

KI und DSGVO: heikel, *aber lösbar*

Teil 2 vom Agenten-Büro. Der einfache Weg mit Langdock, die eigene Schleife mit Presidio, der eigene GPU-Server, was das alles kostet, und die Fragen, die du jedem Anbieter stellen solltest.

@reposprites

reposprites.com

Danke fürs Folgen ✓ · Du hast kommentiert: DSGVO ✓

© 2026 REPOSPRITES · @reposprites · reposprites.com · Persönliches Exemplar, Weitergabe und Verkauf nicht gestattet · ID RS-20261103-F78F92BF



DER MENTOR SAGT

Orientierung, keine Rechtsberatung. Bei sensiblen Daten (Gesundheit, Mandanten, Beschäftigte) sprich mit deinem Datenschutzbeauftragten.



DER MENTOR SAGT

Unabhängig: Ich stehe in keiner Verbindung zu Langdock, und es gibt keine Werbepartnerschaft. Alles hier beruht auf meiner eigenen Erfahrung und Recherche.

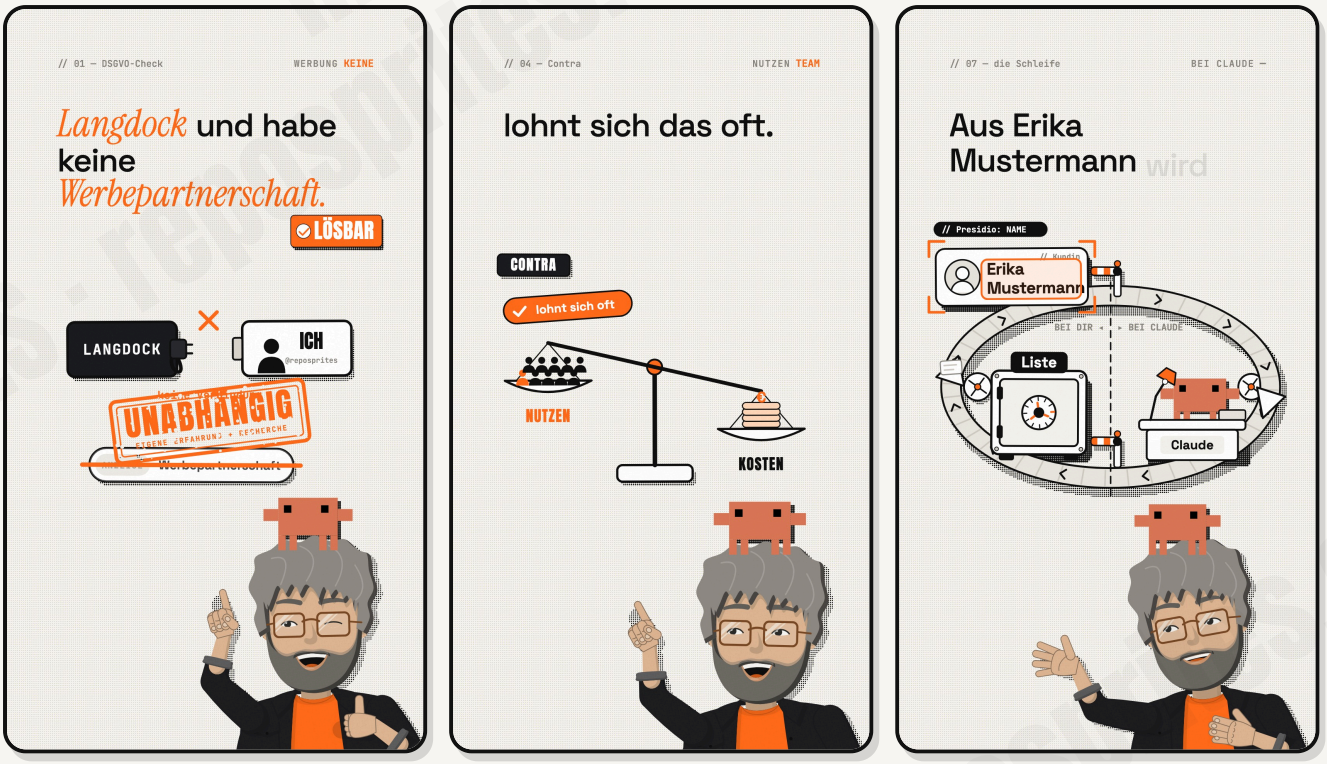
// 01

Auf einen Blick

	LANGDOCK	EIGENE SCHLEIFE	EIGENER GPU-SERVER
Für wen	Teams, die Claude ohne Technik nutzen wollen	Wer Claude nutzt und Namen und Kundendaten selbst schützen will	Wer offene Modelle ganz auf eigener Hardware betreiben will
Technik nötig	Keine, läuft im Browser	Ja: Presidio, ein Gateway oder Hooks	Ja, und zwar am meisten: Server, Updates, Sicherheit
Was das Modell sieht	Deine Eingaben, wie du sie schreibst	Nur Platzhalter wie `<PERSON_1>`	Alles, aber auf deinem Server
Vertrag	AVV automatisch in den AGB	AVV mit deinem Modell-Anbieter bleibt nötig	AVV mit dem Hoster (bei Hetzner im Kundenkonto)
Kosten	Lizenz pro Kopf: Business laut Preisseite 25 € netto pro Nutzer und Monat	Software kostenlos (Open Source), dazu Modellkosten und deine Zeit	Feste Miete, laut Hetzner ab 214 € netto im Monat, dazu deine Zeit
Grenze	Kosten wachsen mit jedem Kopf	Findet nicht alles, Stichproben nötig	Claude läuft dort nicht, nur offene Modelle

