

Transfer Impact Assessment (TIA)

Bewertung von Drittlandübermittlungen gemäß Art. 44 ff. DSGVO, EDPB-Empfehlungen 01/2020

Auftragsverarbeiter	Felix Oskar Griebeler
Kontakt	felix@griebeler.eu
Geltungsbereich	Bewertung der Drittlandübermittlungen im Rahmen der Bereitstellung eines KI-gestützten telefonischen Rezeptionisten für Betriebe des SHK-Handwerks (Sanitär, Heizung, Klima)
Stand / Version	07.07.2026 – Version 1.1
Referenzdokumente	Verzeichnis von Verarbeitungstätigkeiten (VVT), Version 1.10 · Auftragsverarbeitungsvertrag (AVV), Version 1.6 · Technische und organisatorische Maßnahmen (TOM), Version 1.1
Einbindung	Dieses Dokument dient als Referenzdokument zur Auftragsverarbeitungsvereinbarung (AVV) und wird gesondert bereitgestellt.

1. Einleitung und Methodik

Dieses Dokument bewertet, ob die im Verzeichnis von Verarbeitungstätigkeiten (VVT) dokumentierten Übermittlungen personenbezogener Daten in Drittländer durch geeignete Garantien im Sinne von Art. 46 DSGVO abgesichert sind, und ob ergänzende Maßnahmen erforderlich sind. Rechtsgrundlage sind Art. 44 bis 49 DSGVO, insbesondere Art. 46 Abs. 2 lit. c (Standardvertragsklauseln) und Art. 45 DSGVO (Angemessenheitsbeschluss).

Die Bewertung folgt der sechsstufigen Methodik der Empfehlungen 01/2020 des Europäischen Datenschutzausschusses (EDPB) zu Maßnahmen zur Ergänzung von Übermittlungsinstrumenten (Kenntnis der Übermittlungen, Bestimmung des Übermittlungsinstruments, Bewertung des Rechtsrahmens im Drittland, Identifizierung ergänzender Maßnahmen, formale Umsetzung, regelmäßige Neubewertung).

Gegenstand dieser TIA sind die Übermittlungen an Twilio Inc./Twilio Ireland Ltd., Retell AI, Inc. und OpenAI Ireland Ltd. Nicht Gegenstand dieser TIA sind n8n (EU-Verarbeitung, kein Drittlandbezug) und cal.eu/Cal.com, Inc.; Letzteres wird gesondert in Abschnitt 8 behandelt, da hierfür nach Auffassung der Datenschutzkonferenz (DSK) kein klassischer Art.-46-Transfer, sondern eine Eignungsprüfung nach Art. 28 Abs. 1 DSGVO einschlägig ist.

Diese TIA ersetzt keine Rechtsberatung. Sie dokumentiert eine eigenverantwortliche Risikoeinschätzung zum Stand 07.07.2026 auf Basis der zu diesem Zeitpunkt verfügbaren Informationen und wird gemäß Abschnitt 7 regelmäßig neu bewertet.

2. Schritt 1 – Kenntnis der Übermittlungen

Die folgende Tabelle fasst sämtliche im Rahmen der Leistungserbringung stattfindenden Datenflüsse in Drittländer zusammen, unter Bezugnahme auf die in der VVT dokumentierten Tätigkeiten.

Empfänger	Verarbeitungsort	Rolle / Funktion	Bezug VVT	Art der Daten
Twilio Inc. / Twilio Ireland Ltd.	USA	Telefonie-Infrastruktur, SMS-Versand	Tätigkeit 1, 3, 4	Anrufmetadaten, Telefonnummern, SMS-Inhalt

Retell AI, Inc.	USA (angenommen; AWS-Region nicht abschließend bestätigt)	KI-Sprachagent- Plattform	Tätigkeit 1, 5	Vollständiges Gespräch (Audio, Transkript) vor Redaction
OpenAI Ireland Ltd.	Weiterleitung an nicht-EWR- Konzerngesellschaften	Sprachmodell (SMS- Texterstellung)	Tätigkeit 3	Vollständiges, unredactetes Transkript
OpenAI Ireland Ltd.	s. o.	Sprachmodell (Verfügbarkeitsabfrage)	Tätigkeit 2	Abstrakte Verfügbarkeitsdaten – kein Personenbezug (kein Transfer i. S. d. Art. 44 ff.)

