

Dokument: Auftragsverarbeitungsvertrag (AVV)

Anbieter: LocalBot UG (haftungsbeschränkt)

Version: 1.0

Stand: 2026-06-16

Auftragsverarbeitungsvertrag (AVV)

Vereinbarung über die Verarbeitung personenbezogener Daten im Auftrag gemäß Art. 28 DSGVO

Basis: EU-Kommissions-Muster 2021/915 vom 04.06.2021, angepasst an SaaS-Voice.

Vertragsparteien

Verantwortlicher (nachfolgend „Kunde“):

[FIRMA DES KUNDEN]

[ANSCHRIFT]

vertreten durch [GESCHÄFTSFÜHRER / INHABER]

— und —

Auftragsverarbeiter (nachfolgend „Anbieter“):

LocalBot UG (haftungsbeschränkt)

Plather Dorfstraße 12d, 39624 Kalbe (Milde)

eingetragen im Handelsregister des Amtsgerichts Stendal unter HRB 37622

vertreten durch Geschäftsführer Janis Szczepanek

§ 1 Gegenstand, Dauer, Weisungsrecht

(1) Gegenstand: Bereitstellung des KI-Telefonassistenten VoiceAssist Pro gemäß Hauptvertrag.

(2) Dauer: entspricht der Laufzeit des Hauptvertrags.

(3) Der Anbieter verarbeitet personenbezogene Daten **ausschließlich auf dokumentierte Weisung** des Kunden (Art. 28 Abs. 3 S. 2 lit. a DSGVO). Die Nutzung gemäß Hauptvertrag gilt als Weisung.

§ 2 Art und Zweck der Verarbeitung (Art. 28 Abs. 3 S. 1)

- **Art:** Erheben, Speichern, Analysieren, Transkribieren, Übermitteln
- **Zweck:** Entgegennahme, Qualifizierung und strukturierte Aufbereitung eingehender Anrufe; Terminbuchung; Weiterleitung an den Kunden
- **Verfahren:** automatisiert (KI-basiert)

§ 3 Art der personenbezogenen Daten

- Kommunikationsdaten (Telefonnummer, Anrufzeitpunkt, Dauer)
- Inhaltsdaten (Anliegen, gewünschte Termine, frei gesprochene Angaben)
- Gegebenenfalls **Audio-Rohaufnahme** (biometrische Daten, Art. 9 DSGVO) — nur bei ausdrücklicher Einwilligung des Anrufers
- Bei Arztpraxis-Use-Case: Gesundheitsdaten (Art. 9 DSGVO)

§ 4 Kategorien betroffener Personen

- Anrufer (Kunden/Patienten/Gäste des Kunden)
- Mitarbeiter des Kunden (bei Weiterleitung/Rückruf)

§ 5 Pflichten des Anbieters

Der Anbieter verpflichtet sich:

1. Verarbeitung nur auf dokumentierte Weisung (Art. 28 Abs. 3 lit. a)
2. Vertraulichkeitsverpflichtung aller Mitarbeiter (Art. 28 Abs. 3 lit. b, § 5 BDSG)
3. Technische und organisatorische Maßnahmen (Art. 32) gemäß Anlage 1 (TOM-Dokument)
4. Unterstützung des Kunden bei Betroffenenrechten (Art. 28 Abs. 3 lit. e)
5. Unterstützung bei Art. 32–36 DSGVO (Art. 28 Abs. 3 lit. f)
6. Unverzügliche Meldung von Datenschutzverletzungen (Art. 33) spätestens binnen **24 Stunden** nach Kenntnis
7. Löschung/Rückgabe der Daten nach Vertragsende (§ 7)
8. Nachweisführung und Audit-Ermöglichung (Art. 28 Abs. 3 lit. h)
9. Bestellung eines DSB bei Pflicht (Art. 37)
10. Führung eines Verzeichnisses (Art. 30 Abs. 2)

§ 6 Unterauftragsverarbeiter (Subprozessoren)

(1) Der Kunde erteilt dem Anbieter eine **allgemeine Genehmigung** zum Einsatz von Subprozessoren. Die jeweils aktuelle Liste mit Sitz, Zweck, verarbeiteten Datenarten, Drittlandtransfer-Rechtsgrundlage und Vertragslink ist in **Anlage 2 (SUBPROCESSORS.md)** geführt und in der zum Zeitpunkt der Verarbeitung gültigen Fassung Bestandteil dieses Vertrags. Die Mindestbesetzung umfasst aktuell:

| Subprozessor | Sitz | Zweck | Drittlandtransfer-Basis |

|---|---|---|---|

| Hetzner Online GmbH | DE Nürnberg | Hosting, DB | DSGVO-Direkt (kein Drittland) |

| Twilio Inc. | us | Telefonie | DPF + SCC |

Deepgram Inc.	us	Speech-to-Text	SCC + TIA (DPF-Status zu prüfen)
Google LLC (Gemini API)	us / EU-Region	LLM	DPF + DPA; Region `europa-west3` bevorzugt
Cartesia Inc.	us	Text-to-Speech (Basic)	SCC + TIA
ElevenLabs Inc.	us (EU-Datenresidenz verfügbar)	Text-to-Speech (Pro/Premium)	DPF + DPA (Zero Retention nur Enterprise-Tarif — im eingesetzten Standard-Tarif nicht aktiv)
Stripe Payments Europe Ltd.	IE + us	Zahlungsabwicklung	DPF + SCC
Google Workspace (Calendar/Mail)	us + EU	Kalender-Integration	DPF + DPA
Sentry / Functional Software Inc. (*optional*)	us / EU-Region (Frankfurt)	Error-Tracking	DPF + EU-Region erzwungen