© 2026 REPOSPRITES · @reposprites · reposprites.com · Persönliches Exemplar, Weitergabe und Verkauf nicht gestattet · ID RS-20261103-F78F92BF

// AUS DEM VIDEO



// 02

Meine Erfahrung

Ich habe Langdock lange selbst genutzt und war sehr zufrieden. Es war für mich der schnellste Weg, Claude im Alltag einzusetzen, ohne mich um Technik zu kümmern.

Mit der Zeit habe ich mehr Technik verstanden. Ich habe eigene Server aufgesetzt und GPU-Server bei Hetzner gemietet, um offene KI-Modelle selbst zu betreiben. Seitdem sehe ich beide Seiten: wie bequem ein fertiges Werkzeug ist, und was es heißt, alles selbst in der Hand zu haben, mit allen Vor- und Nachteilen.

Darum steht in diesem Leitfaden kein „das eine ist besser“. Es kommt darauf an, wie viele Leute damit arbeiten, wie oft, mit welchen Daten, und wie viel Technik du dir zutraust.

© 2026 REPOSPRITES · @reposprites · reposprites.com · Persönliches Exemplar, Weitergabe und Verkauf nicht gestattet · ID RS-20261103-F78F92BF

// 03

Weg 1: Langdock, der einfache Weg

Langdock ist ein KI-Arbeitsplatz aus Berlin im Browser: Chat, Agenten, Workflows, mit Claude und anderen Modellen. Ich stehe in keiner Verbindung zu Langdock, das hier ist meine eigene Erfahrung und Recherche.

Pro und Contra aus meiner Erfahrung

PRO	CONTRA
Super einfach: anmelden, Modell wählen, loslegen	Lizenz pro Kopf: Jede Person im Team kostet jeden Monat
Auch für Firmen gemacht: Admin-Rollen, Team-Verwaltung, bis zu 1.000 Nutzer im Business-Tarif	Wer es nur ab und zu nutzt, zahlt trotzdem den vollen Monat
Hosting in der EU, AVV automatisch in den AGB	Workflows und API laufen zusätzlich nach Verbrauch
Viele Modelle an einem Ort, Claude inklusive	Du bist an das gebunden, was die Plattform anbietet
Keine Technik, keine Wartung, keine Updates für dich	Kein Tool macht dich automatisch DSGVO-konform, das gilt hier wie überall

