

Anlage D — Transfer Impact Assessment für Drittlandübermittlungen

Auftragsverarbeitungsvereinbarung (AVV) — Anlage D

Stand: September 2026 · Erstellt von KiCo AI LLP, Vancouver, BC, Kanada

1. Zweck, Anwendungsbereich und Methodik

Dieses Dokument bewertet die Rechtslage in den Bestimmungsdrittländern und die Auswirkungen auf den Schutz der übermittelten personenbezogenen Daten. Maßstab sind das Urteil des Gerichtshofs der Europäischen Union in der Rechtssache C-311/18 (Schrems II) und die Empfehlungen 01/2020 des Europäischen Datenschutzausschusses.

Was sich gegenüber der Fassung März 2026 geändert hat. Die Vorfassung trug im Titel einen einzigen Empfänger, Retell AI Inc., und bewertete allein dessen Übermittlung. Die Unterauftragsverarbeiterliste in der Fassung September 2026 weist jedoch 20 Empfänger in den Vereinigten Staaten aus sowie eine Übermittlung nach Singapur, für das kein Angemessenheitsbeschluss besteht. Art. 46 Abs. 2 lit. c verlangt eine Bewertung je Übermittlung. Der Titel ist deshalb von "TIA USA" auf "Drittlandübermittlungen" erweitert, und der Anwendungsbereich umfasst nun 22 Bewertungseinheiten sowie den in Abschnitt 5.2 behandelten Zugriff aus Indonesien, der keine Übermittlung ist, aber in der Vereinbarung genannt wird.

Aufbau. Abschnitt 3 bewertet die Rechtslage der Vereinigten Staaten einmal für alle dortigen Empfänger; sie ist für alle dieselbe. Abschnitt 4 bewertet Singapur, Abschnitt 5 Kanada. Die Abschnitte 6 und 7 enthalten die Einzelbewertungen, gestuft nach dem tragenden Übermittlungsmechanismus.

Die Stufung und ihre Begründung. Wo eine Übermittlung auf einem Angemessenheitsbeschluss beruht — beim EU-US Data Privacy Framework für zertifizierte Empfänger —, greift Art. 45 und nicht Art. 46; eine Bewertung der Drittlandrechtslage ist dann rechtlich nicht gefordert. KiCo führt für diese Empfänger dennoch einen Kurzeintrag, weil eine Zertifizierung erlöschen kann, ohne dass der Anbieter darauf hinweist. Genau dieser Fall ist bei der Prüfung am 10.09.2026 eingetreten und in Abschnitt 6.7 dokumentiert. Der Kurzeintrag hält deshalb je Empfänger den Registerbefund, das Ablaufdatum und die vertragliche Rückfallebene fest.

- **Stufe A — Vollbewertung** (Abschnitt 6): 10 Empfänger, deren Übermittlung allein auf Art. 46 beruht.
- **Stufe B — Kurzbewertung mit Registerbeleg** (Abschnitt 7): 11 Empfänger, deren Übermittlung von einer geprüften Zertifizierung getragen wird, mit den Standardvertragsklauseln als Rückfallebene.
- **Stufe C — Angemessenheitsbeschluss** (Abschnitt 5): Kanada.

Prüfmethode für den Zertifizierungsstatus. Der Status wurde nicht der Selbstauskunft des jeweiligen Anbieters entnommen, sondern am 10.09.2026 einzeln gegen das amtliche Register abgefragt, das der Liste auf dataprivacyframework.gov zugrunde liegt. Abgefragt wurde je Empfänger der Rechtsträger, nicht die Marke — der Unterschied ist erheblich und war bei ClickUp der Grund, weshalb der abgelaufene Eintrag zuvor nicht aufgefallen war. Erhoben wurden Status, Geltung für andere als Beschäftigtendaten, Ablaufdatum, offene Inaktivzeiträume, erfasste Gesellschaften und die Art der Überprüfung. Die Rohdaten des Abrufs sind als Beleg dokumentiert und werden auf Anforderung vorgelegt.

Ein Befund vorweg, der für alle Stufe-B-Empfänger gilt: jede geprüfte Zertifizierung beruht auf Selbstbewertung des Anbieters, keine auf einer Überprüfung durch Dritte. Das mindert die Zertifizierung nicht, es beschreibt ihren Beweiswert.

