Muster-KI-Richtlinie für den Mittelstand

Eine Vorlage, mit der Du den Einsatz von KI in Deinem Unternehmen klar regelst: welche Tools erlaubt sind, welche Daten hinein dürfen und wer wofür zuständig ist.

Umfang	Anpassung	Stand
12 Abschnitte	Platzhalter ausfüllen	November 2026

So nutzt Du diese Vorlage

Schatten-KI entsteht dort, wo Mitarbeitende KI nutzen wollen, aber keine Regeln und kein freigegebenes Tool haben. Eine kurze, verständliche Richtlinie schafft Klarheit für alle und ist zugleich ein Baustein, um die Anforderungen aus DSGVO und EU AI Act nachweisbar zu erfüllen.

1. **Platzhalter ausfüllen.** Alle grün markierten Stellen wie `[Unternehmen]` oder `[Tool]` ersetzt Du durch Eure Angaben.
2. **Kürzen und anpassen.** Streich, was für Dein Unternehmen nicht passt. Ergänze Beispiele aus Euren Abteilungen, das macht die Regeln greifbar.
3. **Abstimmen.** Geh den Entwurf mit Deiner oder Deinem Datenschutzbeauftragten und, falls vorhanden, dem Betriebsrat durch.
4. **Veröffentlichen und schulen.** Mach die Richtlinie für alle zugänglich und erkläre sie in einer kurzen Schulung. Die Schulung dokumentierst Du als Nachweis nach Art. 4 AI Act.
5. **Regelmäßig prüfen.** KI entwickelt sich schnell. Plane mindestens eine jährliche Überprüfung ein.

> Diese Vorlage ist ein Muster und ersetzt keine Rechtsberatung. Sie muss an Dein Unternehmen, Eure Tools und bestehende Regelungen wie IT-Richtlinie, Datenschutzrichtlinie und Betriebsvereinbarungen angepasst werden.

Tipp: Erst das Tool, dann die Regel

Eine Richtlinie wirkt nur, wenn es eine freigegebene KI-Lösung gibt, die im Alltag überzeugt. Sonst bleibt die private Nutzung attraktiver als jede Regel. Leg deshalb in Abschnitt 3 mindestens ein Tool fest, das alle nutzen dürfen.

Vorlage

Richtlinie zum Einsatz von KI bei [Unternehmen]

Version [1.0] · gültig ab [Datum] · verantwortlich: [Funktion, z. B. Geschäftsführung]

1 Zweck und Geltungsbereich

KI-Anwendungen können unsere Arbeit erleichtern und beschleunigen. Diese Richtlinie legt fest, wie wir KI sicher, rechtskonform und verantwortungsvoll einsetzen. Sie schützt die Daten unserer Kund:innen, Geschäftspartner und Mitarbeitenden sowie unsere Geschäftsgeheimnisse.

Die Richtlinie gilt für alle Mitarbeitenden, Auszubildenden, Praktikant:innen und externen Personen, die für [Unternehmen] tätig sind, und für jede dienstliche Nutzung von KI, unabhängig vom Gerät.

2 Begriffe

- **KI-Anwendung:** Software, die mithilfe von KI Texte, Bilder, Code, Audio oder Analysen erzeugt, zum Beispiel Chat-Assistenten, Übersetzungs- und Transkriptionsdienste oder KI-Funktionen in bestehender Software.
- **Freigegebene KI-Anwendung:** eine KI-Anwendung, die in Abschnitt 3 aufgeführt ist und für die ein Auftragsverarbeitungsvertrag besteht.
- **Prompt:** jede Eingabe in eine KI-Anwendung, einschließlich hochgeladener Dateien.

3 Freigegebene KI-Anwendungen

Dienstlich dürfen ausschließlich die folgenden KI-Anwendungen genutzt werden. Die Nutzung erfolgt nur mit dem dienstlichen Account.

KI-Anwendung	Zugelassen für	Höchste Datenklasse	Zugang über
[Tool 1]	[alle Mitarbeitenden]	[vertraulich]	[Firmen-Login]
[Tool 2]	[Abteilung]	[intern]	[Firmen-Login]
[Tool 3]			

Private Accounts und nicht freigegebene KI-Anwendungen dürfen für dienstliche Inhalte nicht genutzt werden. Wer eine weitere Anwendung nutzen möchte, beantragt die Freigabe bei [Ansprechperson / IT].

4 Datenklassen

Welche Inhalte in eine KI-Anwendung eingegeben werden dürfen, richtet sich nach der Datenklasse.

Datenklasse	Beispiele	Freigegebene KI
Öffentlich	Website-Texte, veröffentlichte Pressemitteilungen, Produktbroschüren	✓ erlaubt
Intern	Interne Abläufe, Protokolle ohne Personenbezug, Entwürfe von Präsentationen	✓ erlaubt
Vertraulich	Angebote, Kundenkorrespondenz, Verträge, personenbezogene Daten von Kund:innen	[nur in Tool X]
Streng vertraulich	Personalakten, Gesundheitsdaten, Zugangsdaten, nicht veröffentlichte Finanzzahlen, Konstruktionsdaten	✗ nicht erlaubt [ggf. Ausnahme]

Im Zweifel gilt die höhere Datenklasse. Personenbezogene Daten werden nur eingegeben, wenn sie für die Aufgabe erforderlich sind. Wo möglich, werden Namen und Kennungen vorher entfernt.

