

Auftragsverarbeitungsvertrag gemäß Art. 28 DSGVO



Dieser Auftragsverarbeitungsvertrag wird geschlossen zwischen:

NFON AG
Zielstattstr. 36
81379 München

vertreten durch den Vorstand

Ust-IDNr.DE 254495743

– im Folgenden „NFON“ oder „Auftragsverarbeiter“ i.S.d. Art. 4 Nr. 8 DSGVO genannt –

und der

Firma: _____

Straße: _____

PLZ & Ort: _____

Land: _____

– im Folgenden „Verantwortlicher“ i.S.d. Art. 4 Nr. 7 DSGVO genannt –

– zusammen im Folgenden die „Parteien“ genannt –

Auftragsverarbeitungsvertrag gemäß Art. 28 DSGVO



Präambel	3
01 Gegenstand und Dauer des Auftrags	3
02 Konkretisierung des Auftragsinhalts	4
03 Technisch-organisatorische Maßnahmen	6
04 Berichtigung, Einschränkung und Löschung von Daten	7
05 Qualitätssicherung und sonstige Pflichten des Auftragsverarbeiters	7
06 Unterauftragsverhältnisse	9
07 Kontrollrechte des Verantwortlichen	10
08 Unterstützungs- und Mitwirkungspflichten des Auftragsverarbeiters	11
09 Weisungsbefugnis und sonstige Pflichten des Verantwortlichen	11
10 Löschung und Rückgabe von personenbezogenen Daten	12
11 Haftung	13
12 Unterschriften	13

Präambel

Der Verantwortliche möchte den Auftragsverarbeiter mit den in Ziffer 1 genannten Leistungen beauftragen. Teil der Vertragsdurchführung ist die Verarbeitung von personenbezogenen Daten. Zur Wahrung der in Art. 28 DSGVO genannten Anforderungen schließen die Parteien die nachfolgende Vereinbarung.

01 Gegenstand und Dauer des Auftrags

1. Gegenstand

Der Auftragsverarbeiter erbringt für den Verantwortlichen Leistungen im Bereich Cloud Business Telefonie auf Grundlage des Hauptvertrags, der aktuell gültigen Leistungsbeschreibung und den jeweils gültigen AGB.

Je nach vertraglicher Vereinbarung können dabei einzelne oder mehrere der folgenden Leistungsbereiche Gegenstand der Auftragsverarbeitung sein:

- UCaaS (Unified Communications as a Service) – Bereitstellung cloudbasierter Kommunikationsdienste
- SaaS (Software as a Service) – Nutzung von webbasierten Anwendungen für Kommunikationsdienste und Portalen zur Verwaltung und Konfiguration
- SIP-Trunking – Bereitstellung IP-basierter Sprachverbindungen zur Anbindung eigener Telefonanlagen
- AlaaS (AI as a Service) – Bereitstellung Künstliche Intelligenz (KI)-gestützter Funktionen wie Transkription, Chatbot- oder Voicebot-Nutzung

Zur Konkretisierung der beiderseitigen datenschutzrechtlichen Rechte und Pflichten schließen die Parteien die vorliegende Vereinbarung. Die Regelungen der vorliegenden Vereinbarung gehen im Zweifel den Regelungen des Hauptvertrags vor.

2. Dauer

1. Die Dauer dieses Auftrags (Laufzeit) entspricht der Laufzeit des Hauptvertrages.
2. Das Recht zur außerordentlichen Kündigung bei Vorliegen eines wichtigen Grundes bleibt unberührt. Ein wichtiger Grund im Sinne von § 314 BGB liegt jedoch nur vor, wenn dem kündigenden Teil unter Berücksichtigung aller Umstände des Einzelfalls nach Abwägung der beiderseitigen Interessen die Fortsetzung des Vertragsverhältnisses bis zum Ablauf einer hinreichenden Frist nicht zugemutet werden kann.

