Der EU AI-Act – Regulierung der Künstlichen Intelligenz. Viel Schaden, wenig Nutzen.



Wissen

Copilot, Agenten und KI im Microsoft-Umfeld im Überblick: Microsoft Copilot

Beratung

KI-Inventar, Einstufung nach AI Act und schlanke Nachweise, die eine Prüfung überstehen – gemeinsam aufgesetzt statt im Audit nachgezogen. Sprich mich über die Kontaktseite auf boddenberg.de an.

Schulung

KI-Kompetenz nach Art. 4 AI Act für Fachbereiche, Führungskräfte, IT und Betriebsrat – praxisnah, dokumentierbar, inhouse oder online.

Vor einiger Zeit saß ich in einem Lenkungskreis, in dem das Datenschutzteam eine 80-seitige „AI-Act-Readiness-Analyse“ präsentierte. Ergebnis nach drei Monaten Arbeit: Das Unternehmen betreibt Microsoft 365 Copilot, einen Chatbot auf der Website und eine Rechnungserkennung in der Buchhaltung. Hochrisiko-Systeme: keine. Die eigentliche Pflicht für alle drei Systeme passte auf eine halbe Seite. Die anderen 79,5 Seiten waren Angst in Tabellenform.

Das ist die eine Hälfte der Wahrheit über den **EU AI Act**: Er wird massiv überschätzt, und um ihn herum ist eine Beratungsindustrie entstanden, die von dieser Überschätzung gut lebt. Die andere Hälfte: Wer tatsächlich KI für Personalauswahl, Kreditentscheidungen oder in Medizinprodukten baut, bekommt ein Pflichtenheft, das sich gewaschen hat – mit Risikomanagement, Daten-Governance, technischer Dokumentation, Konformitätsbewertung, CE-Kennzeichen und Registrierung. Für ein Start-up mit zwölf Leuten ist das kein Formular, sondern ein zweites Produkt.

Dieser Beitrag ist für IT-Leitungen, Geschäftsführungen und alle, die im Unternehmen am Ende unterschreiben müssen. Du erfährst, was der AI Act verpflichtend regelt, für wen welche Fristen gelten – inklusive der Verschiebungen durch die Omnibus-Verordnung –, was die Umsetzung wirklich kostet, welche Kostenschätzungen auf wackligen Rechenwegen stehen und wo die Kritik an Bürokratie und Innovationsbremse trifft. Und wo nicht. Der Titel verrät meine Grundhaltung; der Text versucht trotzdem, fair zu bleiben.

Fakten: Der EU AI Act auf einen Blick (Stand Oktober 2026)

- Verordnung (EU) 2024/1689, seit 1. August 2024 in Kraft und als Verordnung in allen Mitgliedstaaten unmittelbar geltend – es gibt kein nationales Umsetzungsgesetz, das die Pflichten abschwächen könnte.
- Verbote nach Art. 5 und die Pflicht zur KI-Kompetenz nach Art. 4 gelten seit 2. Februar 2025, die Regeln für General-Purpose-AI-Modelle seit 2. August 2025, die Transparenzpflichten nach Art. 50 seit 2. August 2026.
- Die Omnibus-Verordnung (EU) 2026/1744 ist seit 27. Juli 2026 in Kraft. Sie verschiebt die Hochrisiko-Pflichten auf den 2. Dezember 2027 (Anhang III) und den 2. August 2028 (Anhang I), entschärft Art. 4 und erweitert die Erleichterungen für KMU auf kleine Midcaps.
- In Deutschland ist seit 29. Juli 2026 das KI-Marktüberwachungs- und Innovationsförderungsgesetz (KI-MIG) in Kraft; zentrale Marktüberwachungsbehörde ist die Bundesnetzagentur.
- Bußgelder: bis 35 Mio. Euro oder 7 % des weltweiten Jahresumsatzes bei verbotenen Praktiken, bis 15 Mio. Euro oder 3 % bei den meisten übrigen Pflichten. Für KMU und kleine Midcaps gilt jeweils der niedrigere Wert.

Was der EU AI Act regelt: Risikoklassen, Einstufung und Zeitplan

Der AI Act reguliert nicht „die KI“, sondern Verwendungszwecke. Dasselbe Sprachmodell kann in einem Kochrezept-Chatbot harmlos und in einem Bewerber-Ranking hochriskant sein. Das ist die wichtigste Erkenntnis überhaupt, und sie erspart dir die meisten Diskussionen: Du fragst nicht „Ist Copilot hochriskant?“, sondern „Wofür setzen wir ihn ein?“.