5 Grundregeln der Nutzung

1. KI-Anwendungen unterstützen die Arbeit, sie ersetzen nicht die eigene fachliche Verantwortung.
2. Passwörter, Zugangsdaten und Sicherheitsinformationen werden niemals in eine KI-Anwendung eingegeben.
3. Inhalte Dritter, etwa Dokumente von Kund:innen, werden nur verarbeitet, wenn dies vertraglich zulässig ist.
4. Einstellungen, die den Datenschutz betreffen, zum Beispiel zum Teilen von Chats, werden nicht eigenmächtig geändert.
5. Browser-Erweiterungen und Apps mit KI-Funktionen werden nur installiert, wenn sie freigegeben sind.

6 Prüfpflicht und Kennzeichnung

KI-Anwendungen können fehlerhafte oder erfundene Inhalte erzeugen. Deshalb gilt:

- Jedes KI-Ergebnis wird vor der Weitergabe an Dritte auf Richtigkeit, Vollständigkeit und Angemessenheit geprüft.
- Zahlen, Zitate, Rechtsauskünfte und Quellen werden immer gegengeprüft.
- Veröffentlichte Inhalte, die wesentlich mit KI erstellt wurden, werden gekennzeichnet, soweit dies gesetzlich vorgeschrieben ist oder [Unternehmen] es festlegt.
- Kommunizieren Kund:innen direkt mit einem KI-System, etwa einem Chatbot, werden sie darauf hingewiesen.

7 Nicht zulässige Anwendungen

Ohne vorherige Prüfung durch Datenschutz und Geschäftsführung ist es nicht zulässig, KI-Anwendungen einzusetzen für:

- Entscheidungen über Einstellung, Beförderung, Bewertung oder Kündigung von Mitarbeitenden,
- die Überwachung von Verhalten oder Leistung von Mitarbeitenden,
- automatisierte Entscheidungen mit rechtlicher Wirkung für Kund:innen,
- die Verarbeitung besonderer Kategorien personenbezogener Daten nach Art. 9 DSGVO, etwa Gesundheitsdaten.

Solche Anwendungen können als Hochrisiko-KI im Sinne des EU AI Act gelten und unterliegen besonderen Pflichten.

8 Zuständigkeiten

Rolle	Aufgabe	Person
Geschäftsführung	Gesamtverantwortung, Freigabe dieser Richtlinie	[Name]
IT-Leitung	Freigabe und Verwaltung von KI-Anwendungen, Rechte und Rollen	[Name]
Datenschutzbeauftragte:r	Datenschutzrechtliche Prüfung, AVV, Datenschutz-Folgenabschätzung	[Name]
KI-Ansprechperson	Erste Anlaufstelle für Fragen, sammelt neue Anwendungsfälle	[Name]

9 Schulung und KI-Kompetenz

Alle Personen, die KI-Anwendungen nutzen, erhalten vor der ersten Nutzung eine Einweisung zu Funktionsweise, Grenzen und Risiken sowie zu dieser Richtlinie. Die Schulung wird auf die jeweilige Rolle zugeschnitten, regelmäßig aufgefrischt und dokumentiert. Damit kommt [Unternehmen] der Pflicht aus Art. 4 der KI-Verordnung (EU) 2024/1689 nach.

10 Datenschutz, Protokollierung und Mitbestimmung

Für jede freigegebene KI-Anwendung besteht ein Auftragsverarbeitungsvertrag nach Art. 28 DSGVO. Eingaben werden nicht zum Training der KI-Modelle des Anbieters verwendet.

Administrative Vorgänge werden protokolliert. Eine Auswertung der Nutzung erfolgt nur in zusammengefasster Form, etwa als Anzahl aktiver Nutzer:innen. Eine Kontrolle einzelner Chatinhalte findet nicht statt [ggf. Ausnahmen gemäß Betriebsvereinbarung]. Die Rechte des Betriebsrats bleiben unberührt.

11 Vorfälle und Verstöße

Wer bemerkt, dass vertrauliche oder personenbezogene Daten in eine nicht freigegebene KI-Anwendung gelangt sind, meldet dies unverzüglich an [IT / Datenschutz, Kontakt]. Eine schnelle

Meldung ist wichtiger als die Frage nach dem Verschulden, denn Datenschutzverletzungen müssen unter Umständen innerhalb von 72 Stunden an die Aufsichtsbehörde gemeldet werden.

Verstöße gegen diese Richtlinie können arbeitsrechtliche Folgen haben.

12 Inkrafttreten und Überprüfung

Diese Richtlinie tritt am [Datum] in Kraft. Sie wird mindestens einmal jährlich sowie bei wesentlichen rechtlichen oder technischen Änderungen überprüft.

Ort, Datum	Geschäftsführung

snutig.ai

Das freigegebene Tool für Abschnitt 3

Eine Richtlinie braucht eine KI-Lösung, die alle nutzen dürfen. snutig.ai ist eine DSGVO-konforme KI-Plattform für Unternehmen:

- KI-Modelle in EU-Rechenzentren, kein Training mit Deinen Daten, AVV nach Art. 28 DSGVO
- Rollen und Rechte, Microsoft-365-Anbindung mit erhaltenen Berechtigungen, Admins lesen keine Chats mit
- Office-Dateien aus eigenen Vorlagen, Wissenssammlungen mit Quellenangabe, eigene Agenten

Demo vereinbaren: snutig.de/leistungen/snutig-ai

Diese Vorlage ist ein Muster und ersetzt keine Rechtsberatung. Microsoft 365 ist eine Marke der Microsoft Corporation. snutig GmbH, Herford.