

Auftragsverarbeitungsvertrag (AVV)

Stand: 12. Mai 2026 · Version 1.1 · Vertrag zur Verarbeitung personenbezogener Daten im Auftrag gemäß **Art. 28 DSGVO**. Diese Fassung ist die öffentliche Master-Version. Die für jede Klinik signierte Variante wird mit dem Annex „Unter-Auftragsverarbeiter“ und den vereinbarten TOM versendet.

Präambel

Dieser Vertrag regelt die Verarbeitung personenbezogener Daten durch die **Lucid AI Labs** (nachstehend „**Auftragsverarbeiter**“) im Auftrag der vertragsschließenden Klinik (nachstehend „**Verantwortlicher**“) im Rahmen des Sprach-Agent-Dienstes („Voice Agent“). Er bildet die rechtliche Grundlage gemäß **Art. 28 Abs. 3 DSGVO** für jede operative Datenverarbeitung im Rahmen der Hauptleistung.

Im Zweifel hat dieser AVV Vorrang vor dem Hauptvertrag, soweit es um den Datenschutz geht.

1. Begriffsbestimmungen

Es gelten die Begriffe der **DSGVO** (Verordnung (EU) 2016/679), insbesondere Art. 4 Nr. 1 (personenbezogene Daten), Nr. 2 (Verarbeitung), Nr. 7 (Verantwortlicher), Nr. 8 (Auftragsverarbeiter), Nr. 12 (Datenpanne) und Nr. 15 (Gesundheitsdaten i. V. m. Art. 9 Abs. 1).

2. Gegenstand, Art und Zweck der Verarbeitung

- **Gegenstand:** Betrieb eines KI-gestützten Telefon-Empfangsagenten für die Klinik. Funktionen: Annahme eingehender Anrufe, Transkription des gesprochenen Wortes, Beantwortung häufiger Fragen, Vereinbarung und Verlegung von Terminen, Eskalation an einen Menschen bei Unsicherheit oder explizitem Patientenwunsch.
- **Art der Verarbeitung:** Erheben, Aufzeichnen (sofern explizit gestattet), Speichern (Transkripte und Metadaten), Übermitteln (an Unter-Auftragsverarbeiter zur Verarbeitung), Löschen.

Cookie-Einstellungen

Wir nutzen Microsoft Clarity für anonyme Heatmaps. Keine personenbezogenen Daten, keine Drittanbieter-Tracker.

[Datenschutzerklärung](#)

Akzeptieren

Ablehnen

Anpassen →

3. A

Kat

• F

ität, Sicherstellung der
rmin-Dokumentation).

atisch mit dem Hauptvertrag.

roffener Personen

- Begleitpersonen (z. B. Eltern, Pflegekräfte, gesetzliche Vertreter)
- Mitarbeitende der Klinik (bei Eskalation und Rückruf)

Datenkategorien (Art. 4 Nr. 1 DSGVO):

- Stammdaten: Name, Geburtsdatum, Versichertennummer (sofern vom Anrufer angegeben)
- Kontaktdaten: Telefonnummer, E-Mail (sofern vom Anrufer angegeben)
- Sprach-Audiodaten (transient, siehe § 10) und Transkripte des Gesprächs
- Termindaten: gewünschter Termin, Anliegen-Kategorie
- Metadaten: Zeitstempel, Anrufdauer, Eskalations-Status

Besondere Datenkategorien (Art. 9 Abs. 1 DSGVO): Gesundheitsdaten in dem Umfang, den Anrufer im Gespräch freiwillig offenlegen (z. B. „Ich habe Schmerzen am Backenzahn“). Rechtsgrundlage: **Art. 9 Abs. 2 lit. h DSGVO** (Verarbeitung zur Gesundheitsversorgung im Rahmen eines Behandlungsvertrags). Die Klinik ist als gesundheitsversorgende Einrichtung Berufsgeheimnisträger im Sinne von **§ 203 StGB**.