Auftragsverarbeitungsvertrag gemäß Art. 28 DSGVO



Insbesondere berechtigt nicht jeder einzelne oder geringfügige Verstoß des Auftragsverarbeiters gegen Bestimmungen der DSGVO oder gegen Bestimmungen dieses Auftragsverarbeitungsvertrages zur außerordentlichen Kündigung.

Vielmehr ist in einem solchen Fall dem Auftragsverarbeiter zunächst eine Frist von 30 Tagen zur Behebung des Mangels zu setzen. Wird der Mangel innerhalb dieser Frist nicht behoben oder liegt ein Wiederholungs- oder Serienverstoß vor oder ein Verstoß mit erheblichem bzw. nachhaltigem Schaden oder Risiko, so ist die außerordentliche Kündigung möglich.

Die Kündigung kann nur erfolgen, wenn dem Verantwortlichen nach Ablauf der Frist die Fortsetzung des Vertragsverhältnisses nicht mehr zugemutet werden kann.

3. Der Vertrag gilt unbeschadet des vorstehenden Absatzes so lange, wie der Auftragsverarbeiter über personenbezogene Daten verfügt, die ihm vom Verantwortlichen zugeleitet wurden oder die er für diesen erhoben hat.

02 Konkretisierung des Auftragsinhalts

1. Art und Zweck der vorgesehenen Verarbeitung von Daten

Art und Zweck der Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter für den Verantwortlichen sind konkret beschrieben im Hauptvertrag.

Je nach vertraglich vereinbarter Leistung kann die Verarbeitung insbesondere folgende Arten und Zwecke umfassen:

- Unterstützung bei der Einrichtung der Services
- Speicherung und Verwaltung des Telefonbuchs des Verantwortlichen
- Speicherung und Implementierung von Wissenssammlungen zur Ermöglichung kontextbezogener Dialoge bei Betrieb und Bereitstellung eines sprachbasierten KI-Assistenzsystems
- Administration und Verwaltung der TK-Anlage und Nebenstellen durch den Kunden als Administrator oder einem zugeordneten Nutzer
- Supportdienstleistungen, Systemüberwachung und Störungsbeseitigung
- Automatisierte Verarbeitung von Sprache und Text in Kundeninteraktionen mittels KI-Systemen
- KI-gestützte Antwortgenerierung über Large Language Models (LLMs)

Auftragsverarbeitungsvertrag gemäß Art. 28 DSGVO



- Protokollierung von Kommunikationsverläufen innerhalb der KI-gestützten Funktionen

Die Datenverarbeitung im Rahmen der optional aktivierbaren Voicemail-Transkriptionen bzw. hinzubuchbaren Features „AI Essentials“ und „Nia Front Desk“ findet auf einer in einem Mitgliedsstaat der Europäischen Union, in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum oder in einem Drittland mit Angemessenheitsbeschluss gem. Art. 45 DSGVO gehosteten Infrastruktur statt. In diesem Zusammenhang erfolgt kein Training von KI-Modellen mit Daten des Verantwortlichen.

Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Verantwortlichen und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind. Sollten diese Anforderungen erfüllt sein, müssen jedoch wichtige datenschutzrechtliche Gründe vorliegen, um der Verlagerung in ein Drittland zu widersprechen.

2. Art der Daten

Im Rahmen der Durchführung des Hauptvertrages kann der Auftragsverarbeiter – abhängig vom jeweils vereinbarten Leistungsumfang – Zugriff auf die nachfolgend näher spezifizierten personenbezogenen Daten erhalten. Diese Daten umfassen

allgemein:

- Kontaktdaten der Beschäftigten des Verantwortlichen
- Stammdaten der Beschäftigten des Verantwortlichen
- Kontaktdaten der Kommunikationspartner des Verantwortlichen innerhalb des Telefonbuchs (bspw. Kunden) und/ oder Wissenssammlung (bei Nia Front Desk)
- Kundenhistorie
- Verkehrsdaten eines Telekommunikationsdienstes (z.B. IP-Adresse, A- und B-Rufnummer, Gesprächsdauer)
- Audioaufzeichnungen (z.B. Voicemails)
- Personenbezogene Daten im Rahmen von System- und Nutzungsprotokollen
- Konfigurationsdaten
- Alle sonstigen personenbezogenen Daten, die der Verantwortliche im Rahmen der Leistung, vor allem im Supportfall, im Auftrag verarbeiten lässt

