## V. Consumers' Right to Know What Personal Information is Being Collected, Right to Access Personal Information (1798.110 CCPA)

As a Consumer you have the right to request from us to disclose to you (1) the Categories of Personal Information we have Collected about you and (2) the Categories of sources from which the Personal Information is Collected, and (3) the Business or Commercial Purpose for Collecting, Selling, or Sharing Personal Information, and (4) the Categories of Third Parties to whom the Business discloses Personal Information, and (5) the specific pieces of Personal Information we have Collected about you.

Please feel free to contact us to exercise your rights.

In accordance with subparagraph (A) of paragraph (5) of Section 1798.130 CCPA in combination with subparagraph (B) of paragraph (5) of subdivision (a) of Section 1798.130 CCPA, for Purposes of subdivision (c) of Section 1798.110 CCPA we hereby disclose the following information:

### A. The list of the Categories of Personal Information we have Collected about Consumers in the preceding 12 months by reference to the enumerated Category or Categories in subdivision (c) of Section 1798.130 CCPA that most closely describe the Personal Information Collected:

The General Categories of Personal Information we use are Consumer Data, Customer Data, Data Of Potential Customers, Data Of Employees, and Data Of Suppliers. Under these General Categories, in the preceding 12 months, we Collected the following Categories of Personal Information:

1. Advertising and Marketing (in Categories: Consumer Data, Customer Data, Data Of Potential Customers, Data Of Suppliers),
2. Cross-Context Behavioral Advertising (in Categories: Consumer Data, Customer Data, Data Of Potential Customers, Data Of Suppliers),


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

3. Aggregate Consumer Information (in Categories: Consumer Data, Customer Data, Data Of Potential Customers, Data Of Employees, Data Of Suppliers),
4. Biometric Information (in Category: Data Of Employees, e.g., fingerprints and face ID for access Control, entry Control and other security Purposes),
5. Personal Information, such as a real name, alias, postal address, Unique Personal Identifier, online identifier, Internet Protocol address, email address, account name, social security number, driver's license number, passport number, or other similar identifiers (in Categories: Consumer Data, Customer Data, Data Of Potential Customers, Data Of Employees, Data Of Suppliers),
6. commercial information, including records of Personal property, products or Services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies (in Categories: Consumer Data, Customer Data, Data Of Potential Customers, Data Of Suppliers),
7. internet or other electronic network activity information, including, but not limited to, browsing history, search history, and information regarding a Consumer's interaction with an internet website application, or advertisement (in Categories: Consumer Data, Customer Data, Data Of Potential Customers, Data Of Employees, Data Of Suppliers),
8. geolocation data (in Categories: Consumer Data, Customer Data, Data Of Potential Customers, Data Of Employees, Data Of Suppliers),
9. audio, electronic, visual, thermal, olfactory, or similar information (in Categories: Consumer Data, Customer Data, Data Of Potential Customers, Data Of Employees, Data Of Suppliers),
10. professional or employment-related information (in Category: Data Of Employees)
11. education information, defined as information that is not Publicly Available Personally identifiable information as defined in the Family Educational Rights and Privacy Act (20 U.S.C. Sec. 1232g; 34 C.F.R. Part 99) (in Category: Data Of Employees), and
12. inferences drawn from any of the information identified to create a profile about a Consumer reflecting the Consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes (in Categories: Consumer Data, Customer Data, Data Of Potential Customers, Data Of Employees, Data Of Suppliers).

## B. The Categories of sources from which Consumers' Personal Information is Collected:

We have Collected Personal Information from the following Categories of Sources:

1. Consumer,
2. Employer Of The Consumer,
3. Service Provider,
4. Contractor,
5. Third Party, and
6. Publicly Available sources.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

### C. The Business or Commercial Purpose for Collecting, Selling, or Sharing Consumers' Personal Information:

The Business or Commercial Purposes for Collecting or Sharing Consumers' Personal Information is the handling of all operations which concern the Business, Consumers, customers, prospective customers, business partners or other contractual or pre-contractual relations between the named groups (in the broadest sense) or legal obligations of the Business. Because we don't Sell Personal Information, we do not name a Purpose for Selling Personal Information here.

### C. The Categories of Third Parties to whom the Business discloses Consumers' Personal Information:

We are disclosing Personal Information to the following Categories of Third Parties:

Online-Services (e.g., when you visit our website, and your IP address is Shared with Third Parties for analytics, advertising, re-marketing purposes etc.).

## VI. Consumers' Right to Know What Personal Information is Sold or Shared and to Whom (1798.115 CCPA)

As a Consumer you have the right to request that we disclose to you if we Sell or Share your Personal Information, or if we disclose Personal Information for a Business Purpose.

This includes the (1) Categories of Personal Information that we Collected about you, and (2) Categories of Personal Information that we Sold or Shared about you, and (3) Categories of Third Parties to whom the Personal Information was Sold or Shared, by Category or Categories of Personal Information for each Category of Third Parties to whom the Personal Information was Sold or Shared, and (4) Categories of Personal Information that we disclosed about you for a Business Purpose, and (5) Categories of Persons to whom it was disclosed for a Business Purpose.

Please feel free to contact us to exercise your rights.

In accordance with subparagraph (A) of paragraph (5) of Section 1798.130 CCPA in combination with subparagraph (C) of paragraph (5) of subdivision (a) of Section 1798.130 CCPA, for the Purposes of paragraphs (1) and (2) of subdivision (c) of Section 1798.115 CCPA we hereby disclose the following information in two separate lists:

### A. A list of the Categories of Personal Information we have Sold or Shared about Consumers in the preceding 12 months by reference to the enumerated Category or Categories in subdivision (c) of Section 1798.130 CCPA that most closely describe the Personal Information Sold or Shared, or if the Business has not Sold or Shared Consumers' Personal Information in the preceding 12 months:


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

**WE HAVE NOT SOLD PERSONAL INFORMATION IN THE PRECEDING 12 MONTH.**

Categories of Personal Information we Shared about Consumers in the preceding 12 months by reference to the enumerated Category:

Category of Personal Information: Data for Cross-Context Behavioral Advertising.

Reference to the enumerated Category: Cross-Context Behavioral Advertising.

## B. A list of the Categories of Personal Information it has disclosed about Consumers for a Business Purpose in the preceding 12 months by reference to the enumerated Category in subdivision (c) that most closely describes the Personal Information disclosed:

The General Categories of Personal Information we use are Consumer Data, Customer Data, Data Of Potential Customers, Data Of Employees, and Data Of Suppliers. Under these General Categories, in the preceding 12 months, we disclosed for a Business Purpose the following Categories of Personal Information:

1. Advertising and Marketing (in Categories: Consumer Data, Customer Data, Data Of Potential Customers, Data Of Suppliers),
2. Cross-Context Behavioral Advertising (in Categories: Consumer Data, Customer Data, Data Of Potential Customers, Data Of Suppliers),
3. Aggregate Consumer Information (in Categories: Consumer Data, Customer Data, Data Of Potential Customers, Data Of Employees, Data Of Suppliers),
4. Biometric Information (in Category: Data Of Employees, e.g., fingerprints and face ID for access Control, entry Control and other security Purposes),
5. Personal Information, such as a real name, alias, postal address, Unique Personal Identifier, online identifier, Internet Protocol address, email address, account name, social security number, driver's license number, passport number, or other similar identifiers (in Categories: Consumer Data, Customer Data, Data Of Potential Customers, Data Of Employees, Data Of Suppliers),
6. commercial information, including records of Personal property, products or Services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies (in Categories: Consumer Data, Customer Data, Data Of Potential Customers, Data Of Suppliers),
7. internet or other electronic network activity information, including, but not limited to, browsing history, search history, and information regarding a Consumer's interaction with an internet website application, or advertisement (in Categories: Consumer Data, Customer Data, Data Of Potential Customers, Data Of Employees, Data Of Suppliers),
8. geolocation data (in Categories: Consumer Data, Customer Data, Data Of Potential Customers, Data Of Employees, Data Of Suppliers),


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

9. audio, electronic, visual, thermal, olfactory, or similar information (in Categories: Consumer Data, Customer Data, Data Of Potential Customers, Data Of Employees, Data Of Suppliers),
10. professional or employment-related information (in Category: Data Of Employees),
11. education information, defined as information that is not Publicly Available Personally identifiable information as defined in the Family Educational Rights and Privacy Act (20 U.S.C. Sec. 1232g; 34 C.F.R. Part 99) (in Category: Data Of Employees), and
12. inferences drawn from any of the information identified to create a profile about a Consumer reflecting the Consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes (in Categories: Consumer Data, Customer Data, Data Of Potential Customers, Data Of Employees, Data Of Suppliers).

## VII. Consumers' Right to Opt Out of Sale or Sharing of Personal Information (1798.120 CCPA)

If we Sell or Share Personal Information about you to Third Parties you have the right, at any time, to direct us, not to Sell or Share your Personal Information. On our websites and in other publications and materials, this right may be referred to as the right to opt-out of Sale or Share.

We hereby provide notice to Consumers, pursuant to subdivision (a) of Section 1798.135 CCPA, that Personal Information may be Sold or Shared, and that Consumers have the "right to opt-out" of the Sale or Share of their Personal Information.

We do not Sell or Share Personal Information if we have actual knowledge that you are less than 16 years of age, unless you, in the case of Consumers at least 13 years of age and less than 16 years of age, or your parent or guardian, in the case of Consumers who are less than 13 years of age, have affirmatively authorized the Sale or Share of the Consumer's Personal Information.

Please feel free to contact us to exercise your rights.

## VIII. Consumers' Right to Limit Use and Disclosure of Sensitive Personal Information (1798.121 CCPA)

Where we Collect Sensitive Personal Information about you to perform the Services set forth in paragraphs (2), (4), (5), and (8) of subdivision (e) of Section 1798.140 CCPA, and as authorized by regulations adopted pursuant to subparagraph (C) of paragraph (19) of subdivision (a) of Section 1798.185 CCPA, you have the right, at any time, to direct us to limit our use of your Consumer's Sensitive Personal Information to that use which is necessary to perform the Services or provide the goods reasonably expected by an average Consumer who requests those goods or Services.

We hereby give notice, pursuant to subdivision (a) of Section 1798.135 CCPA, that your Sensitive Personal Information is Processed for Purposes other than those specified in this clause, and that this information may be used, or disclosed to Service Providers or Contractors, for additional, specified Purposes and that you have the right to limit the use or disclosure of your Sensitive Personal Information.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

The specified Purposes are external hosting and related automated Processing activities for Purposes of hosting in the cloud, or on a server, computer, or other IT infrastructure (including to backup such data for IT security Purposes) that are not based on our own premises and to outsource Processing activities to Service Providers and/or Contractors.

Please feel free to contact us to exercise your rights.

## IX. Consumers' Right of No Retaliation Following Opt Out or Exercise of Other Rights (1798.125 CCPA)

We will not discriminate against you because you exercised any of your rights under CCPA, including, but not limited to, by (a) denying goods or Services to you, and (b) charging different prices or rates for goods or Services, including through the use of discounts or other benefits or imposing penalties, and (c) providing a different level or quality of goods or Services to you, and (d) suggesting that you will receive a different price or rate for goods or Services or a different level or quality of goods or Services, and (e) retaliate against an employee, applicant for employment, or independent Contractor, as defined in subparagraph (A) of paragraph (2) of subdivision (m) of Section 1798.145 CCPA, for exercising their rights under CCPA.

However, we are not prohibited, from charging a Consumer a different price or rate, or from providing a different level or quality of goods or Services to the Consumer, if that difference is reasonably related to the value provided to us by the Consumer's data.

We may offer loyalty, rewards, premium features, discounts, or club card programs consistent with CCPA. We may offer financial incentives, including payments to Consumers as compensation, for the Collection of Personal Information, the Sale or Sharing of Personal Information, or the retention of Personal Information. We may also offer a different price, rate, level, or quality of goods or Services to the Consumer if that price or difference is reasonably related to the value provided to us by the Consumer's data.

If we offer any financial incentives pursuant to Section 1798.125 CCPA, we will notify the Consumers of the financial incentives pursuant to Section 1798.130 CCPA.

We may enter you into a financial incentive program only if you give is prior opt-in Consent pursuant to Section 1798.130 CCPA that clearly describes the material terms of the financial incentive program, and which may be revoked by you at any time. If you refuse to provide opt-in Consent, we wait for at least 12 months before next requesting that you provide opt-in Consent, or as prescribed by regulations adopted pursuant to Section 1798.185 CCPA.

## X. Notice, Disclosure, Correction, and Deletion Requirements (1798.130 CCPA)

As a Consumer, you have two designated methods for submitting requests for information required to be disclosed pursuant to Sections 1798.110 CCPA and 1798.115 CCPA, or requests for deletion or


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

correction pursuant to Sections 1798.105 CCPA and 1798.106 CCPA, respectively, including, a toll-free telephone number.

Please use the toll-free telephone number or the email address mentioned in the beginning of this publication to submit your Consumer request.

Additionally, we maintain an internet website and you may use the published contact form on our website to submit requests for information required to be disclosed pursuant to Sections 1798.110 CCPA and 1798.115 CCPA, or requests for deletion or correction pursuant to Sections 1798.105 CCPA and 1798.106 CCPA.

We might take steps to determine whether the request is a Verifiable Consumer Request under CCPA, including, but not limited to, ask you to identify yourself. We are obliged to make sure that a Person which has send us a request is the Consumer that we Process Personal Information about (required authentication of the Consumer).

If you maintain an account with us, your request shall be made in writing and delivered through your account. If not, you may submit your request in writing by e-mail or electronically at your option.

This publication will be updated at least every 12 months. Please review this publication from time to time.

## XI. Methods of Limiting Sale, Sharing, and Use of Personal Information and Use of Sensitive Personal Information (1798.135 CCPA)

We may provide a clear and conspicuous link titled “Do Not Sell or Share My Personal Information,” that enables you, or a Person authorized by you, to opt-out of the Sale or Sharing of your Personal Information.

We may provide a clear and conspicuous link titled “Limit the Use of My Sensitive Personal Information,” that enables you, or a Person authorized by you, to limit the use or disclosure of your Sensitive Personal Information to those uses authorized by subdivision (a) of Section 1798.121 CCPA.

Above, we included a description of your rights pursuant to Sections 1798.120 CCPA and 1798.121 CCPA, and, if applicable, a separate link to a “Do Not Sell or Share My Personal Information” and a separate link to a “Limit the Use of My Sensitive Personal Information” internet web page will be available in our Privacy Policy. We will respond to and abide by opt-out preference signals sent by the link in our Privacy Policy.

Additionally, a click-box or link with the language “Do Not Sell or Share My Personal Information” was integrated in our cookie-banner. By clicking the click-box or link in the cookie-banner, you communicate us your choice only in regard to Advertising and Marketing data, and only for a 12-month period, providing you don’t delete or change the cookies on your computer, notebook, tablet, mobile phone or other Device in the meantime.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## XII. Providing of goods and Services after Consumer rights are exercised or Consent is withdrawn.

We need to inform you that, when you refuse to give Consent, or exercise one or more of your rights under CCPA, we might not be able to provide you with goods or Services, when Processing of your Personal Information or Sensitive Personal Information is necessary for the provision of our goods or Services, or to administer or bill such goods or Services.

## XIII. Consumer Age

We don't have actual knowledge about the age of any Consumer. If you are a minor, you shall not provide us with your Personal Information or Sensitive Personal Information without Consent of your custodial parent or guardian. If you are a minor only your custodial parent or guardian shall provide us with Personal Information or Sensitive Personal Information about you.

## XIV. Information regarding revised and new CCPA regulations that are in effect from Jan. 1, 2026

### A. Confirmation of Opt-Out Requests including Global Privacy Control Signals

Consumers from California have the right to direct us not to sell or share their personal information with third parties, as those terms are defined under applicable law. We honor valid opt-out requests submitted through our designated privacy request methods, including browser-based opt-out preference signals such as the Global Privacy Control (GPC).

Once your opt-out request has been received and processed, we will provide confirmation that the request has been honored. This confirmation may be displayed through our website, cookie settings center, privacy preference center, account settings, or another reasonably accessible method. For example, you may see a message stating "Opt-Out Request Honored" or a setting indicating that selling or sharing has been turned off for your browser, device, or account.

If we detect a valid GPC signal from your browser or device, we will treat that signal as a request to opt out where required by law and will display or otherwise make available confirmation that the request has been processed. Please note that opt-out preferences may be specific to the browser, device, or account used to submit the request. If you use multiple browsers or devices, you may need to set your preferences on each one unless your request is linked to your authenticated account.

### B. Cookie Consent and Website Tracking Choices

Where we request your consent to use cookies, external connections or similar tracking technologies for advertising, analytics, personalization, or the sale or sharing of personal information, your consent must be provided through a clear and affirmative action. Closing a banner, dismissing a pop-up, continuing to browse, scrolling, navigating to another page, or otherwise taking no action will not be treated as consent.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

When consent is required, we will present your choices in a clear, symmetrical, and understandable manner. Options to accept or decline will not be unfairly emphasized through size, color, contrast, wording, placement, or other interface design choices. You may withdraw or change your consent choices at any time through our cookie settings, privacy preference center, or other methods made available on our website.

If you choose not to consent, non-essential cookies and similar technologies that require consent will not be activated, except where permitted or required for strictly necessary website functions, security, fraud prevention, debugging, or other purposes allowed by applicable law.

## C. Equal and Symmetrical Privacy Choices

Where applicable law gives you the right to opt out of the sale or sharing of your personal information, we provide methods for exercising that right that are easy to use and designed to avoid unnecessary burden. The process for submitting an opt-out request will require the same number of steps or fewer than any process we make available for opting in to the sale or sharing of personal information. We will not require you to navigate a more complex, lengthy, or burdensome process to opt out than to opt in.

Our privacy choices, notices, links, and preference tools are designed to present options in a clear, symmetrical, and understandable manner. We do not use interfaces intended to impair your decision-making, pressure you into a particular choice, or make opting out more difficult than opting in. You may exercise your opt-out rights through privacy choices links, cookie settings, account preferences, cookie deletion within your browser or other methods described in this Privacy Policy. Once processed, your preferences will be honored in accordance with applicable law.

## D. Financial Incentive Programs and Voluntary Participation

We may offer programs, promotions, discounts, loyalty benefits, sweepstakes, or other incentives that involve the collection, processing, retention, sale, sharing, or use of personal information, where permitted by applicable law. Participation in any financial incentive program is entirely voluntary. We will not enroll you automatically or select participation by default. Where your opt-in consent is required, you must take a clear affirmative action to join the program.

When presenting participation choices, we design the options in a clear and symmetrical manner. The option to join a program will not be presented more prominently than the option not to participate through size, color, placement, wording, or other design features intended to influence your decision.

You may withdraw from a financial incentive program at any time by using the method provided at enrollment, through your account settings, by contacting us, or as otherwise described in the applicable program terms. Withdrawal will not affect any rights you have under applicable privacy law. Additional details regarding any material terms, categories of personal information involved, benefits offered, how the value of your data is calculated where required, and how to withdraw will be provided at or before the time you are invited to participate.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## E. Requests to Know and Access to Historical Personal Information

Subject to applicable law, you may request that we disclose the personal information we have collected, used, disclosed, sold, shared, or otherwise processed about you, including information maintained for periods longer than the twelve (12) months preceding your request.

Where we retain personal information for more than twelve (12) months, our request mechanisms will allow you to seek access to personal information collected before that period. Depending on the request method used, you may be able to select a date range, specify the period for which you seek information, or request all personal information we maintain about you that is subject to disclosure rights under applicable law. Unless otherwise limited by law, this may include personal information collected on or after January 1, 2022, where such information is still maintained by us and can be reasonably associated with you.

To submit a request to know, please contact us. We may need to verify your identity before processing your request and may apply legal exceptions or limitations where permitted by law.

## F. Disclosure of Personal Information to Third Parties, Service Providers, and Contractors

In the preceding twelve (12) months, we may have disclosed personal information to third parties, service providers, and contractors for business purposes, including to help us operate our business, provide services, process transactions, maintain security, perform analytics, communicate with companies and persons, conduct audits, prevent fraud, comply with data protection and privacy laws and other legal obligations.

The categories of personal information we may have disclosed for business purposes include identifiers, employee records, customer records and contact information, commercial information, internet or other electronic network activity information, geolocation data where permitted, professional or employment-related information where relevant, inferences drawn from personal information, and other categories of information described in this Transparency Document or our Privacy Policy that are reasonably necessary for our business operations.

We may disclose these categories of personal information to service providers and contractors that perform services on our behalf, such as hosting, payment processing, analytics, customer support, communications delivery, fraud prevention, IT administration and data protection and privacy services. We may also disclose personal information to contractors that process personal information under written agreements for specified business purposes, and to third parties where necessary for operational, legal, regulatory, security, auditing, or other disclosed purposes.

We require third parties, service providers and contractors to process personal information only for authorized purposes and in accordance with applicable contractual and legal obligations. The specific categories of personal information disclosed and the recipients involved may vary depending on your


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

relationship with us and how you interact with our services. For more information regarding the disclosure of your personal information, please feel free to contact us.

## G. Mobile Application Privacy Policy Access

We may have published or provided you with a mobile application. If you use a mobile application published or provided by us, a link to our Privacy Policy is made available within the application's settings menu or a similarly labeled in-app location that is reasonably accessible to users. This in-app link allows you to review our privacy practices, including information about the categories of personal information we collect, how we use and disclose personal information, your privacy rights, and the choices available to you. We encourage users to review this Transparency Document and our Privacy Policy periodically, as it may be updated from time to time to reflect changes in our practices, technologies, legal requirements, or available choices.

## H. Connected Devices, IoT Products, and AR/VR Privacy Notices

Where we collect personal information through connected devices, internet-enabled products, wearable devices, smart home products, gaming systems, or similar technologies, and where applicable law provides a right to opt out of the sale or sharing of personal information, we will provide notice of that right before or at the time the device begins collecting the personal information that may be sold or shared.

Where we collect personal information in augmented reality (AR), virtual reality (VR), mixed reality, immersive, or similar digital environments, and where opt-out rights apply, we will provide notice of the right to opt out before or at the time you enter the relevant environment, or before or at the time you encounter our brand, service, experience, or collection point within that environment, as appropriate.

These notices may be delivered through device setup flows, onboarding screens, companion applications, in-product prompts, layered notices, privacy dashboards, QR codes, account settings, voice or visual prompts, or other methods reasonably designed for the device or environment used. Where required, such notices may also serve as notice at collection and will explain the categories of personal information collected, the purposes for which the information is used, whether the information may be sold or shared and how to exercise applicable opt-out rights. You may update your privacy preferences at any time through available device settings, account controls, companion applications, or the privacy request methods available.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

# ENGLISH: Information about the Processing of Personal Data (Decree Law No. 45 of 2021 (PDPL) - United Arab Emirates)

Dear Sir or Madam,

The Personal Data of every individual who is in a contractual, pre-contractual or other relationship with our company deserve special protection. Our goal is to keep our data protection level on a high standard. Therefore, we are routinely developing new data protection and data security concepts.

Of course, we comply with the statutory provisions of Decree Law No. 45 of 2021 (PDPL). This document fulfills our information obligations towards you.

The terminology of legal regulations is complicated. Unfortunately, the use of legal terms could not be dispensed with in the preparation of this document. Therefore, we would like to point out that you are always welcome to contact us for all questions concerning this document, the used terms or formulations.

## I. Definitions

PDPL means the Decree Law No. 45 of 2021 as issued at the Presidential Palace in Abu Dhabi and published in the Official Gazette which is in force since 2nd of January 2022, as amended or superseded from time to time, and all related Executive Regulations regarding or concretizing the PDPL. The legal definitions from Art. 1 PDPL apply.

