— RECHTLICHES · ANNEX ZUR AVV

Technische und organisatorische Maßnahmen (TOM)

Stand: 21. Mai 2026 · Version 1.0 · Maßnahmen gemäß **Art. 32 DSGVO** zum Schutz personenbezogener Daten im Voice-Agent-Dienst. Dieses Dokument ist verbindlicher Annex zum Auftragsverarbeitungsvertrag in der jeweils zum Vertragsschluss gültigen Fassung.

Präambel und Geltungsbereich

Dieses Dokument beschreibt die technischen und organisatorischen Maßnahmen, mit denen **Lucid AI Labs** (Fabian Ilg, Markt Nittendorf) als Auftragsverarbeiter im Sinne von Art. 28 DSGVO ein dem Risiko angemessenes Schutzniveau gemäß **Art. 32 Abs. 1 DSGVO** gewährleistet. Geltungsbereich: der KI-Telefonagent-Dienst („Voice Agent") sowie alle dafür betriebenen Datenverarbeitungssysteme (Anwendung, Datenbank, Telefonie-Brücke, Klinik-Dashboard).

Die Maßnahmen werden mindestens einmal jährlich überprüft und nach Bedarf an den Stand der Technik, die Implementierungskosten und das konkrete Risikoprofil angepasst (Art. 32 Abs. 1 lit. d DSGVO). Wesentliche Änderungen werden den Verantwortlichen mit 30 Tagen Vorlauf in Textform mitgeteilt.

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

1.1 Pseudonymisierung und Verschlüsselung (lit. a)

- **Transport-Verschlüsselung:** Sämtlicher Datenverkehr zwischen Anrufer, Telefonie-Brücke, Anwendung, Datenbank und Klinik-Dashboard ist mit **TLS 1.3** (Mindestversion 1.2, alte Suiten deaktiviert) gesichert. HSTS mit `max-age=31536000; includeSubDomains; preload` ist auf allen öffentlichen Subdomains aktiv.
- **Datenbank-Verschlüsselung:** Transkripte, Termin-Datensätze und Klinik-Konfiguration liegen in **PostgreSQL auf Hetzner** (Falkenstein) mit voller Festplattenverschlüsselung (**LUKS / dm-crypt,**
- **
- **

nk-Backups werden zusätzlich

ntifizierungs-Token und
abellen** mit symmetrischer
h in der Frontend-Anwendung

n gegen rotierende
er, Eskalations-Status) liegen nach 12 Monaten ausschließlich anonymisiert vor.

1.2 Zutrittskontrolle (physischer Zutritt)

- Anwendungs- und Datenbank-Server stehen ausschließlich in den **Hetzner-Rechenzentren Falkenstein und Nürnberg**. Hetzner ist nach **ISO/IEC 27001** zertifiziert und betreibt Mehrfaktor-Zutrittskontrolle (Kartenleser, biometrische Identifizierung, 24/7-Bewachung, Videoüberwachung). Hetzner-Compliance-Nachweise: hetzner.com/de/unternehmen/zertifizierung.
- Lucid AI Labs hält **keine eigenen On-Premise-Server** mit Klinik-Daten. Entwicklungs-Laptops enthalten keine produktiven Patientendaten.

1.3 Zugangskontrolle (Systemzugang)

- **Multi-Faktor-Authentifizierung (MFA)** ist auf allen administrativen Konten zwingend: Hetzner Cloud Console, GitHub (Code), Vercel (Deployment), Supabase-Studio, Cloudflare (DNS/R2), E-Mail-Konten.
- **SSH-Zugriff** auf Produktionsserver ausschließlich über Ed25519-Schlüssel; Passwort-Login ist deaktiviert. SSH-Port nicht auf 22; `fail2ban` aktiv.
- **Klinik-Dashboard:** Anmeldung über Supabase-Auth mit erzwungener MFA für Praxis-Admin-Rollen. Sessions laufen nach 12 Stunden Inaktivität ab.
- **Datenbank-Direktzugriff** (Port 5432) ist firewall-gesperrt; Zugriff erfolgt ausschließlich über die Anwendungs-API oder, für Wartung, über einen `/pg/query`-Endpunkt mit Service-Role-Bearer-Token (Single-Token, in Postgres-Secrets gespeichert, rotierbar).

