

COMPLIANCE

DSGVO & ChatGPT im Unternehmen: Was gilt 2026?

ChatGPT DSGVO-konform nutzen: Consumer vs. Enterprise, AVV mit OpenAI, Verarbeitungsverzeichnis-Muster und KI-Tool-Vergleich für DACH-KMU.

AUTOR

Strukturaflow-Team

VERÖFFENTLICHT

30. April 2026

ONLINE LESEN

<https://wissen.strukturaflow.it.com/dsgvo-chatgpt-unternehmen/>

Ihre Mitarbeiter nutzen ChatGPT bereits — mit oder ohne interne Freigabe. Das zeigen Erfahrungen aus dem KMU-Alltag immer wieder. Die relevante Frage ist deshalb nicht mehr, ob ChatGPT im Unternehmen eingesetzt wird, sondern wie das rechtssicher gestaltet werden kann.

Dabei ist „ChatGPT“ nicht gleich „ChatGPT“: Die kostenlose Consumer-Version auf chatgpt.com hat grundlegend andere DSGVO-Implikationen als die API oder die Enterprise-Variante. Genau diese Unterscheidung bestimmt Ihr tatsächliches Risiko — und wird in den meisten Ratgebern nicht klar genug gemacht.

Dieser Artikel ist kein Vollgutachten, sondern ein praxistauglicher Fahrplan für KMU ohne eigene Rechtsabteilung. Stand: Juni 2025. Die Rechtslage entwickelt sich weiter — prüfen Sie im Zweifel aktuelle Aufsichtsbehörden-Entscheidungen oder holen Sie eine individuelle Einschätzung ein.

Die entscheidende Grundfrage: Welche ChatGPT-Version nutzen Sie?

Der Ausgangspunkt jeder DSGVO-Analyse ist die konkret eingesetzte Produktvariante. Es gibt drei relevante Szenarien für Unternehmen:

Szenario 1 — ChatGPT Free/Plus (chatgpt.com): Das ist das Consumer-Produkt. Kein Auftragsverarbeitungsvertrag (AVV) verfügbar, Daten können standardmäßig für das Training verwendet werden, kein dedizierter EU-Serverstandort. Für den produktiven Unternehmenseinsatz mit personenbezogenen Daten in der Regel nicht DSGVO-konform nutzbar.

Szenario 2 — ChatGPT Team/Enterprise: Hier stellt OpenAI einen AVV bereit. Training auf Kundendaten ist vertraglich ausgeschlossen. Für viele KMU der praktikabelste Einstieg in eine rechtskonformere Nutzung.

Szenario 3 — OpenAI API (direkte Einbindung): Voller Zugriff auf ein Data Processing Agreement, technische Kontrolle über Datenflüsse, kein Training auf übermittelte Daten. Erfordert technisches Setup, bietet aber die meisten Konfigurationsmöglichkeiten.

Versionsvergleich auf einen Blick

KRITERIUM	CHATGPT FREE/PLUS	CHATGPT TEAM/ENTERPRISE	OPENAI API
AVV verfügbar	☐ Nein	☐ Ja	☐ Ja
Training auf Kundendaten	☒ Standardmäßig ja	☐ Nein	☐ Nein
EU-Serverstandort	☐ Nicht garantiert	☒ Teilweise	☒ Teilweise
<u>Drittlandtransfer</u> -Absicherung	☐ Keine SCCs	☐ SCCs verfügbar	☐ SCCs verfügbar
Empfehlung für KMU mit Personenbezug	☐ Nicht geeignet	☐ Bedingt geeignet	☐ Bedingt geeignet

Die Consumer-Version scheidet für jeden Einsatz mit personenbezogenen Daten aus. Wer sie dennoch im Büro nutzt, sollte dringend klare interne Regeln einführen — dazu später mehr.

Vergleichstabelle der drei ChatGPT-Versionen (Free/Plus, Team/Enterprise, API) mit Fokus auf AVV-Verfügbarkeit, Trainingsschutz, Drittlandtransfer und DSGVO-Eignung für KMU.

Wann werden überhaupt personenbezogene Daten verarbeitet?

Personenbezogene Daten im Sinne der DSGVO sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Im KMU-Alltag betrifft das mehr Situationen, als man zunächst annimmt.

