PRAXISLEITFADEN

Sicher mit KI in Deutschland und der EU

DSGVO • EU AI Act • Urheberrecht • Persönlichkeitsrechte

Was Nutzende heute wissen und praktisch anwenden sollten.

STAND 16. AUGUST 2026

Orientierung, keine Rechtsberatung



Vier Regelwerke – vier Fragen

Sichere KI-Nutzung entsteht nicht durch ein einzelnes Gütesiegel, sondern durch mehrere Prüfungen.

DATEN

DSGVO

Welche personenbezogenen Daten verarbeite ich – und wofür?

RISIKO

EU AI Act

Welche Risiken, Transparenz- und Kompetenzpflichten gelten für diesen Einsatz?

WERKE

Urheberrecht

Darf ich Eingaben, Vorlagen und Ergebnisse so nutzen und veröffentlichen?

PERSONEN

Persönlichkeitsrecht

Wer ist abgebildet, hörbar oder erkennbar – und liegt die nötige Einwilligung vor?

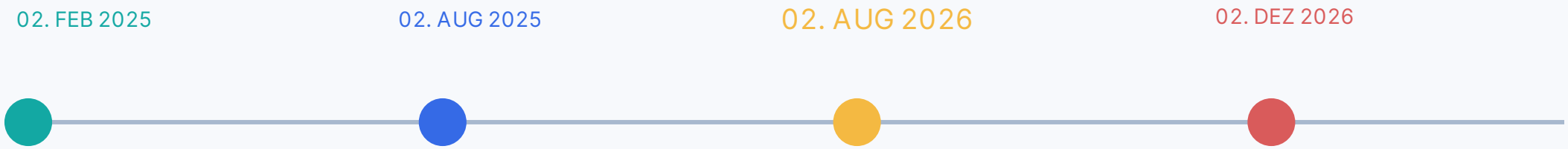
Merksatz

Nicht der Anbietername entscheidet allein sondern Zweck, Daten, Inhalt, Konfiguration und menschliche Prüfung.

Quellen: DSGVO; Verordnung (EU) 2024/1689 (EU AI Act); UrhG §§ 44b, 60d.

Was gilt heute?

Die Regeln gelten nicht alle am selben Tag. Für die Praxis zählt das konkrete Datum.



KI-Kompetenz & Verbote

AI-Literacy-Pflichten und Verbote bestimmter Praktiken gelten.

GPAI-Regeln*

Bestimmte Pflichten für Anbieter allgemeiner KI-Modelle gelten.

*General Purpose AI (alle grossen Anbieter)

AI Act weitgehend anwendbar

Transparenzpflichten nach Art. 50 gelten für die erfassten Fälle.

Übergangsfrist endet

Für bestimmte vor dem 02.08.2026 in Verkehr gebrachte Systeme endet die Frist zur Kennzeichnung.

Wichtig: Die Übergangsfrist betrifft nicht pauschal alle Inhalte und nicht jede Kennzeichnungspflicht. Prüfen Sie den konkreten Anwendungsfall.

Quelle: Europäische Kommission, „Transparency obligations under Article 50 of the AI Act“; EUR-Lex, konsolidierter AI Act, Stand 27.07.2026.

Vor der Eingabe: Daten prüfen

Die DSGVO fragt nicht: „Ist das ein Chatbot?“ – sondern: Welche personenbezogenen Daten werden zu welchem Zweck verarbeitet?

GRÜN • unkritisch

Erfundene Beispiele, eigene neutrale Texte, öffentlich bekannte Angaben.

GELB • anonymisieren

Namen, Kontaktdaten, Kundennummern und Fallangaben nur, wenn wirklich nötig – besser ersetzen.

ROT • nicht eingeben

Gesundheitsdaten, Passwörter, Personalakten, vertrauliche Geschäfts- und Kundendaten.

Die fünf Arbeitsregeln

Zweck	Warum braucht die KI diese Information?
Minimierung	Nur das Nötige eingeben.
Transparenz	Betroffene müssen informiert werden können.
Sicherheit	Konto, Anbieter und Zugriffsrechte prüfen.
Verantwortung	Ergebnis und Folgen menschlich kontrollieren.

Wenn anonymisierte Angaben reichen: Verwenden Sie sie.

Quelle: Datenschutzkonferenz (DSK), Orientierungshilfe „Künstliche Intelligenz und Datenschutz“; Art. 5 DSGVO.

Risiko statt Bauchgefühl

Nicht jede KI-Anwendung wird gleich behandelt. Entscheidend sind System, Zweck und mögliche Auswirkungen.

Unzulässig	Bestimmte manipulative, ausbeuterische oder sozial bewertende Praktiken sind verboten.
Hohes Risiko	Strenge Anforderungen – zum Beispiel in bestimmten Bereichen mit Auswirkungen auf Menschen.
Transparenzrisiko	Menschen müssen erkennen können, wenn sie mit KI interagieren oder bestimmte KI-Inhalte sehen.
Geringes / kein besonderes Risiko	Alltägliche Assistenzaufgaben – trotzdem Ergebnisse prüfen und Datenschutz beachten.

Für Nutzende heißt das:

- KI-Kompetenz aufbauen
- Einsatz und Risiko einordnen
- Transparenzpflichten beachten
- Menschliche Kontrolle sichern

Ein Chatbot ist nicht automatisch ein Hochrisikosystem – der konkrete Einsatz entscheidet.

Quelle: Verordnung (EU) 2024/1689 (EU AI Act), risikobasierter Ansatz und Verbote.

Kennzeichnung: nicht pauschal, sondern fallbezogen

Art. 50 AI Act verlangt Transparenz in bestimmten Situationen – nicht automatisch ein Etikett für jeden KI-unterstützten Text.