- **Hosting:** Microsoft Azure mit Serverstandort in der EU. Laut Langdock laufen die Anwendung und „die meisten“ Modelle vollständig in der EU.
- **AVV:** Teil der AGB, gilt automatisch.
- **Berufsgeheimnisträger:** Im Trust Center gibt es eine Zusatzvereinbarung für Anwälte, Ärzte, Steuerberater (§ 203 StGB).
- **Sicherheit:** ISO 27001, SOC 2 Type II, AES-256, Admin-Rollen, einstellbare Aufbewahrungsfrist für Chats. Kundendaten werden laut Langdock nie zum Training von KI-Modellen genutzt. Was diese Siegel bedeuten, steht weiter unten.
- **MCP:** nur Remote-Server (HTTP oder SSE), keine lokalen.
- **Preis:** Business laut Preisseite 25 € netto pro Nutzer und Monat, Business Max 99 € (fünffache Nutzung). Details im nächsten Abschnitt.

Gut zu wissen: Langdock bietet viele Modelle verschiedener Anbieter an. Laut API-Doku laufen sie je nach Modell über AWS Bedrock, Google Vertex oder direkt beim Anbieter. Welche Region für dein Modell gilt, lässt du dir am besten schriftlich bestätigen. Eine eingebaute Funktion, die Namen vor dem Senden maskiert, habe ich nicht gefunden. Wer das braucht, kombiniert Langdock mit klaren Regeln im Team oder nimmt Weg 2.

© 2026 REPOSPRITES · @reposprites · reposprites.com · Persönliches Exemplar, Weitergabe und Verkauf nicht gestattet · ID RS-20261103-F78F92BF

Was kostet das? Lizenzgebühr für Firmen und Einzelpersonen

Laut Preisseite (geprüft am 03.11.2026, alle Preise netto):

- **Testen:** 7 Tage kostenlos, ohne Kreditkarte, mit 5 € Guthaben für KI-Modelle.
- **Business:** 25 € pro Nutzer und Monat. Chat und Agenten mit den enthaltenen Modellen kosten nichts extra nach Verbrauch.
- **Business Max:** 99 € pro Nutzer und Monat, mit fünfmal so viel Nutzung.
- **Jährlich zahlen:** laut Preisseite bis zu 20 % günstiger.
- **Extra:** Workflows und die API werden nach Verbrauch abgerechnet. Das Governance-Paket ist bis 1. Januar 2027 kostenlos, danach ab 3,50 € pro Nutzer und Monat.
- **Einzelpersonen:** Einen eigenen Tarif für eine Person habe ich nicht gefunden, du nimmst einen Business-Platz.

NUTZER	PRO MONAT (BUSINESS)	PRO JAHR, MONATLICH GEZAHLT
1	25 €	300 €
5	125 €	1.500 €
10	250 €	3.000 €
25	625 €	7.500 €

Nutzen abwägen

Die Lizenz lohnt sich, wenn sie Zeit spart, die mehr wert ist als 25 € im Monat. Eine einfache Rechnung:

- **Team, das täglich damit arbeitet:** Spart jede Person nur eine halbe Stunde pro Woche, sind das rund zwei Stunden im Monat. Bei fast jedem Stundensatz ist die Lizenz damit bezahlt. Hier lohnt es sich oft.
- **Allein und nur ab und zu:** Nutzt du es ein paarmal im Monat, zahlst du trotzdem den vollen Platz. Rechne nach, ob ein Abo direkt beim Modell-Anbieter, ein anderer Anbieter weiter unten oder Weg 2 für dich günstiger ist.
- **Viele Köpfe, gleiche Aufgaben:** Ab etwa neun Nutzern kostet Langdock Business im Monat mehr als die günstigste GPU-Miete bei Hetzner (siehe Weg 3). Das heißt nicht, dass der Server günstiger ist: Deine Zeit für Einrichtung und Pflege kommt dazu, und offene Modelle sind nicht Claude.

Meine Faustregel: Je mehr Leute es täglich nutzen und je weniger Technik im Haus ist, desto eher ist Langdock die richtige Wahl.