Problematische Beispiele aus der Praxis: – Kundenkommunikation in den Prompt kopieren („Schreib eine Antwort auf diese E-Mail von Herrn Müller...“) – Bewerbungsunterlagen zusammenfassen lassen (Name, Wohnort, Lebenslauf) – Patientendaten in einer Arztpraxis eingeben, auch wenn es „nur um den Befund geht“ – Vertragspartner-Namen und Konditionen in Entwürfen nennen – Mitarbeiter-Leistungsbeurteilungen formulieren lassen

Was in der Regel unbedenklich ist: – Allgemeine Texthilfe ohne Echtdaten („Formuliere diesen Absatz professioneller“) – Code-Review ohne personenbezogene Variablen – Brainstorming mit fiktiven Beispielen – Übersetzungen von Allgemeintexten

Praxis-Tipp — Anonymisierungs-Hygiene als Sofortmaßnahme: Bevor etwas in ChatGPT eingegeben wird, Namen, Adressen, Steuernummern und andere direkte Identifikatoren durch Platzhalter ersetzen. „Kunde A“ statt „GmbH Huber KG, Graz“. Das ist keine DSGVO-Lösung, reduziert aber das Risiko erheblich und lässt sich ohne technischen Aufwand sofort einführen.

Der Drittlandtransfer – und was die EU-Niederlassung von OpenAI wirklich ändert

OpenAI ist ein US-amerikanisches Unternehmen. Jede Datenübermittlung an OpenAI ist damit grundsätzlich ein Drittlandtransfer nach Kapitel V DSGVO — mit entsprechenden Anforderungen.

OpenAI Ireland Ltd. als EU-Vertragspartner: Für europäische Nutzer der Team-, Enterprise- und API-Angebote fungiert OpenAI Ireland Ltd. als Vertragspartner. Das ändert die rechtliche Ausgangslage, löst das Drittlandproblem aber nicht vollständig: Die Datenverarbeitung selbst findet nach wie vor auf US-Servern statt, OpenAI Ireland ist lediglich der europäische Vertragsanker.

Standard Contractual Clauses (SCCs): OpenAI setzt SCCs als Transfermechanismus ein. SCCs erlauben Drittlandtransfers, wenn die EU-Standardvertragsklauseln eingehalten werden. Sie sind aber kein Freifahrtschein: Der Verantwortliche — also Ihr Unternehmen — muss prüfen, ob das Schutzniveau im Empfängerland dem der EU tatsächlich entspricht.

Transfer Impact Assessment (TIA): Für Unternehmen, die größere Datenmengen oder besonders sensible Kategorien übermitteln, ist ein TIA empfehlenswert — und je nach Aufsichtsbehörde auch erwartet. Ein TIA dokumentiert, dass Sie die Risiken des Drittlandtransfers bewertet haben. Für die meisten KMU reicht eine einfache, schriftlich dokumentierte Risikobetrachtung.

Ehrliche Einschätzung: Eine vollständige Rechtssicherheit beim Drittlandtransfer zu OpenAI gibt es derzeit nicht. Die italienische Aufsichtsbehörde Garante hat OpenAI bereits mit einer einstweiligen Verfügung konfrontiert, der Hamburgische Datenschutzbeauftragte hat sich mehrfach zum Thema geäußert. Die Rechtslage entwickelt sich. Für KMU bedeutet das: Risiko minimieren, dokumentieren, beobachten.

Neben der DSGVO rückt mit dem EU AI Act ein weiterer Rechtsrahmen in den Fokus — was KMU dort beachten müssen, lesen Sie in unserem Artikel zum EU AI Act für KMU.

Auftragsverarbeitung – wann brauchen Sie einen AVV mit OpenAI?

Ein Auftragsverarbeitungsvertrag (AVV) nach Art. 28 DSGVO ist immer dann Pflicht, wenn ein Dienstleister personenbezogene Daten im Auftrag Ihres Unternehmens verarbeitet. Das trifft auf OpenAI zu, sobald Sie Daten mit Personenbezug übermitteln.