INTERAKTION

Mensch ↔ KI

Menschen sollen erkennen können, wenn sie mit einem KI-System interagieren – sofern dies nicht ohnehin offensichtlich ist.

BILD • TON • VIDEO

Synthetische Medien

Bestimmte KI-generierte oder manipulierte Bilder, Videos und Audios benötigen technische bzw. erkennbare Kennzeichnungen.

TEXT

Texte von öffentlichem Interesse

Bei bestimmten KI-generierten Texten gelten Transparenzregeln; menschliche Kontrolle und redaktionelle Verantwortung sind relevant.

Vor der Veröffentlichung fragen:

- Was wurde durch KI erzeugt oder verändert?
- Gilt eine konkrete Transparenzpflicht?
- Ist die Kennzeichnung sichtbar oder maschinenlesbar nötig?
- Hat ein Mensch Inhalt und Wirkung geprüft?

Zeitpunkt: Art. 50 gilt ab 02.08.2026. Für bestimmte ältere Systeme läuft eine begrenzte Übergangsfrist bis 02.12.2026.

Quelle: Europäische Kommission, FAQ und Leitlinien zu Art. 50 AI Act; Code of Practice zur Transparenz KI-generierter Inhalte.

Urheberrecht & Persönlichkeitsrechte

Zwei typische Fehler: fremde Werke bedenkenlos eingeben – und reale Personen ohne Zustimmung nachahmen.

WERKE & INHALTE

Urheberrecht

- Eigene oder rechtmäßig nutzbare Materialien verwenden
- Nutzungsbedingungen und Bearbeitungsrechte prüfen
- KI-Ausgabe auf Ähnlichkeit zu geschützten Werken prüfen
- Menschliche kreative Beiträge dokumentieren

§ 44b UrhG regelt Text & Data Mining unter Voraussetzungen – keine pauschale Erlaubnis, beliebige fremde Werke in jeden Dienst hochzuladen.

REALE PERSONEN

Persönlichkeitsrecht

- Keine Gesichter, Stimmen oder Avatare realer Personen ohne erforderliche Einwilligung nachahmen
- Bei Bildern, Audio und Video Identifizierbarkeit und Kontext prüfen
- Keine bloßstellenden oder irreführenden Darstellungen erzeugen
- Veröffentlichung und kommerzielle Nutzung gesondert prüfen

„Im Stil von …“ kann zusätzlich marken-, namens- oder persönlichkeitsrechtliche Fragen auslösen.

Faustregel: Nur Material verwenden, das Sie SELBST erstellt haben oder dessen Nutzung Sie nachweisbar erlauben dürfen.

Quellen: UrhG § 44b; UrhG-Systematik zum Schutz menschlicher Schöpfungen; allgemeine Persönlichkeitsrechte.

Vier Fälle – vier sichere nächste Schritte

Die beste Regel ist die, die sich im Alltag anwenden lässt.

Situation	Prüfrisiko	Sicherer nächster Schritt
Kundinnen-Mail überarbeiten	personenbezogene Daten	anonymisieren; nur nötigen Kontext nutzen; Ergebnis prüfen
Öffentlichen Text vereinfachen	meist unkritischer Inhalt	keine neuen Fakten erfinden; menschlich redigieren
Foto mit KI bearbeiten	Rechte & Einwilligung	eigenes Foto oder geklärte Rechte; Einwilligung bei Personen
KI-Text veröffentlichen	Transparenz & Richtigkeit	Quelle, Fakten, Zweck und Kennzeichnungspflicht prüfen

Sicherer Workflow: anonymisieren → formulieren → prüfen → erst dann weitergeben oder veröffentlichen.

Didaktische Beispiele; rechtliche Bewertung hängt vom konkreten Zweck, Inhalt und Einsatz ab.

Die 7-Schritte-Prüfung

Eine kurze Routine verhindert die häufigsten Fehler – vor der Eingabe und vor der Veröffentlichung.

1 Zweck klären

Was soll die KI leisten?

→

2 Daten reduzieren

Was muss wirklich hinein?

→

3 Werkzeug prüfen

Konto, Modell, Regeln, Region

→

4 Prompt formulieren

Ziel, Kontext, Format, Ton

5 Antwort prüfen

Fakten, Quellen, Lücken

→

6 Rechte prüfen

Werke, Personen, Einwilligung

→

7 Verantworten

Freigeben, kennzeichnen, dokumentieren

Für Entscheidungen mit erheblichen Folgen gilt: KI unterstützt – ein Mensch entscheidet und trägt die Verantwortung.

Praxisorientierte Zusammenfassung aus DSGVO-, AI-Act-, Urheber- und Persönlichkeitsrechtsprüfung.

DIE KURZVERSION

Präzise fragen.
Sensible Daten schützen.
Ergebnisse prüfen.

- Keine unnötigen personenbezogenen oder vertraulichen Daten eingeben.
- Konkreten Zweck und Risikostufe des KI-Einsatzes prüfen.
- KI-Inhalte, Quellen, Rechte und Kennzeichnung vor Nutzung prüfen.
- Menschliche Verantwortung bleibt – besonders bei wichtigen Entscheidungen.
- Regeln und Anbieterinformationen regelmäßig aktualisieren.

OFFIZIELLE QUELLEN

Europäische Kommission
AI Act: Transparenzpflichten nach Art. 50
digital-strategy.ec.europa.eu

EUR-Lex
Verordnung (EU) 2024/1689
eli.regulation.eu

Datenschutzkonferenz
Orientierungshilfe KI & Datenschutz
datenschutzkonferenz-online.de

Bundesministerium der Justiz
UrhG § 44b Text & Data Mining
gesetze-im-internet.de

So kennzeichne ich:



