



Auftragsverarbeitungsvertrag (Art. 28 DSGVO)

Version: 14.10.2025

ClickSurance GmbH

Wiener Straße 125
2700 Wiener Neustadt
FN: 630769 b
(Betreiberin von **krankenprofi.at**)

im Folgenden „**Auftragsverarbeiter**“ oder „**ClickSurance**“

verpflichtet sich gegenüber dem **Kunden** (Lizenznehmer/User) als „**Verantwortlicher**“ gemäß DSGVO wie folgt:

1. Präambel und Verhältnis zum Hauptvertrag

- 1.1. Dieser Auftragsverarbeitungsvertrag („**AVV**“) konkretisiert die datenschutzrechtlichen Rechte und Pflichten der Parteien gem. Art. 28 DSGVO für die Nutzung der Plattform **krankenprofi.at** gemäß dem zwischen den Parteien bestehenden Nutzungsvertrag („**Hauptvertrag**“).
- 1.2. Der Verantwortliche entscheidet allein über Zwecke und Mittel der Verarbeitung personenbezogener Daten. ClickSurance verarbeitet personenbezogene Daten **ausschließlich** auf dokumentierte Weisung des Verantwortlichen, soweit nicht eine gesetzliche Verpflichtung iSd Art. 28 Abs. 3 lit. a DSGVO entgegensteht.
- 1.3. Im Falle von Widersprüchen geht dieser AVV den AGB und sonstigen Vertragsbestandteilen **in datenschutzrechtlichen Fragen** vor; im Übrigen gilt der Hauptvertrag.

2. Gegenstand, Art und Zweck der Verarbeitung

- 2.1. **Gegenstand** ist der Betrieb und die Bereitstellung der Plattform **krankenprofi.at** inkl. Berechnungs-/Vergleichs-Tools, Wissensdatenbank, Benutzer- und Rechtemanagement, Support sowie ggf. lokal bereitgestellte Excel-Rechner.
- 2.2. **Zweck** ist die Nutzung der Plattform durch den Verantwortlichen zur Beratung, Vergleichserstellung, Angebotserstellung, Verwaltung und Dokumentation im Versicherungsvermittlungsumfeld.
- 2.3. **Art der Verarbeitung** umfasst insbesondere: Erheben, Speichern, Ordnen, Auslesen, Abfragen, Verwenden, Übermitteln, Einschränken, Löschen/vernichten, sowie Protokollierung (Logging) systembezogener Vorgänge.



3. Kategorien personenbezogener Daten und betroffene Personen

- 3.1. **Datenkategorien (je nach Nutzung):** Personendaten, Daten von Familien- und Haushaltsangehörigen, Kundenwünsche- und Bedürfnisse, Berufs- und Arbeitgeberdaten, Adressdaten, Kommunikationsdaten
- 3.2. Soweit vom Verantwortlichen eingegeben: **besondere Kategorien** iSd Art. 9 DSGVO, insbesondere **Gesundheitsdaten**.
- 3.3. **Betroffene Personen:** Kunden, Interessenten und Mitarbeiter des Verantwortlichen, Kontaktpersonen bei Produktanbietern/Versicherern sowie sonstige durch den Verantwortlichen eingegebene Personen.
- 3.4. Der Verantwortliche stellt sicher, dass für sämtliche Daten eine geeignete **Rechtsgrundlage** (Art. 6 DSGVO; bei Gesundheitsdaten Art. 9 DSGVO, etwa ausdrückliche Einwilligung oder einschlägige Ausnahmen) besteht.

4. Dauer und Beendigung

- 4.1. Die Verarbeitung beginnt mit Leistungsbeginn nach Hauptvertrag und endet mit dessen Beendigung.
- 4.2. Nach Vertragsende löscht oder gibt ClickSurance personenbezogene Daten gemäß Ziff. 12 zurück; gesetzliche Aufbewahrungspflichten bleiben unberührt.

5. Ort der Verarbeitung und Drittlandübermittlungen

- 5.1. Die Verarbeitung erfolgt grundsätzlich in der **EU/EWR**.
- 5.2. Einsätze in Drittländern erfolgen nur, wenn die Voraussetzungen der Art. 44 ff. DSGVO (insb. **EU-Standardvertragsklauseln 2021/914/EU** inkl. ergänzender Maßnahmen, ggf. Angemessenheitsbeschluss) erfüllt sind.