Erst die Vorfrage: Ist das überhaupt ein KI-System?

Art. 3 Nr. 1 definiert ein KI-System als maschinengestütztes System, das mit einem gewissen Grad an Autonomie arbeitet und aus Eingaben ableitet, wie es Ausgaben wie Vorhersagen, Inhalte, Empfehlungen oder Entscheidungen erzeugt. Die Leitlinien der Kommission zur Definition vom Februar 2025 machen klar, was nicht darunter fällt: klassische regelbasierte Software, bei der ein Mensch jede Regel ausprogrammiert hat, einfache Statistik und mathematische Optimierung ohne Lernanteil. Dein Excel-Makro mit 300 verschachtelten WENN-Funktionen ist also kein KI-System. Es ist nur schlimm.

Spannend wird es bei Mischformen: Ein Workflow in Power Automate, der eine E-Mail per KI klassifiziert und dann nach festen Regeln weiterleitet, enthält ein KI-System – nämlich die Klassifikation. Für die Einstufung zählt, was die KI-Komponente im Gesamtprozess bewirkt.

Verbotene Praktiken nach Art. 5

Die Verbote gelten seit 2. Februar 2025 und sind der einzige Teil des AI Act, bei dem es keine Konformitätsbewertung, keine Dokumentation und keine Diskussion gibt. Verboten sind:

- **Manipulation und Ausnutzung von Schwächen:** unterschwellige oder täuschende Techniken sowie das gezielte Ausnutzen von Alter, Behinderung oder sozialer Notlage, wenn dadurch erheblicher Schaden droht.
- **Social Scoring:** Bewertung von Personen anhand ihres Sozialverhaltens oder ihrer Persönlichkeit mit nachteiliger Behandlung in sachfremden Zusammenhängen – nicht nur durch Behörden, sondern auch durch Unternehmen.

- **Vorhersage von Straftaten** allein auf Basis von Profiling oder Persönlichkeitsmerkmalen.
- **Ungezieltes Auslesen von Gesichtsbildern** aus dem Internet oder Videoüberwachung zum Aufbau von Gesichtserkennungsdatenbanken.
- **Emotionserkennung am Arbeitsplatz und in Bildungseinrichtungen**, außer aus medizinischen oder Sicherheitsgründen.
- **Biometrische Kategorisierung**, die auf ethnische Herkunft, politische Meinung, Gewerkschaftszugehörigkeit, Religion oder sexuelle Orientierung schließt.
- **Biometrische Echtzeit-Fernidentifizierung** im öffentlichen Raum zur Strafverfolgung, mit eng begrenzten Ausnahmen.
- **Neu durch die Omnibus-Verordnung, ab 2. Dezember 2026:** KI-Systeme, die intime oder sexuell explizite Bilder erkennbarer Personen ohne deren ausdrückliche Einwilligung erzeugen, sowie KI zur Erzeugung von Darstellungen sexuellen Kindesmissbrauchs.

Für die meisten Unternehmen ist genau ein Punkt praxisrelevant, und der wird regelmäßig übersehen: die Emotionserkennung am Arbeitsplatz. Ich habe Callcenter-Software gesehen, die „Stimmungsanalyse“ nicht nur für die Kundschaft, sondern auch für die Agentinnen und Agenten am Telefon anbot. Die Kundenseite ist zulässig (mit Transparenzpflicht), die Mitarbeiterseite ist seit Februar 2025 schlicht verboten. Die Funktion stand im Admin-Menü auf „ein“.

Warnung: Verbotene Funktionen verstecken sich in Standardsoftware

Prüfe bei Contact-Center-, HR- und Videokonferenz-Lösungen ausdrücklich, ob Funktionen zur Emotions- oder Stimmungserkennung für die eigene Belegschaft aktiviert sind. Der Verstoß liegt beim Betreiber, der die Funktion einsetzt – nicht nur beim Hersteller, der sie anbietet. Bußgeldrahmen: bis 35 Mio. Euro oder 7 % des Jahresumsatzes.

Hochrisiko-Systeme nach Anhang I und Anhang III

Der AI Act kennt zwei Wege in die Hochrisiko-Klasse, und sie funktionieren völlig unterschiedlich.

