



DOSSIER

---

# EU AI Act - Grundlagen

# Der EU AI Act - Grundlagen

## Was Führungskräfte jetzt wissen müssen

---

### „Ist das eigentlich schon KI – und fällt das unter das Gesetz?“

---

Die Frage kommt in einem Leitungskreis, nachdem ein neues Analyse-Tool vorgestellt wurde, angeblich KI-gestützt. Und dann kommt der Satz: „Mit diesem neuen EU-Gesetz müssen wir das ja wahrscheinlich prüfen, oder?“

So beginnt es nicht selten: Die Künstliche Intelligenz (KI) ist längst da – in Tools, Prozessen, Entscheidungen. Hierzu gibt es inzwischen auch ein verbindliches Regelwerk: den EU AI Act. Doch was genau regelt er? Welche Pflichten entstehen und für wen? Was bedeutet das für Organisationen, die nicht KI entwickeln, sondern einfach nur einsetzen?

### 1. Was der EU AI Act genau regelt

---

Der EU AI Act ist das erste umfassende Gesetz zur Regulierung Künstlicher Intelligenz. **In Kraft** ist er seit dem 1. August 2024. **Anwendbar**, also im Grundsatz behördlich durchsetzbar, ist er gestaffelt, seit dem 2. August 2026 in weiten Teilen. Beide Zeitpunkte unterscheiden sich in der praktischen Bedeutung: der eine markiert den formalen Rechtsstatus, der andere den Beginn der behördlichen Durchsetzbarkeit.

#### Wen betrifft das Gesetz?

Es betrifft nicht nur Anbieter, sondern auch alle, die KI-Systeme nutzen, weiterverkaufen, verwalten oder in Prozesse integrieren. Also auch **öffentliche Einrichtungen, Unternehmen jeder Größe und Branchen**, unabhängig davon, ob sie selbst KI entwickeln oder nicht.

Praktisch heißt das: Wer irgendein KI-gestütztes Tool im Einsatz hat, und sei es nur ChatGPT im Vertrieb oder eine KI-Funktion im CRM, ist bereits Adressat des Gesetzes, wenn auch mit unterschiedlichem Pflichtenumfang.

#### Anbieter oder Betreiber?

Was von Ihnen verlangt wird, darüber entscheidet die Rolle.

Sie sind **Anbieter**, wenn Sie ein KI-System selbst entwickeln oder entwickeln lassen und es unter eigenem Namen oder eigener Marke in Verkehr bringen oder in Betrieb nehmen. Das kann beispielsweise ein eigenes KI-Produkt für Kunden sein, aber auch ein für das eigene Unternehmen entwickeltes System. Anbieter tragen deutlich weitergehende Pflichten, etwa zu Risikomanagement, technischer Dokumentation und Konformitätsbewertung.

Sie sind **Betreiber**, wenn Sie ein bereits fertiges System in eigener Verantwortung einsetzen, etwa ein eingekauftes CRM mit KI-Funktion, ein Recruiting-Tool eines Anbieters oder ChatGPT im eigenen Unternehmen nutzen. Betreiber müssen das System richtig verwenden, überwachen und bei Auffälligkeiten reagieren, tragen aber nicht die Entwicklungsverantwortung.

**Die meisten Organisationen sind Betreiber**, mit dem deutlich schlankeren Pflichtenkatalog. Das ist der erste Schritt zur eigenen Einordnung.

## Die Anbieter-Falle

Diese Rolle ist allerdings nicht in Stein gemeißelt. Wer ein bereits vorhandenes System so verändert, dass sich seine Zweckbestimmung wesentlich verschiebt, kann selbst zum Anbieter werden, mit dem vollen Pflichtenprogramm.

Das klassische Beispiel: Ein Unternehmen nimmt ein allgemeines Sprachmodell und baut daraus eine Bewerbervorauswahl. Aus dem Betreiber eines unauffälligen Werkzeugs wird, je nach Ausgestaltung, der Anbieter eines Hochrisiko-Systems. Ob das im Einzelfall zutrifft, lässt sich nicht pauschal beantworten, sondern nur mit Blick auf den konkreten Einsatz.

