

Auftragsverarbeitungsvertrag (AVV)

gemäß Art. 28 DSGVO

Stand: April 2026 | oneKI – app.one-ki.de

Verantwortlicher: Marius Jonda (oneKI) | Nützenberger Str. 175, 42115 Wuppertal | info@one-ki.de

Zwischen

dem Kunden (nachfolgend "Verantwortlicher"), der die oneKI-Plattform nutzt,

und

Marius Jonda, Nützenberger Str. 175, 42115 Wuppertal, E-Mail: info@one-ki.de (nachfolgend "Auftragsverarbeiter" oder "oneKI"),

wird folgender Auftragsverarbeitungsvertrag gemäß Art. 28 DSGVO geschlossen.

§ 1 Gegenstand und Dauer

Dieser AVV regelt die Auftragsverarbeitung im Rahmen der Nutzung der oneKI-Plattform (app.one-ki.de) durch den Verantwortlichen. Er ist Bestandteil des Hauptvertrags (AGB) und gilt für die Dauer des Hauptvertragsverhältnisses.

Gegenstand der Auftragsverarbeitung ist die Bereitstellung der oneKI-SaaS-Dienste, insbesondere:

- Verarbeitung von Gesprächsdaten im Rahmen des Voice Bots (Telefonie)
- Verarbeitung von Chat-Inhalten im Rahmen des Chat Bots
- Verarbeitung von E-Mail-Inhalten im Rahmen des E-Mail Bots
- Speicherung von Transkripten, Zusammenfassungen und Anruferprofilen (Pre-Call Memory)
- Bereitstellung des Dashboards und der Analysefunktionen

§ 2 Art der Daten und Kategorien betroffener Personen

Kategorien betroffener Personen:

- Endnutzer (Anrufer, Chat-Teilnehmer, E-Mail-Absender)
- Autorisierte Nutzer des Kunden (Administratoren, Mitarbeiter)

Kategorien personenbezogener Daten:

- Kontaktdaten (Name, Telefonnummer, E-Mail-Adresse)
- Kommunikationsinhalte (Gesprächstranskripte, Chat-Verläufe, E-Mail-Inhalte)
- Metadaten (Zeitstempel, Gesprächsdauer, Routing-Informationen)
- KI-generierte Zusammenfassungen und Anruferprofile
- Technische Zugriffsdaten (IP-Adresse, Session-Daten)

Besondere Kategorien personenbezogener Daten (Art. 9 DSGVO): Die Verarbeitung besonderer Kategorien ist nicht vorgesehen. Der Verantwortliche ist verpflichtet, Endnutzer anzuweisen, solche Daten nicht zu übermitteln.

§ 3 Weisungsrecht des Verantwortlichen

Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisung des Verantwortlichen. Die Konfiguration der KI-Agenten durch den Kunden gilt als dokumentierte Weisung.

Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, wenn eine erteilte Weisung nach seiner Auffassung gegen die DSGVO oder andere datenschutzrechtliche Vorschriften verstößt.

Sofern der Auftragsverarbeiter zur Verarbeitung nach dem Recht der EU oder eines EU-Mitgliedstaats verpflichtet ist, informiert er den Verantwortlichen hierüber vorab, sofern rechtlich zulässig.

§ 4 Technische und organisatorische Maßnahmen (TOM)

Der Auftragsverarbeiter trifft geeignete technische und organisatorische Maßnahmen gemäß Art. 32 DSGVO, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Zu den implementierten Maßnahmen zählen:

Vertraulichkeit:

- Verschlüsselung der Datenübertragung (TLS 1.2+)
- Verschlüsselung der Datenspeicherung (AES-256)
- Row-Level Security (RLS) in der Datenbank – jeder Tenant sieht ausschließlich seine eigenen Daten
- Rollenbasiertes Zugriffsmodell (super_admin / tenant_admin / tenant_member)
- Webhook-Signatur-Verifizierung und URL-Token-Absicherung

Integrität:

- Audit-Logs für alle sicherheitsrelevanten Aktionen (dauerhaft, nicht löscherbar)
- Idempotency-Keys bei Billing-Events zur Vermeidung von Duplikaten
- Rate Limiting (30 Anrufe/Stunde pro Rufnummer)

Verfügbarkeit:

- Hosting auf Hetzner (Deutschland) mit Redundanz
- Monitoring über Grafana + Loki (self-hosted)
- Strukturierte JSON-Logs mit Request-IDs

Datentrennung:

- Strikte Multi-Tenant-Trennung auf Datenbankebene
- Datenspeicherung der Kerndaten ausschließlich auf Servern innerhalb der EU/des EWR

§ 5 Unterauftragsverarbeiter

Der Auftragsverarbeiter ist berechtigt, Unterauftragsverarbeiter einzusetzen. Der Verantwortliche erteilt hiermit eine allgemeine Genehmigung für den Einsatz der folgenden Unterauftragsverarbeiter:

