AGENTENKOLLEGE · DAVID KOGAN

Drittland-Transfer-Bewertung

Transfer Impact Assessment · Art. 44 ff. DSGVO · Stand: Mai 2026 · agentenkollege.de

Entwurf zur Prüfung. Diese Vorlage wurde sorgfältig erstellt, ist jedoch vor dem Einsatz mit Kunden anwaltlich bzw. datenschutzrechtlich zu prüfen. Die Rechtslage zu Drittlandtransfers ist in Bewegung und laufend zu beobachten.

1. Zweck und Rechtsrahmen

Dieses Dokument dient der Dokumentation und Bewertung von Übermittlungen personenbezogener Daten in Drittländer im Sinne von Art. 44 ff. DSGVO, die im Rahmen des Betriebs von Managed-KI-Agenten durch **David Kogan (Geschäftsbezeichnung: Agentenkollege)** als Auftragsverarbeiter entstehen.

Rechtsgrundlage für Drittlandübermittlungen sind nach Kapitel V DSGVO entweder ein Angemessenheitsbeschluss der EU-Kommission (Art. 45 DSGVO), geeignete Garantien (insbesondere EU-Standardvertragsklauseln nach Art. 46 DSGVO) oder Ausnahmen für bestimmte Situationen (Art. 49 DSGVO). Das Urteil des Europäischen Gerichtshofs vom 16. Juli 2020 ("Schrems II", C-311/18) hat klargestellt, dass allein das formale Vorliegen einer Übermittlungsgrundlage nicht ausreicht; ergänzend ist zu prüfen, ob das Drittland ein dem EU-Niveau im Wesentlichen gleichwertiges Schutzniveau bietet. Wo dies nicht der Fall ist, sind ergänzende technische und organisatorische Maßnahmen (Supplementary Measures) zu treffen.

Diese Transfer Impact Assessment (TIA) dokumentiert:

- alle relevanten Datenflüsse in Drittländer außerhalb des EWR,
- die jeweils anwendbare Übermittlungsgrundlage,
- eine Risikoeinschätzung für jedes betroffene Drittland sowie
- die ergriffenen ergänzenden Schutzmaßnahmen.

Auftragsverarbeiter (Ersteller dieser Bewertung): David Kogan, Engernweg 79, 33100 Paderborn, Deutschland · datenschutz@agentenkollege.de · agentenkollege.de

2. Übersicht der Datenflüsse

Der Betrieb der KI-Agenten erfolgt auf dedizierten Ubuntu-VMs bei **Hetzner Cloud in Deutschland** (Rechenzentren Nürnberg und Falkenstein). Für das Hosting selbst findet damit **kein Transfer in ein Drittland** statt; es handelt sich um eine rein innereuropäische Verarbeitung durch einen deutschen Auftragsverarbeiter.

Drittlandbezug entsteht ausschließlich durch den Einsatz bestimmter Sub-Auftragsverarbeiter für spezialisierte Dienste (LLM-Inferenz, SaaS-Integrationen, Mailboxen). Die folgende Tabelle gibt einen Überblick aller relevanten Empfänger:

