

Transfer Impact Assessment (TIA)

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

Auftragsverarbeiter	Felix Oskar Griebeler
Kontakt	felix@kalendria.org
Geltungsbereich	Bewertung der Drittlandübermittlungen im Rahmen der Bereitstellung eines KI-gestützten telefonischen Rezeptionisten (Telefonassistent) für Betriebe des SHK-Handwerks (Sanitär, Heizung, Klima)
Stand / Version	10.10.2026 – Version 1.2
Referenzdokumente	VVT Absatz 2 · Auftragsverarbeitungsvertrag (AVV), Version 1.8 · Technische und organisatorische Maßnahmen (TOM), Version 1.2 · Datenschutz-Folgenabschätzung (Vorlage), Version 2.0
Einbindung	Anlage 3 zum Auftragsverarbeitungsvertrag (AVV), Version 1.8; wird als gesondertes Dokument bereitgestellt.

1. Einleitung und Methodik

Dieses Dokument bewertet, ob die im VVT Absatz 2 dokumentierten Übermittlungen personenbezogener Daten in Drittländer durch geeignete Garantien abgesichert sind und ob ergänzende Maßnahmen erforderlich sind. Rechtsgrundlage sind Art. 44 bis 49 DSGVO, insbesondere Art. 45 (Angemessenheitsbeschluss), Art. 46 Abs. 2 lit. c (Standardvertragsklauseln) und Art. 47 DSGVO (verbindliche interne Datenschutzvorschriften).

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 – soweit der Auftraggeber die Benachrichtigung per E-Mail wählt – Google Ireland Limited (Google Workspace). OpenAI wird seit Version 1.2 nicht mehr direkt eingesetzt, sondern nur noch als Sub-Subunternehmer von Retell AI. 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 10.10.2026 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 im VVT Absatz 2 dokumentierten Tätigkeiten.

Empfänger	Verarbeitungsort	Rolle / Funktion	Bezug VVT	Art der Daten
Twilio Inc. / Twilio Ireland Ltd.	USA (Anrufsteuerung); Sprachübertragung über Frankfurt am Main	Rufnummer, Telefonverbindung, Weiterleitung, SMS-Versand	Tätigkeit 1, 3, 4	Verbindungsdaten (Rufnummern, Zeitpunkt, Dauer), Sprachübertragung, bei SMS-Weg SMS-Inhalt
Retell AI, Inc.	USA (AWS; laut Retell keine EU-Verarbeitung)	KI-Sprachplattform	Tätigkeit 1 bis 5	Laufendes Gespräch (Audio, Text) in Echtzeit; Verbindungsdaten; Bereinigung der Mitschrift
Google Ireland Limited (Google Workspace)	USA möglich (Google LLC)	Versand von E-Mails an den Auftraggeber	Tätigkeit 3 (nur E-Mail-Weg)	Name, Telefonnummer, Anliegen, ggf. Adresse und Termin

Ergänzend eingesetzt, aber nicht eigene Subunternehmer des Auftragsverarbeiters: Microsoft Azure (Spracherkennung), ElevenLabs (Sprachsynthese) und OpenAI (Sprachmodell für Gesprächsführung und Auswertung nach dem Gespräch) – alle drei von Retell AI im Rahmen des eigenen Verarbeitungsverhältnisses als Sub-Subunternehmer beauftragt und verantwortet (siehe AVV Ziffer 7, TOM Abschnitt 1.1). Da die Daten faktisch über diese Systeme laufen, werden sie 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
Google Ireland Limited (Google Workspace)	EU-US Data Privacy Framework (Google LLC); Standardvertragsklauseln im Zusatz zur Datenverarbeitung	Zusatz zur Datenverarbeitung (Cloud Data Processing Addendum) am 10.10.2026 akzeptiert

Anbieter	Instrument	Status / Anmerkung
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)	Unbekannt	Eigene Vertragskette Retell AI–OpenAI, dem Auftragsverarbeiter nicht im Volltext vorliegend; 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 (Zugriff 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). 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 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.

