PRÜFKARTE CHATGPT UND DATENSCHUTZ

Aus dem Beitrag „ChatGPT im Unternehmen: Datenschutz richtig regeln“. ChatGPT und Datenschutz passen im Unternehmen zusammen, wenn drei Dinge stimmen: Dein Team arbeitet mit einem Firmenkonto, für das es einen Vertrag zur Auftragsverarbeitung (AVV) gibt, die Eingaben fließen nicht ins Training, und es ist klar geregelt, welche Daten überhaupt in den Chat dürfen.

> Diese Karte hilft dir beim Abwägen, eine Rechtsberatung ist sie aber nicht. Was dein Team im Einzelfall eingeben darf, klärst du mit deiner Rechtsberatung und, falls vorhanden, mit deinem Datenschutzbeauftragten. Stand der OpenAI-Angaben: 18. November 2026; sie können sich ändern.

1 · VORHER KLÄREN: BEVOR PERSONENBEZOGENE DATEN IN CHATGPT GEHEN

Ob dein Team Daten von Kundschaft oder Beschäftigten in ChatGPT verarbeiten darf, lässt sich nicht pauschal beantworten. Mindestens diese Punkte klärst du vorher:

- ☐ **Ein Firmenkonto mit Vertrag nach Artikel 28 Absatz 3 DSGVO.** OpenAI nennt einen AVV nur für seine Firmenangebote, etwa ChatGPT Business und ChatGPT Enterprise.
- ☐ **Am besten kein Training mit den Eingaben.** Die deutsche Datenschutzkonferenz (DSK) hält Anwendungen für vorzugswürdig, die Ein- und Ausgaben nicht zum Training verwenden.
- ☐ **Eine Rechtsgrundlage und ein klarer Zweck,** etwa die Antwort auf die Anfrage einer Kundin, und nur so viele Daten, wie dafür nötig sind. Mein Rat: Probier zuerst, ob ein Entwurf ohne Namen reicht, den dein Team danach ergänzt.
- ☐ **Eine geklärte Grundlage für die Übermittlung außerhalb des EWR.** Halte fest, auf welche Grundlage sich die Übermittlung in deinem Vertrag stützt.
- ☐ **Eine Prüfung, ob eine Datenschutz-Folgenabschätzung nötig ist.** Ob dein Fall darunter fällt, klärst du mit der für Datenschutz zuständigen Person.

Wenn einer dieser Punkte offen ist, bleiben personenbezogene Daten draußen, und ChatGPT arbeitet nur mit Texten ohne Personenbezug.

2 · DAS GEHÖRT NIE IN DEN CHAT, AUCH NICHT IM FIRMENKONTO

Ein Firmenkonto regelt, wie OpenAI mit deinen Daten umgeht. Es macht aber nicht jede Eingabe zulässig.

- **Zugangsdaten:** Passwörter, Schlüssel für Schnittstellen sowie Bank- und Zahlungsdaten.
- **Besondere Kategorien nach Artikel 9 DSGVO:** Gesundheitsdaten, Angaben zu Religion, Gewerkschaftszugehörigkeit, sexueller Orientierung und die anderen dort genannten Daten, solange keine Ausnahme aus Artikel 9 Absatz 2 greift und das mit der für Datenschutz zuständigen Person geklärt ist.
- **Daten anderer Menschen in persönlichen Konten:** Kundendaten, Bewerbungen oder Personalnotizen haben dort nichts verloren.
- **Fragen, deren Antwort über eine Person entscheidet:** Lass dir von ChatGPT keine Fakten über Kundinnen, Bewerber oder Beschäftigte liefern, die du nicht selbst prüfst.

3 · IN VIER SCHRITTEN ZUR ENTSCHEIDUNG FÜR DEINEN BETRIEB

Schritt 1 · Bestand aufnehmen

Frag offen, wer ChatGPT heute schon nutzt, mit welchem Konto und für welche Aufgaben. Achte besonders auf private Konten, die für die Arbeit genutzt werden. Die DSK rät, dass die Firma dafür eigene Konten und Geräte stellt.

Nr.	Wer nutzt ChatGPT?	Mit welchem Konto?	Wofür?
1			
2			
3			
4			
5			
6			
7			
8			

Schritt 2 · Kontoart festlegen

Entscheide, ob für die Arbeit ein persönliches Konto nur für Texte ohne Personenbezug reicht oder ob du einen Firmen-Arbeitsbereich mit Vertrag brauchst.

Unsere Entscheidung	

Schritt 3 · Einstellungen setzen

- ☐ Training aus, wo das Konto es zulässt
- ☐ Speicherdauer festgelegt
- ☐ Freigaben für Apps festgelegt
- ☐ Team informiert, wer im Arbeitsbereich Chats einsehen kann

Schritt 4 · Regel aufschreiben und schulen

Halte Kontoart, erlaubte Daten und die Ansprechperson in deiner KI-Richtlinie fest, und erklär sie deinem Team an Beispielen aus deinem Betrieb.

Kontoart	
Erlaubte Daten	
Ansprechperson	
Schulung im Team am	

Im ganzen Beitrag: was sich je Kontoart ändert, der Weg der Daten in die USA und alle Quellen:
https://architect5.com/blog/chatgpt-datenschutz/

architect[5] · Thomas Rettenbacher, AI Workflow Architect
Beitrag vom 19. November 2026 · Stand der OpenAI-Angaben: 18. November 2026