Ergänzend eingesetzt, aber nicht eigener Subunternehmer des Auftragsverarbeiters: Microsoft Azure (Transkription), ElevenLabs (Sprachsynthese) und OpenAI (Dialoggenerierung im Rahmen von Tätigkeit 1) – alle drei von Retell AI im Rahmen des eigenen Verarbeitungsverhältnisses als Sub-Subunternehmer beauftragt und verantwortet (siehe AVV Ziffer 7, TOM Abschnitt 1.1). Die beiden OpenAI-Ireland-Ltd.-Zeilen in der obigen Tabelle betreffen ausschließlich die direkte Nutzung durch den Auftragsverarbeiter selbst (eigener API-Key, Tätigkeit 2 und 3) – nicht diese Retell-interne Dialoggenerierung, die als Sub-Sub-Verhältnis separat zu betrachten ist, auch wenn dieselbe Vertragsentität beteiligt ist. Da die Daten faktisch dennoch über diese Systeme laufen, werden alle drei (Azure, ElevenLabs und OpenAI in dieser Rolle) nachrichtlich in Schritt 2, 3 und 9 mitbehandelt.

3. Schritt 2 – Bestimmung der Übermittlungsinstrumente

Anbieter	Instrument	Status / Anmerkung
Twilio Inc. / Twilio Ireland Ltd.	EU-US Data Privacy Framework (primär); Binding Corporate Rules und Standardvertragsklauseln (nachrangig)	DPF-Zertifizierung aktiv; Rangfolge vertraglich in Twilios eigenem DPA verankert
Retell AI, Inc.	Standardvertragsklauseln, Modul 2, Governing Law Irland	Keine aktive DPF-Zertifizierung; Retells DPA sieht in Schedule 3 Ziffer 5 vor, dass eine künftige DPF-Zertifizierung die SCC-Notwendigkeit entfallen ließe – bislang nicht der Fall
OpenAI Ireland Ltd.	Standardvertragsklauseln oder Angemessenheitsbeschluss (Art. 45 DSGVO)	Laut OpenAI-DPA Ziffer 4.1 wahlweise SCC oder EU-Angemessenheitsbeschluss; im AVV vollständig dokumentiert
ElevenLabs (Sub-Sub von Retell AI)	EU-US Data Privacy Framework (aktiv) und Standardvertragsklauseln	Standard-Tarif, USA-Hosting; EU-Datenresidenz nur im Enterprise-Tier verfügbar
Microsoft Azure (Sub-Sub von Retell AI)	Unbekannt	Region und Übermittlungsinstrument nicht bestätigt

OpenAI (Sub-Sub von Retell AI, Tätigkeit 1)	Unbekannt	Eigene Vertragskette Retell AI–OpenAI, dem Auftragsverarbeiter nicht im Volltext vorliegend; vermutlich analog zur direkten OpenAI-Übermittlung (SCC/Angemessenheitsbeschluss), nicht bestätigt
---	-----------	---

4. Schritt 3 – Bewertung des Rechtsrahmens im Drittland (USA)

4.1 Allgemeiner rechtlicher Rahmen

Für sämtliche US-Übermittlungen ist der Rechtsrahmen nach den European Essential Guarantees des EDPB zu prüfen: FISA Section 702 (Massenzugriff durch Nachrichtendienste), Executive Order 14086 mit dem zweistufigen Rechtsbehelfsmechanismus (CLPO und Data Protection Review Court), sowie der CLOUD Act (Zugriff auf Daten unter Kontrolle eines US-Unternehmens unabhängig vom Speicherort).

Der EU-US-Angemessenheitsbeschluss (DPF) gilt zum Stand dieses Dokuments formal fort. Das Gericht der Europäischen Union hat ihn am 03.09.2025 im Verfahren Latombe (T-553/23) bestätigt; ein Rechtsmittel ist beim EuGH anhängig (C-703/25 P), ein Entscheidungstermin steht nicht fest. Am 29.06.2026 hat der US Supreme Court in Trump v. Slaughter die strukturelle Unabhängigkeit unabhängiger US-Behörden von präsidialer Entlassungsbefugnis für verfassungswidrig erklärt, was strukturell auch das Privacy and Civil Liberties Oversight Board (PCLOB) betrifft. NOYB hat die EU-Kommission am 30.06.2026 schriftlich zum Widerruf des Angemessenheitsbeschlusses aufgefordert. Der DPF ist damit aktuell eine gültige, aber instabile Übermittlungsgrundlage; für jede DPF-gestützte Übermittlung sollte eine SCC-Rückfalloption vertraglich vorgehalten werden.

