

KI-GOVERNANCE FÜR KMU

Wildwest im Büro stoppen

Abhängigkeiten vermeiden: KI im Unternehmen sicher organisieren

Keine Rechtsberatung!

16.09.2026

Peter Moser · unabhängiger Qualitätslotse



PETER MOSER – QUALITÄTSLOTSE

- ▶ **30+** Jahre Projekterfahrung
in kritischen IT Umstellungen & Go-Lives
- ▶ Befähigt Teams, digitale Prozesse nachhaltig zu tragen
- ▶ Risikoreduzierung ohne Innovationsbremse



Die 3 Datenschutz-Fallen

FALLE 1

Der US-Cloud-Act-Irrtum

„Serverstandort Deutschland“ schützt bei US-Anbietern nicht vor dem Zugriff US-amerikanischer Behörden.

FALLE 2

Das unbemerkte Daten-Leck

Kundendaten und Quellcode fließen ungewollt in öffentliche Trainingsdaten der KI-Anbieter.

FALLE 3

Die Schatten-IT

Aus Angst vor Verboten nutzen Mitarbeiter private Accounts für Firmengeheimnisse.



Haftungs-Check: Bei gravierenden Verstößen gegen DSGVO oder EU AI Act haftet die Geschäftsführung im Zweifel persönlich.

*Ein „Ich wusste von nichts“ schützt im digitalen Wildwesten nicht. Die Geschäftsführung trägt die Organisationsverantwortung, aber **jeder Mitarbeitende braucht einfache Regeln**, damit er im Alltag nicht raten muss.*



Wo stehen Sie mit KI in Ihrem Unternehmen?

OPTION A

Wildwest

Jeder nutzt, was er will. Keine Regeln, kein Überblick.

OPTION B

Verbot

KI ist untersagt. Innovation blockiert, Schatten-IT wächst.

OPTION C

Geregelt

Klare Leitplanken. KI produktiv und sicher im Einsatz.

Bitte schreiben Sie Ihre Antwort in den Chat.



Die vier Regelwerke im Überblick



DSGVO

Schutz personenbezogener Daten: Grundlage für jeden KI-Einsatz mit Personendaten.



EU AI Act

Risikobasierte KI-Regulierung mit Pflichten je nach Anwendungsfall.



Urheberrecht

Schutz und Nutzung von KI-Output: Wem gehört das Ergebnis?



ISO/IEC 42001

Managementsystem für KI: Relevant, wenn KI-Nutzung systematisch gemanagt oder auditiert werden soll.
Heute nicht im Fokus.

Keine Rechtsberatung!

Kurzer Überblick

Bitte selbständig vertiefen



Was sind personenbezogene Daten?

DEFINITION (ART. 4 DSGVO)

Alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen.

Auch mittelbar identifizierbar: eine Kombination von Daten, eine einzigartige Eigenschaft (Hausnummer 1503) oder ein seltener Beruf („Bundeskanzler“) kann eine Person identifizieren.

BEISPIELE

- ▶ Klardaten: Name, Adresse, E-Mail, Telefonnummer
- ▶ Online-Kennungen: IP-Adresse, Cookie-ID, Geräte-ID
- ▶ Kunden-/Mitarbeiternummer, Ausweisnummer, Kfz-Kennzeichen
- ▶ IBAN, Standort-, Zahlungs-, Nutzungs- und Log-Daten
- ▶ Foto, Audio- und Video-Aufnahme

BESONDERE KATEGORIEN (ART. 9 DSGVO)

Ethnische Herkunft

Politische Meinung

Religion

Gewerkschaft

Genetische & biometrische Daten

Gesundheitsdaten

Sexualleben/-orientierung



Wichtigste Grundsätze der DSGVO

1 Rechtmäßigkeit & Transparenz

Keine unberechtigte oder intransparente Verarbeitung.

2 Zweckbindung

Nur für festgelegte, legitime Zwecke: keine spätere Änderung.

3 Datenminimierung

Nur so viele Daten wie nötig: kein Sammeln auf Vorrat.

4 Speicherbegrenzung

Nur so lange speichern, wie für den Zweck erforderlich.

5 Integrität & Vertraulichkeit

Schutz vor unbefugter Verarbeitung, Verlust und Zerstörung.

6 Rechenschaftspflicht

Einhaltung nachweisen: technisch und organisatorisch.

7 Privacy by Design

Datenschutz von Anfang an in der Entwicklung mitdenken.

8 Privacy by Default

Datenschutzfreundliche Voreinstellungen ab Werk.



