

AUFTRAGSVERARBEITUNGSVEREINBARUNG

(AVV)

zwischen

HealthCare Consulting GmbH

Kolonitzgasse 2A/DG

1030 Wien

Österreich

Firmenbuch: FN 204710w

– nachfolgend „Anbieter“ –

und dem jeweiligen Unternehmenskunden

– nachfolgend „Kunde“ –

gemeinsam die „Parteien“.

1. GEGENDSTAND UND ROLLEN

- 1.1. Diese Auftragsverarbeitungsvereinbarung („AVV“) gilt, soweit der Anbieter im Rahmen von Convillance personenbezogene Daten im Auftrag des Kunden verarbeitet.
- 1.2. Für diese Verarbeitungen ist der Kunde „Verantwortlicher“ und HealthCare Consulting GmbH „Auftragsverarbeiter“ im Sinne der DSGVO, soweit nicht für einen bestimmten Verarbeitungsvorgang ausdrücklich eine andere Rollenverteilung besteht bzw. vereinbart wurde.
- 1.3. Soweit der Anbieter personenbezogene Daten für eigene administrative Zwecke verarbeitet, insbesondere für Vertragsverwaltung, Abrechnung oder eigene gesetzliche Verpflichtungen, handelt er hierfür als eigenständig Verantwortlicher. Diese Verarbeitung ist nicht Gegenstand dieser AVV.

2. GEGENSTAND UND DAUER DER VERARBEITUNG

- 2.1. Die Verarbeitung erfolgt zur Bereitstellung, Sicherung, Wartung und Unterstützung der Convilance SaaS-Lösung für die Dauer des jeweiligen Vertrags sowie während technisch oder gesetzlich erforderlicher Übergangs-, Backup- oder Löschfristen.

3. ART UND ZWECK DER VERARBEITUNG

- 3.1. Die Verarbeitung kann insbesondere folgende Tätigkeiten umfassen:

- a) Erhebung bzw. technischer Abruf von Daten aus vom Kunden definierten digitalen Kanälen;
- b) Übertragung;
- c) Speicherung;
- d) Strukturierung;
- e) Anzeige;
- f) Suche;
- g) Filterung;
- h) regelbasierte Klassifizierung oder Priorisierung;
- i) Dokumentation von Bearbeitungsschritten;
- j) Erstellung von Audit-Trail-Informationen;
- k) Benachrichtigung definierter Benutzer oder Empfänger;
- l) Export;
- m) Anonymisierung;
- n) Löschung;
- o) Sicherung und Wiederherstellung;
- p) technische Analyse zur Fehlerbehebung.

- 3.2. Der Anbieter verarbeitet personenbezogene Daten nicht für Zwecke, die mit den dokumentierten Weisungen des Kunden unvereinbar sind.

4. KATEGORIEN PERSONENBEZOGENER DATEN

- 4.1. Abhängig von den vom Kunden überwachten Kanälen und Anwendungsfällen, können insbesondere folgende Daten verarbeitet werden:

- a) Name und Kontaktdaten;
- b) Benutzer- oder Social-Media-Kennungen;
- c) öffentliche Profilinformationen;
- d) E-Mail-Adressen;
- e) Kommunikationsinhalte;
- f) Beiträge, Kommentare und Nachrichten;
- g) technische Identifikatoren;
- h) Informationen über Arzneimittel oder Medizinprodukte;
- i) Informationen zu Erkrankungen, Symptomen oder medizinischen Behandlungen;
- j) Informationen über vermutete Nebenwirkungen oder unerwünschte Ereignisse;
- k) Produktbeschwerden;
- l) Angaben zu medizinischem Fachpersonal;
- m) gegebenenfalls besondere Kategorien personenbezogener Daten gemäß Art. 9 DSGVO, insbesondere Gesundheitsdaten.

- 4.2. Der Kunde verpflichtet sich, keine für den vereinbarten Zweck nicht erforderlichen personenbezogenen Daten bewusst in Convilance einzubringen.

5. KATEGORIEN BETROFFENER PERSONEN

- 5.1. Je nach Anwendungsfall können insbesondere betroffen sein:

- a) Patienten;
- b) Verbraucher;
- c) Angehörige;
- d) medizinisches Fachpersonal;
- e) Mitarbeiter und Beauftragte des Kunden;
- f) Benutzer von Convilance;
- g) Nutzer digitaler oder sozialer Medien;
- h) sonstige Personen, die in überwachten Inhalten genannt werden.

6. WEISUNGSGEBUNDENE VERARBEITUNG

- 6.1. Der Anbieter verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisung des Kunden, soweit keine gesetzliche Verpflichtung zu einer Verarbeitung besteht.
- 6.2. Der Vertrag, das angenommene Angebot, die Konfiguration des Kunden und dokumentierte Anweisungen autorisierter Ansprechpartner gelten als Weisungen.
- 6.3. Ist der Anbieter aufgrund von Unionsrecht oder dem Recht eines Mitgliedstaats zu einer Verarbeitung verpflichtet, informiert er den Kunden vor der Verarbeitung über diese Verpflichtung, soweit das betreffende Recht eine solche Information nicht untersagt.
- 6.4. Ist der Anbieter der Ansicht, dass eine Weisung gegen die DSGVO oder andere anwendbare Datenschutzvorschriften verstößt, informiert er den Kunden unverzüglich. Der Anbieter darf die betreffende Weisung aussetzen, bis sie geklärt oder geändert wurde.