© 2026 REPOSPRITES · @reposprites · reposprites.com · Persönliches Exemplar, Weitergabe und Verkauf nicht gestattet · ID RS-20261103-F78F92BF

Die Siegel in einfachen Worten

Langdocks Sicherheitsseite nennt vier Punkte unter Prüfungen und Zertifikaten. Das sind gute Zeichen. Hier steht, was jeder Punkt bedeutet und wo dein eigener Teil beginnt.

SIEGEL	WAS ES BEDEUTET	WO DU GENAUER HINSCHAUST
ISO 27001, „zertifiziert“	Ein externer Prüfer hat bestätigt, dass Langdock ein funktionierendes System für Informationssicherheit betreibt: Risiken, Zugriffe, Backups, Vorfälle. Wird jedes Jahr neu geprüft.	Es gilt nur für das, was im „Geltungsbereich“ des Zertifikats steht. Die Seite nennt weder Geltungsbereich noch Prüfer oder Datum.
SOC 2 Type II, „unabhängig geprüft“	Eine US-Prüfung (AICPA-Standard). „Type II“ heißt: Der Prüfer hat über mehrere Monate kontrolliert, dass die Maßnahmen wirklich funktionieren, nicht nur auf dem Papier stehen.	Der Bericht ist nicht öffentlich, meist bekommst du ihn auf Anfrage unter NDA. Es ist eine Sicherheitsprüfung, keine Datenschutz- oder DSGVO-Prüfung.
DSGVO, „fully aligned“	Langdock führt die DSGVO unter seinen Prüfungen und Zertifikaten und sagt, es sei voll darauf ausgerichtet: AVV in den AGB, Hosting in der EU, Rechte für die Menschen, um deren Daten es geht.	Das ist Langdocks eigene Einschätzung: Ein offizielles DSGVO-Zertifikat zum Vorzeigen gibt es weder für Langdock noch für einen anderen Anbieter. Und kein Werkzeug macht *dich* DSGVO-konform: Rechtsgrundlage, Information der Betroffenen und was du eingibst, bleiben deine Aufgabe.
„Kein Modelltraining“	Laut Langdock werden deine Daten nie genutzt, um KI-Modelle zu trainieren oder zu verbessern. Anthropic und AWS Bedrock sagen dasselbe für die geschäftliche Nutzung.	Nicht trainieren heißt nicht, nicht speichern. Der Modell-Anbieter kann Anfragen trotzdem kurz aufbewahren, etwa um Missbrauch zu prüfen. Wie das pro Modell geregelt ist, steht nicht auf der Seite.

Kurz gesagt: ISO 27001 und SOC 2 Type II zeigen, dass Langdock Sicherheit ernst nimmt und sich von außen prüfen lässt. Langdock macht seinen Teil für die DSGVO, deine eigene Nutzung bleibt deine Sache. Lass dir die Zusagen schriftlich geben, im Vertrag, nicht nur auf einer Webseite.

© 2026 REPOSPRITES · @reposprites · reposprites.com · Persönliches Exemplar, Weitergabe und Verkauf nicht gestattet · ID RS-20261103-F78F92BF

Diese Fragen stellst du jedem Anbieter schriftlich, auch Langdock

- [ ] Über welches Backend und welche Region läuft das Claude-Modell, das wir nutzen?
- [ ] Werden Eingaben dort gespeichert, wie lange, und wer kann sie prüfen?
- [ ] Welche Unterauftragsverarbeiter sind beteiligt, und wo sitzen sie?
- [ ] Gibt es eine Maskierung von Namen oder Kundendaten, bevor sie ans Modell gehen?
- [ ] Was regelt die Zusatzvereinbarung für Berufsgeheimnisträger genau?
- [ ] Können wir das ISO-27001-Zertifikat (Geltungsbereich, Prüfer, gültig bis) und den SOC-2-Type-II-Bericht sehen?
- [ ] Steht „kein Training“ in unserem Vertrag, und gilt es auch beim Modell-Anbieter für unser Modell?