1.4 Zugriffskontrolle (Datenzugriff)

- **Mandantentrennung:** Jede Klinik ist ein separater Tenant. Klinik-spezifische Daten (Transkripte, Termine, Konfiguration) sind durch **Postgres Row-Level-Security (RLS)** getrennt. Eine Klinik kann unter keinen Umständen Daten einer anderen Klinik einsehen.
- **Least-Privilege-Prinzip:** Anwendungs-API-Rollen haben pro Endpunkt nur die minimal nötigen Rechte. Anonymer Zugriff ist auf öffentliche Endpunkte beschränkt; jede Datenoperation prüft die Klinik-ID gegen die Session.
- **Service-Role-Key** (umgeht RLS) wird ausschließlich aus dem Server-Backend genutzt; er ist *nicht* im Frontend-Bundle, niemals im Browser-Speicher und nicht im Git-Repository.
- A… …nzugriff, …`audit_log`-Tabelle mit …ewahrung: 24 Monate.

1.5 …ecken)

- …letzner) sind **auf getrennten** …n.
- …30 Abs. 2 DSGVO; die Daten sind logisch (Tenant-ID) und auf Anwendungsebene (RLS) getrennt.

- Produktion und Entwicklung sind **vollständig getrennte Umgebungen.** In der Entwicklungsdatenbank befinden sich ausschließlich synthetische Test-Daten; produktive Daten werden niemals in Entwicklungs- oder Staging-Umgebungen kopiert.

2. Integrität (Art. 32 Abs. 1 lit. b DSGVO)

2.1 Eingabekontrolle

- Jede schreibende Operation auf personenbezogenen Daten wird mit **Zeitstempel, Akteur (User-ID), Tenant-ID und Aktion** protokolliert.
- Änderungen an Klinik-Konfigurationen erzeugen Versionseinträge mit **Vorher-/Nachher-Werten**; eine Rollback-Funktion ist verfügbar.
- Sicherheitsrelevante Konfigurationen (z. B. Konfidenz-Schwelle für Eskalation, aktive Hard-Trigger-Listen) sind versioniert und nur durch autorisierte Admin-Rollen änderbar.

2.2 Weitergabekontrolle (Übermittlung an Unter-Auftragsverarbeiter)

- Die Liste der eingesetzten Unter-Auftragsverarbeiter ist unter /de/auftragsverarbeiter öffentlich einsehbar.
- Drittland-Übermittlungen erfolgen ausschließlich auf Grundlage von **EU-Standardvertragsklauseln (SCC, Modul 2)**, ergänzt durch Berufung auf den **EU-U.S. Data Privacy Framework** (Angemessenheitsbeschluss vom 10. Juli 2023), soweit der Empfänger DPF-zertifiziert ist.
- Für jeden US-Empfänger ist ein **Transfer Impact Assessment (TIA)** dokumentiert, das insbesondere FISA 702 und Executive Order 12333 adressiert (Schrems-II-Linie). Die TIAs sind auf Anforderung einsehbar.
- Vor Inbetriebnahme eines neuen Unter-Auftragsverarbeiters wird ein **30-Tage-Vorlauf** in Textform an alle aktiven Klinik-Verantwortlichen kommuniziert, einschließlich Widerspruchsrecht (siehe AVV § 4.4).

2.3 Schutz vor Manipulation (LLM-spezifisch)

- **System-Prompt-Constraints:** Das eingesetzte Sprachmodell ist instruiert, weder Diagnosen noch T… -Guardrails verbieten freie
- …herzen", „Atemnot", …g eine Eskalation an einen
- …nter 75 %, wird die Konversation …0,75).
- … Diagnose-/Triage-/Behandlungsempfehlungs-Intentionen mit Konfidenz ≥ 0,7 und unterdrückt jede

medizinisch-inhaltliche Antwort des Hauptmodells.

