

Anlage B — Technische und Organisatorische Maßnahmen (TOMs)

Auftragsverarbeitungsvereinbarung (AVV) — Anlage B

Stand: September 2026

Der Auftragnehmer (KiCo AI LLP) hat die folgenden Sicherheitsmaßnahmen nach Art. 32 DSGVO umgesetzt, um Vertraulichkeit, Integrität und Verfügbarkeit der verarbeiteten Daten zu gewährleisten.

Sicherheitsziel	Maßnahmenbeschreibung
Zutrittskontrolle	Nach ISO 27001 zertifizierte Rechenzentren, betrieben von Hetzner Online GmbH (Falkenstein, Deutschland) sowie Amazon Web Services für die Voice-AI-Plattform Retell AI Inc. Schutz vor unbefugtem physischem Zugang.
Zugangskontrolle	Strikte Rollen- und Rechteverwaltung nach dem Prinzip der geringsten Rechte. Zwei-Faktor-Authentifizierung für alle kritischen Zugriffe. Rollenbasierte Zugriffskontrolle bei allen eingesetzten Plattformen.
Weitergabekontrolle	Verschlüsselung mit TLS 1.3 während der Übertragung und AES 256 im Ruhezustand bei allen Unterauftragsverarbeitern. Jeglicher administrative Zugriff erfolgt ausschliesslich über verschlüsselte, vermittelte Verbindungen.
Zugriff aus Drittländern (neu)	Der Zugriff durch Personal des Auftragnehmers aus Kanada und Indonesien ist wie folgt begrenzt: kein unmittelbar aus dem Internet erreichbarer Dienst — der Zugang läuft ausschliesslich über ein privates, authentifiziertes Netz; jeder Zugriff wird protokolliert und ist einer Person zuordenbar; keine dauerhafte lokale Speicherung von Kundendaten auf Endgeräten; Verschlüsselung der Endgeräte; Rechtevergabe nach dem Prinzip der geringsten Rechte und Entzug bei Wegfall des Bedarfs. Diese Maßnahmen sind der tragende Schutz für den in Anlage D Abschnitt 5.2 beschriebenen Sachverhalt. Ein Tunnel oder VPN allein wird ausdrücklich nicht als Schutzmaßnahme gewertet — er ändert die Netzstrecke, nicht den Aufenthaltsort der zugreifenden Person.
Eingabekontrolle	Protokollierung von Eingabe, Änderung und Löschung der Daten (Audit-Trails).
Verfügbarkeit	Regelmäßige Backups der Datenbestände (täglich beziehungsweise wöchentlich); etablierter Disaster-Recovery-Plan. Für Retell AI besteht eine Verfügbarkeitszusage des Anbieters von 99,99% (Angabe des Anbieters, keine eigene Messung).
Trennungsgebot	Logische Trennung der Kundendaten (Mandantenfähigkeit) auf den Servern. Trennung der Kundenbestände bei Retell AI.
Datenschutzmanagement	Jährliche Datenschutzschulungen der Mitarbeiter. Benennung eines Datenschutzkoordinators. Dokumentierte Prozesse zur Meldung von Datenschutzverletzungen. Benennung eines Vertreters in der Union nach Art. 27 DSGVO als Kontaktstelle für betroffene Personen und Aufsichtsbehörden.
Sprachdatenverarbeitung	Temporäre Speicherung von Audiodaten ausschliesslich für die Echtzeit-Sprachverarbeitung. Langfristige Speicherung von Audioaufnahmen nur mit gesonderter Vereinbarung oder Einwilligung. Automatische Löschung gemäß konfigurierter Fristen. Transkripte: Speicherung gemäß vereinbarter Aufbewahrungsregel, automatische Löschung nach Ablauf. Automatische Entfernung personenbezogener Identifikatoren — Namen, Adressen, Geburtsdaten, Passwörter, PINs, Sozialversicherungsnummern, E-Mail-Adressen — aus Transkripten und Aufnahmen, konfigurierbar je Agent. Informationspflicht: standardisierter Hinweis auf den KI-Einsatz zu Beginn jedes Anrufs.
Wahl der Verarbeitungsstrecke (neu)	Für das Sprachmodell steht eine an die Region Frankfurt gebundene Strecke bereit. Die Bindung ist nicht konfiguriert, sondern technisch erzwungen : die Rechtebegrenzung des Kontos verweigert die US-Variante und die globale Variante des Modells aktiv. Bei erhöhtem Schutzbedarf ist diese Strecke zu wählen.

Sicherheitsziel	Maßnahmenbeschreibung
Unterauftragsverarbeiter-Kontrolle	Transfer Impact Assessment für alle Empfänger ausserhalb der EU (Anlage D, 22 Empfänger). Vertragliche Verpflichtung aller Unterauftragsverarbeiter zu gleichwertigen technischen und organisatorischen Maßnahmen. Überwachung der Unterauftragsverarbeiterlisten der Anbieter auf Änderungen.
Prüfung der Anbieter-Zertifizierungen (neu)	Halbjährliche Prüfung von SOC 2 Type II, ISO 27001 und der Zertifizierung im EU-US Data Privacy Framework, zusätzlich vor jeder Neufassung der Anlage C. Die Prüfung erfolgt gegen das amtliche Register und über den Rechtsträger, nicht über die Marke — Marke und Rechtsträger weichen regelmäßig voneinander ab, und eine Suche nach der Marke findet einen bestehenden Eintrag nicht. Ergebnis je Anbieter mit Status, Geltungsbereich, Ablaufdatum und offenen Inaktivzeiträumen dokumentiert. Erlischt eine Zertifizierung, tragen die Standardvertragsklauseln als Rückfallebene, und die betroffene Zeile der Anlage C wird berichtigt.