Vertrag zur Auftragsverarbeitung (AVV)

gemäß Art. 28 DSGVO

Zwischen

Dem Kunden der Praevera Solutions – nachfolgend „Verantwortlicher“ genannt –

und

Praevera Solutions André Hagemann, Am Wäldele 20, 79312 Windenreute

– nachfolgend „Auftragsverarbeiter“ genannt –

§ 1 Gegenstand und Dauer des Auftrags

1. Der Auftragsverarbeiter stellt dem Verantwortlichen eine Softwarelösung für medizinische Fachkräfte (MFA/VERAH) zur Verfügung.
2. Die Laufzeit dieses Vertrags entspricht der Laufzeit des Hauptvertrages über die Nutzung der Software.

§ 2 Art und Zweck der Verarbeitung

1. Der Auftragsverarbeiter verarbeitet personenbezogene Daten im Auftrag und nach Weisung des Verantwortlichen.
2. **Besonderheit (E2EE):** Die Verarbeitung von Patientendaten erfolgt mittels einer Ende-zu-Ende-Verschlüsselung (E2EE). Der Auftragsverarbeiter stellt die verschlüsselte Infrastruktur bereit, hat jedoch technisch keinen Zugriff auf die im Klartext vorliegenden Patientendaten des Verantwortlichen.

§ 3 Kategorien betroffener Personen und Datenarten

1. **Betroffene Personen:** Patienten des Verantwortlichen, Mitarbeiter (Nutzer) des Verantwortlichen.
2. **Datenarten:**
    - **Stammdaten:** Name, Vorname, E-Mail, Username, Praxisname.
    - **Besondere Kategorien (Art. 9 DSGVO):** Medizinische Daten, Diagnosen, Behandlungsverläufe.
    - **Technische Metadaten:** IP-Adressen, kryptografische Parameter (Salts, Nonces).

§ 4 Pflichten des Auftragsverarbeiters

1. Verarbeitung nur nach dokumentierter Weisung (einschließlich Einhaltung der E2EE-Logik).
2. Verpflichtung der Mitarbeiter auf die Datengeheimnis und Vertraulichkeit.
3. Umsetzung der technischen und organisatorischen Maßnahmen (siehe Anlage).
4. Unterstützung des Verantwortlichen bei der Wahrung von Betroffenenrechten.

§ 5 Unterauftragsverhältnisse

1. Der Verantwortliche genehmigt den Einsatz der **Hetzner Online GmbH** (Rechenzentrum Deutschland) als Unterauftragsverarbeiter für das Hosting.
2. Weitere Unterauftragsverarbeiter sind dem Verantwortlichen anzuzeigen.

§ 6 Kontrollrechte

Der Verantwortliche ist berechtigt, die Einhaltung der Datenschutzvorschriften beim Auftragsverarbeiter in angemessenem Umfang zu prüfen (z.B. durch Selbstauskünfte oder Audits).

§ 7 Löschung und Rückgabe von Daten

Nach Beendigung des Auftrags löscht der Auftragsverarbeiter alle Daten. Da der Auftragsverarbeiter keine Klartext-Schlüssel besitzt, kann eine Datenrückgabe im Klartext technisch nicht erfolgen.

§ 8 Haftung und Schadenersatz

1. Die Parteien haften nach den Bestimmungen des Art. 82 DSGVO.
2. Für einfache Fahrlässigkeit ist die Haftung auf den typischerweise vorhersehbaren Schaden begrenzt.
3. **Haftungsausschluss bei Schlüsselverlust:** Da der Auftragsverarbeiter aufgrund der E2EE-Architektur keinen Zugriff auf die Praxis-Passphrase hat, trägt der Verantwortliche die alleinige Verantwortung für die Sicherung dieses Schlüssels. Der Auftragsverarbeiter haftet nicht für Datenverluste, die durch den Verlust der Passphrase durch den Verantwortlichen entstehen.

ANLAGE: Technische und Organisatorische Maßnahmen (TOMs)

1. Vertraulichkeit

- **Zutrittskontrolle:** Hosting bei Hetzner (ISO 27001 zertifiziert), physischer Schutz der Server.
- **Zugangskontrolle:** Authentifizierung via Username/Passwort (gehasht mit Argon2/BCrypt). TLS-Verschlüsselung (HTTPS).
- **Zugriffskontrolle:** Zero-Knowledge-Architektur. Patientendaten sind mit AES-256 verschlüsselt. Zugriff nur mit dem lokalen Key des Nutzers möglich.

2. Integrität

- **Weitergabekontrolle:** Alle Datenflüsse sind Ende-zu-Ende verschlüsselt.
- **Eingabekontrolle:** Protokollierung von Systemzugriffen (Logs werden 7 Tage vorgehalten).

3. Verfügbarkeit und Belastbarkeit

- **Verfügbarkeit:** Tägliche Backups der verschlüsselten Datenbanken bei Hetzner.
- **Wiederherstellbarkeit:** Getestete Backup-Restore-Prozesse.

4. Verfahren zur regelmäßigen Überprüfung

- Regelmäßige Security-Updates der Django-Applikation und Server-Umgebung.