7 Fragen, **die zeigen, ob ein KI-Anbieter DSGVO-konform ist.**

Ein 5-Minuten-Test für Geschäftsführer – bevor Sie unterschreiben.

HERAUSGEBER
Nexoria
KI-Betriebssystem für den europäischen Mittelstand

ZUM BLOGBEITRAG
nexoria-systems.de/blog/ki-anbieter-datenschutz-transparenz

EINFÜHRUNG

Warum diese Checkliste existiert.

„DSGVO-konform" ist zum meistmissbrauchten Label der deutschen KI-Branche geworden. Jeder Anbieter schreibt es drauf. Die wenigsten können es belegen.

Wer heute einen KI-Anbieter prüft, kämpft sich durch 15-seitige Datenschutzerklärungen voller juristischer Formulierungen, die alles sagen und nichts bedeuten. „Externe KI-Dienstleister" ohne Namen. „Drittlandtransfers können nicht ausgeschlossen werden" – versteckt auf Seite 12. Und auf der Startseite prominent: DSGVO-konform.

Diese Checkliste ändert das. Sieben Fragen. Fünf Minuten. Wer auf mehr als zwei davon keine klare Antwort geben kann, hat entweder ein Transparenzproblem oder ein Architekturproblem. Beides disqualifiziert in regulierten Branchen.

SO NUTZEN SIE DIESE CHECKLISTE

Drucken. Mitnehmen. Fragen stellen.

Jede Frage adressiert einen spezifischen Angriffsvektor für DSGVO-Verletzungen in KI-Architekturen. Ein seriöser Anbieter beantwortet alle sieben Fragen in wenigen Minuten – konkret, ohne Ausweichformeln.

SCORING

Was die Antworten bedeuten.

7 / 7 klare Antworten
Anbieter ist transparent und strukturell DSGVO-konform.

5 – 6 / 7
Grundsätzlich prüfenswert, aber Einzelaspekte klären.

Unter 5 / 7
Nicht enterprise-ready. Weitersuchen.

DIE CHECKLISTE

Fragen 1 – 3.

01 Welches Sprachmodell (LLM) nutzen Sie konkret?

Ein seriöser Anbieter nennt ein spezifisches Modell und den dahinterliegenden Anbieter. Ohne konkrete Nennung ist keine Bewertung der Jurisdiktion, Datenverarbeitung oder Trainingspolitik möglich.

ERWARTETE ANTWORT

Konkreter Modellname plus Anbieter – z. B. „Mistral Large 2 von Mistral AI, Paris" oder „GPT-4o von OpenAI, San Francisco".

WARNSIGNALE

„Proprietär". „Aus wettbewerblichen Gründen vertraulich". „Externer KI-Dienstleister".

02 In welcher Jurisdiktion sitzt der LLM-Anbieter?

US-Anbieter unterliegen dem CLOUD Act (18 U.S.C. § 2713). US-Behörden können die Herausgabe Ihrer Daten anordnen – unabhängig vom Serverstandort, oft ohne Ihr Wissen (Gag Orders).

ERWARTETE ANTWORT

Land und Rechtsraum des Anbieter-Unternehmens, nicht nur des Servers.

WARNSIGNALE

„Der Serverstandort ist in der EU" – das ist nicht dasselbe wie ein EU-Unternehmen.

03 Werden unsere Daten für KI-Training verwendet?

Diese Frage muss sowohl für den direkten Anbieter als auch für jeden Sub-Processor (insb. den LLM-Anbieter) beantwortet werden. Die Trainingsrichtlinien großer LLM-Anbieter wurden mehrfach nachträglich angepasst.

ERWARTETE ANTWORT

Klare Nein-Aussage über die gesamte Verarbeitungskette, vertraglich abgesichert.

WARNSIGNALE

„Nicht von uns" – ohne Aussage zum LLM-Sub-Processor.

DIE CHECKLISTE

Fragen 4 – 6.

04 Verlassen unsere Daten zu irgendeinem Zeitpunkt den EU-Rechtsraum?

EU-Hosting bedeutet nicht automatisch EU-Verarbeitung. Wenn der API-Call an ein US-Unternehmen geht, verlassen die Daten den EU-Rechtsraum – auch wenn die physischen Server in Frankfurt stehen.

ERWARTETE ANTWORT

Ein klares Nein, mit Benennung der vollständigen Verarbeitungskette.

WARNSIGNALE

„In der Regel nicht". „Grundsätzlich nicht". „Je nach Konfiguration".

05 Existiert ein AVV nach Art. 28 DSGVO mit dem LLM-Anbieter?

Art. 28 DSGVO verlangt einen Auftragsverarbeitungsvertrag mit jedem Sub-Processor – nicht nur mit dem Chatbot-Anbieter, der Ihre Rechnung schreibt, sondern mit jedem Unternehmen in der Kette.

ERWARTETE ANTWORT

AVV als PDF zum direkten Download, ohne Zwischenschritte.