Empfänger / Dienst	Land	Funktion im Agenten-Stack	Übermittelte Datenkategorien	Transfer-Grundlage
Hetzner Cloud GmbH	Deutschland (EU)	VM-Hosting, Rechen- und Speicherinfrastruktur	Alle auf der VM verarbeiteten Daten	**Kein Drittlandtransfer**; Verarbeitung in Deutschland
Cloudflare Germany GmbH	Deutschland (EU)	CDN, TLS-Terminierung, DDoS-Schutz (EU-Rechenzentren)	Verbindungsmetadaten, ggf. HTTP-Anfragen	**Kein Drittlandtransfer**; EU-Verarbeitung konfiguriert
Stripe Technology Europe Ltd.	Irland (EU)	Zahlungsabwicklung (Kundenseite)	Zahlungs- und Rechnungsdaten	**Kein Drittlandtransfer**; Irland ist EU-Mitgliedstaat
Z.AI / GLM (EU-Modell-Variante)	EU / EWR	LLM-Inferenz (EU-Hosting-Variante)	Prompt-Inhalte, Kontext	**Kein Drittlandtransfer**; EU-Hosting gewählt
OpenAI, LLC	USA	LLM-Inferenz (GPT-Modelle)	Prompt-Inhalte, Kontext, ggf. Nutzerdaten im Prompt	EU-US Data Privacy Framework (Angemessenheitsbeschluss) und/oder SCC Modul 2 (**je nach DPF-Zertifizierungsstatus zu prüfen**)
Anthropic, PBC	USA	LLM-Inferenz (Claude-Modelle)	Prompt-Inhalte, Kontext, ggf. Nutzerdaten im Prompt	EU-US Data Privacy Framework (Angemessenheitsbeschluss) und/oder SCC Modul 2 (**je nach DPF-Zertifizierungsstatus zu prüfen**)
Composio, Inc.	USA	SaaS-Integrationen (Tool-Layer, 250+ Konnektoren)	API-Zugangsdaten, Workflow-Daten, ggf. Kunden- und Geschäftsdaten	SCC Modul 2 (Art. 46 Abs. 2 lit. c DSGVO) und/oder DPF (**DPF-Status prüfen**)
AgentMail	USA	Dedizierte Mailboxen pro Agent	E-Mail-Inhalte, Empfänger-/Absenderdaten, ggf. personenbezogene Kommunikationsinhalte	SCC Modul 2 (Art. 46 Abs. 2 lit. c DSGVO) und/oder DPF (**DPF-Status prüfen**)

Hinweis: Modelle aus der Volksrepublik China (insbesondere Moonshot AI / Kimi) werden von Agentenkollege nicht eingesetzt. Eine Drittstaaten-Übermittlung in die VR China findet daher im Rahmen dieses Auftrags nicht statt. Abschnitt 5 dokumentiert die zugrunde liegende Risikoabwägung.

3. Transfer-Grundlagen

3a. EU-Standardvertragsklauseln (SCC)

Für US-Anbieter, die nicht oder nicht mehr gültig nach dem EU-US Data Privacy Framework (DPF) zertifiziert sind, werden die EU-Standardvertragsklauseln gemäß Durchführungsbeschluss (EU) 2021/914 der Kommission vom 4. Juni 2021 als Übermittlungsgrundlage nach Art. 46 Abs. 2 lit. c DSGVO herangezogen.

Anwendbares Modul: **Modul 2 (Verantwortlicher → Auftragsverarbeiter)**, da Agentenkollege als Auftragsverarbeiter des Kunden (Verantwortlicher) handelt und die Sub-Auftragsverarbeiter ihrerseits als Unter-Auftragsverarbeiter tätig sind. Im Verhältnis Agentenkollege ↔ Sub-Auftragsverarbeiter (US) kommen die SCC in der Konstellation Auftragsverarbeiter → Unter-Auftragsverarbeiter (Modul 3) in Betracht. Die genaue Modulwahl ist im jeweiligen Einzelvertrag zu dokumentieren.

Wichtig: Die SCC verpflichten den Datenimporteur, den Datenexporteur unverzüglich zu informieren, wenn er von Behörden mit Zugriffsbegehren konfrontiert wird, und sofern rechtlich zulässig dagegen vorzugehen.

3b. EU-US Data Privacy Framework (DPF)

Am 10. Juli 2023 hat die EU-Kommission den Angemessenheitsbeschluss gemäß Art. 45 DSGVO für das EU-US Data Privacy Framework erlassen (Durchführungsbeschluss (EU) 2023/1795). Für US-Unternehmen, die nach dem DPF zertifiziert sind, kann die Übermittlung auf diesen Angemessenheitsbeschluss gestützt werden, ohne dass ergänzend SCC erforderlich wären.

Voraussetzung ist eine **gültige, aktive DPF-Zertifizierung** des jeweiligen US-Anbieters. Dies ist vor Abschluss des Auftragsverarbeitungsvertrags und danach regelmäßig zu prüfen (Zertifizierungsliste unter *dataprivacyframework.gov*). Der Zertifizierungsstatus sowie das Prüfdatum sind im Tenant-AVV des jeweiligen Kunden zu dokumentieren.