Was muss KMU beim AI Act beachten?

01.08.2024

In Kraft getreten

EU AI Act tritt in Kraft.

02.02.2025

Verbote & KI Kompetenz

Verbotene KI-Praktiken sind untersagt.
Unternehmen müssen **KI-Kompetenz** bei Nutzenden sicherstellen.

02.08.2025

GPAI-Pflichten

Für KMU indirekt nützlich:
mehr Transparenz zu Modellen, Trainingsdaten, Copyright und Risiken.

02.08.2026

Generelle Anwendbarkeit

Hochrisiko-Pflichten + **Kennzeichnungspflicht** (Art. 50).

02.08.2027

Volle Wirkung

Alle Risikokategorien inkl. Annex I.

Ausnahme: u.a. redaktionell geprüfte Texte mit menschlicher Verantwortung.
Die Icons sind frei nutzbar, ersetzen aber die Kennzeichnung nicht.



Basissymbol

Grundkennzeichnung für KI.

AI GENERATED

Vollständig KI-erzeugt

Inhalt komplett von KI erstellt.

AI MODIFIED

KI-verändert

Inhalt von KI bearbeitet/verändert.



Nicht jede KI Nutzung ist gleich kritisch

MINIMAL / GERING

Normale Bürohilfe, meist keine besonderen AI-Act-Pflichten

- Textentwurf
- Ideen
- Zusammenfassung

→ meist unkritisch, wenn die Daten passen

TRANSPARENZPFLICHT

Menschen müssen erkennen, dass KI im Spiel ist

- Chatbot
- KI-generierte Inhalte

→ kenntlich machen und informieren

HOCHRISIKO

Strenge Anforderungen, wenn KI über Menschen, Sicherheit oder Grundrechte mitentscheidet

- Bewerberauswahl
- Leistungsbewertung
- Sicherheit

→ vorher prüfen, dokumentieren, Aufsicht festlegen

VERBOTEN

Darf nicht eingesetzt werden

- Emotionserkennung
- Manipulation
- Scoring
- Biometrie & sensible Eigenschaften

→ nicht einsetzen



Verbotene KI-Praktiken

‣ **Emotionserkennung am Arbeitsplatz**

Tool bewertet Stimmung, Stress, Motivation oder Aufmerksamkeit aus Gesicht, Stimme oder Webcam.

‣ **Manipulative Systeme**

KI drängt Menschen gezielt zu Entscheidungen, die ihnen erheblich schaden können.

‣ **Social Scoring / Mitarbeiter-Scoring**

KI bildet Zuverlässigkeits- oder Verhaltensscores aus E-Mails, Krankheitstagen, Chat-Aktivität, Pünktlichkeit oder ähnlichen Daten.

‣ **Biometrische Ableitung sensibler Eigenschaften**

KI leitet aus Gesicht, Stimme oder Körpermerkmalen politische Meinung, Religion, Gesundheit, sexuelle Orientierung o.ä. ab.

MERKSATZ

Wenn KI Menschen bewertet, beeinflusst oder überwacht: STOPP.

Erst rechtlich und organisatorisch prüfen.



Urheberrecht bei KI-Output

✓ Das ist geklärt

- ✓ Urheberrecht schützt nur menschliche Schöpfung (§ 2 Abs. 2, § 7 UrhG).
- ✓ Reines Prompting reicht nicht für einen eigenen Schutz.
- ✓ Die Nutzung von KI-Output ist grundsätzlich erlaubt, auch kommerziell.

! Zwei Restrisiken

Kein eigener Schutz

Wettbewerber dürfen das Ergebnis übernehmen.

Trainingsdaten-Risiko

Der Output kann bestehende Werke Dritter verletzen.

MERKSATZ

Nicht jeder KI-Text ist ein Rechtsproblem.

Aber je externer und verbindlicher die Nutzung, desto wichtiger ist eine Freigabe.



Ihre KI-Spielregeln: Was konkret zu regeln ist

DSGVO

- ✓ Datenkategorien (inkl. besonderer Kategorien nach Art. 9) festlegen
- ✓ Personenbezogene Daten nur freigeben nutzen
- ✓ Daten minimieren: nur das Nötigste

EU AI Act

- ✓ KI-Kompetenz sicherstellen
- ✓ Risikoklasse je Anwendungsfall prüfen
- ✓ Kennzeichnung und Tabus beachten

Urheberrecht

- ✓ KI-Output ist i. d. R. nicht eigen geschützt
- ✓ Trainingsdaten-Risiko bei Kundenprojekten prüfen
- ✓ Verwendungszweck vorab klären

Tool-Auswahl

- ✓ Auftragsverarbeitungsvertrag (AVV/DPA) und Datenschutz prüfen
- ✓ Datenflüsse, Hosting und Training klären
- ✓ Freigabeliste erlaubter Tools pflegen

Das 3-Fragen-Praxistool



1

Die Daten-Frage

Darf das überhaupt hinein?

