— LEGAL

Data Processing Agreement (DPA)

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: 12 May 2026 · Version 1.1 · Agreement on the processing of personal data on behalf of the controller pursuant to **Art. 28 GDPR**. This version is the public master version. The variant signed for each clinic is sent with the Annex "Sub-Processors" and the agreed TOM.

Preamble

This agreement governs the processing of personal data by **Lucid AI Labs** (hereinafter "**Processor**") on behalf of the contracting clinic (hereinafter "**Controller**") within the scope of the voice agent service ("Voice Agent"). It forms the legal basis pursuant to **Art. 28 para. 3 GDPR** for any operational data processing within the scope of the main service.

In case of doubt, this DPA takes precedence over the main contract insofar as data protection is concerned.

1. Definitions

The terms of the **GDPR** (Regulation (EU) 2016/679) apply, in particular Art. 4 No. 1 (personal data), No. 2 (processing), No. 7 (controller), No. 8 (processor), No. 12 (data breach) and No. 15 (health data in conjunction with Art. 9 para. 1).

2. Subject Matter, Nature and Purpose of the Processing

- **Subject matter:** Operation of an AI-supported telephone reception agent for the clinic. Functions: answering incoming calls, transcription of the spoken word, answering frequent questions, scheduling and rescheduling of appointments, escalation to a human in the event of uncertainty or e
- permitted), storage (transcripts etion.
- quality, ensuring the escalation ent documentation).
- ically with the main contract.

3. Type of Personal Data and Categories of Data Subjects

Categories of data subjects:

- Patients of the clinic (callers)
- Accompanying persons (e. g. parents, caregivers, legal representatives)
- Clinic staff (in the case of escalation and call-back)

Data categories (Art. 4 No. 1 GDPR):

- Master data: name, date of birth, insurance number (insofar as provided by the caller)
- Contact data: telephone number, email (insofar as provided by the caller)
- Voice audio data (transient, see § 10) and transcripts of the conversation
- Appointment data: requested appointment, concern category
- Metadata: timestamp, call duration, escalation status

Special categories of data (Art. 9 para. 1 GDPR): Health data to the extent that callers voluntarily disclose it in the conversation (e. g. "I have pain in my molar tooth"). Lawful basis: **Art. 9 para. 2 lit. h GDPR** (processing for healthcare provision within the scope of a treatment contract). The clinic, as a healthcare institution, is a professional secrecy holder within the meaning of **§ 203 StGB**.

4. Obligations of the Processor (Art. 28 para. 3 GDPR)

The Processor undertakes pursuant to **Art. 28 para. 3 GDPR** in particular the following (§§ 4.1–4.8 correspond to the minimum elements lit. a–h):

4.1 Processing Only on Instruction (lit. a)

The Processor processes personal data exclusively on documented instruction of the Controller, including with regard to transfers to third countries (cf. § 9). If it is obliged to process by Union or Member State law, it informs the Controller of these legal requirements before the processing, unless the law in question prohibits such information on important grounds of public interest. Verbal instructions are confirmed in writing (including by email) without undue delay.

4.2 C

The …nal data have committed ther… …ecrecy. This applies in part…

4.3

The …es pursuant to **Art. 32 GDPR**. These are concretely set out in the Annex "Technical and Organisational Measures (TOM)" and cover at

least: pseudonymisation and encryption (TLS 1.3 in transit, AES-256 at rest), availability and resilience (Hetzner hosting in Falkenstein/Nuremberg), procedures for regular review, access control (least privilege, audit logging).

4.4 Sub-Processors (lit. d in conjunction with Art. 28 para. 2 GDPR)

The Controller grants the Processor **general written authorisation pursuant to Art. 28 para. 2 sentence 2 GDPR** for the engagement of the sub-processors listed in Annex A (List of Sub-Processors). The **Annex A list in the version at the time of conclusion of the contract** is separately approved by the clinic during onboarding (clickwrap confirmation with timestamp); the authorisation relates specifically to this snapshot version. The website version serves as an ongoing reference. In the case of engagement of further sub-processors or replacement of existing ones, the Processor informs the Controller at least **30 days in advance** in text form and thereby gives it the opportunity to object to this change.

In the event of objection by the Controller, the parties negotiate in good faith on a solution. If no agreement can be reached within 14 days, either party may terminate the main contract without observing a notice period.

The Processor obligates every sub-processor to the same data protection obligations as in this DPA, in particular with regard to sufficient guarantees pursuant to Art. 32 GDPR.

4.5 Support with Data Subject Rights (lit. e)

The Processor supports the Controller, taking into account the nature of the processing, with appropriate technical and organisational measures in the fulfilment of the requests of data subjects pursuant to Chapter III GDPR (Art. 15 access, Art. 16 rectification, Art. 17 erasure, Art. 18 restriction, Art. 20 data portability, Art. 21 objection). Requests to the Processor are forwarded to the Controller within **5 working days**.

4.6 Support with Compliance Obligations (lit. f)

The Processor supports the Controller, taking into account the nature of the processing and the information available to it, in the compliance with the obligations pursuant to **Art. 32 to 36 GDPR**, in particular with data protection impact assessments (Art. 35) and consultations with the supervisory authority (Art. 36).