Anhang I – KI in regulierten Produkten. Ist ein KI-System selbst ein Produkt oder ein Sicherheitsbauteil eines Produkts, das unter EU-Harmonisierungsrecht fällt – Medizinprodukte, Maschinen, Spielzeug, Aufzüge, Funkanlagen – und muss dieses Produkt von einer externen Stelle geprüft werden, ist die KI hochriskant. Die Omnibus-Verordnung hat den Begriff „Sicherheitsbauteil“ enger gefasst: Eine KI, die nur Komfort- oder Qualitätskontrollzwecken dient und deren Ausfall niemanden gefährdet, ist kein Sicherheitsbauteil. Die Bilderkennung, die Kratzer auf Blechteilen findet, ist also kein Hochrisiko-System, die Kamera, die den Roboterarm stoppt, wenn ein Mensch in die Zelle greift, schon. Außerdem wurde die Maschinenverordnung in Abschnitt B von Anhang I verschoben; KI-Anforderungen kommen dort künftig über delegierte Rechtsakte der Maschinenverordnung selbst.

Anhang III – eigenständige Systeme in sensiblen Bereichen. Hier entscheidet der Einsatzzweck. Anhang III listet acht Bereiche:

Bereich (Anhang III)	Typisch hochriskant	Typisch nicht hochriskant
1 Biometrie	Fernidentifizierung, Emotionserkennung (wo erlaubt), biometrische Kategorisierung	Face-ID zum Entsperren des Diensthandys (reine Verifizierung)
2 Kritische Infrastruktur	Sicherheitsbauteile in Steuerung von Strom-, Gas-, Wasser-, Wärmenetzen, Verkehr	Lastprognose für die Kantine

Bereich (Anhang III)	Typisch hochriskant	Typisch nicht hochriskant
3 Bildung	Zulassung, Bewertung von Prüfungen, Erkennung von Täuschung bei Prüfungen	Lernassistent, der Übungsaufgaben erklärt
4 Beschäftigung und Personal	Ausschreibung gezielt schalten, Bewerbungen filtern und bewerten, Beförderung, Kündigung, Aufgabenzuweisung nach Verhalten, Leistungsüberwachung	Copilot formuliert eine Stellenanzeige, die ein Mensch freigibt
5 Wesentliche Dienste	Kreditwürdigkeit, Risiko- und Preisbildung in Lebens- und Krankenversicherung, Sozialleistungen, Triage von Notrufen	Betrugserkennung bei Zahlungen (ausdrücklich ausgenommen)
6 Strafverfolgung	Beweiswürdigung, Rückfallrisiko, Lügendetektoren	–
7 Migration, Asyl, Grenze	Risikobewertung, Prüfung von Anträgen	–
8 Justiz und Demokratie	Unterstützung richterlicher Entscheidungen, Beeinflussung von Wahlen	Kampagnen-Logistik ohne Kontakt zu Wählerinnen und Wählern

Für Unternehmen außerhalb von Banken, Versicherungen und Behörden ist Bereich 4 der eigentliche Elefant im Raum. Jede KI, die über Menschen in einem Arbeitsverhältnis mitentscheidet, landet dort – vom CV-Parser mit Ranking bis zum Agenten, der Schichtpläne nach „Zuverlässigkeit“ verteilt.

Die Ausnahme nach Art. 6 Abs. 3 – und warum du sie dokumentieren musst

Ein System aus Anhang III ist nicht hochriskant, wenn es kein erhebliches Risiko für Gesundheit, Sicherheit oder Grundrechte birgt und eine von vier Bedingungen erfüllt: Es erledigt eine eng begrenzte Verfahrensaufgabe, es verbessert das Ergebnis einer bereits abgeschlossenen menschlichen Tätigkeit, es erkennt Entscheidungsmuster oder Abweichungen, ohne die menschliche Bewertung zu ersetzen, oder es erledigt eine vorbereitende Aufgabe. Ein Tool, das eingegangene Bewerbungen nur nach Sprache sortiert, kann darunter fallen. Eines, das sie nach Eignung sortiert, nicht.

Die harte Grenze: **Profiling natürlicher Personen ist immer hochriskant.** Und die Ausnahme ist kein Freifahrtschein. Wer sich darauf beruft, muss die Bewertung vor dem Inverkehrbringen dokumentieren und das System trotzdem in der EU-Datenbank registrieren. Die Kommission wollte diese Registrierung mit der Omnibus-Verordnung streichen; Parlament und Rat haben sie behalten, aber die Pflichtangaben verschlankt.

