PRAEVERA SOLUTIONS

Vertrag zur Auftragsverarbeitung (AVV)

gemäß Art. 28 DSGVO

Version 3.0 | Stand: Juli 2026

Parteien

Zwischen

dem Kunden der Praevera Solutions

– nachfolgend „Verantwortlicher“ genannt –

und

Praevera Solutions, André Hagemann, Am Wäldele 20, 79312 Windenreute

– nachfolgend „Auftragsverarbeiter“ genannt –

– gemeinsam nachfolgend „Parteien“ genannt –

Präambel

Der Auftragsverarbeiter stellt dem Verantwortlichen eine Softwarelösung für medizinische Fachkräfte (MFA/VERAH) bereit, die auf einer Ende-zu-Ende-Verschlüsselung (E2EE) basiert. Der Auftragsverarbeiter betreibt eine Zero-Knowledge-Infrastruktur: Patientendaten werden clientseitig mit einem vom Verantwortlichen kontrollierten Schlüssel verschlüsselt. Der Auftragsverarbeiter hat technisch keinen Zugriff auf Klartext-Patientendaten. Dieser Vertrag regelt die datenschutzrechtlichen Pflichten beider Parteien gemäß Art. 28 DSGVO.

§ 1 Gegenstand und Dauer des Auftrags

1. Der Auftragsverarbeiter stellt dem Verantwortlichen eine cloudbasierte Softwarelösung zur Unterstützung medizinischer Fachkräfte (MFA/VERAH) in der Praxisorganisation und Patientenverwaltung zur Verfügung.

2. Die Laufzeit dieses Vertrags entspricht der Laufzeit des Hauptvertrages über die Nutzung der Software. Er endet automatisch mit Beendigung des Hauptvertrages, soweit keine gesonderten Vereinbarungen über Datenlöschung oder -aufbewahrung getroffen wurden.
3. Änderungen und Ergänzungen dieses Vertrags bedürfen der Schriftform oder der Textform (E-Mail).

§ 2 Art, Zweck und Ort der Verarbeitung

1. Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschließlich im Auftrag und nach dokumentierter Weisung des Verantwortlichen, es sei denn, er ist durch das Recht der EU oder des Mitgliedstaates zur Verarbeitung verpflichtet (Art. 28 Abs. 3 lit. a DSGVO).
2. **Zweck der Verarbeitung:** Bereitstellung, Betrieb und Wartung der Softwarelösung für die Praxisorganisation, Terminplanung, Aufgabenverwaltung und Patientenkommunikation.
3. **Art der Verarbeitung:** Erhebung, Speicherung, Übermittlung, Abruf und Löschung personenbezogener Daten im Rahmen des Softwarebetriebs.
4. **Besonderheit (E2EE/Zero-Knowledge):** Die Verarbeitung von Patientendaten erfolgt mittels AES-256-Verschlüsselung. Der Auftragsverarbeiter hat keinen Zugriff auf Klartext-Patientendaten. Alle kryptografischen Schlüssel verbleiben ausschließlich beim Verantwortlichen.
5. **Ort der Verarbeitung:** Ausschließlich innerhalb der EU/EWR. Serverstandort: Deutschland (Hetzner Online GmbH). Eine Übermittlung in Drittländer findet nicht statt; sollte eine solche erforderlich werden, bedarf sie der vorherigen schriftlichen Zustimmung des Verantwortlichen und der Einhaltung der Art. 44 ff. DSGVO.

§ 3 Kategorien betroffener Personen und Datenarten

1. **Betroffene Personen:**
   - Patienten des Verantwortlichen
   - Mitarbeitende und Nutzende der Praxis des Verantwortlichen (MFA/VERAH)
2. **Datenarten:**
   - **Stammdaten:** Name, Vorname, E-Mail-Adresse, Benutzername, Praxisname
   - **Besondere Kategorien (Art. 9 DSGVO):** Gesundheitsdaten, medizinische Diagnosen, Behandlungsverläufe, Medikamentenpläne (ausschließlich in verschlüsselter Form gespeichert)

- **Technische Metadaten:** IP-Adressen, Zeitstempel, kryptografische Parameter (Salts, Nonces, verschlüsselte Schlüsselcontainer)

3. Der Verantwortliche ist allein verantwortlich für eine geeignete Rechtsgrundlage nach Art. 9 DSGVO (z. B. Art. 9 Abs. 2 lit. h DSGVO i. V. m. § 22 BDSG).