4. Pflichten des Auftragsverarbeiters (Art. 28 Abs. 3 DSGVO)

Der Auftragsverarbeiter verpflichtet sich gemäß **Art. 28 Abs. 3 DSGVO** insbesondere zu Folgendem (§§ 4.1–4.8 entsprechen den Mindestelementen lit. a–h):

4.1 Verarbeitung nur nach Weisung (lit. a)

Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisung des Verantwortlichen, einschließlich hinsichtlich Übermittlungen in Drittländer (vgl. § 9). Sollte er aufgrund Unions- oder mitgliedstaatlichen Rechts zur Verarbeitung verpflichtet sein, teilt er dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht aus wichtigen Gründen des öffentlichen Interesses verbietet. Mündliche Weisungen werden unverzüglich schriftlich (auch per E-Mail) bestätigt.

4.2 Verpflichtung zur Vertraulichkeit (lit. b)

Der Auftragsverarbeiter stellt sicher, dass alle zur Verarbeitung der personenbezogenen Daten befugten Personen sich zur Vertraulichkeit verpflichtet haben oder einer gesetzlichen

Ger
mit

Cookie-Einstellungen

Wir nutzen Microsoft Clarity für anonyme Heatmaps. Keine personenbezogenen Daten, keine Drittanbieter-Tracker.

[Datenschutzerklärung](#)

4.3

Der
Art.
fest
AES

auf **§ 203 Abs. 4 StGB** für

satorischen Maßnahmen gemäß
Maßnahmen (TOM)" konkret
chlüsselung (TLS 1.3 in transit,
alkenstein/Nürnberg),

Verfahren zur regelmäßigen Überprüfung, Zugriffskontrolle (least privilege, Audit-Logging).

4.4 Unter-Auftragsverarbeiter (lit. d i. V. m. Art. 28 Abs. 2 DSGVO)

Der Verantwortliche erteilt dem Auftragsverarbeiter **allgemeine schriftliche Genehmigung gemäß Art. 28 Abs. 2 Satz 2 DSGVO** zur Hinzuziehung der im Annex A (Liste der Unter-Auftragsverarbeiter) aufgeführten Unter-Auftragsverarbeiter. Die **Annex-A-Liste in der Fassung zum Zeitpunkt des Vertragsschlusses** wird der Klinik beim Onboarding gesondert (Klickwrap-Bestätigung mit Zeitstempel) genehmigt; die Genehmigung bezieht sich konkret auf diese Snapshot-Fassung. Die Webseiten-Version dient als laufende Referenz. Bei Hinzuziehung weiterer oder Austausch bestehender Unter-Auftragsverarbeiter informiert der Auftragsverarbeiter den Verantwortlichen **mindestens 30 Tage im Voraus** in Textform und gibt ihm damit Gelegenheit, dieser Änderung zu widersprechen.

Bei Widerspruch des Verantwortlichen verhandeln die Parteien in gutem Glauben über eine Lösung. Lässt sich binnen 14 Tagen keine Einigung erzielen, kann jede Partei den Hauptvertrag ohne Einhaltung einer Kündigungsfrist beenden.

Der Auftragsverarbeiter verpflichtet jeden Unter-Auftragsverarbeiter zu denselben Datenschutzpflichten wie in diesem AVV, insbesondere im Hinblick auf hinreichende Garantien gemäß Art. 32 DSGVO.

4.5 Unterstützung bei Betroffenenrechten (lit. e)

Der Auftragsverarbeiter unterstützt den Verantwortlichen unter Berücksichtigung der Art der Verarbeitung mit geeigneten technischen und organisatorischen Maßnahmen bei der Erfüllung der Anträge betroffener Personen gemäß Kapitel III DSGVO (Art. 15 Auskunft, Art. 16 Berichtigung, Art. 17 Löschung, Art. 18 Einschränkung, Art. 20 Datenübertragbarkeit, Art. 21 Widerspruch). Anfragen an den Auftragsverarbeiter werden binnen **5 Werktagen** an den Verantwortlichen weitergeleitet.

4.6 Unterstützung bei Compliance-Pflichten (lit. f)

Der Auftragsverarbeiter unterstützt den Verantwortlichen unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen bei der Einhaltung der Pflichten gemäß **Art. 32 bis 36 DSGVO**, insbesondere bei Datenschutz-Folgenabschätzungen (Art. 35) und Konsultationen mit der Aufsichtsbehörde (Art. 36).