Wichtig: Wer die Einstufung vornimmt

Niemand genehmigt deine Einstufung vorab. Der Anbieter stuft in eigener Verantwortung ein, der Betreiber prüft, ob sein Einsatzzweck dazu passt. Die Marktüberwachung – in Deutschland die Bundesnetzagentur – kann die Einstufung nach Art. 80 überprüfen, eine Neueinstufung verlangen und bei bewusster Fehleinstufung Bußgelder verhängen. Eine sauber begründete Einstufung, die du heute schreibst, ist deshalb dein wichtigstes Dokument im ganzen AI-Act-

Projekt.

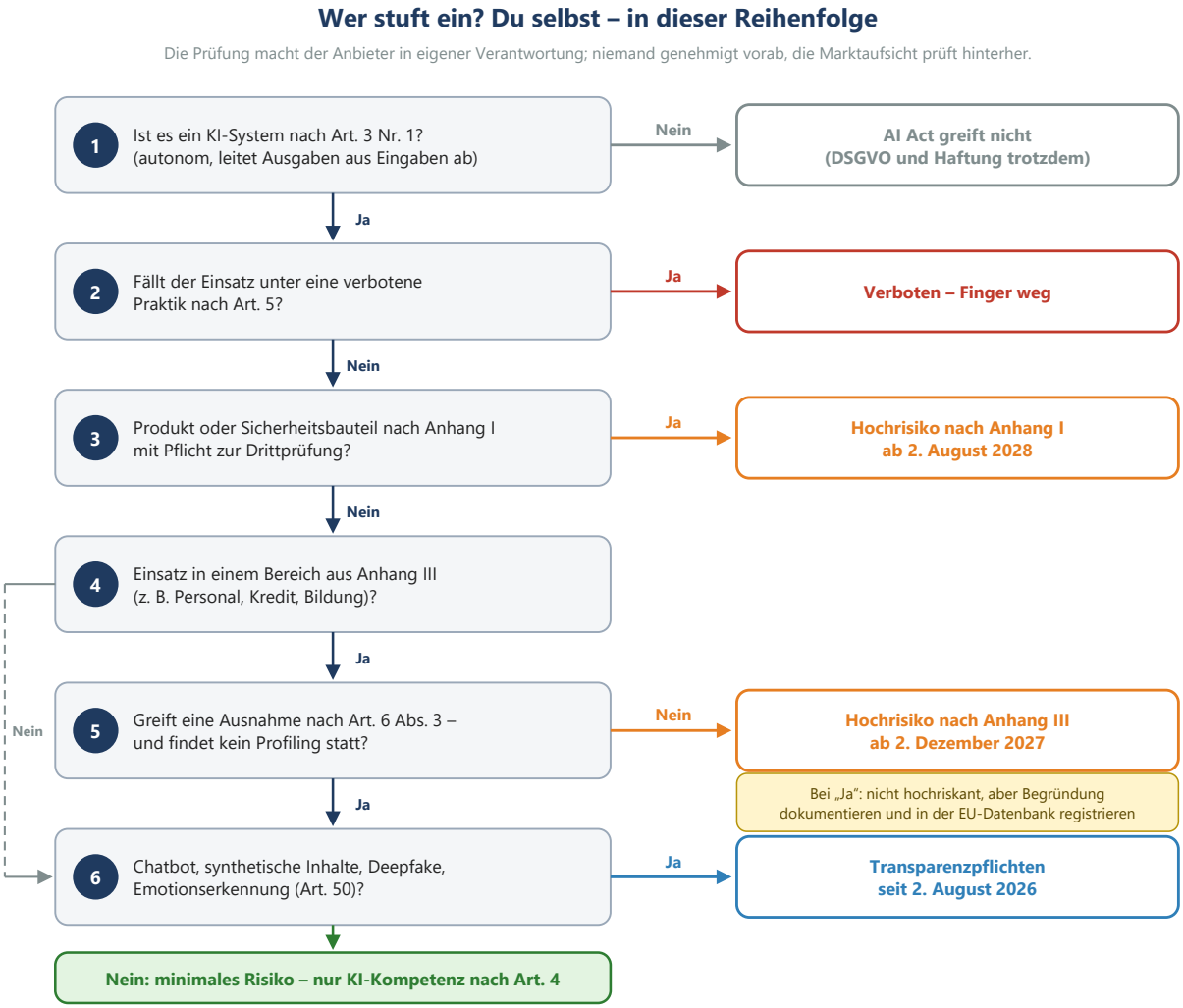


Abbildung 1: Prüfreihenfolge zur Einstufung eines KI-Systems: Definition, Verbote, Anhang I, Anhang III mit Ausnahme nach Art. 6 Abs. 3, Transparenzpflichten