Personenbezogene Daten oder
Firmengeheimnisse?

2

Die Qualitäts-Frage

Wer haftet für das Ergebnis?

Der Mensch prüft und verantwortet die
Richtigkeit.

3

Die Urheberrechts-Frage

Darf ich das Ergebnis so nutzen?

Intern okay, extern gelten Freigaben.



Die Daten-Frage

GRÜN: das darf hinein

- ✓ Eigene, allgemein formulierte Ideen
- ✓ Öffentliche Texte und Informationen
- ✓ Fiktive Beispiele und Testdaten

ROT: das bleibt draußen

- ✗ Personenbezogene Daten
- ✗ Firmengeheimnisse und interne Zahlen
- ✗ Nicht freigegebene Kundendaten

Die Regel: Bei **ROT** nichts eingeben, außer über eine freigegebene, datenschutzkonforme Firmen-Schnittstelle (z.B. KI Tool mit Anonymisierung).



Die Qualitäts-Frage

KI

Die KI ist der Assistent

Liefert schnell Entwürfe und Vorschläge,
ohne Verantwortung für die Richtigkeit.



✓ MENSCH

Der Mitarbeiter ist der Chefredakteur

Übernimmt die **volle** Verantwortung:
prüfen, korrigieren, freigeben.

MERKSATZ

Wenn das Ergebnis zählt:
Schreiben Sie Ihr Vorgehen und Spielregeln auf und sorgen Sie dafür, dass die KI sich daran hält.



Die Urheberrechts-Frage

Grundsatz: KI-generierte Werke sind in der Regel nicht urheberrechtlich geschützt.

Interne Nutzung: unkritisch

- ✓ Notizen und Zusammenfassungen
- ✓ Entwürfe und Textideen
- ✓ Recherche und Ideenfindung
- ✓ Interne Vorlagen und Bausteine

Kundenprojekte & Marke: Vorsicht

- Gesonderte interne Freigaben nötig
- EU-Kennzeichnungspflicht gilt **seit 02.08.2026**

Die drei offiziellen Kennzeichen:

AI

AI GENERATED

AI MODIFIED



Die Vorarbeit: Bewertung pro Anwendungsfall

Zur Daten-Frage

Datenkategorien festlegen:

öffentlich

intern

personenbezogen

Geschäftsgeheimnis

Freigabeliste an Tools mit AVV oder EU-Hosting. Relevante Daten kategorisieren und als Regeln definieren (Leitplanken).

Zur Qualitäts-Frage

Prüftiefe je Anwendungsfall:

interne Notiz

Kundenangebot

Produktivcode

Je höher die Wirkung, desto gründlicher die Prüfung. Relevant für u.a. Inhalt, Tonalität und Verbindlichkeit.

Zur Urheberrechts-Frage

Verwendungszweck kategorisieren:

rein intern

extern-informell

kommerziell-extern

Mit passender Kennzeichnungs- und Freigaberegeln.

MERKSATZ

Schreiben Sie Ihr Vorgehen und Spielregeln auf und sorgen Sie dafür, dass die KI sich daran hält und Ihre Mitarbeiter dies als gemeinsame Grundlage nutzen („Betriebliches QMS“ / Betriebsprozesse).



Antwortentwurf für eine Kundenanfrage formulieren

3 FRAGEN KONKRET

Daten:

Enthält die Anfrage personenbezogene Daten, Preise, Vertragsdetails oder Interna?

Qualität:

Kann die Antwort Zusagen, Fristen, Preise oder Rechtsfolgen auslösen?

Urheberrecht:

Wird der Text extern an Kunden verschickt?

BEWERTUNG

JA

JA

JA

LÖSUNG FÜR ANWENDUNGSFALL

Alle relevanten Daten gemäß **[LEITPLANKE: DATENKATALOG]** anonymisieren oder **[LEITPLANKE: FREIGEgebenES TOOL]** nutzen.