4.7 Rückgabe oder Löschung nach Vertragsende (lit. g)

Nach Wahl des Verantwortlichen
alle zlichen Aufbewahrungspflichten
bes Standard-Löschfrist nach
Ver Datenschutzerklärung
4.8
Der Informationen zum Nachweis
der Er ermöglicht und unterstützt
Überprüfungen durch den verantwortlichen oder einen vom verantwortlichen beauftragten Prüfer

Cookie-Einstellungen

Wir nutzen Microsoft Clarity für anonyme Heatmaps. Keine personenbezogenen Daten, keine Drittanbieter-Tracker.

[Datenschutzerklärung](#)

(Audits, Inspektionen). Der Verantwortliche kann ein Audit pro Kalenderjahr mit einer Vorankündigungsfrist von **30 Tagen** verlangen; weitere Audits bei begründetem Verdacht (z. B. nach einer Datenpanne) jederzeit ohne Frist.

Sollte eine Weisung des Verantwortlichen nach Auffassung des Auftragsverarbeiters gegen die DSGVO oder andere Datenschutzbestimmungen verstoßen, informiert er den Verantwortlichen unverzüglich (Art. 28 Abs. 3 Satz 3 DSGVO).

5. Pflichten des Verantwortlichen

- **Rechtmäßigkeit:** Der Verantwortliche stellt sicher, dass die Verarbeitung auf einer gültigen Rechtsgrundlage gemäß Art. 6 und Art. 9 DSGVO erfolgt und Anrufer ordnungsgemäß informiert sind (Art. 13/14 DSGVO).
- **KI-Ankündigung:** Der Verantwortliche bestätigt, dass die in § 10.1 festgelegte KI-Ankündigung am Anfang jedes Anrufs gespielt wird und in seiner Datenschutzerklärung sowie auf seiner Website auf den Einsatz des Voice Agents hingewiesen wird.
- **§ 203 StGB:** Der Verantwortliche ist als Berufsgeheimnisträger identifiziert und autorisiert hiermit die Hinzuziehung des Auftragsverarbeiters und der im Annex genannten Unter-Auftragsverarbeiter ausdrücklich (siehe § 10.2).
- **Mitteilung von Vorfällen:** Der Verantwortliche meldet dem Auftragsverarbeiter eigene relevante Vorfälle (z. B. kompromittierte Klinik-Endgeräte), soweit diese Auswirkungen auf den Vertragsgegenstand haben.
- **Ansprechpartner:** Der Verantwortliche benennt eine kontaktierbare Person für Datenschutzfragen.

6. Datensicherheits-Vorfälle (Art. 33, 34 DSGVO)

Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, spätestens **innerhalb von 48 Stunden** nach Kenntniserlangung, über jede Verletzung des Schutzes personenbezogener Daten (Art. 33 Abs. 2 DSGVO). Die Mitteilung enthält mindestens: Beschreibung der Art der Verletzung, betroffene Datenkategorien und Personenanzahl, wahrscheinliche Folgen, ergriffene oder vorgeschlagene Maßnahmen.

Die 72-Stunden-Mitteilungspflicht für Auftragsverarbeiter (Art. 34 Abs. 1 DSGVO) bleibt Pflicht des Verantwortlichen.

7. T

Die

(Ver

Auf

weil

werden dem Verantwortlichen mitgeteilt.

Cookie-Einstellungen

Wir nutzen Microsoft Clarity für anonyme Heatmaps. Keine personenbezogenen Daten, keine Drittanbieter-Tracker.

[Datenschutzerklärung](#)

Annex A separat aufgeführt

erfügbarkeit, Belastbarkeit,

richtig, die TOM

Wesentliche Änderungen

8. Verarbeitungsorte und Datenresidenz

Primäre Datenspeicherung (Transkripte, Metadaten, Anwendungsdatenbank) erfolgt in der Europäischen Union auf Servern der **Hetzner Online GmbH** (Falkenstein und Nürnberg, Deutschland). Bestimmte Unter-Auftragsverarbeiter (Sprach-Synthese, Sprach-zu-Text, Telefonie, LLM) verarbeiten Daten in den USA bzw. anderen Drittländern; siehe § 9 und Annex „Unter-Auftragsverarbeiter“.

