

Anleitung zur Nutzung von KI-Tools – DSGVO- & AI-Act-konform

◆ **1. Grundsätze für den KI-Einsatz**

- **KI darf unterstützen, nicht entscheiden:** KI-Tools dürfen **niemals ohne menschliche Kontrolle** Entscheidungen über Mitarbeiter, Mandanten oder finanzielle Belange treffen.
- **Vertraulichkeit und Datenschutz stehen an erster Stelle:** Alle eingesetzten KI-Systeme müssen DSGVO-konform sein.
- **Transparenzpflicht:** Der Einsatz von KI muss erkennbar und nachvollziehbar sein.

◆ **2. Was ist erlaubt?**

Zulässige KI-Nutzung im Büroalltag:

Anwendung	Beispiel
Texterkennung (OCR)	Auslesen von Rechnungen oder Lohnabrechnungen
Sprachassistent/Chatbots	Kundenbegrüßung oder erste Infos
Textvorschläge	KI-Tools zur Formulierung von E-Mails
Unterstützung bei Controlling	Analysen auf Basis anonymisierter Daten

3. Was ist verboten?

Nicht erlaubt nach AI Act & DSGVO:

- **Profiling von Mitarbeitern** z. B. über Krankheitstage oder Leistung
- **Automatisierte Bewertung** zur Auswahl, Beförderung oder Kündigung
- **Emotionserkennung** oder Stimm-/Gesichtsanalyse
- **Verwendung sensibler Daten in KI-Tools**, z. B. Gesundheitsdaten oder Religionszugehörigkeit
- **Nutzung von KI ohne Wissen der betroffenen Person**



⚠ 4. Risikoeinstufung (gemäß AI Act)

Risiko-Stufe	Beschreibung	Beispiele	Maßnahmen bei der Risikostufe
Hoch ●	KI entscheidet über Mitarbeiter oder Mandanten	Leistungsmessung, Krankheitsmuster, Kreditbewertung, Controlling	Nur mit Genehmigung, Risikomanagement, Dokumentation , menschlicher Kontrolle, Kein automatisiertes Scoring oder Profiling, Keine personenbezogenen Bewertungen
Begrenzt ●	Interaktion mit KI erkennbar, keine automatischen Entscheidungen	Chatbots,	Transparenzpflicht , Kennzeichnung, dass es sich um KI handelt
Gering ●	Kein Einfluss auf Menschen oder Rechte	Spam-Filter, Terminplanung, Textvorschläge (Antwortschreiben), Recherche	Keine sensiblen Daten eingeben, Antworten prüfen

🛡 5. Konkrete Maßnahmen & Verhaltensregeln

🔒 Datenschutz beachten:

- Keine sensiblen oder personenbezogenen Daten in KI-Systeme eingeben, es sei denn, sie sind ausdrücklich freigegeben – ansonsten sind Daten zu anonymisieren
- Bei Zweifeln Rücksprache mit dem Datenschutzbeauftragten halten

📄 Dokumentationspflicht:

- Alle KI-Systeme, die verwendet werden, müssen im KI-Verzeichnis des Büros (in Notion.so) aufgeführt sein
- Nutzung muss nachvollziehbar dokumentiert sein

🧠 Menschliche Kontrolle:

- KI darf nur **unter Aufsicht** eingesetzt werden – keine vollautomatischen Entscheidungen
- Der Mensch hat **immer das letzte Wort**

🗣️ Transparenz:

- Kunden und Mitarbeitende müssen wissen, wenn sie mit einem KI-System interagieren
- Hinweis z. B. „Diese Antwort wurde durch ein KI-System erstellt“ genügt

 Schulung & Awareness:

- Alle Mitarbeiter werden regelmäßig über den sicheren Einsatz von KI informiert
 - Bei Änderungen an Tools oder rechtlichen Rahmenbedingungen erfolgt ein Update (bitte notion.so beachten)
-

6. Was tun bei Unsicherheit?

- **Fragen Sie im Zweifel immer** bei der zuständigen Stelle (Datenschutzbeauftragte:r, IT, Führungskraft, AI Officer) nach
- **Melden Sie** auffälliges Verhalten von KI-Systemen sofort
- **Nutzen Sie keine privaten KI-Tools mit Daten der Sozietät** (z. B. ChatGPT, Grammarly etc.) ohne Prüfung durch die Geschäftsleitung