4.7

Afte ne Controller, deletes all
pers exist. The deletion is confirmed
in te 30 days for live data, **90 days**
for l

4.8 Demonstration and Audit (lit. h)

The Processor makes available to the Controller all information necessary to demonstrate compliance with the obligations laid down in this DPA. It enables and supports reviews by the Controller or an auditor mandated by the Controller (audits, inspections). The Controller may request one audit per calendar year with a notice period of **30 days**; further audits in the case of substantiated suspicion (e. g. after a data breach) at any time without a notice period.

Should an instruction of the Controller in the opinion of the Processor infringe the GDPR or other data protection provisions, it informs the Controller without undue delay (Art. 28 para. 3 sentence 3 GDPR).

5. Obligations of the Controller

- **Lawfulness:** The Controller ensures that the processing takes place on a valid lawful basis pursuant to Art. 6 and Art. 9 GDPR and that callers are properly informed (Art. 13/14 GDPR).
- **AI announcement:** The Controller confirms that the AI announcement laid down in § 10.1 is played at the beginning of every call and that the use of the Voice Agent is referred to in its privacy policy as well as on its website.
- **§ 203 StGB:** The Controller is identified as a professional secrecy holder and hereby expressly authorises the engagement of the Processor and the sub-processors named in the Annex (see § 10.2).
- **Notification of incidents:** The Controller reports its own relevant incidents (e. g. compromised clinic end devices) to the Processor, insofar as these have effects on the subject matter of the contract.
- **Contact person:** The Controller names a contactable person for data protection questions.

6. Data Security Incidents (Art. 33, 34 GDPR)

The Processor informs the Controller without undue delay, at the latest **within 48 hours** of becoming aware, of any breach of the protection of personal data (Art. 33 para. 2 GDPR). The notification contains at minimum: description of the nature of the breach, affected data categories and number of persons, likely consequences, measures taken or proposed.

The **72-hour notification obligation to the supervisory authority** (Art. 33 para. 1 GDPR) remains an obligation of the Controller.

7. T

The tely in Annex A (encryption, phy ilability, resilience, processing con the TOM, provided that the prot o the Controller.

8. Processing Locations and Data Residency

Primary data storage (transcripts, metadata, application database) takes place in the **European Union** on servers of **Hetzner Online GmbH** (Falkenstein and Nuremberg, Germany). Certain sub-processors (speech synthesis, speech-to-text, telephony, LLM) process data in the USA or other third countries; see § 9 and Annex "Sub-Processors".

9. Third-Country Transfers

Insofar as processing takes place in third countries, the Processor ensures an adequate level of protection pursuant to **Chapter V GDPR (Art. 44–49)**:

- **Standard contractual clauses (SCC)** of the European Commission pursuant to Implementing Decision (EU) 2021/914 with all modules 2 (controller → processor) and, where applicable, 3 (processor → processor)
- **Transfer Impact Assessment (TIA)** for each US recipient with regard to FISA 702 / Executive Order 12333 (Schrems II line)
- Insofar as the recipient is certified under the **EU-U.S. Data Privacy Framework (DPF)** (e. g. Telnyx, Resend, Microsoft, Vercel, Anthropic), additionally reliance on the adequacy decision of 10 July 2023.

10. Voice-Agent-Specific Clauses

10.1 AI Announcement at Call Start (AI Act Art. 50)

The Processor plays at the beginning of every call a clear, distinctly intelligible notice that the caller is interacting with an AI system (example: "You are speaking with the AI telephone assistant of the practice Dr. X. If you would prefer to speak with a human, simply say 'human'"). This obligation arises from **Art. 50 AI Regulation (EU) 2024/1689**; the applicability is dated to 2 August 2026. Lucid AI Labs fulfils this obligation *ahead of schedule* from the start of the contract.

10.2 Professional Secrecy (§ 203 StGB)

By signing this DPA, the Controller expressly authorises the Processor as well as all sub-processors nam **nd 4 StGB**. The assisting persons are ligations. The Processor only dep statutory obligation of secrecy.

Dut sation as "assisting persons" purs ection information of patients purs rvice (incl. the sub-processors with s, before making use of the prac ception service, (ii) the data

flows including third-country transfer on the basis of SCC + DPF, and (iii) their data subject rights (Art. 15–22 GDPR). The Processor provides templates for this (practice notice, privacy policy snippet, telephone announcement).

10.3 Recording (§ 201 StGB)

Default: *No* permanent audio recording takes place. Voice data is processed transiently (streaming) and deleted within 60 seconds after generation of the transcript. Transcripts are stored.

Optional recording: Insofar as the Controller explicitly commissions an additional audio recording in the main contract (e. g. for quality assurance), an additional notice is played at the beginning of every call ("This call is recorded for quality assurance. If you do not agree with this, please say 'no recording'"). In the event of objection, the recording is immediately and verifiably deactivated. A recording without notice and possibility of consent does not take place under any circumstances, as this would constitute a violation of **§ 201 StGB**.