// 04

Weg 2: die eigene Schleife

Die Idee: Namen und Kundendaten verlassen dein Haus gar nicht erst.

1. Dein Text geht zuerst durch ein Werkzeug auf deinem Rechner, zum Beispiel Presidio.
2. Es ersetzt Namen, IBANs und Ausweisnummern durch Platzhalter: Aus Erika Mustermann wird `<PERSON_1>`.
3. Die Zuordnungsliste (`<PERSON_1>` = Erika Mustermann) bleibt bei dir.
4. Nur der Platzhalter-Text geht an Claude.
5. Die Antwort kommt mit Platzhaltern zurück, und deine Schleife setzt die echten Namen wieder ein.

© 2026 REPOSPRITES · @reposprites · reposprites.com · Persönliches Exemplar, Weitergabe und Verkauf nicht gestattet · ID RS-20261103-F78F92BF

Presidio

- Open Source, MIT-Lizenz, früher ein Microsoft-Projekt, heute Community-Projekt „Data Privacy Stack“. Letztes Release am 27.10.2026.
- Findet Namen, E-Mails, Telefonnummern, IBANs und mehr, mit Spracherkennung, Mustern und Prüfsummen. Ersetzen, schwärzen, hashen oder verschlüsseln. Es gibt auch eine Schwärzung in Bildern.
- **Deutsch:** Standard ist Englisch. Für deutsche Texte brauchst du ein deutsches Sprachmodell (spaCy). Es gibt 13 deutsche Erkenner (Steuer-ID, Personalausweis, Reisepass, Kfz-Kennzeichen, Handelsregister und mehr), die standardmäßig ausgeschaltet sind. Schalte sie ein.
- **Grenze:** Presidio sagt selbst, dass es keine Garantie gibt, alles zu finden. Ungewöhnliche Namen oder indirekte Hinweise („der Chef der Bäckerei am Marktplatz“) rutschen durch.
- **Tipp:** Lege deine Kundennamen aus dem CRM als eigene Liste an, dann findet Presidio sie sicher.

Presidio · github.com/data-privacy-stack/presidio
`github.com ↗`

`// 05`

Fertige Bausteine

- **LiteLLM Presidio-Guardrail** (Open Source): ein Gateway vor dem Modell. `pre_call` maskiert jede Anfrage, `output_parse_pii: True` setzt die Originalwerte in der Antwort wieder ein. `presidio_language: "de"` wird unterstützt. Claude Code kann über `ANTHROPIC_BASE_URL` auf so ein Gateway zeigen.
- **Claude Code Hook:** ein Wächter, der auf deinem Rechner läuft, bevor etwas rausgeht. Details im Abschnitt „Der Hook in Claude Code“ unten.
- **Nicht empfohlen:** LLM Guard ist archiviert und kann kein Deutsch. NeMo Guardrails dokumentiert nur Englisch.

LiteLLM PII-Guardrail · docs.litellm.ai
`docs.litellm.ai ↗`

Claude Code Hooks · code.claude.com
`code.claude.com ↗`

© 2026 REPOSPRITES · @reposprites · reposprites.com · Persönliches Exemplar, Weitergabe und Verkauf nicht gestattet · ID RS-20261103-F78F92BF

// 06

Der Hook in Claude Code: Gehen da nicht schon echte Daten raus?

Nein, wenn er richtig eingerichtet ist. Wichtig ist der Unterschied zwischen zwei Dingen, die fast gleich heißen:

- **Claude Code** ist ein Programm, das auf deinem Rechner läuft (oder auf deinem Server).
- **Claude**, das KI-Modell, läuft beim Anbieter: bei Anthropic, oder über AWS Bedrock in der EU.

Ein Hook ist ein kleines Skript, das Claude Code **auf deinem Rechner** startet, an festen Stellen.