2. Inventar der bewerteten Übermittlungen

Empfänger (Rechtsträger)	Drittland	Tragender Mechanismus	Registerbefund 10.09.2026	Stufe
Anthropic Ireland, Limited (Verarbeitung USA)	USA	SCC Modul 2	kein Eintrag	A
Retell AI Inc.	USA	SCC Modul 3	kein Eintrag	A
Airtable, Inc.	USA	SCC	kein Eintrag	A
Docusign Inc.	USA	Verbindliche interne Datenschutzvorschriften, ergänzend SCC Modul 2 und 3	kein Eintrag	A
Mango Technologies, Inc. (DBA ClickUp)	USA	SCC Modul 2 und 3	Inactive - Lapse , offen seit 25.02.2024	A
Doppler Technologies, Inc.	USA	SCC Modul 2 und 3	kein Eintrag	A
Voiceflow Inc. (US-Anteil)	USA	SCC Modul 2 und 3	kein Eintrag	A
Lovable-Kette: Anthropic und AWS in den USA	USA	SCC über die Vereinbarung mit Lovable Labs Sweden AB	kein Eintrag für Lovable	A
Manychat, Inc.	USA	SCC Modul 2 und 3, Zertifizierung unter Vorbehalt	Active - Re-certification under Review, bis 25.08.2027	A
Notion Labs, Inc.	USA	SCC Modul 2, Zertifizierung unter Vorbehalt	Active - Re-certification under Review, Periode endete 08.10.2025	A
Netlify, Inc.	USA	Zertifizierung, hilfsweise SCC Modul 2 und 3	Active, bis 17.12.2026	B
Clerk, Inc.	USA	Zertifizierung, ergänzend SCC	Active, bis 30.06.2027	B
Cloudflare, Inc.	USA	Zertifizierung, ergänzend SCC Modul 2 und 3	Active, bis 23.09.2026	B
Calendly LLC	USA	Zertifizierung, ergänzend SCC Modul 2	Active, bis 21.10.2026	B
Twilio Inc.	USA	Zertifizierung, ergänzend SCC Modul 3	Active, bis 20.04.2027	B
Telnyx LLC	USA	Zertifizierung, ergänzend SCC Modul 1 bis 3	Active, bis 22.01.2027	B
Perplexity AI, Inc.	USA	Zertifizierung, ergänzend SCC Modul 2	Active, bis 08.10.2026	B
Bitwarden, Inc.	USA	Zertifizierung, ergänzend SCC	Active, bis 04.02.2027	B
Slack Technologies, LLC	USA	Verbindliche interne Datenschutzvorschriften der Gruppe, ergänzend Zertifizierung und SCC	erfasste Gesellschaft der Salesforce, Inc., Active, bis 20.10.2026	B
Neon, LLC	USA (Daten in Frankfurt)	Zertifizierung der Muttergesellschaft, ergänzend SCC	erfasste Gesellschaft der Databricks, Inc., Active, bis 10.08.2027	B
Supabase Pte. Ltd	Singapur (Daten in Frankfurt)	SCC	kein Angemessenheitsbeschluss für Singapur	A

Empfänger (Rechtsträger)	Drittland	Tragender Mechanismus	Registerbefund 10.09.2026	Stufe
Google Cloud Canada Corporation · ZOHO Canada Corporation · Voiceflow Inc. (Kanada-Anteil)	Kanada	Angemessenheitsbeschluss	—	C
Zugriff eines Partners von KiCo AI LLP aus Indonesien	Indonesien	keine Übermittlung nach Kapitel V — kein vom Exporteur verschiedener Empfänger	—	siehe 5.2

3. Rechtslage in den Vereinigten Staaten

Dieser Abschnitt gilt für alle in Abschnitt 2 genannten Empfänger in den Vereinigten Staaten.

3.1 Maßgebliche Vorschriften

Vorschrift / Risiko	Beschreibung	Bewertung	Wirkung auf die hier bewerteten Übermittlungen
FISA Section 702	Erlaubt den Zugriff auf Daten von Personen außerhalb der Vereinigten Staaten bei Anbietern elektronischer Kommunikationsdienste.	MITTEL	Erfasst grundsätzlich jeden hier genannten Empfänger, der als solcher Anbieter einzuordnen ist. Die Reichweite hängt nicht vom Speicherort ab.
Cloud Act	Verpflichtet US-Unternehmen zur Herausgabe von Daten in ihrem Gewahrsam, unabhängig vom Speicherort.	MITTEL	Betrifft auch die Empfänger, deren Daten physisch in der Union liegen — namentlich Neon und Supabase. Der Speicherort in Frankfurt beseitigt den Zugriff nicht, er erschwert ihn tatsächlich.
Executive Order 12333	Auslandsaufklärung außerhalb des FISA-Rahmens, ohne richterliche Kontrolle.	MITTEL	Kein vertraglicher Mechanismus wirkt dagegen unmittelbar; nur Verschlüsselung und Datenminimierung wirken.
Executive Order 14086	Bindet die Signalaufklärung an Erforderlichkeit und Verhältnismäßigkeit und schafft einen zweistufigen Rechtsbehelf bis zum Data Protection Review Court.	POSITIV	Gilt für alle US-Empfänger, nicht nur für zertifizierte. Trägt den Angemessenheitsbeschluss aus dem Jahr 2023.
National Security Letters	Erlauben dem FBI die Anforderung von Bestands- und Verkehrsdaten ohne richterliche Anordnung.	GERING	Zielen auf Anbieter von Telekommunikations- und Finanzdiensten. Für die Telefonie-Empfänger dieser Liste ist das Risiko höher einzuschätzen als für die übrigen.
Rechtsstaatlichkeit	Unabhängige Gerichte, Gewaltenteilung, Schutz durch den vierten Zusatzartikel.	POSITIV	Trägt die Anfechtungspflicht nach Klausel 15 Abs. 2 der Standardvertragsklauseln praktisch.