## II. Cases of Processing Personal Data without your Consent (Art. 4 PDPL)

In general, we will not Process your Personal Data without your Consent. However, we may Process your Personal Data without your Consent in the following cases, in which Processing is considered lawful, namely (1) if the Processing is necessary to protect the public interest, or (2) if the Processing is for Personal Data that has become available and known to the public by an act of you, or (3) if the Processing is necessary to initiate or defend against any actions to claim rights or legal proceedings, or related to judicial or security procedures, or (4) if the Processing is necessary for the purposes of occupational or preventive medicine, for assessment of the working capacity of an employee, medical diagnosis, provision of health or social care, treatment or health insurance services, or management of health or social care systems and services, in accordance with the legislation in force in the United Arab Emirates, or (5) if the Processing is necessary to protect public health, including the protection from communicable diseases and epidemics, or for the purposes of ensuring the safety and quality of health care, medicines, drugs and medical devices, in accordance with the legislation in force in the United Arab Emirates, or (6) if the Processing is necessary for archival purposes or for scientific, historical and statistical studies, in accordance with the legislation in force in the United Arab Emirates, or (7) if the Processing is necessary to protect your interests, or (8) if the Processing is necessary for us or you to fulfill obligations and exercise legally established rights in the field of employment, social security or laws on social protection, to the


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

extent permitted by those laws, or (9) if the Processing is necessary to perform a contract to which you are a party or to take, at your request, procedures for concluding, amending or terminating a contract, or (10) if the Processing is necessary to fulfill obligations imposed by other laws of the United Arab Emirates on us, or (11) in any other cases set by the Executive Regulations of PDPL.

## III. Conditions for Consent to Data Processing (Art. 6 PDPL)

Consent must be given in a clear, simple, unambiguous and easily accessible manner, whether in writing or electronic form. Therefore, we kindly ask you to inform us if you do not understand our Consent language or if you think, that the Consent is not clear, simple, unambiguous or easily accessible.

In any case, you have the right to withdraw your Consent to the Processing of your Personal Data at any time and the withdrawal must be easy. Hence, please feel free to use any means available to you (e.g., online form, email, or phone) to withdraw your Consent with us at any time. We inform you that the withdrawal of Consent shall not affect the legality and lawfulness of the Processing made based on the Consent given prior to the withdrawal.

## IV. Data Protection Officer (Article 10 PDPL)

We appointed a Data Protection Officer who has sufficient skills and knowledge of Personal Data Protection. The contact address of the Data Protection Officer is mentioned above.

You have the right to send requests and complaints related to Personal Data in accordance with the provisions of PDPL and the Executive Regulations of PDPL to our Data Protection Officer.

You may communicate directly with the Data Protection Officer for any matters related to your Personal Data and the Processing, thereof in order to exercise your rights in accordance with the provisions of PDPL.

## V. Right to Obtain Information (Article 13 PDPL)

You have the right to obtain the following information (without charge):

### a. The types of Personal Data that is Processed:

Customer data

Data of potential customers

Data of employees

Data of suppliers

### b. Purposes of Processing:

The purpose of the Processing of Personal Data is the handling of all operations which concern the controller, customers, prospective customers, business partners or other contractual or pre-contractual relations between the named groups (in the broadest sense) or legal obligations of the controller.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

If the Processing is necessary to protect the public interest, the purpose of the Processing is to take into consideration and process to protect the public interest. If the Processing is for Personal Data that has become available and known to the public by an act of you, the purpose of the Processing is to fulfill our business goals. If the Processing is necessary to initiate or defend against any actions to claim rights or legal proceedings, or related to judicial or security procedures, the purpose of the Processing is to act in or for the required proceedings. If the Processing is necessary for the purposes of occupational or preventive medicine, for assessment of the working capacity of an employee, medical diagnosis, provision of health or social care, treatment or health insurance services, or management of health or social care systems and services, in accordance with the legislation in force in the United Arab Emirates, the purpose of the Processing is to fulfill all requirements of those laws and to achieve our business goals and legitimate interests. If the Processing is necessary to protect public health, including the protection from communicable diseases and epidemics, or for the purposes of ensuring the safety and quality of health care, medicines, drugs and medical devices, in accordance with the legislation in force in the United Arab Emirates, the purpose of the Processing is to fulfill the necessary requirements of those laws. If the Processing is necessary for archival purposes or for scientific, historical and statistical studies, in accordance with the legislation in force in the United Arab Emirates, the purpose of the Processing is to fulfill the necessary requirements. If the Processing is necessary to protect the interests of you, the purpose of the Processing is to protect these interests. If the Processing is necessary for us or you to fulfill his/her obligations and exercise his/her legally established rights in the field of employment, social security or laws on social protection, to the extent permitted by those laws, the purpose of the Processing is to fulfill the requirements of those laws. If the Processing is necessary to perform a contract to which you are a party or to take, at the request of yourself, procedures for concluding, amending or terminating a contract, the purpose of the Processing is to act in compliance with or under, or to fulfill the contract. If the Processing is necessary to fulfill obligations imposed by other laws of the United Arab Emirates on us, the purpose of the Processing is legal compliance. If the Processing is necessary for any other case set by the Executive Regulations of PDPL, the purpose of the Processing is to comply with such regulations.

## c. Decisions made based on Automated Processing, including Profiling.

As a responsible company, we do not use automatic decision-making or profiling.

## d. Targeted sectors or establishments with which Personal Data is to be shared, whether inside or outside the United Arab Emirates.

Public authorities

External bodies

Further external bodies

Internal Processing

Intragroup Processing


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

Other bodies

## e. Controls and standards for the periods of storing and keeping Personal Data.

**Measures of pseudonymization and encryption of Personal Data:** Pseudonymization of Personal Data that are no longer needed in plain text; Encryption of websites (SSL); Encryption of e-mail (TLS 1.2 or 1.3).

**Measures for ensuring ongoing confidentiality, integrity, availability and resilience of Processing systems and services:** Confidentiality agreements with employees; NDAs with third parties; Data Protection agreements with employees; Firewall; Anti-Virus; Regular backups.

**Measures for ensuring the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident:** Regular backups of the whole system; Regular test of backup and recovery; Regular training of IT staff.

**Processes for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures in order to ensure the security of the Processing:** In-house checks; Regular review of Processes by IT; Regular audits (e.g., by the DPO).

**Measures for user identification and authorization:** Authentication with username / password; Regular checks of authorizations; Password guideline; Limitation of the number of administrators; Management of rights by system administrator.

**Measures for the protection of data during transmission:** Use of encryption technologies; Logging of activities and events; Encryption of email (TLS 1.2 or 1.3); Use of company internal / restricted drives.

**Measures for the protection of data during storage:** Logging of actions and events; Limitation of the number of administrator's; Firewall.

**Measures for ensuring physical security of locations at which Personal Data are Processed:** Manual locking system; Security locks; Key control.

**Measures for ensuring events logging:** Logging activated on application level; Regular manual checks of logs.

**Measures for ensuring system configuration, including default configuration:** Configuration change control process; Data protection by default is observed; Configuration only by system administrator; Regular training of IT staff.

**Measures for internal IT and IT security governance and management:** IT security policy; Training of employees on data security; IT team with clear roles and responsibilities.

**Measures for certification/assurance of Processes and products:** Clear overview of the provisions applicable to the provided products/services/Processes; Regular internal and/or external audits; Assignment of audit responsibilities to certified experts.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

**Measures for ensuring data minimization:** Identification of the purpose of Processing; Assessment of a link between Processing and purpose; Identification of the applicable retention periods for each data category; Secure erasure of the data after expiration of the retention period.

**Measures for ensuring data quality:** Logging of entry and modification of data; Assignment of rights for data entry; Traceability of entry, modification of data by individual user names (not user groups).

**Measures for ensuring limited data retention:** Regular training on retention periods; Regular audit and assessment of retained data.

**Measures for ensuring accountability:** Provision of training / awareness rising; Regular controls and checks; Appropriate policies on data protection; Conclusion of SCCs.

**Measures for allowing data portability and ensuring erasure:** Personal Data is stored in a structured format; Monitoring of legal deadline ensured; Observation of retention periods; Establishment of data portability Process; Proper handling of data subject requests; Secure data erasure and data carrier destruction.

## f. Procedures for correcting, erasing or limiting the Processing and objection to Personal Data.

The procedure is to involve our Data Protection Officer, that shall be informed by every employee, third party or can be involved by you regarding the exercising of any of the Data Subjects Rights. The Data Protection Officer coordinates the correction, erasure and limiting the Processing, and objection to Personal Data Processing with the respective departments, and received feedback from them, when the correction, erasure and limiting the Processing, or the objection is processed or fulfilled. Later, the Data Protection Officer will inform you regarding your request.

## g. Protection measures for Cross-Border Processing made in accordance with Articles (22) and (23) PDPL.

We agreed with every Cross-Border data recipient (at least) on the following protection measures:

**Measures of pseudonymization and encryption of Personal Data:** Pseudonymization of Personal Data that are no longer needed in plain text; Encryption of websites (SSL); Encryption of e-mail (TLS 1.2 or 1.3).

**Measures for ensuring ongoing confidentiality, integrity, availability and resilience of Processing systems and services:** Confidentiality agreements with employees; NDAs with third parties; Data Protection agreements with employees; Firewall; Anti-Virus; Regular backups.

**Measures for ensuring the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident:** Regular backups of the whole system; Regular test of backup and recovery; Regular training of IT staff.


© All rights reserved by Heiko Maniero.

**Processes for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures in order to ensure the security of the Processing:** In-house checks; Regular review of Processes by IT; Regular audits (e.g., by the DPO).

**Measures for user identification and authorization:** Authentication with username / password; Regular checks of authorizations; Password guideline; Limitation of the number of administrators; Management of rights by system administrator.

**Measures for the protection of data during transmission:** Use of encryption technologies; Logging of activities and events; Encryption of email (TLS 1.2 or 1.3); Use of company internal / restricted drives.

**Measures for the protection of data during storage:** Logging of actions and events; Limitation of the number of administrator's; Firewall.

**Measures for ensuring physical security of locations at which Personal Data are Processed:** Manual locking system; Security locks; Key control.

**Measures for ensuring events logging:** Logging activated on application level; Regular manual checks of logs.

**Measures for ensuring system configuration, including default configuration:** Configuration change control process; Data protection by default is observed; Configuration only by system administrator; Regular training of IT staff.

**Measures for internal IT and IT security governance and management:** IT security policy; Training of employees on data security; IT team with clear roles and responsibilities.

**Measures for certification/assurance of Processes and products:** Clear overview of the provisions applicable to the provided products/services/Processes; Regular internal and/or external audits; Assignment of audit responsibilities to certified experts.

**Measures for ensuring data minimization:** Identification of the purpose of Processing; Assessment of a link between Processing and purpose; Identification of the applicable retention periods for each data category; Secure erasure of the data after expiration of the retention period.

**Measures for ensuring data quality:** Logging of entry and modification of data; Assignment of rights for data entry; Traceability of entry, modification of data by individual user names (not user groups).

**Measures for ensuring limited data retention:** Regular training on retention periods; Regular audit and assessment of retained data.

**Measures for ensuring accountability:** Provision of training / awareness rising; Regular controls and checks; Appropriate policies on data protection; Conclusion of SCCs.

**Measures for allowing data portability and ensuring erasure:** Personal Data is stored in a structured format; Monitoring of legal deadline ensured; Observation of retention periods; Establishment of data


© All rights reserved by Heiko Maniero.

portability Process; Proper handling of data subject requests; Secure data erasure and data carrier destruction.

## h. Procedures to be taken in the event of a breach or infringement of Personal Data, especially if the breach or infringement poses a direct and serious threat to the privacy and confidentiality of Personal Data.

The procedure is to involve our Data Protection Officer, which shall advise us regarding all necessary steps. However, we will immediately upon becoming aware of any infringement or breach of the Personal Data of you that would prejudice the privacy, confidentiality and security of such data, report such infringement or breach and the results of the investigation to the UAE Data Office within such period and in accordance with such procedures and conditions as set by the Executive Regulations of PDPL.

The reporting will be accompanied by the following data and documents (a) the nature, form, causes, approximate number and records of the infringement or breach, and (b) the data of the Data Protection Officer appointed by us, and (c) the potential and expected effects of the infringement or breach, and (d) the procedures and measures taken by us and proposed to be applied to address this infringement or breach and reduce its negative effects, and (e) documentation of the infringement or breach and the corrective actions taken by us, and (f) any other requirements by the UAE Data Office.

In all cases, we will notify you in the event that the infringement or breach would prejudice the privacy, confidentiality and security of his/her Personal Data and advise him/her of the procedures taken by us, within such period and in accordance with such procedures and conditions as set by the Executive Regulations of PDPL.

Our Processors agreed, immediately upon becoming aware of any infringement or breach of the Personal Data of you, to notify us of such infringement or breach in order for us, in turn, to report it to the UAE Data Office in accordance with the law.

## i. The Process of filing complaints with the UAE Data Office.

If you want to file a complaint, please contact the UAE Data Office established by Decree-Law No. 44 of 2021.

## j. Additional information.

We shall, before starting the Processing, provide you with the information in Paragraphs (b), (d) and (g) above. However, we decided to provide you with more information for transparency reasons. If you need additional or specific information, please submit a request to us or our Data Protection Officer.

We want to inform you, that we may refuse your request to obtain information, if it is found out that (a) the request is not related to the information referred to Article 13 (1) PDPL or is excessively repetitive, or (b) the request conflicts with the judicial procedures or investigations made by the competent authorities, or (c) the request may adversely affect the efforts of us to protect information security, or (d) the request affects the privacy and confidentiality of the Personal Data of others.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## VI. Right to Request Personal Data Transfer (Article 14 PDPL)

You have the right to obtain your Personal Data provided to us for Processing in a structured and machine-readable manner, so long as the Processing is based on your Consent or is necessary for the fulfillment of a contractual obligation and is made by automated means.

You have the right to request the transfer of your Personal Data to another Controller whenever this is technically feasible.

## VII. Right to Correction or Erasure of Personal Data (Article 15 PDPL)

You have the right to request the correction or completion of your inaccurate Personal Data held with us without undue delay.

Without prejudice to the legislation in force in the United Arab Emirates and what is required by the public interest, you have the right to request the erasure of your Personal Data held with us, when (a) your Personal Data is no longer required for the purposes for which it is collected or Processed, or (b) if you withdraw your Consent on which the Processing is based, or (c) if your object to the Processing or if there are no legitimate reasons for us to continue the Processing, or (d) if your Personal Data is Processed in violation of the provisions of PDPL and the legislation in force, and the erasure Process is necessary to comply with the applicable legislation and approved standards in this regard.

Except for what is in Article 15 (2) PDPL, you have no right to request erasure of your Personal Data held by us (a) if the request is for the erasure of your Personal Data related to public health and held with private establishments, or (b) if the request affects the investigation procedures, claims for rights and legal proceedings or defense of us, or (c) if the request conflicts with other legislation to which we are subject, or (d) in any other cases set by the Executive Regulations of PDPL.

## VIII. Right to Restrict Processing (Article 16 PDPL)

You have the right to oblige us to restrict and stop Processing (a) if you object to the accuracy of your Personal Data, in which case the Processing shall be restricted to a specific period allowing us to verify accuracy of the data, or (b) if you object to the Processing of your Personal Data in violation of the agreed purposes, or (c) if the Processing is made in violation of the provisions of PDPL and the legislation in force.

You have the right to request us to continue to keep your Personal Data after fulfillment of the purposes of Processing, if such data is necessary to complete procedures related to claiming or defending rights and legal proceedings.

Notwithstanding the provisions of Article 16 (1) PDPL, we may proceed with the Processing of your Personal Data without your Consent (a) if the Processing is limited to storing Personal Data, or (b) if the Processing is necessary to initiate or defend against any actions to claim rights or legal proceedings, or


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

related to judicial procedures, or (c) if the Processing is necessary to protect the rights of third parties in accordance with the legislation in force, or (d) if the Processing is necessary to protect the public interest.

## IX. Right to Stop Processing (Article 17 PDPL)

You have the right to object to and stop the Processing of your Personal Data (1) if the Processing is for direct marketing purposes, including Profiling related to direct marketing, or (2) if the Processing is for the purposes of conducting statistical surveys, unless the Processing is necessary to achieve the public interest, or (3) if the Processing is in violation of the provisions of Article 5 PDPL.

## X. Right to Processing and Automated Processing (Article 18 PDPL)

You have the right to object to decisions issued with respect to Automated Processing that have legal consequences or seriously affect you, including Profiling.

Notwithstanding the provisions of Art. 18 (1) PDPL, you may not object to the decisions issued with respect to Automated Processing (a) if the Automated Processing is included in the terms of the contract entered into between you and us, or (b) if the Automated Processing is necessary according to other legislation in force in the United Arab Emirates, or (c) if you gave your prior Consent on the Automated Processing in accordance with the conditions set out in Article 6 PDPL.

We apply appropriate procedures and measures to protect the privacy and confidentiality of your Personal Data in the cases referred to Article 18 (2) PDPL, without prejudice to your rights.

At your request we engage human resources in reviewing Automated Processing decisions.

## XI. Communication with the Controller (Article 19 PDPL)

We shall provide appropriate and clear ways and mechanisms to enable you to communicate with us and request the exercise of any of your rights stipulated herein.

Therefore, we inform you, that you can contact us and our Data Protection Officer at any time by email or any other means.

## XII. Filing a Complaint (Article 24 PDPL)

You have the right to file a complaint with the UAE Data Office if you have reasons to believe that any violation of the provisions of PDPL has occurred, or that we Process your Personal Data in violation of the provisions of PDPL, in accordance with the procedures and rules established by the USA Data Office in this regard.


© All rights reserved by Heiko Maniero.

# ARABIC: Information about the Processing of Personal Data (Decree Law No. 45 of 2021 (PDPL) - United Arab Emirates)

معلومات حول معالجة البيانات الشخصية (المرسوم القانوني رقم 45 لعام 2021 (قانون حماية البيانات الشخصية) الإمارات العربية المتحدة)

سيدي / سيدتي :

تستحق البيانات الشخصية حماية متميزة لكل فرد له أي علاقة بشركتنا سواء كان متعاقداً أو ما قبل التعاقد أو له أي علاقة أخرى بنا ، فهدفنا هو حفظ بياناتكم لدينا على أعلى مستوى لذلك نقوم على نحو بشكل روتيني بتطوير مفاهيم حماية البيانات و أمنها

بالطبع مع الامتثال للأحكام القانونية للمرسوم القانوني رقم 45 لعام 2021 (قانون حماية البيانات الشخصية) ، حيث يفي هذا المستند بالتزاماتنا بتقديم المعلومات تجاهك .

إن مصطلحات اللوائح القانونية معقدة و للأسف لا يمكن الاستغناء عن استخدام المصطلحات القانونية في اعداد هذا المستند لذلك نود الإشارة أنه يمكنك دائماً التواصل معنا حول أية أسئلة تخص هذا المستند أو المصطلحات أو الصياغات المستخدمة .

## أولاً- تعاريف:

إن قانون حماية البيانات الشخصية هو مرسوم قانوني رقم 45 لعام 2021 و الذي صُدر من قصر الرئاسة في أبو ظبي و المنشور في الجريدة الرسمية و الذي أصبح ساري المفعول منذ الثاني من شهر كانون الثاني/يناير لعام 2022 ، بصيغته المعدلة أو المستبدلة من وقت لآخر ، بالإضافة إلى جميع اللوائح التنظيمية ذات الصلة بالمرسوم أو تجسيدها و تطبق التعاريف القانونية من المادة الأولى من قانون حماية البيانات الشخصية .

## ثانياً- حالات معالجة بيانات الحماية بدون موافقة العميل : ( المادة الرابعة من قانون حماية البيانات الشخصية )

لا نقوم عادة بمعالجة بيانات العميل الخاصة دون موافقته بشكل عام و لكننا قد نعالجها من دون موافقة في الحالات التالية و التي تعتبر قانونية و هي : (1) إذا كانت المعالجة ضرورية لحماية المصلحة العامة ، أو (2) إذا كانت المعالجة تخص البيانات الشخصية للعميل و التي أصبحت متاحة و عامة بسبب فعل قام به االعميل ، أو (3) إذا كانت المعالجة ضرورية لبدء أو لدفاع ضد أي إجراءات قانونية أو المطالبة بحقوق أو ان كانت تتعلق بإجراءات قضائية أو أمنية ، أو (4) إذا كانت المعالجة ضرورية لأغراض الطب المهني أو الوقائي من أجل تقييم قدرة الموظف على العمل ، أو من أجل التشخيص الطبي و توفير الرعاية الصحية و الاجتماعية ،


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

أو العلاج و خدمات التأمين الصحي ، أو من أجل إدارة أنظمة الرعاية الصحية و الاجتماعية و خدماتها وفقاً للتشريعات المعمول بها في دولة الإمارات العربية المتحدة ، أو (5) إذا كانت المعالجة ضرورية لحماية الصحة العامة و التي تتضمن الحماية من الأمراض المعدية و الأوبئة ، أو لأغراض ضمان سلامة و جودة الرعاية الصحية و الأدوية و العقاقير و الأجهزة الطبية وفقاً للتشريعات المعمول بها في دولة الإمارات العربية المتحدة ، أو (6) إذا كانت المعالجة ضرورية لأغراض الأرشفة أو للدراسات العلمية و التاريخية و الإحصائية وفقاً للتشريعات المعمول بها في دولة الإمارات العربية المتحدة ، أو (7) إذا كانت المعالجة ضرورية من أجل حماية مصالحك الشخصية ، أو (8) إذا كانت المعالجة ضرورية لنا أو لكم للإيفاء بالالتزامات و ممارسة الحقوق المقررة قانونياً في مجال التوظيف أو الضمان الاجتماعي أو قوانين الحماية الاجتماعية بالقدر الذي تسمح به تلك القوانين ، أو (9) إذا كانت المعالجة ضرورية لتنفيذ عقد يكون العميل طرفاً فيه أو لاتخاذ إجراءات كإبرام العقد أو تعديله أو إنهائه بناءً على طلبه ، أو (10) إذا كانت المعالجة ضرورية للإيفاء بالالتزامات المفروضة علينا بموجب قوانين أخرى للإمارات العربية المتحدة ، (11) أو أي حالات أخرى يحددها النظام التنفيذي لقانون حماية البيانات الشخصية .

## ثالثاً- شروط الموافقة على معالجة البيانات :( المادة السادسة من قانون حماية البيانات الشخصية )

يجب إعطاء الموافقة بطريقة واضحة و بسيطة لا لبس فيها و يسهل الوصول إليها ، سواء بشكل كتابي أو الكتروني ، لذلك نرجو منك إبلاغنا إذا كنت لا تفهم اللغة الخاصة بنا أو إذا كنت تعتقد أن الموافقة ليست واضحة أو بسيطة لا لبس فيها أو لا يسهل الوصول إليها.

و في حال أراد العميل سحب موافقته على معالجة البيانات الشخصية فإنه يحق له ذلك في أي وقت و سوف تكون عملية السحب في غاية اليسر و له الحرية المطلقة في استخدام أي وسيلة متاحة له ( على سبيل المثال : عبر الاستمارة الالكترونية أو البريد الالكتروني أو عبر الهاتف ) . يرجى العلم أن سحب الموافقة لن يؤثر على شرعية و قانونية المعالجة التي تمت بناءً على الموافقة الممنوحة قبل السحب .

## رابعاً- موظف حماية البيانات : ( المادة العاشرة من قانون حماية البيانات الشخصية )

لقد قمنا بتعيين مسؤول حماية البيانات الذي لديه المهارات و المعرفة الكافية لحماية البيانات الشخصية و قد ذُكر عنوانه أعلاه . يحق للعميل إرسال الطلبات و الشكاوى المتعلقة بالبيانات الشخصية وفقاً لأحكام قانون حماية البيانات الشخصية و لوائحه التنفيذية إلى مسؤول حماية البيانات لدينا .

و بإمكان العميل التواصل مع مسؤول الحماية بشأن أي مسألة تتعلق بالبيانات الشخصية و معالجتها كي تتمكن من ممارسة حقوقك وفقاً لأحكام القانون .