Retell AI verarbeitet das vollständige Gespräch in Echtzeit, einschließlich etwaiger besonderer Kategorien, die ein Anrufer von sich aus nennt (z. B. Gesundheitsangaben). Mitschrift und Aufnahme werden dort jedoch nicht dauerhaft gespeichert („Basic Attributes Only“); nach dem Gespräch entfernt Retell AI Namen, Rufnummern, Adressen und vergleichbare Angaben, und nur diese bereinigte Fassung gelangt in das Qualitätsarchiv bei n8n in der EU. Gegenüber Version 1.1 entfällt die direkte Übermittlung vollständiger, unbereinigter Mitschriften an OpenAI zur SMS-Erstellung. Retells eigene DPA geht von „Sensitive Categories of Data: N/A“ aus; dies bleibt eine optimistische Grundannahme.

Die Benachrichtigungs-E-Mails an den Auftraggeber enthalten Name, Telefonnummer und Anliegen in Klartext. Sie liegen 30 Tage im Versandkonto von Kalendria und werden danach automatisch in den Papierkorb verschoben (endgültige Löschung nach höchstens weiteren 30 Tagen); ein Speicherort ausschließlich in der EU ist dabei nicht festgelegt.

4.3 Einzelbewertung je Anbieter

Anbieter	Rechtsrahmen-Bewertung
Twilio	DPF-Zertifizierung aktiv und rechtlich fortgeltend; SCC/BCR als Rückfall vertraglich abgesichert. Verarbeitete Daten (Verbindungsdaten, Sprachübertragung, SMS-Text) von geringer Sensibilität; Verbindungsdaten werden nach 40 Tagen, SMS nach 7 Tagen gelöscht.
Retell AI	Ausschließlich SCC als Grundlage, keine DPF-Absicherung. Verarbeitet das laufende Gespräch – höchste Datensensibilität aller Übermittlungen –, speichert Mitschrift und Aufnahme aber nicht dauerhaft. Verarbeitungsort laut Retell: AWS in den USA.
Google	DPF (Google LLC) und SCC. Erhält Benachrichtigungen mit Klartextdaten nur, wenn der Auftraggeber den E-Mail-Weg wählt; Speicherdauer begrenzt (30 Tage, danach Papierkorb).
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)	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.

5. Schritt 4 – Ergänzende Maßnahmen

5.1 Bereits vorhandene Maßnahmen (Bezug TOM-Dokument)

- Kategorie 2 (Pseudonymisierung): keine dauerhafte Speicherung von Mitschrift und Aufnahme bei Retell AI; automatische Bereinigung der Mitschrift; Qualitätsarchiv nur in bereinigter Form in der EU.
- Kategorie 3 (Verschlüsselung): vertraglich zugesicherte Verschlüsselung in transit/at rest bei allen Subunternehmern; eigene TLS/HTTPS-Absicherung sämtlicher API-/Webhook-Verbindungen; Header-Token-Authentifizierung der Funktionsaufrufe zwischen Retell AI und n8n.
- Kategorie 4 (Zugriffsschutz): MFA bei Twilio, n8n, cal.eu und Google Workspace; bei Retell AI kompensierend ein besonders langes, einzigartiges Passwort mangels MFA-Option; FileVault-Verschlüsselung des Verwaltungsgeräts.
- Kategorie 7 (Wirksamkeitsprüfung): jährliche Prüfung der Sicherheitsnachweise sämtlicher Subunternehmer.
- Kategorie 10 (Löschfristen): kurze, automatisch durchgesetzte Speicherfristen (Retell AI 7 Tage für Verbindungsdaten; Twilio 40 Tage für Verbindungsdaten und 7 Tage für SMS, Sicherungskopien abgeschaltet; gesendete E-Mails 30 Tage, danach Papierkorb).

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)

Retell-AI-DPA:

- Feste Meldefrist von 48 Stunden bei Sicherheitsvorfällen („Specified Notice Period“, Ziffer 1.19).
- 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.

Google Workspace:

- Zusatz zur Datenverarbeitung (Cloud Data Processing Addendum, akzeptiert am 10.10.2026) einschließlich Standardvertragsklauseln; Google LLC ist nach dem EU-US Data Privacy Framework zertifiziert.

5.4 Bewertete Lücken

- Keine exporteurseitig kontrollierte Verschlüsselung möglich (SaaS-Abhängigkeit ohne eigene Infrastruktur).
- Retell AI verarbeitet das laufende Gespräch in den USA ohne DPF-Absicherung; es besteht keine EU-Verarbeitungsoption.
- Benachrichtigungs-E-Mails liegen bis zur Löschung in Klartext im Google-Konto; ein Speicherort ausschließlich in der EU ist nicht festgelegt.
- 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). Wer die Übermittlung an Google vermeiden möchte, kann als Benachrichtigungsweg SMS wählen.

