Transfer Impact Assessment (TIA)

Stand: 26.08.2026 · Version 1.1 · Dokumentensatz 2026-08_v1

1. Zweck und Maßstab

Dieses Transfer Impact Assessment bewertet nach den Maßstäben des EuGH-Urteils C-311/18 (Schrems II) und der EDSA-Empfehlungen 01/2020, ob bei der Nutzung der EchoCall-Plattform ein der EU gleichwertiges Schutzniveau für personenbezogene Daten gewährleistet ist. Es ergänzt den AVV und die Standardvertragsklauseln (Anlage 4 des AVV) und wird mindestens jährlich sowie anlassbezogen überprüft.

2. Ausgangslage: Wo werden Daten tatsächlich verarbeitet?

- Produktivdaten (Datenbank, Dateien, Anwendungsbetrieb): ausschließlich EU (IONOS-Rechenzentren Deutschland/Frankreich)
- Sprach- und Chat-Verarbeitung einschließlich LLM-Inferenz der Standardprofile: vollständig eigene Software mit eigenen Modellen auf der EchoCall-Infrastruktur in der EU, kein externer Sprach- oder Modell-Dienstleister. Optionale externe Modellprofile sind von diesem TIA nicht erfasst; ihre Auswahl liegt in der alleinigen Verantwortung des Kunden
- Telefonnummern-Beschaffung: EU (Irland); SIP-Trunk auf EchoCall-Infrastruktur in der EU
- Zahlungsdaten: beim jeweiligen Zahlungsdienstleister (EU/USA, PCI-DSS)
- Vertragspartner der Kunden ist die EchoCall LLC, eine Gesellschaft nach US-Recht (Wyoming), die aus Deutschland heraus operiert

Der relevante Drittlandbezug besteht damit weniger in einem physischen Datenexport als in der Rechtsform des Anbieters und der US-Konzernzugehörigkeit einzelner Unterauftragsverarbeiter: US-Behörden könnten theoretisch versuchen, über US-Rechtsträger Zugriff auf in der EU gespeicherte Daten zu verlangen (CLOUD Act).

3. Relevante US-Rechtsgrundlagen

- FISA Section 702: verpflichtet "electronic communication service providers" zur Mitwirkung an Auslandsaufklärung. Die Programme richten sich in der Praxis an große Kommunikations- und Cloud-Anbieter; EchoCall ist ein kleines B2B-SaaS-Unternehmen ohne für Section-702-Programme typisches Profil.
- CLOUD Act (18 U.S.C. § 2713): erlaubt US-Behörden, von US-Anbietern die Herausgabe von Daten in deren Besitz oder Kontrolle zu verlangen, unabhängig vom Speicherort. Betroffen wären Daten, auf die die EchoCall LLC Zugriff hat.
- Executive Order 14086 und der EU-US-Angemessenheitsbeschluss vom 10.07.2023 (Data Privacy Framework): begrenzen Zugriffe auf das Erforderliche und Verhältnismäßige und schaffen mit dem Data Protection Review Court einen Rechtsbehelf für EU-Betroffene. Diese Garantien gelten unabhängig davon, ob ein Anbieter DPF-zertifiziert ist.

4. Praktische Risikobewertung

- Bisherige Behördenanfragen: Die EchoCall LLC hat bis zum Stand dieses Dokuments keine einzige Anfrage einer US-Behörde (oder einer anderen Drittlandbehörde) auf Herausgabe von Kundendaten erhalten.
- Datenkategorien: B2B-Gesprächs- und Konfigurationsdaten mittelständischer Unternehmen; kein für Auslandsaufklärung typisches Zielprofil.
- Datenstandort und Zugriffswege: Daten liegen in der EU; ein Zugriff setzte ein an die EchoCall LLC gerichtetes, rechtlich durchsetzbares Herausgabeverlangen voraus und würde nicht unbemerkt auf Infrastrukturebene erfolgen.
- Unterauftragsverarbeiter mit US-Bezug verarbeiten entweder in der EU (EU-Ingest) oder erhalten nur begrenzte Datenkategorien (Zahlungsdaten, Vertriebskontaktdaten); Gesprächsinhalte erreichen keinen US-Dienstleister. Alle sind über SCC und teilweise zusätzlich über das Data Privacy Framework abgesichert.

5. Ergänzende Maßnahmen

- Technisch: EU-Datenresidenz als Standard, TLS 1.3, Verschlüsselung ruhender Daten auf Storage-Ebene, verschlüsselte Speicherung von Zugangsdaten und 2FA-Geheimnissen, strikte Mandantentrennung, konfigurierbare Aufbewahrungsfristen, Zero-PII-Modus (Details im TOM-Dokument)
- Organisatorisch: EchoCall prüft jedes behördliche Herausgabeverlangen auf Rechtmäßigkeit, ficht unverhältnismäßige oder rechtswidrige Verlangen mit allen zumutbaren Rechtsmitteln an, gibt Daten nur im rechtlich zwingend erforderlichen Mindestumfang heraus und informiert den betroffenen Kunden vorab, soweit gesetzlich zulässig
- Vertraglich: EU-Standardvertragsklauseln (Module 2 und 3) mit allen Kunden vereinbart; gleichwertige Pflichten an alle Unterauftragsverarbeiter weitergegeben; Transparenzbericht-Zusage (Zero-Requests-Stand wird bei Änderung aktualisiert)

6. Ergebnis

Unter Berücksichtigung der tatsächlichen EU-Verarbeitung, der Datenkategorien, der bisherigen Anfragelage, der Garantien aus Executive Order 14086 und der beschriebenen technischen, organisatorischen und vertraglichen Maßnahmen bewertet EchoCall das Restrisiko eines unverhältnismäßigen Drittlandzugriffs als gering. Die Übermittlungssachverhalte können auf die Standardvertragsklauseln in Verbindung mit den ergänzenden Maßnahmen gestützt werden. Kunden können dieses TIA für ihre eigene Dokumentation nach Art. 44 ff. DSGVO verwenden.

Nächste planmäßige Überprüfung: August 2027 oder anlassbezogen früher (Rechtsänderungen, neue Unterauftragsverarbeiter, erste Behördenanfrage).
