ChatGPT & Co. rechtssicher nutzen

Praktischer Ratgeber für den
Einsatz generativer KI im Unternehmen

In diesem Ratgeber erfahren Sie:

- Welche Daten Sie niemals eingeben sollten
- Wie Sie Datenschutz und DSGVO einhalten
- Was bei KI-generierten Inhalten zu beachten ist
- Wie Sie eine Unternehmensrichtlinie erstellen

AI-Legal-Flow GmbH
www.ai-legal-flow.de

Stand: Dezember 2025

Inhaltsverzeichnis

Einleitung: Die neue Realität

ChatGPT, Microsoft Copilot, Google Gemini, Claude – generative KI ist im Arbeitsalltag angekommen. Laut Umfragen nutzen bereits über 60% der Büroangestellten KI-Tools, oft täglich.

Das bringt enorme Produktivitätsgewinne, aber auch **rechtliche Risiken**, die viele Unternehmen unterschätzen:

- Datenschutzverstöße durch Eingabe sensibler Daten
- Urheberrechtliche Probleme bei KI-Inhalten
- Haftung für fehlerhafte KI-Ausgaben
- Compliance-Verstöße gegen die KI-Verordnung

Gute Nachricht: Mit dem richtigen Wissen und klaren Regeln lassen sich diese Risiken beherrschen. Dieser Ratgeber zeigt Ihnen wie.

Risiko 1: Datenschutz und Vertraulichkeit

Das Problem

Wenn Sie Text in ChatGPT eingeben, verlässt dieser Text Ihr Unternehmen. Er wird:

- An Server (meist in den USA) übertragen
- Von OpenAI verarbeitet
- Möglicherweise für Training verwendet (je nach Einstellung)
- Potenziell von Mitarbeitern eingesehen (bei Content Moderation)

Kritisch: Alles, was Sie in ChatGPT eingeben, sollten Sie so behandeln, als würden Sie es öffentlich machen. Auch wenn es nicht öffentlich wird – das Risiko besteht.

Was Sie NIEMALS eingeben sollten

1. **Personenbezogene Daten**
   - Namen von Kunden oder Mitarbeitern
   - E-Mail-Adressen, Telefonnummern
   - Adressen, Geburtsdaten
   - Gesundheitsdaten, Gehaltsinformationen
2. **Vertrauliche Geschäftsinformationen**
   - Unveröffentlichte Finanzdaten
   - Strategische Pläne
   - Kundenlisten, Preiskalkulationen
   - Interne Berichte

3. **Geistiges Eigentum**
    - Quellcode (vor der Veröffentlichung)
    - Patentanmeldungen
    - Unveröffentlichte Designs
4. **Zugangsdaten**
    - Passwörter
    - API-Keys
    - Zertifikate

DSGVO-Konformität

Die DSGVO gilt auch bei KI-Nutzung. Wenn Sie personenbezogene Daten in KI-Systeme eingeben:

- Brauchen Sie eine **Rechtsgrundlage** (meist schwierig)
- Müssen Sie **Betroffene informieren**
- Ist ein **Auftragsverarbeitungsvertrag** (AVV) nötig
- Muss der **Drittlandtransfer** geregelt sein (USA!)

Einfache Regel: Geben Sie keine personenbezogenen Daten ein. Dann haben Sie auch kein DSGVO-Problem mit ChatGPT.

Praktische Tipps

1. **Anonymisieren Sie**
    - Statt „Herr Müller hat am 15.3. gekündigt“ schreiben Sie „Ein Mitarbeiter hat kürzlich gekündigt“
    - Ersetzen Sie Namen durch Platzhalter: „Kunde A“, „Projekt X“
2. **Nutzen Sie Unternehmensversionen**
    - ChatGPT Enterprise, Microsoft 365 Copilot etc.
    - Diese bieten besseren Datenschutz (AVV, kein Training)
3. **Deaktivieren Sie Chat-History (wenn möglich)**
    - Bei ChatGPT: Settings > Data Controls > Chat History

Risiko 2: Urheberrecht bei KI-Inhalten

Wem gehören KI-generierte Inhalte?

Die Rechtslage ist noch nicht abschließend geklärt, aber:

- **KI selbst kann kein Urheberrecht haben** (nur Menschen)
- **Rein KI-generierte Inhalte** sind vermutlich gemeinfrei
- **Mit menschlicher Bearbeitung** können sie schutzfähig werden

Risiko: Plagiate und Rechtsverletzungen

KI-Modelle wurden mit riesigen Datenmengen trainiert, darunter:

- Urheberrechtlich geschützte Texte
- Bilder von Künstlern
- Musik, Code, etc.

Es kann vorkommen, dass KI **bestehende Werke reproduziert** oder stark anlehnt.

Ihre Haftung: Wenn Sie KI-generierte Inhalte verwenden, die Urheberrechte verletzen, haften SIE – nicht die KI, nicht OpenAI.