So läuft es ab

1. Du tippst einen Prompt und drückst Enter.
2. Bevor irgendetwas an das Modell geht, startet Claude Code deinen `UserPromptSubmit`-Hook, lokal.
3. Der Hook prüft den Text, zum Beispiel mit Presidio oder einer Liste deiner Kundennamen.
4. Findet er Kundendaten, blockiert er (Exit-Code 2). Laut Claude-Code-Doku erreicht ein blockierter Prompt das Modell **nie**. Du bekommst eine Meldung wie „Bitte erst pseudonymisieren".
5. Findet er nichts, geht der Prompt ganz normal ans Modell.

Für Dateien gibt es einen zweiten Hook: Wenn Claude eine Datei liest, passiert das Lesen lokal. Ein `PostToolUse`-Hook kann das Ergebnis maskieren (`updatedToolOutput`), und erst der maskierte Text geht ans Modell.

Grenzen, ehrlich

- **Er stoppt nur, was er erkennt.** Ein Name, den Presidio oder deine Liste übersieht, geht mit raus. Darum Stichproben.
- **Stoppen, nicht umschreiben:** Ein `UserPromptSubmit`-Hook kann deinen Prompt nicht automatisch pseudonymisieren. Dafür nimmst du die Schleife oder den LiteLLM-Guardrail.
- **Nur lokal:** In Cloud-Sessions von Claude Code (im Browser) laufen deine lokalen Hooks nicht. Der Schutz gilt für Claude Code auf deinem Rechner oder Server.
- **Du baust ihn selbst:** Einen fertigen, geprüften Presidio-Hook für Claude Code habe ich nicht gefunden. Teste ihn mit Beispieltexten ohne echte Daten.
- **Kein Ersatz für den Vertrag:** Alles, was nicht gestoppt wird, geht ans Modell. Den AVV mit deinem Anbieter brauchst du trotzdem.

© 2026 REPOSPRITES · @reposprites · reposprites.com · Persönliches Exemplar, Weitergabe und Verkauf nicht gestattet · ID RS-20261103-F78F92BF

Prompt zum Kopieren

```
Bau mir einen UserPromptSubmit-Hook für Claude Code, der lokal läuft. Er soll jeden Prompt mit Presidio (deutsches spaCy-Modell, deutsche Erkenner eingeschaltet) und meiner Kundenliste kunden.txt prüfen und blockieren, sobald ein Name, eine IBAN oder eine E-Mail gefunden wird. Die Meldung soll sagen, was gefunden wurde. Trag ihn in .claude/settings.json ein und teste ihn mit drei Beispielprompts ohne echte Daten.
```

// 07

Weg 3: der eigene GPU-Server

So arbeite ich heute für einen Teil meiner Aufgaben: ein gemieteter Server mit Grafikkarte, auf dem ein offenes KI-Modell läuft. Die Daten verlassen deinen Server nicht, es gibt keine Lizenz pro Kopf, sondern eine feste Miete.

Was du brauchst

- **Einen GPU-Server**, zum Beispiel bei Hetzner. Laut Hetzner (geprüft am 03.11.2026, netto):

MODELL	GRAFIKKARTE	MIETE PRO MONAT	EINRICHTUNG EINMALIG	STANDORT
GEX45	1× NVIDIA RTX PRO 4000 Blackwell, 24 GB	214 €	209 €	Helsinki (Finnland)
GEX63	1× NVIDIA RTX PRO 6000 Blackwell Max-Q, 96 GB	999 €	999 €	Helsinki (Finnland)
GEX131	1× NVIDIA RTX PRO 6000 Blackwell Max-Q, 96 GB	ab 1.499 €	1.499 €	Falkenstein (Deutschland), Helsinki

- **Ein offenes Modell** und eine Software, die es bereitstellt, zum Beispiel Ollama oder vLLM. Je größer das Modell, desto mehr Grafikspeicher brauchst du.
- **Eine Oberfläche für dein Team**, zum Beispiel Open WebUI, damit es sich wie ein Chat im Browser anfühlt.
- **Den AVV mit dem Hoster.** Bei Hetzner schließt du ihn direkt im Kundenkonto ab, ohne Unterschrift auf Papier. Dedizierte Server stehen laut Hetzner ausschließlich in der EU.