## خامساً- الحق في الحصول على المعلومات : (المادة الثالثة من قانون حماية البيانات)


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

للعميل الحق في الحصول على الحقوق التالي ذكرها (بدون مقابل ) :

أ- أنواع البيانات الشخصية التي تتم معالجتها :

بيانات العميل

بيانات العملاء المحتملين

بيانات الموظفين

بيانات الموردين

ب- أغراض المعالجة :

إن الغرض من معالجة البيانات الشخصية هو إدارة جميع العلميات التي تخص المراقب المالي أو العملاء الحاليين أو المحتلمين أو شركاء الأعمال أو العلاقات التعاقدية أو السابقة للتعاقد بين المجموعات المذكورة (بالمعنى الأوسع) أو الالتزامات القانونية للمراقب.

إذا كانت المعالجة ضرورية لحماية المصلحة العامة فإن الغرض من المعالجة هو مراعاة المصلحة العامة و معالجتها ، و إذا كانت المعالجة للبيانات الشخصية و التي أصبحت متاحة و معروفة للعامة بسبب فعل قام به العميل فإن الغرض من المعالجة هو تحقيق أهداف أعمالنا ، و في حال كانت المعالجة ضرورية لبدء أو لدفاع ضد أي إجراءات قانونية أو المطالبة بحقوق أو حتى أنها تتعلق بإجراءات قضائية أو أمنية فإن الغرض من المعالجة هو التصرف في الإجراءات المطلوبة أو من أجلها ، و عندما تكون المعالجة ضرورية لأغراض الطب المهني أو الوقائي من أجل تقييم قدرة الموظف على العمل ، أو من أجل التشخيص الطبي و توفير الرعاية الصحية و الاجتماعية ، أو العلاج و خدمات التأمين الصحي ، أو من أجل إدارة أنظمة الرعاية الصحية و الاجتماعية و خدماتها وفقاً للتشريعات المعمول بها في دولة الإمارات العربية المتحدة فإن الغرض من المعالجة هو تلبية جميع متطلبات تلك القوانين و تحقيق أهداف أعمالنا و مصالحنا المشروعة . و في حين كانت المعالجة ضرورية لحماية الصحة العامة و التي تتضمن الحماية من الأمراض المعدية و الأوبئة ، أو لأغراض ضمان سلامة و جودة الرعاية الصحية و الأدوية و العقاقير و الأجهزة الطبية وفقاً للتشريعات المعمول بها في دولة الإمارات العربية المتحدة فإن الغرض من المعالجة هو تلبية المتطلبات اللازمة لتلك القوانين ، و إذا كانت المعالجة ضرورية لأغراض الأرشفة أو للدراسات العلمية و التاريخية و الإحصائية وفقاً للتشريعات المعمول بها في دولة الإمارات العربية المتحدة فإن الغرض من معالجة البيانات هو الإيفاء بالمتطلبات اللازمة و إذا كانت المعالجة ضرورية لنا أو لكم للإيفاء بالالتزامات و ممارسة الحقوق المقررة قانونياً في مجال التوظيف أو الضمان الاجتماعي أو قوانين الحماية الاجتماعية بالقدر الذي تسمح به تلك القوانين فإن الغرض من المعالجة هو الوفاء بمتطلبات تلك القوانين ، إذا كانت المعالجة ضرورية لنا أو لكم للإيفاء بالالتزامات و ممارسة الحقوق المقررة قانونياً في مجال التوظيف أو الضمان الاجتماعي أو قوانين الحماية الاجتماعية بالقدر الذي تسمح به تلك القوانين فإن الغرض من المعالجة هو الامتثال لتلك القوانين ، و في حال كانت المعالجة ضرورية لتفي بالالتزامات التي تفرضها علينا القوانين الأخرى لدولة الامارات العربية المتحدة فإن الغرض من المعالجة هو الامتثال القانوني ، و عند ما تكون المعالجة ضرورية لأي حالة أخرى تحددها اللوائح التنفيذية لقانون حماية البيانات الشخصية فإن غرض المعالجة هو الامتثال لتلك اللوائح .


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

أ - القرارات المُتخذة بناءً على المعالجة المؤتمتة، بما في ذلك التنميط:

بصفتنا شركة مسؤولة فنحن لا نقوم بأي عمليات لاتخاذ القرار آليا ولا نستخدم التنميط الآلي .

أ - القطاعات والمؤسسات المستهدفة التي ستتم مشاركة البيانات الشخصية معها، سواء داخل دولة الإمارات العربية المتحدة أو خارجها:

السلطات العامة

الهيئات الخارجية

الهيئات الخارجية الأخرى

المعالجة داخل المجموعة

الهيئات الأخرى

أ - الضوابط والمعايير الخاصة بالمدة الزمنية لتخزين البيانات الشخصية والمحافظة عليها

**إجراءات تمويه وتشفير البيانات الشخصية:** تمويه البيانات الشخصية التي لم تعد ضرورية في النص العادي. تشفير المواقع الالكترونية SSL وتشفير البريد الالكتروني TLS 1.2 او 1.3

**الاجراءات الخاصة بضمان السرية الدائمة لأنظمة المعالجة وخدماتها وضمان نزاهتها ومرونتها وتوافرها:** الاتفاقات السرية مع الموظفين، اتفاقيات عدم الافصاح مع أطراف ثالثة، اتفاقيات حماية البيانات مع الموظفين، جدار الحماية؛ مضاد الفيروسات، النسخ الاحتياطية المنتظمة

**الإجراءات الخاصة بضمان القدرة على استعادة توافر البيانات الشخصية والوصول اليها في الوقت المحدد في حال وقوع حادث مادي او تقني:** (انشاء) نسخ احتياطية منتظمة لكامل النظام. (عمل)اختبار منتظم لعملية النسخة الاحتياطية والاستعادة. (القيام) بتدريب منتظم لفريق عمل تكنولوجيا المعلومات.

**العمليات الخاصة باختبار وتقدير وتقييم فعالية الاجراءات التقنية والتنظيمية بشكل منتظم لضمان أمن المعالجة:** عمليات الفحص والتحقق الداخلية، المراجعة الدورية للعمليات من قبل قسم تكنولوجيا المعلومات؛ التدقيق المنتظم

(على سبيل المثال: من قبل مسؤول حماية البيانات)


© All rights reserved by Heiko Maniero.

**إجراءات تحديد هوية المستخدم والحصول على إذن منه:** التوثيق باستعمال اسم المستخدم / كلمة السر؛ التأكد الدوري من التفويضات؛ الدليل الإرشادي لكلمة السر؛ الحد من عدد المدراء؛ إدارة الحقوق بواسطة مدير النظام.

**إجراءات حماية البيانات أثناء الإرسال:** استخدام تقنيات التشفير؛ تسجيل الأنشطة والفعاليات؛ تشفير البريد الإلكتروني ( TLS 1.2 أو 1.3)؛ استخدام محركات الشركة الداخلية/ وهي محركات محظورة الاستعمال من قبل مستخدمين آخرين باستثناء الشركة.

**إجراءات حماية البيانات أثناء التخزين:** تسجيل الأعمال والفعاليات؛ الحد من عدد المدراء؛ جدار الحماية.

**إجراءات لضمان الأمن المادي للمواقع التي يتم فيها معالجة البيانات الشخصية:** نظام القفل اليدوي؛ أقفال أمنية؛ التحكم في المفاتيح.

**إجراءات ضمان تسجيل الفعاليات:** تفعيل على مستوى التطبيق؛ التأكد اليدوي المنتظم من السجلات.

**إجراءات لضمان تشكيل النظام، بما في ذلك التشكيل الافتراضي:** عملية التحكم في تغيير التشكيل؛ ومراقبة حماية البيانات افتراضياً؛ التشكيل فقط بواسطة مدير النظام؛ تدريب دوري لموظفي تكنولوجيا المعلومات.

**إجراءات الحوكمة الداخلية لأمن تكنولوجيا المعلومات وتكنولوجيا المعلومات وإدارتها:** سياسة أمن تكنولوجيا المعلومات؛ تدريب الموظفين على أمن البيانات؛ فريق تكنولوجيا المعلومات مع أدوار ومسؤوليات واضحة.

**إجراءات المصادقة/تأكيد العمليات والمنتجات:** نظرة عامة واضحة على الأحكام المطبقة على المنتجات/الخدمات/العمليات المقدمة؛ التدقيق الداخلية و/أو الخارجية المنتظمة للحسابات؛ إسناد مسؤوليات تدقيق الحسابات إلى خبراء معتمدين.

**إجراءات لضمان التقليل إلى الحد الأدنى من البيانات:** تحديد هدف المعالجة؛ تقييم الصلة بين المعالجة والهدف منها؛ تحديد فترات الاحتفاظ المطبقة لكل فئة من فئات البيانات؛ تأمين محو البيانات بعد انتهاء فترة الاحتفاظ بها.

**إجراءات لضمان جودة البيانات:** تسجيل الدخول وتعديل البيانات؛ تخصيص الحقوق المتعلقة بإدخال البيانات؛ إمكانية تتبع الإدخال، وتعديل البيانات حسب أسماء المستخدمين الفردية (وليس مستخدمي المجموعات).

**الإجراءات الرامية إلى ضمان الاحتفاظ ببيانات محدودة:** التدريب الدوري على فترات الاحتفاظ؛ تدقيق وتقييم منتظمين للبيانات المحتفظ بها.

**إجراءات لضمان المساءلة:** توفير التدريب/ رفع الوعي؛ ضوابط وفحوصات دورية؛ السياسات الملائمة لحماية البيانات، استنتاج SCCs.

**إجراءات السماح بنقل البيانات وضمان حذفها:** يتم تخزين البيانات الشخصية بشكل منظم؛ التأكيد على رصد الموعد النهائي القانوني؛ مراقبة فترات الاحتفاظ؛ إنشاء عملية نقل البيانات؛ المعالجة المناسبة لطلبات مواضيع البيانات؛ حذف آمن للبيانات وتدمير ناقل البيانات.


© All rights reserved by Heiko Maniero.

أ - إجراءات تصحيح أو حذف أو التقليل من المعالجة والاعتراض على البيانات الشخصية.

الإجراء هو إشراك مسؤول حماية البيانات لدينا، والذي يجب أن يتم إبلاغه من قبل كل موظف أو طرف ثالث أو يمكن أن تشارك من قبلك فيما يتعلق بممارسة أي حق من حقوق مواضيع البيانات. يقوم موظف حماية البيانات بتنسيق عملية التصحيح والحذف والتقليل من المعالجة، والاعتراض على معالجة البيانات الشخصية مع الإدارات المعنية، وتلقي تعليقات منها، وعند الانتهاء من القيام بعملية المعالجة أو استيفاء عملية التصحيح والحذف والحد من المعالجة، أو الاعتراض، سيقوم مسؤول حماية البيانات بإعلامك بالمجريات التي تمت بخصوص طلبك.

أ - إجراءات حماية المعالجة عبر الحدود المتخذة وفقا للمادتين (22) و (23) من قانون حماية البيانات الشخصية

اتفقنا مع كل متلقي للبيانات عبر الحدود (على الأقل) على إجراءات الحماية التالية:

**إجراءات التسمية المستعارة وتشفير البيانات الشخصية:** التسمية المستعارة للبيانات الشخصية التي لم تعد هناك حاجة إليها في النص العادي؛ تشفير المواقع الشبكية (SSL)؛ تشفير البريد الإلكتروني (TLS 1.2 أو 1.3).

**إجراءات لضمان السرية والنزاهة والإتاحة والمرونة المستمرة لنظم وخدمات المعالجة:** اتفاقيات الحفاظ على السرية مع الموظفين؛ اتفاقيات عدم إفشاء المعلومات مع أطراف ثالثة؛ اتفاقيات حماية البيانات مع الموظفين؛ جدار الحماية؛ مكافحة الفيروسات؛ النسخ الاحتياطية العادية.

**إجراءات لضمان القدرة على استعادة توافر البيانات الشخصية والحصول عليها في الوقت المناسب في حال وقوع حادث مادي أو تقني:** النسخ الاحتياطية الدورية للنظام بأكمله؛ اختبار دوري للنسخ الاحتياطي والاسترداد؛ تدريب دوري لموظفي تكنولوجيا المعلومات.

**عمليات لاختبار فعالية الإجراءات التقنية والتنظيمية وتقييمها بانتظام من أجل ضمان أمن المعالجة:** عمليات التحقق الداخلية؛ المراجعة الدورية للعمليات بواسطة تكنولوجيا المعلومات؛ التدقيق الدوري للحسابات (على سبيل المثال، من قبل مسؤول حماية البيانات).

**إجراءات تحديد هوية المستخدم والحصول على إذن منه:** التوثيق باستعمال اسم المستخدم / كلمة السر؛ التأكد الدوري من التفويضات؛ الدليل الإرشادي لكلمة السر؛ الحد من عدد المدراء؛ إدارة الحقوق بواسطة مدير النظام.

**إجراءات حماية البيانات أثناء الإرسال:** استخدام تقنيات التشفير؛ تسجيل الأنشطة والفعاليات؛ تشفير البريد الإلكتروني ( TLS 1.2 أو 1.3)؛ استخدام محركات الشركة الداخلية/ وهي محركات محظورة الاستعمال من قبل مستخدمين آخرين باستثناء الشركة.

**إجراءات حماية البيانات أثناء التخزين:** تسجيل الأعمال والفعاليات؛ الحد من عدد المدراء؛ جدار الحماية.

**إجراءات لضمان الأمن المادي للمواقع التي يتم فيها معالجة البيانات الشخصية:** نظام القفل اليدوي؛ أقفال أمنية؛ التحكم في المفاتيح.

**إجراءات ضمان تسجيل الفعاليات:** تفعيل على مستوى التطبيق؛ التأكد اليدوي المنتظم من السجلات.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

**إجراءات لضمان تشكيل النظام، بما في ذلك التشكيل الافتراضي:** عملية التحكم في تغيير التشكيل؛ ومراقبة حماية البيانات افتراضياً؛ التشكيل فقط بواسطة مدير النظام؛ تدريب دوري لموظفي تكنولوجيا المعلومات.

**إجراءات الحوكمة الداخلية لأمن تكنولوجيا المعلومات وتكنولوجيا المعلومات وإدارتها:** سياسة أمن تكنولوجيا المعلومات؛ تدريب الموظفين على أمن البيانات؛ فريق تكنولوجيا المعلومات مع أدوار ومسؤوليات واضحة.

**إجراءات المصادقة/تأكيد العمليات والمنتجات:** نظرة عامة واضحة على الأحكام المطبقة على المنتجات/الخدمات/العمليات المقدمة؛ التدقيق الداخلية و/أو الخارجية المنتظمة للحسابات؛ إسناد مسؤوليات تدقيق الحسابات إلى خبراء معتمدين.

**إجراءات لضمان التقليل إلى الحد الأدنى من البيانات:** تحديد هدف المعالجة؛ تقييم الصلة بين المعالجة والهدف منها؛ تحديد فترات الاحتفاظ المطبقة لكل فئة من فئات البيانات؛ تأمين محو البيانات بعد انتهاء فترة الاحتفاظ بها.

**إجراءات لضمان جودة البيانات:** تسجيل الدخول وتعديل البيانات؛ تخصيص الحقوق المتعلقة بإدخال البيانات؛ إمكانية تتبع الإدخال، وتعديل البيانات حسب أسماء المستخدمين الفردية (وليس مستخدمي المجموعات).

**الإجراءات الرامية إلى ضمان الاحتفاظ ببيانات محدودة:** التدريب الدوري على فترات الاحتفاظ؛ تدقيق وتقييم منتظمين للبيانات المحتفظ بها.

**إجراءات لضمان المساءلة:** توفير التدريب/ رفع الوعي؛ ضوابط وفحوصات دورية؛ السياسات الملائمة لحماية البيانات، استنتاج SCCs.

**إجراءات السماح بنقل البيانات وضمان حذفها:** يتم تخزين البيانات الشخصية بشكل منظم؛ التأكيد على رصد الموعد النهائي القانوني؛ مراقبة فترات الاحتفاظ؛ إنشاء عملية نقل البيانات؛ المعالجة المناسبة لطلبات مواضيع البيانات؛ حذف آمن للبيانات وتدمير ناقل البيانات.

أ - الإجراءات الواجب اتخاذها في حالة انتهاك أو خرق البيانات الشخصية، خاصة إذا كان الانتهاك أو الخرق يشكل تهديداً مباشراً وخطيراً لخصوصية البيانات الشخصية وسريتها.

الإجراء هو إشراك مسؤول حماية البيانات لدينا، والذي سيقدم لنا المشورة بشأن جميع الخطوات اللازمة. ومع ذلك، فور علمنا بأي انتهاك أو خرق للبيانات الشخصية الخاصة بك والذي من شأنه أن يضر بالخصوصية، وسرية هذه البيانات وأمنها، فإننا سنقوم بإبلاغ مكتب البيانات في الإمارات العربية المتحدة عن هذا الانتهاك أو الخرق ونتائج التحقيق في غضون هذه الفترة وفقاً للإجراءات والشروط المنصوص عليها في اللائحة التنفيذية لاتفاقية حقوق حماية البيانات الشخصية.

وسيكون الإبلاغ مرفقاً بالبيانات والوثائق التالية (أ) طبيعة الانتهاك وشكله وأسبابه وعدده التقريبي وسجلاته؛ (ب) وبيانات موظف حماية البيانات المعين من قبلنا؛ (ج) الآثار المحتملة والمتوقعة للانتهاك أو الخرق؛ (د) والإجراءات والتدابير التي اتخذناها


© All rights reserved by Heiko Maniero.

والمقترح تطبيقها لمعالجة هذا الانتهاك والتقليل من آثاره السلبية؛ (هـ) وتوثيق الانتهاك أو الانتهاك والإجراءات التصحيحية التي اتخذناها، (و) وأي متطلبات أخرى يصدرها مكتب البيانات في الإمارات العربية المتحدة.

في كل الحالات، سنقوم بإبلاغك في حال كان الانتهاك أو الخرق سيضر بخصوصية وسرية وأمن بياناته/ بياناتها الشخصية وإبلاغه/ إبلاغها بالإجراءات التي اتخذناها، خلال هذه الفترة ووفقاً للإجراءات والشروط المنصوص عليها في اللائحة التنفيذية لـقانون حماية البيانات الشخصية.

وافق المسؤولون عن المعالجة لدينا، فور علمهم بأي انتهاك أو خرق للبيانات الشخصية الخاصة بك، على إخطارنا بمثل هذا الانتهاك أو الخرق حتى نتمكن بدورنا من إبلاغ مكتب البيانات في الإمارات العربية المتحدة به وفقاً للقانون.

### أ - عملية تقديم الشكاوى لدى مكتب البيانات في الإمارات العربية المتحدة.

إذا كنت ترغب بتقديم شكوى، فيرجى الاتصال بمكتب البيانات في الإمارات العربية المتحدة المنشأ بموجب مرسوم القانون رقم 44 لعام 2021.

### ب - معلومات إضافية.

سنقوم قبل بدء المعالجة، بتزويدك بالمعلومات الواردة في الفقرات (ب) و (د) و (ز) أعلاه. ومع ذلك، قررنا تزويدك بمزيد من المعلومات لأسباب تتعلق بالشفافية. إذا كنت بحاجة إلى معلومات إضافية أو محددة، فيرجى تقديم طلب إلينا أو إلى مسؤول حماية البيانات لدينا.

نود إعلامك، أنه يمكننا رفض طلبك للحصول على معلومات، إذا تم اكتشاف أن (أ) الطلب ليس له علاقة بالمعلومات المشار إليها في المادة 13 (1) من قانون حماية البيانات الشخصية أو أنه متكرر بشكل مفرط، أو أن (ب) الطلب يتعارض مع الإجراءات القضائية أو التحقيقات التي تجريها السلطات المختصة، أو (ج) أن الطلب قد يؤثر سلباً على الجهود التي نبذلها لحماية أمن المعلومات، أو (د) أن الطلب قد يؤثر على خصوصية وسرية البيانات الشخصية للآخرين.

## سادساً- الحق في طلب نقل البيانات الشخصية (المادة 14 من قانون حماية البيانات الشخصية)

يحق لك الحصول على بياناتك الشخصية المقدمة لنا للمعالجة بطريقة منظمة ومقروءة آلياً، طالما أن المعالجة تستند إلى موافقتك أو ضرورية للوفاء بالتزام تعاقدي ويتم إجراؤها بوسائل آلية.

يحق لك طلب نقل بياناتك الشخصية إلى مراقب آخر في حال كان ذلك ممكناً من الناحية التقنية.

## سابعاً - الحق في تصحيح البيانات الشخصية أو حذفها (المادة 15 من قانون حماية البيانات الشخصية)


© All rights reserved by Heiko Maniero.

يحق لك طلب تصحيح أو استكمال بياناتك الشخصية غير الدقيقة المحتفظ بها لدينا بدون أي تأخير لا داعي له.

دون المساس بالتشريعات النافذة في دولة الإمارات العربية المتحدة وما تقتضيه المصلحة العامة، يحق لك أن تطلب حذف بياناتك الشخصية المحفوظة لدينا، عندما (أ) لم تعد بياناتك الشخصية مطلوبة للأغراض التي تم جمعها أو معالجتها من أجلها، أو (ب) إذا سحبت موافقتك التي تستند إليها المعالجة، أو (ج) إذا كان هدفك في المعالجة أو إذا لم تكن هناك أسباب مشروعة لدينا لمواصلة المعالجة، أو (د) إذا كانت معالجة بياناتك الشخصية تنتهك أحكام قانون حماية البيانات الشخصية والتشريعات المطبقة، وكانت عملية الحذف ضرورية للالتزام بالتشريعات المطبقة والمعايير المعتمدة بهذا الصدد.

باستثناء ما هو موجود في المادة 15 (2) من قانون حماية البيانات الشخصية، لا يحق لك طلب حذف بياناتك الشخصية التي نحتفظ بها (أ) إذا كان الطلب يتعلق بحذف بياناتك الشخصية المتعلقة بالصحة العامة والمودعة لدى مؤسسات خاصة، أو (ب) إذا كان الطلب يؤثر على إجراءات التحقيق أو المطالبات بالحقوق والإجراءات القانونية أو الدفاع عنا، أو (ج) إذا تعارض الطلب مع التشريعات الأخرى التي نخضع لها، أو (د) في أي حالات أخرى تحددها الأنظمة التنفيذية لقانون حماية البيانات الشخصية.

## ثامناً- الحق في تقييد المعالجة (المادة 16 من قانون حماية البيانات الشخصية)

يحق لك إلزامنا بالتقييد والتوقف عن المعالجة (أ) إذا اعترضت على دقة بياناتك الشخصية، وفي هذه الحالة تقتصر المعالجة على فترة محددة تسمح لنا بالتحقق من دقة البيانات، أو (ب) إذا اعترضت على معالجة بياناتك الشخصية في حدوث انتهاك للأهداف المتفق عليها، أو (ج) إذا كانت المعالجة مخالفة لأحكام قانون امن قانون حماية البيانات الشخصية والتشريعات السارية المفعول.

يحق لك أن تطلب منا الاستمرار بالاحتفاظ ببياناتك الشخصية بعد تحقيق أغراض المعالجة، إذا كانت هذه البيانات ضرورية لإكمال الإجراءات المتعلقة بالمطالبة أو الدفاع عن الحقوق والإجراءات القانونية.

على الرغم من أحكام المادة 16 (1) من قانون حماية البيانات الشخصية، يمكننا المضي قدماً في معالجة بياناتك الشخصية دون موافقتك (أ) إذا اقتصرت المعالجة على تخزين البيانات الشخصية، أو (ب) إذا كانت المعالجة ضرورية للشروع في أي إجراءات للمطالبة بالحقوق أو الإجراءات القانونية أو للدفاع عنها، أو فيما يتصل بالإجراءات القضائية، أو (ج) إذا كانت المعالجة ضرورية لحماية حقوق الأطراف الثالثة وفقا للتشريعات السارية، أو (د) إذا كانت المعالجة ضرورية لحماية المصلحة العامة.

## تاسعاً- الحق في التوقف عن المعالجة (المادة 17 من قانون حماية البيانات الشخصية)

يحق لك الاعتراض على معالجة بياناتك الشخصية ووقفها (1) إذا كانت المعالجة لأغراض التسويق المباشر، بما في ذلك الملفات المتعلقة بالتسويق المباشر، أو (2) إذا كانت المعالجة لأغراض إجراء استبيانات إحصائية، ما لم تكن المعالجة ضرورية لتحقيق المصلحة العامة، أو (3) إذا كانت المعالجة تنتهك أحكام المادة 5 من قانون حماية البيانات الشخصية.