§ 4 Pflichten des Auftragsverarbeiters

Der Auftragsverarbeiter verpflichtet sich:

1. Personenbezogene Daten ausschließlich auf dokumentierte Weisung des Verantwortlichen hin zu verarbeiten (inkl. E2EE-Logik) und keine Daten für eigene Zwecke zu nutzen.
2. Alle mit der Verarbeitung befassten Personen zur Vertraulichkeit zu verpflichten (Art. 28 Abs. 3 lit. b DSGVO).
3. Die erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 32 DSGVO umzusetzen (siehe Anlage TOMs).
4. Den Verantwortlichen bei der Erfüllung von Betroffenenrechten (Art. 15–22 DSGVO) zu unterstützen, soweit technisch möglich. Aufgrund der E2EE-Architektur ist eine Auskunft über Klartext-Inhalte technisch nicht möglich.
5. Den Verantwortlichen bei DSFA (Art. 35 DSGVO) und vorheriger Konsultation der Aufsichtsbehörde (Art. 36 DSGVO) zu unterstützen.
6. Alle Informationen für das Verarbeitungsverzeichnis nach Art. 30 DSGVO bereitzustellen.
7. Mit der Aufsichtsbehörde zu kooperieren (Art. 31 DSGVO).
8. Den Verantwortlichen unverzüglich zu informieren, wenn eine Weisung gegen die DSGVO oder andere Datenschutzvorschriften verstößt.

§ 5 Meldepflichten bei Datenpannen

1. Der Auftragsverarbeiter unterstützt den Verantwortlichen bei der Einhaltung der Art. 33 und 34 DSGVO.
2. Der Auftragsverarbeiter meldet dem Verantwortlichen jede Datenschutzverletzung unverzüglich, spätestens innerhalb von 24 Stunden nach Bekanntwerden (Ziel: Einhaltung der 72-Stunden-Frist nach Art. 33 DSGVO).
3. **Die Meldung enthält mindestens:**
   - Art der Verletzung und betroffene Datenkategorien
   - Ungefähre Anzahl betroffener Personen und Datensätze
   - Kontaktdaten der Anlaufstelle

- Beschreibung der wahrscheinlichen Folgen
- Ergriffene oder vorgeschlagene Abhilfemaßnahmen

4. **Besonderheit E2EE:** Da Patientendaten ausschließlich verschlüsselt gespeichert werden, ist eine Verletzung der Vertraulichkeit von Patienteninhalten durch Unbefugte technisch weitgehend ausgeschlossen. Eine Datenpanne kann dennoch vorliegen, wenn verschlüsselte Datensätze verloren gehen oder die Systemverfügbarkeit beeinträchtigt wird.

---

§ 6 Unterauftragsverhältnisse

1. Der Verantwortliche erteilt die allgemeine Genehmigung zur Einschaltung von Unterauftragsverarbeitern. Derzeit genehmigt:

Unternehmen	Leistung	Serverstandort
Hetzner Online GmbH, Industriestr. 25, 91710 Gunzenhausen	Server-Hosting, Datenbankinfrastruktur	Deutschland (ISO 27001)

2. **Hinzunahme neuer Unterauftragsverarbeiter:** Vorlauffrist mind. 30 Tage. Der Verantwortliche kann innerhalb von 14 Tagen Widerspruch einlegen. Ohne Widerspruch gilt die Genehmigung als erteilt. Wird kein einvernehmlicher Ersatz gefunden, kann der Verantwortliche den Hauptvertrag außerordentlich kündigen.
3. Der Auftragsverarbeiter verpflichtet Unterauftragsverarbeiter vertraglich zu denselben Datenschutzverpflichtungen (Art. 28 Abs. 4 DSGVO).
4. Der Auftragsverarbeiter bleibt für die Erfüllung der datenschutzrechtlichen Pflichten der Unterauftragsverarbeiter vollumfänglich verantwortlich.