7. VERTRAULICHKEIT

- 7.1. Der Anbieter stellt sicher, dass Personen, die zur Verarbeitung personenbezogener Daten befugt sind, einer angemessenen gesetzlichen oder vertraglichen Vertraulichkeitsverpflichtung unterliegen.
- 7.2. Zugriff auf personenbezogene Daten erhalten nur Personen, die diesen Zugriff zur Erfüllung ihrer Aufgaben benötigen.

8. SICHERHEIT DER VERARBEITUNG

- 8.1. Der Anbieter trifft angemessene technische und organisatorische Maßnahmen (TOM) gemäß Art. 32 DSGVO.
- 8.2. Der Anbieter darf die Maßnahmen während der Vertragsdauer weiterentwickeln, sofern das vereinbarte Schutzniveau insgesamt nicht wesentlich reduziert wird.

9. SUBPROZESSOREN

- 9.1. Der Kunde erteilt dem Anbieter eine allgemeine Genehmigung zum Einsatz von Subprozessoren, soweit die nachstehenden Bedingungen eingehalten werden.
- 9.2. Die jeweils aktuellen wesentlichen Subprozessoren werden in einer Subprozessorenliste dokumentiert.
- 9.3. Vor Aufnahme eines neuen Subprozessors, der Kundendaten verarbeitet, informiert der Anbieter den Kunden grundsätzlich mindestens 30 Tage im Voraus, soweit dies praktisch möglich ist.
- 9.4. Der Kunde kann einem neuen Subprozessor aus nachweislich berechtigten datenschutzrechtlichen Gründen widersprechen. Die Parteien werden in diesem Fall nach einer wirtschaftlich und technisch angemessenen Lösung suchen. Kann keine angemessene Lösung gefunden werden, kann der Kunde den ausschließlich vom neuen Subprozessor betroffenen Service unter Einhaltung einer angemessenen Frist kündigen.
- 9.5. Der Anbieter verpflichtet Subprozessoren zu Datenschutzpflichten, die hinsichtlich des Schutzes personenbezogener Daten im Wesentlichen den Verpflichtungen dieser AVV entsprechen.
- 9.6. Der Anbieter bleibt gegenüber dem Kunden für die Erfüllung der ihm nach Art. 28 DSGVO obliegenden Pflichten durch seine Subprozessoren verantwortlich.

10. INTERNATIONALE DATENÜBERMITTLUNGEN

- 10.1. Der Anbieter verarbeitet Kundendaten grundsätzlich in folgender Region:
 - a) Primäre Hosting-/Verarbeitungsregion: EU/EWR
- 10.2. Soweit personenbezogene Daten in ein Drittland außerhalb des EWR übertragen werden, erfolgt dies nur unter Einhaltung der Voraussetzungen der Kapitel V DSGVO.
- 10.3. Soweit erforderlich, werden insbesondere eingesetzt:
 - a) Angemessenheitsbeschlüsse der Europäischen Kommission;
 - b) Standardvertragsklauseln der Europäischen Kommission;

c) sonstige gesetzlich anerkannte Transfermechanismen.

- 10.4. Soweit erforderlich, prüft der Anbieter ergänzende technische, vertragliche oder organisatorische Schutzmaßnahmen.

11. UNTERSTÜTZUNG BEI BETROFFENENRECHTEN

- 11.1. Soweit dies unter Berücksichtigung der Art der Verarbeitung möglich ist, unterstützt der Anbieter den Kunden durch angemessene technische und organisatorische Maßnahmen bei der Erfüllung von Betroffenenrechten.
- 11.2. Erhält der Anbieter unmittelbar ein Ersuchen einer betroffenen Person, das sich auf Kundendaten bezieht, wird er das Ersuchen grundsätzlich an den Kunden weiterleiten und nicht selbst inhaltlich beantworten, soweit keine gesetzliche Verpflichtung besteht.
- 11.3. Soweit eine Unterstützung erheblich über die gewöhnliche Bereitstellung von Convilance hinausgeht, können angemessene zusätzliche Aufwände nach vorheriger Abstimmung vergütet werden.

12. UNTERSTÜTZUNG BEI DATENSCHUTZPFLICHTEN

- 12.1. Der Anbieter unterstützt den Kunden unter Berücksichtigung der Art der Verarbeitung und der ihm verfügbaren Informationen in angemessenem Umfang bei:
- a) der Sicherheit der Verarbeitung;
 - b) der Meldung von Datenschutzverletzungen;
 - c) der Benachrichtigung betroffener Personen;
 - d) Datenschutz-Folgenabschätzungen;
 - e) erforderlichen Konsultationen mit Aufsichtsbehörden.
- 12.2. Die gesetzliche Verantwortlichkeit des Kunden als Verantwortlicher bleibt unberührt.