## عاشراً- الحق في المعالجة والمعالجة الآلية (المادة 18 من قانون حماية البيانات الشخصية)


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

يحق لك الاعتراض على القرارات الصادرة فيما يتعلق بالمعالجة الآلية التي ينجم عنها عواقب قانونية أو تؤثر عليك بشكل خطير، بما في ذلك التصنيف.

على الرغم من أحكام المادة 18 (1) من قانون حماية البيانات الشخصية، لا يمكنك الاعتراض على القرارات الصادرة فيما يتعلق بالمعالجة الآلية (أ) إذا كانت المعالجة الآلية مدرجة في شروط العقد المبرم بيننا وبينك، أو (ب) إذا كانت المعالجة الآلية ضرورية وفقا للتشريعات الأخرى السارية في الإمارات العربية المتحدة، أو (ج) إذا أعطيت موافقتك المسبقة على المعالجة الآلية وفقاً للشروط المنصوص عليها في المادة 6 من قانون حماية البيانات الشخصية.

نحن نطبق الإجراءات والتدابير المناسبة لحماية خصوصية وسرية بياناتك الشخصية في الحالات المشار إليها في المادة 18 (2) من قانون حماية البيانات الشخصية، دون المساس بحقوقك.

بناءً على طلبك، نشرك الموارد البشرية في مراجعة قرارات المعالجة الآلية.

## إحدى عشر- التواصل مع المراقب المالي (المادة 19 من قانون حماية البيانات الشخصية)

سنوفر السبل والآليات المناسبة والواضحة لتمكينك من التواصل معنا وطلب ممارسة أي حق من حقوقك المنصوص عليها في هذه الوثيقة.

لذلك، يرجى العلم أنه يمكنك الاتصال بنا وبمسؤول حماية البيانات لدينا في أي وقت عبر البريد الإلكتروني أو أي وسيلة أخرى.

## اثني عشر- تقديم شكوى (المادة 24 من قانون حماية البيانات الشخصية)

يحق لك تقديم شكوى إلى مكتب البيانات في الإمارات العربية المتحدة إذا كانت لديك أسباب للاعتقاد بحدوث أي انتهاك لأحكام قانون حماية البيانات الشخصية، أو أننا نعالج بياناتك الشخصية بطريقة تنتهك أحكام قانون حماية البيانات الشخصية، وفقاً للإجراءات والقواعد التي وضعها مكتب البيانات بالولايات المتحدة الأمريكية في هذا الصدد.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

# ENGLISH: Information about the Handling of Personal Data, including Personal Information Handling Rules (Personal Information Protection Law of the People's Republic of China - PIPL)

Dear Sir or Madam,

The Personal Information of every individual who is in a contractual, pre-contractual or other relationship with our company deserve special protection. Our goal is to keep our data protection level on a high standard. Therefore, we are routinely developing new data protection and data security concepts.

Of course, we comply with the statutory provisions of the Personal Information Protection Law of the People's Republic of China (PIPL). This document fulfills our information obligations towards you. Our Personal Information Handling Rules are made public and are convenient to read and store. Please feel free to store a copy of our published Personal Information Handling Rules.

The terminology of legal regulations is complicated. Unfortunately, the use of legal terms could not be dispensed with in the preparation of this document. Therefore, we would like to point out that you are always welcome to contact us for all questions concerning this document, the used terms or formulations.

## I. Definitions

**PIPL** means the Personal Information Protection Law of the People's Republic of China, passed at the 30th meeting of the Standing Committee of the 13th National People's Congress on August 20, 2021, that entered into force on November 1, 2021, as amended or superseded from time to time. The legal definitions from Article 73 PIPL are applicable.

**Personal Information** means all kinds of information, recorded by electronic or other means, related to identified or identifiable natural persons, not including information after anonymization Handling.

**Personal Information Handling** includes Personal Information collection, storage, use, processing, transmission, provision, disclosure, deletion, etc.

**Sensitive Personal Information** means Personal Information that, once leaked or illegally used, may easily cause harm to the dignity of natural persons grave harm to personal or property security, including information on biometric characteristics, religious beliefs, specially-designated status, medical health, financial accounts, individual location tracking, etc., as well as the Personal Information of minors under the age of 14.

**Data Protection Officer** means the Personal Information Protection Officer.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## II. When do we Handle your Personal Information? (Article 13 PIPL)

As a Personal Information Handler, we Handle your Personal Information only (a) where we obtain your Consent, or (b) where it is necessary to conclude or fulfill a contract in which you are an interested party, or where necessary to conduct human resources management according to lawfully formulated labor rules and structures and lawfully concluded collective contracts, or (c) where it is necessary to fulfill statutory duties and responsibilities or statutory obligations, or (d) where it is necessary to respond to sudden public health incidents or protect natural persons' lives and health, or the security of their property, under emergency conditions, or (e) where we are Handling Personal Information within a reasonable scope to implement news reporting, public opinion supervision, and other such activities for the public interest, or (f) where we are Handling Personal Information disclosed by persons themselves or otherwise already lawfully disclosed, within a reasonable scope in accordance with the provisions of PIPL, or (g) in other circumstances provided in laws and administrative regulations.

In accordance with all other relevant provisions, when Handling Personal Information, we obtain your Consent. However, obtaining your Consent is not required under conditions in items (b) through (g) above.

## III. Voluntary Consent with full knowledge by means of an explicit statement and the possibility to withdraw your Consent. (Article 14, 15, 16 PIPL)

Where we Handle your Personal Information based on your Consent, you gave us Consent under the precondition of full knowledge. Full knowledge means that you had access to all information published in this Transparency Document before you gave Consent. Your Consent will always be voluntary and part of an explicit statement. You are, in any case, not obliged to give your Consent to us. Where laws or administrative regulations provide that separate Consent or written Consent shall be obtained to Handle your Personal Information, we will follow those laws. Where a change occurs in the purpose of Personal Information Handling, the Handling method, or the categories of your Handled Personal Information, your Consent will be obtained again.

Where we Handle your Personal Information based on your Consent, you have the right to withdraw your Consent at any time. Please feel free to use any convenient way to withdraw your Consent. You may use an email, a letter, an online contact form, or any other convenient method to withdraw your Consent. The withdrawal of your Consent does not affect the lawfulness and legality of Personal Information Handling activities undertaken based on your Consent before the withdrawal of your Consent.

We will not refuse to provide products or services to you on the basis that you do not Consent to the Handling of your Personal Information or withdraw your Consent, except where Handling Personal Information is necessary for the provision of our products or services.

After you have been previously fully informed by means of this Transparency Document (e.g., by receiving a link to the document or having otherwise access to this publication), and when you decide


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

afterwards, to send or transfer your Personal Information by email or other electronic means to us, you automatically Consent by your action to the Handling of your Personal Information, including but not limited to Cross-Border transfers to all data recipients listed in our “List of (sub) processors, recipients in third countries and international organizations”. You have the right to withdraw your Consent at any time. The withdrawal of your Consent does not affect the lawfulness and legality of Personal Information Handling activities undertaken based on your Consent before the withdrawal of your Consent.

## IV. Name or personal name and contact method of the Personal Information Handler. (Article 17 (1) PIPL)

The name or personal name and contact method of the Personal Information Handler is mentioned above, more precisely, in the beginning of this document, in section “A. Identity and the contact details of the Controller”. You may use an email, a letter, an online contact form, or any other convenient method to contact the Personal Information Handler, including contacting the named Data Protection Officer.

## V. Purpose of Personal Information Handling and the Handling methods, the categories of Handled Personal Information, and the retention period. (Article 17 (2) PIPL)

The purpose of Personal Information Handling is the Handling of all operations which concern the Personal Information Handler, customers, prospective customers, business partners or other contractual or pre-contractual relations between the named groups (in the broadest sense) or legal obligations of the Personal Information Handler.

Where Handling of Personal Information is necessary to conclude or fulfill a contract in which you are an interested party, the purpose of the Handling of Personal Information is to conclude or fulfill the contract or to conduct pre-contractual arrangements or execute procedures for amending or terminating the contract.

Where Handling of Personal Information is necessary to conduct human resources management according to lawfully formulated labor rules and structures and lawfully concluded collective contracts, the purpose of the Handling of Personal Information is Handling and management of human resources.

Where Handling of Personal Information is necessary to fulfill statutory duties and responsibilities or statutory obligations, the purpose of the Handling of Personal Information is legal compliance.

Where Handling of Personal Information is necessary to respond to sudden public health incidents or protect natural persons’ lives and health, or the security of their property, under emergency conditions, the purpose of the Handling of Personal Information is to protect public health, the lives and health of individuals, and the security of their property under given emergency conditions.

Where Handling of Personal Information is conducted to Handle Personal Information within a reasonable scope to implement news reporting, public opinion supervision, and other such activities for the public interest, the purpose of the Handling of Personal Information is to protect and act in the public interest.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

Where Handling of Personal Information is conducted to Handle Personal Information disclosed by persons themselves or otherwise already lawfully disclosed, within a reasonable scope in accordance with the provisions of PIPL, the purpose of the Handling of Personal Information is to conduct and fulfill our legitimate business interests.

Where Handling of Personal Information is conducted to Handle in other circumstances provided in laws and administrative regulations, the purpose of the Handling of Personal Information is legal compliance.

In case we Handle Sensitive Personal Information, the specific purpose and a need to fulfill, and the circumstances of strict protection measures, are documented separately and internally, with the goal to protect the individuals. If we Handle your Sensitive Personal Information, please feel free to request specific and additional information from us at any time.

We use the following Handling methods to Handle Personal Information: Manual Handling, Automated Handling, Online Handling, Offline Handling.

The Categories of Handled Personal Information are: Customer data, data of potential customers, data of employees, and data of suppliers.

Except where laws or administrative regulations provide otherwise, our personal information retention periods are the shortest period necessary to realize the purpose of the personal information handling.. After expiration of that period, the corresponding data is routinely deleted, as long as it is no longer necessary for the fulfillment of the contract or the initiation of a contract. Except where laws or administrative regulations provide otherwise, the retention period chosen by us is the shortest period necessary to realize the purpose of the Personal Information Handling.

## VI. Methods and procedures for individuals to exercise the rights provided in PIPL. (Article 17 (3) PIPL)

You may use an email, a letter, an online contact form, or any other convenient method to contact the Personal Information Handler, including contacting the Data Protection Officer, to exercise the rights provided by PIPL.

## VII. Information and Consent regarding cases where we as a personal information handler provide other personal information handlers with the personal information we handle, including personal information handlers located in the People's Republic of China (Article 23 PIPL)

For any case where we, as a personal information handler provide other personal information handlers (including personal information handlers located in the People's Republic of China) with the personal information we handle, we hereby notify you as follows:


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

The name or personal name of the recipient, their contact method, the handling purpose, handling method, and personal information categories are published on our Website in our “List of (sub) processors, recipients in third countries and international organizations”.

In the mentioned document, the “personal name of the recipient” is published as “Company name”, the “contact method” is published as the “Link to website”, which will allow you to use all contact methods mentioned on the other parties website, the “Handling purpose” is published as “Subject matter of (sub-) processing”, the “Handling methods” are published as “Nature of (sub-) processing”, and the “Personal Information categories” are published as “Categories of Personal Data”.

After you have been previously fully informed by means of this Transparency Document (e.g., by receiving a link to the document or having otherwise access to this publication), and when you decide afterwards, to send or transfer your Personal Information by email or other electronic means to us, you automatically separately Consent by your action to the Handling of your Personal Information, including but not limited to companies located in the People’s Republic of China, by all data recipients listed in our “List of (sub) processors, recipients in third countries and international organizations”. You have the right to withdraw your Consent at any time. The withdrawal of your Consent does not affect the lawfulness and legality of Personal Information Handling activities undertaken based on your Consent before the withdrawal of your Consent.

## VIII. Sensitive Personal Information. (Article 28, 29, 30 PIPL)

We may Handle your Sensitive Personal Information, where there is a specific purpose and a need to fulfill. If we Handle your Sensitive Personal Information, we apply strict protection measures.

If we Handle your Sensitive Personal Information, separate Consent was or is obtained from you, and where laws or administrative regulations provide that written Consent shall be obtained for Handling Sensitive Personal Information, we obtain written Consent in compliance with the provisions of such laws or administrative regulations.

If we Handle your Sensitive Personal Information, we notify you of the necessity and influence on your rights and interests of Handling the Sensitive Personal Information by using separate Consent language. Please feel free to request a copy of such separate Consent language from us at any time. If we Handle your Sensitive Personal Information, please feel free to request specific or additional information from us at any time.

## IX. Information about providing Personal Information outside of the borders of the People’s Republic of China (Article 39 PIPL)

We transfer Personal Information to receivers outside of the borders of the People’s Republic of China. Therefore, we notify you about the foreign receiving side’s name or personal name, contact method, Handling purpose, Handling methods, and Personal Information categories, as well as ways or procedures for individuals to exercise the rights provided by PIPL with the foreign receiving side, and other such matters, by means of our “List of (sub) processors, recipients in third countries and


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

international organizations", which is published on our Website, or by the following. In the mentioned document, the "side's name or personal name" is published as "Company name", the "contact method" is published as the "Link to website", which will allow you to use all contact methods mentioned on the other parties website, the "Handling purpose" is published as "Subject matter of (sub-) processing", the "Handling methods" are published as "Nature of (sub-) processing", and the "Personal Information categories" are published as "Categories of Personal Data".

We concluded an agreement with the foreign receiving side, and the foreign receiving side shall implement procedures for individuals to exercise their rights provided by PIPL. You shall contact our Data Protection Officer and the Data Protection Officer of the foreign receiving side to exercise your rights by email. We obtain your separate Consent to transfer the Personal Information with separate Consent language. Please feel free to request a copy of such separate Consent language from us at any time.

## X. Right to know about and right to decide relating to your Personal Information (Article 44 PIPL)

You have the right to know about and the right to decide relating to your Personal Information. You have the right to limit or refuse the Handling of your Personal Information by us, unless laws or administrative regulations stipulate otherwise. If you want to exercise these rights, please feel free to contact our Data Protection Officer.

## XI. Right to consult us, to receive a copy of Personal Information and right to a transfer to a designated Personal Information Handler (Article 45 PIPL)

You have the right to consult us and receive a copy of your Personal Information from us, except in circumstances provided in Article 18 (1), or Article 35 of PIPL. If you request a consultation or if you want to receive a copy of your Personal Information, we will initiate the consultation and provide you with a copy of your Personal Information in a timely manner.

You can request that your Personal Information is transferred to a Personal Information Handler that you designated. We will provide a channel to transfer Personal Information to your designated Personal Information Handler, meeting the conditions of the State cybersecurity and informatization department. If you want to exercise these rights, please feel free to contact our Data Protection Officer.

## XII. Right to Correction, Completion and Supplementation (Article 46 PIPL)

If you discover that your Personal Information is incorrect or incomplete, you have the right to request us to correct or complete your Personal Information. When you request to correct or complete your Personal Information, we will verify your Personal Information and correct or complete it in a timely manner. When you request to correct or supplement your Personal Information, we will verify your Personal Information, and correct or supplement it in a timely manner. If you want to exercise these rights, please feel free to contact our Data Protection Officer.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## XIII. Right to Deletion (Article 47 PIPL)

We will proactively delete your Personal Information where one of the following circumstances occurs, namely (1) the Handling purpose has been achieved, is impossible to achieve, or the Personal Information is no longer necessary to achieve the Handling purpose, or (2) we or the Personal Information Handler cease the provision of products or services, or the retention period has expired, or (3) you withdraw your Consent, or (4) we or the Personal Information Handler Handled Personal Information in violation of laws, administrative regulations, or agreements, or (5) in other circumstances provided by laws or administrative regulations.

If we did not delete your Personal Information in the circumstances mentioned above, you have the right to request deletion.

Where the retention period provided by laws or administrative regulations has not expired, or Personal Information deletion is technically hard to realize, we will cease Personal Information Handling except for storage and taking necessary security protective measures. If you want to exercise this right, please feel free to contact our Data Protection Officer.

## XIV. Right to request an explanation of Personal Information Handling Rules (Article 48 PIPL)

You have the right to request us to explain Personal Information Handling rules. If you want to get an explanation about our Personal Information Handling rules, please feel free to contact our Data Protection Officer.

## XV. Inheritance of Rights (Article 49 PIPL)

If your next of kin, a natural person is deceased, you have the right, for the sake of your own lawful, legitimate interests, to exercise the rights provided by Chapter IV PIPL to consult, copy, correct, delete, etc., the Personal Information of the deceased, except where the deceased has arranged otherwise before their death. If you want to exercise your right, please feel free to contact our Data Protection Officer.

## XVI. Exercising your Rights, right to sue us if we reject your request to exercise your rights (Article 50 PIPL)

You may use an email, a letter, an online contact form, or any other convenient method or mechanism to exercise your rights. If you want to exercise any of your rights, please feel free to contact our Data Protection Officer. If we reject your request to exercise your rights, you may file a lawsuit with a People's Court according to the law.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## XVII. Right to file a complaint or report about unlawful Personal Information Handling (Article 50 PIPL)

You have the right to file a complaint or report about unlawful Personal Information Handling activities with departments fulfilling Personal Information protection duties and responsibilities. The Departments fulfilling Personal Information protection duties and responsibilities published their contact methods to accept complaints and reports.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

# 中译文：个人数据处理（包括个人信息处理规则）告知书（中华人民共和国个人信息保护法-PIPL）

敬启者：

凡与本公司存在合同、先合同或其他关系的个人，其个人信息值得特殊保护。保持高标准的数据保护水平是我们的目标。因此，我们将**例行**展新的数据保护和数据安全概念。

当然，本公司也应遵守《中华人民共和国个人信息保护法》（PIPL）的规定。为履行本公司向您承担的告知义务，我们编制了本文件。本公司的《个人信息处理规则》已经公开发布，且便于阅读和存储，欢迎随时下载和保存副本。

法规中使用的术语繁复难懂，而在编制本文件的过程中，我们也不免使用一些法律术语。因此，如您对本文件或其中使用的术语或表达有任何疑问，请随时联系我们。

## I. 定义

**PIPL**指2021年8月20日第十三届全国人民代表大会常务委员会第三十次会议表决通过，自2021年11月1日起施行的《中华人民共和国个人信息保护法》，可能会不时进行修正或被取代。PIPL第73条中的定义适用于本文件。

**个人信息**指以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息，不包括匿名化处理后的信息。

**个人信息处理**包括个人信息的收集、存储、使用、加工、传输、提供、公开、删除等。

**敏感个人信息**指一旦泄露或者非法使用，容易导致自然人的人格尊严受到侵害或者使自然人的人身、财产安全受到危害的个人信息，包括生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹等信息，以及不满十四周岁未成年人的个人信息。

## II. 我们会在哪些情况下处理您的个人信息？（PIPL第十三条）

**作**为个人信息处理者，我们只会在下列情况下处理您的个人信息：（a）取得您的同意；或（b）为订立、履行您作为一方当事人的合同所必需，或者按照依法制定的劳动规章制度和依法签订的集体合同实


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

施人力资源管理所必需；或（c）为履行法定职责或者法定义务所必需；或（d）为应对突发公共卫生事件，或者在紧急情况下为保护自然人的生命健康和财产安全所必需；或（e）为公共利益实施新闻报道、舆论监督等行为，在合理的范围内处理个人信息；或（f）依照PIPL规定在合理的范围内处理个人自行公开或者其他已经合法公开的个人信息；或（g）法律、行政法规规定的其他情形。

根据其他有关规定，处理个人信息时，我们会取得您的同意。然而，在前文（b）项至（g）项所述的情况下，我们在处理个人信息时不必取得您的同意。

## III. 您应当在充分知情的前提下自愿、明确同意我们处理您的个人信息，并有权撤回您的同意。（PIPL第十四条、第十五条、第十六条）

**如**果我们基于您的同意处理您的个人信息，您应当在充分知情的前提下给予同意。充分知情指在给予同意前，您有权查阅本《告知书》中发布的全部信息。您应当始终自愿、明确地作出同意。但不论在任何情况下，您都没有义务必须作出同意。如果法律、行政法规规定处理您的个人信息应当取得您的单独同意或者书面同意，我们将遵守该等规定。如果个人信息的处理目的、处理方式和处理的个人信息种类发生变更，我们将重新取得您的同意。

如果我们基于您的同意处理您的个人信息，您有权随时撤回您的同意。您可使用任何便捷的方式撤回您的同意。您可使用电子邮件、信件、在线联系方式、或者任何其他便捷的方式撤回您的同意。您撤回同意，不影响撤回前基于您的同意已进行的个人信息处理活动的合法性和正当性。

我们不会以您不同意处理您的个人信息或者撤回您的同意为由，拒绝向您提供产品或者服务，但处理个人信息属于提供我们的产品或者服务所必需的除外。

在您已经通过各种方式对本《告知书》充分知情后（例如，收到本文件的链接或者有权通过其他方式查阅本文件），当您决定通过电子邮件或者其他电子方式向我们发送或传输您的个人信息时，您的该等行为将被自动视为同意我们处理您的个人信息，包括但不限于向本公司“（受托）处理者、第三国接收者及国际组织名单”列明的所有数据接收者进行跨境传输。您有权随时撤回您的同意。您撤回同意，不影响撤回前基于您的同意已进行的个人信息处理活动的合法性和正当性。


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## IV. 个人信息处理者的名称或姓名和联系方式。（PIPL第十七条第一款）

关于个人信息处理者的名称或姓名和联系方式已在前文提及，具体请参见前文标题为“A. 控制者身份和联系方式”的部分。您可使用电子邮件、信件、在线联系方式、或者任何其他便捷的方式联系个人信息处理者，包括联系指定的个人信息保护负责人。

## V. 个人信息的处理目的、处理方式，处理的个人信息种类、保存期限。（PIPL第十七条第二款）

个人信息的处理目的是处理所有涉及个人信息处理者、客户、潜在客户、业务合作伙伴或指定团体（指广义上的团体）之间的其他合同或先合同关系或个人信息处理者的法律义务的业务。

我们在为订立、履行您作为一方当事人的合同所必需的情况下处理您的个人信息的，个人信息的处理目的为订立或履行合同、或开展先合同安排、或执行合同修改或终止程序。

我们在为按照依法制定的劳动规章制度和依法签订的集体合同实施人力资源管理所必需的情况下处理您的个人信息的，个人信息的处理目的为处理及管理人力资源。

我们在为履行法定职责或者法定义务所必需的情况下处理您的个人信息的，个人信息的处理目的为遵守法律。

我们在为应对突发公共卫生事件，或者紧急情况下为保护自然人的生命健康和财产安全所必需的情况下处理您的个人信息的，个人信息的处理目的为保护公众健康、或在相关紧急情况下保护自然人的生命健康和财产安全。

如果我们为公共利益实施新闻报道、舆论监督等行为，在合理的范围内处理您的个人信息，个人信息的处理目的为维护公共利益，并为公共利益行事。

如果我们依照PIPL规定在合理的范围内处理个人自行公开或者其他已经合法公开的个人信息，个人信息的处理目的为实施和满足本公司正当商业利益。

如果我们在法律、行政法规规定的其他情形下处理个人信息，个人信息的处理目的为遵守法律。


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

如果我们处理敏感个人信息，我们将在内部单独记录处理该等信息的特定目的和必要性、以及我们为此采取的严格保护措施，以保护相关个人。如果我们处理了您的敏感个人信息，您可以随时要求我们提供具体及额外信息。

我们采用下述处理方式处理个人信息：人工处理、自动化处理、线上处理、线下处理。

我们处理的个人信息种类包括：客户数据、潜在客户数据、员工数据、以及供应商数据。

除法律或行政法规另有规定之外，我们保留个人信息的期限是实现个人信息处理目的所需的最短期限。。任何数据的保存期限届满后，如不再为履行或订立合同所必要，我们通常会删除数据。除法律、行政法规另有规定外，在本公司，个人信息的保存期限应当为实现处理目的所必要的最短时间。