4.2 Datensensibilität und Verhältnismäßigkeit

Die im Rahmen der Verarbeitung anfallenden Daten (Name, Telefonnummer, Adresse, Anliegenbeschreibung) sind für sich genommen kein typisches Ziel nachrichtendienstlicher Massenüberwachung, was das abstrakte Zugriffsrisiko im Rahmen der Verhältnismäßigkeitsprüfung mindert.

Risikoerhöhender Faktor: Bei Tätigkeit 3 wird das vollständige, nicht redactete Gesprächstranskript an OpenAI übermittelt (bestätigt). Die bei Retell AI umgesetzte PII-Redaction (TOM, Kategorie 2) betrifft ausschließlich die dort gespeicherte Kopie, nicht den an OpenAI übergebenen Input. Enthält ein Gespräch besondere Kategorien personenbezogener Daten (z. B. Gesundheits- oder Finanzangaben, die ein Anrufer von sich aus nennt), gelangen diese unredactet zu OpenAI. Risikomindernd wirken hierbei: OpenAI verarbeitet die Daten vertraglich ausschließlich zur Leistungserbringung ohne Zweckänderung (OpenAI-DPA Ziffer 1.2, 5.1), und die Speicherfrist ist auf 30 Tage begrenzt – bezieht sich dabei jedoch sowohl auf Input als auch Output (VVT, Tätigkeit 3), nicht nur auf den Output. Ergänzend bestätigt sich dieselbe optimistische Grundannahme auch in Retells eigener DPA (Schedule 1: „Sensitive Categories of Data: N/A“), obwohl auch Retell das vollständige Gespräch vor Redaction verarbeitet – dies untermauert den bereits benannten Risikopunkt, ist aber kein neuer, eigenständiger Befund.

4.3 Einzelbewertung je Anbieter

Anbieter	Rechtsrahmen-Bewertung
Twilio	DPF-Zertifizierung aktiv und rechtlich fortgeltend; SCC/BCR als Rückfall vertraglich abgesichert. Verarbeitete Daten (Anrufmetadaten, SMS-Text) von geringer Sensibilität.
Retell AI	Ausschließlich SCC als Grundlage, keine DPF-Absicherung. Verarbeitet das vollständige, noch nicht redactete Gespräch – höchste Datensensibilität aller Übermittlungen. Verarbeitungsort (AWS-Region) nicht bestätigt.

OpenAI (Tätigkeit 3)	SCC bzw. wahlweise Angemessenheitsbeschluss. Erhält unredactetes Transkript (siehe 4.2); vertraglich keine Zweckänderung, 30-Tage-Frist für Input und Output.
OpenAI (Tätigkeit 2)	Kein Transfer personenbezogener Daten – Rechtsrahmen-Bewertung insoweit nicht einschlägig.
ElevenLabs (Sub-Sub)	DPF und SCC vorhanden; Verantwortung liegt bei Retell AI. Verarbeitet Sprachausgabertext, keine strukturierten Anruferdaten.
Azure (Sub-Sub)	Nicht bewertbar – Region und Instrument unbestätigt.
OpenAI (Sub-Sub, Tätigkeit 1)	Nicht direkt bewertbar – eigene Vertragskette Retell AI–OpenAI, dem Auftragsverarbeiter nicht vorliegend. Verantwortung liegt vertraglich bei Retell AI (Art. 28 Abs. 4 DSGVO); verarbeitet laufenden Gesprächsinhalt in Echtzeit, analog zur Datensensibilität bei Retell AI selbst.

5. Schritt 4 – Ergänzende Maßnahmen

5.1 Bereits vorhandene Maßnahmen (Bezug TOM-Dokument)

- Kategorie 2 (Pseudonymisierung): automatisierte PII-Redaction der bei Retell AI gespeicherten Gesprächskopie (Platzhalter im Transkript, akustische Überdeckung in der Audioaufzeichnung).
- Kategorie 3 (Verschlüsselung): vertraglich zugesicherte Verschlüsselung in transit/at rest bei allen Subunternehmern; eigene TLS/HTTPS-Absicherung sämtlicher API/Webhook-Verbindungen; Header-Token-Authentifizierung zwischen Retell AI und n8n.
- Kategorie 4 (Zugriffsschutz): MFA bei Twilio, n8n, OpenAI und cal.eu; bei Retell AI kompensierend ein besonders langes, einzigartiges Passwort mangels MFA-Option; FileVault-Verschlüsselung des Verwaltungsgeräts.
- Kategorie 7 (Wirksamkeitsprüfung): jährliche Prüfung der SOC-2-Type-II-Zertifizierung sämtlicher Subunternehmer.
- Kategorie 10 (Löschfristen): kurze, plattformseitig automatisierte Speicherfristen (Retell AI 7 Tage; OpenAI 30 Tage für Input und Output; Twilio 13 Monate für SMS-Inhalte).

