Auftragsverarbeitungsvereinbarung (AVV) – Anlage B: TOMs

Stand: März 2026

Technische und Organisatorische Maßnahmen (TOMs)

Der Datenimporteur (KiCo AI LLP) hat folgende Sicherheitsmaßnahmen implementiert, um die Vertraulichkeit, Integrität und Verfügbarkeit der verarbeiteten Daten zu gewährleisten:

Sicherheitsziel	Maßnahmenbeschreibung
Zutrittskontrolle	ISO 27001-zertifizierte Rechenzentren, betrieben von Hetzner Online GmbH (Falkenstein/Deutschland) sowie Amazon Web Services (AWS) für die Voice-AI-Plattform Retell AI Inc. Schutz vor unbefugtem physischem Zugang.
Zugangskontrolle	Strikte Rollen- und Rechteverwaltung nach dem Least-Privilege-Prinzip. Zwei-Faktor-Authentifizierung (2FA) für alle kritischen Zugriffe. Rollenbasierte Zugriffskontrolle (RBAC) bei allen eingesetzten Plattformen.
Weitergabekontrolle	Ende-zu-Ende-Verschlüsselung (VPN und TLS 1.3) bei jeglichem Zugriff oder Datentransfer, insbesondere durch Personal in Kanada und Indonesien. Verschlüsselung at rest und in transit bei allen Unterauftragsverarbeitern.
Eingabekontrolle	Protokollierung der Eingabe, Änderung und Löschung von Daten (Audit-Trails).
Verfügbarkeit	Regelmäßige Backups der Datenbestände (täglich/wöchentlich); etablierter Disaster Recovery Plan. Retell AI: 99,99% Uptime SLA.
Trennungsgebot	Logische Trennung der Kundendaten (Mandantenfähigkeit) auf den Servern. Multi-Tenant-Isolation bei Retell AI.
Datenschutzmanagement	Jährliche Datenschutzschulungen der Mitarbeiter. Benennung eines externen/internen Datenschutzkoordinators. Dokumentierte Prozesse zur Meldung von Datenschutzverletzungen.
Sprachdatenverarbeitung (NEU)	Temporäre Speicherung von Audiodaten ausschließlich für die Echtzeit-Sprachverarbeitung (STT/TTS). Langfristige Speicherung von Audioaufnahmen nur mit gesonderter Vereinbarung oder Einwilligung. Automatische Löschung gemäß konfigurierter Fristen. Transkripte: Speicherung gemäß vereinbarter Retention-Policy, automatische Löschung nach Ablauf. PII-Redaction: Automatische Entfernung von Namen, Adressen, Geburtsdaten, Passwörtern, PINs, SSNs, E-Mail-Adressen aus Transkripten und Aufnahmen (konfigurierbar pro Agent). Informationspflicht: Standardisierter Begrüßungshinweis zu Beginn jedes Anrufs.
Unterauftragsverarbeiter-Kontrolle (NEU)	Transfer Impact Assessment (TIA) für alle Nicht-EU-Unterauftragsverarbeiter. Regelmäßige Überprüfung der Sicherheitszertifizierungen (SOC 2 Type II, ISO 27001). Vertragliche Verpflichtung aller Unterauftragsverarbeiter zu gleichwertigen technischen und organisatorischen Maßnahmen. Überwachung der Unterauftragsverarbeiterlisten auf Änderungen.