## VI. 个人行使PIPL规定权利的方式和程序。（PIPL第十七条第三款）

如您想要行使PIPL规定的权利，您可使用电子邮件、信件、在线联系方式、或者任何其他便捷的方式联系个人信息处理者，包括联系指定的个人信息保护负责人。

## VII. 关于我们作为个人信息处理者向其他个人信息处理者（包括位于中华人民共和国境内的个人信息处理者）提供我们所处理的个人信息情况的信息和同意（PIPL第二十三条）

关于我们作为个人信息处理者向其他个人信息处理者（包括位于中华人民共和国境内的个人信息处理者）提供我们所处理的个人信息的任何情况，我们特此通知您如下事宜：

接收方的名称或姓名、联系方式、信息处理目的、处理方法和个人信息类别会在我们网站中的“第三国以及国际组织的（委托）处理者、接收方列表”中进行公示。

在上述文件中，“接收方的姓名”显示为“公司名称”，“联系方式”显示为“网站链接”（由此您可使用其他方网站上提到的所有联系方式），“处理目的”显示为“（委托）处理主题”，“处理方法”显示为“（委托）处理的性质”，“个人信息类别”显示为“个人数据的类别”。


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

如您已经通过本《告知书》充分知情（例如，收到本文件的链接或者有权通过其他方式查阅本文件），以及当您决定通过电子邮件或者其他电子方式向我们发送或传输您的个人信息时，您自动将被视为就我们处理您的个人信息进行了单独同意，包括但不限于同意由位于中华人民共和国境内的公司以及由我们“第三国和国际组织的（委托）处理者、接收方列表”中列出的所有数据接收方进行处理。您有权随时撤回您的同意。您撤回同意，不影响撤回前基于您的同意已进行的个人信息处理活动的合法性和正当性。

## VIII. 敏感个人信息。（PIPL第二十八条、第二十九条、第三十条）

**我**们可能会在具有特定目的和充分必要性的情况下处理您的敏感个人信息。如果我们处理您的敏感个人信息，我们将采取严格保护措施。

当我们处理您的敏感个人信息时，我们将取得或确保已经取得您的单独同意，如法律、行政法规规定处理敏感个人信息应当取得书面同意的，我们将按照其规定取得您的书面同意。

如果我们处理您的敏感个人信息，我们会使用单独的同意书向您告知处理敏感个人信息的必要性以及对您个人权益的影响。您可随时要求我们提供该单独的同意书的副本。如果我们处理您的敏感个人信息，您可随时要求我们提供具体或额外信息。

## IX. 个人信息处理者向中华人民共和国境外提供个人信息（PIPL第三十九条）

**我**们向中华人民共和国境外的接收方提供个人信息。因此，我们会通过本公司的“（受托）处理者、第三国接收者及国际组织名单”（该名单已经发布在本公司网站上）或通过下述方式向您告知境外接收方的名称或者姓名、联系方式、处理目的、处理方式、个人信息的种类以及个人向境外接收方行使PIPL规定权利的方式和程序等事项。在前述文件中，“境外接收方的名称或姓名”显示为“公司名称”；“联系方式”显示为“网站链接”（允许您使用其他方网站提供的所有联系方式）；“处理目的”显示为“（委托）处理的主题事项”；“处理方式”显示为“（委托）处理的性质”；“个人信息的种类”显示为“个人数据的种类”。

我们已经与境外接收方订立了协议，境外接收方将实施个人行使PIPL规定权利的程序。如您想要行使这些权利，请通过电子邮件联系本公司及境外接收方的个人信息保护负责人。向中华人民共和国境外提供


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

您的个人信息时，我们会使用单独的同意书取得您的同意。您可随时要求我们提供该单独的同意书的副本。

## X. 您对您的个人信息享有知情权及决定权（PIPL第四十四条）

**您**对您的个人信息享有知情权及决定权。您还有权限制或者拒绝本公司对您的个人信息进行处理，但法律、行政法规另有规定的除外。如果您想要行使这些权利，请联系本公司个人信息保护负责人。

## XI. 您有权向我们查阅、复制您的个人信息，并有权请求将您的个人信息转移至您指定的个人信息处理者（PIPL第四十五条）

**您**有权向我们查阅、复制您的个人信息，但有PIPL第十八条第一款、第三十五条规定情形的除外。如您请求查阅您的个人信息，或者如您想要获得您个人信息的副本，我们将及时提供。

您可请求将您的个人信息转移至您指定的个人信息处理者。符合中国国家网信部门规定条件的，我们会提供转移途径，将个人信息传输给您指定的个人信息处理者。如果您想要行使这些权利，请随时联系本公司个人信息保护负责人。

## XII. 您有权请求更正、补充您的个人信息（PIPL第四十六条）

**如**果您发现您的个人信息不准确或者不完整，您有权请求我们更正、补充。当您请求更正、补充您的个人信息时，我们将对您的个人信息予以核实，并及时更正、补充。如果您想要行使这些权利，请联系本公司个人信息保护负责人。

## XIII. 您有权请求删除您的个人信息（PIPL第四十七条）

**有**下列情形之一的，本公司将主动删除您的个人信息，即：（1）处理目的已实现、无法实现或者个人信息已非为实现处理目的所必要；或（2）本公司或个人信息处理者停止提供产品或者服务，或者保存期限已届满；或（3）您撤回同意；或（4）本公司或个人信息处理者违反法律、行政法规或者违反约定处理个人信息；或（5）法律、行政法规规定的其他情形。

如果本公司在前述情形下未删除您的个人信息，您有权请求删除。


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

法律、行政法规规定的保存期限未届满，或者删除个人信息从技术上难以实现的，我们将停止除存储和采取必要的安全保护措施之外的个人信息处理。如果您想要行使该项权利，请联系本公司个人信息保护负责人。

## XIV. 您有权要求我们对本公司个人信息处理规则进行解释说明（PIPL第四十八条）

**您**有权要求我们对本公司个人信息处理规则进行解释说明。如果您想要获得本公司个人信息处理规则的解释说明，请联系本公司个人信息保护负责人。

## XV. 权利继承（PIPL第四十九条）

**您**的近亲属死亡后，您为了自身的合法、正当利益，可以对死者的相关个人信息行使PIPL第四章规定的查阅、复制、更正、删除等权利，死者生前另有安排的除外。如果您想行使您的权利，请联系本公司个人信息保护负责人。

## XVI. 如果我们拒绝您行使权利的请求，您有权起诉我们（PIPL第五十条）

**您**可使用电子邮件、信件、在线联系方式、或者任何其他便捷的方式或机制行使您的权利。如果您想要行使您的任何权利，请联系本公司个人信息保护负责人。如果本公司拒绝您行使权利的请求，您可依法向人民法院提起诉讼。

## XVII. 您有权投诉或举报非法个人信息处理行为（PIPL第五十条）

**您**有权向履行个人信息保护职责的部门投诉或举报非法个人信息处理行为。履行个人信息保护职责的部门已经公布了受理投诉、举报的联系方式。


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

# ENGLISH: Information about the Processing of Personal Data (Digital Personal Data Protection Act, 2022 of India - DPDPA)

Dear Sir or Madam,

The Personal Data of every individual who is in a contractual, pre-contractual or other relationship with our company deserve special protection. Our goal is to keep our data protection level on a high standard. Therefore, we are routinely developing new data protection and data security concepts.

Of course, we will comply with the statutory provisions of the Digital Personal Data Protection Act, 2022 of India (DPDPA). Because we value privacy, we decided to grant you the rights and inform you based on the proposed law, published by the Ministry of Electronics & Information Technology of India, already before DPDPA is officially in force. This document fulfills our information obligations towards you.

The terminology of legal regulations is complicated. Unfortunately, the use of legal terms could not be dispensed with in the preparation of this document. Therefore, we would like to point out that you are always welcome to contact us for all questions concerning this document, the used terms or formulations.

## I. Definitions

"DPDPA" means the Digital Personal Data Protection Act, 2022, in force from such date decided by the Central Government, after notification in the Official Gazette, and any order by the Central Government published in the Official Gazette, as amended or superseded from time to time. The legal definitions from Section 2 DPDPA are applicable.

## II. Processing in accordance with DPDPA (Section 5 DPDPA)

We Process your Personal Data only in accordance with the provisions of DPDPA and Rules made under DPDPA, for a lawful Purpose for which you have given or where it is deemed that you have given your Consent in accordance with the provisions of DPDPA. "Lawful Purpose" means any Purpose which is not expressly forbidden by law.

## III. Notice (Section 6 DPDPA)

A. In the moment or before we request your Consent, we grant you access to this Transparency Document, that is an itemised notice in clear and plain language, and that contains a description of Personal Data that will be collected by us and the Purpose of Processing of such Personal Data.

***a) Description of Personal Data that will be collected by us:***

We Process customer data, data of potential customers, data of employees, and data of suppliers. We Process the data sets (individual items) that you gave to us or that are obtained in accordance with the law, and that are specifically mentioned in the Consent language or in the form(s) you filled for or with us.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

***b) Purpose of Processing of Personal Data:***

The Purpose of Processing of Personal Data is the handling of all operations which concern us, customers, prospective customers, business partners or other contractual or pre-contractual relations between the named groups (in the broadest sense) or legal obligations of us.

Where we Process your Personal Data in a situation where you voluntarily provided your Personal Data to us, and it is reasonably expected that you would provide such Personal Data, the Purpose of the Processing of your Personal Information is to fulfill our business purpose.

Where we Process your Personal Data for the performance of any function under any law, or the provision of any service or benefit to you, or the issuance of any certificate, license, or permit for any action or activity of us, by the State or any instrumentality of the State, the Purpose of the Processing of Personal Data is to act under that function, provide the service or benefit, or certificate, license, or permit, or to perform or fulfill our business purpose.

Where we Process your Personal Data for compliance with any judgment or order issued under any law, the Purpose of the Processing of Personal Data is legal compliance.

Where we Process your Personal Data for responding to a medical emergency involving a threat to the life or immediate threat to the health of you or any other individual, the Purpose of the Processing of Personal Data is to respond to the medical emergency and to save lives.

Where we Process your Personal Data for taking measures to provide medical treatment or health services to any individual during an epidemic, outbreak of disease, or any other threat to public health, the Purpose of the Processing of Personal Data is to provide medical treatment or health services.

Where we Process your Personal Data for taking measures to ensure safety of, or provide assistance or services to any individual during any disaster, or any breakdown of public order, the Purpose of the Processing of Personal Data is to ensure safety of, or provide assistance or services to the individual(s).

Where we Process your Personal Data for the Purposes related to employment, including prevention of corporate espionage, maintenance of confidentiality of trade secrets, intellectual property, classified information, recruitment, termination of employment, provision of any service or benefit sought by you who is an employee, verification of attendance and assessment of performance the Purpose of the Processing of Personal Data is to review and fulfill contractual obligations and achieve your and/or our contractual and legal interests.

Where we Process your Personal Data in the public interest, including for (a) prevention and detection of fraud, or (b) mergers, acquisitions, any other similar combinations or corporate restructuring transactions in accordance with the provisions of applicable laws, or (c) network and information security, or (d) credit scoring, or (e) operation of search engines for Processing of publicly available Personal Data, or (f) Processing of publicly available Personal Data, or (g) recovery of debt the Purpose of the Processing of Personal Data is to fulfill the respective public interest.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

Where we Process your Personal Data for any fair and reasonable Purpose as may be prescribed after taking into consideration (a) whether the legitimate interests of us in Processing for that Purpose outweigh any adverse effect on your rights, and (b) any public interest in Processing for that Purpose, and (c) the reasonable expectations of you having regard to the context of the Processing, the Purpose of the Processing of Personal Data is to achieve our legitimate interest.

Where Processing of Personal Data is necessary for enforcing any legal right or claim, the Purpose of the Processing of Personal Data is to enforce the legal right or claim.

Where Processing of Personal Data by any court or tribunal or any other body in India is necessary for the performance of any judicial or quasi-judicial function the Purpose of the Processing of Personal Data is to process to achieve the judicial or quasi-judicial function.

Where Personal Data is Processed in the interest of prevention, detection, investigation or prosecution of any offence or contravention of any law the Purpose of the Processing of Personal Data is to achieve the respected interest.

Where Personal Data of Data Principals is not Processed within the territory of India, pursuant to any contract entered into with any person outside the territory of India by any person based in India, the Purpose of the Processing of Personal Data is to fulfill the contract.

B. Where you have given your Consent to the Processing of your Personal Data before the commencement of DPDPA, we should give to you an itemised notice in clear and plain language containing a description of Personal Data of you collected by us and the Purpose for which such Personal Data has been Processed, as soon as it is reasonably practicable. The information mentioned in this Transparency Documents serves as well for this purpose and is given to you as soon as reasonably practical, e.g., by means a link.

## IV. Consent (Section 7 DPDPA) and giving your Consent to share, transfer or transmit your Personal Data (Section 9 DPDPA)

Consent means any freely given, specific, informed and unambiguous indication of your wishes by which you, by a clear affirmative action, signify agreement to the Processing of your Personal Data for the specified Purpose. Our specified Purposes are described above.

Consent requests are always presented to you in clear and plain language. The contact details of a Data Protection Officer are mentioned in this Transparency Document (above). Our Data Protection Officer will respond to any communication from you for the Purpose of exercising your rights under the provisions of DPDPA. We will give you the option to access any Consent request / Consent language in English or any language specified in the Eighth Schedule to the Constitution of India.

Where you gave us Consent for the Processing of your Personal Data, you have the right to withdraw your Consent at any time. We will bear the consequences of such withdrawal. The withdrawal of Consent shall not affect the lawfulness of Processing of the Personal Data based on Consent before its withdrawal.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

The ease of such withdrawal shall be comparable to the ease with which Consent may be given. Hence, please feel free to use any convenient way to withdraw your Consent. You may use an email, a letter, an online contact form, or any other convenient method to withdraw your Consent.

If you withdraw your Consent to the Processing of Personal Data, we will, within a reasonable time, cease and cause our Data Processors to cease Processing of your Personal Data unless such Processing without the Data Principal's Consent is required or authorised under the provisions of DPDPA or any other law.

You may give, manage, review or withdraw your Consent with us through a Consent Manager. "Consent Manager" means a Data Fiduciary which enables you to give, manage, review and withdraw your Consent through an accessible, transparent and interoperable platform. Any Consent Manager used is accountable to you and acts on behalf of you.

We inform you that we regularly share, transfer or transmit the Personal Data to other Data Fiduciaries, or engage, appoint, use or involve Data Processors to Process Personal Data on our behalf, under a valid contract. Such Data Processor may, if permitted under the respective contract with us, further engage, appoint, use, or involve other Data Processors in Processing Personal Data under a valid contract. All data recipients are listed in our "List of (sub) processors, recipients in third countries and international organizations".

**By transferring, transmitting, sending, or giving any Personal Data to us, your automatically Consent to the sharing, transferring, or transmitting of such Personal Data to other Data Fiduciaries, and to the engagement, appointment, using, or involving Data Processors to Process Personal Data on our behalf, under a valid contract. All data recipients are listed in our "List of (sub) processors, recipients in third countries and international organizations". You have the right to withdraw your Consent at any time. The withdrawal of Consent shall not affect the lawfulness of Processing of the Personal Data based on Consent before its withdrawal. Please feel free to use any convenient way to withdraw your Consent. You may use an email, a letter, an online contact form, or any other convenient method to withdraw your Consent.**

## V. Deemed Consent (Section 8 DPDPA)

You are deemed to have given Consent to the Processing of your Personal Data if such Processing is necessary, (a) in a situation where you voluntarily provide your Personal Data to us and it is reasonably expected that you would provide such Personal Data, or (b) for the performance of any function under any law, or the provision of any service or benefit to you, or the issuance of any certificate, license, or permit for any action or activity of you, by the State or any instrumentality of the State, or (c) for compliance with any judgment or order issued under any law, or (d) for responding to a medical emergency involving a threat to the life or immediate threat to the health of you or any other individual, or (e) for taking measures to provide medical treatment or health services to any individual during an epidemic, outbreak of disease, or any other threat to public health, or (f) for taking measures to ensure safety of, or provide assistance or services to any individual during any disaster, or any breakdown of


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

public order, or (g) for the Purposes related to employment, including prevention of corporate espionage, maintenance of confidentiality of trade secrets, intellectual property, classified information, recruitment, termination of employment, provision of any service or benefit sought by you who is an employee, verification of attendance and assessment of performance, or (h) in the public interest, including for prevention and detection of fraud; and mergers, acquisitions, any other similar combinations or corporate restructuring transactions in accordance with the provisions of applicable laws; and network and information security; and credit scoring; and operation of search engines for Processing of publicly available Personal Data; and Processing of publicly available Personal Data; and recovery of debt; and (i) for any fair and reasonable Purpose as may be prescribed after taking into consideration whether the legitimate interests of us in Processing for that Purpose outweigh any adverse effect on your rights; any public interest in Processing for that Purpose; and the reasonable expectations of you having regard to the context of the Processing.

## VI. Publication of Data Protection Officer (Section 9 DPDPA)

We published the business contact information of our Data Protection Officer in this Transparency Document. The Data Protection Officer is able to answer your questions about the Processing of your Personal Data on behalf of us.

## VII. Additional obligations in relation to Processing of Personal Data of children (Section 10 DPDPA)

We will, before Processing any Personal Data of a child, obtain verifiable parental Consent in such manner as may be prescribed. Parental Consent may be obtained from a lawful guardian, where applicable.

**By transferring, transmitting, sending, or giving any Personal Data to us, your automatically confirm that you have completed eighteen years of age, and that you are not a child under DPDPA, or under guardianship.**

## VIII. Right to information about Personal Data (Section 12 DPDPA)

You have the right to obtain from us (a) the confirmation whether we are Processing or have Processed Personal Data about you, and (b) a summary of the Personal Data of you being Processed or that has been Processed by us and the Processing activities undertaken by us with respect to your Personal Data, and (c) in one place, the identities of all the Data Fiduciaries with whom the Personal Data has been shared along with the categories of Personal Data so shared; and (d) any other information as may be prescribed.

## IX. Right to correction and erasure of Personal Data (Section 13 DPDPA)

You have the right to correction and erasure of your Personal Data, in accordance with the applicable laws and in such manner as may be prescribed. Upon receiving a request for such correction and erasure


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

from you, we will (a) correct your inaccurate or misleading Personal Data, or (b) complete your incomplete Personal Data, or (c) update your Personal Data, or (e) erase your Personal Data if it is no longer necessary for the Purpose for which it was Processed unless retention is necessary for a legal Purpose.

## X. Right of grievance redressal (Section 14 DPDPA)

You have the right to readily available means of registering a grievance with us. If you are not satisfied with our response to your grievance or receive no response within seven days or such shorter period as may be prescribed, you may register a complaint with the Board in such manner as may be prescribed.

## XI. Right to nominate (Section 15 DPDPA)

You have the right to nominate, in such manner as may be prescribed, any other individual, who shall, in the event of death or incapacity of yourself, exercise your rights in accordance with the provisions of DPDPA. "Incapacity" means inability to exercise your rights under the provisions of DPDPA due to unsoundness of mind or body.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

# GERMAN: Information über die Bearbeitung von Personendaten nach dem Datenschutzgesetz (DSG) und der Datenschutzverordnung (DSV) der Schweiz

Sehr geehrte Damen und Herren,

dieses Transparenzdokument bezweckt, die betroffenen Personen, über die wir Personendaten bearbeiten, über die Bearbeitung aufzuklären, zum Schutz der Persönlichkeit und der Grundrechte der natürlichen Personen beizutragen und den betroffenen Personen Informationen über die Beschaffung von Personendaten in präziser, transparenter, verständlicher und leicht zugänglicher Form mitzuteilen. Dieses Dokument beinhaltet allgemeingültige Angaben. Sollten Sie spezifischere Informationen von uns benötigen, bitte wenden Sie sich an den nachstehend genannten Datenschutzberater. Dieses Transparenzdokument soll für alle Sachverhalte gelten, die sich in der Schweiz auswirken, auch wenn sie im Ausland veranlasst werden.

## A. Datenschutz-Aufsichtsbehörde (Art. 4 DSG)

Der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB) beaufsichtigt die Anwendung der bundesrechtlichen Datenschutzvorschriften und ist deshalb die für uns zuständige Datenschutz-Aufsichtsbehörde. Beschwerden über unsere Organisation können beim EDÖB anhängig gemacht werden.

Der EDÖB kann über die Webseite https://www.edoeb.admin.ch/ kontaktiert werden.

## B. Aufgaben und Kontaktdaten des Datenschutzberaters (Art. 10 DSG)

Wir haben folgende natürliche Person als Datenschutzberater für die Schweiz ernannt:

Antoine Parella
c/o Cancellarius AG
Pflanzschulstrasse 3
8400 Winterthur
Switzerland
E-Mail: office@cancellarius.ch

Unser Datenschutzberater wirkt bei der Anwendung der Datenschutzvorschriften mit. Er ist auch die Anlaufstelle für alle betroffenen Personen aus der Schweiz. Als betroffene Person wenden Sie sich bitte in allen Fragen rund um den Datenschutz in der Schweiz direkt an unseren Datenschutzberater.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

Der Datenschutzberater ist insbesondere für die Schulung und Beratung unserer Organisation in allen Fragen des Datenschutzes zuständig. Er übt seine Funktion gegenüber uns fachlich unabhängig und weisungsungebunden aus. Er übt ferner keine Tätigkeiten aus, die mit seinen Aufgaben als Datenschutzberater unvereinbar sind und verfügt über die erforderlichen Fachkenntnisse.

## C. Vertretung in der Schweiz (Art. 14 DSG)

Sofern wir einen Sitz oder Wohnsitz im Ausland haben und Daten von betroffenen Personen aus der Schweiz bearbeiten, bezeichnen wir die folgende Person als unsere Vertretung in der Schweiz, die als Anlaufstelle für die betroffenen Personen und den EDÖB dient und auf Anfrage den betroffenen Personen Auskünfte darüber erteilt, wie Sie Ihre Rechte ausüben können:

Prof. Dr. h.c. Heiko Maniero, LL.B., LL.M. mult., M.L.E.
c/o Cancellarius AG
Pflanzschulstrasse 3
8400 Winterthur
Switzerland
E-Mail: info@dg-datenschutz.de

## D. Informationspflicht bei der Beschaffung von Personendaten (Art. 19 DSG)

Nachstehend informieren wir Sie – als betroffene Person – angemessen über die Beschaffung von Personendaten. Wir teilen Ihnen im Folgenden diejenigen Informationen mit, die erforderlich sind, damit Sie Ihre Rechte nach dem Bundesgesetz über Datenschutz (DSG) und der Datenschutzverordnung (DSV) geltend machen können und eine transparente Datenbearbeitung gewährleistet ist.

## E. Identität und Kontaktdaten des Verantwortlichen:

Siehe oben unter “A. Identity and the contact details of the Controller”.

## F. Bearbeitungszwecke und Rechtsgrundlagen:

Allgemeiner Zweck der Bearbeitung von Personendaten ist die Abwicklung sämtlicher Vorgänge, die den Verantwortlichen, Kunden, Interessenten, Geschäftspartner oder sonstige vertragliche oder vorvertragliche Beziehungen zwischen den genannten Gruppen (im weitesten Sinne) oder gesetzliche Pflichten des Verantwortlichen betreffen.

Ihre Zustimmung dient unserem Unternehmen als Rechtsgrundlage für Bearbeitungsvorgänge, bei denen wir eine Einwilligung für einen bestimmten Bearbeitungszweck einholen (Art. 31 Abs. 1 Alt. 1 DSG).

Wir stützen die Bearbeitung Ihrer Personendaten entweder auf die Einwilligung oder auf überwiegende private Interessen (Art. 31 Abs. 1 Alt. 2 DSG), auf überwiegende öffentliche Interessen (Art. 31 Abs. 1


© All rights reserved by Heiko Maniero.

Alt. 3 DSG) oder auf Gesetze (Art. 31 Abs. 1 Alt. 4 DSG). Die geltenden Gesetze dienen uns immer dann als Rechtsgrundlage für die Bearbeitung, wenn wir einer rechtlichen Verpflichtung unterliegen, die eine Bearbeitung von Personendaten erforderlich macht, wie beispielsweise die Erfüllung steuerlicher Verpflichtungen.