5.2 Einordnung nach EDPB-Kategorisierung

Die vorgenannten Maßnahmen wirken überwiegend risikomindernd bzw. schadensbegrenzend (Reduktion der Auswirkungen im Falle eines behördlichen Zugriffs), nicht als vollständige Zugriffsverhinderung. Eine Zugriffsverhinderung im engeren EDPB-Sinn würde eine exporteurseitig exklusiv kontrollierte Verschlüsselung voraussetzen; dies ist mangels eigener Serverinfrastruktur und angesichts der Notwendigkeit der Klartext-Verarbeitung durch die eingesetzten KI-Dienste nicht umsetzbar. Diese Einschränkung ist als strukturelles Restrisiko zu dokumentieren, nicht als Versäumnis.

5.3 Vertragliche Maßnahmen (ergänzend aus den Subunternehmer-DPAs)

OpenAI-DPA:

- Benachrichtigungspflicht bei behördlichen Herausgabeersuchen, soweit rechtlich zulässig (Ziffer 2.2).
- Auditrecht des Auftragsverarbeiters, bis zu einmal jährlich (Ziffer 2.8).
- Transparente, laufend aktualisierte Sub-Processor-Liste (Ziffer 2.9, platform.openai.com/subprocessors).

Retell-AI-DPA:

- Feste Meldefrist von 48 Stunden bei Sicherheitsvorfällen („Specified Notice Period“, Ziffer 1.19) – konkreter und kürzer gefasst als bei OpenAI („without undue delay“).
- SOC-2-Type-II-Bericht als primärer, vertraglich verankerter Prüfmechanismus; Auditrecht erst subsidiär bei Nichtvorlage oder Mängeln (Ziffer 9.3).
- Vertraglich vorgesehene DPF-Option (Schedule 3, Ziffer 5): Sollte Retell künftig eine aktive DPF-Zertifizierung erlangen, gälte die Übermittlung nicht mehr als Restricted Transfer.

5.4 Bewertete Lücken

- Keine exporteurseitig kontrollierte Verschlüsselung möglich (SaaS-Abhängigkeit ohne eigene Infrastruktur).
- Die Redaction bei Retell AI schützt nur die dort gespeicherte Kopie, nicht den an OpenAI übermittelten Input bei Tätigkeit 3 – akzeptiertes Restrisiko, siehe 4.2.
- Verarbeitungsort von Azure (Sub-Sub) unbestätigt, dadurch keine abschließende Bewertung möglich.

Es werden keine weiteren, derzeit umsetzbaren ergänzenden Maßnahmen identifiziert, die über die in 5.1 und 5.3 dokumentierten hinausgehen. Das verbleibende Risiko wird als Restrisiko dokumentiert und akzeptiert (siehe Abschnitt 9).

6. Schritt 5 – Formale Umsetzung

Die identifizierten Übermittlungsinstrumente sind in der AVV-Subunternehmer-Übersicht sowie in der VVT-Drittland-Tabelle (Art. 30 Abs. 2 lit. c DSGVO) dokumentiert. Der OpenAI-DPA ist unterzeichnet (Signatur 13.06.2026). Der Retell-AI-DPA liegt vor und wurde ausgewertet (Governing Law und zuständiger Mitgliedstaat: Irland; SCC Modul 2; 48-Stunden-Meldefrist bei Sicherheitsvorfällen); die konkrete AWS-Verarbeitungsregion und die vollständige Subprocessor-Liste ergeben sich daraus jedoch nicht und bleiben unbestätigt. Die DPF-Zertifizierung von Twilio wurde extern verifiziert.

Ein externer Datenschutzbeauftragter ist noch nicht bestellt (siehe VVT und AVV); die Datenschutz-Folgenabschätzung nach Art. 35 DSGVO steht noch aus und ist vor dem ersten Kunden-Onboarding durchzuführen. Diese TIA dient dieser DSFA als Zulieferdokument für den Bereich Drittlandtransfers.