WARNSIGNALE

„Wir kontaktieren Sie dazu gerne" statt direktem Zugriff.

06 Ist die Sub-Processor-Liste öffentlich einsehbar?

Seriöse Anbieter führen eine öffentliche Liste aller Sub-Processor – mit Sitz, Zweck und Art der Datenverarbeitung. Ohne Login, ohne NDA, ohne Formular. Das ist seit Jahren Industriestandard in Enterprise-SaaS.

ERWARTETE ANTWORT

Direkter URL-Link auf eine öffentlich zugängliche Seite mit tabellarischer Übersicht.

WARNSIGNALE

„Verfügbar auf Anfrage". „Unter NDA". „Für Bestandskunden".

DIE CHECKLISTE

Die entscheidende Frage.

07 Können Sie in einem Satz sagen, wo die Daten landen?

Der Stresstest. Ein Anbieter mit klarer Architektur beantwortet diese Frage in 30 Sekunden. Wer es nicht in einem Satz kann, hat keine saubere Architektur – oder versteckt sie bewusst.

ERWARTETE ANTWORT

Ein konkreter Satz mit Unternehmensnamen, Standorten und dem Wort „Ende".

WARNSIGNALE

Antwort dauert länger als 30 Sekunden oder enthält „grundsätzlich", „in der Regel", „je nach".

FAZIT

Die sieben Fragen sind der Filter.

Wer sie alle klar beantwortet, hat seine Architektur im Griff und respektiert die DSGVO nicht nur als Label, sondern als Grundlage. Wer mehr als zwei Fragen ausweicht, ist im regulierten B2B-Umfeld kein ernsthafter Partner – unabhängig davon, wie beeindruckend die Produktdemo wirkt.

AUF DER NÄCHSTEN SEITE

Nexoria beantwortet alle sieben Fragen.

Nicht weil wir es müssen – sondern weil wir finden, dass es Industriestandard sein sollte. Die vollständige Analyse der Branche mit allen Mustern und Quellen finden Sie im Blogbeitrag.

DER BENCHMARK

So beantwortet Nexoria diese sieben Fragen.

Wenn wir die Branche an sieben Fragen messen, müssen wir uns selbst an denselben Fragen messen lassen. Das ist der ganze Punkt.

01	Welches LLM?	**Mistral Large von Mistral AI (Paris, Frankreich)**
02	Sitz des LLM-Anbieters?	**Frankreich – keine US-Jurisdiktion, kein CLOUD Act**
03	Daten für KI-Training?	**Nein. Weder bei Nexoria noch bei Mistral.**
04	Daten verlassen die EU?	**Nein. Vollständige EU-Verarbeitungskette.**
05	AVV mit LLM-Anbieter?	**Ja. Öffentlich zum Download.**
06	Sub-Processor-Liste öffentlich?	**Ja. Ohne Login, ohne Formular.**
07	Wo landen die Daten?	**Deutsche Server, europäische Dienstleister. Ende.**

ZUM BLOGBEITRAG

Die ausführliche Analyse mit allen fünf Mustern aus der Branche – inklusive Quellenangaben zu Art. 13, 28 und 30 DSGVO:

nexoria-systems.de/blog/ki-anbieter-datenschutz-transparenz

ANHANG

Rechtliche Grundlagen & Hinweise.

RECHTLICHE GRUNDLAGEN

Art. 13 DSGVO	Informationspflichten bei Erhebung personenbezogener Daten
Art. 28 DSGVO	Auftragsverarbeitung – Pflichten und Verträge
Art. 30 DSGVO	Verzeichnis von Verarbeitungstätigkeiten
Art. 25 DSGVO	Datenschutz durch Technikgestaltung und Voreinstellungen
CLOUD Act	18 U.S.C. § 2713 – extraterritoriale Datenherausgabe durch US-Anbieter
EuGH C-311/18	„Schrems II" – Ungültigkeit des EU-US Privacy Shield
FISA Section 702	US-Überwachungsbefugnis mit weitreichendem Datenzugriff

HINWEIS

Diese Checkliste wurde von Nexoria erstellt und darf frei geteilt, weitergegeben und in Beschaffungs- sowie Evaluationsprozessen verwendet werden. Sie dient der praxisnahen Bewertung von KI-Anbietern und ersetzt keine individuelle rechtliche Beratung.

Bei konkreten Fragen zur DSGVO-Konformität im Kontext einer Beschaffung wenden Sie sich an Ihren Datenschutzbeauftragten oder einen auf IT- und Datenschutzrecht spezialisierten Rechtsanwalt. Die in dieser Checkliste genannten rechtlichen Grundlagen stellen keine abschließende juristische Würdigung dar.

HERAUSGEBER
Nexoria
Bonn, Deutschland

EDITION
2026 · Version 1.0

ZUM BLOGBEITRAG
nexoria-systems.de/blog/ki-anbieter-datenschutz-transparenz