

CHECKLISTE FÜR DEN MITTELSTAND

DSGVO-konforme LLMs 2026

DSGVO-Konformität ist kein Modell-Attribut, sondern eine Frage des Gesamt-Setups: Hosting-Region, AVV, Trainings-Opt-Out, Vertragslage und eure eigenen Prozesse. Diese Checkliste bringt euch in unter einer Stunde zu einer belastbaren Entscheidung.

1 Konform vs. nicht konform — auf einen Blick

KLAR KONFORM BETREIBBAR	NICHT OHNE WEITERES KONFORM
✓ Azure OpenAI (EU-Regionen) ✓ Anthropic Claude (API + Work, EU-Hosting) ✓ Mistral La Plateforme (Paris) ✓ AWS Bedrock (Frankfurt/Irland) ✓ Google Vertex AI (EU-Regionen) ✓ On-prem: Llama 4, Mistral, Qwen 3.5, DeepSeek V4	✗ Consumer-ChatGPT (Free/Plus) ✗ Claude.ai ohne Workspace-Tier ✗ Google Gemini (Consumer) ✗ Perplexity ohne Enterprise ✗ DeepSeek/Qwen/GLM in der China-Cloud ✗ OpenAI-API in Nicht-EU-Region ohne DPF-Setup

2 Vor dem Go-Live prüfen

- ☐ **DPF-Zertifizierung** des Anbieters auf dataprivacyframework.gov nachschlagen
- ☐ **Vertragsentität** auf der eigenen Rechnung klären — mit dieser schließt ihr den AVV
- ☐ **AVV (Art. 28 DSGVO) aktiv abschließen** — Trainings-Opt-Out, Sub-Prozessoren, Löschpflichten lesen
- ☐ **Region im API-Setup explizit setzen** (nicht Default) — z. B. Sweden Central, Frankfurt, Paris
- ☐ **Rechtsgrundlage nach Art. 6** festlegen (Einwilligung oder Betriebsvereinbarung; berechtigtes Interesse trägt selten)
- ☐ **DSFA (Art. 35)** durchführen, sobald personenbezogene Daten systematisch verarbeitet werden
- ☐ **Transparenz (Art. 13/14)** — Anbieter, Rechtsgrundlage und Drittland-Garantie in die Datenschutzerklärung
- ☐ **Logging-Verhalten** klären: welche Logs, wer hat Zugriff, Aufbewahrungsfrist
- ☐ **Modell-Lifecycle** prüfen (Deprecation, Pinning) und Vendor-Lock-in vermeiden
- ☐ **Art. 9 DSGVO** beachten — Gesundheits-, Gewerkschafts-, ethnische Daten brauchen Zusatz-Erlaubnis

3 Datenklassifizierung in drei Stufen

- ☒ **Grün (öffentlich)**

Marketingtexte, allgemeine Recherche, anonymisierte Auswertungen — geht über jeden Kanal.

● **Gelb (intern)**

Konzepte, interne Mails ohne Personenbezug, Code-Snippets — nur über Business-Tier mit AVV.

● **Rot (sensibel)**

Kunden-, Personal-, Gesundheits-, Finanz-, Steuerdaten, Geschäftsgeheimnisse — nur EU-gehostet mit AVV + DSFA oder on-prem.

4 Pragmatische Empfehlung

Standard-Start: Azure OpenAI (Sweden Central) oder Anthropic Claude mit EU-Hosting.

Souveränitäts-Profil: Mistral La Plateforme + on-prem Llama 4 Scout als Backup.

On-prem-Pflicht: Llama 4 Scout oder Mistral Medium 3.5 mit vLLM. Tier-1 ab ~15-35 T€.

Vor Personendaten: pseudonymisieren, bevor sie ans LLM gehen.

5 Was ihr heute nicht tun solltet

- Keine Consumer-LLMs mit personenbezogenen Geschäftsdaten füttern.
- Keine chinesischen Cloud-APIs (DeepSeek-/Qwen-Cloud) für deutsche Mittelstandsdaten — selbst hosten ist ok.
- Keine „wir warten ab“-Strategie — wer 2026 startet, hat 2-3 Jahre Vorsprung.

Unsicher, ob euer aktueller Setup hält?

Ein kostenloses 30-Minuten-Erstgespräch klärt meistens, ob euer AI-Stack DSGVO-fest ist oder wo nachzuarbeiten ist. Termin buchen auf krynexlabs.de/kontakt