

denic KI-Agentur

Vereinbarung über die Auftragsverarbeitung

nach Art. 28 DSGVO / Art. 9 nDSG

| Auftraggeber (Verantwortlicher) | Auftragnehmer (Verarbeiter) |
|--|--|
| [Firmenname Kunde] [Adresse] [PLZ Ort, Land] [E-Mail] | Alexander Denic / denic KI-Agentur Riedstrasse 74 8604 Volketswil, Schweiz info@denic.swiss |
| (im Folgenden: Auftraggeber) | (im Folgenden: Auftragnehmer) |

Gemeinsam als «Parteien» bezeichnet.

Datum: _____

1. Hintergrund und Spezifikation der Datenverarbeitung

1.1 Der Auftragnehmer ist ein Unternehmen, das folgende Dienstleistungen erbringt:

- Konfiguration, Verwaltung und Bereitstellung eines KI-Telefonie-Assistenten auf Basis der fonio.ai-Plattform.

1.2 Der Auftraggeber ist ein Unternehmen, das die Dienstleistungen des Auftragnehmers in Anspruch nehmen möchte.

1.3 Diese Vereinbarung über die Auftragsverarbeitung (AVV) legt die Bedingungen für die Verarbeitung personenbezogener Daten durch den Auftragnehmer fest. Sie gilt ergänzend zum Hauptvertrag zwischen den Parteien.

1.4 Der Auftragnehmer handelt ausschliesslich als Auftragsverarbeiter im Sinne von Art. 28 DSGVO bzw. Art. 9 nDSG und verarbeitet personenbezogene Daten nur nach dokumentierten Weisungen des Auftraggebers.

2. Art, Zweck, Gegenstand und Rechtsgrundlage

2.1 **Art der Verarbeitung:** Erhebung, Speicherung, Übermittlung, Verwendung und Löschung personenbezogener Daten.

2.2 **Zweck der Verarbeitung:** Automatisierte Entgegennahme und Weiterleitung von Telefonanrufen, Terminbuchung, Kundenbetreuung sowie Erstellung technischer Logs.

2.3 **Rechtsgrundlagen:** Art. 6 Abs. 1 lit. b und/oder lit. f DSGVO sowie Art. 31 nDSG.

3. Betroffene Daten und Personenkategorien

3.1 Im Rahmen dieser AVV werden folgende Kategorien personenbezogener Daten verarbeitet:

- Telefonnummern der Anrufer
- Audiodaten (Sprachaufzeichnungen von Anrufen)
- Kontaktinformationen (Name, soweit im Gespräch genannt)
- Technische Metadaten (Anrufdauer, Zeitstempel, Geräte-IDs)
- Technische Logs (Systemprotokolle)

3.2 **Betroffene Personenkategorien:** Kunden und Geschäftspartner des Auftraggebers, die den KI-Telefonie-Assistenten kontaktieren.

4. Pflichten des Auftragnehmers

4.1 **Weisungsgebundenheit:** Der Auftragnehmer verarbeitet personenbezogene Daten ausschliesslich auf Grundlage dokumentierter Weisungen des Auftraggebers, einschliesslich dieser AVV.

4.2 **Vertraulichkeit:** Der Auftragnehmer stellt sicher, dass alle zur Verarbeitung befugten Personen zur Vertraulichkeit verpflichtet sind oder einer gesetzlichen Verschwiegenheitspflicht unterliegen.

4.3 **Technische Massnahmen:** Der Auftragnehmer trifft alle nach Art. 32 DSGVO / Art. 8 nDSG erforderlichen technischen und organisatorischen Massnahmen (vgl. Anhang 1).

4.4 **Betroffenenrechte:** Der Auftragnehmer unterstützt den Auftraggeber bei der Erfüllung von Betroffenenrechten (Auskunft, Berichtigung, Löschung, Einschränkung, Datenübertragbarkeit,

Widerspruch).

4.5 Meldepflicht: Bei Kenntnis einer Datenschutzverletzung informiert der Auftragnehmer den Auftraggeber unverzüglich, spätestens innerhalb von 48 Stunden nach Bekanntwerden.

4.6 Nachweisführung: Der Auftragnehmer stellt alle erforderlichen Informationen zur Nachweisführung bereit und ermöglicht Überprüfungen durch den Auftraggeber oder beauftragte Prüfer.

5. Sub-Auftragsverarbeiter (Unterauftragnehmer)

5.1 Der Auftraggeber erteilt hiermit die allgemeine Genehmigung für den Einsatz folgender Sub-Auftragsverarbeiter:

| Unternehmen | Sitz | Funktion | Garantie |
|------------------|--------------------|---------------------------------------|-------------------|
| fonio GmbH | Wien, AT | KI-Telefonie-Plattform, Infrastruktur | Art. 28 DSGVO AVV |
| OpenAI, L.L.C. | San Francisco, USA | Spracherkennung, KI-Verarbeitung | Swiss-US DPF |
| ElevenLabs, Inc. | USA | Text-zu-Sprache | Swiss-US DPF |
| Deepgram, Inc. | USA | Sprache-zu-Text | Swiss-US DPF |

5.2 Änderungen (Hinzuziehung / Austausch) von Sub-Auftragsverarbeitern werden dem Auftraggeber mindestens **zwei Wochen** im Voraus schriftlich mitgeteilt. Der Auftraggeber hat ein Widerspruchsrecht.