---

§ 7 Pflichten des Verantwortlichen

1. Der Verantwortliche ist für die Rechtmäßigkeit der Datenverarbeitung und die Einholung etwaiger Einwilligungen allein verantwortlich.
2. Der Verantwortliche erteilt alle Weisungen schriftlich oder in Textform. Mündliche Weisungen sind unverzüglich schriftlich zu bestätigen.
3. Der Verantwortliche stellt sicher, dass er für die Verarbeitung von Gesundheitsdaten (Art. 9 DSGVO) eine geeignete Rechtsgrundlage besitzt.
4. Der Verantwortliche ist für die sichere Verwahrung seines Praxis-Kennworts allein verantwortlich. Der Auftragsverarbeiter kann bei Verlust keine Wiederherstellung der Klartext-Daten gewährleisten.

5. Der Verantwortliche informiert den Auftragsverarbeiter unverzüglich über festgestellte Fehler oder Unregelmäßigkeiten.

§ 8 Kontrollrechte

1. Der Verantwortliche ist berechtigt, die Einhaltung dieses Vertrages zu kontrollieren, z. B. durch:
   - Anforderung von Selbstauskünften und Nachweisen (z. B. Zertifizierungen, Prüfberichte)
   - Ankündigung von Audits mit einer Vorlauffrist von mindestens 14 Tagen
2. Der Auftragsverarbeiter gewährt alle erforderlichen Auskünfte und ermöglicht Überprüfungen; er ist berechtigt, den Zugang auf das notwendige Maß zu beschränken.
3. Als gleichwertige Nachweise können Testate, Berichte oder Berichtsauszüge unabhängiger Prüfer (z. B. Penetrationstests, ISO-Zertifikate) vorgelegt werden.

§ 9 Löschung und Rückgabe von Daten

1. Nach Beendigung des Auftrags löscht der Auftragsverarbeiter alle personenbezogenen Daten oder gibt sie zurück – nach Wahl des Verantwortlichen – soweit keine Aufbewahrungspflicht besteht.
2. **Besonderheit E2EE:** Der Auftragsverarbeiter kann Klartext-Daten technisch nicht zurückgeben. Auf Anfrage werden verschlüsselte Rohdaten in einem gängigen Format (z. B. SQL-Dump, JSON-Export) zur Verfügung gestellt.
3. Die Löschung wird auf Anfrage des Verantwortlichen schriftlich bestätigt.

§ 10 Haftung und Schadensersatz

1. Die Parteien haften nach den Bestimmungen des Art. 82 DSGVO.
2. Für einfache Fahrlässigkeit ist die Haftung des Auftragsverarbeiters auf den typischerweise vorhersehbaren Schaden begrenzt. Diese Beschränkung gilt nicht bei Verletzung von Leben, Körper oder Gesundheit sowie bei Verstößen gegen wesentliche Vertragspflichten.
3. **Haftungsausschluss bei Schlüsselverlust:** Da der Auftragsverarbeiter keinen Zugriff auf die Praxis-Passphrase hat, trägt der Verantwortliche die alleinige Verantwortung für die Verwaltung seiner kryptografischen Schlüssel. Datenverluste durch Verlust der Passphrase oder Schlüssel liegen im Verantwortungsbereich des Verantwortlichen.
4. Der Auftragsverarbeiter kann sich nur entlasten, wenn er nachweist, dass er für den schadenbegründenden Umstand nicht verantwortlich ist (Art. 82 Abs. 3 DSGVO).

§ 11 Schlussbestimmungen

1. **Textform:** Änderungen und Ergänzungen dieses Vertrages bedürfen der Textform (E-Mail genügt). Dies gilt auch für die Aufhebung des Textformerfordernisses selbst.
2. **Rechtswahl:** Es gilt das Recht der Bundesrepublik Deutschland unter Ausschluss des UN-Kaufrechts.
3. **Gerichtsstand:** Gerichtsstand ist, soweit gesetzlich zulässig, der Sitz des Auftragsverarbeiters.
4. **Salvatorische Klausel:** Unwirksame Bestimmungen berühren die Wirksamkeit der übrigen Bestimmungen nicht. Die Parteien verpflichten sich zum wirtschaftlich zweckentsprechenden Ersatz.
5. **Vollständigkeit:** Dieser Vertrag und seine Anlagen ersetzen alle früheren Vereinbarungen zum Datenschutz.
6. **Vorrang:** Im Falle von Widersprüchen zwischen diesem AVV und dem Hauptvertrag hat dieser AVV in datenschutzrechtlichen Belangen Vorrang.

