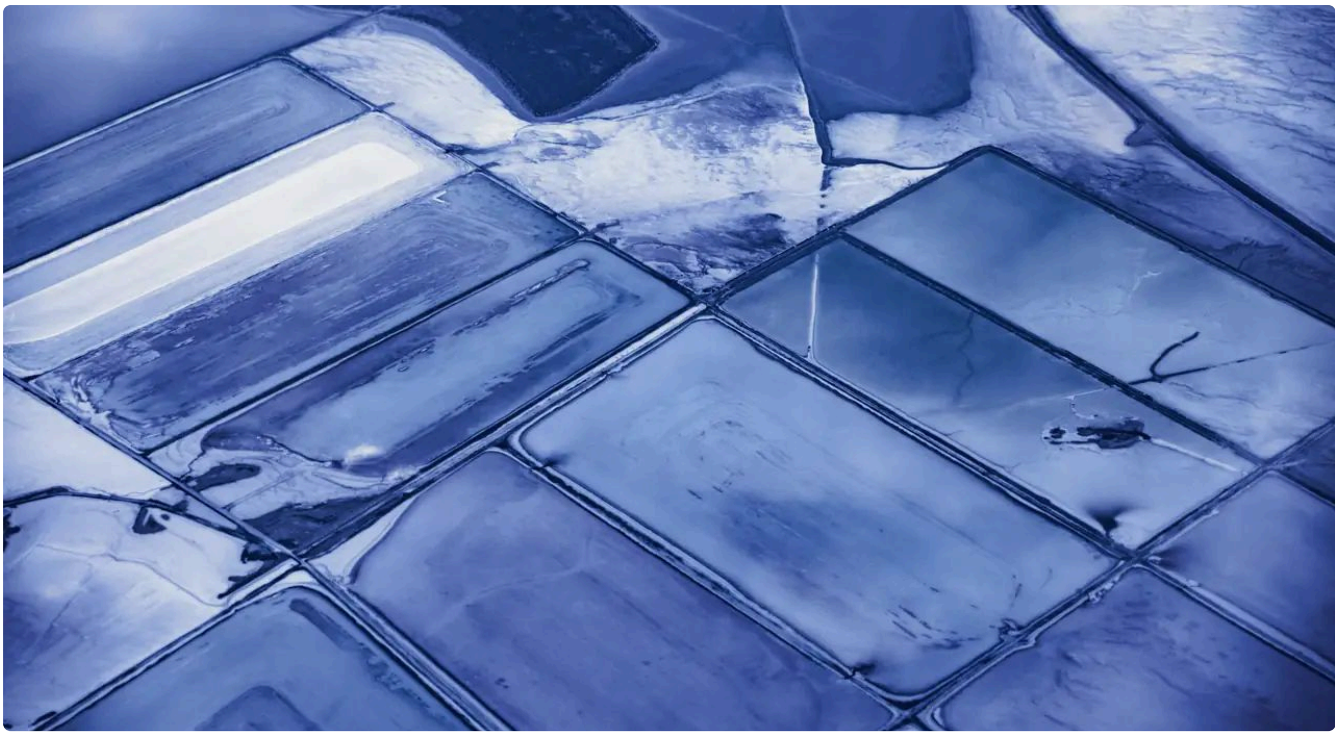


LEITFADEN · NOVEMBER 2026 · 11 MIN. LESEZEIT

EU AI Act ohne Aufregung

Was seit wann gilt, welche Rolle Ihr Unternehmen hat und wie Sie sich in fünf Schritten vorbereiten



Philipp Pöschke
Founder, Paice

AUF EINEN BLICK

- Für die meisten Unternehmen gelten heute drei Pflichten aus dem AI Act: Maßnahmen zur AI-Kompetenz, der Verzicht auf verbotene Praktiken und, je nach Einsatz, Transparenzpflichten, etwa bei Chatbots oder AI-erzeugten Bildern.
- Die Pflichten für Hochrisiko-Systeme, etwa in der Bewerberauswahl oder bei der Kreditprüfung, gelten nach einer Änderung vom Juli 2026 ab 2. Dezember 2027, für AI in regulierten Produkten ab 2. August 2028.
- Wer jetzt seine AI-Systeme erfasst und Rolle und Risikoklasse je System begründet dokumentiert, schafft die Grundlage für alle späteren Pflichten.