> **Handlungspflicht:** Agentenkollege prüft vor Einsatz jedes US-Anbieters dessen DPF-Zertifizierungsstatus und hält das Ergebnis mit Prüfdatum im Tenant-AVV fest. Ist keine gültige DPF-Zertifizierung vorhanden, werden SCC Modul 2/3 geschlossen. Bei Verlust der Zertifizierung ist auf SCC umzustellen oder der Anbieter auszutauschen.

4. Bewertung USA

4a. Rechtsrahmen und behördliche Zugriffsmöglichkeiten

Die USA verfügen über weitreichende Geheimdienstgesetze, die potenziellen Behördenzugriff auf bei US-Unternehmen gespeicherte oder verarbeitete Daten erlauben. Besonders relevant ist **Section 702 des Foreign Intelligence Surveillance Act (FISA 702)**, der US-Nachrichtendiensten, insbesondere der NSA, die massenhafte Erhebung von Kommunikationsdaten elektronischer Kommunikationsanbieter unter gerichtlicher Aufsicht (FISC) gestattet. Ergänzend bestehen Befugnisse nach Executive Order 12.333. Das "Schrems II"-Urteil des EuGH (C-311/18) hat festgestellt, dass allein die SCC kein gleichwertiges Schutzniveau garantieren, solange US-Recht derartige Zugriffe ermöglicht.

4b. Verbesserungen durch das EU-US Data Privacy Framework

Das DPF adressiert die im Schrems-II-Urteil identifizierten Defizite durch mehrere US-seitige Maßnahmen:

- **Executive Order 14086** (Oktober 2022): Beschränkung von Geheimdienstaktivitäten auf das Notwendige und Verhältnismäßige; Einführung neuer Rechtsschutzmechanismen für EU-Bürger.
- **Data Protection Review Court (DPRC)**: Unabhängige Beschwerdeinstanz für EU-Bürger bei behaupteten Datenschutzverletzungen durch US-Nachrichtendienste.
- **Jährliche Überprüfung** des DPF durch EU-Kommission und US-Behörden.

Der Angemessenheitsbeschluss der EU-Kommission vom Juli 2023 bewertet das durch das DPF geschaffene Schutzniveau als dem EU-Recht im Wesentlichen gleichwertig. Gleichwohl ist zu beachten, dass datenschutzrechtliche Klagen gegen das DPF vor dem EuGH anhängig sein können; die Rechtslage ist laufend zu beobachten.

4c. Gesamtbewertung USA

Das Risiko eines unbefugten behördlichen Zugriffs auf die von LLM- und Tool-Anbietern verarbeiteten Daten wird als **mittel** eingestuft. Der Einsatz von DPF-zertifizierten Anbietern reduziert das Risiko auf ein vertretbares Maß; wo keine DPF-Zertifizierung vorliegt, bieten SCC in Verbindung mit den unter Abschnitt 6 genannten ergänzenden Maßnahmen ein angemessenes Schutzniveau. Für datenschutzkritische Verarbeitungen (z. B. besondere Kategorien personenbezogener Daten gem. Art. 9 DSGVO) empfiehlt Agentenkollege den Einsatz der EU-Modell-Variante.

5. Bewertung China (kein Einsatz)

Agentenkollege setzt **keine LLM-Anbieter mit Sitz in der Volksrepublik China** ein. Insbesondere kommen Modelle von Moonshot AI / Kimi nicht zum Einsatz, weder im Standardfall noch als optionale Variante. Eine Datenübermittlung in die VR China findet im Rahmen dieses Auftrags daher nicht statt.