3.2 Gesamtbewertung der US-Rechtslage

Die Vereinigten Staaten verfügen über Vorschriften, die Behörden den Zugriff auf Daten bei dortigen Unternehmen ermöglichen. Die Executive Order 14086 hat den Zugriff seit dem Jahr 2022 an Erforderlichkeit und Verhältnismäßigkeit gebunden und einen Rechtsbehelf geschaffen; auf dieser Grundlage hat die Kommission im Jahr 2023 den Angemessenheitsbeschluss für das EU-US Data Privacy Framework erlassen. Die dort verankerten Beschränkungen wirken für alle US-Unternehmen, auch für nicht zertifizierte. Das ist der tragende Grund, weshalb auch die Stufe-A-Übermittlungen dieser Liste als zulässig bewertet werden.

Was diese Bewertung nicht trägt. Sie trägt keine Übermittlung besonderer Kategorien nach Art. 9 und keine Übermittlung, bei der ein Anbieter Kundendaten zum Training verwendet. Beides ist in den Verträgen ausgeschlossen und in Abschnitt 8 als Auslöser für eine Neubewertung benannt.

3.3 Branchenspezifische Erfahrung

KiCo AI hat keine Kenntnis von Behördenzugriffen auf Daten bei einem der hier genannten Empfänger. Der Wirtschaftszweig — Kundenkommunikation und Terminvereinbarung für kleine und mittlere Unternehmen — steht nicht im Fokus nachrichtendienstlicher Interessen. Die verarbeiteten Daten sind Kontaktdaten, Terminwünsche und Gesprächsinhalte zu Handwerks-, Gesundheits- und Dienstleistungsanliegen.

4. Rechtslage in Singapur

Betrifft Supabase Pte. Ltd als Vertragspartei. Für Singapur besteht **kein Angemessenheitsbeschluss**; die Übermittlung stützt sich allein auf die Standardvertragsklauseln.

Maßgeblich ist der Personal Data Protection Act, ergänzt um Zugriffsbefugnisse aus dem Criminal Procedure Code und dem Internal Security Act. Die Aufsicht führt die Personal Data Protection Commission. Ein dem Data Protection Review Court vergleichbarer Rechtsbehelf für Betroffene aus der Union besteht nicht.

Entscheidend für die Bewertung ist hier die Datenlage, nicht die Rechtslage. Die Projekte von KiCo liegen in der Region Frankfurt; nach Singapur übermittelt wird nicht der Datenbestand, sondern die Möglichkeit administrativen Zugriffs durch die Vertragspartei. Der Schutzbedarf richtet sich damit auf die Zugriffskontrolle beim Anbieter, nicht auf den Speicherort.

Ergebnis: zulässig mit ergänzenden Maßnahmen. Tragend sind die Standardvertragsklauseln, die Belegenheit der Daten in der Union, die Verschlüsselung im Ruhezustand und während der Übertragung sowie die Beschränkung administrativer Zugriffe. **Offen und in Abschnitt 8 als Prüfauftrag geführt:** ob der Anbieter administrative Zugriffe aus Singapur protokolliert und auf Anforderung nachweist.

5. Weitere Drittlandbezüge

5.1 Kanada — Angemessenheitsbeschluss

Betrifft Google Cloud Canada Corporation, ZOHO Canada Corporation und den kanadischen Anteil von Voiceflow Inc.

Für Kanada besteht ein fortgeltender Angemessenheitsbeschluss, soweit die Verarbeitung dem Personal Information Protection and Electronic Documents Act unterfällt — das ist bei gewerblicher Tätigkeit der Fall und trifft auf alle drei Empfänger zu. Die Übermittlung stützt sich damit auf Art. 45; eine Bewertung nach Art. 46 ist nicht erforderlich. Für den US-Anteil von Voiceflow gilt die Bewertung in Abschnitt 6.6.

5.2 Zugriff aus Indonesien — kein Empfänger, aber ein Drittlandbezug

Die Auftragsverarbeitungsvereinbarung nennt „Indonesien und andere Drittländer“ und hängt dafür die Standardvertragsklauseln an. Das ist **keine Vorlagenrestanz, sondern gewollt**: ein Partner von KiCo AI LLP arbeitet aus Indonesien und greift von dort auf die Systeme zu. Weil dieses Dokument nicht mehr allein die Vereinigten Staaten behandelt, gehört der Sachverhalt hierher.

Einordnung. Es liegt **keine Übermittlung im Sinne von Kapitel V** vor. Eine solche setzt nach den Leitlinien 05/2021 des Europäischen Datenschutzausschusses einen vom Exporteur **verschiedenen** Empfänger voraus. Zugriff eigenen Personals derselben Gesellschaft ist das nicht — es gibt keinen Importeur, und damit auch nichts, worauf Art. 46 anzuwenden wäre. Aus demselben Grund trägt Indonesien **keine Zeile in Anlage C**: dort stehen beauftragte Dritte.

