

# EU AI Act — Einordnung der KI-Nutzung über AISecurityGateway

**MUSTER — kein Rechtsrat.** Vor Verwendung durch DSB/Fachanwalt prüfen lassen.  
Betreiber: [Firma] · Stand: [Datum] · Version: 1.0

Die **KI-Verordnung (VO (EU) 2024/1689, „EU AI Act“)** ist seit 2024 in Kraft und gilt gestaffelt. Sie ergänzt die DSGVO um **produkt- und nutzungsbezogene** Pflichten. Dieses Dokument ordnet ein, welche Rolle der Betreiber einnimmt und welche Pflichten daraus folgen.

## 1. Welche Rolle hat der Betreiber?

| Rolle (Art. 3)                                        | Trifft zu?      | Bedeutung                                                                          |
|-------------------------------------------------------|-----------------|------------------------------------------------------------------------------------|
| <b>Anbieter</b> (entwickelt/vermarktet ein KI-System) | [i. d. R. nein] | Wer ein KI-System selbst entwickelt oder unter eigenem Namen in Verkehr bringt     |
| <b>Betreiber/Deployer</b> (nutzt ein KI-System)       | [i. d. R. ja]   | Wer ein fremdes KI-System (z. B. OpenAI/Anthropic) im beruflichen Kontext einsetzt |

**Regelfall:** Bei bloßer Nutzung fremder LLM-APIs über das Gateway ist [Firma] **Betreiber/Deployer**, nicht Anbieter. Die Kernpflichten der Anbieter (technische Doku, Konformitätsbewertung) treffen die KI-Anbieter, nicht [Firma].

**Achtung Rollenwechsel:** Wer ein KI-System wesentlich verändert, unter eigenem Namen anbietet oder ein Hochrisiko-System zweckentfremdet, kann selbst zum **Anbieter** werden (Art. 25). Bei reiner Nutzung als Arbeitswerkzeug nicht der Fall.

## 2. Risikoklasse der Nutzung

| Klasse                                          | Beispiele                                                         | Einordnung [Firma]                         |
|-------------------------------------------------|-------------------------------------------------------------------|--------------------------------------------|
| <b>Verboten</b> (Art. 5)                        | Social Scoring, biometr. Massenüberwachung, manipulatives KI      | [nicht einschlägig]                        |
| <b>Hochrisiko</b> (Anhang III)                  | KI in Personalauswahl, Bonität, kritischer Infrastruktur, Bildung | [prüfen — nur falls KI so eingesetzt wird] |
| <b>Begrenztes Risiko</b> (Transparenz, Art. 50) | Chatbots, KI-generierte Texte/Bilder/Audio                        | [i. d. R. ja]                              |
| <b>Minimales Risiko</b>                         | Rechtschreibhilfe, Spam-Filter                                    | [ggf.]                                     |

**Regelfall** für allgemeine Text-/Chat-/Inhaltsunterstützung: **begrenztes Risiko**  
→ es greifen v. a. **Transparenzpflichten** (Abschnitt 3), keine Hochrisiko-Pflichten.

**Hochrisiko-Trigger prüfen:** Wird KI für **Bewerber-/Personalentscheidungen**, **Kreditwürdigkeit**, **Zugang zu Bildung/Leistungen** o. Ä. genutzt, kann die Verarbeitung Hochrisiko sein → zusätzliche Pflichten (u. a. Grundrechte-Folgenabschätzung Art. 27, menschliche Aufsicht, Protokollierung). Dann gesondert bewerten.

## 3. Transparenzpflichten (Art. 50) — praktische Umsetzung

Diese treffen den Betreiber direkt bei begrenztem Risiko:

| Situation                                                                                    | Pflicht                            | Umsetzung bei [Firma]                |
|----------------------------------------------------------------------------------------------|------------------------------------|--------------------------------------|
| Direkter Kontakt Mensch ↔ KI (Chatbot)                                                       | Offenlegen, dass es KI ist         | [Hinweis im Chat-UI / bei Support]   |
| KI-generierte/-bearbeitete <b>Texte</b> zur öffentl. Information Als KI-erzeugt kennzeichnen |                                    | [Redaktions-/Kennzeichnungsregel]    |
| KI-generierte <b>Bilder/Audio/Video</b> (auch „Deepfakes“)                                   | Als künstlich erzeugt kennzeichnen | [Kennzeichnung bei Veröffentlichung] |

Verweis in der öffentlichen Datenschutz-/Nutzungsinfo: siehe 12-Datenschutzerklärung-Baustein.md (Abschnitt „Kennzeichnung KI-generierter Inhalte“).

## 4. KI-Kompetenz / AI Literacy (Art. 4) — gilt bereits

Seit **Februar 2025** verpflichtet Art. 4 Anbieter und **Betreiber**, für ein **ausreichendes KI-Kompetenzniveau** ihres mit KI befassten Personals zu sorgen.

- [ ] KI-Schulung/Awareness für betroffene Beschäftigte durchgeführt
- [ ] Nachweis geführt (siehe 11-Schulungsnachweis.md)
- [ ] KI-Nutzungsrichtlinie kommuniziert (siehe 01-KI-Nutzungsrichtlinie.md)

Diese vorhandenen Vorlagen decken den Nachweis nach Art. 4 mit ab.

## 5. Wie das Gateway hier unterstützt (kein Ersatz)

- Datenminimierung/Grundrechtsschutz:** Pseudonymisierung reduziert die Menge personenbezogener Daten, die in KI-Systeme fließen — stützt die DSGVO-Flankierung des AI Act, ersetzt aber keine AI-Act-Pflicht.
- Nachweisbarkeit:** Audit-Log dokumentiert Nutzung (Metadaten) — hilfreich für interne KI-Governance/Aufsicht.
- Keine Konformitätszusage:** AISecurityGateway ist Werkzeug (siehe SCHUTZKONZEPT.md §5), nicht KI-System i. S. d. AI Act und trifft keine Aussage zur AI-Act-Konformität einer konkreten Nutzung.

## 6. Zeitliche Staffelung (Orientierung)

**Ab****Wirksam**

Feb 2025 Verbotene Praktiken (Art. 5) + KI-Kompetenz (Art. 4)

Aug 2025 Pflichten für GPAI-Modelle (General-Purpose AI)

Aug 2026 Transparenzpflichten (Art. 50) + Hochrisiko (Anhang III) im Regelfall

Aug 2027 Hochrisiko in regulierten Produkten (Anhang I)

[Fristen zum Prüfzeitpunkt gegen den aktuellen Stand abgleichen.]

---

**Ergebnis der Einordnung [ausfüllen]**

- Rolle: [Betreiber/Deployer]
- Risikoklasse der Nutzung: [begrenztes Risiko / Hochrisiko-Prüfung: ...]
- Transparenzmaßnahmen umgesetzt: [ja/nein — welche]
- Art.-4-Kompetenznachweis vorhanden: [ja/nein]

Freigegeben: [Name/Funktion], [Datum]