© 2026 REPOSPRITES · @reposprites · reposprites.com · Persönliches Exemplar, Weitergabe und Verkauf nicht gestattet · ID RS-20261103-F78F92BF

Pro und Contra

PRO	CONTRA
Die Daten bleiben auf deinem Server, kein Modell-Anbieter sieht sie	Claude läuft dort nicht. Offene Modelle sind gut, aber für viele Aufgaben nicht auf Claude-Niveau
Feste Miete, egal wie viele Leute es nutzen	Ab 214 € im Monat, auch wenn niemand es nutzt
Volle Kontrolle über Modell, Speicherdauer und Zugriffe	Einrichtung, Updates, Backups und Sicherheit machst du selbst
Gut kombinierbar: sensible Aufgaben auf dem Server, der Rest bei Claude	Wenn der Server ausfällt, bist du der Support

Für wen: für Firmen mit Technik im Haus oder einem Dienstleister, viele Nutzer oder sehr sensible Daten. Für die meisten Einsteiger ist das zu viel auf einmal. Ich habe auch mit Langdock angefangen.

// 08

Welcher Weg passt zu dir?

DEINE LAGE	MEIN VORSCHLAG
Allein, ab und zu, keine Kundendaten	Erst testen, ob sich ein Platz lohnt. Sonst ein einfaches Abo direkt beim Modell-Anbieter
Kleines Team, täglich, keine Technik im Haus	Langdock: schnell startklar, AVV inklusive
Team mit Kundendaten in Texten (Angebote, Mails)	Langdock oder Claude direkt, plus die Schleife mit Presidio für genau diese Aufgaben
Viele Nutzer oder sehr sensible Daten, Technik im Haus	Eigener GPU-Server für das Sensible, Claude für den Rest
Unsicher	Klein anfangen: 7 Tage Langdock testen und parallel zehn Texte durch Presidio schicken

© 2026 REPOSPRITES · @reposprites · reposprites.com · Persönliches Exemplar, Weitergabe und Verkauf nicht gestattet · ID RS-20261103-F78F92BF

// 09

Deine DSGVO-Pflichten, egal welcher Weg

Kein Anbieter und keine Schleife nimmt dir diese Punkte ab. Sie gelten für Langdock genauso wie für die eigene Schleife.

PFLICHT	WAS DU KONKRET TUST
Rechtsgrundlage (Art. 6 DSGVO)	Klären, warum du die Daten verarbeiten darfst, etwa zur Vertragserfüllung oder aus berechtigtem Interesse. Für Gesundheitsdaten und andere besondere Daten gilt zusätzlich Art. 9.
AVV (Art. 28)	Mit jedem Anbieter, der Daten für dich verarbeitet, einen Auftragsverarbeitungsvertrag haben. Bei Langdock steckt er in den AGB, beim Modell-Anbieter der Schleife schließt du ihn selbst.
Verarbeitungsverzeichnis (Art. 30)	Das KI-Werkzeug als eigene Verarbeitung eintragen: Zweck, Datenarten, Empfänger, Löschfristen.
Information (Art. 13 und 14)	Datenschutzerklärung und Kundeninformation ergänzen: Welche KI-Dienste nutzt du, wofür, und wohin gehen die Daten.
Drittland (Art. 44 ff.)	Gehen Daten in die USA, braucht es eine Grundlage, etwa das EU-US Data Privacy Framework oder Standardvertragsklauseln. Prüfe, worauf sich der Anbieter beruft.
Sicherheit (Art. 32)	Zugänge mit Rollen und Zwei-Faktor-Anmeldung, Aufbewahrung der Chats so kurz wie möglich einstellen.
Folgenabschätzung (Art. 35)	Bei hohem Risiko vorher prüfen und dokumentieren, zum Beispiel bei Gesundheits- oder Mandantendaten in größerem Umfang.
Rechte der Betroffenen (Art. 15 bis 17)	Auskunft und Löschung müssen auch für das klappen, was im KI-Werkzeug liegt. Wisse, wo du Chats findest und löschst.
KI-Kompetenz (Art. 4 KI-Verordnung)	Seit 2. Februar 2025 Pflicht: Wer im Team mit KI arbeitet, wird geschult. Eine kurze interne Regel, was rein darf und was nicht, ist der Anfang.

Faustregel: Je weniger echte Namen und Kundendaten das Modell sieht, desto kleiner wird jede dieser Aufgaben. Genau dafür ist die Schleife da.

© 2026 REPOSPRITES · @reposprites · reposprites.com · Persönliches Exemplar, Weitergabe und Verkauf nicht gestattet · ID RS-20261103-F78F92BF

// 10

Zwei ehrliche Hinweise

- **Presidio findet nicht alles.** Prüf regelmäßig Stichproben von Hand, gerade am Anfang.
- **Für dich bleiben die Daten personenbezogen.** Du hast die Zuordnungsliste, also gilt die DSGVO weiter (Erwägungsgrund 26, EDPB-Leitlinien 01/2025). Die Schleife senkt das Risiko und hilft bei der Datenminimierung, ersetzt aber keinen AVV mit deinem Modell-Anbieter. Nur echte Anonymisierung nimmt Daten aus der DSGVO heraus.

// 11

Weitere Anbieter ohne Technik

ANBIETER	PREIS (LAUT PREISSEITE)	BESONDERHEIT
nele.ai	Credit-Modell ab 10 € netto im Monat	Server in der EU, Claude verfügbar, optionale Filterung persönlicher Daten vor der KI
meinGPT	ab 18 € pro Nutzer und Monat plus Modellbudget	Gehostet in Deutschland und der EU, ISO 27001
Mistral Le Chat Team	24,99 USD pro Nutzer und Monat	Französischer Anbieter, kein Claude

Bei allen gilt: Frag schriftlich nach Backend, Region, Speicherdauer und AVV.

// 12

Deine erste Stunde

- [ ] Entscheiden: einfach (Langdock), Kontrolle (Schleife), eigener Server, oder eine Mischung. Die Tabelle „Welcher Weg passt zu dir?“ hilft.
- [ ] Rechnen: Wie viele Leute nutzen es, wie oft? Lizenz mal Köpfe gegen die gesparte Zeit.
- [ ] Bei Langdock: Testzugang anlegen und die sieben Fragen oben schriftlich stellen.
- [ ] Bei der Schleife: Presidio installieren, deutsches Sprachmodell und die deutschen Erkenner einschalten.
- [ ] Zehn eigene Texte ohne echte Kundendaten durchschicken und prüfen, was gefunden wird.
- [ ] Erst danach mit echten Daten arbeiten, mit Stichproben.

© 2026 REPOSPRITES · @reposprites · reposprites.com · Persönliches Exemplar, Weitergabe und Verkauf nicht gestattet · ID RS-20261103-F78F92BF

// 13

Mein Tipp

Fang einfach an, so wie ich: Langdock (oder ein anderer fertiger Arbeitsplatz) für das Team im Alltag, ohne Kundendaten. Dazu eine Schleife mit Presidio für die eine Aufgabe, bei der Namen drinstecken, zum Beispiel Angebote oder Kundenmails. Wenn du merkst, dass ihr viele Köpfe seid oder Daten habt, die nie rausgehen sollen, ist der eigene Server der nächste Schritt. Rechne vorher nach, nicht hinterher.

Alle Preise, Funktionen und Links am 01.11.2026 auf den Seiten der Anbieter und in den Dokumentationen geprüft, die Sicherheitsangaben und Preise von Langdock sowie die GPU-Server und der AVV von Hetzner am 03.11.2026 auf langdock.com und hetzner.com. Preise ändern sich, schau vor dem Kauf nach.

— *@reposprites*

Du willst auch so animierte Videos machen? Dann besuch meine Webseite und hol dir die Reel-Engine.

reposprites.com ↗

© 2026 REPOSPRITES · @reposprites · reposprites.com · Persönliches Exemplar, Weitergabe und Verkauf nicht gestattet · ID RS-20261103-F78F92BF