## Wie funktioniert der AI Act?

Vereinfacht – und nicht als formale gesetzliche Klassifikation – lassen sich KI-Anwendungen in **vier Risikostufen** einordnen.

Entscheidend dabei ist nicht die Technologie selbst, sondern wofür sie eingesetzt wird und welche Auswirkungen das auf Menschen haben kann. Ein und dasselbe System kann deshalb in einem Unternehmen unproblematisch sein und in einem anderen streng reguliert, je nachdem, wozu es genutzt wird.

### Verbotene KI:

Bestimmte besonders problematische KI-Praktiken sind vollständig untersagt, etwa manipulatives KI-Verhalten mit erheblichem Schadenspotenzial, Social Scoring oder Emotionserkennung am Arbeitsplatz – mit engen Ausnahmen etwa für medizinische oder sicherheitsbezogene Zwecke.

Mit dem Digital Omnibus sind zwei weitere Tatbestände hinzugekommen (ab dem 2. Dezember 2026): KI-Systeme für nicht einvernehmlich erstellte intime Darstellungen sowie Systeme zur Erzeugung von Missbrauchsdarstellungen Minderjähriger.

### Hochrisiko-KI:

Systeme, die wesentliche Lebensbereiche betreffen, etwa Bildung, Personal, Justiz, Kreditvergabe oder Gesundheitswesen.

Beispiele aus der Praxis: ein Tool zur automatisierten Bewerbervorauswahl, ein System zur Kreditwürdigkeitsprüfung, KI-gestützte Leistungsbeurteilung von Mitarbeitenden.

Im öffentlichen Bereich zusätzlich relevant: KI bei Sozialleistungen, Strafverfolgung, Migration oder Grenzkontrolle.

### Begrenztes Risiko:

Systeme mit potenziellen Risiken, die durch Transparenzpflichten ausreichend abgesichert werden können.

Beispiele: ein Chatbot im Kundenservice, ein KI-Sprachassistent am Telefon oder bestimmte KI-generierte bzw. manipulierte Inhalte, für die Transparenz- oder Kennzeichnungspflichten gelten.

### Minimales Risiko:

Systeme mit sehr geringem Risiko.

Beispiele: Rechtschreibkorrektur, automatische Sortierfunktionen, Spamfilter, KI-Vorschläge in Texteditoren.

**Generative KI wie ChatGPT** ist nicht automatisch einer Risikostufe zugeordnet. Entscheidend ist der konkrete Einsatz: Wird KI beispielsweise für eine in Anhang III erfasste Personalentscheidung eingesetzt, können Hochrisiko-Regeln greifen.

## 2. Ab wann was gilt – die Zeitleiste zur Umsetzung

Durch die Digital-Omnibus-Verordnung, in Kraft seit 27. Juli 2026, wurde der ursprüngliche Zeitplan geändert. Welche Frist für Sie zählt, hängt von der Risikoklasse Ihrer Systeme ab, die Sie im Abschnitt oben eingeordnet haben.

### Bereits verbindlich, für alle Unternehmen:

- **2. Februar 2025** – Verbot illegaler KI-Praktiken, Pflicht zur Förderung von KI-Kompetenz. Gilt unabhängig von der Risikoklasse für Anbieter und Betreiber von KI-Systemen.
- **2. August 2026** – Die Transparenzpflichten nach Art. 50 gelten grundsätzlich. Für bestimmte bereits vor diesem Datum angebotene Systeme zur Erzeugung synthetischer Inhalte läuft eine Übergangsfrist bis zum 2. Dezember 2026.
- **2. Dezember 2026** – Die zwei neuen Verbotstatbestände greifen (siehe oben).

### Nur relevant, wenn Sie Hochrisiko-Systeme einsetzen oder anbieten:

- **2. Dezember 2027** – Hochrisiko-Pflichten für eigenständige Systeme nach Anhang III (Personalauswahl, Bildung, Kreditvergabe, kritische Infrastruktur u. a.). Ursprünglich 2. August 2026, um 16 Monate verschoben.
- **2. August 2028** – Hochrisiko-Pflichten für Systeme, die als Sicherheitsbauteil in bereits regulierte Produkte eingebettet sind, etwa Maschinen oder Medizinprodukte. Ursprünglich 2. August 2027, um 12 Monate verschoben. Betrifft in erster Linie Hersteller, seltener den reinen Betreiber.

