— LEGAL · ANNEX TO THE DPA

Technical and Organisational Measures (TOM)

This is an English translation provided for convenience. The legally binding version of this document is the German original (German original). In case of any discrepancy, the German version prevails.

As of: 21 May 2026 · Version 1.0 · Measures pursuant to **Art. 32 GDPR** for the protection of personal data in the voice agent service. This document is a binding annex to the Data Processing Agreement in the version effective at the time of contract conclusion.

Preamble and Scope

This document describes the technical and organisational measures with which **Lucid AI Labs** (Fabian Ilg, Markt Nittendorf, Germany), as a processor within the meaning of Art. 28 GDPR, ensures a level of protection appropriate to the risk pursuant to **Art. 32 para. 1 GDPR**. Scope: the AI telephone agent service ("Voice Agent") and all data-processing systems operated for it (application, database, telephony bridge, clinic dashboard).

The measures are reviewed at least annually and adjusted as needed to the state of the art, implementation costs and the specific risk profile (Art. 32 para. 1 lit. d GDPR). Material changes are communicated to controllers 30 days in advance in text form.

1. Confidentiality (Art. 32 para. 1 lit. b GDPR)

1.1 Pseudonymisation and Encryption (lit. a)

- **Transport encryption:** All data traffic between caller, telephony bridge, application, database and clinic dashboard is secured with **TLS 1.3** (minimum version 1.2, legacy suites disabled). HSTS with `max-age=31536000; includeSubDomains; preload` is active on all public subdomains.
- **Database encryption:** Transcripts, appointment records and clinic configuration reside in **PostgreSQL on Hetzner** (Falkenstein) with full disk encryption (**LUKS / dm-crypt, AES-256-XTS**) on
- d external provider keys are
- th rotating pseudonym keys.

e only in anonymised form after 12 months.

1.2 Physical Access Control

- Application and database servers are located exclusively in the **Hetzner data centres in Falkenstein and Nuremberg, Germany**. Hetzner is certified to **ISO/IEC 27001** and operates multi-factor physical access control (card readers, biometric identification, 24/7 security, video surveillance). Hetzner compliance: hetzner.com/unternehmen/zertifizierung.
- Lucid AI Labs operates **no on-premise servers** containing clinic data. Development laptops contain no production patient data.

1.3 System Access Control

- **Multi-factor authentication (MFA)** is enforced on all administrative accounts: Hetzner Cloud Console, GitHub (code), Vercel (deployment), Supabase Studio, Cloudflare (DNS/R2), email accounts.
- **SSH access** to production servers exclusively via Ed25519 keys; password login is disabled. SSH port not on 22; `fail2ban` active.
- **Clinic dashboard:** Login via Supabase Auth with enforced MFA for practice admin roles. Sessions expire after 12 hours of inactivity.
- **Database direct access** (port 5432) is firewalled off; access is exclusively via the application API or, for maintenance, via a `/pg/query` endpoint with a service-role bearer token (single token, stored in Postgres secrets, rotatable).

1.4 Data Access Control

- **Tenant separation:** Every clinic is a separate tenant. Clinic-specific data (transcripts, appointments, configuration) is separated by **Postgres Row-Level Security (RLS)**. Under no circumstances can one clinic see another clinic's data.
- **Least-privilege principle:** Application API roles hold only the minimum rights necessary per endpoint. Anonymous access is limited to public endpoints; every data operation checks the clinic ID against the session.
- **Service-role key** (bypasses RLS) is used exclusively from the server backend; it is *not* in the frontend bundle, never in browser storage, and not in the Git repository.
- **Audit logging:** Security-relevant operations (sign-in, data access, configuration change, data export) are documented in a separate `audit_log` table with immutable append-only write mode.

1.5

- r) are operated on **separate**
- nt to Art. 30 para. 2 GDPR; data

- Production and development are **fully separated environments**. The development database contains exclusively synthetic test data; production data is never copied into development or staging environments.

2. Integrity (Art. 32 para. 1 lit. b GDPR)

2.1 Input Control

- Every write operation on personal data is logged with **timestamp, actor (user ID), tenant ID, and action**.
- Changes to clinic configurations create version entries with **before/after values**; a rollback function is available.
- Security-relevant configurations (e. g. confidence threshold for escalation, active hard-trigger lists) are versioned and only modifiable by authorised admin roles.

2.2 Transfer Control (transmission to sub-processors)

- The list of engaged sub-processors is publicly available at /sub-processors.
- Third-country transfers take place exclusively on the basis of **EU Standard Contractual Clauses (SCC, Module 2)**, supplemented by reliance on the **EU-U.S. Data Privacy Framework** (adequacy decision of 10 July 2023), insofar as the recipient is DPF-certified.
- For each US recipient, a **Transfer Impact Assessment (TIA)** is documented, addressing in particular FISA 702 and Executive Order 12333 (Schrems II line). The TIAs are available for inspection on request.
- Before bringing a new sub-processor into service, a **30-day advance notice** in text form is communicated to all active clinic controllers, including the right of objection (see DPA § 4.4).

2.3 Protection Against Manipulation (LLM-specific)

- **System-prompt constraints:** The deployed language model is instructed to give neither diagnoses, triage nor treatment recommendations; anti-hallucination guardrails prohibit free medical statements.
- **Hard-trigger list:** Emergency and diagnosis terms (e. g. "chest pain", "shortness of breath", …on trigger an escalation to a
- …below 75 %, the conversation is
- …e/treatment-recommendation …esponse from the main model.

- **Prompt-injection protection:** The separation between clinic configuration and caller input is enforced at the application layer; callers cannot override clinic instructions.