7. Schritt 6 – Regelmäßige Neubewertung

Diese TIA wird bei Eintritt eines der folgenden Ereignisse zeitnah neu bewertet, unabhängig von der jährlichen Regelüberprüfung:

- Entscheidung des EuGH im Verfahren C-703/25 P über den EU-US-Angemessenheitsbeschluss.
- Weitere strukturelle Entwicklungen beim PCLOB oder der Anwendung von Executive Order 14086.
- Bestätigung der tatsächlichen AWS-Verarbeitungsregion von Retell AI, z. B. über die Subprocessor-Liste unter trust.retellai.com/subprocessors.
- Erlangung einer aktiven DPF-Zertifizierung durch Retell AI (vgl. Schedule 3, Ziffer 5 der Retell-AI-DPA).
- Hinzuziehung, Austausch oder Änderung der Konfiguration eines der bewerteten Subunternehmer.

Unabhängig davon erfolgt eine jährliche Regelüberprüfung im Rahmen der in TOM-Kategorie 7 dokumentierten Zertifizierungsprüfung der Subunternehmer.

8. Sonderfall cal.eu / Cal.com, Inc.

Cal.com, Inc. hat als Unternehmen seinen Sitz in den USA; die Datenverarbeitung im Rahmen von cal.eu ist jedoch vertraglich auf EU-Datenresidenz beschränkt. Nach dem Beschluss der

Datenschutzkonferenz (DSK) vom 31.01.2023 begründet die bloße konzernrechtliche Beherrschung eines Auftragsverarbeiters durch ein US-Mutterunternehmen für sich genommen noch keinen Drittlandtransfer im Sinne von Art. 44 ff. DSGVO, sofern die Verarbeitung selbst faktisch innerhalb der EU stattfindet. Ein formales TIA-Verfahren nach Art. 46 DSGVO ist für cal.eu daher nach dieser Auffassung nicht zwingend erforderlich.

Die abstrakte Zugriffsmöglichkeit über den CLOUD Act (Herausgabeanspruch gegenüber der US-Muttergesellschaft unabhängig vom Speicherort) sowie ein etwaiges Weisungsrisiko der US-Mutter sind gleichwohl im Rahmen der Eignungsprüfung des Auftragsverarbeiters nach Art. 28 Abs. 1 DSGVO zu berücksichtigen – als gesonderter Prüfpunkt außerhalb dieser TIA. Es wird empfohlen, diesen Punkt im Rahmen der noch ausstehenden Datenschutz-Folgenabschätzung (Art. 35 DSGVO) aufzugreifen.

9. Zusammenfassende Risikotabelle und Gesamtergebnis

Anbieter	Instrument	Datensensibilität	Restrisiko	Bewertung
Twilio	DPF + SCC/BCR	Gering	Gering	Angemessen
Retell AI	SCC	Erhöht (volles Gespräch)	Mittel – Region unbestätigt	Angemessen unter Vorbehalt der Regionsbestätigung
OpenAI (Tätigkeit 3)	SCC / Angemessenheitsbeschluss	Mittel–erhöht (unredacted Input)	Mittel – akzeptiertes Restrisiko	Angemessen, dokumentiert akzeptiert
OpenAI (Tätigkeit 2)	n. z.	Kein Personenbezug	Keines	Kein Transfer i. S. d. Art. 44 ff.
ElevenLabs (Sub-Sub)	DPF + SCC	Gering	Gering	Angemessen (Verantwortung bei Retell AI)
Azure (Sub-Sub)	Unbekannt	Unbekannt	Unbekannt	Offen
OpenAI (Sub-Sub, Tätigkeit 1)	Unbekannt	Erhöht (Echtzeit-Dialoginhalt)	Nicht direkt bewertbar	Offen (Instrument unbestätigt; Verantwortung bei Retell AI)

Gesamtergebnis: Die bewerteten Übermittlungen sind auf Basis der zum Stand 07.07.2026 bekannten Fakten überwiegend durch geeignete Garantien abgesichert. Das Restrisiko bei Retell AI und bei der OpenAI-Übermittlung im Rahmen von Tätigkeit 3 wird als akzeptabel eingestuft, insbesondere aufgrund der kurzen Speicherfristen, der fehlenden Zweckänderung und der strukturellen Mandantentrennung – dies stellt jedoch eine bewusste unternehmerische Risikoentscheidung dar und keine Beseitigung des Restrisikos. Die tatsächliche AWS-Verarbeitungsregion von Retell AI sowie die Verarbeitungsregion von Microsoft Azure sind unbestätigt und sollten vor dem ersten Kunden-Onboarding geklärt werden. Diese TIA wird gemäß Abschnitt 7 bei Eintritt der dort genannten Ereignisse aktualisiert.