Wann gilt OpenAI als Auftragsverarbeiter? Wenn OpenAI die Daten nach Ihren Weisungen verarbeitet und keinen eigenen Zweck verfolgt — zum Beispiel beim Einsatz der API mit deaktiviertem Training. In der Consumer-Version hingegen agiert OpenAI als eigenverantwortlicher Verarbeiter, weil die Daten auch für eigene Zwecke (Training) genutzt werden können. Dort ist kein AVV verfügbar — und das ist das Problem.

So schließen Sie einen AVV mit OpenAI ab:

1. Für ChatGPT Team/Enterprise: Der DPA (Data Processing Agreement) wird im Rahmen der Nutzungsbedingungen automatisch einbezogen. In den Account-Einstellungen unter „Privacy“ oder „Data Controls“ finden Sie entsprechende Verweise. Empfehlung: Screenshot des akzeptierten DPA als Nachweis sichern.
2. Für die OpenAI API: Der DPA ist unter platform.openai.com in den Nutzungsbedingungen abrufbar und gilt mit Annahme der Terms of Service. Auch hier: Dokumentation sichern.
3. Consumer-Version: Kein AVV verfügbar. Punkt. Keine personenbezogenen Daten eingeben.

Wichtig: Den AVV allein abzuschließen reicht nicht. Er muss auch gelebt werden — das heißt, technische und organisatorische Maßnahmen (TOMs) müssen passen.

Das Verarbeitungsverzeichnis – so tragen Sie ChatGPT korrekt ein

Fast alle Unternehmen ab einer gewissen Größe sind nach Art. 30 DSGVO verpflichtet, ein Verarbeitungsverzeichnis zu führen. In der Praxis fehlt darin aber häufig der Eintrag für KI-Tools — obwohl ChatGPT schon seit Monaten im Einsatz ist.

Jede Verarbeitungstätigkeit mit personenbezogenen Daten gehört eingetragen. Das gilt auch für den Einsatz von ChatGPT, sobald Daten mit Personenbezug übermittelt werden.

Wer KI-Tools in die eigene Website einbettet, sollte außerdem die Cookie-Banner-Pflichten im Blick behalten — mehr dazu in unserem Artikel zur Cookie-Banner-Pflicht.

Mustereintrag (zum Kopieren und Anpassen)

Bezeichnung der Verarbeitungstätigkeit:

KI-gestützte Textassistent (ChatGPT / OpenAI API)

Verantwortlicher:

[Ihr Unternehmen, Adresse]

Zweck der Verarbeitung:

Unterstützung bei der Erstellung von Texten, E-Mails, Angeboten und internen Dokumenten durch KI-Sprachmodell.

Rechtsgrundlage:

Art. 6 Abs. 1 lit. f DSGVO (berechtigzte Interessen) –
alternativ: Art. 6 Abs. 1 lit. b bei Vertragsabwicklung.
[Je nach Einzelfall prüfen und anpassen.]

Kategorien betroffener Personen:

Mitarbeiter, Kunden, Interessenten, Geschäftspartner
[nur soweit tatsächlich Daten dieser Personen eingegeben werden]

Kategorien personenbezogener Daten:

Namen, Kontaktdaten, Kommunikationsinhalte, ggf. weitere betriebliche Informationen mit Personenbezug.
[Besondere Kategorien nach Art. 9 DSGVO: NICHT eingeben!]

Empfänger / Auftragsverarbeiter:

OpenAI Ireland Ltd., 1 Shelbourne Road, Dublin 4, Irland
(Muttergesellschaft: OpenAI LLC, USA)

Drittlandtransfer:

Ja – USA. Absicherung über Standard Contractual Clauses (SCCs) gemäß EU-Standardvertragsklauseln 2021.
Transfer Impact Assessment: [Datum und Ergebnis eintragen]

AVV abgeschlossen:

Ja – [Datum der Annahme der OpenAI DPA / Enterprise Terms]

Technische und organisatorische Maßnahmen:

[Verweis auf Ihr TOM-Dokument]

Löschfristen / Datenspeicherung:

Eingaben werden von OpenAI laut DPA nicht dauerhaft gespeichert (bei aktiviertem No-Training). Interne Protokolle/Outputs: [gemäß eigener Löschrichtlinie, z.B. 30 Tage]

Hinweis:

Dieser Mustereintrag dient als Arbeitsgrundlage und ersetzt keine individuelle Rechtsberatung.