Der EU AI Act, auf Deutsch KI-Verordnung (Verordnung (EU) 2024/1689), ist seit 1. August 2024 in Kraft und wird stufenweise anwendbar. Er stuft AI-Systeme nach ihrem Risiko ein und verteilt die Pflichten auf alle, die ein System entwickeln, vertreiben oder einsetzen. Damit betrifft er auch Unternehmen, die selbst keine AI entwickeln.

Im Juli 2026 hat sich der Rahmen zweimal verändert. Die EU hat die Verordnung mit der Digital-Omnibus-Verordnung zur KI (Verordnung (EU) 2026/1744) geändert; die Änderung ist seit 27. Juli 2026 in Kraft. Sie verschiebt die Pflichten für Hochrisiko-Systeme, fasst die Pflicht zur AI-Kompetenz neu und ergänzt zwei Verbote. Zwei Tage später trat in Deutschland das KI-Marktüberwachungs- und Innovationsförderungsgesetz (KI-MIG) in Kraft. Es macht die Bundesnetzagentur zur zentralen Aufsichtsbehörde.

Dieser Leitfaden zeigt, was seit wann gilt, wie Sie die Rolle Ihres Unternehmens bestimmen und welche Pflichten daraus folgen. Er richtet sich vor allem an Unternehmen, die AI einsetzen, und gibt den Stand vom 17. November 2026 wieder.

Was seit wann gilt

ABBILDUNG 1

Was seit wann gilt (Stand 17. November 2026)

1. August 2024
KI-Verordnung tritt in Kraft

2. Februar 2025
Verbotene Praktiken (Art. 5) und Pflicht zur AI-Kompetenz (Art. 4)

2. August 2025
Pflichten für Anbieter von Modellen mit allgemeinem Verwendungszweck, Regeln zu Behörden und Bußgeldern

27. und 29. Juli 2026
Änderungsverordnung (EU) 2026/1744 und deutsches KI-MIG in Kraft

2. August 2026
Allgemeine Geltung, darunter die Transparenzpflichten (Art. 50)

2. Dezember 2026
Zwei neue Verbote; maschinenlesbare Kennzeichnung (Art. 50 Abs. 2) auch für Systeme, die schon vor August 2026 auf dem Markt waren

2. Dezember 2027
Hochrisiko-Systeme nach Anhang III, etwa Personal, Kredit, Bildung, kritische Infrastruktur

2. August 2028
Hochrisiko-Systeme in Produkten nach Anhang I

Paice nach Art. 111 und 113 der Verordnung (EU) 2024/1689 in der Fassung der Verordnung (EU) 2026/1744 (EUR-Lex, konsolidierte Fassung vom 27.07.2026) und Bundesnetzagentur

Die Geltungsdaten stehen in Art. 113 der KI-Verordnung, die Übergangsregeln für Systeme und Modelle, die vor einem Stichtag auf dem Markt waren, in Art. 111. Für ein Unternehmen, das AI einsetzt, sind damit

heute drei Pflichtengruppen anwendbar. Die Verbote nach Art. 5 und die Pflicht zur AI-Kompetenz nach Art. 4 gelten seit 2. Februar 2025, die Transparenzpflichten nach Art. 50 seit 2. August 2026. Die umfangreichen Pflichten für Hochrisiko-Systeme folgen ab 2. Dezember 2027 für die Einsatzbereiche in Anhang III und ab 2. August 2028 für AI in Produkten nach Anhang I.

Die Verschiebung schafft Zeit. Die Anforderungen selbst bleiben für Betreiber weitgehend gleich. Wer ein Hochrisiko-System betreibt, braucht bis zum Stichtag benannte Aufsichtspersonen, eine Protokollierung und Meldewege, die im Alltag funktionieren. Das braucht Vorlauf, vor allem wenn mehrere Fachbereiche und der Betriebsrat beteiligt sind.