Prüfe Inhalt, Tonalität und Verbindlichkeit; **Anpassungen durchführen.**

Kennzeichnung und Urheberrechtsschutz ok? **[LEITPLANKE :INHALTLICH FREIGEBEN]**

→ Nutzung von Leitplanken

→ HI-Ansatz

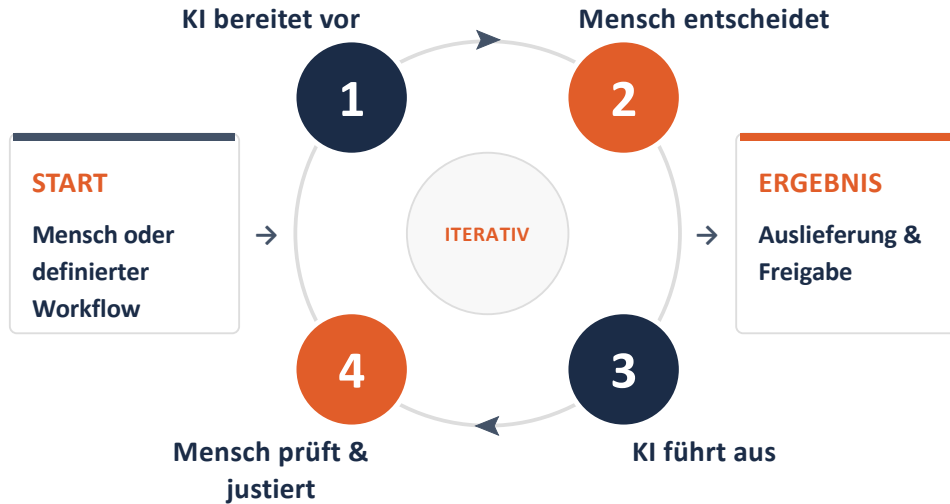
→ Klarheit über Freigaben

MERKSATZ

Der Mensch ist für das Ergebnis verantwortlich. Leitplanken erleichtern die Arbeit.



Human Intelligence - der Mensch entscheidet.



Iterativ im Kreislauf, bis das Ergebnis passt, dann Auslieferung



Nicht alles selbst bauen, aber bewusst entscheiden

1 - DATEN IM HAUS BEHALTEN

Vertrauliche Daten nur in freigegebenen Tools nutzen.

Wo möglich: anonymisieren, pseudonymisieren oder lokal verarbeiten.

2 - NUR RAUSGEBEN, WAS NÖTIG IST

Prompts schlank halten.

Keine kompletten Kundendossiers, Verträge, Quellcodes oder internen Zahlen eingeben, wenn ein Ausschnitt reicht.

3 - UNABHÄNGIG BLEIBEN

Keine Arbeitsabläufe bauen, die nur mit einem Anbieter funktionieren.

Wissen, Prompts, Vorlagen und Entscheidungen im Unternehmen dokumentieren.

MERKSATZ

Souverän ist, wer KI nutzt, ohne Kontrolle über Daten, Wissen und Prozesse abzugeben.



So wird aus Wildwest eine gemeinsame KI-Spielregel

1 - KLARHEIT SCHAFFEN

- ▷ Wo nutzt das Team heute KI?
- ▷ Welche Daten, Tools und Risiken gibt es?
- ▷ Was ist erlaubt, was braucht Freigabe?

2 - REGELN MIT DEM TEAM ENTWICKELN

- ▷ 3-Fragen-Tool auf eigene Fälle anwenden
- ▷ Tool-Freigabeliste und Datenkategorien festlegen
- ▷ Rollen, Prüfung und Eskalationswege klären

3 - IM ALLTAG VERANKERN

- ▷ Pilot-Anwendungsfälle testen
- ▷ Mitarbeitende befähigen
- ▷ KI-Spielregeln dokumentieren und nachschärfen

ECKDATEN DER FÖRDERUNG

80% Zuschuss zu den Beratungskosten

**Start über kostenlose INQA-Erstberatung /
Beratungsscheck**

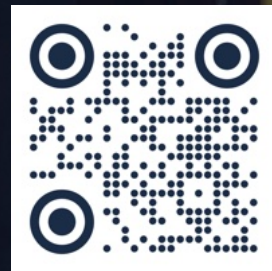
- ▷ Für KMU mit 2-250 Beschäftigten
- ▷ Betrieb besteht seit mind. 2 Jahren
- ▷ Bis zu 12 Beratungstage
- ▷ Abschluss innerhalb von 7 Monaten

Moderation statt fertiger Schubladenlösung.

Im Coaching entstehen die passenden KI-Spielregeln
gemeinsam mit Geschäftsführung und Mitarbeitenden.

DANKESCHÖN

PETERMOSER.DE



PETER MOSER
IT QUALITY CONSULTING