KI-Tools im DSGVO-Vergleich: ChatGPT, Copilot, Gemini

Kein KI-Tool ist automatisch „DSGVO-konform“ — es geht immer um Risikominimierung und korrekte Dokumentation. Trotzdem gibt es relevante Unterschiede zwischen den gängigen Lösungen.

KRITERIUM	CHATGPT ENTERPRISE (OPENAI)	MICROSOFT COPILOT FOR M365	GOOGLE GEMINI FOR WORKSPACE
AVV verfügbar	☐ Ja	☐ Ja	☐ Ja
EU-Datenspeicherung	⚠ Teilweise (EU <u>Data Residency</u> in Entwicklung)	☐ <u>EU Data Boundary</u> verfügbar	⚠ Teilweise
Training auf Kundendaten	☐ Nein	☐ Nein	☐ Nein (bei Workspace)
Aufsichtsbehörden-Status	⚠ Unter Beobachtung	☐ Bislang wenig Beanstandungen	⚠ Vereinzelte Anfragen
Empfehlung für DACH-KMU	☐ Für reine Text-KI gut geeignet	☐ Vorteil bei bestehendem M365	☐ Vorteil bei Google Workspace

Ehrliche Einschätzung: Microsoft Copilot for M365 hat durch die EU Data Boundary-Initiative einen praktischen Vorteil für DACH-KMU, die bereits Microsoft 365 einsetzen — Daten können innerhalb der EU gespeichert und verarbeitet werden. Wer noch kein M365-Ökosystem hat, gewinnt durch einen Wechsel allein wegen ChatGPT wenig.

Entscheidend ist nicht das Tool, sondern die Implementierung: Welche Daten fließen wohin, wer hat Zugriff, was ist dokumentiert?

Branchenspezifische Risiken – wo besondere Vorsicht gilt

Für manche Branchen gelten über die DSGVO hinaus zusätzliche Anforderungen, die den Einsatz externer KI-Tools erheblich einschränken.

Anwaltskanzleien und Steuerberater

Neben der DSGVO gilt hier die Berufsgeheimnispflicht nach § 203 StGB. Mandantendaten dürfen nicht ungefiltert in externe Cloud-KI-Dienste fließen — unabhängig davon, ob ein AVV besteht. Wer als Anwalt oder Steuerberater ChatGPT nutzt, muss entweder strikte Anonymisierungspflichten einführen oder lokale LLM-Alternativen prüfen, bei denen keine Daten das eigene Netzwerk verlassen. Mehr zu konkreten Einsatzmöglichkeiten finden Sie im Artikel ChatGPT für Steuerberater in Österreich.

Arztpraxen und Gesundheitsberufe

Gesundheitsdaten fallen unter Art. 9 DSGVO — besondere Kategorie, höchste Schutzanforderungen. Eine explizite Einwilligung der Patienten reicht für die Übermittlung an externe KI-Tools in der Regel nicht aus, weil die Verarbeitung durch OpenAI nicht zwingend dem ursprünglichen Behandlungszweck entspricht. Die Empfehlung ist eindeutig: Keine Patientendaten in externe KI-Tools eingeben. Punkt. Für administrative Aufgaben ohne Patientenbezug (Terminvorlagen, interne Kommunikation) kann ChatGPT Enterprise dagegen sinnvoll sein.

HR-Abteilungen und Recruiting

Bewerberdaten, Gehaltsinfos und Leistungsbeurteilungen sind hochsensibel. In Österreich und Deutschland muss der Betriebsrat bei der Einführung von KI-Systemen zur Personalbeurteilung einbezogen werden (§ 87 BetrVG in Deutschland, § 96 ArbVG in Österreich). Zusätzlich bestehen Transparenzpflichten gegenüber Bewerbern: Wenn KI bei Vorauswahlentscheidungen beteiligt ist, muss das kommuniziert werden — sowohl in der Datenschutzerklärung als auch auf Nachfrage. Wer KI im Recruiting einsetzt, ohne das zu dokumentieren, riskiert nicht nur DSGVO-Bußgelder, sondern auch arbeitsrechtliche Konsequenzen.