Maßgeblich ist die jeweils aktuelle konsolidierte Fassung auf EUR-Lex. Dazu kommen Leitlinien der Kommission. Sie sind nicht verbindlich, zeigen aber, wie die Kommission die Verordnung auslegt. Zur Einstufung von Hochrisiko-Systemen hat sie im Mai 2026 einen Entwurf veröffentlicht; auf ihrer Website stand am 17. November 2026 weiterhin der Entwurf.

Welche Rolle hat Ihr Unternehmen?

Welche Pflichten gelten, hängt von der Rolle ab, die ein Unternehmen bei einem bestimmten System hat. Die Verordnung unterscheidet vor allem zwei Rollen (Art. 3):

- **Anbieter** entwickeln ein AI-System oder lassen es entwickeln und bringen es unter eigenem Namen in Verkehr oder nehmen es in Betrieb, entgeltlich oder unentgeltlich.
- **Betreiber** verwenden ein AI-System in eigener Verantwortung. Ausgenommen ist nur die rein private Nutzung.

Daneben kennt die Verordnung Einführer, Händler und Bevollmächtigte. Die meisten Pflichten tragen die Anbieter.

Die meisten Unternehmen sind überwiegend Betreiber. Sie kaufen Software mit AI-Funktionen und setzen sie ein. Drei Konstellationen machen aus einem Betreiber einen Anbieter:

01 **Eigene Entwicklung, auch für den internen Gebrauch.** Als Inbetriebnahme gilt nach Art. 3 Nr. 11 auch die Bereitstellung zum Eigengebrauch. Wer auf Basis eines eingekauften Sprachmodells einen eigenen Assistenten baut und im Unternehmen einsetzt, ist für dieses System Anbieter und Betreiber zugleich. Bei einem System ohne hohes Risiko bleiben die zusätzlichen Pflichten überschaubar.

02 **Eingriffe in Hochrisiko-Systeme.** Nach Art. 25 übernimmt die Pflichten eines Anbieters, wer ein Hochrisiko-System unter eigenem Namen vertreibt, es wesentlich verändert oder ein anderes System so umwidmet, dass es hochriskant wird.

03 **Erheblich veränderte Modelle.** Wer ein Modell mit allgemeinem Verwendungszweck über eine Schnittstelle nutzt, wird dadurch nicht dessen Anbieter. Erst erhebliche Veränderungen am Modell können Anbieterpflichten auslösen. Wo die Grenze liegt, beschreiben die Leitlinien der Kommission für diese Modelle.

Die Rolle bestimmen Sie deshalb je System. Ein Unternehmen kann bei einem Werkzeug Betreiber und beim nächsten Anbieter sein.

Ein Beispiel

Ein konstruiertes Beispiel zeigt, wie unterschiedlich das ausfällt. Ein Industrieunternehmen nutzt drei AI-Anwendungen.

- **Ein eingekaufter Schreibassistent in der Bürosoftware.** Das Unternehmen ist Betreiber eines Systems ohne hohes Risiko. Es gilt vor allem die Pflicht zur AI-Kompetenz.
- **Ein selbst gebauter Chatbot auf der Website.** Das Unternehmen ist Anbieter. Seit 2. August 2026 muss der Chatbot so gestaltet sein, dass Nutzer erkennen, dass sie mit einem AI-System sprechen (Art. 50 Abs. 1).
- **Ein Bewerbermanagement, das Bewerbungen vorsortiert.** Systeme, die Bewerbungen filtern oder Bewerber bewerten, nennt Anhang III Nr. 4 ausdrücklich. Das Unternehmen ist damit in aller Regel Betreiber eines Hochrisiko-Systems und hat ab 2. Dezember 2027 die Pflichten nach Art. 26. Unabhängig vom AI Act ist der Betriebsrat schon bei der Planung zu unterrichten; § 90 BetrVG nennt den Einsatz von Künstlicher Intelligenz ausdrücklich.

Pflichten nach Risikoklasse

Maßgeblich für die Einstufung ist der Einsatzzweck. Geprüft wird von oben nach unten, von den verbotenen Praktiken bis zu den Systemen, für die keine besonderen Pflichten gelten.