13. VERLETZUNG DES SCHUTZES PERSONENBEZOGENER DATEN

- 13.1. Der Anbieter informiert den Kunden nach Bekanntwerden einer Verletzung des Schutzes personenbezogener Kundendaten unverzüglich und, soweit vernünftigerweise möglich, innerhalb von 24 Stunden nach Bekanntwerden.
- 13.2. Eine Erstmeldung kann auf den zu diesem Zeitpunkt verfügbaren Informationen beruhen und wird bei Bedarf schrittweise ergänzt.
- 13.3. Die Meldung enthält, soweit verfügbar:
 - a) Beschreibung der Art des Vorfalls;
 - b) Kategorien der betroffenen Daten;
 - c) Kategorien bzw. ungefähre Anzahl betroffener Personen, soweit feststellbar;
 - d) wahrscheinliche Folgen;
 - e) ergriffene oder geplante Abhilfemaßnahmen;
 - f) Ansprechpartner für weitere Informationen.
- 13.4. Eine solche Mitteilung stellt kein Anerkenntnis einer Pflichtverletzung oder Haftung dar.
- 13.5. Die Entscheidung darüber, ob eine Meldung an eine Aufsichtsbehörde oder betroffene Personen erforderlich ist, obliegt grundsätzlich dem Kunden als Verantwortlichem.

14. AUDITS UND NACHWEISE

- 14.1. Der Anbieter stellt dem Kunden alle Informationen zur Verfügung, die vernünftigerweise erforderlich sind, um die Einhaltung der Pflichten gemäß Art. 28 DSGVO nachzuweisen.
- 14.2. Soweit verfügbar, soll der Nachweis vorrangig durch geeignete standardisierte Unterlagen erfolgen, insbesondere:
 - a) Security- und Compliance-Dokumentation;
 - b) TOMs;
 - c) Auditberichte, soweit vorhanden.

14.3. Soweit solche Unterlagen nicht ausreichen, darf der Kunde oder ein zur Vertraulichkeit verpflichteter unabhängiger Auditor ein angemessenes Audit durchführen.

14.4. Audits sollen grundsätzlich:

- a) mit mindestens 30 Tagen Vorlauf angekündigt werden;
- b) während üblicher Geschäftszeiten erfolgen;
- c) den Betrieb des Anbieters nicht unangemessen beeinträchtigen;
- d) keine Daten anderer Kunden offenlegen.

14.5. Die Beschränkung auf ein Audit pro Jahr gilt nicht, soweit:

- a) eine zuständige Aufsichtsbehörde ein Audit verlangt;
- b) eine wesentliche Datenschutzverletzung Anlass für eine zusätzliche Prüfung gibt;
- c) konkrete Anhaltspunkte für einen erheblichen Verstoß bestehen.

15. LÖSCHUNG UND RÜCKGABE

15.1. Nach Ende der Leistungserbringung kann der Kunde verfügbare Datenexporte nach Maßgabe der AGBs beziehen.

15.2. Soweit nichts anderes vereinbart ist, bleiben produktive Kundendaten nach Vertragsende für bis zu 60 Tage zur vereinbarten Datenherausgabe verfügbar.

15.3. Danach löscht oder anonymisiert der Anbieter die personenbezogenen Kundendaten, soweit keine gesetzliche Aufbewahrungspflicht besteht.

15.4. Daten in technisch getrennten Sicherungskopien können für einen begrenzten Zeitraum fortbestehen und werden im Rahmen des regulären Backup-Lebenszyklus überschrieben bzw. gelöscht.

15.5. Solange personenbezogene Daten ausschließlich in Backups fortbestehen, werden sie nicht für operative Zwecke wiederhergestellt, sofern dies nicht aus Gründen der Notfallwiederherstellung oder aufgrund gesetzlicher Anforderungen erforderlich ist.

16. BEHÖRDLICHE ANFRAGEN

- 16.1. Soweit rechtlich zulässig, informiert der Anbieter den Kunden über verbindliche behördliche oder gerichtliche Anfragen, die auf die Offenlegung von Kundendaten gerichtet sind.
- 16.2. Der Anbieter wird keine Kundendaten offenlegen, die über das rechtlich Erforderliche hinausgehen.

17. HAFTUNG

- 17.1. Die Haftung aus dieser AVV richtet sich nach den zwischen den Parteien vereinbarten Haftungsregelungen der AGBs und des akzeptierten Angebots, soweit zwingendes Datenschutzrecht nichts anderes verlangt.

18. LAUFZEIT

- 18.1. Diese AVV gilt so lange, wie der Anbieter personenbezogene Daten im Auftrag des Kunden verarbeitet.
- 18.2. Datenschutz-, Lösungs-, Vertraulichkeits- und Nachweispflichten, die ihrem Zweck nach über das Vertragsende hinausgelten, bleiben bestehen.

Stand: Jänner 2025 / Convilance_AVV_V2_2025-01