

Interne Richtlinie zur Nutzung von KI-Tools im Unternehmen

1. Zweck und Ziel der Richtlinie

Diese Richtlinie regelt den verantwortungsvollen, sicheren und datenschutzkonformen Umgang mit KI-gestützten Software-Tools im Unternehmen.

Ziel ist es,

- Mitarbeiter beim sicheren Einsatz von KI-Tools zu unterstützen,
- den Schutz personenbezogener und besonderer personenbezogener Daten sicherzustellen,
- Fehlverwendungen, Datenschutzverstöße und Fehlinformationen zu vermeiden,
- Transparenz darüber zu schaffen, was erlaubt ist und was nicht.

Diese Richtlinie gilt für alle Mitarbeiter, unabhängig von Funktion, Position oder Beschäftigungsart.

2. Was sind KI-Tools?

KI-Tools (Künstliche-Intelligenz-Tools) sind Softwareanwendungen, die Inhalte analysieren, erstellen, zusammenfassen, strukturieren oder Vorschläge generieren können, z. B.:

- Text- und Dokumentenerstellung
- Auswertungen und Zusammenfassungen
- Unterstützung bei Recherche oder Formulierungen
- Prozess- und Strukturhilfe

Alle heute gebräuchlichen KI-Tools sind sogenannte große Sprachmodelle (Large Language Models LLM). Sie denken nicht selbst, sondern erzeugen Ergebnisse auf Basis von statistischen Wahrscheinlichkeiten. Das heißt, die Ergebnisse „klingen gut“, aber sie müssen nicht richtig sein. Die Ergebnisse können unvollständig, fehlerhaft oder missverständlich sein.

3. Zulässige Nutzung – nur freigegebene KI-Tools

3.1 Grundsatz



Es dürfen ausschließlich die vom Arbeitgeber ausdrücklich freigegebenen KI-Tools genutzt werden. Bei Rückfragen hierzu ist die IT-Abteilung erreichbar.



Die Nutzung privater oder nicht genehmigter KI-Anwendungen (z. B. private Accounts, frei zugängliche Online-KI-Dienste) ist untersagt, insbesondere für dienstliche Zwecke.

3.2 Zugang und Nutzung

- Die Nutzung erfolgt ausschließlich über dienstliche Benutzerkonten, welche von der IT vergeben werden
- Eigene private Log-ins oder anonyme Nutzung sind nicht zulässig
- Zugangsdaten dürfen nicht weitergegeben werden

Der Arbeitgeber stellt sicher, dass die eingesetzten KI-Tools ein angemessenes Datenschutz- und Sicherheitsniveau gemäß DSGVO einhalten bzw. lässt sich von dessen Anbietern die Einhaltung des Datenschutzes per Vertrag zusichern.

4. Grundregeln für den sorgsamen Umgang mit KI-Tools

4.1 Ergebnisqualität hängt vom Prompt ab.

Die Qualität der „Prompts“, also der Eingabeaufforderungen entscheidet massiv darüber, wie hilfreich, richtig oder qualitativ gut die Antworten sind. Der Unterschied liegt fast immer in Klarheit, Kontext und Ziel. Hier sind konkrete Beispiele

Zu vage:

- „Erklär mir Sport.“
👉 Problem: Riesiges Thema, kein Fokus → nur oberflächliche Infos.
- „Ich will fitter werden.“
👉 Problem: Ich weiß nicht: Wie fit? Wofür? Mit welchen Einschränkungen?

Klar + konkret

- „Erklär mir die Vorteile von Krafttraining für Anfänger in 5 kurzen Punkten.“
👉 Gut: klarer Umfang + Zielgruppe + Struktur
- „Gib mir 5 gesunde Frühstücksideen unter 400 kcal in Stichpunkten.“
👉 Gut: Direkt nutzbare Antworten

4.2 Datenminimierung und Datensparsamkeit

So wenig Daten wie möglich – nur so viel wie unbedingt nötig.

- Es dürfen nur die für den konkreten Zweck erforderlichen Informationen eingegeben werden
- Wo möglich, sollen Namen, konkrete Identifikationsmerkmale oder detailreiche Fallbeschreibungen vermieden werden. Wenn nicht möglich, gilt das Prinzip der Datensparsamkeit
- Wo möglich, sind Daten zu anonymisieren

✅ Beispiel (richtig):

„Formuliere eine sachliche Antwort auf eine Beschwerde eines Kunden wegen verspäteter Lieferung.“

❌ Beispiel (falsch):

„Formuliere eine Antwort an Frau Müller, geboren am 12.03.1980, wohnhaft in ...“

4.3 Keine Vorschnelligkeit – KI ersetzt keine Prüfung

KI-Ergebnisse sind Vorschläge, keine verbindlichen Fakten.