Mitarbeiter-Richtlinie ChatGPT – was eine gute Policy enthält

Eine interne KI-Nutzungsrichtlinie ist kein Nice-to-have. Wer ChatGPT im Unternehmen zulässt, ohne schriftlich zu regeln, was erlaubt ist und was nicht, haftet für das, was Mitarbeiter damit anstellen. Und erfahrungsgemäß stellen Mitarbeiter einiges damit an.

Eine praxistaugliche ChatGPT-Policy für KMU enthält mindestens:

- **Freigabe-Regelung:** Welche Version ist freigegeben? (Consumer-Version: nein. Enterprise/API: ja, unter Bedingungen.) Diese Aussage muss eindeutig sein.
- **Datenkategorien:** Welche Daten dürfen eingegeben werden? (Empfehlung: Positivliste statt Negativliste — also genau benennen, was erlaubt ist, nicht was verboten ist.)
- **Output-Kennzeichnung:** Wie werden KI-generierte Texte intern markiert? Wer prüft vor der Verwendung?
- **Verantwortlichkeiten:** Wer ist Ansprechpartner bei Fragen? Wer entscheidet über neue Anwendungsfälle?
- **Schulungspflicht:** Mitarbeiter müssen die Policy kennen — und das sollte dokumentiert werden (Unterschrift oder digitale Bestätigung).
- **Review-Zyklus:** Die Rechtslage ändert sich. Die Policy sollte mindestens einmal jährlich überprüft und aktualisiert werden.

Eine solche Policy muss nicht lang sein. Zwei Seiten mit klaren Regeln sind wirkungsvoller als ein zehnzeitiges Dokument, das niemand liest.

Praxis-Tipp: In drei Schritten zur rechtskonformen ChatGPT-Nutzung

Diese drei Schritte decken den Kern ab — ohne Vollgutachten, aber mit solider Grundlage.

Schritt 1 — Consumer-Version für geschäftliche Zwecke mit Personenbezug abschalten. Kommunizieren Sie klar, dass chatgpt.com für Echtdaten nicht freigegeben ist. Wechseln Sie auf ChatGPT Enterprise oder die OpenAI API. Das ist der wichtigste Schritt und hat sofortige Wirkung.

Schritt 2 — Dokumentation in Ordnung bringen. AVV mit OpenAI prüfen und nachweislich annehmen. Verarbeitungsverzeichnis um den Eintrag „KI-Textassistent“ ergänzen (Muster oben). Transfer Impact Assessment dokumentieren — auch eine kurze schriftliche Risikobetrachtung ist besser als gar keine.

Schritt 3 — Interne Richtlinie erstellen und kommunizieren. Mitarbeiter schriftlich informieren, was erlaubt ist und was nicht. Schulung durchführen oder zumindest schriftliche Einweisung dokumentieren. Policy in den Jahres-Review-Kalender aufnehmen.

Diese Schritte sind machbar — aber es gibt Fallstricke, die je nach Branche und bestehender IT-Infrastruktur variieren. Wer in einer Kanzlei oder Praxis tätig ist, hat andere Anforderungen als ein Handwerksbetrieb. Und wer bereits Microsoft 365 im Einsatz hat, kommt mit Copilot möglicherweise günstiger und rechtskonformer ans Ziel als mit einem separaten OpenAI-Vertrag.

Wenn Sie unsicher sind, welche Version für Ihr Unternehmen die richtige ist, oder wie ein Verarbeitungsverzeichnis-Eintrag in Ihrem konkreten Fall aussehen sollte — genau dafür ist unser unverbindliches Beratungsgespräch da.

FAQ: Die häufigsten Fragen zu DSGVO und ChatGPT

Darf ich ChatGPT für die Arbeit nutzen, wenn ich die Einstellungen anpasse?

Der Opt-out aus dem Training in der Consumer-Version (unter „Datenkontrolle“ in den Einstellungen) ist ein sinnvoller Schritt, löst aber das eigentliche Problem nicht: Ohne AVV fehlt die vertragliche Grundlage für die Auftragsverarbeitung, und der Drittlandtransfer ist nicht ausreichend abgesichert. Personenbezogene Daten gehören damit weiterhin nicht in die Consumer-Version.

Was passiert, wenn mein Mitarbeiter unerlaubt Kundendaten in ChatGPT eingibt?