Auf überwiegende private Interessen des Verantwortlichen stützen wir uns unter anderem bei der Bearbeitung (1) von Personendaten über unsere Vertragspartner und Vertragspartnerinnen, wenn die Bearbeitung in unmittelbarem Zusammenhang mit dem Abschluss oder der Abwicklung eines Vertrags stattfindet, und/oder (2) von Personendaten von wirtschaftlichen Wettbewerbern oder von Personen mit denen wir künftig in wirtschaftlichem Wettbewerb treten, die wir zu diesem Zweck bearbeiten und die wir Dritten nicht bekanntgeben, und/oder (3) von Personendaten zur Prüfung der Kreditwürdigkeit der betroffenen Person, wobei es sich weder um besonders schützenswerte Personendaten noch um ein Profiling mit hohem Risiko handelt, und die Daten Dritten nur bekanntgegeben werden, wenn diese die Daten für den Abschluss oder die Abwicklung eines Vertrags mit der betroffenen Person benötigen, und die Daten nicht älter als zehn Jahre sind, und die betroffene Person volljährig ist, und/oder (4) von Personendaten für nicht personenbezogene Zwecke, insbesondere für Forschung, Planung oder Statistik, wobei wir die Daten anonymisieren, sobald der Bearbeitungszweck dies erlaubt und wenn eine Anonymisierung unmöglich ist oder unverhältnismäßigen Aufwand erfordert, angemessene Maßnahmen treffen, um die Bestimmbarkeit der betroffenen Person zu verhindern, und wenn es sich um besonders schützenswerte Personendaten handelt, diese Dritten nur so bekannt gegeben werden, dass die betroffenen Personen nicht bestimmbar sind und sofern dies nicht möglich ist, gewährleistet ist, dass die Dritten die Daten nur zu nicht personenbezogenen Zwecken bearbeiten, und die Ergebnisse so veröffentlicht werden, dass die betroffenen Personen nicht bestimmbar sind, und/oder (5) Personendaten über eine Person des öffentlichen Lebens sammeln, die sich auf das Wirken dieser Person in der Öffentlichkeit beziehen.

Auf überwiegende öffentliche Interessen stützen wir uns insbesondere, wenn wir Daten zu einem höheren Zweck bearbeiten, der dem Allgemeinwohl dienlich ist oder dieses zumindest fördert.

## G. Kategorien von Empfängerinnen und Empfängern, denen Personendaten bekanntgegeben werden:

Öffentliche Stellen

Externe Stellen

Weitere externe Stellen

Interne Bearbeitung

Konzerninterne Bearbeitung

Sonstige Stellen


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## H. Kategorien der bearbeiteten Personendaten:

Kundendaten

Interessentendaten

Beschäftigtendaten

Lieferantendaten

## I. Informationen hinsichtlich der Bekanntgabe ins Ausland:

Bei einer Bekanntgabe von Personendaten ins Ausland, ist der betroffenen Person auch der Staat oder das internationale Organ und gegebenenfalls die Garantien nach Art. 16 Abs. 2 DSG oder die Anwendung einer Ausnahme nach Art. 17 DSG mitzuteilen.

Der Staat oder das internationale Organ ergibt sich aus der von uns publizierten Liste der (Unter-) Auftragsverarbeiter. Diese Liste finden Sie auf unserer Webseite. Als Garantie nach Art. 16 Abs. 2 DSG, setzen wir grundsätzlich Standarddatenschutzklauseln, die der EDÖB vorgängig genehmigt hat (Art. 16 Abs. 2 lit. d DSG) ein.

Sollten wir im Zusammenhang mit einer Bekanntgabe ins Ausland ausnahmsweise keine Standarddatenschutzklauseln abschließen, holen wir grundsätzlich eine ausdrückliche Einwilligung von Ihnen ein. Davon ausgenommen sind Bekanntgaben ins Ausland, die in unmittelbarem Zusammenhang mit dem Abschluss oder der Abwicklung eines Vertrags zwischen uns und Ihnen, oder mit einem in Ihrem Interesse abgeschlossenen Vertrag zwischen uns und einem anderen Vertragspartner stehen.

Zudem geben wir gegebenenfalls Personendaten ohne Standarddatenschutzklauseln und ohne Ihre ausdrückliche Einwilligung ins Ausland bekannt, wenn dies notwendig ist für (1) die Wahrung eines überwiegenden öffentlichen Interesses, oder (2) die Feststellung, Ausübung oder Durchsetzung von Rechtsansprüchen vor einem Gericht oder einer anderen zuständigen ausländischen Behörde, oder (3) um Ihr Leben oder Ihre körperliche Unversehrtheit oder das Leben oder die körperliche Unversehrtheit eines Dritten zu schützen, wenn es nicht möglich ist, innerhalb einer angemessenen Frist Ihre Einwilligung einzuholen, oder (4) wenn Sie die Personendaten allgemein zugänglich gemacht und eine Bearbeitung nicht ausdrücklich untersagt haben, oder (5) wenn die Personendaten aus einem gesetzlich vorgesehenen Register stammen, das öffentlich oder Personen mit einem schutzwürdigen Interesse zugänglich ist, soweit im Einzelfall die gesetzlichen Voraussetzungen der Einsichtnahme erfüllt sind.

## J. Informationspflicht bei einer automatisierten Einzelentscheidung (Art. 21 DSG)

Entscheidungen, die ausschließlich auf einer automatisierten Bearbeitung beruhen und die für Sie mit einer Rechtsfolge verbunden sind oder Sie erheblich beeinträchtigen (automatisierte Einzelentscheidung) werden von uns nicht getroffen. Ausgenommen sind automatisierte


© All rights reserved by Heiko Maniero.

Einzelentscheidungen, die in unmittelbarem Zusammenhang mit dem Abschluss oder der Abwicklung eines Vertrags zwischen Ihnen und uns stehen, und wenn Ihrem Begehren stattgegeben wird, oder wenn Sie ausdrücklich eingewilligt haben, dass die Entscheidung automatisiert erfolgt.

## K. Auskunftsrecht (Art. 25 DSG, Art. 16, 17, 18, 19 DSV)

Sie haben das Recht von uns Auskunft darüber zu verlangen, ob Personendaten über Sie bearbeitet werden. Zur Ausübung dieses Rechts stellen Sie bitte einen schriftlichen Antrag an uns (auch per E-Mail). Die Auskunftserteilung erfolgt schriftlich oder in der Form, in der uns die Daten vorliegen. Das Auskunftsbegehren und die Auskunftserteilung können auf elektronischem Weg erfolgen (z.B. per E-Mail).

Wir müssen angemessene Maßnahmen treffen, um Sie vor Erteilung einer Auskunft als betroffene Person zu identifizieren. Sie sind zur Mitwirkung, insbesondere zur Identifizierung Ihrer Person gegenüber uns, verpflichtet.

Bearbeiten wir Ihre Personendaten gemeinsam mit einem oder mehreren anderen Verantwortlichen, so können Sie das Auskunftsrecht bei jedem Verantwortlichen geltend machen. Betrifft Ihr Begehren Daten, die von einem Auftragsbearbeiter bearbeitet werden, so unterstützt unser Auftragsbearbeiter uns bei der Erteilung der Auskunft, sofern er Ihr Begehren nicht in unserem Auftrag beantwortet.

Wir erteilen Ihnen die Auskunft innerhalb von 30 Tagen seit dem Eingang des Begehrens. Sofern wir die Auskunft nicht innerhalb von 30 Tagen erteilen, so informieren wir Sie darüber und teilen Ihnen mit, innerhalb welcher Frist die Auskunft erfolgt. Verweigern wir die Auskunft, schränken sie ein oder schieben sie auf, so teilen wir Ihnen dies innerhalb derselben Frist mit.

Ist die Erteilung der Auskunft mit einem unverhältnismäßigen Aufwand verbunden, so können wir von Ihnen verlangen, dass sie sich an den Kosten angemessen beteiligen. Die Beteiligung beträgt maximal 300.- Schweizer Franken. Wir müssen Ihnen die Höhe der Beteiligung vor der Auskunftserteilung mitteilen. Bestätigen Sie dann das Gesuch nicht innerhalb von zehn Tagen nach der Mitteilung, so gilt Ihr Gesuch als – ohne Kostenfolge – zurückgezogen.

Wir weisen darauf hin, dass wir berechtigt sind die Auskunft zu verweigern, einzuschränken oder aufzuschieben, wenn die gesetzlichen Voraussetzungen gemäß Art. 26, 27 DSG erfüllt sind.

Nachfolgend erhalten Sie weitere allgemeingültige Informationen, die erforderlich sind und publiziert werden können, damit Sie Ihre Rechte nach dem DSG geltend machen können und eine transparente Datenbearbeitung gewährleistet ist.

## L. die Identität und die Kontaktdaten des Verantwortlichen:

Siehe oben unter “A. Identity and the contact details of the Controller”.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## M. die bearbeiteten Personendaten als solche;

Die von uns über Sie bearbeiteten Personendaten stellen wir Ihnen auf Anfrage gerne in Kopie zur Verfügung.

## N. der Bearbeitungszweck;

Allgemeiner Zweck der Bearbeitung von Personendaten ist, wie oben bereits ausgeführt, die Abwicklung sämtlicher Vorgänge, die den Verantwortlichen, Kunden, Interessenten, Geschäftspartner oder sonstige vertragliche oder vorvertragliche Beziehungen zwischen den genannten Gruppen (im weitesten Sinne) oder gesetzliche Pflichten des Verantwortlichen betreffen. Individuelle Zwecke teilen wir Ihnen gerne auf Anfrage mit.

## O. die Aufbewahrungsdauer der Personendaten oder, falls dies nicht möglich ist, die Kriterien zur Festlegung dieser Dauer;

Das Kriterium für die Festlegung der Aufbewahrungsdauer von Personendaten ist die jeweilige gesetzliche Aufbewahrungsfrist. Nach Ablauf der Frist werden die entsprechenden Daten routinemäßig gelöscht, sofern sie nicht mehr zur Vertragserfüllung oder Vertragsanbahnung erforderlich sind.

## P. die verfügbaren Angaben über die Herkunft der Personendaten, soweit sie nicht bei der betroffenen Person beschafft wurden;

Die verfügbaren Angaben über die Herkunft Ihrer Personendaten, soweit sie nicht bei Ihnen beschafft wurden, stellen wir Ihnen auf Anfrage gerne in Kopie zur Verfügung.

## Q. gegebenenfalls das Vorliegen einer automatisierten Einzelentscheidung sowie die Logik, auf der die Entscheidung beruht;

Siehe oben unter “Informationspflicht bei einer automatisierten Einzelentscheidung (Art. 21 DSG)“.

## R. Kategorien von Empfängerinnen und Empfängern, denen Personendaten bekanntgegeben werden, sowie die Informationen nach Art. 19 Abs. 4 DSG.

Öffentliche Stellen

Externe Stellen

Weitere externe Stellen

Interne Bearbeitung

Konzerninterne Bearbeitung

Sonstige Stellen

Die Informationen nach Art. 19 Abs. 4 DSG finden Sie oben unter „Informationen hinsichtlich der Bekanntgabe ins Ausland“.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## S. Recht auf Datenherausgabe oder -übertragung (Art. 28 DSG, Art. 20 DSV)

Sie haben das Recht, kostenlos die Herausgabe Ihrer Personendaten, die Sie uns bekanntgegeben haben, in einem gängigen elektronischen Format von uns zu verlangen, wenn (1) wir die Daten automatisiert bearbeiten und (2) die Daten mit Ihrer Einwilligung oder in unmittelbarem Zusammenhang mit dem Abschluss oder der Abwicklung eines Vertrags zwischen Ihnen und uns bearbeitet werden.

Sie können zudem vom uns verlangen, dass wir Ihre Personendaten kostenlos einem anderen Verantwortlichen übertragen, wenn die Voraussetzungen nach Art. 28 Abs. 1 DSG erfüllt sind und dies keinen unverhältnismäßigen Aufwand erfordert. Ihre Rechte werden gegebenenfalls über Art. 29 DSG eingeschränkt.

Als Personendaten, die Sie uns bekanntgegeben haben, gelten (1) Daten, die Sie uns wissentlich und willentlich zur Verfügung gestellt haben, und (2) Daten, die wir über Sie und Ihr Verhalten im Rahmen der Nutzung eines Diensts oder Geräts erhoben haben. Personendaten, die wir durch eigene Auswertung der bereitgestellten oder beobachteten Personendaten erzeugt haben, gelten nicht als Personendaten, die Sie uns bekannt gegeben haben.

## T. Rechtsansprüche (Art. 32 DSG)

Sie können verlangen, dass unrichtige Personendaten berichtigt werden, es sei denn (1) eine gesetzliche Vorschrift verbietet die Änderung, oder (2) die Personendaten werden zu Archivzwecken im öffentlichen Interesse bearbeitet.

Klagen zum Schutz der Persönlichkeit richten sich nach den Art. 28, 28a sowie 28g–28l des Zivilgesetzbuchs. Als klagende Partei können Sie insbesondere verlangen, dass (1) eine bestimmte Datenbearbeitung verboten wird, und (2) eine bestimmte Bekanntgabe von Personendaten an Dritte untersagt wird, und (3) dass Personendaten gelöscht oder vernichtet werden. Kann weder die Richtigkeit noch die Unrichtigkeit der betreffenden Personendaten festgestellt werden, so können Sie als klagende Partei verlangen, dass ein Bestreitungsvermerk angebracht wird. Außerdem können Sie als klagende Partei zudem verlangen, dass die Berichtigung, die Löschung oder die Vernichtung, das Verbot der Bearbeitung oder der Bekanntgabe an Dritte, der Bestreitungsvermerk oder das Urteil Dritten mitgeteilt oder veröffentlicht wird.

## U. Anwendbares Recht

Das anwendbare Verfahrensrecht regelt die Bearbeitung von Personendaten und die Rechte der betroffenen Personen in Gerichtsverfahren und in Verfahren nach bundesrechtlichen Verfahrensordnungen. Auf erstinstanzliche Verwaltungsverfahren sind die Bestimmungen des DSG anwendbar. Für privatrechtliche Ansprüche gilt das Bundesgesetz über das Internationale Privatrecht in der jeweils aktuellen Fassung.

## V. EU-U.S. Data Privacy Framework (EU-U.S. DPF), UK Extension to the EU-U.S. DPF, Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF)


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

Wenn unsere Organisation ein zertifiziertes Mitglied des EU-U.S. Data Privacy Framework (EU-U.S. DPF) und/oder der UK Extension to the EU-U.S. DPF und/oder des Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF) ist, gilt das Folgende:

Wir halten uns an das EU-U.S. Data Privacy Framework (EU-U.S. DPF) und die UK Extension to the EU-U.S. DPF sowie an das Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF), wie es vom U.S. Department of Commerce festgelegt wurde. Unser Unternehmen hat gegenüber dem US-Handelsministerium bestätigt, dass es die EU-U.S. Data Privacy Framework Principles (EU-U.S. DPF Principles) in Bezug auf die Verarbeitung personenbezogener Daten einhält, die es aus der Europäischen Union und dem Vereinigten Königreich unter Berufung auf das EU-U.S. DPF und die UK Extension to the EU-U.S. DPF erhält. Unser Unternehmen hat gegenüber dem US-Handelsministerium bestätigt, dass es die Swiss-U.S. Data Privacy Framework Principles (Swiss-U.S. DPF Principles) in Bezug auf die Verarbeitung personenbezogener Daten, die es aus der Schweiz unter Berufung auf die Swiss-U.S. DPF erhält, einhält. Im Falle eines Widerspruchs zwischen den Bestimmungen unserer Datenschutzerklärung und den EU-U.S. DPF Principles und/oder den Swiss-U.S. DPF Principles sind die Principles maßgebend.

Um mehr über das Data Privacy Framework (DPF) Programm zu erfahren und um unsere Zertifizierung einzusehen, besuchen Sie bitte https://www.dataprivacyframework.gov/.

Die anderen US-Einheiten oder US-Tochtergesellschaften unseres Unternehmens, die sich ebenfalls an die EU-U.S. DPF Principals halten, einschließlich der UK Extension to the EU-U.S. DPF und der Swiss-U.S. DPF Principals, sofern vorhanden, werden in unserer Datenschutzerklärung genannt.

In Übereinstimmung mit dem EU-U.S. DPF und der UK Extension to the EU-U.S. DPF sowie des Swiss-U.S. DPF verpflichtet sich unser Unternehmen, mit dem von den EU-Datenschutzbehörden und dem britischen Information Commissioner's Office (ICO) sowie dem Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) eingerichteten Gremium zusammenzuarbeiten und dessen Ratschläge in Bezug auf ungelöste Beschwerden über unseren Umgang mit personenbezogenen Daten zu befolgen, die wir unter Berufung auf die EU-U.S. DPF und die UK Extension to the EU-U.S. DPF und die Swiss-U.S. DPF erhalten haben.

Wir informieren die betroffenen Personen über die zuständigen europäischen Datenschutzbehörden, die für die Bearbeitung von Beschwerden über den Umgang unserer Organisation mit personenbezogenen Daten zuständig sind, im oberen Teil dieses Transparenzdokuments und darüber, dass wir den betroffenen Personen einen angemessenen und kostenlosen Rechtsbehelf anbieten.

Wir informieren alle betroffenen Personen darüber, dass unser Unternehmen den Ermittlungs- und Durchsetzungsbefugnissen der Federal Trade Commission (FTC) unterliegt.

Betroffene Personen haben unter bestimmten Voraussetzungen die Möglichkeit, ein verbindliches Schiedsverfahren in Anspruch zu nehmen. Unsere Organisation ist verpflichtet, Ansprüche zu schlichten und die Bedingungen gemäß Anhang I der DPF-Principals einzuhalten, sofern die betroffene Person ein


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

verbindliches Schiedsverfahren beantragt hat, indem sie unsere Organisation benachrichtigt hat und die Verfahren und Bedingungen gemäß Anhang I der Principals eingehalten hat.

Wir informieren hiermit alle betroffenen Personen über die Haftung unserer Organisation im Falle der Weitergabe von personenbezogenen Daten an Dritte.

Für Fragen der betroffenen Personen oder der Datenschutzaufsichtsbehörden haben wir die oben in diesem Transparenzdokument genannten lokalen Vertreter benannt.

Wir bieten Ihnen die Möglichkeit zu wählen (Opt-out), ob Ihre personenbezogenen Daten (i) an Dritte weitergegeben oder (ii) für einen Zweck verwendet werden sollen, der sich wesentlich von dem/den Zweck(en) unterscheidet, für den/die sie ursprünglich erhoben oder später von Ihnen genehmigt wurden. Der eindeutige, gut sichtbare und leicht zugängliche Mechanismus zur Ausübung Ihres Wahlrechts besteht darin, unseren Datenschutzbeauftragten (DSB) per E-Mail zu kontaktieren. Sie haben keine Wahlmöglichkeit und wir sind auch nicht dazu verpflichtet, wenn die Daten an einen Dritten weitergegeben werden, der als Beauftragter oder Auftragsverarbeiter in unserem Namen und auf unsere Anweisung hin Aufgaben wahrnimmt. Wir schließen jedoch immer einen Vertrag mit einem solchen Beauftragten oder Auftragsverarbeiter ab.

Für sensible Daten (d. h. personenbezogene Daten, die Angaben über den Gesundheitszustand, die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, die Mitgliedschaft in einer Gewerkschaft oder Angaben zum Sexualleben der betreffenden Person enthalten) holen wir Ihre ausdrückliche Zustimmung (Opt-in) ein, wenn diese Daten (i) an Dritte weitergegeben oder (ii) für einen anderen Zweck als denjenigen verwendet werden sollen, für den sie ursprünglich erhoben wurden oder für den Sie nachträglich Ihre Zustimmung erteilt haben, indem Sie Ihre Opt-in-Wahl getroffen haben. Darüber hinaus behandeln wir alle personenbezogenen Daten, die wir von Dritten erhalten, als sensibel, wenn der Dritte sie als sensibel identifiziert und behandelt.

Wir informieren Sie hiermit über das Erfordernis, personenbezogene Daten in Reaktion auf rechtmäßige Anfragen von Behörden offenzulegen, einschließlich der Erfüllung von Anforderungen der nationalen Sicherheit oder der Strafverfolgung.

Bei der Übermittlung personenbezogener Daten an einen Dritten, der als Verantwortlicher handelt, halten wir uns an die Principals der Benachrichtigung und der Wahlmöglichkeit. Außerdem schließen wir mit dem Dritten, der für die Verarbeitung verantwortlich ist, einen Vertrag ab, der vorsieht, dass diese Daten nur für begrenzte und festgelegte Zwecke in Übereinstimmung mit der von Ihnen erteilten Einwilligung verarbeitet werden dürfen und dass der Empfänger das gleiche Schutzniveau wie die Principals des DPF bietet und uns benachrichtigt, wenn er feststellt, dass er diese Verpflichtung nicht mehr erfüllen kann. Der Vertrag sieht vor, dass der Dritte, der Verantwortlicher ist, die Verarbeitung einstellt oder andere angemessene und geeignete Maßnahmen ergreift, um Abhilfe zu schaffen, wenn eine solche Feststellung getroffen wird.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

Bei der Übermittlung personenbezogener Daten an einen Dritten, der als Beauftragter oder Auftragsverarbeiter handelt, (i) übermitteln wir diese Daten nur für begrenzte und festgelegte Zwecke; (ii) vergewissern wir uns, dass der Beauftragte oder Auftragsverarbeiter verpflichtet ist, mindestens das gleiche Maß an Datenschutz zu gewährleisten, wie es die DPF-Principals verlangen; (iii) ergreifen wir angemessene und geeignete Maßnahmen, um sicherzustellen, dass der Beauftragte oder Auftragsverarbeiter die übermittelten personenbezogenen Daten tatsächlich in einer Weise verarbeitet, die mit unseren Verpflichtungen gemäß den DPF-Principals übereinstimmt; (iv) von dem Beauftragten oder Auftragsverarbeiter zu verlangen, dass er unsere Organisation benachrichtigt, wenn er feststellt, dass er seiner Verpflichtung nicht mehr nachkommen kann, das gleiche Schutzniveau zu bieten, wie es die DPF-Principals vorsehen; (v) nach einer Benachrichtigung, auch unter (iv), angemessene und geeignete Schritte zu unternehmen, um die unbefugte Verarbeitung zu stoppen und Abhilfe zu schaffen; und (vi) dem DPF Department auf Anfrage eine Zusammenfassung oder ein repräsentatives Exemplar der einschlägigen Datenschutzbestimmungen seines Vertrags mit diesem Beauftragten zur Verfügung zu stellen.

In Übereinstimmung mit dem EU-U.S. DPF und/oder der UK Extension to the EU-U.S. DPF und/oder der Swiss-U.S. DPF verpflichtet sich unsere Organisation, mit dem von den EU-Datenschutzbehörden und dem britischen Information Commissioner's Office (ICO) bzw. dem Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) eingerichteten Gremium zusammenzuarbeiten und dessen Ratschläge in Bezug auf ungelöste Beschwerden über unseren Umgang mit Personaldaten, die wir unter Berufung auf die EU-U.S. DPF und der UK-Erweiterung der EU-U.S. DPF und der Swiss-U.S. DPF im Zusammenhang mit dem Arbeitsverhältnis erhalten, zu befolgen.

Allen betroffenen Personen, die sich vorübergehend in der Europäischen Union (EU), im Europäischen Wirtschaftsraum (EWR) oder im Vereinigten Königreich aufhalten oder dort ihren Wohnsitz oder gewöhnlichen Aufenthaltsort haben, stehen die in unserem Transparenzdokument publizierten Rechte und Betroffenenrechte zu, die sich auch aus Artikeln 15 bis 22 DS-GVO ergeben, inklusive dem Recht auf Auskunft. Diese Informationen haben wir in allen Sprachen der EU und des EWR zur Verfügung gestellt. Die englische Sprachfassung gilt für das Vereinigte Königreich.