Jeder Mitarbeiter ist verpflichtet,

- Inhalte zu prüfen, zu bewerten und ggf. zu korrigieren
- fachliche, rechtliche und sprachliche Richtigkeit sicherzustellen
- KI-Texte nicht ungeprüft weiterzugeben oder zu versenden

⚠️ Verantwortung verbleibt immer beim Menschen, nicht bei der KI.

5. Besondere Kategorien personenbezogener Daten (Art. 9 DSGVO)

5.1 Was zählt zu besonderen personenbezogenen Daten?

Besondere Kategorien personenbezogener Daten sind insbesondere Informationen über:

- Gesundheitsdaten (z. B. Krankheiten, Pflegebedürftigkeit, Diagnosen)
- Behinderungen oder Gleichstellungen
- religiöse oder weltanschauliche Überzeugungen
- Politische Meinungen oder Gewerkschaftszugehörigkeit
- biometrische oder genetische Daten
- Angaben zur sexuellen Orientierung
- Daten von Kindern und Heranwachsenden bis 18 Jahre

Diese Daten genießen **besonderen Schutz**. Sie finden sich im Artikel 9 und Artikel 10 der DSGVO.

5.2 Grundsatz für den Einsatz von KI-Tools

 Diese Daten dürfen grundsätzlich NICHT in KI-Tools eingegeben werden.

Eine Ausnahme ist nur dann zulässig, wenn alle folgenden Voraussetzungen erfüllt sind:

1. absolute Notwendigkeit für die konkrete Aufgabe
2. vorherige Rücksprache und Freigabe durch den zuständigen Vorgesetzten
3. Zweckprüfung und Datenminimierung
4. Nutzung eines vom Arbeitgeber freigegebenen KI-Tools

Ohne ausdrückliche Freigabe ist die Eingabe solcher Daten unzulässig.

5.3 Verständliche Beispiele

 **Zulässig (nach Freigabe):**

- Unterstützung bei der neutralen Formulierung eines allgemeinen Informationsschreibens, ohne konkrete Gesundheitsangaben einzelner Personen
- Strukturhilfe für einen allgemeinen Prozess, ohne personenbezogene Daten

 **Unzulässig:**

- Eingabe konkreter Krankheitsverläufe
- Beschreibung einzelner Pflege- oder Betreuungsfälle mit identifizierbaren Details
- Hochladen von vollständigen Personalakten, Arztbriefen oder Gutachten

6. Typische erlaubte Anwendungsbeispiele

Beispiel 1: Textunterstützung

 **Erlaubt:**

„Bitte formuliere einen neutralen Entwurf für eine interne E-Mail zur Erinnerung an Dokumentationspflichten.“

Beispiel 2: Strukturhilfe

✅ Erlaubt:

„Erstelle eine übersichtliche Checkliste für einen standardisierten Onboarding-Prozess ohne personenbezogene Details.“

7. Unzulässige Nutzung

❌ Untersagt ist insbesondere:

- Nutzung nicht genehmigter KI-Tools bzw. Anbieter
- Eingabe sensibler Daten ohne Freigabe
- Nutzung zur Leistungs- oder Verhaltenskontrolle von Mitarbeitenden
- Veröffentlichung oder Weitergabe ungeprüfter KI-Inhalte
- Umgehung interner Sicherheits- oder Datenschutzvorgaben

8. Verantwortung, Schulung und Konsequenzen

- Alle Mitarbeiter sind verpflichtet, diese Richtlinie einzuhalten
- Verstöße können arbeitsrechtliche Konsequenzen nach sich ziehen
- Bei Unsicherheiten gilt: vorher fragen, nicht nachher erklären

Ansprechstellen:

- direkte Führungskraft
- Datenschutzbeauftragter

9. Inkrafttreten und Unterweisung

Diese Richtlinie tritt mit Veröffentlichung in Kraft.

Alle Mitarbeiter werden verbindlich unterwiesen und bestätigen die Kenntnisnahme. Des Weiteren wird mit Unterschrift bestätigt, das hierzugehörige Schulungsvideo (30 Minuten) vollständig angeschaut und verinnerlicht zu haben. Offene Fragen wurden vor Unterschriftsleistung beantwortet.

Emstek, Stand vom 30.07.2026

Name in Druckbuchstaben:

i.V. 

Unterschrift Datenschutzkoordinator

Unterschrift Mitarbeiter