5.3 Die US-amerikanischen Sub-Auftragsverarbeiter sind unter dem Swiss-US Data Privacy Framework (Swiss-US DPF) zertifiziert, was als angemessene Datenschutzgarantie im Sinne des nDSG anerkannt ist.

6. Prüfung und Einhaltung

6.1 Der Auftragnehmer stellt dem Auftraggeber auf Anfrage alle erforderlichen Informationen zur Nachweisführung der Einhaltung dieser AVV zur Verfügung.

6.2 Audits durch den Auftraggeber oder beauftragte Dritte sind mit angemessener Vorankündigung (mindestens 14 Tage) möglich. Die Kosten trägt der Auftraggeber.

6.3 Der Auftragnehmer kann anstelle eines Vor-Ort-Audits entsprechende Zertifizierungen oder Prüfberichte vorlegen.

7. Laufzeit und Vertragsende

7.1 Diese AVV tritt mit Unterzeichnung in Kraft und gilt für die Dauer der Hauptvertragsbeziehung.

7.2 Nach Beendigung hat der Auftragnehmer nach Wahl des Auftraggebers alle personenbezogenen Daten zu löschen oder zurückzugeben, sofern keine gesetzlichen Aufbewahrungspflichten entgegenstehen.

7.3 Sofern keine ausdrückliche Weisung zur Rückgabe erfolgt, werden personenbezogene Daten standardmässig **spätestens 6 Monate** nach Vertragsende gelöscht.

8. Schlussbestimmungen

8.1 Anwendbares Recht: Diese AVV untersteht dem Schweizer Recht (nDSG). Soweit EU-Recht (DSGVO) anwendbar ist, gilt dieses vorrangig.

8.2 Gerichtsstand: Volketswil (Kanton Zürich), Schweiz.

8.3 Schriftform: Änderungen und Ergänzungen dieser AVV bedürfen der Schriftform.

8.4 Vorrang: Im Widerspruchsfall zwischen dieser AVV und dem Hauptvertrag hat die AVV in datenschutzrechtlichen Belangen Vorrang.

| Auftraggeber | Auftragnehmer |
|--|-------------------------------------|
| [Ort], _____ | Volketswil, _____ |
| _____ | _____ |
| [Unterschrift & Stempel] [Name, Funktion] | Alexander Denic denic KI-Agentur |

Anhang 1 – Technische und Organisatorische Massnahmen (TOMs)

Gemäss Art. 32 DSGVO / Art. 8 nDSG setzt der Auftragnehmer die folgenden Massnahmen um:

A. Technische Massnahmen

- **Zertifizierung:** ISO 27001-Zertifizierung der zugrundeliegenden Infrastruktur
- **Verschlüsselung:** TLS 1.2+ in Transit, AES-256 at Rest für alle personenbezogenen Daten
- **Zugriffskontrolle:** Rollenbasierte Zugriffssteuerung (RBAC), Prinzip der minimalen Rechte
- **Authentifizierung:** Multi-Faktor-Authentifizierung (MFA) für alle Systemzugänge
- **Netzwerksicherheit:** Firewall-Systeme, Intrusion Detection/Prevention (IDS/IPS)
- **Schwachstellen:** Regelmässige Penetrationstests und automatisierte Schwachstellenscans
- **Logging:** Vollständige Protokollierung aller Datenzugriffe und Verarbeitungsvorgänge
- **Backup:** Automatische, verschlüsselte Backups mit regelmässigen Wiederherstellungstests
- **Verfügbarkeit:** Redundante Infrastruktur, SLA-gesicherte Verfügbarkeit

B. Organisatorische Massnahmen

- **Datenschutzverantwortlicher:** Benennung eines Datenschutzverantwortlichen
- **Mitarbeiterschulungen:** Regelmässige Schulungen zu Datenschutz und Informationssicherheit
- **Vertraulichkeit:** Schriftliche Verschwiegenheitsverpflichtung aller Personen mit Datenzugang
- **Incident Response:** Dokumentierte Notfall- und Reaktionspläne bei Datenschutzverletzungen
- **Datenlöschung:** Automatisierte Löschroutinen nach Ablauf der Aufbewahrungsfristen
- **Subunternehmer-Prüfung:** Sorgfältige Auswahl und vertragliche Bindung aller Sub-Auftragsverarbeiter

Anhang 2 – KI-Modellentwicklung und Datennutzung

Ergänzende Bestimmung zur Nutzung personenbezogener Daten für KI-Systeme:

Keine Nutzung für KI-Training: Die im Rahmen dieser Vereinbarung verarbeiteten personenbezogenen Daten (insbesondere Audiodaten, Transkriptionen, Kontaktinformationen) werden **nicht** für das Training, die Weiterentwicklung oder Verbesserung von KI-Modellen verwendet. Dies gilt für den Auftragnehmer und alle eingesetzten Sub-Auftragsverarbeiter gleichermassen.

Datenzweckbindung: Personenbezogene Daten werden ausschliesslich für die vertraglich vereinbarten Zwecke (Telefonie-Assistent, Terminbuchung, Kundenbetreuung) verwendet.

Berufsgeheimnis-Hinweis: Für Kunden, die dem Berufsgeheimnis unterliegen (Treuhand, Rechtsanwälte, Ärzte): Diese AVV deckt den Bereich der Terminbuchung und des Routings ab, bei dem keine vertraulichen Mandanteninhalte verarbeitet werden. Sobald inhaltliche Mandanteninformationen verarbeitet werden sollen, ist eine zusätzliche Verschwiegenheitsvereinbarung (NDA / Side Letter) erforderlich, welche vom Endkunden beizubringen ist.