

Datenschutz-Folgenabschätzung (DSFA)

gemäß Art. 35 DSGVO

für den Einsatz von Voice-AI-Diensten mit Retell AI

Stand: März 2026

Erstellt von: KiCo AI LLP

Verantwortlich: Elliott Schweigert, Geschäftsführer

1. Beschreibung der Verarbeitung

1.1 Verarbeitungstätigkeit

Einsatz KI-gestützter Sprachagenten (Voice AI) zur automatisierten Anrufbearbeitung, Terminvereinbarung und Lead-Qualifizierung im Auftrag von Kunden (Verantwortliche) im DACH-Raum.

1.2 Zweck

Automatisierung eingehender und ausgehender Telefonanrufe mittels Sprach-KI. Die Voice Agents beantworten Kundenanfragen, buchen Termine, qualifizieren Leads und leiten relevante Informationen an die Systeme des Kunden weiter.

1.3 Datenfluss-Architektur

```

Anrufer → Telefonnummer (Twilio/SIP) → Retell AI (USA/AWS)      ↓      STT →
LLM (Azure OpenAI) → TTS      ↓      Webhook → n8n (KiCo)      ↓      CRM /
Kalender / E-Mail      ↓      Hetzner (EU/Deutschland)
  
```

Audioaufnahmen: Temporär bei Retell (konfigurierbar)

Transkripte: Bei Retell + via Webhook an KiCo-Systeme

Ergebnisdaten (Termine, Leads): EU-Infrastruktur (Hetzner)

1.4 Beteiligte Parteien

Verantwortlicher: Kunde (AG) im DACH-Raum

Auftragsverarbeiter: KiCo AI LLP, Vancouver, Kanada

Unterauftragsverarbeiter: Retell AI Inc. (USA), Twilio (Irland/USA), Hetzner (DE), Microsoft/Azure OpenAI (EU)

1.5 Kategorien betroffener Personen und Daten

Betroffene: Anrufer (Endkunden, Interessenten, Geschäftspartner des AG)

Datenkategorien: Name, Telefonnummer, Sprachdaten (Audio), automatisierte Transkripte, Anrufzeitpunkte/-dauer, Gesprächsinhalte in Textform, ggf. Adresse, Terminwünsche, Objektinteresse, Fahrzeugdaten, Berufserfahrung (branchenabhängig).

Besondere Kategorien (Art. 9 DSGVO): Grundsätzlich NEIN. In Ausnahmefällen könnte im Recruiting-Kontext (PERSOX GmbH) Berufserfahrung Hinweise auf besondere Kategorien enthalten.

2. Notwendigkeit und Verhältnismäßigkeit

Die Verarbeitung ist für die Erbringung der vertraglich vereinbarten Voice-AI-Dienstleistungen erforderlich (Art. 6 Abs. 1 lit. b DSGVO bzw. berechtigtes Interesse Art. 6 Abs. 1 lit. f DSGVO des Kunden). Ohne Sprachverarbeitung ist der Dienst technisch nicht erbringbar.

Datenminimierung: PII-Redaction entfernt Kernidentifikatoren aus Transkripten und Aufnahmen. Audio wird nur bei expliziter Konfiguration persistent gespeichert. Transkripte unterliegen konfigurierbaren Retention-Fristen.

Verhältnismäßigkeit der US-Verarbeitung: Die Nutzung von Retell AI ist alternativlos für die gewünschte Qualität und Latenz (~600ms). Kein vergleichbarer EU-Anbieter bietet dieselbe Funktionalität und Sprachqualität.

3. Risikobewertung

Risiko	Eintrittswahrsch.	Schwere	Stufe	Maßnahme
Unbefugter Zugriff auf Sprachdaten bei Retell	Gering	Mittel	MITTEL	SOC 2 Type II, Verschlüsselung, RBAC, PII-Redaction
US-Behördenzugriff (FISA 702, Cloud Act)	Gering	Mittel	MITTEL	SCCs Modul 3, TIA, keine besonderen Datenkategorien, PII-Redaction
Datenverlust bei Übertragung	Sehr gering	Gering	NIEDRIG	TLS 1.3, AWS-Redundanz, 99,99% Uptime
Fehlerhafte Transkription	Mittel	Gering	NIEDRIG	Bestätigungslogik, Kundenverifikation
Fehlende Information des Anrufers	Gering	Mittel	MITTEL	Standardisierter Begrüßungshinweis
Unzulässig lange Speicherung	Gering	Mittel	MITTEL	Konfigurierte Fristen, automatische Löschung
Re-Identifizierung nach PII-Redaction	Sehr gering	Gering	NIEDRIG	PII-Redaction entfernt Kernidentifikatoren
Prompt Injection / Missbrauch	Gering	Gering	NIEDRIG	Guardrails, keine Zahlungsauslösung möglich

4. Maßnahmen zur Risikominderung

4.1 Vertragliche Maßnahmen

- DPA mit Retell AI unterzeichnet (Self-Service unter <https://click-agreements.retellai.com/>)
- SCCs Modul 3 (Processor to Processor) für den US-Transfer
- Transfer Impact Assessment (TIA) für die USA durchgeführt
- Aktualisierte AVV mit transparenter Ausweisung des US-Transfers
- Aktualisierte Anlage C mit vollständiger Unterauftragsverarbeiterliste

4.2 Technische Maßnahmen

- PII-Redaction bei Retell für alle Agenten aktiviert
- Verschlüsselung: End-to-End, at rest und in transit
- SOC 2 Type II Zertifizierung bei Retell AI
- RBAC (rollenbasierte Zugriffskontrolle)
- Multi-Tenant-Isolation
- Audioaufnahme-Retention konfiguriert (temporär = Standard)
- Automatische Löschung nach konfigurierten Fristen

4.3 Organisatorische Maßnahmen

- Standardisierter Begrüßungshinweis in allen Voice Agents
- Regelmäßige Überprüfung der Sicherheitszertifizierungen
- Überwachung der Retell-Unterauftragsverarbeiterliste auf Änderungen
- Muster-Datenschutzerklärung für Kunden
- Jährliche Datenschutzs Schulungen

5. Gesamtergebnis

ERGEBNIS: AKZEPTABLES RESTRISIKO

Begründung:

1. Keine besonderen Kategorien personenbezogener Daten (Art. 9 DSGVO) werden systematisch verarbeitet.
2. Keine Zahlungsdaten über Voice AI.
3. Kein aktiver Verkauf – nur Information, Termine, Lead-Qualifizierung.
4. SOC 2 Type II Zertifizierung bei Retell AI.
5. PII-Redaction verfügbar und aktiviert.
6. SCCs Modul 3 und TIA für US-Transfer implementiert.
7. Überwiegend allgemeine Kontaktdaten mit geringem Schadenspotenzial.

Konsultation der Aufsichtsbehörde (Art. 36 DSGVO):

NICHT ERFORDERLICH – das verbleibende Risiko wurde durch die oben beschriebenen Maßnahmen auf ein akzeptables Niveau gesenkt.

6. Überprüfung

Diese DSFA wird spätestens alle 12 Monate oder bei wesentlichen Änderungen der Verarbeitungstätigkeit (z.B. neue Unterauftragsverarbeiter, Ungültigerklärung des EU-US DPF, Änderung der Retell-Infrastruktur) überprüft.

Vancouver, den 10.03.2026



Elliott Schweigert, Geschäftsführer KiCo AI LLP