Auftragsverarbeitungsvertrag gemäß Art. 28 DSGVO



im Rahmen von KI-Features:

- Kontakt- u. Stammdaten der Beschäftigten des Verantwortlichen
- Sprach- und Texteingaben sowie -ausgaben, transkribierte Inhalte (STT-, TTS-Services) und Zusammenfassungen
- Sitzungsdaten (Session-ID, Zeitstempel)
- Konversationshistorie

3. Kategorien betroffener Personen

Die Kategorien der durch die Verarbeitung betroffenen Personen können in Abhängigkeit des Leistungsumfanges umfassen:

- Kunden des Verantwortlichen
- Interessenten des Verantwortlichen
- Beschäftigte des Verantwortlichen
- Lieferanten und Dienstleister des Verantwortlichen
- Ansprechpartner – freie und angestellte – des Verantwortlichen
- Kommunikationspartner des Verantwortlichen
- Endnutzer der KI-gestützten Funktionen

03 Technisch-organisatorische Maßnahmen

1. Der Auftragsverarbeiter hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten und erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung zu dokumentieren und dem Verantwortlichen zur Prüfung zu übergeben. Bei Akzeptanz durch den Verantwortlichen werden die in Anlage 1 – „Technische und organisatorische Maßnahmen“ dokumentierten Maßnahmen Grundlage des Auftrags. Soweit die Prüfung/ein Audit des Verantwortlichen einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.
2. Der Auftragsverarbeiter hat die Sicherheit gem. Art. 28 Abs. 3 lit. c, 32 DSGVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DSGVO herzustellen. Insgesamt handelt es sich bei den zu

treffenden Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DSGVO zu berücksichtigen [Einzelheiten in Anlage 1].

3. Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit bleibt es dem Auftragsverarbeiter vorbehalten alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren und über die üblichen Kommunikationswege, auf der Webseite des Auftragsverarbeiters, zu veröffentlichen.

04 Berichtigung, Einschränkung und Löschung von Daten

1. Der Auftragsverarbeiter darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Verantwortlichen berichtigen, löschen oder deren Verarbeitung einschränken, soweit keine gesetzlichen Anforderungen dazu verpflichten. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragsverarbeiter wendet, wird der Auftragsverarbeiter dieses Ersuchen unverzüglich an den Verantwortlichen weiterleiten.
2. Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Verantwortlichen unmittelbar durch den Auftragsverarbeiter sicherzustellen.

05 Qualitätssicherung und sonstige Pflichten des Auftragsverarbeiters

Der Auftragsverarbeiter hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Art. 28 bis 33 DSGVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

- Schriftliche Bestellung eines Datenschutzbeauftragten, soweit gesetzlich verpflichtend, der seine Tätigkeit gemäß Art. 38 und 39 DSGVO ausübt.
- Die Kontaktdaten des Datenschutzbeauftragten werden auf der Homepage des Auftragsverarbeiters veröffentlicht.
- Die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DSGVO. Der Auftragsverarbeiter setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit (Art. 28 Abs. 3 UAbs. 1 S. 2 lit.b) DSGVO) und das

Auftragsverarbeitungsvertrag gemäß Art. 28 DSGVO



Fernmeldegeheimnis nach § 3 TDDDG verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Der Auftragsverarbeiter und jede dem Auftragsverarbeiter unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Verantwortlichen verarbeiten, einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.

- Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 28 Abs. 3 S. 2 lit. c, 32 DSGVO [Einzelheiten in Anlage 1].
- Der Verantwortliche und der Auftragsverarbeiter und ggf. deren Vertreter arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.
- Die unverzügliche Information des Verantwortlichen über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diese konkrete und grundsätzliche Beauftragung beziehen und dies gesetzlich nicht verboten ist. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragsverarbeiter ermittelt.
- Soweit der Verantwortliche seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragsverarbeiter ausgesetzt ist, hat ihn der Auftragsverarbeiter nach besten Kräften zu unterstützen, soweit dies gesetzlich erlaubt ist.
- Der Auftragsverarbeiter kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird.
- Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Verantwortlichen im Rahmen seiner Kontrollbefugnisse nach Ziffer 7 dieses Vertrages.
- Der Auftragsverarbeiter unterstützt den Verantwortlichen im erforderlichen Umfang bei der Durchführung von Datenschutz-Folgenabschätzungen gemäß Art. 35 DSGVO, sofern dies für die jeweilige Verarbeitung erforderlich ist.
- Der Auftragsverarbeiter unterstützt den Verantwortlichen mit geeigneten technischen und organisatorischen Maßnahmen bei der Erfüllung der Pflichten des Verantwortlichen nach Art. 12-22 DSGVO.
- Macht eine betroffene Person Rechte, etwa auf Auskunftserteilung, Berichtigung oder Löschung hinsichtlich ihrer Daten, unmittelbar gegenüber dem Auftragsverarbeiter geltend, so reagiert dieser nicht selbstständig, sondern

Auftragsverarbeitungsvertrag gemäß Art. 28 DSGVO



verweist die betroffene Person unverzüglich an den Verantwortlichen und wartet dessen Weisungen ab.

06 Unterauftragsverhältnisse

1. Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftragsverarbeiter z.B. als Telekommunikationsleistungen, Post-, Transport- und Versandleistungen, Reinigungsleistungen, Bewachungsdienste sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt. Wartungsleistungen stellen Unterauftragsverhältnisse im Sinne dieses Absatzes dar, soweit diese für IT-Systeme erbracht werden, die auch im Zusammenhang mit der Erbringung von Leistungen für den Verantwortlichen genutzt werden. Der Auftragsverarbeiter ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Verantwortlichen auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.
2. Die vertraglich vereinbarten Leistungen werden unter Einschaltung der in Anlage 2 – „Unterauftragsverhältnisse“ genannten Unterauftragsverarbeiter durchgeführt. Mit Abschluss dieses Vertrages gelten diese als durch den Verantwortlichen genehmigt. Der Auftragsverarbeiter ist im Rahmen seiner vertraglichen Verpflichtungen befugt, Unterauftragsverarbeiter (weitere Auftragsverarbeiter) zu beauftragen, soweit er den Verantwortlichen vorab in Textform über deren Beauftragung informiert. Der Verantwortliche kann gegen die Änderung nur aus wichtigem Grund Einspruch erheben. Der Einspruch hat binnen 14 Kalendertagen zu erfolgen und alle wichtigen Gründe ausdrücklich zu benennen. Ist diese Frist abgelaufen, gilt der Unterauftragsverarbeiter seitens des Verantwortlichen als genehmigt. Einsprüche müssen mindestens in Textform an datenschutz@nfon.com gemeldet werden.
3. Erbringt der Unterauftragsverarbeiter die vereinbarte Leistung außerhalb der EU/des EWR, stellt der Auftragsverarbeiter sicher, dass beim jeweiligen Unterauftragsverarbeiter ein angemessenes Datenschutzniveau gewährleistet ist, gemäß den Anforderungen nach Kapitel 5 der DSGVO (z.B. durch Abschluss einer Vereinbarung auf Basis der EU-Standarddatenschutzklauseln oder Angemessenheitsbeschluss durch die EU-Kommission). Der Auftragsverarbeiter wird dem Verantwortlichen auf Verlangen den Abschluss der vorgenannten Vereinbarungen mit seinen Unterauftragsverarbeitern nachweisen.
4. Sämtliche vertraglichen Regelungen in der Vertragskette sind auch weiteren Unterauftragsverarbeitern aufzuerlegen. Die technischen und organisatorischen Maßnahmen von Unterauftragsverarbeitern sind an die hier definierten technischen und

Auftragsverarbeitungsvertrag gemäß Art. 28 DSGVO



organisatorischen Maßnahmen angelehnt, können aber ein risikoorientiertes geringeres Niveau besitzen.