ANLAGE: Technische und Organisatorische Maßnahmen (TOMs)

gemäß Art. 32 DSGVO

---

1. Vertraulichkeit

Zutrittskontrolle

- Hosting bei Hetzner Online GmbH, Rechenzentrum Deutschland, ISO 27001 zertifiziert
- Physische Sicherung durch Hetzner (Zutrittskontrollsysteme, Videoüberwachung)

Zugangskontrolle

- Benutzerauthentifizierung via Username/Passwort (gehasht)
- TLS 1.2/1.3-Verschlüsselung für alle Datenübertragungen
- Automatischer Sitzungsablauf nach Inaktivität

Zugriffskontrolle

- Zero-Knowledge-Architektur: Patientendaten mit AES-256 clientseitig verschlüsselt
- Zugriff auf Klartextdaten ausschließlich mit lokalem Schlüssel der Nutzenden
- Strenge Rollentrennung; kein Administratorzugriff auf Klartext-Patientendaten

Trennungskontrolle

- Mandantentrennung auf Datenbankebene
- Kryptografische Isolation der Mandantendaten durch individuelle Schlüssel

2. Integrität

Weitergabekontrolle

- Alle Datenflüsse zwischen Client und Server sind TLS-verschlüsselt
- Daten verlassen den Server ausschließlich in verschlüsselter Form

Eingabekontrolle

- Protokollierung von Systemzugriffen und sicherheitsrelevanten Ereignissen
- Logs werden 7 Tage vorgehalten und sind gegen Manipulation geschützt

3. Verfügbarkeit und Belastbarkeit

Verfügbarkeitskontrolle

- Tägliche automatisierte Backups bei Hetzner
- Monitoring mit automatischen Alerts

Wiederherstellbarkeit

PRAEVERA Solutions
André Hagemann
Am Wäldele 20
79312 Emmendingen

info@praevera.de
www.praevera.de
+49 151 587 450 86

IBAN: DE39 2022 0800 0056 5758 82

- Dokumentierte und getestete Backup-Restore-Prozesse
- Regelmäßige Wiederherstellungstests

4. Regelmäßige Überprüfung, Bewertung und Evaluierung

- Regelmäßige Security-Updates (Django, Abhängigkeiten, Server-Umgebung)
- Regelmäßige Überprüfung der Zugriffsrechte
- Code-Reviews und Abhängigkeits-Scans
- Dokumentierter Incident-Response-Prozess

5. Besondere Maßnahmen für Gesundheitsdaten (Art. 9 DSGVO)

- Verschlüsselung at rest: AES-256 für alle Gesundheitsdaten
- Verschlüsselung in transit: TLS 1.2/1.3
- Pseudonymisierung: Logs und IP-Adressen werden getrennt von Patientendaten verarbeitet
- Schlüsselmanagement: Kryptografische Schlüssel verbleiben ausschließlich beim Verantwortlichen
- Datensparsamkeit: Nur für den Betrieb notwendige Daten werden erhoben
- Mitarbeitersensibilisierung: Regelmäßige Schulungen zu Datenschutz und Datensicherheit

---

Unterzeichnung

Dieser Vertrag wird in zwei gleichlautenden Exemplaren ausgefertigt. Jede Partei erhält ein Exemplar.

Verantwortlicher

Ort, Datum:

Name/Praxis:

Funktion:

_____
Unterschrift

Auftragsverarbeiter

Ort, Datum: Windenreute,

_____

Name: André Hagemann

Unternehmen: Praevera Solutions

Funktion: Inhaber

_____
Unterschrift

Hinweis: Dieser AVV (Version 3.0) ersetzt alle vorherigen Versionen. Bitte vor Unterzeichnung rechtlich prüfen lassen.

PRAEVERA Solutions
André Hagemann
Am Wäldele 20
79312 Emmendingen

info@praevera.de
www.praevera.de
+49 151 587 450 86

IBAN: DE39 2022 0800 0056 5758 82