3. Availability and Resilience (Art. 32 para. 1 lit. b GDPR)

3.1 Availability

- **Application hosting:** Application and database run on a dedicated Hetzner server with ECC RAM and RAID storage; SSL certificates are renewed automatically via Let's Encrypt.
- **Telephony availability:** Telnyx operates multiple POPs; in the event of a regional outage, traffic is automatically rerouted.
- **Planned target availability:** 99.5 % per month, measured at the voice agent endpoint. Values are recorded internally monthly.
- **Monitoring:** Health endpoints are checked at 60-second intervals; alerts are sent via push notification to the controller.

3.2 Resilience and Data Recovery

- **Database backups:** Daily full snapshots (`pg_dump`); retention 7 days locally on the server.
- **Offsite replication:** Encrypted backups are replicated daily to a separate store (Cloudflare R2, eu-central). Retention 90 days; automatic deletion thereafter.
- **Restore test:** A full restore test (backup → empty database → application running) is documented and performed quarterly. Last successful restore documented: 16 May 2026.
- **Recovery objectives:** RPO (maximum data loss) ≤ 24 hours, RTO (recovery time) ≤ 4 hours for a Hetzner hardware failure, ≤ 24 hours for a complete data centre loss.

4. Procedures for Regular Review, Assessment and Evaluation (Art. 32 para. 1 lit. d GDPR)

4.1 Processing Control

- Processing takes place exclusively on **documented instructions** from clinic controllers (see DPA
- **identiality**, including § 203
- n writing (date, changes,

4.2 Data Protection Impact Assessment (Art. 35 GDPR)

- A full **data protection impact assessment (DPIA)** for the use of the voice agent in healthcare is documented and made available to the clinic on request (email to Fabi@lucid-ai.app).
- Material changes to the system (new sub-processor, new data category, new processing purpose) trigger a DPIA update.

4.3 External Audits

- Clinic controllers may request one audit per calendar year (DPA § 4.8). Lead time: 30 days. In the case of substantiated suspicion (e. g. after a data breach), at any time without a notice period.
- Third-party audits (penetration tests, external code reviews) are not currently subject to certification requirements. A formal ISO/IEC 27001 certification is not currently in preparation; if a customer requires one, this will be assessed separately.

5. Incident Management (Art. 33, 34 GDPR)

- **Awareness:** Data protection incidents are documented internally within 24 hours (incident ID, timestamp, affected data, likely cause, immediate measures).
- **Notification to controllers (clinic):** At the latest **48 hours** after awareness (DPA § 6). The notification contains the nature of the incident, data categories, number of persons, likely consequences, measures taken.
- **72-hour notification to the supervisory authority** (Art. 33 para. 1 GDPR): remains the obligation of the controller; Lucid AI Labs supports with all required information.
- **Notification of data subjects** (Art. 34 GDPR): performed by the controller; Lucid AI Labs provides content drafts and statements of affected data.
- **Lessons-learned process:** After every incident, a post-mortem document is created; resulting measures are transferred to the TOM update backlog.

6. Retention and Deletion

- **Live audio stream:** transient (streaming), max. 60 seconds of buffering, then irretrievable deletion. No permanent audio recording in standard operation.
-
- gation; max. 10 years under
- with no personal reference).
- ievable deletion.
- fter contract termination: live data deleted within 30 days, backups within a further 90 days.

- **Audit logs:** 24 months, then deletion (security-relevant incident logs retained longer per statutory requirement).

7. Personnel and Responsibility

Lucid AI Labs is currently a **solo-engineer operation**. The sole employee (Fabian Ilg) is simultaneously controller, technical operator, security officer and first escalation point for data protection matters. This constellation is communicated transparently and is part of the clinic's risk profile. Before onboarding the first paying clinic, an external data protection officer (DSB) is appointed; until then, data protection matters are handled directly by the controller (see Privacy Policy § 1).

The **professional liability insurance** (Hiscox IT, 500,000 € insured sum) covers IT risks including data protection incidents. Scope: Federal Republic of Germany, with EU extension per policy.

8. Hetzner Compliance Context

The hosting provider **Hetzner Online GmbH** (Industriestr. 25, 91710 Gunzenhausen, Germany) is certified to **ISO/IEC 27001:2022** and meets the German IT-Grundschutz (BSI) standards. Data centres in Falkenstein and Nuremberg are ISO-certified. Hetzner DPA: hetzner.com/AV. Compliance overview: hetzner.com/unternehmen/zertifizierung.

Hetzner is responsible exclusively for **infrastructure security** (power, cooling, physical security, network connectivity). Application security, database configuration and code quality are entirely the responsibility of Lucid AI Labs.

9. Application-Specific Clinic Configuration

Per clinic, the following security parameters are agreed during onboarding and only modifiable by authorised practice admins:

- Confidence threshold for escalation (default: 0.75)
- Optional audio recording (default: off)
- Transcript retention period (default: 90 days, configurable 7 – 365 days)
- Emergency escalation path (practice hotline phone number for escalation)
- ded, clinic-specific extension

10.

Tem snippet (for inclusion in the clin nt: notice of AI telephone

assistant, affected data categories, escalation to humans, third-country transfer on SCC + DPF basis, data subject rights.

11. Change History

- **Version 1.0, 21 May 2026:** Initial publication as a binding annex to DPA v1.1.

Related Documents

- Data Processing Agreement (DPA)
- List of Sub-Processors
- Privacy Policy
- Privacy FAQ for Clinic Owners (plain language)
- Imprint
- Deutsche Fassung (Technische und organisatorische Maßnahmen)