9. Drittland-Übermittlungen

Sofern Verarbeitungen in Drittländern stattfinden, gewährleistet der Auftragsverarbeiter ein angemessenes Schutzniveau gemäß **Kapitel V DSGVO (Art. 44–49)**:

- **Standard-Vertragsklauseln (SCC)** der Europäischen Kommission gemäß Durchführungsbeschluss (EU) 2021/914 mit allen Modulen 2 (Verantwortlicher → Auftragsverarbeiter) und ggf. 3 (Auftragsverarbeiter → Auftragsverarbeiter)
- **Transfer Impact Assessment (TIA)** für jeden US-Empfänger im Hinblick auf FISA 702 / Executive Order 12333 (Schrems II-Linie)
- Soweit der Empfänger unter dem **EU-U.S. Data Privacy Framework (DPF)** zertifiziert ist (z. B. Telnyx, Resend, Microsoft, Vercel, Anthropic), zusätzlich Berufung auf den Angemessenheitsbeschluss vom 10. Juli 2023.

10. Voice-Agent-spezifische Klauseln

10.1 KI-Ankündigung beim Anrufstart (AI Act Art. 50)

Der Auftragsverarbeiter spielt zu Beginn jedes Anrufs einen klaren, deutlich verständlichen Hinweis ab, dass der Anrufer mit einem KI-System interagiert (Beispiel: „Sie sprechen mit dem KI-Telefonassistenten der Praxis Dr. X. Wenn Sie lieber mit einem Menschen sprechen möchten, sagen Sie einfach ‚Mensch‘“). Diese Pflicht ergibt sich aus **Art. 50 KI-Verordnung (EU) 2024/1689**; die Anwendbarkeit ist auf den 2. August 2026 datiert. Lucid AI Labs erfüllt diese Pflicht *vorzeitig* ab Vertragsstart.

10.2 Berufsaheimnis (§ 203 StGB)

Der
Ann
„mit
Ver
Pers
unte
Mit
Pers

Cookie-Einstellungen

Wir nutzen Microsoft Clarity für anonyme Heatmaps. Keine personenbezogenen Daten, keine Drittanbieter-Tracker.

[Datenschutzerklärung](#)

tragsverarbeiter sowie alle im
Abs. 3 und 4 StGB als
durch eigene
Auftragsverarbeiter setzt nur
lichen Geheimhaltungspflicht
utorisierung als „mitwirkende
enschutzrechtliche Aufklärung

der Patienten gemäß Art. 13/14 DSGVO über die Einbindung des Voice-Agent-Dienstes (inkl. der im Annex aufgeführten Sub-Prozessoren mit US-Bezug). Der Verantwortliche stellt sicher, dass Patienten vor Inanspruchnahme der Praxis-Telefonie über (i) den Einsatz eines KI-gestützten Empfangs-Dienstes, (ii) die Datenflüsse einschließlich Drittlandtransfer auf Grundlage von SCC + DPF, und (iii) ihre Betroffenenrechte (Art. 15–22 DSGVO) informiert werden. Der Auftragsverarbeiter stellt hierfür Vorlagen (Praxis-Aushang, DSE-Snippet, Telefon-Ansage) bereit.

10.3 Aufzeichnung (§ 201 StGB)

Standard: Es findet *keine* dauerhafte Audio-Aufzeichnung statt. Sprachdaten werden transient verarbeitet (Streaming) und nach Generierung des Transkripts binnen 60 Sekunden gelöscht. Transkripte werden gespeichert.

Optionale Aufzeichnung: Sofern der Verantwortliche im Hauptvertrag explizit eine zusätzliche Audio-Aufzeichnung beauftragt (z. B. zur Qualitätssicherung), wird zu Beginn jedes Anrufs ein zusätzlicher Hinweis abgespielt („Dieser Anruf wird zur Qualitätssicherung aufgezeichnet. Wenn Sie damit nicht einverstanden sind, sagen Sie bitte ‚nein aufzeichnen‘“). Bei Widerspruch wird die Aufzeichnung sofort und nachweislich deaktiviert. Eine Aufzeichnung ohne Hinweis und Einwilligungsmöglichkeit erfolgt unter keinen Umständen, da dies einen Verstoß gegen § 201 StGB darstellen würde.

