KI Datenschutz & DSGVO: ChatGPT & Co. rechtssicher nutzen

Sobald ein KI-Tool im Unternehmen läuft und dabei personenbezogene Daten verarbeitet, greift der Datenschutz. Das gilt für ChatGPT bei Kundenanfragen genauso wie für Claude bei Analysen oder Gemini in der Office-Umgebung. Und die erste Frage, die uns Mittelständler:innen am häufigsten stellen, lautet nicht „Welches Modell ist das beste?", sondern „Darf ich das überhaupt nutzen?".

Die Antwort lautet ja. ChatGPT, Claude und Gemini lassen sich datenschutzkonform einsetzen, aber keines davon ist es automatisch. Es kommt darauf an, welchen Tarif du nutzt, wie der Datentransfer abgesichert ist und ob du ein paar organisatorische Hausaufgaben erledigt hast. Genau die gehen wir hier durch.

Ist ChatGPT, Claude oder Gemini DSGVO-konform?

Die ehrliche Antwort gilt für alle gängigen KI-Tools gleichermaßen, ob ChatGPT, Claude, Gemini oder Microsoft Copilot. Keines dieser Tools ist automatisch DSGVO-konform, mit dem richtigen Setup aber sehr wohl einsetzbar. Entscheidend ist oft nicht das KI-Modell, sondern die konkreten Bereiche, in denen es eingesetzt werden soll. Welche KI-Tools aktuell auf dem Markt sind und wo die Anbieter jeweils führen, zeigt unser Marktüberblick zu KI-Tools 2026.

Gratis- und Privatversionen: für Unternehmen ungeeignet

Über alle großen Tools hinweg verläuft dieselbe Trennlinie. Die kostenlosen und privaten Versionen (ChatGPT Free, Claude Free und Pro, die Gemini-Apps) sind für die Verarbeitung personenbezogener Daten im Unternehmen nicht geeignet, denn sie verarbeiten Eingaben auf Servern außerhalb der EU und nutzen sie in der Regel als Trainingsdaten zur Verbesserung der Modelle. Für Kund:innen- oder Mitarbeitendendaten ist das keine tragfähige Grundlage.

Business- und Enterprise-Versionen: mit AVV nutzbar

Geschäftstauglich werden sie in den Business- und Enterprise-Versionen: ChatGPT Enterprise und Team, Claude for Work oder die API, Gemini in Google Workspace, Microsoft Copilot über Microsoft 365. Dort ist ein Auftragsverarbeitungsvertrag (AVV, auch AV-Vertrag genannt) Bestandteil der Bedingungen, die Eingaben fließen nicht in die Trainingsdaten der Anbieter, und der Drittlandtransfer in die USA ist über das EU-U.S. Data Privacy Framework oder Standardvertragsklauseln abgesichert.

Serverstandort und sensible Daten

Ein Unterschied bleibt beim Serverstandort. Wer eine garantierte Datenverarbeitung in der EU braucht, erreicht das je nach Tool über unterschiedliche Wege: bei ChatGPT über die EU-Datenresidenz der Enterprise-Version oder Azure OpenAI, bei Claude über einen Cloud-Anbieter wie AWS Bedrock oder Google Vertex AI in einer EU-Region, bei Gemini über Google Workspace beziehungsweise Vertex AI mit EU-Endpunkten, bei Microsoft Copilot über die EU-Datengrenze von Microsoft 365. Welcher Pfad der richtige ist, hängt von deiner bestehenden Infrastruktur und deinen KI-Anwendungen ab.

Unabhängig vom Tool gehören auch in der Business-Variante besonders sensible Daten, etwa Gesundheits- oder Finanzinformationen, grundsätzlich nicht in ein Cloud-KI-Tool. Vor dem Einsatz braucht es zudem eine Datenschutz-Folgenabschätzung.

Europäische Alternativen

Wer von vornherein auf EU-Datenverarbeitung setzen will, findet zudem in europäischen Anbietern wie Mistral AI (Frankreich) oder Aleph Alpha (Deutschland) leistungsfähige Alternativen mit Datenhaltung in der EU. Der Preis dafür sind kleinere Ökosysteme. Welche europäischen Anbieter und Modelle sich im Detail lohnen, zeigt unsere Übersicht zu europäischer KI.

Welche KI ist DSGVO-konform?

Von Haus aus ist keines dieser Tools DSGVO-konform. Datenschutzkonform einsetzen lassen sie sich aber alle, wenn vier Bedingungen erfüllt sind. Wir empfehlen, jedes Tool vor dem Einsatz an dieser Checkliste zu messen:

- Geschäftstarif statt Gratis- oder Privatversion (Enterprise, Team oder API)
- Abgeschlossener Auftragsverarbeitungsvertrag (AVV bzw. AV-Vertrag) nach Art. 28 DSGVO, inklusive klarer technischer und organisatorischer Maßnahmen
- Abgesicherter Drittlandtransfer (Data Privacy Framework oder Standardvertragsklauseln), idealerweise EU-Hosting über Azure, AWS Bedrock oder Vertex AI
- Training mit den eigenen Daten vertraglich ausgeschlossen und eine Datenschutz-Folgenabschätzung durchgeführt

Sind diese Voraussetzungen erfüllt, sind ChatGPT, Claude, Gemini und Copilot gleichermaßen rechtssicher nutzbar. Die DSGVO-Konformität liegt weniger im Modell als im Setup.