ABBILDUNG 2

Pflichten nach Risikoklasse

01

Verboten (Art. 5)

Seit 2. Februar 2025, etwa Emotionserkennung am Arbeitsplatz, Social Scoring und manipulative Techniken. Ab 2. Dezember 2026 auch AI, die intime Darstellungen ohne Einwilligung oder Missbrauchsdarstellungen von Kindern erzeugt.

02

Hochrisiko (Art. 6, Anhänge I und III)

Etwa Bewerberauswahl, Kreditwürdigkeit, Bildung, kritische Infrastruktur oder AI als Sicherheitsbauteil in Produkten. Betreiberpflichten nach Art. 26 ab 2. Dezember 2027, bei Produkten ab 2. August 2028.

03

Transparenz (Art. 50)

Seit 2. August 2026. Chatbots geben sich als AI zu erkennen, erzeugte Inhalte werden maschinenlesbar markiert, Deepfakes werden offengelegt.

04

Alle übrigen Systeme

Keine besonderen Pflichten außer der AI-Kompetenz (Art. 4). Nach Einschätzung der Kommission fällt die große Mehrheit der genutzten AI-Systeme in diese Gruppe.

05

Modelle mit allgemeinem Verwendungszweck (Kapitel V)

Pflichten für die Anbieter der Modelle seit 2. August 2025, etwa technische Dokumentation und eine Strategie zum Urheberrecht. Wer ein Modell nur nutzt, ist davon in der Regel nicht betroffen.

Paice nach Verordnung (EU) 2024/1689 in der Fassung der Verordnung (EU) 2026/1744 und Europäischer Kommission

Für Betreiber werden die Transparenzpflichten vor allem bei Deepfakes relevant und bei AI-erzeugten Texten, die die Öffentlichkeit über Angelegenheiten von öffentlichem Interesse informieren sollen. Bei solchen Texten entfällt die Offenlegung, wenn ein Mensch sie geprüft hat und jemand die redaktionelle Verantwortung trägt (Art. 50 Abs. 4). Die Kommission hat im Juli 2026 Leitlinien zu Art. 50 veröffentlicht.

Was Betreiber von Hochrisiko-Systemen tun müssen

Art. 26 verpflichtet Betreiber unter anderem,

- das System gemäß der Gebrauchsanweisung des Anbieters zu verwenden,
- die menschliche Aufsicht Personen zu übertragen, die dafür befähigt, geschult und befugt sind,
- dafür zu sorgen, dass Eingabedaten, soweit sie unter ihrer Kontrolle stehen, dem Zweck entsprechen und ausreichend repräsentativ sind,
- den Betrieb zu überwachen und Risiken sowie schwerwiegende Vorfälle zu melden,
- automatisch erzeugte Protokolle mindestens sechs Monate aufzubewahren,
- Arbeitnehmervertretung und betroffene Beschäftigte vor dem Einsatz am Arbeitsplatz zu informieren,
- Personen zu informieren, über die das System Entscheidungen trifft oder bei solchen Entscheidungen unterstützt.

Öffentliche Stellen, private Erbringer öffentlicher Dienste sowie Betreiber von Systemen zur Kreditwürdigkeitsprüfung und zur Risikobewertung und Preisbildung in der Lebens- und Krankenversicherung müssen vor dem ersten Einsatz zusätzlich eine Grundrechte-Folgenabschätzung durchführen (Art. 27).

AI-Kompetenz nach der Neufassung

Die Änderung vom Juli 2026 hat Art. 4 neu gefasst. Anbieter und Betreiber müssen Maßnahmen ergreifen, um die AI-Kompetenz (im Gesetz: KI-Kompetenz) ihres Personals und anderer Personen zu fördern, die in ihrem Auftrag mit AI-Systemen arbeiten. Ein bestimmtes Kompetenzniveau je Person schulden sie ausdrücklich nicht. Die Maßnahmen sollen zu Vorwissen, Einsatzkontext und den betroffenen Personen passen. Für die Aufsicht über Hochrisiko-Systeme bleibt die strengere Anforderung aus Art. 26 bestehen.