6. Pflichten des Auftragsverarbeiters

- 6.1. **Weisungen:** Verarbeitung ausschließlich auf dokumentierte Weisungen des Verantwortlichen. ClickSurance informiert den Verantwortlichen unverzüglich, wenn eine Weisung offenkundig rechtswidrig ist; die Umsetzung kann bis zur Bestätigung/modifizierten Weisung ausgesetzt werden.
- 6.2. **Vertraulichkeit:** ClickSurance verpflichtet sämtliche dem Auftrag zugeordnete Personen schriftlich auf Vertraulichkeit und Datengeheimnis; Nachweise werden auf Verlangen vorgelegt.
- 6.3. **Technische und organisatorische Maßnahmen (TOM):** ClickSurance unterhält TOM gemäß **Anlage 2** nach Art. 32 DSGVO (Stand der Technik, Risikoangemessenheit). Gleichwertige Anpassungen sind zulässig, sofern das Schutzniveau nicht unterschritten wird.
- 6.4. **Unterstützungspflichten:** ClickSurance unterstützt den Verantwortlichen in angemessenem Umfang bei: (i) Beantwortung von Betroffenenanfragen (Kap. III DSGVO), (ii)



Datensicherheitsvorfällen (Art. 33/34 DSGVO), (iii) Datenschutz-Folgenabschätzungen inkl. Konsultationen (Art. 35/36 DSGVO), (iv) Umsetzung von Löschung, Berichtigung, Einschränkung und Datenübertragbarkeit.

6.5. **Meldung von Verletzungen:** ClickSurance meldet **unverzüglich** und **ohne schuldhaftes Zögern** (jedenfalls **spätestens binnen 24 Stunden** nach Kenntniserlangung) Verletzungen des Schutzes personenbezogener Daten mit den nach Art. 33 Abs. 3 DSGVO erforderlichen Angaben.

6.6. **Nachweise und Audits:** ClickSurance stellt die zur Einhaltung dieses AVV erforderlichen Informationen zur Verfügung und ermöglicht Audits/Inspektionen durch den Verantwortlichen oder von ihm beauftragte, nicht in Wettbewerbsbeziehung stehende Prüfer, mit angemessener Vorankündigung, zu üblichen Geschäftszeiten und unter Wahrung der Vertraulichkeit. Der Verantwortliche trägt den dabei anfallenden angemessenen Aufwand von ClickSurance.

6.7. **Datenminimierung und Speicherbegrenzung:** ClickSurance implementiert Prozesse zur Rollen-/Rechtevergabe, Protokollierung, Löschung und Anonymisierung/Pseudonymisierung gemäß Anlage 2.

7. Pflichten des Verantwortlichen

7.1. Der Verantwortliche ist für die **Rechtmäßigkeit** der Verarbeitung, die **Informationspflichten** nach Art. 13/14 DSGVO, die Betroffenenrechte, die Datenqualität (Richtigkeit/Aktualität) und die Rechtsgrundlage bei besonderen Kategorien (Art. 9 DSGVO) verantwortlich.

7.2. Der Verantwortliche verwaltet Benutzer und Berechtigungen eigenverantwortlich, wahrt Geheimhaltungspflichten bzgl. Zugangsdaten und trifft angemessene Sicherheitsmaßnahmen innerhalb seiner Sphäre (Endgeräte, Netzwerke, Schnittstellen).

8. Sub-Auftragsverarbeiter

8.1. Der Verantwortliche erteilt eine **allgemeine Genehmigung** zum Einsatz von Sub-Auftragsverarbeitern. Die jeweils aktuelle Liste wird in **Anlage 1** geführt und auf Anfrage bereitgestellt.

8.2. ClickSurance informiert den Verantwortlichen **vorab** über geplante Änderungen (Hinzunahme/Ersetzung) in **Textform**. Der Verantwortliche kann binnen **10 Werktagen** ab Zugang begründeten Widerspruch erheben. Erfolgt ein Widerspruch und ist keine zumutbare Alternative verfügbar, sind beide Parteien zur **Sonderkündigung** des Hauptvertrags/AVV zum Änderungsstichtag berechtigt.

8.3. ClickSurance verpflichtet Sub-Auftragsverarbeiter schriftlich auf **Pflichten, die mindestens dem Schutzniveau dieses AVV entsprechen**, inkl. TOM, Weisungsgebundenheit, Löschung/Rückgabe und Unterstützungspflichten.



9. Vertraulichkeit, Geheimhaltung, Geschäftsgeheimnisse

9.1. Parteien behandeln alle im Zusammenhang mit diesem AVV bekanntwerdenden Informationen streng vertraulich. Gesetzliche Offenlegungspflichten bleiben unberührt.