Allen betroffenen Personen, die sich vorübergehend in der Schweiz aufhalten oder dort ihren Wohnsitz oder gewöhnlichen Aufenthaltsort haben, stehen die in unserem Transparenzdokument publizierten Rechte und Betroffenenrechte aus dem Schweizer Datenschutzgesetz (DSG) und der Schweizer Datenschutzverordnung (DSV) zu, inklusive dem Recht auf Auskunft. Diese Informationen haben wir in den drei offiziellen Sprachen der Schweiz (Deutsch, Italienisch und Französisch) zur Verfügung gestellt.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

# ITALIAN: Informazioni sul trattamento dei dati personali ai sensi della Legge sulla protezione dei dati (DSG) e dell'Ordinanza sulla protezione dei dati (DSV ) della Svizzera.

Gentili signore e signori,

lo scopo del presente documento di trasparenza è quello di informare gli interessati che trattano dati personali in merito al trattamento, di contribuire alla tutela della personalità e dei diritti fondamentali delle persone fisiche e di fornire agli interessati informazioni sull'acquisizione dei dati personali in forma precisa, trasparente, comprensibile e facilmente accessibile. Il presente documento contiene informazioni di carattere generale. Se desiderate ricevere da noi informazioni più specifiche, siete pregati di contattare il consulente per la protezione dei dati personali indicato di seguito. Il presente documento di trasparenza si applica a tutte le questioni che hanno un impatto in Svizzera, anche se vengono avviate all'estero.

## A. Autorità di controllo della protezione dei dati (art. 4 FADP)

L'Incaricato federale della protezione dei dati e delle informazioni (IFPDT) vigila sull'applicazione delle norme federali in materia di protezione dei dati ed è pertanto l'autorità di controllo responsabile per noi. I reclami relativi alla nostra organizzazione possono essere presentati all'IFPDT.

L'FDPIC può essere contattato tramite il sito web https://www.edoeb.admin.ch/.

## B. Compiti e dati di contatto del consulente per la protezione dei dati (art. 10 FADP)

Abbiamo nominato la seguente persona fisica come consulente per la protezione dei dati per la Svizzera:

Antoine Parella
c/o Cancellarius AG
Pflanzschulstrasse 3
8400 Winterthur
Svizzera
E-mail: office@cancellarius.ch

Il nostro consulente per la protezione dei dati si occupa dell'applicazione delle norme sulla protezione dei dati. È anche il punto di contatto per tutti gli interessati dalla Svizzera. In qualità di persona interessata, la preghiamo di contattare direttamente il nostro consulente per la protezione dei dati per tutte le domande relative alla protezione dei dati in Svizzera.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

Il consulente per la protezione dei dati è responsabile in particolare della formazione e della consulenza alla nostra organizzazione su tutte le questioni relative alla protezione dei dati. Deve esercitare la sua funzione nei nostri confronti in modo professionalmente indipendente e non vincolato da istruzioni. Inoltre, non deve svolgere attività incompatibili con i suoi compiti di consulente per la protezione dei dati e deve possedere le competenze necessarie.

## C. Rappresentanza in Svizzera (art. 14 LADP)

Se abbiamo una sede o un luogo di residenza all'estero e trattiamo i dati di persone interessate dalla Svizzera, designiamo la seguente persona come nostro rappresentante in Svizzera per fungere da punto di contatto per le persone interessate e l'IFPDT e, su richiesta, per fornire informazioni alle persone interessate su come esercitare i propri diritti:

Prof. Dr. h.c. Heiko Maniero, LL.B., LL.M. mult., M.L.E.
c/o Cancellarius AG
Pflanzschulstrasse 3
8400 Winterthur
Svizzera
E-mail: info@dg-datenschutz.de

## D. Obbligo di fornire informazioni quando si ottengono dati personali (art. 19 FADP)

Di seguito vi forniamo, in qualità di interessati, informazioni adeguate sull'acquisizione dei dati personali. Di seguito vi forniamo le informazioni necessarie per far valere i vostri diritti ai sensi della Legge federale sulla protezione dei dati (LDP) e dell'Ordinanza sulla protezione dei dati (LPD) e per garantire un trattamento trasparente dei dati.

## E. Identità e dati di contatto della persona responsabile:

Si veda il punto "A. Identità e dati di contatto del Titolare del trattamento".

## F. Finalità del trattamento e basi giuridiche:

La finalità generale del trattamento dei dati personali è la gestione di tutte le operazioni riguardanti il titolare del trattamento, i clienti, gli interessati, i partner commerciali o altri rapporti contrattuali o precontrattuali tra i suddetti gruppi (in senso lato) o gli obblighi legali del titolare del trattamento.

Il vostro consenso serve alla nostra azienda come base giuridica per le operazioni di trattamento in cui otteniamo il consenso per uno scopo di trattamento specifico (Art. 31 Par. 1 Alt. 1 DSG).

Il trattamento dei vostri dati personali si basa sul consenso o su interessi privati prevalenti (art. 31 par. 1 alt. 2 LADP), su interessi pubblici prevalenti (art. 31 par. 1 alt. 3 LADP) o sulla legge (art. 31 par. 1 alt. 4 LADP). Le leggi applicabili fungono sempre da base giuridica per il trattamento se siamo soggetti a un


© All rights reserved by Heiko Maniero.

obbligo legale che rende necessario il trattamento dei dati personali, come ad esempio l'adempimento di obblighi fiscali.

Ci basiamo sugli interessi privati prevalenti del titolare del trattamento, tra l'altro, quando trattiamo (1) dati personali relativi ai nostri partner contrattuali, se il trattamento è direttamente connesso alla conclusione o all'esecuzione di un contratto, e/o (2) dati personali relativi a concorrenti economici o a persone con cui entreremo in concorrenza economica in futuro, che trattiamo a tal fine e che non divulghiamo a terzi, e/o (3) di dati personali per verificare la solvibilità dell'interessato, laddove i dati personali non siano particolarmente sensibili né comportino una profilazione ad alto rischio, e i dati siano comunicati a terzi solo se questi ne hanno bisogno per la conclusione o l'esecuzione di un contratto con l'interessato e i dati non abbiano più di dieci anni, e l'interessato è maggiorenne, e/o (4) di dati personali per scopi non personali, in particolare per la ricerca, la pianificazione o la statistica, per cui rendiamo anonimi i dati non appena lo scopo del trattamento lo consente e, se l'anonimizzazione è impossibile o richiederebbe uno sforzo sproporzionato, adottiamo misure appropriate per impedire l'identificazione dell'interessato, e se i dati personali sono particolarmente sensibili, divulgare tali dati a terzi solo in modo tale che gli interessati non possano essere identificati e, qualora ciò non sia possibile, garantire che i terzi trattino i dati solo per scopi non personali e pubblichino i risultati in modo tale che gli interessati non possano essere identificati, e/o (5) raccogliere dati personali su un personaggio pubblico che si riferiscono alle attività di tale persona in pubblico.

Ci basiamo su interessi pubblici prevalenti, in particolare se trattiamo i dati per uno scopo superiore che serve o almeno promuove il bene pubblico.

## G. Categorie di destinatari a cui vengono comunicati i dati personali:

Enti pubblici

Organismi esterni

Altri organismi esterni

Elaborazione interna

Elaborazione intragruppo

Altri esterni

## H. Categorie di dati personali trattati:

Dati del cliente

Dati delle parti interessate

Dati dei dipendenti

Dati del fornitore


© All rights reserved by Heiko Maniero.

## I. Informazioni sulla divulgazione all'estero:

Se i dati personali vengono divulgati all'estero, la persona interessata deve essere informata anche dello Stato o dell'organismo internazionale e, se del caso, delle garanzie di cui all'art. 16 cpv. 2 LADP o dell'applicazione di un'eccezione ai sensi dell'art. 17 LADP.

L'ente statale o internazionale può essere individuato nell'elenco dei (sotto)processori da noi pubblicato. L'elenco è disponibile sul nostro sito web. Come garanzia ai sensi dell'art. 16 cpv. 2 LADP, utilizziamo generalmente clausole standard di protezione dei dati preventivamente approvate dall'IFPDT (art. 16 cpv. 2 lett. d LADP).

Se, in via eccezionale, non stipuliamo clausole standard di protezione dei dati in relazione a una divulgazione all'estero, otterremo sempre il vostro consenso esplicito. Ciò non vale per le divulgazioni all'estero che sono direttamente collegate alla conclusione o all'esecuzione di un contratto tra noi e voi, o a un contratto concluso nel vostro interesse tra noi e un altro partner contrattuale.

Inoltre, possiamo divulgare i dati personali all'estero senza clausole standard di protezione dei dati e senza il vostro consenso esplicito se ciò è necessario per (1) la protezione di un interesse pubblico prevalente, o (2) l'istituzione, l'esercizio o l'applicazione di rivendicazioni legali presso un tribunale o un'altra autorità estera competente, o (3) per proteggere la vostra vita o integrità fisica o la vita o l'integrità fisica di una terza parte, se non è possibile ottenere il vostro consenso entro un periodo di tempo ragionevole, o (4) se avete reso i dati personali generalmente accessibili e non ne avete espressamente vietato il trattamento, o (5) se i dati personali provengono da un registro previsto dalla legge che è accessibile al pubblico o a persone con un interesse meritevole di protezione, a condizione che i requisiti legali per la consultazione siano soddisfatti nel singolo caso.

## J. Obbligo di informazione in caso di decisione individuale automatizzata (art. 21 FADP)

Le decisioni che si basano esclusivamente su un trattamento automatizzato e che comportano una conseguenza legale per l'utente o che lo riguardano in modo significativo (decisione individuale automatizzata) non vengono prese da noi. Fanno eccezione le decisioni individuali automatizzate che sono direttamente collegate alla conclusione o all'esecuzione di un contratto tra voi e noi e se la vostra richiesta viene accolta o se avete espressamente acconsentito alla decisione automatica.

## K. Diritto all'informazione (art. 25 FADP, artt. 16, 17, 18, 19 FADP)

Avete il diritto di richiederci informazioni sul trattamento dei vostri dati personali. Per esercitare questo diritto, vi preghiamo di inviarci una richiesta scritta (anche via e-mail). Le informazioni saranno fornite per iscritto o nella forma in cui disponiamo dei dati. La richiesta di informazioni e la fornitura di informazioni possono essere effettuate per via elettronica (ad es. via e-mail).


© All rights reserved by Heiko Maniero.

Dobbiamo adottare misure ragionevoli per identificarvi come soggetti interessati prima di fornirvi informazioni. Siete obbligati a collaborare, in particolare a identificarvi.

Se trattiamo i vostri dati personali insieme a uno o più incaricati del trattamento, potete esercitare il vostro diritto di accesso presso ciascun incaricato del trattamento. Se la vostra richiesta riguarda dati trattati da un incaricato del trattamento, il nostro incaricato del trattamento ci assisterà nel fornire le informazioni, a meno che non risponda alla vostra richiesta per nostro conto.

Le informazioni saranno fornite entro 30 giorni dal ricevimento della richiesta. Se non forniamo le informazioni entro 30 giorni, ne informeremo l'utente e gli indicheremo il periodo entro il quale le informazioni saranno fornite. Se rifiutiamo, limitiamo o rinviamo le informazioni, vi informeremo entro lo stesso termine.

Se fornire le informazioni comporta uno sforzo sproporzionato, possiamo chiedervi di contribuire in modo ragionevole ai costi. Il contributo massimo è di 300 franchi svizzeri. L'importo del contributo deve essere comunicato prima di fornire le informazioni. Se non confermate la richiesta entro dieci giorni dalla notifica, la vostra richiesta sarà considerata ritirata, senza alcuna conseguenza in termini di costi.

Desideriamo sottolineare che abbiamo il diritto di rifiutare, limitare o rinviare la fornitura di informazioni se sono soddisfatti i requisiti legali ai sensi degli artt. 26 e 27 DSG.

Qui di seguito troverete ulteriori informazioni di carattere generale che sono necessarie e possono essere pubblicate in modo che possiate far valere i vostri diritti ai sensi della FADP e che sia garantito un trattamento trasparente dei dati.

## L. l'identità e i dati di contatto della persona responsabile:

Si veda il punto "A. Identità e dati di contatto del Titolare del trattamento".

## M. i dati personali trattati in quanto tali;

Su richiesta, saremo lieti di fornirvi una copia dei dati personali che trattiamo su di voi.

## N. la finalità del trattamento;

La finalità generale del trattamento dei dati personali è, come già detto, la gestione di tutte le operazioni riguardanti il titolare del trattamento, i clienti, gli interessati, i partner commerciali o altri rapporti contrattuali o precontrattuali tra i suddetti gruppi (in senso lato) o gli obblighi legali del titolare del trattamento. Saremo lieti di informarvi sulle singole finalità su richiesta.

## O. il periodo di conservazione dei dati personali o, se ciò non è possibile, i criteri per determinare tale periodo;

Il criterio per determinare il periodo di conservazione dei dati personali è il rispettivo periodo di conservazione legale. Allo scadere del periodo, i dati corrispondenti vengono cancellati di routine se non sono più necessari per l'adempimento del contratto o per l'avvio del contratto.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## P. le informazioni disponibili sull'origine dei dati personali, nella misura in cui non sono state ottenute dall'interessato;

Saremo lieti di fornirvi su richiesta una copia delle informazioni disponibili sull'origine dei vostri dati personali, nella misura in cui non siano state ottenute da voi.

## Q. se del caso, l'esistenza di una decisione individuale automatizzata e la logica su cui si basa la decisione;

Si veda il punto "Obbligo di informazione in caso di decisione individuale automatizzata (art. 21 LADP)".

## R. le categorie di destinatari a cui vengono comunicati i dati personali e l'informativa ai sensi dell'art. 19 comma 4 LADP.

Enti pubblici

Organismi esterni

Altri organismi esterni

Elaborazione interna

Elaborazione intragruppo

Altri messaggi

Le informazioni ai sensi dell'art. 19 cpv. 4 LADP sono riportate sopra alla voce "Informazioni sulla divulgazione all'estero".

## S. Diritto al rilascio o alla trasmissione dei dati (art. 28 FADP, art. 20 DDO)

Avete il diritto di richiederci, gratuitamente, la divulgazione dei vostri dati personali che ci avete comunicato in un formato elettronico di uso comune se (1) i dati vengono elaborati automaticamente e (2) i dati vengono elaborati con il vostro consenso o in diretta connessione con la conclusione o l'esecuzione di un contratto tra voi e noi.

Potete anche chiedere che i vostri dati personali vengano trasferiti gratuitamente a un altro titolare del trattamento, se sono soddisfatti i requisiti di cui all'articolo 28, paragrafo 1, della LADP e se ciò non richiede uno sforzo sproporzionato. I vostri diritti possono essere limitati dall'art. 29 della LADP.

I dati personali che ci avete comunicato sono (1) i dati che ci avete fornito consapevolmente e volontariamente e (2) i dati che abbiamo raccolto su di voi e sul vostro comportamento durante l'utilizzo di un servizio o di un dispositivo. I dati personali che abbiamo generato attraverso la nostra analisi dei dati personali forniti o osservati non sono considerati dati personali che ci avete comunicato.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## T. Richieste legali (art. 32 LADP)

L'utente può richiedere la rettifica dei dati personali inesatti, a meno che (1) una disposizione di legge non vieti la modifica, o (2) i dati personali siano trattati per scopi di archiviazione nel pubblico interesse.

Le azioni a tutela della personalità sono disciplinate dagli articoli 28, 28a e 28g-28l del Codice Civile. In qualità di querelante, potete in particolare chiedere (1) che venga vietato un determinato trattamento dei dati, (2) che venga vietata una determinata divulgazione dei dati personali a terzi e (3) che i dati personali vengano cancellati o distrutti. Se non è possibile stabilire né l'esattezza né l'inesattezza dei dati personali in questione, il reclamante può richiedere l'apposizione di un avviso di contestazione. Inoltre, il reclamante può anche richiedere che la rettifica, la cancellazione o la distruzione, il divieto di trattamento o di divulgazione a terzi, l'avviso di contestazione o la sentenza siano comunicati a terzi o pubblicati.

## U. Legge applicabile

Il diritto procedurale applicabile disciplina il trattamento dei dati personali e i diritti delle persone interessate nei procedimenti giudiziari e nei procedimenti previsti dai codici procedurali federali. Le disposizioni della FADP si applicano ai procedimenti amministrativi di primo grado. Per le rivendicazioni di diritto privato, si applica la legge federale sul diritto internazionale privato, come modificata di volta in volta.

## V. EU-U.S. Data Privacy Framework (EU-U.S. DPF), UK Extension to the EU-U.S. DPF, Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF)

Se la nostra organizzazione è un membro certificato dell'EU-U.S. Data Privacy Framework (EU-U.S. DPF) e/o della UK Extension to the EU-U.S. DPF e/o del Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF), si applica quanto segue:

Ci atteniamo all'EU-U.S. Data Privacy Framework (EU-U.S. DPF) e alla UK Extension to the EU-U.S. DPF, così come al Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF), come stabilito dal U.S. Department of Commerce. La nostra azienda ha confermato al Dipartimento del Commercio degli Stati Uniti che rispetta gli EU-U.S. Data Privacy Framework Principles (EU-U.S. DPF Principles) relativamente al trattamento dei dati personali che riceve dall'Unione Europea e dal Regno Unito in base all'EU-U.S. DPF e alla UK Extension to the EU-U.S. DPF. La nostra azienda ha anche confermato di rispettare i Swiss-U.S. Data Privacy Framework Principles (Swiss-U.S. DPF Principles) per quanto riguarda il trattamento dei dati personali ricevuti dalla Svizzera in base al Swiss-U.S. DPF. In caso di contraddizione tra le disposizioni della nostra politica sulla privacy e gli EU-U.S. DPF Principles e/o i Swiss-U.S. DPF Principles, i Principles prevarranno.

Per saperne di più sul programma Data Privacy Framework (DPF) e per visualizzare la nostra certificazione, si prega di visitare https://www.dataprivacyframework.gov/.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

Le altre unità statunitensi o le filiali della nostra azienda che aderiscono anche agli EU-U.S. DPF Principals, inclusa la UK Extension to the EU-U.S. DPF e i Swiss-U.S. DPF Principals, se presenti, sono elencate nella nostra politica sulla privacy.

In conformità con l'EU-U.S. DPF, la UK Extension to the EU-U.S. DPF e il Swiss-U.S. DPF, la nostra azienda si impegna a collaborare con il comitato istituito dalle autorità europee per la protezione dei dati, l'Information Commissioner's Office (ICO) del Regno Unito e il Commissario federale per la protezione dei dati e la trasparenza (EDÖB) della Svizzera, e a seguire i loro consigli riguardo alle lamentele irrisolte sul nostro trattamento dei dati personali che riceviamo in base all'EU-U.S. DPF, alla UK Extension to the EU-U.S. DPF e al Swiss-U.S. DPF.

Informiamo le persone interessate riguardo alle autorità europee per la protezione dei dati competenti per gestire le lamentele sul trattamento dei dati personali da parte della nostra organizzazione, nella parte superiore di questo documento di trasparenza, e che offriamo un rimedio legale adeguato e gratuito.

Informiamo tutte le persone interessate che la nostra azienda è soggetta ai poteri di indagine e di enforcement della Federal Trade Commission (FTC).

Le persone interessate hanno la possibilità, in determinate condizioni, di richiedere un arbitrato vincolante. La nostra organizzazione è obbligata a risolvere le richieste e ad aderire alle condizioni dell'Allegato I dei DPF-Principals, a condizione che la persona interessata abbia richiesto un arbitrato vincolante notificando la nostra organizzazione e che le procedure e le condizioni dell'Allegato I dei Principals siano state rispettate.

Informiamo qui tutte le persone interessate sulla responsabilità della nostra organizzazione in caso di trasferimento di dati personali a terzi.

Per domande delle persone interessate o delle autorità di controllo della protezione dei dati, abbiamo nominato i rappresentanti locali menzionati nella parte superiore di questo documento di trasparenza.

Offriamo la possibilità di scegliere (Opt-out) se i dati personali (i) devono essere condivisi con terzi o (ii) utilizzati per scopi sostanzialmente diversi da quelli per i quali sono stati originariamente raccolti o successivamente autorizzati. Il meccanismo chiaro, ben visibile e facilmente accessibile per esercitare il proprio diritto di scelta consiste nel contattare il nostro Data Protection Officer (DSB) via email. Non si ha alcuna possibilità di scelta e non siamo obbligati quando i dati sono condivisi con un terzo che agisce come agente o processore per nostro conto e secondo le nostre istruzioni. Tuttavia, stipuliamo sempre un contratto con tale agente o processore.

Per i dati sensibili (ovvero dati personali che includono informazioni sulla salute, l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale o informazioni sulla vita sessuale della persona interessata), otteniamo il vostro consenso esplicito (Opt-in) se tali dati (i) devono essere condivisi o (ii) utilizzati per scopi diversi da quelli per cui sono stati originariamente raccolti o per cui avete successivamente dato il vostro consenso, facendo la vostra scelta di Opt-in. Inoltre,


© All rights reserved by Heiko Maniero.

trattiamo tutti i dati personali che riceviamo da terzi come sensibili se il terzo li ha identificati e trattati come tali.

Vi informiamo qui sulla necessità di divulgare dati personali in risposta a richieste legali dalle autorità, inclusa l'esecuzione delle richieste di sicurezza nazionale o di applicazione della legge.

Nel trasferimento di dati personali a un terzo che agisce come responsabile, ci atteniamo ai Principals di notifica e scelta. Inoltre, stipuliamo un contratto con il terzo responsabile del trattamento che prevede che questi dati possano essere trattati solo per scopi limitati e specifici in conformità con il consenso fornito e che il destinatario offra lo stesso livello di protezione dei Principals del DPF e ci notifichi se determina di non poter più soddisfare questo obbligo. Il contratto prevede che il terzo, che agisce come responsabile, interrompa il trattamento o adotti altre misure ragionevoli e appropriate per rimediare se tale determinazione viene fatta.

Nel trasferimento di dati personali a un terzo che agisce come agente o processore, (i) trasferiamo questi dati solo per scopi limitati e specifici; (ii) ci assicuriamo che l'agente o il processore sia obbligato a fornire almeno lo stesso livello di protezione dei dati richiesto dai DPF-Principals; (iii) adottiamo misure ragionevoli e appropriate per garantire che l'agente o il processore tratti effettivamente i dati personali trasferiti in modo conforme ai nostri obblighi ai sensi dei DPF-Principals; (iv) richiediamo che l'agente o il processore ci notifichi se determina di non poter più soddisfare il suo obbligo di fornire lo stesso livello di protezione richiesto dai DPF-Principals; (v) dopo tale notifica, anche sotto (iv), adottiamo misure ragionevoli e appropriate per interrompere il trattamento non autorizzato e rimediare; e (vi) forniamo al DPF Department, su richiesta, un riassunto o un esemplare rappresentativo delle disposizioni pertinenti sulla privacy del nostro contratto con tale agente.

In conformità con l'EU-U.S. DPF e/o la UK Extension to the EU-U.S. DPF e/o il Swiss-U.S. DPF, la nostra organizzazione si impegna a cooperare con il comitato istituito dalle autorità di protezione dei dati dell'UE e dall'Information Commissioner's Office (ICO) del Regno Unito e dal Commissario federale per la protezione dei dati e la trasparenza (EDÖB) della Svizzera, e a seguire i loro consigli riguardo le lamentele irrisolte sul nostro trattamento dei dati personali che riceviamo in relazione al lavoro sotto l'EU-U.S. DPF, la UK Extension to the EU-U.S. DPF e il Swiss-U.S. DPF.

Tutti gli interessati che si trovano temporaneamente nell'Unione Europea (UE), nello Spazio Economico Europeo (SEE) o nel Regno Unito, o che vi hanno il domicilio o la residenza abituale, hanno diritto ai diritti e alle prerogative degli interessati pubblicati nel nostro Documento sulla trasparenza, che derivano anche dagli articoli da 15 a 22 del GDPR, compreso il diritto di accesso ai dati personali. Abbiamo reso disponibili queste informazioni in tutte le lingue dell'UE e del SEE. La versione in lingua inglese si applica al Regno Unito.