Consent documentation (verifiability): If the recording is activated, the Processor documents per call: (a) call ID, (b) timestamp of the playing of the notice, (c) caller reaction (silence / explicit consent / objection) with timestamp, (d) recording status (started / prevented). Upon the objection word ("no", "do not record", "no recording") or upon detection of an objection by the soft classifier, the recording is stopped within 1 second and the previous audio buffer is irretrievably deleted. The consent logs are retained for the duration of the recording storage period (see § 11) and are to be presented to the Controller on request.

10.4 Functional Limitation (High-Risk AI Avoidance)

The Voice Agent **provides no diagnosis**, performs **no triage** and gives **no medical assessments**. For any substantive medical concern, an escalation to a human takes place. This functional limitation avoids a classification as a high-risk AI system pursuant to Annex III of the AI Regulation.

The functional limitation is implemented technically through the following safeguards:

- **Hard-trigger list** of medical diagnosis/triage/emergency terms (e. g. "chest pain", "heart attack", "shortness of breath", "unconsciousness"), upon detection of which in the live transcript the escalation is triggered immediately and without further model evaluation (spec: `docs/voice-agent-notruf-spec.md`).
- **Confidence threshold:** in the case of model uncertainty below 75 %, the conversation is
- nts, which at a confidence of
  edical-content response of the
- no diagnosis, triage or therapy
  statements.

- **Quarterly tests** with synthetic emergency and diagnosis dialogues, the results of which are internally logged; anomalies trigger a retraining of the trigger list or an adjustment of the soft classifier.

10.5 Escalation

The Processor ensures that an escalation to a human is possible at any time and that this takes place at the latest when (a) the caller expressly requests this, (b) the confidence level of the model falls below the agreed threshold (default: 75 %), or (c) a substantive medical concern is detected.

11. Storage Duration

- Live audio stream: transient, max. 60 seconds buffering, then deleted.
- Transcript of the conversation: 90 days (default); configurable per clinic specification.
- Appointment record (name, date, concern category): until lapse of the clinic-internal retention obligation; max. 10 years according to treatment-law retention periods.
- Call metadata (timestamp, duration, escalation status): 12 months, then anonymised.
- Optional audio recording (insofar as explicitly activated): 30 days, then irretrievably deleted.

12. Liability

The liability of the parties follows the main contract and, additionally, **Art. 82 GDPR**. In the case of breaches of duty that are attributable exclusively to fault of the Controller (e. g. insufficient own privacy policy), the liability of the Processor lapses. A professional liability insurance exists (Hiscox IT, 500,000 € insured sum).

13. Termination

This DPA ends with the main contract. A separate termination is not required. § 4.7 (return / deletion) applies independently of the reason for termination.

14. Final Provisions

- verability clause: should a
- er within the meaning of § 13 / Amtsgericht Regensburg).
- ial changes are communicated

Annex A: Sub-Processors

Complete current list: /sub-processors. Excerpt as of 28 April 2026:

- **Hetzner Online GmbH** (Industriestr. 25, 91710 Gunzenhausen, DE): Hosting of the application DB and transcripts. Data residency: Falkenstein/Nuremberg/Helsinki. No third-country transfer. DPA: hetzner.com/AV.
- **Vercel Inc.** (340 S Lemon Ave #4133, Walnut, CA 91789, USA): Hosting of the marketing and clinic dashboard interface. Third-country transfer to the USA, safeguarded by SCC + DPF. DPA: vercel.com/legal/data-processing-addendum.
- **Anthropic PBC** (548 Market St PMB 90375, San Francisco, CA 94104, USA): Speech processing (LLM for conversation and appointment logic). API mode: no use of the data for training purposes (Commercial Terms). SCC + DPF. DPA: anthropic.com/legal/commercial-terms.
- **Deepgram Inc.** (1438 Webster St STE 100, Oakland, CA 94612, USA): Speech-to-text (STT). SCC. DPA: deepgram.com/legal.
- **ElevenLabs Inc.** (228 Park Ave S PMB 30661, New York, NY 10003, USA): Speech synthesis (TTS). SCC. DPA: elevenlabs.io/dpa.
- **Telnyx LLC** (311 W Superior Street, Suite 504, Chicago, IL 60654, USA): Telephony (SIP trunk, call answering, routing, German geo telephone numbers). SCC + EU-U.S. DPF. EU representative: Telnyx Ireland Limited (Dublin). DPA: telnyx.com/legal/data-processing-addendum.
- **Resend Inc.** (San Francisco, CA, USA): Transactional email (appointment confirmations). SCC + DPF. DPA: resend.com/legal/dpa.

Acceptance

Upon clicking "I accept the DPA" in the onboarding portal or by conclusive conduct (commencement of use of the voice agent service), this agreement enters into force. The acceptance record (user ID, timestamp, IP address, DPA version) is stored in the table `avv_acceptances` (Art. 28 para. 9 GDPR fulfilled, electronic form). The signature-ready PDF is available via the download button at the top; for a clinic-specific filled-in variant (Annex A snapshot, agreed TOM adjustments), write to Fabi@lucid-ai.app.

Related Documents

- Deutsche Fassung (AVV)