6. Schritt 5 – Formale Umsetzung

Die identifizierten Übermittlungsinstrumente sind in der Subunternehmer-Übersicht des AVV (Anlage 1) sowie in der Drittland-Tabelle des VVT Absatz 2 (Art. 30 Abs. 2 lit. c DSGVO) dokumentiert. Der Retell-AI-DPA liegt vor und wurde ausgewertet (Governing Law und zuständiger Mitgliedstaat: Irland; SCC Modul 2; 48-Stunden-Meldefrist bei Sicherheitsvorfällen); laut Retell erfolgt die Verarbeitung auf AWS in den USA, eine EU-Verarbeitung wird nicht angeboten (geprüft am 09.10.2026). Die DPF-Zertifizierung von Twilio wurde extern verifiziert. Der Zusatz zur Datenverarbeitung von Google (Cloud Data Processing Addendum) wurde am 10.10.2026 akzeptiert. Die Vereinbarung mit OpenAI ist seit Version 1.2 nicht mehr Grundlage einer Übermittlung.

Ein externer Datenschutzbeauftragter ist noch nicht bestellt (siehe VVT Absatz 2 und AVV). Die Datenschutz-Folgenabschätzung nach Art. 35 DSGVO liegt als Vorlage (Version 2.0) vor und wird je Auftraggeber vor dem Go-Live erstellt; diese TIA dient ihr als Zulieferdokument für den Bereich Drittlandübermittlungen.

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 oder Widerruf bzw. Änderung des Beschlusses durch die EU-Kommission.

- Weitere strukturelle Entwicklungen beim PCLOB oder der Anwendung von Executive Order 14086.
- Erlangung einer aktiven DPF-Zertifizierung durch Retell AI (vgl. Schedule 3, Ziffer 5 der Retell-AI-DPA) oder Angebot einer EU-Verarbeitung.
- Hinzuziehung, Austausch oder Änderung der Konfiguration eines der bewerteten Subunternehmer.

Unabhängig davon erfolgt eine jährliche Regelüberprüfung im Rahmen der in TOM-Kategorie 7 dokumentierten Prüfung der Sicherheitsnachweise 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 im Rahmen der Eignungsprüfung nach Art. 28 Abs. 1 DSGVO berücksichtigt; die Datenschutz-Folgenabschätzung (Vorlage Version 2.0, Risiko 7) bewertet dieses Risiko nach den Maßnahmen als gering.

9. Zusammenfassende Risikotabelle und Gesamtergebnis

Anbieter	Instrument	Datensensibilität	Restrisiko	Bewertung
Twilio	DPF + SCC/BCR	Gering	Gering	Angemessen
Retell AI	SCC	Erhöht (laufendes Gespräch, keine dauerhafte Speicherung)	Mittel – akzeptiert	Angemessen, dokumentiert akzeptiert
Google (nur E-Mail-Weg)	DPF + SCC	Mittel (Klartext-Benachrichtigung, befristet)	Gering	Angemessen
ElevenLabs (Sub-Sub)	DPF + SCC	Gering	Gering	Angemessen (Verantwortung bei Retell AI)
Azure (Sub-Sub)	Unbekannt	Unbekannt	Unbekannt	Offen
OpenAI (Sub-Sub)	Unbekannt	Erhöht (Echtzeit-Dialoginhalt)	Nicht direkt bewertbar	Offen (Instrument unbestätigt; Verantwortung bei Retell AI)

Gesamtergebnis: Die bewerteten Übermittlungen sind auf Basis der zum Stand 10.10.2026 bekannten Fakten überwiegend durch geeignete Garantien abgesichert. Gegenüber Version 1.1 ist das Risiko gesunken, weil keine vollständigen Mitschriften mehr direkt an OpenAI übermittelt werden und Retell AI Mitschrift und Aufnahme nicht mehr dauerhaft speichert. Das Restrisiko bei Retell AI wird als

akzeptabel eingestuft, insbesondere aufgrund der fehlenden dauerhaften Speicherung, der kurzen Speicherfristen, der fehlenden Zweckänderung und der Trennung je Auftraggeber – dies stellt jedoch eine bewusste unternehmerische Risikoentscheidung dar und keine Beseitigung des Restrisikos. Die Verarbeitungsregion von Microsoft Azure ist unbestätigt. Diese TIA wird gemäß Abschnitt 7 bei Eintritt der dort genannten Ereignisse aktualisiert.