Tutti gli interessati che risiedono temporaneamente in Svizzera o che vi hanno il domicilio o la residenza abituale hanno diritto ai diritti e alle prerogative degli interessati ai sensi della Legge svizzera sulla protezione dei dati (LPD) e del Regolamento svizzero sulla protezione dei dati (RGPD), pubblicati nel


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

nostro Documento sulla trasparenza, compreso il diritto di accesso ai dati personali. Abbiamo fornito queste informazioni nelle tre lingue ufficiali della Svizzera (tedesco, italiano e francese).


© All rights reserved by Heiko Maniero.

# FRENCH: Information sur le traitement des données personnelles conformément à la loi sur la protection des données (LPD) et à l'ordonnance sur la protection des données (OPD) de la Suisse

Mesdames et Messieurs

le présent document de transparence a pour but d'informer les personnes concernées au sujet desquelles nous traitons des données personnelles sur le traitement, de contribuer à la protection de la personnalité et des droits fondamentaux des personnes physiques et de communiquer aux personnes concernées des informations sur la collecte de données personnelles sous une forme précise, transparente, compréhensible et facilement accessible. Ce document contient des informations d'ordre général. Si vous avez besoin d'informations plus spécifiques de notre part, veuillez vous adresser au conseiller à la protection des données mentionné ci-dessous. Ce document de transparence doit s'appliquer à tous les faits qui ont des répercussions en Suisse, même s'ils sont initiés à l'étranger.

## A. Autorité de surveillance de la protection des données (art. 4 LPD)

Le Préposé fédéral à la protection des données et à la transparence (PFPDT) surveille l'application des dispositions fédérales en matière de protection des données et est donc l'autorité de surveillance de la protection des données compétente pour nous. Les plaintes concernant notre organisation peuvent être déposées auprès du PFPDT.

Le PFPDT peut être contacté via le site https://www.edoeb.admin.ch/.

## B. Tâches et coordonnées du conseiller à la protection des données (art. 10 LPD)

Nous avons désigné la personne physique suivante comme conseiller à la protection des données pour la Suisse :

Antoine Parella
c/o Cancellarius AG
Rue de l'école des plantes 3
8400 Winterthur
Suisse
Courrier électronique : office@cancellarius.ch


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

Notre conseiller en matière de protection des données participe à l'application des règles de protection des données. Il est également le point de contact pour toutes les personnes concernées en Suisse. En tant que personne concernée, veuillez vous adresser directement à notre conseiller à la protection des données pour toutes les questions relatives à la protection des données en Suisse.

Le conseiller à la protection des données est notamment chargé de former et de conseiller notre organisation sur toutes les questions relatives à la protection des données. Il exerce sa fonction à notre égard de manière professionnellement indépendante et sans recevoir d'instructions. En outre, il n'exerce aucune activité incompatible avec ses fonctions de conseiller à la protection des données et dispose des connaissances techniques nécessaires.

## C. Représentation en Suisse (art. 14 LPD)

Dans la mesure où nous avons un siège ou un domicile à l'étranger et que nous traitons des données de personnes concernées résidant en Suisse, nous désignons la personne suivante comme notre représentant en Suisse, qui servira de point de contact pour les personnes concernées et le PFPDT et qui, sur demande, fournira aux personnes concernées des informations sur la manière dont vous pouvez exercer vos droits:

Prof. Dr. h.c. Heiko Maniero, LL.B., LL.M. mult, M.L.E.
c/o Cancellarius AG
Rue de l'école des plantes 3
8400 Winterthur
Suisse
Courrier électronique : info@dg-datenschutz.de

## D. Obligation d'informer lors de la collecte de données personnelles (art. 19 LPD)

Nous vous informons ci-après - en tant que personne concernée - de manière appropriée sur la collecte de données personnelles. Nous vous communiquons ci-après les informations nécessaires pour que vous puissiez faire valoir vos droits conformément à la loi fédérale sur la protection des données (LPD) et au règlement sur la protection des données (RGPD) et pour garantir un traitement transparent des données.

## E. l'identité et les coordonnées du responsable :

Voir ci-dessus sous "A. Identity and the contact details of the Controller".

## F. les finalités du traitement et les bases juridiques :

La finalité générale du traitement des données personnelles est l'exécution de toutes les opérations concernant le responsable, les clients, les prospects, les partenaires commerciaux ou d'autres relations


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

contractuelles ou précontractuelles entre les groupes mentionnés (au sens large) ou les obligations légales du responsable.

Votre consentement sert de base juridique à notre entreprise pour les processus de traitement pour lesquels nous demandons un consentement pour une finalité de traitement spécifique (art. 31, al. 1, al. 1, LPD).

Nous fondons le traitement de vos données personnelles soit sur le consentement, soit sur des intérêts privés prépondérants (art. 31, al. 1, al. 2 LPD), sur des intérêts publics prépondérants (art. 31, al. 1, al. 3 LPD) ou sur des lois (art. 31, al. 1, al. 4 LPD). Les lois en vigueur nous servent toujours de base juridique pour le traitement lorsque nous sommes soumis à une obligation légale qui rend nécessaire le traitement de données personnelles, comme par exemple le respect des obligations fiscales.

Nous nous appuyons sur des intérêts privés prépondérants du responsable, entre autres, pour traiter (1) des données personnelles concernant nos partenaires contractuels, lorsque le traitement a lieu en relation directe avec la conclusion ou l'exécution d'un contrat, et/ou (2) des données personnelles de concurrents économiques ou de personnes avec lesquelles nous entrerons en concurrence économique à l'avenir, que nous traitons à cette fin et que nous ne communiquons pas à des tiers, et/ou (3) de données personnelles destinées à vérifier la solvabilité de la personne concernée, étant entendu qu'il ne s'agit ni de données personnelles sensibles ni d'un profilage à haut risque et que les données ne sont communiquées à des tiers que si ceux-ci ont besoin des données pour la conclusion ou l'exécution d'un contrat avec la personne concernée et que les données ne datent pas de plus de dix ans, et que la personne concernée est majeure, et/ou (4) de données personnelles à des fins non personnelles, notamment pour la recherche, la planification ou les statistiques, auquel cas nous rendons les données anonymes dès que le but du traitement le permet et, si une anonymisation est impossible ou nécessite des efforts disproportionnés, nous prenons des mesures appropriées pour empêcher l'identification de la personne concernée, et s'il s'agit de données personnelles sensibles, ne les communiquent à des tiers que de manière à ce que les personnes concernées ne soient pas identifiables et, si cela n'est pas possible, garantissent que les tiers ne traitent les données qu'à des fins non personnelles et publient les résultats de manière à ce que les personnes concernées ne soient pas identifiables, et/ou (5) collectent des données personnelles sur une personne publique qui se rapportent aux activités de cette personne dans le public.

Nous nous appuyons notamment sur des intérêts publics prépondérants lorsque nous traitons des données dans un but supérieur, qui sert l'intérêt général ou du moins le favorise.

## G. Catégories de destinataires auxquels les données personnelles sont communiquées :

Organismes publics

Organismes externes


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

Autres organismes externes

Traitement interne

Traitement interne au groupe

Autres postes

## H. les catégories de données personnelles traitées :

Données des clients

Données des personnes intéressées

Données sur l'emploi

Données des fournisseurs

## I. Informations concernant la communication à l'étranger :

En cas de communication de données personnelles à l'étranger, la personne concernée doit également être informée de l'Etat ou de l'organe international et, le cas échéant, des garanties prévues à l'art. 16 al. 2 LPD ou de l'application d'une exception au sens de l'art. 17 LPD.

L'État ou l'organe international est déterminé par la liste des (sous-)traitants que nous publions. Vous trouverez cette liste sur notre site web. En tant que garantie selon l'art. 16 al. 2 LPD, nous utilisons en principe des clauses standard de protection des données que le PFPDT a préalablement approuvées (art. 16 al. 2 let. d LPD).

Si, dans le cadre d'une communication à l'étranger, nous ne concluons exceptionnellement pas de clauses standard de protection des données, nous vous demandons en principe votre consentement exprès. Font exception à cette règle les communications à l'étranger qui sont directement liées à la conclusion ou à l'exécution d'un contrat entre vous et nous, ou à un contrat conclu dans votre intérêt entre nous et un autre partenaire contractuel.

En outre, nous communiquons le cas échéant des données personnelles à l'étranger sans clauses standard de protection des données et sans votre consentement exprès si cela est nécessaire pour (1) la sauvegarde d'un intérêt public prépondérant, ou (2) la constatation, l'exercice ou la défense de droits en justice devant un tribunal ou une autre autorité étrangère compétente, ou (3) pour protéger votre vie ou votre intégrité physique ou la vie ou l'intégrité physique d'un tiers, s'il n'est pas possible d'obtenir votre consentement dans un délai raisonnable, ou (4) si vous avez rendu les données personnelles accessibles à tous et n'avez pas expressément interdit leur traitement, ou (5) si les données personnelles proviennent d'un registre prévu par la loi qui est public ou accessible aux personnes ayant un intérêt digne de protection, pour autant que les conditions légales de consultation soient remplies dans le cas particulier.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## J. Obligation d'information en cas de décision individuelle automatisée (art. 21 LPD)

Nous ne prenons pas de décisions qui reposent exclusivement sur un traitement automatisé et qui sont liées à une conséquence juridique pour vous ou qui vous affectent considérablement (décision individuelle automatisée). Sont exclues les décisions individuelles automatisées qui sont directement liées à la conclusion ou à l'exécution d'un contrat entre vous et nous, et si votre demande est acceptée ou si vous avez expressément consenti à ce que la décision soit prise de manière automatisée.

## K. Droit d'accès (art. 25 LPD, art. 16, 17, 18, 19 OLPD)

Vous avez le droit de nous demander si des données personnelles vous concernant sont traitées. Pour exercer ce droit, veuillez nous adresser une demande écrite (également par e-mail). La demande de renseignements se fait par écrit ou sous la forme sous laquelle nous disposons des données. La demande de renseignements et la communication des informations peuvent être effectuées par voie électronique (par exemple par e-mail).

Nous devons prendre des mesures raisonnables pour vous identifier en tant que personne concernée avant de vous fournir des informations. Vous êtes tenu(e) de coopérer, notamment en vous identifiant auprès de nous.

Si nous traitons vos données personnelles conjointement avec un ou plusieurs autres responsables, vous pouvez faire valoir votre droit d'accès auprès de chacun d'entre eux. Si votre demande concerne des données traitées par un sous-traitant, notre sous-traitant nous aide à fournir l'accès dans la mesure où il ne répond pas à votre demande en notre nom.

Nous vous fournissons les informations dans un délai de 30 jours à compter de la réception de la demande. Si nous ne fournissons pas les informations dans les 30 jours, nous vous en informons et vous indiquons le délai dans lequel les informations seront fournies. Si nous refusons de fournir les informations, si nous les limitons ou si nous les reportons, nous vous en informons dans le même délai.

Si la communication des renseignements entraîne des frais disproportionnés, nous pouvons exiger de vous une participation raisonnable aux frais. Cette participation s'élève au maximum à 300 francs suisses. Nous devons vous communiquer le montant de la participation avant de vous fournir les renseignements. Si vous ne confirmez alors pas la demande dans les dix jours suivant la communication, votre demande est considérée comme retirée - sans frais.

Nous attirons votre attention sur le fait que nous sommes en droit de refuser, de restreindre ou de différer l'accès aux informations si les conditions légales sont remplies conformément aux articles 26 et 27 de la LPD.

Vous trouverez ci-dessous d'autres informations générales qui sont nécessaires et qui peuvent être publiées afin que vous puissiez faire valoir vos droits selon la LPD et qu'un traitement transparent des données soit garanti.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## L. l'identité et les coordonnées du responsable :

Voir ci-dessus sous "A. Identity and the contact details of the Controller".

## M. les données personnelles traitées en tant que telles ;

Sur demande, nous mettons volontiers à votre disposition une copie des données personnelles que nous traitons à votre sujet.

## N. le but du traitement ;

La finalité générale du traitement des données personnelles est, comme indiqué ci-dessus, le déroulement de toutes les opérations concernant le responsable du traitement, les clients, les personnes intéressées, les partenaires commerciaux ou d'autres relations contractuelles ou précontractuelles entre les groupes mentionnés (au sens large) ou les obligations légales du responsable du traitement. Nous vous communiquerons volontiers les finalités individuelles sur demande.

## O. la durée de conservation des données personnelles ou, si cela n'est pas possible, les critères de détermination de cette durée ;

Le critère pour déterminer la durée de conservation des données personnelles est le délai de conservation légal correspondant. Une fois ce délai écoulé, les données correspondantes sont effacées de manière routinière, dans la mesure où elles ne sont plus nécessaires à l'exécution du contrat ou à la préparation du contrat.

## P. les informations disponibles sur l'origine des données personnelles, dans la mesure où elles n'ont pas été collectées auprès de la personne concernée ;

Sur demande, nous mettons volontiers à votre disposition une copie des informations disponibles sur l'origine de vos données personnelles, dans la mesure où elles n'ont pas été collectées auprès de vous.

## Q. le cas échéant, l'existence d'une décision individuelle automatisée et la logique sur laquelle repose cette décision ;

Voir ci-dessus sous "Obligation d'information en cas de décision individuelle automatisée (art. 21 LPD)".

## R. les catégories de destinataires auxquels les données personnelles sont communiquées ainsi que les informations selon l'art. 19 al. 4 LPD.

Organismes publics

Organismes externes

Autres organismes externes

Traitement interne

Traitement interne au groupe

Autres postes


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

Vous trouverez les informations selon l'art. 19 al. 4 LPD ci-dessus sous "Informations concernant la communication à l'étranger".

## S. Droit à la remise ou à la transmission de données (art. 28 LPD, art. 20 OLPD)

Vous avez le droit de nous demander gratuitement de vous remettre les données personnelles que vous nous avez communiquées dans un format électronique courant, si (1) nous traitons les données de manière automatisée et (2) si les données sont traitées avec votre consentement ou en relation directe avec la conclusion ou l'exécution d'un contrat entre vous et nous.

Vous pouvez en outre nous demander de transférer gratuitement vos données personnelles à un autre responsable si les conditions de l'art. 28, al. 1, LPD sont remplies et si cela ne nécessite pas un effort disproportionné. Le cas échéant, vos droits sont limités par l'art. 29 LPD.

Sont considérées comme des données personnelles que vous nous avez communiquées (1) les données que vous avez mises à notre disposition en connaissance de cause et volontairement et (2) les données que nous avons collectées sur vous et votre comportement dans le cadre de l'utilisation d'un service ou d'un appareil. Les données personnelles que nous avons créées en analysant nous-mêmes les données personnelles mises à disposition ou observées ne sont pas considérées comme des données personnelles que vous nous avez communiquées.

## T. Droits juridiques (art. 32 LPD)

Vous pouvez demander que des données personnelles inexactes soient rectifiées, sauf (1) si une disposition légale interdit leur modification ou (2) si les données personnelles sont traitées à des fins d'archivage dans l'intérêt public.

Les actions en protection de la personnalité sont régies par les articles 28, 28a et 28g-28l du Code civil. En tant que partie plaignante, vous pouvez notamment exiger (1) l'interdiction d'un certain traitement de données et (2) l'interdiction d'une certaine communication de données personnelles à des tiers, et (3) l'effacement ou la destruction de données personnelles. Si ni l'exactitude ni l'inexactitude des données personnelles concernées ne peut être établie, vous pouvez, en tant que partie plaignante, exiger qu'une mention de contestation soit apposée. En outre, vous pouvez, en tant que partie plaignante, exiger que la rectification, l'effacement ou la destruction, l'interdiction de traitement ou de communication à des tiers, la mention de contestation ou le jugement soient communiqués à des tiers ou publiés.

## U. Droit applicable

Le droit de procédure applicable régit le traitement des données personnelles et les droits des personnes concernées dans les procédures judiciaires et dans les procédures régies par les codes de procédure fédéraux. Les dispositions de la LPD s'appliquent aux procédures administratives de première instance. Pour les droits de droit privé, la loi fédérale sur le droit international privé s'applique dans sa version actuelle.


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

## V. EU-U.S. Data Privacy Framework (EU-U.S. DPF), UK Extension to the EU-U.S. DPF, Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF)

Si notre organisation est un membre certifié de l'EU-U.S. Data Privacy Framework (EU-U.S. DPF) et/ou de la UK Extension to the EU-U.S. DPF et/ou du Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF), les dispositions suivantes s'appliquent:

Nous adhérons à l'EU-U.S. Data Privacy Framework (EU-U.S. DPF) et à la UK Extension to the EU-U.S. DPF ainsi qu'au Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF), tel qu'établi par le U.S. Department of Commerce. Notre entreprise a confirmé au U.S. Department of Commerce qu'elle respecte les EU-U.S. Data Privacy Framework Principles (EU-U.S. DPF Principles) concernant le traitement des données personnelles qu'elle reçoit de l'Union européenne et du Royaume-Uni en vertu de l'EU-U.S. DPF et de la UK Extension to the EU-U.S. DPF. Notre entreprise a également confirmé qu'elle respecte les Swiss-U.S. Data Privacy Framework Principles (Swiss-U.S. DPF Principles) concernant le traitement des données personnelles qu'elle reçoit de la Suisse sous le Swiss-U.S. DPF. En cas de contradiction entre les dispositions de notre politique de confidentialité et les EU-U.S. DPF Principles et/ou les Swiss-U.S. DPF Principles, les Principles prévalent.

Pour en savoir plus sur le programme Data Privacy Framework (DPF) et consulter notre certification, veuillez visiter https://www.dataprivacyframework.gov/.

Les autres entités américaines ou filiales de notre entreprise qui adhèrent également aux EU-U.S. DPF Principals, y compris la UK Extension to the EU-U.S. DPF et les Swiss-U.S. DPF Principals, si elles existent, sont mentionnées dans notre politique de confidentialité.

Conformément à l'EU-U.S. DPF, à la UK Extension to the EU-U.S. DPF et au Swiss-U.S. DPF, notre entreprise s'engage à coopérer avec le comité établi par les autorités de protection des données de l'UE, le UK Information Commissioner's Office (ICO) et le Préposé fédéral à la protection des données et à la transparence (EDÖB) de Suisse, et à suivre leurs conseils concernant les plaintes non résolues sur notre gestion des données personnelles que nous recevons sous l'EU-U.S. DPF, la UK Extension to the EU-U.S. DPF et le Swiss-U.S. DPF.

Nous informons les personnes concernées des autorités européennes de protection des données compétentes pour traiter les plaintes concernant la manière dont notre organisation gère les données personnelles, en haut de ce document de transparence, et que nous offrons un recours juridique adéquat et gratuit.

Nous informons toutes les personnes concernées que notre entreprise est soumise aux pouvoirs d'enquête et de contrôle de la Federal Trade Commission (FTC).

Les personnes affectées ont la possibilité, sous certaines conditions, de demander un arbitrage contraignant. Notre organisation est tenue de régler les réclamations et de respecter les conditions


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

énoncées à l'Annexe I des DPF-Principals, à condition que la personne concernée ait demandé un arbitrage contraignant en notifiant notre organisation et que les procédures et conditions de l'Annexe I des Principals aient été respectées.

Nous informons par la présente toutes les personnes concernées de la responsabilité de notre organisation en cas de transfert de données personnelles à des tiers.

Pour les questions des personnes affectées ou des autorités de contrôle de la protection des données, nous avons nommé les représentants locaux mentionnés en haut de ce document de transparence.

Nous vous offrons la possibilité de choisir (Opt-out), si vos données personnelles (i) doivent être partagées avec des tiers ou (ii) doivent être utilisées à des fins substantiellement différentes de celles pour lesquelles elles ont été initialement collectées ou ultérieurement autorisées par vous. Le mécanisme clair, bien visible et facilement accessible pour exercer votre droit de choix consiste à contacter notre responsable de la protection des données (DSB) par courriel. Vous n'avez pas le choix et nous ne sommes pas obligés lorsque les données sont partagées avec un tiers qui agit en tant qu'agent ou processeur en notre nom et selon nos instructions. Nous concluons cependant toujours un contrat avec un tel agent ou processeur.

Pour les données sensibles (c'est-à-dire les données personnelles incluant des informations sur l'état de santé, l'origine raciale ou ethnique, les opinions politiques, les croyances religieuses ou philosophiques, l'appartenance syndicale ou les informations sur la vie sexuelle de la personne), nous obtenons votre consentement explicite (Opt-in) si ces données (i) doivent être partagées ou (ii) doivent être utilisées à des fins différentes de celles pour lesquelles elles ont été initialement collectées ou pour lesquelles vous avez ensuite donné votre consentement, en faisant votre choix d'Opt-in. De plus, nous traitons toutes les données personnelles que nous recevons de tiers comme sensibles si le tiers les a identifiées et traitées comme telles.

Nous vous informons de la nécessité de divulguer des données personnelles en réponse à des demandes légales des autorités, y compris pour répondre aux exigences de la sécurité nationale ou de l'application de la loi.

Lors du transfert de données personnelles à un tiers qui agit en tant que contrôleur, nous respectons les Principals de notification et de choix. En outre, nous concluons un contrat avec le tiers responsable du traitement qui stipule que ces données ne peuvent être traitées que pour des fins limitées et spécifiées conformément au consentement que vous avez fourni et que le destinataire offre le même niveau de protection que les Principals du DPF et nous informe s'il détermine qu'il ne peut plus remplir cette obligation. Le contrat prévoit que le tiers, qui agit en tant que contrôleur, doit cesser le traitement ou prendre d'autres mesures raisonnables et appropriées pour remédier à la situation si une telle détermination est faite.

Lors du transfert de données personnelles à un tiers qui agit en tant qu'agent ou processeur, (i) nous transférons ces données uniquement à des fins limitées et spécifiées ; (ii) nous nous assurons que l'agent


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.

ou le processeur est tenu de fournir au moins le même niveau de protection des données exigé par les DPF-Principals ; (iii) nous prenons des mesures raisonnables et appropriées pour nous assurer que l'agent ou le processeur traite réellement les données personnelles transférées d'une manière conforme à nos obligations en vertu des DPF-Principals ; (iv) nous exigeons que l'agent ou le processeur nous informe s'il détermine qu'il ne peut plus respecter son obligation de fournir le même niveau de protection requis par les DPF-Principals ; (v) après une telle notification, également sous (iv), nous prenons des mesures raisonnables et appropriées pour arrêter le traitement non autorisé et remédier à la situation ; et (vi) nous fournissons au DPF Department, sur demande, un résumé ou un exemplaire représentatif des dispositions pertinentes de confidentialité de notre contrat avec cet agent.

Conformément à l'EU-U.S. DPF et/ou à la UK Extension to the EU-U.S. DPF et/ou au Swiss-U.S. DPF, notre organisation s'engage à coopérer avec le comité établi par les autorités de protection des données de l'UE et le UK Information Commissioner's Office (ICO) ainsi que le Préposé fédéral à la protection des données et à la transparence (EDÖB) de Suisse, et à suivre leurs conseils concernant les plaintes non résolues sur notre gestion des données personnelles que nous recevons en relation avec l'emploi sous l'EU-U.S. DPF, la UK Extension to the EU-U.S. DPF et le Swiss-U.S. DPF.

Toutes les personnes concernées qui se trouvent temporairement dans l'Union européenne (UE), l'Espace économique européen (EEE) ou le Royaume-Uni, ou qui y ont leur domicile ou leur résidence habituelle, bénéficient des droits et des droits des personnes concernées publiés dans notre document de transparence, qui découlent également des articles 15 à 22 du RGPD, y compris le droit d'accès aux données à caractère personnel. Ces informations sont disponibles dans toutes les langues de l'UE et de l'EEE. La version anglaise s'applique au Royaume-Uni.

Toutes les personnes concernées qui résident temporairement en Suisse ou qui y ont leur domicile ou leur résidence habituelle bénéficient des droits et des droits des personnes concernées en vertu de la loi suisse sur la protection des données (LPD) et du règlement suisse sur la protection des données (RGPD) qui sont publiés dans notre document de transparence, y compris le droit d'accès aux données à caractère personnel. Nous avons fourni ces informations dans les trois langues officielles de la Suisse (allemand, italien et français).


Powered by ICB International Certification Body.
© All rights reserved by Heiko Maniero.