

KI-Anbieter nach technischer Datensouveränität

MAKETTO

Geordnet nach Kontrollierbarkeit von Infrastruktur und Datenwegen – keine rechtliche DSGVO-Zertifizierung (keine Gewähr, Irrtümer vorbehalten, keine Rechtsberatung), Stand August 2026

Rang-gruppe	Anbieter / Lösung	Betriebsmodell	Verarbeitung der KI	Externe Modellanbieter	Kontrolle über Datenwege	Eignung für sehr sensible Daten*	Wichtige Einschränkung	Quelle
1	GiKS Suite – Offline-KI	Lokal / On-Premises; ohne notwendige Cloudverbindung	In eigener oder kontrollierter Infrastruktur	Im vorgesehenen Offline-Betrieb nicht erforderlich	Sehr hoch	Sehr hoch – bei geeigneter Konzeption	Kein automatischer Zugriff auf zahlreiche wechselnde Spitzenmodelle; Einführung und Betrieb müssen geplant werden	https://integrierte-ki-systeme.de/
1	basebox On-Premises	Installation im eigenen Netzwerk	Auf eigener oder dedizierter Infrastruktur	Nicht zwingend; eigene Modelle möglich	Sehr hoch	Sehr hoch – laut Anbieter für regulierte Bereiche konzipiert	Hardware, Administration und konkrete Konfiguration bleiben entscheidend	https://basebox.ai/
2	Langdock Enterprise – individuelles Hosting	Hosting in Kundeninfrastruktur möglich	Abhängig von vereinbarter Infrastruktur und Modellauswahl	Konfigurierbar	Hoch bis sehr hoch	Hoch	Individuelles Deployment laut Anbieter vor allem für große Organisationen	https://langdock.com/enterprise
2	basebox EU-Cloud	Kontrollierte EU-Cloud	Laut Anbieter auf dedizierten Servern, nicht auf öffentlichen KI-Plattformen	Eingeschränkt bzw. kontrolliert	Hoch	Hoch – genaue Architektur prüfen	Cloudbetrieb bleibt externe Verarbeitung; Vertrags- und Subprozessorenprüfung erforderlich	https://basebox.ai/
3	meinGPT – EU Only	Deutsche Plattform; Hetzner-Hosting; Datenschutzlevel wählbar	Bei EU Only über ausgewählte EU-Unternehmen und EU-Server	Teilweise; abhängig vom freigegebenen Datenschutzlevel	Hoch – bei verbindlicher EU-Only-Konfiguration	Bedingt bis hoch	Das Sicherheitsniveau ändert sich mit Modell- und Datenschutzlevel	https://meingpt.com/docs/privacy-security/provider-selection
3	Langdock – EU-konfiguriert	Cloudplattform mit EU-Hosting	Viele Modelle laut Anbieter vollständig in der EU konfigurierbar	Ja; abhängig vom Modell	Mittel bis hoch	Bedingt	Die konkrete Modellroute muss je Workspace und Modell geprüft werden	https://langdock.com/security
3	innoGPT	Deutsche Plattform; Datenhaltung in Frankfurt	Zahlreiche Modelle laut Anbieter EU-gehostet	Ja; u. a. OpenAI, Anthropic und Google	Mittel bis hoch	Bedingt	EU-Hosting ist je Modell zu verifizieren; US-Infrastrukturanbieter können beteiligt sein	https://www.innogpt.de/datenschutz-sicherheit
3	nele.ai	Deutsche Plattform; Speicherung in Deutschland / EU	OpenAI, Azure, Anthropic oder dedizierte offene Modelle	Ja; dedizierte Umgebung teilweise möglich	Mittel bis hoch	Bedingt	Pseudonymisierung erkennt nicht zwingend alle personenbezogenen Informationen	https://www.nele.ai/de
4	DeutschlandGPT	Deutsche Plattform mit deutschem Hosting	Über unterschiedliche führende Modelle	Ja	Mittel	Einzelfallprüfung erforderlich	Öffentliche Angaben differenzieren die Datenwege nicht für jedes Modell gleich detailliert	https://www.deutschlandgpt.de/
4	Dust	Europäische Cloudplattform; EU-Datenresidenz wählbar	Plattformdaten in der EU; externe Modelle mit Zero-Retention-Vereinbarungen	Ja	Mittel	Eher bedingt	Zero Retention bedeutet nicht, dass keine externe Verarbeitung stattfindet	https://dust.tt/home/security
4	LLMBase	Anwendung und API-Grenze in Europa	Abhängig vom ausgewählten Modell und verfügbarer Infrastruktur	Ja; europäische und außereuropäische Anbieter	Mittel bis begrenzt	Nur mit eindeutig ausgewiesener Modellroute	LLMBase weist selbst darauf hin, dass nicht jedes Modell in der EU verarbeitet wird	https://llmbase.ai/de/
4	Corporate LLM	EU-gehostete Multi-LLM-Plattform	Abhängig von Modell bzw. Bring-your-own-Model	Ja	Öffentlich noch nicht ausreichend nachvollziehbar	Vor Einsatz detailliert prüfen	Hosting-, Modell- und Subprozessorenwege im konkreten Angebot abfragen	https://corporatellm.de/
4	LLMrouter.eu	Europäische Modellrouting- und API-Plattform	Routing zu unterschiedlichen Modellen	Ja	Abhängig von Routingregeln und Protokollierung	Einzelfallprüfung erforderlich	Eher technischer API-Baustein als fertig kontrollierter Mitarbeiter-Chat	https://llmrouter.eu/en