Transparenzpflichten und minimales Risiko

Seit 2. August 2026 gelten die Transparenzpflichten nach Art. 50. Sie sind die Pflichten, die die meisten Unternehmen tatsächlich treffen, und sie sind überschaubar:

- **Chatbots und KI-Assistenten** müssen erkennbar machen, dass man mit einer KI spricht – es sei denn, das ist aus dem Kontext offensichtlich. Pflicht des Anbieters, im Kundenportal aber faktisch deine.
- **Synthetische Inhalte** (Text, Bild, Audio, Video) müssen vom Anbieter des generierenden Systems maschinenlesbar gekennzeichnet werden. Für generative Systeme, die vor dem 2. August 2026 auf dem Markt waren, läuft dafür eine Übergangsfrist bis 2. Dezember 2026.
- **Deepfakes** muss der Betreiber offenlegen, bei erkennbar künstlerischen oder satirischen Werken in abgeschwächter Form. KI-generierte Texte zu Angelegenheiten von öffentlichem Interesse brauchen einen Hinweis, sofern sie nicht redaktionell geprüft und verantwortet werden.
- **Emotionserkennung und biometrische Kategorisierung**, soweit erlaubt, erfordern die Information der betroffenen Personen.

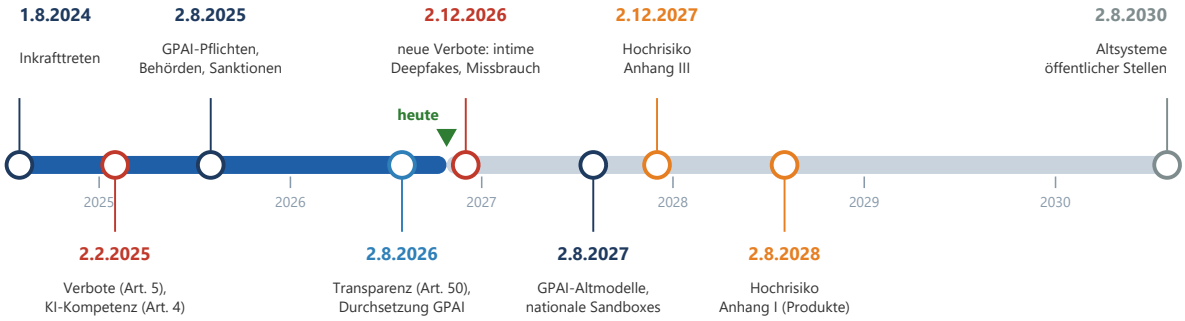
Alles andere – Spamfilter, Übersetzung, Textzusammenfassung, Codevervollständigung, Copilot im Büroalltag – fällt unter minimales Risiko. Dafür gibt es keine eigenen Pflichten, mit einer Ausnahme, die für alle gilt: KI-Kompetenz nach Art. 4. Dazu unten mehr.

Risikoklasse	Beispiel	Abgrenzungsfall	Pflichten	Gilt seit/ab
Verboten (Art. 5)	Emotionserkennung im Callcenter für die Belegschaft	Stimmungsanalyse der Kundschaft: erlaubt, aber transparent machen	Einsatz unzulässig	2.2.2025
Hochrisiko Anhang III	Bewerber-Ranking, Kredit-Scoring	Sortierung nach Sprache: Ausnahme Art. 6 Abs. 3 möglich	Art. 9–15, Konformität, Registrierung	2.12.2027
Hochrisiko Anhang I	KI-Diagnose als Medizinprodukt, Not-Halt-Erkennung an Maschinen	Kratzererkennung in der Qualitätskontrolle	wie oben, über Sektorrecht	2.8.2028
Transparenz (Art. 50)	Website-Chatbot, Bildgenerator, Deepfake-Werbespot	interner Copilot-Entwurf, den ein Mensch verantwortet	Kennzeichnung, Hinweis	2.8.2026
Minimal	Spamfilter, Übersetzung, Copilot im Büro	–	nur KI-Kompetenz (Art. 4)	2.2.2025