### Nur relevant für die großen KI-Anbieter selbst:

- **Seit 2. August 2025** – Pflichten für Anbieter von KI-Modellen mit allgemeinem Verwendungszweck (GPAI), etwa die Anbieter großer Basismodelle. Für bereits vor diesem Datum angebotene Modelle bestehen Übergangsfristen. Für normale Unternehmen, die ChatGPT, Claude & Co. lediglich nutzen, sind diese Anbieterpflichten grundsätzlich nicht einschlägig.

### Warum die Verschiebung bei Hochrisiko-KI?

Die harmonisierten Normen, an denen sich Unternehmen orientieren sollen, sind selbst noch nicht fertig. Das Pflichtenprogramm selbst bleibt unverändert, nur der Stichtag verschiebt sich.

**Für Führungskräfte gilt:** Auch ohne Hochrisiko-KI bestehen bereits Pflichten, insbesondere zur Förderung der KI-Kompetenz und – soweit einschlägig – zur Transparenz. Wer Hochrisiko-Systeme einsetzt oder anbietet, sollte die Zeit bis 2027/2028 zur Vorbereitung nutzen.

## 3. Welche Pflichten sich daraus für Organisationen ergeben

Je nach Risikoklasse gelten unterschiedliche Anforderungen. Entscheidend ist: **Wer KI einsetzt, trägt Verantwortung, auch wenn das System von außen kommt.**

Für die meisten Organisationen entstehen dabei folgende zentrale **Pflichten**:

### Transparenzpflicht

Für bestimmte KI-Systeme gelten Transparenzpflichten. Menschen müssen etwa erkennen können, wenn sie mit einem KI-System interagieren. Für Deepfakes und bestimmte KI-generierte oder manipulierte Inhalte gelten zusätzliche Kennzeichnungs- bzw. Offenlegungspflichten.

## **KI-Kompetenz**

Organisationen müssen Maßnahmen ergreifen, damit ihr Personal versteht, was ein eingesetztes KI-System kann und wo seine Grenzen liegen.

Seit der Überarbeitung durch den Digital Omnibus im Juli 2026 ist das eine Unterstützungspflicht, keine Garantie für ein bestimmtes Kompetenzniveau. Die Pflicht gilt seit Februar 2025 und erfasst alle relevanten Personen in der Organisation – je nach Rolle und KI-Nutzung also auch Führungskräfte.

## **Risikoprüfung**

Bei Hochrisiko-KI gelten umfangreiche zusätzliche Anforderungen. Welche davon eine Organisation selbst erfüllen muss, hängt insbesondere davon ab, ob sie Anbieter oder Betreiber ist. Für bestimmte Betreiber und Einsatzbereiche kann vor dem Einsatz zusätzlich eine Grundrechte-Folgenabschätzung erforderlich sein.

## **Technische & organisatorische Maßnahmen**

Bei Hochrisiko-KI bestehen je nach Rolle unterschiedliche technische und organisatorische Pflichten. Betreiber müssen solche Systeme insbesondere entsprechend den Vorgaben einsetzen, ihren Betrieb überwachen und bei Auffälligkeiten reagieren.

## **Registrierungs- und Informationspflichten**

Für bestimmte Hochrisiko-Systeme bestehen Registrierungs- und Informationspflichten. Wer diese erfüllen muss, hängt von der jeweiligen Rolle und dem Einsatzbereich ab. Für Betreiber gelten darüber hinaus eigene Informations- und Dokumentationspflichten.

## **Sanktionen**

Der Bußgeldrahmen reicht bis zu 35 Mio. Euro oder 7 % des weltweiten Jahresumsatzes bei Verstößen gegen die verbotenen Praktiken, das ist die höchste Stufe. Für die meisten übrigen Verstöße, etwa gegen die Transparenzpflicht, liegt der Rahmen bei bis zu 15 Mio. Euro oder 3 %.