Bußgelder

Die Bußgelder sind gestaffelt (Art. 99). Verstöße gegen die Verbote können bis zu 35 Mio. Euro oder 7 % des weltweiten Jahresumsatzes kosten, Verstöße gegen die meisten anderen Pflichten, darunter Art. 26 und Art. 50, bis zu 15 Mio. Euro oder 3 %. Für falsche oder irreführende Angaben gegenüber Behörden sind es bis zu 7,5 Mio. Euro oder 1 %. Grundsätzlich gilt der höhere Betrag. Für kleine und mittlere Unternehmen gilt der niedrigere, seit der Änderung bei den beiden unteren Stufen auch für kleine Midcap-Unternehmen.

Wer in Deutschland zuständig ist

Nach dem KI-MIG ist die Bundesnetzagentur Marktüberwachungsbehörde, soweit das Gesetz nichts anderes bestimmt (§ 2 Abs. 1 KI-MIG). Sie ist außerdem zentrale Anlaufstelle und nimmt Beschwerden entgegen. Für Unternehmen betreibt sie einen KI-Service-Desk mit einem Online-Werkzeug zur ersten Einschätzung der Risikoklasse. Für einzelne Bereiche bleiben andere Behörden zuständig:

- die BaFin für AI-Systeme, die unmittelbar mit beaufsichtigten Finanzdienstleistungen zusammenhängen,
- die bisherigen Marktüberwachungsbehörden für AI in Produkten wie Medizinprodukten, Aufzügen oder Spielzeug,
- Behörden der Länder für AI, die öffentliche Stellen der Länder einsetzen, und für Mediendienste.

Die Anbieter von Modellen mit allgemeinem Verwendungszweck beaufsichtigt auf EU-Ebene das AI Office der Kommission.

In fünf Schritten vorbereiten

ABBILDUNG 3

In fünf Schritten vorbereiten

01

Inventar

Alle AI-Systeme erfassen, auch AI-Funktionen in eingekaufter Software

02

Rollen klären

Je System festhalten, ob Sie Anbieter, Betreiber oder beides sind

03

Risiko einstufen

Verbote ausschließen, Hochrisiko prüfen, Transparenzpflichten zuordnen

04

Pflichten umsetzen

AI-Kompetenz, Transparenz und Aufsicht mit klaren Zuständigkeiten organisieren

05

Nachweise führen

Einstufung, Schulungen und Entscheidungen dokumentieren und aktuell halten

Paice

01 **Inventar.** Erfassen Sie alle AI-Systeme, die im Einsatz oder geplant sind, auch AI-Funktionen in eingekaufter Software und Werkzeuge, die Fachbereiche auf eigene Faust nutzen. Für den Anfang

genügen je System wenige Angaben: Zweck, Fachbereich, verantwortliche Person, Hersteller, verarbeitete Daten und betroffene Personen. Ob eine Software überhaupt ein AI-System im Sinne von Art. 3 Nr. 1 ist, erläutern Leitlinien der Kommission vom Februar 2025.

02 **Rollen klären.** Halten Sie je System fest, ob Sie Anbieter, Betreiber oder beides sind. Eigenentwicklungen und Änderungen an eingekauften Systemen verdienen dabei einen zweiten Blick.

03 **Risiko einstufen.** Schließen Sie zuerst verbotene Praktiken aus, prüfen Sie dann Anhang I und III und zuletzt die Transparenzpflichten. Bei eingekauften Systemen hilft die Zweckbestimmung des Anbieters. Setzen Sie ein System anders ein als vorgesehen, kann sich die Einstufung ändern. Wer als Anbieter ein System aus Anhang III nach Art. 6 Abs. 3 für nicht hochriskant hält, muss das vor dem Inverkehrbringen dokumentieren und das System registrieren (Art. 6 Abs. 4, Art. 49 Abs. 2).

04 **Pflichten umsetzen.** Jetzt fällig sind Maßnahmen zur AI-Kompetenz, abgestuft nach Rolle, dazu Nutzungsregeln, Transparenzhinweise und die Beteiligung des Betriebsrats. Für Hochrisiko-Systeme kommen bis Dezember 2027 benannte und geschulte Aufsichtspersonen hinzu, außerdem Protokollierung, Meldewege und Verträge, die regeln, welche Informationen und welche Unterstützung der Anbieter liefert.