Der Zeitplan nach der Omnibus-Verordnung

Der AI Act wird gestaffelt anwendbar, und die Staffel hat sich 2026 noch einmal verschoben. Ursprünglich sollten die Hochrisiko-Pflichten für Anhang-III-Systeme ab 2. August 2026 gelten. Weil die harmonisierten Normen von CEN und CENELEC nicht rechtzeitig fertig wurden und viele Mitgliedstaaten ihre Behörden noch nicht aufgestellt hatten, schlug die Kommission im November 2025 im Rahmen ihres Digital-Omnibus-Pakets eine Verschiebung vor. Ihr Vorschlag koppelte den Starttermin an die Verfügbarkeit von Normen – mit Höchstfristen. Parlament und Rat haben daraus feste Termine gemacht: Das Parlament stimmte am 16. Juni 2026 zu, der Rat am 29. Juni, die Verordnung (EU) 2026/1744 ist seit 27. Juli 2026 in Kraft.

Zeitplan des EU AI Act nach der Omnibus-Verordnung (EU) 2026/1744



Ursprünglich sollten Anhang-III-Systeme ab 2.8.2026 und Anhang-I-Produkte ab 2.8.2027 erfasst werden. Die Omnibus-Verordnung (in Kraft seit 27.7.2026) hat diese Termine fest verschoben – nicht gestrichen.

Abbildung 2: Gestaffelte Anwendung des EU AI Act mit den durch die Omnibus-Verordnung verschobenen Hochrisiko-Terminen

Termin	Was gilt	Wen es trifft
2.2.2025	Verbote nach Art. 5, KI-Kompetenz nach Art. 4	alle Anbieter und Betreiber
2.8.2025	Pflichten für GPAI-Modelle, Governance, Sanktionsregeln der Mitgliedstaaten	Modellanbieter, Behörden
2.8.2026	Transparenzpflichten nach Art. 50; Durchsetzungsbefugnisse des KI-Büros gegenüber GPAI-Anbietern	Chatbot-Betreiber, Anbieter generativer KI, Modellanbieter
2.12.2026	neue Verbote (nicht einvernehmliche intime Bilder, Missbrauchsdarstellungen); Ende der Übergangsfrist für Kennzeichnung bei generativen Altsystemen	Anbieter generativer KI
2.8.2027	GPAI-Modelle, die vor dem 2.8.2025 auf dem Markt waren, müssen konform sein; jeder Mitgliedstaat betreibt mindestens ein KI-Reallabor	Modellanbieter, Behörden
2.12.2027	Hochrisiko-Pflichten für Anhang-III-Systeme	Anbieter und Betreiber, z. B. HR, Kredit, Bildung
2.8.2028	Hochrisiko-Pflichten für KI in Produkten nach Anhang I	Hersteller regulierter Produkte
2.8.2030	Hochrisiko-Altsysteme öffentlicher Stellen müssen konform sein	Behörden

Was viele übersehen: Verschoben wurde der Termin, nicht die Anforderung. Ein Bewerbermanagement mit KI-Ranking, das du 2027 einführst, musst du heute schon so auswählen, dass der Anbieter bis Dezember 2027 eine Konformitätserklärung liefern kann. Für Systeme, die vor dem Stichtag in Verkehr gebracht wurden, gilt eine Bestandsschutzregel nach Art. 111: Sie bleiben außen vor, bis sie wesentlich geändert werden. Die Omnibus-Verordnung stellt klar, dass es auf das erste Exemplar eines Typs ankommt – baugleiche Einheiten dürfen weiter verkauft werden, jede wesentliche Designänderung löst die vollen Pflichten aus.

Hochrisiko-KI: Pflichten, Rollen und Konformitätsbewertung

Wenn dein System hochriskant ist, beginnt die eigentliche Arbeit. Und hier ist die Kritik am AI Act am berechtigtsten, weil die Anforderungen für sich genommen vernünftig klingen, in ihrer Summe aber ein Projekt erzeugen, das gerade kleine Anbieter überfordert.