Einwilligungs-Dokumentation (Nachweisbarkeit): Wird die Aufzeichnung aktiviert, dokumentiert der Auftragsverarbeiter je Anruf: (a) Anruf-ID, (b) Zeitstempel des Hinweis-Abspielens, (c) Anruferreaktion (Schweigen / explizite Einwilligung / Widerspruch) mit Zeitstempel, (d) Aufzeichnungs-Status (gestartet / unterbunden). Beim Widerspruchs-Wort („nein“, „nicht aufzeichnen“, „kein Mitschnitt“) oder bei Erkennung eines Widerspruchs durch den Soft-Classifer wird die Aufzeichnung binnen 1 Sekunde gestoppt und der bisherige Audio-Puffer unwiederbringlich gelöscht. Die Einwilligungs-Logs werden für die Dauer der Aufzeichnungsspeicherungsdauer (siehe § 11) aufbewahrt und sind dem Verantwortlichen auf Anforderung vorzulegen.

10.4 Funktionsbegrenzung (Hochrisiko-KI-Vermeidung)

Der Voice Agent **stellt keine Diagnose**, führt **keine Triage durch** und gibt **keine medizinischen Bewertungen** ab. Bei jedem inhaltlichen medizinischen Anliegen erfolgt Eskalation an einen Menschen. Diese Funktionsbegrenzung vermeidet eine Einstufung als Hochrisiko-KI-System gemäß Anhang III KI-VO.

Die

Cookie-Einstellungen

- Wir nutzen Microsoft Clarity für anonyme Heatmaps. Keine personenbezogenen Daten, keine Drittanbieter-Tracker.
[Datenschutzerklärung](#)
-

ngesetzt:

e (z. B. „Brustschmerzen“,
n Live-Transkript die Eskalation
docs/voice-agent-notruf-

onversation sofort an einen

- **Soft-Classifizier** für Diagnose-/Triage-/Behandlungsempfehlungs-Intentionen, der bei Konfidenz $\geq 0,7$ die Eskalation auslöst und gleichzeitig jede medizinisch-inhaltliche Antwort des Hauptmodells unterdrückt.
- **System-Prompt-Constraints**: das LLM ist explizit angewiesen, keine Diagnose, Triage oder Therapie-Empfehlung zu geben; Anti-Halluzinations-Guardrails verbieten freie medizinische Aussagen.
- **Quartalsweise Tests** mit synthetischen Notfall- und Diagnose-Dialogen, deren Ergebnisse intern protokolliert werden; Auffälligkeiten lösen ein Retraining der Trigger-Liste oder eine Anpassung des Soft-Classifiziers aus.

10.5 Eskalation

Der Auftragsverarbeiter stellt sicher, dass jederzeit eine Eskalation an einen Menschen möglich ist und diese spätestens dann erfolgt, wenn (a) der Anrufer dies ausdrücklich verlangt, (b) das Vertrauensniveau des Modells unter den vereinbarten Schwellwert (Standard: 75 %) fällt, oder (c) ein medizinisch-inhaltliches Anliegen erkannt wird.

11. Speicherdauer

- Live-Audiostream: transient, max. 60 Sekunden Pufferung, danach gelöscht.
- Transkript des Gesprächs: 90 Tage (Standard); konfigurierbar nach Klinik-Vorgabe.
- Termin-Datensatz (Name, Datum, Anliegen-Kategorie): bis Wegfall der Klinik-internen Aufbewahrungspflicht; max. 10 Jahre nach behandlungsrechtlichen Aufbewahrungsfristen.
- Anruf-Metadaten (Zeitstempel, Dauer, Eskalations-Status): 12 Monate, dann anonymisiert.
- Optionale Audio-Aufzeichnung (sofern explizit aktiviert): 30 Tage, dann unwiederbringlich gelöscht.

12. Haftung

Die Haftung der Parteien folgt dem Hauptvertrag und ergänzend **Art. 82 DSGVO**. Bei Pflichtverletzungen, die ausschließlich auf Verschulden des Verantwortlichen zurückzuführen sind (z. B. unzureichende eigene Datenschutzerklärung), entfällt die Haftung des Auftragsverarbeiters. Es besteht eine **Haftungssumme**.