DSGVO und KI: Was Unternehmen beachten müssen

Die Datenschutz-Grundverordnung kennt keine Ausnahme für künstliche Intelligenz. Sobald ein KI-Tool personenbezogene Daten verarbeitet, also Namen, E-Mail-Adressen, IP-Adressen, Bewerbungsunterlagen oder Kund:innendaten, gelten ihre Kernanforderungen in vollem Umfang. Diese Verarbeitung personenbezogener Daten passiert schneller, als viele denken. Schon ein KI-Chatbot, der eine Kundenanfrage mit Klarnamen beantwortet, fällt darunter.

Für jede Verarbeitung braucht es eine Rechtsgrundlage, etwa Einwilligung, Vertragserfüllung oder ein berechtigtes Interesse. Dazu kommen der Grundsatz der Datenminimierung, Transparenz gegenüber den betroffenen Personen sowie deren Auskunfts-, Lösch- und Widerspruchsrechte. Gerade bei KI ist hier besondere Sorgfalt gefragt, weil diese Systeme große Datenmengen verarbeiten und ihre Verarbeitungslogik oft schwer nachvollziehbar ist. Die deutschen Datenschutzaufsichtsbehörden haben in ihren Orientierungshilfen betont, dass beim Einsatz von KI in der Regel von einem erhöhten Risiko auszugehen ist.

Wichtig zur Einordnung: Datenschutz und DSGVO sind nicht dasselbe wie der EU AI Act. Die DSGVO regelt den Umgang mit personenbezogenen Daten. Der AI Act regelt KI-Systeme als Technologie, unabhängig davon, ob personenbezogene Daten im Spiel sind. Beide Regelwerke gelten parallel, und genau diese Trennung sorgt in der Praxis oft für Verwirrung.

Wo der EU AI Act ins Spiel kommt

Der EU AI Act ist seit August 2024 in Kraft. Diese KI-Verordnung (kurz KI-VO) ergänzt die DSGVO um eine zweite Ebene. Ihr Fokus liegt nicht auf dem Datenschutz, sondern auf der Sicherheit und Vertrauenswürdigkeit von KI-Systemen. Sie folgt einem risikobasierten Ansatz mit vier Stufen: verbotene Praktiken, Hochrisiko-KI-Systeme, KI-Modelle mit allgemeinem Verwendungszweck (GPAI, etwa ChatGPT, Claude oder Gemini) sowie Anwendungen mit geringem Risiko, für die im Wesentlichen Transparenzpflichten gelten.

Was für Anwender:innen zählt

Für die meisten Mittelständler:innen, die KI als Anwendende nutzen, sind drei Punkte des KI-Rechts relevant. Die Verbote (Art. 5) gelten seit Februar 2025, die GPAI-Transparenzpflichten seit August 2025, und die KI-Verordnung misst der KI-Kompetenz der Mitarbeiter:innen ausdrücklich Bedeutung bei (Art. 4), worauf gerade Führungskräfte früh hinwirken sollten. Für die Compliance gehören Schulung und Dokumentation damit von Anfang an dazu.

Was sich 2026 beim Zeitplan ändert

Beim Zeitplan hat sich 2026 etwas Wesentliches verändert. Über den sogenannten Digital Omnibus werden die strengen Pflichten für eigenständige Hochrisiko-KI-Systeme nach

hinten verschoben, von August 2026 auf den 2. Dezember 2027, für in Produkte eingebettete Systeme auf den 2. August 2028.

Dieser Schritt ist inzwischen beschlossen. Das Europäische Parlament stimmte am 16. Juni 2026 zu, der Rat der EU gab am 29. Juni 2026 sein finales grünes Licht; die Veröffentlichung im EU-Amtsblatt folgt. Verschoben werden allein die Durchsetzungsdaten, nicht die inhaltlichen Anforderungen, und die Verbote (seit Februar 2025) sowie die GPAI- und Transparenzpflichten bleiben unberührt. Aktuelle Übersichten und Leitfäden zum Umsetzungsstand veröffentlicht die EU laufend.

Für die Praxis bedeutet das Entwarnung. Die meisten Anwenderunternehmen betreiben gar keine Hochrisiko-KI und waren von der August-Frist ohnehin kaum betroffen. Die eigentliche Aufgabe bleibt, die eigenen KI-Systeme einer Risikoklasse zuzuordnen. Erst daraus ergibt sich, welche Pflichten greifen.