- Hetzner Online GmbH, Industriestr. 25, 91710 Gunzenhausen, Deutschland – Server-Hosting (Voice Bot, n8n, Monitoring)
- Supabase Inc. (Supabase GmbH), Frankfurt (eu-central-1) – Datenbank, Auth, Edge Functions
- TENIOS GmbH – Telefonieprovider (SIP-Trunk, Rufnummern)
- Deepgram, Inc., 548 Market St PMB 86613, San Francisco, CA 94104, USA – Speech-to-Text (EU-API-Endpunkt; Standardvertragsklauseln)
- Mistral AI S.A.S., 15 rue des Halles, 75001 Paris, Frankreich – Large Language Model
- Cartesia Inc., USA – Text-to-Speech (EU-Hosting; Standardvertragsklauseln)
- LiveKit Inc., 340 S Lemon Ave #8044, Walnut, CA 91789, USA – WebRTC Voice Transport (EU-Instanz; Standardvertragsklauseln)
- Stripe Payments Europe, Ltd., 1 Grand Canal Street Lower, Dublin, Irland – Zahlungsabwicklung

Der Auftragsverarbeiter informiert den Verantwortlichen über beabsichtigte Änderungen (Hinzunahme oder Austausch von Unterauftragsverarbeitern) mit angemessener Frist. Der Verantwortliche kann Einwände gegen wesentliche Änderungen schriftlich erheben. Mit allen Unterauftragsverarbeitern werden datenschutzkonforme Vereinbarungen abgeschlossen.

§ 6 Unterstützungspflichten des Auftragsverarbeiters

Der Auftragsverarbeiter unterstützt den Verantwortlichen bei der Erfüllung seiner Pflichten aus Art. 32–36 DSGVO, insbesondere:

- Unterstützung bei der Beantwortung von Betroffenenanfragen (Art. 15–22 DSGVO), soweit technisch möglich;
- Meldung von Verletzungen des Schutzes personenbezogener Daten an den Verantwortlichen unverzüglich, spätestens innerhalb von 72 Stunden nach Kenntniserlangung (Art. 33, 34 DSGVO);
- Unterstützung bei Datenschutz-Folgenabschätzungen (Art. 35 DSGVO), soweit erforderlich.

§ 7 Berichtigung, Löschung und Portabilität

Der Auftragsverarbeiter berichtigt, löscht oder sperrt Daten auf Weisung des Verantwortlichen. Die konfigurierbaren Löschrufen (Transkripte: 90 Tage, Audio: 30 Tage) werden automatisch durch das System umgesetzt. Der Verantwortliche kann Daten über das Dashboard jederzeit manuell löschen. Auf Anfrage des Verantwortlichen werden dessen Daten in einem gängigen, maschinenlesbaren Format herausgegeben.

Nach Beendigung des Hauptvertrags werden alle Kundendaten innerhalb von 90 Tagen unwiderruflich gelöscht, sofern keine gesetzlichen Aufbewahrungspflichten entgegenstehen.

§ 8 Datentransfer

Alle Kerndaten werden innerhalb der EU/des EWR verarbeitet. Soweit einzelne Unterauftragsverarbeiter Datenübermittlungen in Drittländer vornehmen, wird dies ausschließlich auf Basis geeigneter Garantien gemäß Art. 46 DSGVO abgesichert (insbesondere Standardvertragsklauseln).

§ 9 Vertraulichkeit

Der Auftragsverarbeiter stellt sicher, dass alle Personen, die Zugang zu personenbezogenen Daten haben, zur Vertraulichkeit verpflichtet sind.

§ 10 Kontrollrechte des Verantwortlichen

Der Verantwortliche ist berechtigt, die Einhaltung dieses AVV und der geltenden Datenschutzvorschriften zu kontrollieren. Kontrollen können durch Anforderung von Nachweisen (z. B. Zertifikate, Prüfberichte) oder – nach Ankündigung mit angemessener Frist – durch Vor-Ort-Prüfungen durchgeführt werden. Der Auftragsverarbeiter stellt alle erforderlichen Informationen zur Verfügung.

§ 11 Schlussbestimmungen

Dieser AVV ist Bestandteil des Hauptvertrags zwischen Verantwortlichem und Auftragsverarbeiter. Im Falle von Widersprüchen gehen die Regelungen dieses AVV vor. Änderungen bedürfen der Textform. Es gilt deutsches Recht.

Dieser AVV kommt mit Abschluss des Hauptvertrags (Registrierung auf app.one-ki.de und Akzeptanz der AGB) wirksam zustande. Einer gesonderten Unterzeichnung bedarf es nicht.

Marius Jonda (oneKI) | Nützenberger Str. 175, 42115 Wuppertal | info@one-ki.de