13. Wir nutzen Microsoft Clarity für anonyme Heatmaps. Keine personenbezogenen Daten, keine Drittanbieter-Tracker.

Dies: [Datenschutzerklärung](#)

/ Lö

cht erforderlich. § 4.7 (Rückgabe

Cookie-Einstellungen

14. Schlussbestimmungen

- Änderungen und Ergänzungen bedürfen der Textform (E-Mail genügt). Salvatorische Klausel: sollte eine Bestimmung unwirksam sein, bleibt der übrige Vertrag wirksam.
- Es gilt deutsches Recht.
- Gerichtsstand: Sitz des Verantwortlichen, sofern dieser Verbraucher i. S. v. § 13 BGB ist; ansonsten der Sitz des Auftragsverarbeiters (Amtsgericht Regensburg).
- Die jeweils aktuelle Fassung dieses AVV ist unter [/de/avv](#) abrufbar. Wesentliche Änderungen werden mit 30 Tagen Vorlauf in Textform mitgeteilt.

Annex A, Unter-Auftragsverarbeiter

Vollständige aktuelle Liste: [/de/auftragsverarbeiter](#). Auszug zum Stand 28. April 2026:

- **Hetzner Online GmbH** (Industriestr. 25, 91710 Gunzenhausen, DE), Hosting der Anwendungs-DB und Transkripte. Datenresidenz: Falkenstein/Nürnberg/Helsinki. Keine Drittlandübermittlung. AVV: [hetzner.com/AV](#).
- **Vercel Inc.** (340 S Lemon Ave #4133, Walnut, CA 91789, USA), Hosting der Marketing- und Klinik-Dashboard-Oberfläche. Drittlandübermittlung in die USA, abgesichert durch SCC + DPF. AVV: [vercel.com/legal/data-processing-addendum](#).
- **Anthropic PBC** (548 Market St PMB 90375, San Francisco, CA 94104, USA), Sprachverarbeitung (LLM für Konversation und Termin-Logik). API-Modus: keine Verwendung der Daten zu Trainingszwecken (Commercial Terms). SCC + DPF. AVV: [anthropic.com/legal/commercial-terms](#).
- **Deepgram Inc.** (1438 Webster St STE 100, Oakland, CA 94612, USA), Sprach-zu-Text (STT). SCC. AVV: [deepgram.com/legal](#).
- **ElevenLabs Inc.** (228 Park Ave S PMB 30661, New York, NY 10003, USA), Sprach-Synthese (TTS). SCC. AVV: [elevenlabs.io/dpa](#).
- **Telnyx LLC** (311 W Superior Street, Suite 504, Chicago, IL 60654, USA), Telefonie (SIP-Trunk, Anrufentgegennahme, Routing, deutsche Geo-Rufnummern). SCC + EU-U.S. DPF. EU-Vertretung: Telnyx Ireland Limited (Dublin). AVV: [telnyx.com/legal/data-processing-addendum](#).
- **Record Inq.** (San Francisco, CA, USA), Transkriptionale E-Mail/Termin-Bestätigungen). SCC + DPF.

Cookie-Einstellungen

Wir nutzen Microsoft Clarity für anonyme Heatmaps. Keine personenbezogenen Daten, keine Drittanbieter-Tracker.

[Datenschutzerklärung](#)

Ak

Mit

(Inb

(Use

(Art

durch konkludentes Verhalten

Der Akzeptanz-Datensatz

[_acceptances](#) gespeichert

PDF-Fassung ist oben über den

Download-Button verfügbar; für eine klinik-spezifisch ausgefüllte Variante (Annex-A-Snapshot, vereinbarte TOM-Anpassungen) schreiben Sie an Fabi@lucid-ai.app.

Verwandte Dokumente

- [Datenschutzerklärung](#)
- [Datenschutz-FAQ für Klinik-Inhaber \(Klartext\)](#)
- [Technische und organisatorische Maßnahmen \(TOM, Art. 32 DSGVO\)](#)
- [Liste der Unter-Auftragsverarbeiter](#)
- [Impressum](#)
- [English version \(AVV / DPA\)](#)

Cookie-Einstellungen

Wir nutzen Microsoft Clarity für anonyme Heatmaps. Keine personenbezogenen Daten, keine Drittanbieter-Tracker.

[Datenschutzerklärung](#)