

Technische und organisatorische Maßnahmen

Anlage 1 zum AVV – Kundenfassung

Stand: **20. September 2026** Fassung: **v1.0.10** Anbieterin: **Praxis-Clara GmbH, Berlin**

Anlage 1 zum Auftragsverarbeitungsvertrag. Die Maßnahmen wurden am Quellcode der Plattform verifiziert (Prüfstand 2026-08-04) und werden nach AVV § 13 Abs. 5 fortgeschrieben, ohne dass das Schutzniveau sinkt.

1. Zutritt, Zugang, Zugriff

- **Standort:** KI-Dienst, E-Mail-Versand und Fehler-Monitoring laufen auf eigener Hardware in abgeschlossenen Räumen auf umzäuntem Gelände in Rotenburg (Wümme), Deutschland; Zutritt nur für die Geschäftsführung der Betreiberin, USV, Brand- und Temperaturüberwachung, verschlüsselte Datenträger.
- **Anmeldung:** Benutzerkonten mit Passwort; Zwei-Faktor-Authentisierung (zeitbasierte Einmalkennwörter mit Wiederherstellungscodes) wird bereitgestellt und für Konten mit Zugriff auf Gesundheitsdaten dringend empfohlen; Ratenbegrenzung und Schutz der Anmeldeseiten vor automatisierten Zugriffen (Cloudflare Turnstile).
- **Rollen:** Rollenbasierte Zugriffskontrolle je Praxis (Inhaber, Beauftragte, Mitarbeitende); Freigaben nur durch berechtigte Rollen; administrative Zugänge der Betreiberin nur mit Mehrfaktor-Authentisierung und aufgabenbezogen.

2. Trennung, Verschlüsselung, Pseudonymisierung

- **Mandantentrennung:** Zeilenbasierte Zugriffsregeln (Row Level Security) auf allen Anwendungstabellen; jede Praxis sieht ausschließlich eigene Daten.
- **Transport:** TLS mit HSTS für alle Verbindungen; keine unverschlüsselten Übertragungen.
- **Ruhezustand:** Verschlüsselte Speicherung bei Datenbank- und Dateispeicher-Anbieter in der EU (Frankfurt am Main); keine Ende-zu-Ende-Verschlüsselung gegenüber der Betreiberin, dafür Zugriffsregeln und Protokollierung.
- **Audio:** Roh-Audio von Teambesprechungen wird abschnittsweise transkribiert und sofort verworfen, nie gespeichert; automatische Maskierung typischer patientenidentifizierender Muster im Transkript.

- **Protokolle:** IP-Adressen in Missbrauchsschutz-Zählern nur als schlüsselgebundener, gekürzter Hash; KI-Nutzungsprotokoll ohne Prompt- und Antwortinhalte; Fehler-Monitoring ohne Inhalte und Namen.

3. Integrität und Nachweis

- **Änderungsprotokoll:** Unveränderliches Protokoll regulatorisch relevanter Aktionen je Praxis.
- **Signaturen:** Einweisungs- und Besprechungssignaturen mit Zeitpunkt und technischen Begleitdaten, nachträglich nicht veränderbar.
- **Prüfbare Ausdrücke:** PDF-Exporte tragen eine serverseitige Prüfsumme, verifizierbar per QR-Code.
- **Human-in-the-Loop:** Kein Ergebnis eines Sprachmodells löst eine Aktion aus; Freigabe nur durch die Praxis.

4. Verfügbarkeit und Wiederherstellung

- **Sicherungen:** Rollierende Datenbanksicherungen beim Anbieter; Überschreibung mit Ablauf des Sicherungszyklus; Wiederherstellungsverfahren dokumentiert.
- **Betrieb:** Überwachung der geplanten Löschläufe und Dienste; Trennung von Produktiv- und Testsystem; Aktualisierung von Abhängigkeiten.

5. Löschung und Weisungsbindung

- **Löschläufe:** Automatisierte Löschung von Benachrichtigungen, geprüften Transkripten und Suchindex nach den Fristen der Datenschutzerklärung (Ziffer 4); Praxislöschung als Kaskade über alle Bestände einschließlich Dateispeicher und Zugangskonten 30 Tage nach Vormerkung.
- **Weisung:** Verarbeitung nur auf dokumentierte Weisung; persönliche Einsichtnahme durch den technischen Betrieb nur mit dokumentiertem Anlass und Weisung; Supportzugriffe werden protokolliert.
- **Unterauftragsverarbeiter:** Vertraglich zu gleichwertigen Pflichten verpflichtet (Anlage 2); Prüfung vor Beauftragung und in angemessenen Abständen.