Empfehlungen

1. **KI-Output prüfen**
   - Bei wichtigen Texten: Plagiatsprüfung durchführen
   - Bei Bildern: Ähnlichkeitssuche nutzen
2. **Nicht 1:1 übernehmen**
   - KI als Ausgangspunkt nutzen, dann bearbeiten
   - Eigene Formulierungen einbringen
3. **Vorsicht bei Stilimitationen**
   - „Schreibe wie [bekannter Autor]“ kann problematisch sein
4. **Transparenz bei Bedarf**
   - Bei wissenschaftlichen Arbeiten: KI-Nutzung angeben
   - Bei Kundenaufträgen: Ggf. klären, ob KI-Einsatz akzeptiert wird

Risiko 3: Fehlerhafte Informationen

Das Halluzinations-Problem

Generative KI „erfindet“ manchmal Informationen:

- Falsche Fakten, die plausibel klingen
- Erfundene Zitate und Quellenangaben
- Veraltete Informationen (Wissenscutoff)
- Logische Fehler bei komplexen Themen

Haftungsrisiko

Wenn Sie fehlerhafte KI-Informationen weitergeben:

- **Beratungshaftung:** Falsche Beratung kann Schadensersatzpflichten auslösen
- **Produkthaftung:** Bei Verwendung in Produkten
- **Reputationsschäden:** Vertrauensverlust bei Kunden
- **Arbeitsrechtlich:** Fehler durch Mitarbeiter

Goldene Regel: KI-Output ist ein **Entwurf**, kein fertiges Ergebnis. Immer prüfen, bevor Sie es verwenden.

Prüfpflichten je nach Kontext

Kontext	Erforderliche Prüfung
Interne Notizen	Minimale Prüfung auf Plausibilität
Externe Kommunikation	Faktencheck für alle wichtigen Aussagen
Rechtliche/medizinische Themen	Fachliche Überprüfung durch Experten
Veröffentlichte Inhalte	Vollständige redaktionelle Prüfung

Risiko 4: KI-Verordnung

Was fordert der AI Act?

Ab August 2026 gilt die **Kompetenzpflicht** nach Artikel 4:

Unternehmen müssen sicherstellen, dass Mitarbeiter, die KI-Systeme nutzen, über ein „ausreichendes Maß an KI-Kompetenz“ verfügen.

Was bedeutet das konkret?

Für ChatGPT-Nutzer bedeutet „KI-Kompetenz“:

1. **Verstehen**, wie das Tool grundsätzlich funktioniert
2. **Kennen** der Risiken und Grenzen
3. **Fähigkeit**, Ergebnisse kritisch zu bewerten
4. **Wissen**, welche Daten nicht eingegeben werden dürfen

Nachweis durch Schulung

Der einfachste Weg, die Kompetenzpflicht zu erfüllen:

- Strukturierte Schulung für alle KI-Nutzer
- Dokumentation der Teilnahme
- Zertifikate als Nachweis

Unternehmensrichtlinie erstellen

Warum eine Richtlinie?

Eine KI-Richtlinie:

- Gibt Mitarbeitern **Orientierung**
- **Reduziert Risiken** durch klare Regeln
- Dient als **Nachweis** für Compliance-Bemühungen
- Ermöglicht **konsistentes Handeln** im Unternehmen

Muster-Richtlinie für ChatGPT & Co.

Muster: KI-Nutzungsrichtlinie (Kurzfassung)

1. Erlaubte Nutzung
Die Nutzung von ChatGPT/[Tool] ist für folgende Zwecke freigegeben:

- Unterstützung bei Texterstellung
- Recherche und Brainstorming
- Übersetzungen und Zusammenfassungen
- Code-Unterstützung (ohne sensiblen Code)

2. Verbotene Eingaben
Folgende Daten dürfen NICHT eingegeben werden:

- Personenbezogene Daten (Namen, E-Mails, etc.)
- Vertrauliche Geschäftsinformationen
- Passwörter oder Zugangsdaten
- Unveröffentlichter Quellcode

3. Qualitätskontrolle
KI-generierte Inhalte müssen vor Verwendung auf Richtigkeit geprüft werden. Die Verantwortung für den Inhalt liegt beim Mitarbeiter.
4. Kennzeichnung
Bei Bedarf sind KI-generierte Inhalte als solche zu kennzeichnen.
5. Schulungspflicht
Alle Mitarbeiter, die KI-Tools nutzen, müssen die KI-Grundlagenschulung absolvieren.

Checkliste: Rechtssicherer KI-Einsatz

Vor jeder Eingabe

☐ Enthält mein Text personenbezogene Daten?

☐ Enthält er vertrauliche Geschäftsinformationen?

☐ Würde ich diese Information öffentlich teilen?

☐ Kann ich den Text anonymisieren?

Nach jeder Ausgabe

☐ Habe ich die Fakten überprüft?

☐ Sind Quellen/Zitate korrekt?

☐ Ist der Text frei von Plagiaten?

☐ Habe ich den Text für meinen Zweck angepasst?

Im Unternehmen

☐ Gibt es eine KI-Nutzungsrichtlinie?

☐ Wurden alle KI-Nutzer geschult?

☐ Gibt es einen Ansprechpartner für Fragen?

☐ Werden Schulungsnachweise dokumentiert?

Fazit: Nutzen, aber richtig

ChatGPT und andere KI-Tools sind mächtige Werkzeuge, die die Produktivität steigern können. Aber wie bei jedem Werkzeug kommt es auf den richtigen Umgang an.

Die wichtigsten Regeln:

1. **Keine sensiblen Daten eingeben**
2. **Ergebnisse immer prüfen**
3. **Verantwortung nicht an die KI delegieren**
4. **Mitarbeiter schulen und informieren**

Mit diesen Grundsätzen nutzen Sie KI effektiv und rechtssicher.

Zusammenfassung auf einen Blick

Thema	Kernpunkt
Datenschutz	Keine personenbezogenen Daten eingeben
Vertraulichkeit	Geschäftsgeheimnisse nie in KI-Tools
Urheberrecht	KI-Output prüfen, nicht 1:1 übernehmen
Fakten	Alles verifizieren, KI kann „halluzinieren“
Haftung	Sie haften für KI-Output, nicht die KI
KI-Verordnung	Schulung aller KI-Nutzer bis August 2026
Richtlinie	Klare Regeln für alle Mitarbeiter