Für KMU gilt dabei der niedrigere der beiden Beträge als Obergrenze, bei großen Unternehmen der höhere. Für Behörden und öffentliche Stellen richtet sich die mögliche Verhängung von Geldbußen zusätzlich nach nationalem Recht.

## **Persönliche Verantwortung**

Die Sanktionen oben treffen das Unternehmen. Daneben gilt, unabhängig vom EU AI Act, die allgemeine Sorgfaltspflicht von Geschäftsführung und Vorstand (§ 43 GmbHG, § 93 AktG), mit der Sorgfalt eines ordentlichen und gewissenhaften Geschäftsleiters zu handeln.

Diese Pflicht ist technologieneutral. Sie galt schon vor dem EU AI Act und gilt für KI-gestützte Entscheidungen genauso wie für jede andere unternehmerische Entscheidung.

Der Punkt, der in der Praxis oft überrascht: Zur Sorgfalts- und Organisationsverantwortung gehört natürlich auch, relevante gesetzliche Anforderungen wie den EU AI Act zu kennen und angemessene organisatorische Maßnahmen zu treffen. Eine unzureichende Organisation kann daher auch unabhängig von einer einzelnen fehlerhaften KI-Entscheidung haftungsrechtlich relevant werden.

Geschäftsführer:innen können sich deshalb nicht darauf beschränken, von KI-Nutzung und den damit verbundenen Anforderungen im Unternehmen nichts zu wissen. Zu ihrer Organisationsverantwortung gehört auch, relevante regulatorische Anforderungen zu erkennen und angemessen darauf zu reagieren.

## 4. Verantwortung bleibt – auch bei externen Tools

Viele Organisationen entwickeln keine eigenen KI-Systeme, sondern kaufen Tools ein oder nutzen KI-Funktionen, die in Standardsoftware bereits enthalten sind.

Genau hier entsteht ein blinder Fleck: Nur weil eine KI „von außen“ kommt, entfällt die eigene Verantwortung nicht. Auch wer ein KI-System nicht selbst entwickelt, sondern lediglich einsetzt, kann eigene Pflichten haben.

### Externe Anbieter entbinden nicht von Pflichten

Auch bei zugekauften Systemen muss die Organisation selbst prüfen, ob es sich um KI mit Risiko handelt, ob Transparenzpflichten bestehen oder eine Risikobewertung notwendig ist. Ein Verweis auf das Whitepaper des Herstellers genügt dafür nicht.

### Gefahr durch Embedded KI

Besonders anspruchsvoll sind versteckte KI-Funktionen, etwa in CRM-Systemen, HR-Software oder Kundenportalen. Sie sind häufig standardmäßig aktiviert, ohne dass jemand das bewusst eingeschaltet hätte, und werden deshalb gar nicht als eigenständige KI erkannt.

Auch eingebettete KI-Funktionen können Pflichten auslösen. Organisationen sollten deshalb wissen, welche KI-Funktionen in ihrer Software tatsächlich eingesetzt werden und wie diese rechtlich einzuordnen sind.

### Führungsimplication: Tool-Auswahl wird zur Compliance-Frage

Die Auswahl digitaler Werkzeuge ist damit nicht mehr nur eine IT- oder Effizienzentscheidung. Wer KI-Tools einführt, kann damit auch neue Pflichten auslösen. Vor der Einführung lohnt es sich deshalb, gezielt zu fragen:

- **Ist der Anbieter AI-Act-konform aufgestellt?**
- **Liegen aussagekräftige Risikoeinschätzungen vor?**
- **Wer verantwortet die Überprüfung bei externer Software?**

## 5. Deutscher Rahmen

Ein EU-Gesetz gilt zwar formal in jedem Mitgliedstaat, aber ohne nationale Zuständigkeit ist zunächst unklar, wer es durchsetzt und wer bei Fragen zur Verfügung steht. Genau diese Lücke schließt Deutschland seit dem 29. Juli 2026 mit dem KI-Marktüberwachungs- und Innovationsförderungsgesetz (KI-MIG):