5a. Begründung der Entscheidung

Für die Volksrepublik China besteht kein Angemessenheitsbeschluss der EU-Kommission. Das chinesische Recht enthält weitreichende staatliche Zugriffsbefugnisse auf Daten, die bei in China ansässigen Unternehmen verarbeitet werden, insbesondere durch:

- **Nationales Geheimdienstgesetz (NSG, Art. 7)**: Verpflichtung aller Organisationen und Bürger zur Unterstützung staatlicher Geheimdiensttätigkeit.
- **Cybersicherheitsgesetz (CSL) und Datensicherheitsgesetz (DSL)**: Weitreichende Befugnisse zur Datenlokalisierung und staatlichen Datenzugang.
- **Fehlen eines unabhängigen Rechtsschutzes** für betroffene EU-Bürger gegen staatliche Zugriffsmaßnahmen.

Das Risiko eines unbefugten staatlichen Zugriffs ist damit strukturell höher als bei US-Anbietern, da keine dem DPF vergleichbaren Schutzgarantien existieren. Die mit einem Einsatz verbundenen Compliance-Aufwände (gesonderte Einwilligung pro Kunde, vertiefte TIA-Prüfung, expliziter Subprozessor-Eintrag) stehen aus Sicht von Agentenkollege in keinem angemessenen Verhältnis zum Mehrwert; EU- und US-Modelle decken die im Katalog vorgesehenen Use-Cases vollständig ab.

5b. Alternative Modelle

Für Use-Cases mit geringem bis mittlerem Sensitivitätsbedarf kommt vorrangig die EU-Variante zum Einsatz: **Z.AI / GLM 5.1 (EU-Hosting)** oder **Mistral Large (EU)**. Beide Anbieter unterhalten EU-Infrastruktur, sodass eine Drittstaaten-Übermittlung für die LLM-Inferenz entfällt. Für Use-Cases, die US-Modelle erfordern (z. B. GPT-5.5, Claude Opus), erfolgt die Übermittlung auf Grundlage des DPF und/oder SCC (siehe Abschnitt 4).

6. Ergänzende Maßnahmen (Supplementary Measures)

Gemäß den EDPB-Empfehlungen 01/2020 zu Maßnahmen als Ergänzung zu Übermittlungsinstrumenten setzt Agentenkollege folgende technische und organisatorische Maßnahmen ein:

6a. Technische Maßnahmen

- **Transportverschlüsselung (TLS 1.2/1.3):** Alle Kommunikationsverbindungen zwischen der Agent-VM und externen Sub-Auftragsverarbeitern sind zwingend TLS-verschlüsselt. Eine unverschlüsselte Übermittlung ist technisch ausgeschlossen.
- **Dedizierte VM-Isolation:** Jeder Agent läuft auf einer dedizierten Ubuntu-VM bei Hetzner Cloud in Deutschland. Mandantentrennung ist durch VM-Isolation auf Infrastrukturebene sichergestellt; kein Shared-Memory-Zugriff zwischen Kundeninstanzen.
- **Keine Persistenz bei LLM-Anbietern:** API-Anfragen an LLM-Anbieter werden so konfiguriert, dass keine Speicherung von Prompt-Daten für Trainings- oder andere Zwecke durch den Anbieter erfolgt (soweit technisch und vertraglich sichergestellt). Entsprechende Data-Processing-Agreements sind abzuschließen.

6b. Datenminimierung und Zweckbindung

- **Prompt-Minimierung:** An LLM-APIs werden nur die für die jeweilige Aufgabe notwendigen Daten übermittelt. Unnötige personenbezogene Daten werden im Prompt nicht aufgenommen.
- **Zweckbindung:** Sub-Auftragsverarbeiter werden vertraglich (SCC/DPA) auf die Verarbeitung ausschließlich für die beauftragten Zwecke verpflichtet. Eine Nutzung für eigene Zwecke (Training, Produktverbesserung) ist vertraglich auszuschließen.
- **Datenkategorien-Beschränkung:** Besondere Kategorien personenbezogener Daten (Art. 9 DSGVO), insbesondere Gesundheits-, Religions- oder politische Daten, werden standardmäßig nicht an US-Anbieter übermittelt, es sei denn, der Kunde hat dies ausdrücklich beauftragt und eine entsprechende Risikoabwägung liegt vor. China-Anbieter werden grundsätzlich nicht eingesetzt.