10. Haftung

10.1. Die Haftung der Parteien richtet sich nach den gesetzlichen Bestimmungen der DSGVO sowie den Regelungen des Hauptvertrags. Nichts in diesem AVV begründet eine weitergehende Haftung als nach Hauptvertrag/gesetzlich vorgesehen.

11. Rückgabe und Löschung von Daten

11.1. Nach Beendigung des Hauptvertrags wird ClickSurance auf dokumentierte Weisung des Verantwortlichen personenbezogene Daten in einem **gängigen, strukturierten, maschinenlesbaren Format** bereitstellen und anschließend **löschen**, sofern keine gesetzliche Aufbewahrungspflicht entgegensteht.

11.2. Sofern nicht anders vereinbart, erfolgt die vollständige Löschung **spätestens binnen 60 Tagen** nach Weisung durch den Verantwortlichen. Protokolle über Löschungen werden bereitgestellt. Angemessene Aufwände für Datenexporte können nach tatsächlich angefallenem Aufwand verrechnet werden.

12. Schlussbestimmungen

12.1. **Anwendbares Recht/Gerichtsstand:** Es gilt österreichisches Recht; ausschließlicher Gerichtsstand ist – soweit zulässig – **Wiener Neustadt**.

12.2. **Schriftform/Änderungen:** Änderungen/Ergänzungen dieses AVV bedürfen der Schriftform (E-Mail genügt). Dies gilt auch für das Abgehen vom Schriftformerfordernis.

12.3. **Salvatorische Klausel:** Sollten Bestimmungen dieses AVV unwirksam sein/werden, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt; anstelle der unwirksamen Bestimmung gilt eine wirksame Regelung, die dem wirtschaftlichen Zweck am nächsten kommt.



Anlage 1: Liste der Sub-Auftragsverarbeiter

Diese Liste ist aktuell zu halten; Eintragungen/Änderungen werden dem Verantwortlichen gemäß Ziff. 8.2 mitgeteilt.

- Hetzner Online GmbH, Industriestr. 25, 91710 Gunzenhausen: Serverhosting
- IONOS SE Elgendorfer Str. 57 56410 Montabaur: Serverhosting, Webmail

Anlage 2: Technische und organisatorische Maßnahmen (Art. 32 DSGVO)

Sicherheitsorganisation & Governance - Datenschutz-Management, Informationssicherheitsrichtlinien, Rollen-/Rechtekonzept, Need-to-know-Prinzip, Schulungen/Verpflichtung auf Vertraulichkeit.

Zutritts-, Zugangs- und Zugriffskontrolle – Schlüsselgesicherte Zugriffe, rollenbasierte Berechtigungen, Passwortgesicherte Zugänge, Protokollierung administrativer Zugriffe, Trennung von Produktiv/ Test

Weitergabe-/Übertragungskontrolle Gesicherte Schnittstellen/APIs, Restriktion externer Datenträger, definierte Exportprozesse. Weisung der Mitarbeiter zum datenschutzkonformen Umgang mit personenbezogenen Daten.

Eingabe-/Protokollkontrolle - Logging relevanter Ereignisse (Login, Rollenänderungen, Datenexporte), Zeitstempel, Speicherung gemäß Aufbewahrungsregeln.

Trennungsgebot - Logische Mandantentrennung, Trennung Produktiv- und Testsysteme, Festlegung von Datenbankrechten

Verfügbarkeits- und Wiederherstellungskontrolle - Redundanzen, Monitoring/Alerting, Backup-/Restore-Prozesse, USV/Brandschutz im RZ

Datenschutz durch Technikgestaltung und Voreinstellungen (Art. 25 DSGVO) - Datenminimierung, Speicherbegrenzung, Pseudonymisierung/Anonymisierung wo möglich

Lieferanten-/Sub-Prozessor-Management - Vertragliche Verpflichtung nach Art. 28, Sicherheitsbewertung vor Einsatz, laufendes Monitoring, SCC/zusätzliche Maßnahmen bei Drittländern.

Sichere Entwicklung & Änderungen - Gesicherter Entwicklungsprozess (Code-Reviews, Versionskontrolle, Staging), Schwachstellen-Scans, Patch-Management.



Vorfallmanagement - Prozesse zur Erkennung, Meldung und Behandlung von Sicherheitsvorfällen, dokumentierte Kommunikationswege, Lessons-learned.

Datenlöschung - Lösch-/Anonymisierungs-Konzepte mit Fristen; sichere Vernichtung von Datenträgern.

Die TOM werden regelmäßig an den Stand der Technik und das konkrete Risiko angepasst; gleichwertige Änderungen sind zulässig, sofern das Schutzniveau nicht reduziert wird.