Das Risiko verschwindet damit nicht, es verschiebt sich. Person und Endgerät befinden sich in einem Drittland und unterliegen dessen Recht und dessen Zugriffsmöglichkeiten. Der Schutz liegt deshalb nicht in einem Übermittlungsinstrument, sondern in der Zugriffsarchitektur.

Ausdrücklich festgehalten, weil die Annahme naheliegt und falsch ist: ein VPN oder ein Tunnel heilt hier nichts. Der Austritt über einen Knoten in der Union ändert die IP-Adresse, nicht den Aufenthaltsort der zugreifenden Person. Eine Bewertung, die sich auf den Tunnel stützt, wäre schwächer als eine, die den Sachverhalt benennt und die Kontrollen beschreibt.

Tragende Maßnahmen — sie gehören als technische und organisatorische Maßnahmen in Anlage B und sind dort zu führen: kein unmittelbar exponierter Dienst; vermittelter und protokollierter Zugriff über das private Netz; keine dauerhafte lokale Speicherung von Kundendaten auf dem Endgerät; Verschlüsselung des Endgeräts; rollenbasierte Rechte nach dem Prinzip der geringsten Rechte.

Zur Rechtslage vor Ort, weil sie die Risikoeinschätzung mitträgt und sich gerade ändert: Indonesien hat mit dem Law No. 27 of 2022 ein Datenschutzgesetz; die Durchführungsverordnung Government Regulation No. 33 of 2026 mit 225 Artikeln wurde am 16.07.2026 verkündet und wird am 16.01.2027 wirksam. Sie verlangt für grenzüberschreitende Übermittlungen zunächst eine Prüfung des Schutzniveaus im Empfängerland (Art. 165), hilfsweise verbindliche Garantien und erst zuletzt eine Einwilligung unter engen Zusatzbedingungen (Art. 173). Der Sanktionsrahmen liegt bei bis zu 2% des Jahresumsatzes.

Zwei Einschränkungen sind zu benennen. Erstens ist die Aufsichtsbehörde nach dem Stand vom 10.09.2026 **noch nicht förmlich errichtet**, und die Übermittlungsinstrumente sind noch nicht ausgegeben — es gibt vor Ort also noch keine Stelle, die das Regime durchsetzt. Zweitens beruhen diese Angaben auf **Sekundärquellen**; der Verordnungstext selbst wurde nicht gelesen. Für die Bewertung in diesem Dokument ist das tragbar, weil der Befund die Einordnung nicht ändert — es liegt ohnehin keine Übermittlung nach Kapitel V vor. Für eine Aussage gegenüber Dritten über indonesisches Recht wäre es nicht tragbar.

Ergebnis: kein Übermittlungstatbestand, Schutz über die Zugriffsarchitektur. Die Nennung Indonesiens in der Auftragsverarbeitungsvereinbarung ist als Offenlegung des Sachverhalts richtig und soll dort bleiben. **Zu prüfen** bleibt, ob die beschriebenen Kontrollen in Anlage B tatsächlich geführt sind — der Prüfpunkt steht in Abschnitt 8.

6. Stufe A — Einzelbewertungen

Jede Bewertung nennt die übermittelten Datenkategorien, die tragenden Garantien und das Ergebnis. Die Rechtslage des Bestimmungslands ist in Abschnitt 3 beziehungsweise 4 bewertet und wird nicht wiederholt.

6.1 Anthropic Ireland, Limited — Sprachmodell und Entwicklungsumgebung

Datenimporteur und Vertragspartei: Anthropic Ireland, Limited für Kunden im Europäischen Wirtschaftsraum.

Verarbeitungsort: Vereinigte Staaten. Die Schnittstelle bietet keine europäische Region; der Parameter zur Datenbelegenheit kennt nur die Werte für die Vereinigten Staaten und global.

Datenkategorien: Inhalte der Anfragen an das Modell. Bei der Belegauswertung sind das Dokumenteninhalte einschließlich der darin enthaltenen Namen und Anschriften; bei der Entwicklungsumgebung Quelltext und Konfiguration.

Mechanismus: SCC Modul 2, einbezogen über die Commercial Terms. **Kein Eintrag im Register.**

Tragende Garantien: kein Training auf Kundendaten; Standardaufbewahrung 30 Tage; Anfechtungspflicht nach Klausel 15 Abs. 2. **Wesentlich für die Bewertung:** die zweite Modellstrecke über AWS ist an die Region Frankfurt gebunden, und die Rechtebegrenzung des Kontos verweigert die US-Variante aktiv. Für Verarbeitungen mit erhöhtem Schutzbedarf steht damit eine Strecke zur Verfügung, die das Drittland nicht berührt.

Ergebnis: zulässig mit ergänzenden Maßnahmen. Datenminimierung in den Anfragen und die Bevorzugung der EU-gebundenen Strecke bei Dokumenten mit Personenbezug sind die tragenden Maßnahmen.