6c. Organisatorische Maßnahmen

- **Vertragliche Absicherung:** Mit allen Sub-Auftragsverarbeitern werden Auftragsverarbeitungsverträge nach Art. 28 DSGVO (bzw. SCC) geschlossen, die auch die jeweiligen EDPB-konformen Zusatzklauseln zu Behördenbegehren enthalten.
- **Laufende Überwachung:** DPF-Zertifizierungsstatus der US-Anbieter wird mindestens halbjährlich geprüft. Änderungen der Rechtslage (insbesondere EuGH-Urteile zum DPF) werden beobachtet und bei Relevanz unverzüglich umgesetzt.
- **Sub-Auftragsverarbeiter-Transparenz:** Der Kunde erhält im Tenant-AVV eine vollständige, aktuelle Liste aller Sub-Auftragsverarbeiter einschließlich deren Drittlandstatus. Änderungen werden dem Kunden rechtzeitig vorab mitgeteilt.

6d. EU-Only-Variante als Alternative

- Agentenkollege bietet optional eine **vollständige EU-Only-Konfiguration** an: Hosting bei Hetzner Cloud Deutschland (Standard), LLM-Inferenz ausschließlich über EU-Anbieter (Z.AI / GLM mit EU-Hosting, Mistral). In dieser Konfiguration entstehen keinerlei Drittlandtransfers.
- Für Kunden mit besonders strengen Datenschutzanforderungen wird diese Variante aktiv empfohlen und als Standardkonfiguration angeboten.

7. Ergebnis

Die Gesamtbewertung ergibt folgendes Bild:

Bereich	Ergebnis
Hosting (Hetzner Cloud, Deutschland)	Kein Drittlandtransfer. Verarbeitung ausschließlich in Deutschland durch deutschen Auftragsverarbeiter. Standard-AVV nach Art. 28 DSGVO ausreichend.
LLM-Inferenz USA (OpenAI, Anthropic)	Transfer auf Basis DPF-Angemessenheitsbeschluss (bei gültiger Zertifizierung) oder SCC Modul 2/3. Ergänzende Maßnahmen (TLS, Prompt-Minimierung, No-Training-Klauseln) reduzieren Risiko auf vertretbares Maß.
Tool-Layer USA (Composio)	Transfer auf Basis DPF (bei Zertifizierung) oder SCC Modul 2/3. Datenminimierung und Zweckbindung vertraglich sichergestellt.
Mailbox USA (AgentMail)	Transfer auf Basis DPF (bei Zertifizierung) oder SCC Modul 2/3. E-Mail-Inhalte sind per TLS verschlüsselt.
LLM-Inferenz China	Nicht im Einsatz. Modelle aus der Volksrepublik China (insbesondere Moonshot AI / Kimi) werden von Agentenkollege nicht eingesetzt; eine Übermittlung nach China findet nicht statt.
EU-Only-Konfiguration	Vollständig EU-intern (Z.AI/GLM EU oder Mistral EU); kein Drittlandtransfer. Empfehlung für Kunden mit erhöhten Datenschutzanforderungen.

Agentenkollege gelangt zu dem Ergebnis, dass die eingesetzten Übermittlungsgrundlagen (DPF-Angemessenheitsbeschluss, SCC Modul 2/3) in Verbindung mit den beschriebenen ergänzenden technischen und organisatorischen Maßnahmen ein dem EU-Datenschutzrecht entsprechendes Schutzniveau für die durchgeführten Drittlandübermittlungen gewährleisten.

> **Vorbehalt laufender Rechtsentwicklung:** Die Rechtslage zu Drittlandtransfers, insbesondere die Beständigkeit des EU-US Data Privacy Framework und mögliche Folgeklagen vor dem EuGH, ist dynamisch. Diese Transfer Impact Assessment wird regelmäßig, mindestens jährlich sowie anlassbezogen bei wesentlichen Rechtsänderungen, überprüft und aktualisiert. **Datum der letzten Überprüfung: Mai 2026.**

Agentenkollege · David Kogan · Engernweg 79 · 33100 Paderborn · datenschutz@agentenkollege.de