Sicherheitsüberblick

Modell, Hosting, Verträge und Prüfung bei Intellagens

Stand: 8. November 2026 · Intellagens · kontakt@intellagens.de

Auf einen Blick

Claude ist unsere erste Wahl für Agenten-Qualität. Sie entscheiden über Hosting und Modell. Wo Daten besonders geschützt sein müssen, setzen wir offene Modelle bei einem Anbieter in der EU ein. Dürfen sie das Haus nicht verlassen, läuft das Modell auf einem Server bei Ihnen.

Dieser Überblick nennt, was wir zusagen, in welchen Abläufen wir arbeiten und wo unsere Grenzen liegen. Er enthält nur Zusagen und Abläufe, keine Angaben zu unserer eigenen Infrastruktur, die wir nicht belegen können.

Drei Hosting-Stufen

Hinter einer einheitlichen Schnittstelle (einer selbst gehosteten Vermittlungsschicht nach dem quelloffenen Baustein LiteLLM) sind die Modelle austauschbar. Sie wählen die Stufe.

Stufe	Inhalt	Für wen	Stand
Cloud-EU	Claude über Amazon Bedrock oder Google Vertex in einer europäischen Region.	Unternehmen mit bestehendem Cloud-Vertrag bei AWS oder Google.	Europa ist für beide Dienste gelistet. Regionale Endpunkte halten Speicherung und Verarbeitung in der Region.
Souverän	Offene Modelle (Mistral, gpt-oss) bei einem Anbieter mit Rechenzentren in Deutschland, etwa STACKIT (Region eu01).	Unternehmen mit strengen Datenvorgaben.	STACKIT betreibt seine Regionen ausschließlich in Deutschland (eu01) und Österreich (eu02); bei anderen Anbietern wie IONOS klären wir den Standort im Vertrag. Die Qualität belegen wir im Modellwechsel-Test.
Vor Ort	Modelle auf einem Server in Ihrem Haus.	Unternehmen, deren Daten das Haus nicht verlassen dürfen.	auf Anfrage

Quellen:

- Anthropic: Regional Compliance
- STACKIT Docs: AI Model Serving
- STACKIT Docs: Regionen
- IONOS: AI Model Hub

Der Weg Ihrer Daten

Für jedes Projekt zeichnen wir den Datenfluss konkret auf und legen ihn Ihnen vor dem Start vor. Der Weg:

1. **Eingang:** Ihre Mail, Liste oder Schnittstelle
2. **Vermittlungsschicht:** Schlüssel, Budgets, Modellwahl
3. **Modell:** in der gewählten Stufe
4. **Prüfoberfläche:** Ihr Team sieht jeden Vorschlag
5. **Ihre Software:** ERP oder Postfach

Unter allen Schritten läuft ein Protokoll.

Was wir zusagen

- Ein Datenfluss-Diagramm für Ihr Projekt, bevor Daten fließen.
- Die Liste der Auftragsverarbeiter und Unterauftragnehmer vor dem Start.
- Den Vertrag zur Auftragsverarbeitung, bevor die ersten Daten verarbeitet werden.
- Einen Modellwechsel-Test: dieselben Prüffälle auf mindestens zwei Modellen.
- Den Hinweis, welches Modell wo verarbeitet.
- Kein Training mit Ihren Daten. Das regeln die Verträge mit den Diensten, wir legen sie vor dem Start offen.
- Jede Lieferung prüft ein Mensch, bevor sie zu Ihnen geht.
- Wir legen offen, wo KI eingesetzt wird.

Was wir nicht versprechen

- Hundert Prozent Souveränität. Auch mit EU-Region unterliegen US-Cloudanbieter weiter US-Recht.
- Gleiche Qualität auf allen Modellen. Offene Modelle liegen bei Agentenaufgaben vermutlich zurück. Wir messen das im Modellwechsel-Test.
- Ein Gütesiegel für Datenschutz. Ob ein Einsatz rechtmäßig ist, hängt von Ihrem Fall ab.
- Dass eine Rechtspflicht, etwa aus der KI-Verordnung, mit uns erledigt ist.

Auftragsverarbeitung und Unterauftragnehmer

1. **Vor dem Auftrag.** Sie erhalten Datenfluss-Diagramm, Liste der Unterauftragnehmer und Entwurf des Vertrags zur Auftragsverarbeitung.
2. **Prüfung bei Ihnen.** Datenschutz, Einkauf und, wo nötig, der Betriebsrat prüfen die Unterlagen. Änderungen arbeiten wir ein.
3. **Vor den ersten Daten.** Der Vertrag ist unterschrieben. Erst danach verarbeiten wir Daten.
4. **Im Betrieb.** Wechselt ein Unterauftragnehmer oder ein Modell, informieren wir Sie vorab schriftlich.

Modellwechsel-Test

Vor dem Betrieb lassen wir dieselben Prüffälle auf mindestens zwei Modellen laufen und legen Ihnen die Ergebnisse vor. So sehen Sie, was ein anderes Modell oder ein anderes Hosting leistet, bevor Sie sich festlegen.

Prüfung durch Menschen

Jede Lieferung prüft ein Mensch, bevor sie zu Ihnen geht. Was ein Agent nicht entscheiden soll, legen wir mit Ihrer Abteilung vorab fest. Es bleibt bei Ihrem Team.

Unterlagen für Ihren Einkauf

Vor dem Start erhalten Sie:

- Vertrag zur Auftragsverarbeitung (AVV)
- Dokument zu den technischen und organisatorischen Maßnahmen
- Liste der Unterauftragnehmer
- Ausgefüllter Sicherheitsfragebogen
- Handreichung für den Betriebsrat
- Antworten auf Fragen zur NIS2-Richtlinie

Zertifizierungsstand

Ein Zertifikat haben wir noch nicht. Unsere Sicherheitsunterlagen bekommen Sie vor dem Start.

Kontakt

Intellagens ist eine Marke von Apex Automate.

Achtern Born 85, 22549 Hamburg, Deutschland

E-Mail: kontakt@intellagens.de · Telefon: +49 174 5470224