6.2 Retell AI Inc. — Voice-KI-Plattform

Datenimporteur: Retell AI Inc., 1121 Industrial Rd, Ste 500, San Carlos, CA 94070. **Mechanismus:** SCC Modul 3, DPA unterzeichnet. **Kein Eintrag im Register** — die Bewertung der Fassung März 2026 ist an diesem Punkt bestätigt.

Datenkategorien: Sprachdaten in der Echtzeitverarbeitung, Transkripte, Rufnummern der Anrufenden, Gesprächszeitpunkte und -dauer sowie im Gespräch genannte Namen und Anschriften.

Tragende Garantien: Entfernung personenbezogener Identifikatoren aus Transkripten und Aufzeichnungen, für alle Agenten aktiviert; Sprachaufzeichnung standardmäßig abgeschaltet, sodass keine dauerhafte Audiodatei im Drittland entsteht; Verschlüsselung mit AES 256 im Ruhezustand und TLS 1.3 während der Übertragung; rollenbasierte Zugriffskontrolle; Zertifizierung nach SOC 2 Type II.

Ergebnis: zulässig mit ergänzenden Maßnahmen. Unverändert gegenüber der Fassung März 2026.

6.3 Airtable, Inc. — Aufbau- und Testumgebungen

Mechanismus: SCC in der Vereinbarung. **Kein Eintrag im Register.** Europäische Datenhaltung bietet der Anbieter erst im Tarif Enterprise Scale an; KiCo nutzt den Tarif Team, der vollständig in den Vereinigten Staaten liegt.

Datenkategorien: Aufbau- und Testdaten. Produktive Kundendaten liegen in der Datenbank des Kundenportals in Frankfurt. Wo Airtable das CRM des Kunden ist, läuft es auf dessen Konto und ist Auftragsverarbeiter des Kunden, nicht von KiCo.

Ergebnis: zulässig mit ergänzenden Maßnahmen — mit einem offenen Prüfpunkt. Ob die Testumgebungen echte oder synthetische personenbezogene Daten enthalten, ist nicht abschließend geprüft. Produktionsdaten in Testumgebungen wären angesichts der vollständigen US-Belegenheit dieses Tarifs der kritische Fall. Der Prüfpunkt steht in Abschnitt 8.

6.4 Docusign Inc. — Elektronische Unterschrift

Mechanismus: verbindliche interne Datenschutzvorschriften für Auftragsverarbeiter nach Art. 47 als vorrangiger Mechanismus, ergänzend SCC Modul 2 und 3, Recht und Gerichtsstand Irland. **Kein Eintrag im Register** — der Anbieter stützt sich nicht auf die Zertifizierung, sondern auf den stärkeren Mechanismus. Vertragspartei ist die US-Gesellschaft, belegt am Rechnungskopf.

Datenkategorien: Name, E-Mail-Adresse und Unterschrift der unterzeichnenden Person sowie der Inhalt des Vertragsdokuments.

Ergebnis: zulässig. Verbindliche interne Datenschutzvorschriften unterliegen der Genehmigung durch eine Aufsichtsbehörde und binden die gesamte Unternehmensgruppe; sie bieten ein höheres Maß an Verbindlichkeit als die Standardvertragsklauseln.

6.5 Mango Technologies, Inc. (DBA ClickUp) — Projekt- und Aufgabenverwaltung

Dieser Empfänger ist der Grund für die Stufung in Abschnitt 1. Die veröffentlichte Anlage C hat für ClickUp bis zum 10.09.2026 eine Zertifizierung im EU-US Data Privacy Framework ausgewiesen. Die Abfrage des Registers hat ergeben, dass die Zertifizierung des Rechtsträgers am 26.01.2024 ausgelaufen und seit dem 25.02.2024 durchgehend inaktiv ist. Die Angabe war seit mehr als zwei Jahren unzutreffend und stand auch schon in der Fassung März 2026.

Warum es nicht aufgefallen ist: die Marke lautet ClickUp, der Rechtsträger Mango Technologies, Inc. Eine Suche nach der Marke findet den Eintrag nicht.

Mechanismus nach der Berichtigung: allein SCC Modul 2 und 3. **Datenkategorien:** Aufgabentexte, Projektunterlagen und darin genannte Kundennamen. **Tragende Garantien:** Zertifizierungen nach SOC 2 Type II und ISO 27001; wählbarer Verarbeitungsort, der auf die Union gestellt werden kann.

Ergebnis: zulässig mit ergänzenden Maßnahmen — die Standardvertragsklauseln tragen die Übermittlung eigenständig. **Maßnahme mit Vorrang:** den Verarbeitungsort des Arbeitsbereichs auf die Union stellen, sofern der gebuchte Tarif das zulässt. Die Zeile in Anlage C ist am 10.09.2026 berichtigt worden.