5. Eine Vor-Ort-Kontrolle beim Unterauftragsverarbeiter erfolgt ausschließlich durch den Auftragsverarbeiter und höchstens in jährlichen Abständen. Eine Vor-Ort-Kontrolle kann durch den Nachweis einer datenschutzkonformen Verarbeitung unter den gleichen Voraussetzungen nach Ziffer 7.3 ersetzt werden.

07 Kontrollrechte des Verantwortlichen

1. Der Verantwortliche hat das Recht, mit dem Auftragsverarbeiter Überprüfungen nach vorheriger Abstimmung mit dem Auftragsverarbeiter selbst durchzuführen oder durch im Einzelfall vom Verantwortlichen zu benennende Prüfer, sofern diese nicht in einem Wettbewerbsverhältnis zum Auftragsverarbeiter stehen, durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig und spätestens 14 Kalendertage vorab anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragsverarbeiter in dessen Geschäftsbetrieb zu den üblichen Geschäftszeiten zu überzeugen. Der Verantwortliche wird Kontrollen nur im erforderlichen Umfang durchführen und die Betriebsabläufe des Auftragsverarbeiters dabei nicht unverhältnismäßig stören. Solche Überprüfungen sind auf eine (1) Vor-Ort-Kontrolle pro Kalenderjahr beschränkt.
2. Der Auftragsverarbeiter stellt sicher, dass sich der Verantwortliche von der Einhaltung der Pflichten des Auftragsverarbeiters nach Art. 28 DSGVO überzeugen kann. Der Auftragsverarbeiter verpflichtet sich, dem Verantwortlichen auf Anforderung die erforderlichen Auskünfte innerhalb einer angemessenen Frist zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.
3. Der Nachweis solcher Maßnahmen, kann erfolgen durch
 - die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DSGVO;
 - die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DSGVO;
 - aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzaudatoren, Qualitätsaudatoren);
 - eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. ISO 27001).
4. Der Verantwortliche dokumentiert das Ergebnis der von ihm durchgeführten Kontrollen und teilt es dem Auftragsverarbeiter mit. Bei Fehlern oder Unregelmäßigkeiten, die der Verantwortliche insbesondere bei der Prüfung von Auftragsergebnissen feststellt, hat er den Auftragsverarbeiter unverzüglich zu informieren. Werden bei der Kontrolle Sachverhalte

Auftragsverarbeitungsvertrag gemäß Art. 28 DSGVO



festgestellt, deren zukünftige Vermeidung Änderungen des angeordneten Verfahrensablaufs erfordern, teilt der Verantwortliche dem Auftragsverarbeiter die notwendigen Verfahrensänderungen unverzüglich mit.

5. Der Verantwortliche vergütet dem Auftragsverarbeiter den angemessenen Aufwand, der ihm im Rahmen der Kontrolle entsteht. Der Aufwand einer Vor-Ort-Kontrolle ist für den Auftragsverarbeiter grundsätzlich auf einen Tag pro Kalenderjahr beschränkt. Bei anlassbezogenen Audits, die aufgrund eines vom Auftragsverarbeiter zu vertretenden Vorkommnisses durchgeführt werden, insbesondere bei Datenschutzverletzungen oder anderen Verstößen gegen datenschutzrechtliche Verpflichtungen, trägt jede Partei die ihr damit im Zusammenhang entstehenden Kosten selbst. Dies umfasst insbesondere Personalkosten, Reisekosten sowie Kosten für die Bereitstellung von Informationen und Dokumentationen.

08 Unterstützungs- und Mitwirkungspflichten des Auftragsverarbeiters

Der Auftragsverarbeiter unterstützt den Verantwortlichen bei der Einhaltung der in den Artikeln 32 bis 36 der DSGVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen. Hierzu gehören u.a.