- **Prompt-Injection-Schutz:** Die Trennung zwischen Klinik-Konfiguration und Anrufer-Eingabe wird auf Anwendungsebene erzwungen; Anrufer können keine Klinik-Anweisungen überschreiben.

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

3.1 Verfügbarkeit

- **Anwendungs-Hosting:** Anwendung und Datenbank laufen auf einem dedizierten Hetzner-Server mit ECC-RAM und RAID-Speicher; SSL-Zertifikate werden automatisch über Let's Encrypt erneuert.
- **Telefonie-Verfügbarkeit:** Telnyx betreibt mehrere POPs; bei Ausfall einer Region wird automatisch umgeroutet.
- **Geplante Ziel-Verfügbarkeit:** 99,5 % pro Monat, gemessen am Voice-Agent-Endpunkt. Werte werden intern monatlich erhoben.
- **Monitoring:** Health-Endpunkte werden im 60-Sekunden-Takt geprüft; Alarmierung erfolgt per Push-Notification an den Verantwortlichen.

3.2 Belastbarkeit und Datenrettung

- **Datenbank-Backups:** Tägliche vollständige Snapshots (`pg_dump`); Aufbewahrung 7 Tage lokal auf dem Server.
- **Offsite-Replikation:** Verschlüsselte Backups werden täglich an einen separaten Speicher repliziert (Cloudflare R2, eu-central). Aufbewahrung 90 Tage; danach automatische Löschung.
- **Restore-Test:** Vollständiger Wiederherstellungs-Test (Backup → leere Datenbank → Anwendung läuft) wird quartalsweise dokumentiert ausgeführt. Letzte erfolgreiche Wiederherstellung dokumentiert: 16. Mai 2026.
- **Recovery-Ziele:** RPO (max. Datenverlust) ≤ 24 Stunden, RTO (Wiederherstellungszeit) ≤ 4 Stunden bei einem Hetzner-Hardwareausfall, ≤ 24 Stunden bei vollständigem Datacenter-Verlust.

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs

4.1

- Klinik-Verantwortlichen (siehe
form bestätigt.
- lichkeit verpflichtet,
- ch dokumentiert (Datum, Änderungen, Verantwortlicher).

4.2 Datenschutz-Folgenabschätzung (Art. 35 DSGVO)

- Eine vollständige **Datenschutz-Folgenabschätzung (DSFA)** für den Voice-Agent-Einsatz im Gesundheitswesen ist dokumentiert und wird der Klinik auf Anfrage zur Verfügung gestellt (E-Mail an Fabi@lucid-ai.app).
- Wesentliche Änderungen am System (neuer Sub-Prozessor, neue Datenkategorie, neuer Verarbeitungszweck) lösen eine DSFA-Aktualisierung aus.

4.3 Externe Audits

- Klinik-Verantwortliche können einmal pro Kalenderjahr ein Audit verlangen (AVV § 4.8). Vorlaufzeit: 30 Tage. Bei begründetem Verdacht (z. B. nach einer Datenpanne) jederzeit ohne Frist.
- Drittpartei-Audits (Penetration Tests, externe Code-Reviews) sind derzeit nicht zertifizierungspflichtig. Eine formale ISO/IEC 27001-Zertifizierung ist aktuell nicht in Vorbereitung; bei Bedarf eines Kunden wird sie gesondert geprüft.

5. Vorfallsmanagement (Art. 33, 34 DSGVO)

- **Kenntniserlangung:** Datenschutz-Vorfälle werden binnen 24 Stunden intern dokumentiert (Vorfall-ID, Zeitstempel, betroffene Daten, mögliche Ursache, Sofortmaßnahmen).
- **Meldung an Verantwortliche (Klinik):** Spätestens **48 Stunden** nach Kenntnis (AVV § 6). Die Meldung enthält Art des Vorfalls, Datenkategorien, Personenanzahl, wahrscheinliche Folgen, ergriffene Maßnahmen.
- **72-Stunden-Meldung an Aufsichtsbehörde** (Art. 33 Abs. 1 DSGVO): bleibt Pflicht des Verantwortlichen; Lucid AI Labs unterstützt mit allen erforderlichen Informationen.
- **Benachrichtigung Betroffener** (Art. 34 DSGVO): erfolgt durch den Verantwortlichen; Lucid AI Labs liefert Inhaltsentwürfe und betroffene Daten-Aufstellungen.
- **Lessons-Learned-Prozess:** Nach jedem Vorfall wird ein Post-Mortem-Dokument erstellt; entstandene Maßnahmen werden in das TOM-Update-Backlog überführt.