6.6 Voiceflow Inc. — Chatbot- und Voicebot-Entwicklung

Kanadische Gesellschaft; der kanadische Anteil ist von Abschnitt 5 gedeckt. Für den US-Anteil der Verarbeitung tragen SCC Modul 2 und 3. **Kein Eintrag im Register.** **Datenkategorien:** Gesprächsinhalte der Chat- und Sprachdialoge sowie die dort erhobenen Kontaktdaten. **Tragende Garantie:** kein Training auf Kundendaten. **Ergebnis: zulässig mit ergänzenden Maßnahmen.**

6.7 Doppler Technologies, Inc. — Verwaltung der Zugangsdaten

Mechanismus: SCC Modul 2 und 3, Recht und Gerichtsstand Irland. **Kein Eintrag im Register.** Ein gleichnamiger Eintrag "Doppler LLC" in Palo Alto ist ein anderer Rechtsträger und für diese Bewertung ohne Bedeutung.

Datenkategorien: Zugangsdaten zu Systemen. Personenbezogene Daten von Endkunden werden hier nicht verarbeitet; der Schutzbedarf ergibt sich aus der Schlüsselgewalt, nicht aus dem Personenbezug. **Tragende Garantien:** Verschlüsselung im Ruhezustand, rollenbasierte Zugriffskontrolle, getrennte Projekte je Kunde.

Ergebnis: zulässig. Die Übermittlung betrifft keine Endkundendaten.

6.8 Lovable-Kette — Anthropic und AWS in den Vereinigten Staaten

Vertragspartei ist Lovable Labs Sweden AB in Stockholm, also innerhalb der Union; die Auftragsverarbeitungsvereinbarung ist im gebuchten Tarif Business enthalten. **Kein Eintrag im Register**, was hier ohne Bedeutung ist, weil die Gesellschaft nicht in den Vereinigten Staaten sitzt.

Die Drittlandübermittlung entsteht erst in der Kette: nach dem Trust Center des Anbieters laufen Google Cloud in der Union für Anwendungen und Datenbanken, Cloudflare für Edge-Dienste sowie Anthropic und AWS in den Vereinigten Staaten. Für die beiden letztgenannten gelten die Bewertungen in Abschnitt 6.1 sinngemäß, vermittelt über die Vereinbarung mit dem Anbieter.

Datenkategorien: Inhalte der Kunden-Websites und die über deren Formulare erhobenen Kontaktdaten.

Ergebnis: zulässig mit ergänzenden Maßnahmen. Offener Prüfpunkt: ob der Anbieter die Kette vertraglich in derselben Tiefe absichert, wie KiCo sie gegenüber den eigenen Kunden zusagt. Der Prüfpunkt steht in Abschnitt 8.

6.9 Manychat, Inc. — Chatbot- und Messenger-Marketing

Registerbefund: Status "Active - Re-certification under Review", Geltung bis 25.08.2027. Der Status weist eine laufende, aber noch nicht abgeschlossene Rezertifizierung aus. Weil er nicht "Active" lautet, führt KiCo den Empfänger in Stufe A und stützt die Übermittlung auf SCC Modul 2 und 3, die vertraglich mit deutschem Recht und deutschem Gerichtsstand nach Klausel 17 und 18 vereinbart sind.

Datenkategorien: Kontaktdaten und Nachrichtenverläufe aus Messenger-Kanälen.

Ergebnis: zulässig mit ergänzenden Maßnahmen. Die Standardvertragsklauseln tragen unabhängig vom Ausgang der Rezertifizierung. **Nebenbefund:** der Rechtsträger ist im Register mit Sitz in West Hollywood geführt, während Anlage C die Anschrift 1 World Trade Center, New York, 10007 nennt. Die Abweichung ist in Abschnitt 8 als Prüfpunkt vermerkt.

6.10 Notion Labs, Inc. — Onboarding- und Projektdokumentation

Registerbefund: Status "Active - Re-certification under Review"; die zertifizierte Periode endete am 08.10.2025 und die Rezertifizierung ist seither nicht abgeschlossen. Von allen geprüften Einträgen ist dies der am längsten schwebende. KiCo führt den Empfänger deshalb in Stufe A und stützt die Übermittlung auf SCC Modul 2.

Datenkategorien: Onboarding-Angaben der Kunden und Projektdokumentation, einschließlich Ansprechpartnern und deren Kontaktdaten. Eine europäische Region bietet der Anbieter nicht an.

Ergebnis: zulässig mit ergänzenden Maßnahmen. Maßnahme: den Schwebezustand halbjährlich nachprüfen; bei Übergang auf "Inactive" ist der Fall wie bei ClickUp zu behandeln.

6.11 Supabase Pte. Ltd — Datenbank des Kundenportals

Bewertet in Abschnitt 4. Die Vertragspartei sitzt in Singapur, die Daten liegen in Frankfurt. **Ergebnis: zulässig mit ergänzenden Maßnahmen.**

7. Stufe B — Kurzbewertungen mit Registerbeleg

Für die folgenden Empfänger beruht die Übermittlung auf einer am 10.09.2026 gegen das amtliche Register geprüften Zertifizierung. Damit greift Art. 45; eine Bewertung nach Art. 46 ist rechtlich nicht gefordert. Die Standardvertragsklauseln sind jeweils zusätzlich vereinbart und tragen die Übermittlung, falls die Zertifizierung endet.