- die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen
- die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Verantwortlichen zu melden
- die Verpflichtung, dem Verantwortlichen im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen
- die Unterstützung des Verantwortlichen für dessen Datenschutz-Folgeabschätzung
- die Unterstützung des Verantwortlichen im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde

09 Weisungsbefugnis und sonstige Pflichten des Verantwortlichen

1. Der Auftragsverarbeiter darf Daten nur im Rahmen des Hauptvertrags und der Leistungsbeschreibung und gemäß den Weisungen des Verantwortlichen verarbeiten. Wird

Auftragsverarbeitungsvertrag gemäß Art. 28 DSGVO



der Auftragsverarbeiter durch das Recht der Europäischen Union oder der Mitgliedstaaten, dem er unterliegt, zu weiteren Verarbeitungen verpflichtet, teilt er dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern ihm dies rechtlich gestattet ist.

2. Die Weisungen des Verantwortlichen werden anfänglich durch diesen Vertrag festgelegt und können vom Verantwortlichen danach in Textform durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). Mündliche Weisungen bestätigt der Verantwortliche unverzüglich (mind. Textform).
3. Der Auftragsverarbeiter hat den Verantwortlichen unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Der Auftragsverarbeiter ist berechtigt, die Durchführung der entsprechenden Weisung so lange auszusetzen, bis sie durch den Verantwortlichen bestätigt oder geändert wird. Der Auftragsverarbeiter darf die Durchführung einer offensichtlich rechtswidrigen Weisung ablehnen.
4. Der Verantwortliche ist im Rahmen dieses Vertrages für die Einhaltung der gesetzlichen Bestimmungen der Datenschutzgesetze, insbesondere für die Rechtmäßigkeit der Datenweitergabe an den Auftragsverarbeiter sowie für die Rechtmäßigkeit der Verarbeitung allein verantwortlich (Verantwortlicher i.S.v. Art. 4 Nr. 7 DSGVO) sowie für die Einhaltung der für ihn geltenden Vorschriften nach der KI-VO (Verordnung (EU) 2024/1689 des Europäischen Parlaments und des Rates vom 13. Juni 2024 zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz). Dies gilt auch im Hinblick auf den in dieser Vereinbarung geregelten Gegenstand, Umfang, Art und Zweck der Datenverarbeitung und die Beschreibung der betroffenen Datenkategorien.

10 Löschung und Rückgabe von personenbezogenen Daten

1. Kopien oder Duplikate der Daten werden ohne Wissen des Verantwortlichen nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.
2. Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Verantwortlichen – spätestens mit Beendigung der Leistungsvereinbarung – hat der Auftragsverarbeiter sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Verantwortlichen auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Eine Löschbestätigung ist auf Anforderung vorzulegen.
3. Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragsverarbeiter entsprechend der jeweiligen

Auftragsverarbeitungsvertrag gemäß Art. 28 DSGVO



Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Verantwortlichen übergeben.

11 Haftung

1. Verantwortlicher und Auftragsverarbeiter haften gegenüber betroffenen Personen entsprechend der in Art. 82 DSGVO getroffenen Regelung. Der Auftragsverarbeiter stimmt eine etwaige Erfüllung von Haftungsansprüchen mit dem Verantwortlichen ab.
2. Die Parteien stellen sich jeweils von der Haftung frei, wenn/ soweit eine Partei nachweist, dass sie in keinerlei Hinsicht für den Umstand, durch den der Schaden bei einer betroffenen Person eingetreten ist, verantwortlich ist. Im Übrigen gilt Art. 82 Abs. 5 DSGVO.
3. Sofern vorstehend nicht anders geregelt, richtet sich die Haftung im Rahmen dieses Vertrages nach den Haftungsregelungen des Hauptvertrages.

12 Unterschriften

Ort, Datum

Unterschrift NFON AG

Unterschrift NFON AG

Ort, Datum

Name Verantwortlicher

Unterschrift Verantwortlicher