Das ist ein Datenschutzvorfall, der intern zu dokumentieren ist. Je nach Art und Umfang der betroffenen Daten besteht eine Meldepflicht an die Aufsichtsbehörde innerhalb von 72 Stunden ([Art. 33 DSGVO](#)) – und unter Umständen auch eine Benachrichtigungspflicht gegenüber den betroffenen Personen (Art. 34 DSGVO). Bußgelder sind möglich. Die beste Prävention ist eine klare schriftliche Policy, bevor etwas passiert.

Ist ChatGPT Enterprise wirklich [DSGVO](#)-konform?

„Konformer“ ist die treffendere Formulierung. Kein Tool ist automatisch DSGVO-konform – das hängt immer davon ab, wie es eingesetzt wird, welche Daten eingegeben werden und ob die Dokumentation stimmt. ChatGPT Enterprise bietet mit AVV, deaktiviertem Training und SCCs eine deutlich bessere Ausgangslage als die Consumer-Version. Aber es bleibt ein US-Dienst mit Drittlandtransfer, und die Implementierung im eigenen Unternehmen muss passen.

Muss ich meine Kunden informieren, wenn ich KI für Kommunikation nutze?

Nach Art. 13 und 14 DSGVO sind Sie verpflichtet, Betroffene über die Verarbeitung ihrer Daten zu informieren. Wenn Kundendaten in KI-Tools fließen, gehört das in die Datenschutzerklärung. Ob darüber hinaus eine aktive Benachrichtigung notwendig ist, hängt vom Einzelfall ab. Grundregel: Datenschutzerklärung auf den aktuellen Stand bringen, sobald neue Tools im Einsatz sind.

Welche [Datenschutzbehörde](#) ist für OpenAI in Deutschland zuständig?

Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit hat sich als federführende deutsche Aufsichtsbehörde für OpenAI positioniert, da OpenAI keine deutsche Niederlassung hat. Für Österreich ist die Datenschutzbehörde (DSB) in Wien zuständig, wenn es um Beschwerden österreichischer Nutzer geht. Die Koordination auf EU-Ebene läuft über den Europäischen Datenschutzausschuss ([EDSA](#)). Stand dieser Zuständigkeitsverteilung: Juni 2025 – Änderungen sind möglich.

Nächste Schritte – und wo Sie konkrete Unterstützung bekommen

Die wichtigsten To-dos im Überblick:

1. Consumer-Version für geschäftliche Echtdaten intern sperren oder klar als „privat, kein Personenbezug“ einschränken
2. Auf ChatGPT Enterprise oder OpenAI API wechseln und AVV nachweislich annehmen
3. Verarbeitungsverzeichnis um den KI-Eintrag ergänzen (Muster oben als Ausgangspunkt)
4. Transfer Impact Assessment dokumentieren
5. Interne KI-Nutzungsrichtlinie erstellen, kommunizieren und Mitarbeiter schriftlich einweisen

Wer diese Schritte konsequent umsetzt, hat eine deutlich solidere DSGVO-Basis als die Mehrheit der KMU, die ChatGPT derzeit ohne jegliche Dokumentation einsetzen.

Die Schritte sind bekannt — aber die Umsetzung hängt immer von den Details ab: Welche Daten verarbeiten Sie tatsächlich? Welche Branchenregeln kommen oben drauf? Passt ChatGPT Enterprise zu Ihrer bestehenden IT, oder wäre Microsoft Copilot die bessere Wahl, weil Sie ohnehin M365 nutzen?

Genau für solche Fragen bieten wir bei Strukturaflow ein unverbindliches 30-Minuten-Beratungsgespräch an. Kein Verkaufsgespräch, sondern eine ehrliche Einschätzung Ihrer konkreten Situation — damit Sie wissen, was Sie als nächstes tun sollten, bevor Sie etwas Falsches dokumentieren oder freigeben.

NÄCHSTER SCHRITT

Mehr praktische KI-Anleitungen für KMU

Dieser Artikel ist Teil des KI-Hubs von Strukturaflow — einer deutschsprachigen Plattform für den praktischen KI-Einsatz in kleinen und mittleren Unternehmen.

<https://wissen.strukturaflow.it.com>