- **Zentrale Zuständigkeit:** Die Bundesnetzagentur wird zur zentralen Marktüberwachungs-, Anlauf- und Beschwerdestelle für die KI-Verordnung. Für viele Organisationen ist sie damit die zentrale erste Anlaufstelle für Fragen zur KI-Verordnung.
- **Koordination & Kompetenzzentrum:** Bei der Bundesnetzagentur entsteht zusätzlich das KoKIVO, mit einem KI-Service-Desk für konkrete Fragen und KI-Reallaboren, in denen Organisationen, gerade auch kleinere, neue KI-Anwendungen unter behördlicher Begleitung testen können, bevor sie live gehen.

- **Anknüpfen an Bestehendes:** Wo die KI-Verordnung in bereits regulierte Produktbereiche hineinwirkt, etwa Medizinprodukte oder Maschinen, bleiben die bisherigen Marktüberwachungsbehörden zuständig. Das KI-MIG ersetzt vertraute Zuständigkeiten also nicht, sondern schließt nur die Lücke dort, wo bisher niemand zuständig war.
- **Finanzsektor-Spezifik:** Im Finanzbereich übernimmt die BaFin die Marktüberwachung, wenn KI-Systeme direkt mit regulierten Finanztätigkeiten verbunden sind, in Abstimmung mit der Bundesnetzagentur.
- **Unabhängigkeit & Kontrolle:** Für einen engen, besonders grundrechtssensiblen Bereich, etwa Biometrie bei Strafverfolgung oder Migration, richtet das Gesetz eine eigene, unabhängige Kammer bei der Bundesnetzagentur ein, die jährlich an den Bundestag berichtet. Für den überwiegenden Teil der Wirtschaft bleibt aber die Bundesnetzagentur selbst der erste Ansprechpartner, nicht diese Kammer.

**Was Marktüberwachung praktisch bedeutet:** Als Marktüberwachungsbehörde kann die Bundesnetzagentur Auskünfte und Dokumentation zu eingesetzten Hochrisiko-Systemen verlangen, Prüfungen durchführen und, wenn ein System nicht konform ist, Korrekturmaßnahmen oder im äußersten Fall die Marktrücknahme anordnen.

Bundesnetzagentur ist darüber hinaus auch Beschwerdestelle. Das bedeutet, dass nicht nur anlasslose Prüfungen möglich sind, sondern auch Dritte, etwa Kunden, Mitarbeitende oder Wettbewerber, eine Beschwerde einreichen können, die dann eine Prüfung auslöst. Die Kontrolle geht also nicht nur von der Behörde selbst aus.

**Für Organisationen heißt das:** Es gibt seit Ende Juli 2026 zum ersten Mal eine klare Antwort auf die Frage, wer im Zweifel zuständig ist, und mit dem Service-Desk auch eine konkrete erste Anlaufstelle für Praxisfragen, bevor man extern Rat sucht.

## 6. Europäische Initiativen: AI Continent & Apply AI

Neben dem AI Act arbeitet die EU an **zwei Förderprogrammen**, die zeigen: Regulierung allein reicht nicht, wenn Europa im KI-Bereich mithalten will, es braucht auch eigene Infrastruktur und Anwendungsförderung.

Der **AI Continent Action Plan (April 2025)** legt den Fokus auf Infrastruktur und Investitionen, die **Apply AI Strategy (Oktober 2025)** auf die Nutzung in der Breite, unter anderem in Fertigung, Mobilität und Gesundheit.

Konkret nutzbar, unabhängig von der Größe der Organisation:

- **AI Factories:** ein Netzwerk europäischer Supercomputer, mit priorisiertem Zugang für Start-ups und KMU, zwei Standorte in Deutschland. Gibt Zugang zu Rechenleistung für eigene KI-Projekte, die sich viele Organisationen sonst gar nicht leisten könnten.
- **European Digital Innovation Hubs:** über 250 regionale Anlaufstellen, offen für Organisationen jeder Art, die bei der KI-Einführung konkret beraten, oft der niedrigschwelligste erste Kontakt, bevor man eine kostenpflichtige externe Beratung beauftragt.
- **AI Act Service Desk der Kommission:** ein kostenfreier Compliance-Checker, ergänzt um einen „AI Act Explorer“ und die Möglichkeit, Einstufungsfragen direkt an ein Expertenteam zu stellen.