* Keine Freigabe für sensible Daten. Die tatsächliche Eignung hängt zusätzlich von Rechtsgrundlage, Zweck, Berechtigungen, Löschkonzept, technischer Umsetzung und gegebenenfalls einer Datenschutz-Folgenabschätzung ab.

Ranggruppe	Bedeutung	Typisches Merkmal	Farbcode
1	Maximale technische Kontrolle	Verarbeitung kann vollständig in selbst kontrollierter Infrastruktur stattfinden	Grün
2	Dedizierte, stark kontrollierbare Umgebung	Infrastruktur und Modelle können weitgehend abgegrenzt werden	Blau
3	Kontrollierte EU-Cloud	Gute Governance; Datenweg bleibt von Modell und Konfiguration abhängig	Gelb
4	Multi-LLM-Cloud / Informationslage begrenzt	Variierende Modellwege oder noch nicht ausreichend detaillierte öffentliche Angaben	Grau

Die Reihenfolge bewertet nicht pauschal die DSGVO-Konformität eines Anbieters. Sie beschreibt die Nähe zu technischer Datensouveränität anhand öffentlich zugänglicher Anbieterinformationen. Derselbe Anbieter kann je nach Tarif, Modell, Hostingregion und Konfiguration auf unterschiedlichen Stufen liegen. Stand: August 2026. Anbieterangaben können sich ändern.

Prüffrage	Warum wichtig?	Beispiel	Nachweis
Wo läuft die Benutzeroberfläche?	Zeigt den Plattformstandort	Deutschland / EU	Vertrag, Datenschutzerklärung
Wo werden Chats und Dokumente gespeichert?	Betrifft Datenhaltung und Löschung	Deutsches Rechenzentrum	AVV, TOM, Löschkonzept
Wo verarbeitet das Modell die Eingabe?	Entscheidender tatsächlicher Datenweg	EU-Endpunkt / lokales Modell	Modellliste, Subprozessoren
Werden Eingaben protokolliert?	Kein Training ist nicht gleich keine Speicherung	Zero Retention	Vertragliche Zusicherung
Kann die Modellwahl zentral begrenzt werden?	Verhindert unkontrollierte Datenwege	EU-Only-Modus	<<<<