05 **Nachweise führen.** Dokumentieren Sie Inventar, Einstufung mit Begründung, Schulungen und Zuständigkeiten. Verankern Sie die Prüfung in den bestehenden Abläufen für Einkauf, Datenschutz und Informationssicherheit, damit jedes neue System diese Schritte durchläuft. Ein Managementsystem nach ISO/IEC 42001 kann den Rahmen bilden. Für Anbieter von Hochrisiko-Systemen gibt es seit Oktober 2026 mit EN 18286 die erste harmonisierte Norm zum AI Act; sie betrifft das Qualitätsmanagement nach Art. 17.

> Ein gepflegtes Verzeichnis der AI-Systeme ist die Grundlage jeder weiteren Pflicht und macht die Freigabe neuer Vorhaben planbar.

Typische Fehler

- **Nur eigene Projekte erfassen.** AI-Funktionen kommen auch per Update in Standardsoftware, ohne dass jemand ein AI-Projekt beschlossen hat.
- **Die Verschiebung als Entwarnung lesen.** Verbote, AI-Kompetenz und Transparenzpflichten gelten bereits, und die Vorbereitung auf Hochrisiko-Pflichten braucht Vorlauf.
- **Die Rolle einmal für das ganze Unternehmen festlegen.** Sie gilt je System. Wer intern ein eigenes AI-System baut, ist dafür Anbieter.
- **AI-Kompetenz mit einer Pflichtschulung abhaken.** Art. 4 verlangt Maßnahmen, die zu Rolle und Einsatz passen. Wer ein Hochrisiko-System beaufsichtigt, braucht mehr als eine Grundschulung (Art. 26 Abs. 2).
- **Den AI Act isoliert betrachten.** Für Hochrisiko-Systeme verweist Art. 26 Abs. 9 auf die Datenschutz-Folgenabschätzung nach der DSGVO. Bei technischen Einrichtungen, die Verhalten oder Leistung von Beschäftigten überwachen können, bestimmt der Betriebsrat mit (§ 87 Abs. 1 Nr. 6 BetrVG).

Dieser Leitfaden ersetzt keine Rechtsberatung. Er gibt den Stand vom 17. November 2026 wieder und vereinfacht an mehreren Stellen. Ob ein bestimmtes System hochriskant ist und welche Rolle Ihr Unternehmen dabei hat, sollte im Zweifel rechtlich geprüft werden.

Quellen

- Verordnung (EU) 2024/1689 (KI-Verordnung), konsolidierte Fassung, EUR-Lex, Stand 27.07.2026
- Verordnung (EU) 2026/1744 (Digital-Omnibus-Verordnung zur KI), Amtsblatt der EU, 24.07.2026
- AI Act: Zeitplan und Überblick, Europäische Kommission
- Leitlinien zu verbotenen Praktiken, Europäische Kommission, 04.02.2025
- Leitlinien für Anbieter von Modellen mit allgemeinem Verwendungszweck, Europäische Kommission
- Leitlinien zu den Transparenzpflichten nach Art. 50, Europäische Kommission, 2026
- Entwurf der Leitlinien zur Einstufung von Hochrisiko-Systemen, Europäische Kommission, 19.05.2026
- Erste harmonisierte Norm zum AI Act (EN 18286), Europäische Kommission, 19.10.2026
- AI Act Service Desk, Europäische Kommission
- KI-Marktüberwachungs- und Innovationsförderungsgesetz (KI-MIG), BGBl. 2026 I Nr. 223, gesetze-im-internet.de
- Bundesnetzagentur übernimmt zentrale Rolle bei der Umsetzung der KI-Verordnung, Bundesnetzagentur, 29.07.2026
- KI-Service-Desk, Bundesnetzagentur
- § 87 Betriebsverfassungsgesetz, gesetze-im-internet.de
- § 90 Betriebsverfassungsgesetz, gesetze-im-internet.de



AUTOR

Philipp Pöschke

Founder, Paice

Philipp Pöschke hat Paice 2026 in Bremen gegründet. Er verantwortet jedes Vorhaben persönlich und arbeitet selbst an Analysen, Prototypen und Lösungen mit. Die Beiträge unter Insights verantwortet er als Autor.