Briefing von **Alexander Alber** · Gründer inzpyre.me · KI-Consulting für KMU

Stand: Mai 2026

KI-Agent für den Mittelstand: Datenschutz-Optionen & Empfehlung

Wie sicher ist KI wirklich, und welche Option passt zu dir? **Ein ehrlicher Überblick — damit du weißt, wo du stehst und welcher Weg zu deinem Betrieb passt.**

Damit du dich orientieren kannst und siehst, welche Option zu dir passt.

1 Die ehrliche Ausgangslage

Wenn du KI in deinem Betrieb einsetzen willst, kommen meistens zwei Sorgen auf. Beide sind berechtigt — und sie haben unterschiedliche Antworten.

SORGE 1

„Ist das rechtlich sauber?"

Lösbar mit Standard-Werkzeugen. Mit den Geschäftskunden-Tarifen lässt sich ein AVV schließen, es wird nicht auf den Daten trainiert, internationale Übermittlungen sind über SCCs abgesichert. **DSGVO-vertretbar.**

SORGE 2

„Wo liegen meine Daten physisch?"

Hier unterscheiden sich die Optionen wirklich. Nicht um Verträge, sondern um den tatsächlichen Ort der Verarbeitung und ob eine US-Firma im Spiel ist.

Der wichtigste Fakt, den viele übersehen: Das normale Claude-Abo verarbeitet die Daten per Default auf **US-Infrastruktur**. Wer die Verarbeitung in der EU halten will, muss Claude über AWS Bedrock oder Google Vertex in einer EU-Region nutzen — nur über eine **eigene Anbindung**, nicht über das fertige Chat-Abo.

2 Die vier Fragen, kurz beantwortet

AV-Vertrag (AVV) mit Anthropic?	**Ja** · Claude Team, Enterprise, API unter Commercial Terms. DPA automatisch Bestandteil.
Kein Training auf meinen Daten?	**Ja** · vertraglich zugesichert für alle Geschäftskunden-Tarife und die API.
Kurze oder keine Speicherung?	**Teils** · API-Standard 7 Tage. Zero Data Retention für Enterprise-API per Vereinbarung möglich.
Bleiben die Daten in der EU?	**Nur über Umweg** · Standard-Claude-Abo = US-Verarbeitung. EU-Verarbeitung nur via AWS Bedrock EU / Google Vertex EU, also über einen Custom-Build.

3 Die Optionen im Abgleich

OPTION	DATEN	TRAINING	WORAUF VERTRAUEN	HAUPTRISIKO	KOSTEN
0 · Gratis-Chat ChatGPT/Claude privat	**USA**	Möglich	Standard-Datenschutzerklärung	Kein AVV, Mitarbeiter pasten alles rein	0 €
1 · Claude Team / Enterprise mit AVV	**USA** (SCC)	Nein (vertraglich)	Anthropic (US) + SCC	US-Verarbeitung; keine Integration	~25 €/ Nutzer/ Monat
2 · Custom-Agent + Claude über AWS Bedrock EU EMPFEHLUNG	**EU** (Frankfurt)	Nein; ZDR möglich	AWS/Anthropic — EU-Region	US-Mutterkonzern trotz EU-Region	~120–450 €/Mo + Bau
3 · Custom-Agent + Open-Source bei DE-Hoster z.B. IONOS	**EU / DE**	Nein	EU-Hoster (deutsche Firma)	Schwächere Modellqualität, mehr Feintuning	~200–600 €/Mo + Bau
4 · Eigene GPU, alles im Haus	**Im Haus**	Nein	Nur dich selbst	Hohe Kosten, eigene Wartung	700–2.400 €/ Mo oder Kauf 7–10k €

Hinweis: *Optionen 1–4 sind alle DSGVO-tauglich machbar. Sie unterscheiden sich im* **Ort der Verarbeitung** *und darin, wer technisch Zugriff haben könnte.*

4 Was den Custom-Agent vom Chat-Abo unterscheidet

Ein Chat-Abo und ein Custom-Agent sind **nicht „dasselbe, nur sicherer"**. Sie machen verschiedene Dinge.

1 Datenminimierung

Der Agent schickt pro Aufgabe nur die Felder ans Modell, die er wirklich braucht. Beim Chat-Abo kippt der Mitarbeiter im Stress oft das ganze Dokument rein.

Daten bleiben in eigenen Systemen

Der Agent liest aus und schreibt zurück in sevDesk, HubSpot, OneDrive. Wissen liegt auf einem Server, den du kontrollierst.

3 EU-Verarbeitung erst möglich

Nur über die Bedrock-/Vertex-EU-Anbindung bleiben die Daten in Frankfurt. Das fertige Abo kann das nicht.

Er erledigt die Arbeit

Der Agent automatisiert komplette Abläufe über mehrere Tools. Das Chat-Abo ist eine Box, in die ma copy-pastet.

Anbieter-unabhängig

Das Modell ist austauschbar. Wird Claude EU zu teuer, wechselt man auf Mistral oder einen EU-Hoster, ohne neu zu bauen.

5 Empfehlung & Entscheidungslogik

> **Die Faustregel:** Welche Option für dich passt, hängt davon ab, welche der beiden Sorgen für dich im Vordergrund steht.

Wenn dir eine Chat-Hilfe reicht und EU nicht das Hauptthema ist

Dann reicht **Option 1 (Claude Team mit AVV)** — ein fertiges Abo. Ich helfe bei Tarifwahl, AVV und Schulung.

Wenn du Abläufe automatisieren willst — und EU-Verarbeitung brauchst

Dann ist **Option 2 (Custom-Agent + Claude über AWS Bedrock EU)** der beste Kompromiss. Verarbeitung in Frankfurt, kein Training, optional ZDR — plus echte Automatisierung.

Wenn keine US-Firma deine Daten anfassen darf

Dann ist **Option 3 (Open-Source-Modell bei deutschem Hoster)** dein Weg — auch das Modell läuft bei einer EU-Firma. Etwas teurer, dafür maximale Souveränität.

Wenn deine Daten das Haus nie verlassen dürfen

Dann lohnt sich **Option 4 (eigene GPU im Haus)** — Daten bleiben bei dir. Für die meisten überdimensioniert, bei strenger Compliance die richtige Wahl.

> **Wichtig — egal welche Option:** DSGVO ist mehr als der Verarbeitungsort. Verarbeitungsverzeichnis, Zugriffsrechte, Löschkonzept. Bei Rechnungen, Verträgen, Kundenmails bleibt ein **Mensch in der Schleife**: der Agent bereitet vor, der Mensch bestätigt.

MEIN ANGEBOT FÜR DICH

Erst schauen wir, was geht. Dann richte ich es ein.

1. **Gratis-Assessment:** Welche Themen hast du, welche Option passt?
2. Ich richte den passenden Weg ein, DSGVO-konform und mit EU-Verarbeitung wo nötig.
3. Du zahlst nur die Einrichtungszeit. Das Assessment kostet nichts.

→ Lust drauf? **Schreib mir.**
Ich zeige dir an deinem eigenen Betrieb, was geht.

Alexander Alber · inzpyre.me · KI-Consulting für den Mittelstand · We are Builders · info@inzpyre.me

QUELLEN & HINWEIS

anthropic.com (Commercial Terms, Datenrichtlinien Mai 2026) · compound.law/claude-enterprise (EU Data Residency) · AWS Bedrock / Google Vertex EU-Regionen · Modell-Tarife und EU-Residenz-Optionen ändern sich; vor Vertragsschluss aktuelle Konditionen und AVV prüfen.