6. Aufbewahrung und Löschung

- ung, danach unwiederbringliche
  eb.
-
- pflicht; max. 10 Jahre nach
- tion ohne Personenbezug).
- ann unwiederbringliche Löschung.

- **Backup-Snapshots:** 90 Tage offsite, danach automatische Löschung. Nach Vertragsende: Live-Daten binnen 30 Tagen gelöscht, Backups binnen weiteren 90 Tagen.
- **Audit-Logs:** 24 Monate, danach Löschung (sicherheitsrelevante Vorfalls-Logs nach gesetzlicher Anforderung länger).

7. Beteiligte und Verantwortung

Lucid AI Labs ist derzeit ein **Solo-Engineer-Betrieb**. Der einzige Mitarbeiter (Fabian Ilg) ist gleichzeitig Verantwortlicher, technischer Betreiber, Sicherheitsbeauftragter und erster Eskalationspunkt für Datenschutz-Anliegen. Diese Konstellation wird transparent kommuniziert und ist Teil des Risikoprofils der Klinik. Vor dem Onboarding der ersten zahlenden Klinik wird ein externer Datenschutzbeauftragter bestellt; bis dahin werden Datenschutz-Anliegen direkt vom Verantwortlichen bearbeitet (siehe Datenschutzerklärung § 1).

Die **Berufshaftpflichtversicherung** (Hiscox IT, 500.000 € Versicherungssumme) deckt IT-Risiken einschließlich Datenschutzpannen ab. Geltungsbereich Bundesrepublik Deutschland, mit EU-Erweiterung gemäß Police.

8. Hetzner-Compliance-Kontext

Der Hosting-Anbieter **Hetzner Online GmbH** (Industriestr. 25, 91710 Gunzenhausen) ist nach **ISO/IEC 27001:2022** zertifiziert und erfüllt den deutschen IT-Grundschutz nach BSI-Standards. Rechenzentren in Falkenstein und Nürnberg sind ISO-zertifiziert. Hetzner-AVV: hetzner.com/AV. Compliance-Übersicht: hetzner.com/de/unternehmen/zertifizierung.

Hetzner ist ausschließlich für die **Infrastruktur-Sicherheit** verantwortlich (Stromversorgung, Kühlung, physische Sicherheit, Netzwerk-Anbindung). Anwendungs-Sicherheit, Datenbank-Konfiguration und Code-Qualität liegen vollständig in der Verantwortung von Lucid AI Labs.

9. Anwendungsspezifische Klinik-Konfiguration

Pro Klinik werden folgende Sicherheitsparameter im Onboarding festgelegt und nur durch autorisierte Praxis-Admins änderbar:

-
-
- rbar 7 – 365 Tage)
-
- vorgegeben, klinik-spezifisch

10. Patientenkommunikation und Aushänge

Vorlagen für Praxis-Aushänge, Telefon-Ansage und Datenschutz-Snippet (zur Aufnahme in die Klinik-Datenschutzerklärung) werden mit dem Onboarding-Paket bereitgestellt. Inhalt: Hinweis auf KI-Telefon-Assistent, betroffene Datenkategorien, Eskalation an Menschen, Drittlandübermittlung auf SCC+DPF-Basis, Betroffenenrechte.

11. Änderungshistorie

- **Version 1.0, 21. Mai 2026:** Erstveröffentlichung als verbindlicher Annex zur AVV v1.1.

Verwandte Dokumente

- Auftragsverarbeitungsvertrag (AVV)
- Liste der Unter-Auftragsverarbeiter
- Datenschutzerklärung
- Datenschutz-FAQ für Klinik-Inhaber (Klartext)
- Impressum
- English version (Technical and Organisational Measures)