Empfänger	Status im Register	Gültig bis	Für andere als Beschäftigtendaten	Rückfallebene	Datenkategorien
Netlify, Inc.	Active	17.12.2026	ja	SCC Modul 2 und 3, Recht Irland	Zugriffsdaten der Auswertungsoberflächen
Clerk, Inc.	Active	30.06.2027	ja	SCC Modul 1 bis 3	Anmeldedaten, E-Mail-Adressen
Cloudflare, Inc.	Active	23.09.2026	ja	SCC Modul 2 und 3	Verbindungsdaten, IP-Adressen
Calendly LLC	Active	21.10.2026	ja	SCC Modul 2	Name, E-Mail-Adresse, Terminwunsch
Twilio Inc.	Active	20.04.2027	ja	SCC Modul 3	Rufnummern, Verbindungsdaten
Telnyx LLC	Active	22.01.2027	ja	SCC Modul 1 bis 3, Recht Irland	Rufnummern, Verbindungsdaten
Perplexity AI, Inc.	Active	08.10.2026	ja	SCC Modul 2	Rechercheanfragen
Bitwarden, Inc.	Active	04.02.2027	ja	SCC	Zugangsdaten, keine Endkundendaten
Slack Technologies, LLC	Active als erfasste Gesellschaft der Salesforce, Inc.	20.10.2026	ja	Verbindliche interne Datenschutzvorschriften der Gruppe, ergänzend SCC Modul 2 und 3	Nachrichteninhalte, Kundenkanäle
Neon, LLC	Active als erfasste Gesellschaft der Databricks, Inc.	10.08.2027	ja	SCC in der Databricks-Vereinbarung	Auswertungsdaten, Daten liegen in Frankfurt

Zwei Hinweise, die aus der Tabelle nicht hervorgehen. Erstens läuft die Zertifizierung von Cloudflare am 23.09.2026 ab, also innerhalb von zwei Wochen nach dem Stand dieses Dokuments; sie ist vorrangig nachzuprüfen. Zweitens beruhen sämtliche Einträge dieser Tabelle auf Selbstbewertung des jeweiligen Anbieters. Keiner ist durch einen Dritten überprüft.

8. Ergänzende Maßnahmen und offene Prüfpunkte

8.1 Vertragliche Maßnahmen

Standardvertragsklauseln im jeweils einschlägigen Modul mit allen Empfängern der Stufe A; Auftragsverarbeitungsvereinbarungen nach Art. 28 durchgehend abgeschlossen; Benachrichtigungspflicht des Importeurs bei Behördenzugriff nach Klausel 15 Abs. 1; Pflicht zur Prüfung und gegebenenfalls Anfechtung von Offenlegungsersuchen nach Klausel 15 Abs. 2; Aussetzungsrecht nach Klausel 16; vertragliches Verbot des Trainings auf Kundendaten; Ausschluss besonderer Kategorien nach Art. 9.

8.2 Technische Maßnahmen

Entfernung personenbezogener Identifikatoren bei der Sprachverarbeitung; Verschlüsselung mit AES 256 im Ruhezustand und TLS 1.3 während der Übertragung; Sprachaufzeichnung standardmäßig abgeschaltet; kurze Aufbewahrungsfristen mit automatischer Löschung; rollenbasierte Zugriffskontrolle nach dem Prinzip der geringsten Rechte; Trennung der Kundenbestände; Belegenheit der produktiven Datenbestände in der Union, wo der Anbieter sie anbietet; EU-gebundene Modellstrecke, deren Bindung durch die Rechtebegrenzung des Kontos erzwungen und nicht nur konfiguriert ist.

8.3 Organisatorische Maßnahmen

Vertreter in der Union nach Art. 27: KiCo AI LLP hat seinen Sitz ausserhalb der Union; die Ausnahme greift nicht. Benannt ist die **Prighter Group** mit ihren lokalen Partnern als Vertreter und Kontaktstelle für die Europäische Union. Betroffene erreichen sie unmittelbar über das Portal des Vertreters; die Benennung tritt nicht an die Stelle der Rechte gegenüber KiCo.

Prüfung des Zertifizierungsstatus **gegen das amtliche Register und über den Rechtsträger, nicht über die Marke** — halbjährlich sowie vor jeder Neufassung der Anlage C; Führung eines Nachweisordners mit den Anbieterdokumenten; Beobachtung der Unterauftragsverarbeiterlisten der Anbieter; jährliche Neubewertung dieses Dokuments; Beobachtung der Rechtsprechung und der Hinweise der Aufsichtsbehörden.

Zum Nachweisordner: KiCo führt zu diesem Dokument einen Nachweisordner mit den Datenschutzvereinbarungen und Registerauszügen der Empfänger, jeweils mit Quelle, Abrufdatum und Prüfsumme. Er wird auf Anforderung vorgelegt. Von 26 vorgesehenen Anbieterdokumenten sind 21 gesichert; 5 sind noch nachzulegen.