Die Anforderungen nach Art. 9 bis 15

Pflicht	Was konkret verlangt wird	Was in der Praxis Aufwand treibt
Risikomanagement (Art. 9)	Kontinuierlicher Prozess über den gesamten Lebenszyklus: Risiken für Gesundheit, Sicherheit, Grundrechte erkennen, bewerten, mindern, Restrisiko begründen, testen	Grundrechtsrisiken sind für Technikteams Neuland; ohne Normen fehlt der Maßstab, wann es „genug“ ist
Daten-Governance (Art. 10)	Trainings-, Validierungs- und Testdaten relevant, repräsentativ, möglichst fehlerfrei; Prüfung auf Verzerrungen; dokumentierte	Bias-Prüfung braucht oft sensible Daten – die Omnibus-Verordnung schafft dafür

Pflicht	Was konkret verlangt wird	Was in der Praxis Aufwand treibt
	Herkunft	mit Art. 4a eine Rechtsgrundlage
Technische Dokumentation (Art. 11, Anhang IV)	Zweck, Architektur, Daten, Metriken, Tests, Änderungen, Aufsichtsmaßnahmen; Aufbewahrung zehn Jahre	Wird nachträglich geschrieben statt nebenbei erzeugt; KMU und kleine Midcaps dürfen ein vereinfachtes Formular nutzen
Protokollierung (Art. 12)	Automatische Aufzeichnung von Ereignissen zur Rückverfolgbarkeit, Aufbewahrung beim Anbieter mindestens sechs Monate	Logging-Konzept muss Datenschutz und Nachweiszweck gleichzeitig bedienen
Transparenz für Betreiber (Art. 13)	Gebrauchsanweisung mit Leistungsgrenzen, bekannten Risiken, Aufsichtsmaßnahmen	Ehrliche Grenzen aufzuschreiben fällt dem Vertrieb schwer
Menschliche Aufsicht (Art. 14)	Mensch kann Ausgaben verstehen, ignorieren, übersteuern, System stoppen; Schutz vor Automatisierungsgläubigkeit	Ein Freigabe-Klick ist keine Aufsicht – Zeit und Befugnis müssen real sein
Genauigkeit, Robustheit, Cybersicherheit (Art. 15)	Angemessene Genauigkeit mit erklärten Metriken, Resilienz gegen Fehler und Angriffe wie Datenvergiftung oder Prompt Injection	Wer den Cyber Resilience Act erfüllt, gilt nach der Omnibus-Verordnung insoweit als konform
Qualitätsmanagement (Art. 17)	Dokumentiertes QMS für Entwicklung, Test, Änderungen, Vorfälle	Skaliert seit der Omnibus-Verordnung nach Unternehmensgröße; KMU ohne Partnerunternehmen dürfen Teile vereinfachen

Ein Satz aus einem Projekt bei einem HR-Software-Anbieter ist mir hängen geblieben. Der Entwicklungsleiter sagte nach dem ersten Workshop: „Das meiste davon hätten wir machen sollen, auch ohne Gesetz. Wir hätten es nur nicht aufgeschrieben." Genau da liegt der Kern: Ein großer Teil des Hochrisiko-Katalogs ist ordentliches Software-Engineering. Der Aufwand entsteht durch den Nachweis – und durch die Unsicherheit, welcher Nachweis reicht.

Anbieter oder Betreiber – und wann du unfreiwillig Anbieter wirst

Der AI Act verteilt die Pflichten nach Rollen. **Anbieter** ist, wer ein KI-System entwickelt oder entwickeln lässt und unter eigenem Namen in Verkehr bringt oder in Betrieb nimmt – auch für den eigenen Gebrauch. **Betreiber** ist, wer ein KI-System in eigener Verantwortung beruflich einsetzt. Daneben gibt es Einführer und Händler mit Prüfpflichten in der Lieferkette.

Die meisten Unternehmen sind Betreiber. Ihre Pflichten nach Art. 26 sind deutlich schlanker: das System nach Gebrauchsanweisung nutzen, menschliche Aufsicht durch Personen mit Kompetenz und Befugnis sicherstellen, Eingabedaten im eigenen Verantwortungsbereich relevant halten, den Betrieb überwachen, Logs mindestens sechs Monate aufbewahren, Vorfälle melden, die Belegschaft und ihre Vertretung vor dem Einsatz am Arbeitsplatz informieren und betroffene Personen darüber aufklären, dass eine Hochrisiko-KI über sie mitentscheidet. Öffentliche Stellen, private Anbieter öffentlicher Dienste sowie Betreiber von Kredit-Scoring und Versicherungs-Tarifierung müssen zusätzlich eine Grundrechte-Folgenabschätzung nach Art. 27 erstellen, die auf eine vorhandene Datenschutz-Folgenabschätzung verweisen darf.