## Was Organisationen jetzt tun sollten

Der EU AI Act ist für die Geschäftsführung vor allem eine Organisationsaufgabe. Sie müssen nicht jedes technische Detail selbst prüfen. Aber Sie sollten sicherstellen, dass klar ist, wo KI eingesetzt wird, welche Risiken daraus entstehen und wer im Unternehmen dafür Verantwortung trägt.

Als Geschäftsführung oder Vorstand sollten Sie deshalb **fünf Fragen** beantworten können:

### 1. Welche KI setzen wir tatsächlich ein?

Auch KI-Funktionen in bestehender Software und bislang informell genutzte Tools berücksichtigen.

### 2. Gibt es darunter sensible oder potenziell hochriskante Anwendungen?

Besonders Anwendungen in Bereichen wie Personal, Kredit, Bildung oder anderen regulierten Entscheidungen prüfen.

### 3. Wer entscheidet bei uns über neue KI-Anwendungen?

Verantwortung für Prüfung, Freigabe und Dokumentation klar festlegen.

### 4. Wie fördern wir die notwendige KI-Kompetenz?

Maßnahmen an Rollen, Vorwissen und konkrete Nutzung anpassen.

### 5. Können wir unsere KI-Nutzung im Zweifel erklären und belegen?

Eingesetzte Systeme, Zuständigkeiten und wesentliche Prüfentscheidungen so festhalten, dass sie intern und gegenüber Dritten nachvollziehbar sind.

## Künstliche Intelligenz weiterdenken

Was in diesem Dossier zwangsläufig offenbleiben musste: Ob und wie genau die einzelnen Punkte für Ihr Unternehmen zutreffen, lässt sich generisch nicht beantworten, das hängt an Ihrer konkreten Systemlandschaft. Genau dafür gibt es **The AI Leader**, ein 1:1-Format für Geschäftsführer:innen, in dem wir diese Fragen gemeinsam für Ihr Unternehmen konkret klären. Melden Sie sich gern, wenn Sie nähere Informationen zu diesem Angebot möchten.

**Unverbindliche Beratung:** <https://calendly.com/freuding/beratung-ki>

**Kontakt:** Dr. Beate Freuding, [freuding@digital-leader.eu](mailto:freuding@digital-leader.eu), 0152 05188026

**Weitere Dossiers & E-Books zum Download:** [ki-briefing.kit.com](https://ki-briefing.kit.com)

Die diesem Dossier zugrunde liegenden Quellen werden aus Platzgründen hier nicht vollständig aufgeführt. Auf Anfrage senden wir sie gerne zu.

Hinweis: Die Regulierung innerhalb Europas entwickelt sich sehr schnell. Dieses Dokument ist im August 2026 erstellt worden. Zum Zeitpunkt des Lesens können die im Dokument genannten Fakten bereits überholt sein.

Dieses Dokument dient der allgemeinen Information und Orientierung und ist in enger Zusammenarbeit mit Künstlicher Intelligenz entstanden. Es stellt keine Rechtsberatung dar und kann eine individuelle juristische Prüfung im Einzelfall nicht ersetzen.

Alle Angaben wurden sorgfältig recherchiert und nach bestem Wissen erstellt. Dennoch übernimmt die Autorin keine Gewähr für die Aktualität, Vollständigkeit oder Richtigkeit der Inhalte, insbesondere im Hinblick auf sich fortentwickelnde gesetzliche Vorgaben.

Für Entscheidungen, die auf Basis dieses Dokuments getroffen werden, übernimmt die Autorin keine Haftung. Die Umsetzung rechtlicher Anforderungen – insbesondere im Bereich KI-Governance – sollte stets in Abstimmung mit fachkundiger Rechtsberatung erfolgen.