8.4 Offene Prüfpunkte

Prüfpunkt	Betrifft	Warum er offen ist
Enthalten die Testumgebungen echte personenbezogene Daten?	Airtable	Der genutzte Tarif liegt vollständig in den Vereinigten Staaten; bei echten Daten ändert sich der Schutzbedarf dieser Zeile.
Protokolliert der Anbieter administrative Zugriffe aus dem Drittland?	Supabase	Die Bewertung stützt sich auf die Zugriffskontrolle beim Anbieter; ohne Protokoll ist sie nicht nachweisbar.
Sichert der Anbieter seine eigene Kette in derselben Tiefe ab?	Lovable	Die Übermittlung entsteht erst bei den Unterauftragnehmern; die Zusage gegenüber unseren Kunden reicht weiter als der geprüfte Nachweis.
Anschrift des Rechtsträgers	Manychat	Register und Anlage C nennen verschiedene Orte.
Zertifizierung läuft am 23.09.2026 ab	Cloudflare	Innerhalb von zwei Wochen nach dem Stand dieses Dokuments.
Rezertifizierung seit dem 08.10.2025 schwebend	Notion Labs	Längster schwebender Status der Prüfung.
Verarbeitungsort auf die Union stellen	ClickUp	Der Tarif lässt die Wahl zu; die Maßnahme beseitigt die Übermittlung ganz.
5 fehlende Anbieterdokumente	Nachweisordner	Ohne Browser nicht abrufbar.
Sind die Kontrollen für den Zugriff aus Indonesien in Anlage B geführt?	Zugriffsarchitektur	Der Schutz beruht allein auf ihnen, nicht auf einem Übermittlungsinstrument.

9. Gesamtergebnis

ERGEBNIS: DIE BEWERTETEN ÜBERMITTLUNGEN SIND ZULÄSSIG, JEWEILS MIT DEN IN ABSCHNITT 8 GENANNTEN ERGÄNZENDEN MASSNAHMEN.

Tragende Gründe:

- Die übermittelten Daten sind allgemeine Kontakt-, Termin- und Gesprächsdaten. Besondere Kategorien nach Art. 9 sind vertraglich ausgeschlossen; Zahlungsdaten werden nicht an diese Empfänger übermittelt.
- Für 11 Empfänger trägt ein Angemessenheitsbeschluss, dessen Geltung je Rechtsträger am amtlichen Register geprüft und in Abschnitt 7 mit Datum belegt ist.
- Für die übrigen tragen die Standardvertragsklauseln oder — bei Docusign und Slack — verbindliche interne Datenschutzvorschriften, die einer aufsichtsbehördlichen Genehmigung unterliegen.
- Die Executive Order 14086 beschränkt den Zugriff der Nachrichtendienste auf das verhältnismäßig Notwendige und wirkt für alle US-Empfänger, auch für nicht zertifizierte.

5. Die technischen Maßnahmen mindern den Personenbezug an der Stelle, an der er am dichtesten ist: in der Sprachverarbeitung.
6. Für Verarbeitungen mit erhöhtem Schutzbedarf steht eine Modellstrecke zur Verfügung, die das Drittland nicht berührt und deren Bindung technisch erzwungen ist.
7. Der Wirtschaftszweig hat keinen nachrichtendienstlichen Wert.

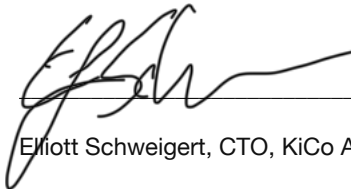
Was dieses Ergebnis ausdrücklich nicht deckt: die in Abschnitt 8.4 genannten Prüfpunkte. Sie ändern das Ergebnis nicht, aber sie sind nicht abgearbeitet, und dieses Dokument stellt sie nicht als abgearbeitet dar.

10. Nächste Überprüfung

Dieses Dokument wird spätestens im **September 2027** erneut bewertet, darüber hinaus bei Eintritt eines der folgenden Ereignisse:

- Der Gerichtshof erklärt den Angemessenheitsbeschluss für das EU-US Data Privacy Framework für ungültig.
- Die Zertifizierung eines Empfängers der Stufe B endet, wird widerrufen oder geht in den Status "Inactive" über. **Die Prüfung erfolgt gegen den Rechtsträger, nicht gegen die Marke.**
- Die US-Rechtslage ändert sich wesentlich, insbesondere durch Aufhebung oder Änderung der Executive Order 14086.
- Ein Behördenzugriff auf Daten bei einem der Empfänger wird bekannt.
- Ein Empfänger kommt hinzu, fällt weg oder ändert seinen Verarbeitungsort oder seine Unterauftragnehmer wesentlich.
- Die verarbeiteten Datenkategorien ändern sich wesentlich, insbesondere wenn besondere Kategorien nach Art. 9 hinzukämen.
- Das indonesische Regime wird am 16.01.2027 wirksam und die dortige Aufsichtsbehörde wird errichtet; die Einordnung in Abschnitt 5.2 ist dann nachzuprüfen.

Vancouver, den [Datum]

 08.09.26
Elliott Schweigert, CTO, KiCo AI LLP