(2) Der Anbieter informiert den Kunden über Änderungen (Aufnahme/Austausch) spätestens **30 Tage vor Einsatz** in Textform. Der Kunde kann binnen **14 Tagen** in Textform widersprechen; erfolgt Widerspruch, steht dem Anbieter ein Sonderkündigungsrecht zu.

(3) Jeder Subprozessor wird vertraglich auf gleichwertige Datenschutzpflichten verpflichtet (Art. 28 Abs. 4).

(4) **Drittlandtransfer** in die USA (Deepgram, Cartesia, ggf. Google/Twilio/Stripe): erfolgt auf Basis **EU-US Data Privacy Framework** (sofern zertifiziert) und zusätzlich **Standardvertragsklauseln der EU-Kommission (2021/914)** sowie Transfer Impact Assessment (TIA) nach EDPB-Empfehlung 01/2020. TIA-Dokumentation und TOM-Nachweis pro Subprozessor stellt der Anbieter dem Kunden auf Anforderung zur Verfügung.

(5) **Technische Schutzmaßnahmen bei Drittlandtransfer** (unabhängig vom DPF-Status): Audio at-rest verschlüsselt (AES-256-GCM; im Design-B-Betrieb wird zudem kein Anrufer-Audio dauerhaft gespeichert), Transkripte mit Field-Level-Encryption (AES-256-GCM), Pseudonymisierung der Telefonnummer (HMAC-SHA-256 + Salt). — In Vorbereitung (noch nicht produktiv, daher nicht als erfüllt zugesichert): Deepgram EU-Endpoint. Der ElevenLabs Zero-Retention-Mode ist ausschließlich im **Enterprise-Tarif** verfügbar und im genutzten Standard-/Pro-/Premium-Tarif nicht aktivierbar; der Transfer stützt sich insoweit auf DPF + DPA + SCC/TIA. Ein Gemini-Region-Pinning auf `europa-west3` ist über die genutzte Direkt-Gemini-API nicht verfügbar; der Transfer stützt sich insoweit auf DPF/SCC.

§ 7 Löschung und Rückgabe (Art. 28 Abs. 3 lit. g)

(1) Nach Beendigung des Hauptvertrags löscht der Anbieter alle personenbezogenen Daten **spätestens 30 Tage** nach Vertragsende, es sei denn, gesetzliche Aufbewahrungspflichten stehen entgegen.

(2) Auf Wunsch des Kunden stellt der Anbieter Daten vor Löschung im Format CSV/JSON zur Verfügung.

(3) Die Löschung wird auf Anforderung schriftlich bestätigt.

§ 8 Audit (Art. 28 Abs. 3 lit. h)

(1) Der Kunde hat das Recht, die Einhaltung dieser Vereinbarung zu kontrollieren. Der Anbieter stellt hierzu die notwendigen Informationen zur Verfügung, insbesondere:

- ISO 27001-Zertifikate der Subprozessoren (falls vorhanden)
- TOM-Dokumentation

- Audit-Berichte des Anbieters

(2) Vor-Ort-Kontrollen sind mit angemessener Frist (mind. 14 Tage) anzukündigen und dürfen den Betriebsablauf nicht unangemessen stören. Max. 1 Audit pro Jahr auf eigene Kosten des Kunden; anlassbezogene Audits bei begründetem Verdacht bleiben unberührt.

§ 9 Haftung

Die Haftung richtet sich nach Art. 82 DSGVO sowie nach den Regelungen des Hauptvertrags. Im Innenverhältnis tragen die Parteien den Schaden anteilig gemäß Verursachungsbeitrag.

§ 10 Schlussbestimmungen

(1) Bei Widersprüchen zwischen AVV und Hauptvertrag geht der AVV vor (Datenschutz).

(2) Schriftform, auch Textform (§ 126b BGB) genügt.

(3) Gerichtsstand: Kalbe (Milde).

Ort, Datum, Unterschriften:

[ORT], den [DATUM]

Für den Kunden: Für den Anbieter:

[NAME] Janis Sczepanek

[FUNKTION] Geschäftsführer LocalBot UG

Anlage 1: Technische und organisatorische Maßnahmen (`08_TOM.md`)

Anlage 2: Subprozessoren-Liste (`SUBPROCESSORS.md` — gilt in der jeweils aktuellen Fassung; Änderungen nach § 6 Abs. 2)

LocalBot UG (haftungsbeschränkt) · Plather Dorfstraße 12d · 39624 Kalbe (Milde) · Deutschland
voiceassist@localbotai.de · +49 175 861 6280 · Amtsgericht Stendal · HRB 37622

Diese PDF wurde aus `Recht/06_AVV.md` generiert (2026-06-16). Bei Widerspruch zwischen PDF und Quell-MD gilt die Quell-MD.