In wenigen Schritten zur rechtssicheren KI-Nutzung

Damit aus der Theorie ein belastbarer Prozess wird, hat sich aus unserer Erfahrung diese Reihenfolge bewährt:

1. **Bestandsaufnahme.** Erstelle ein KI-Register: Welche Tools sind im Einsatz, zu welchem Zweck, mit welchen Daten, in welchen Abteilungen, mit welchem Speicherort?
2. **Risikobewertung.** Ordne jedes System einer AI-Act-Risikoklasse zu. Die meisten Tools fallen in die niedrigen Stufen. Beim Einsatz von KI im HR, etwa in der Bewerbungsauswahl, oder bei Kreditentscheidungen kann es aber Hochrisiko sein.
3. **Interne KI-Richtlinie.** Lege fest, welche Tools erlaubt sind, welche Daten nicht eingegeben werden dürfen, wie Ergebnisse geprüft werden und wer, etwa als Datenschutzbeauftragte:r, verantwortlich ist. Mitarbeiter:innen sollten nur Unternehmens-Accounts mit deaktivierter Verlaufsspeicherung nutzen.
4. **Datenschutz-Folgenabschätzung (DSFA).** Bei KI-Systemen ist nach Art. 35 DSGVO meist eine DSFA erforderlich. Sie dokumentiert die Risiken für die betroffenen Personen, die Schutzmaßnahmen und die Verhältnismäßigkeit der Verarbeitung und hilft, Probleme früh zu erkennen.
5. **Auftragsverarbeitungsvertrag.** Schließe mit jedem externen Anbieter einen AVV ab. Achte auf Weisungsbindung, Subunternehmer und klare technische und organisatorische Maßnahmen. Prüfe außerdem, dass eine Nutzung der Daten als Trainingsdaten ausgeschlossen ist.
6. **Mitarbeitende schulen.** Die Teams sind der Schlüssel. Sie müssen wissen, welche Daten in KI-Tools dürfen, wie man Halluzinationen erkennt und wie man bei Datenpannen reagiert.
7. **Kontinuierliches Monitoring.** Das KI-Recht entwickelt sich schnell. Prüfe mindestens jährlich, ob deine KI-Systeme noch den Anforderungen entsprechen, und dokumentiere Änderungen.

Besonderheiten für den Mittelstand

Neben den allgemeinen Anforderungen gibt es Punkte, die speziell mittelständische Unternehmen betreffen. Werden KI-Tools zur Überwachung oder Leistungsbewertung von Mitarbeitenden geeignet eingesetzt, hat der Betriebsrat ein Mitbestimmungsrecht. Das betrifft auch Produktivitäts-Tools, die Arbeitsabläufe analysieren. Eine Betriebsvereinbarung schafft hier früh Klarheit.

Hinzu kommt der Ressourcenmangel. Viele Mittelständler:innen haben weder eigene Datenschutzbeauftragte noch IT-Sicherheitsexpert:innen. Die rechtlichen Pflichten und Compliance-Anforderungen gelten trotzdem. Hier helfen externe Datenschutzberatung, eine spezialisierte Anwaltskanzlei oder KI-Compliance-Dienstleister, die diese Herausforderungen routiniert begleiten.

Wie andere Unternehmen genau diese Hürden in der Praxis gelöst haben, von der rechtssicheren Einführung bis zum Alltag mit KI, lässt sich am besten im direkten Austausch lernen. Auf der Mittelstands-Stage der d:u27 am 13. und 14. April 2027 in Münster steht genau dieser Transfer im Mittelpunkt.

Fazit: Rechtssicher mit KI ist machbar

Die rechtlichen Anforderungen an KI-Tools sind komplex, aber keineswegs unüberwindbar. Entscheidend ist ein strukturiertes Vorgehen, das sowohl die Datenschutz-Grundverordnung (DSGVO) als auch den AI Act berücksichtigt, da beide Regelwerke parallel gelten und beachtet werden müssen. Eine frühzeitige und sorgfältige Planung hilft, teure Nachbesserungen und Bußgelder zu vermeiden. Dabei ist kein tiefgehendes juristisches Fachwissen erforderlich, wohl aber ein solides Grundverständnis sowie klare Prozesse und Verantwortlichkeiten im Unternehmen.

KI bietet gerade für den Mittelstand enorme Chancen, etwa durch Effizienzsteigerungen, Kostenreduktionen und bessere Entscheidungsgrundlagen. Um diese Potenziale sicher und rechtlich konform zu nutzen, ist die Investition in KI-Kompetenz und kontinuierliche Weiterbildung unerlässlich. So kann dein Unternehmen die Vorteile der Technologie voll ausschöpfen und gleichzeitig die Einhaltung der gesetzlichen Vorgaben gewährleisten.

Wer KI im Unternehmen rechtssicher einsetzen will, ohne teure Compliance-Nachbesserungen, findet die passenden Antworten auf der d:u27 am 13. und 14. April 2027 in Münster. Auf sechs Stages, mit über 80 Masterclasses und mehr als 350 Speaker:innen kommen rund 17.000 Teilnehmende zusammen. Es geht dort auch um DSGVO und EU AI Act, KI-Governance und rechtssichere KI-Implementierung im direkten Austausch mit Compliance-Verantwortlichen, IT-Leads und Geschäftsführunge Natürlich stehen neben den rechtlichen Rahmenbedingungen konkrete KI-Anwendungen im Fokus, d.h. KI-Use Cases aus den unterschiedlichsten Branchen, sowie die neuesten KI Tools und Hacks. Jetzt Tickets für die d:u27 sichern!