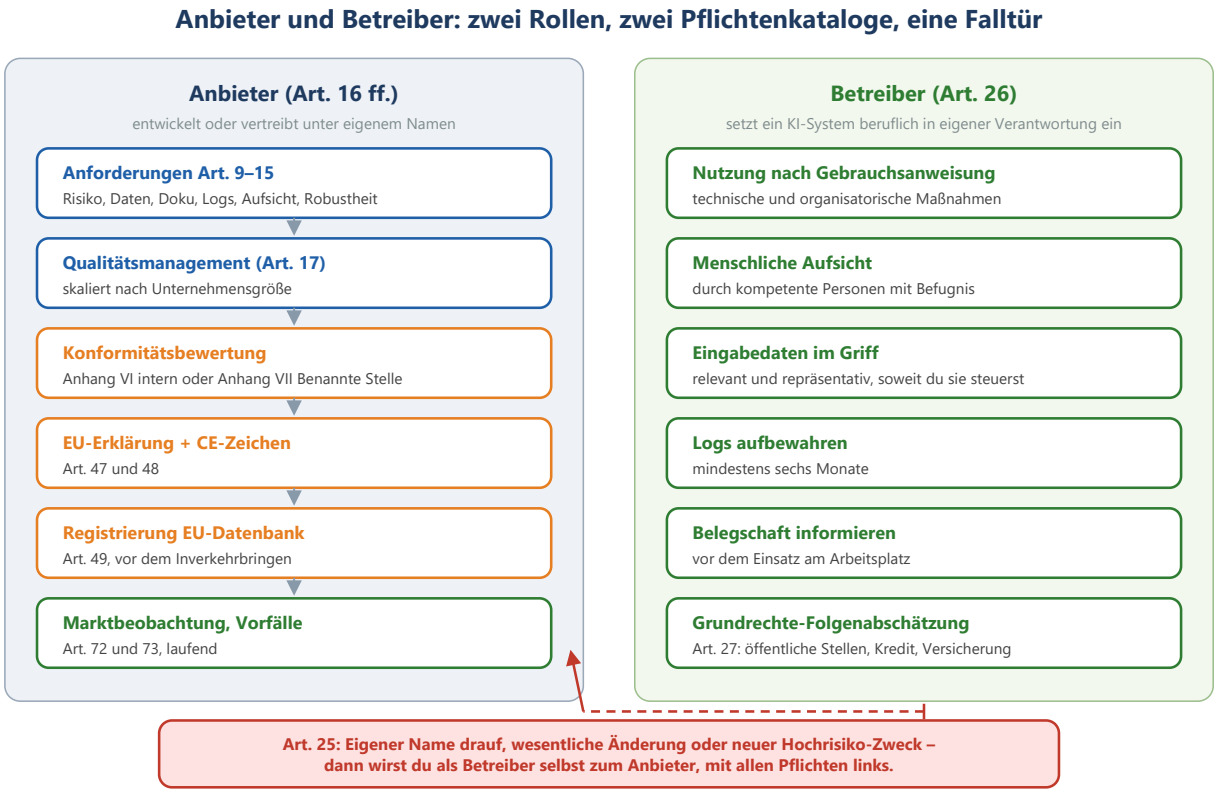


Abbildung 3: Pflichten von Anbieter und Betreiber einer Hochrisiko-KI und der Rollenwechsel nach Art. 25

Die Falltür heißt Art. 25. Du wirst als Betreiber selbst zum Anbieter, wenn du ein Hochrisiko-System unter eigenem Namen oder eigener Marke anbietest, wenn du es wesentlich veränderst oder wenn du den Zweck eines nicht hochriskanten Systems so änderst, dass es hochriskant wird. Letzteres ist der Klassiker: Ein Copilot-Agent, der eigentlich Fragen zur Reisekostenrichtlinie beantworten sollte, bekommt von einem engagierten Personaler den Auftrag „Bewerte diese 40 Lebensläufe und sag mir die besten fünf“. Herzlichen Glückwunsch, ihr habt gerade ein Hochrisiko-System in Betrieb genommen und seid dessen Anbieter. Ab Dezember 2027 mit allen Pflichten.

Warnung: Zweckänderung durch die Hintertür

Allgemeine Assistenten wie Microsoft 365 Copilot, ChatGPT Enterprise oder selbst gebaute Agenten sind nicht hochriskant – bis jemand sie für einen Zweck aus Anhang III einsetzt. Leg in der Nutzungsrichtlinie fest, welche Zwecke ausgeschlossen sind (Bewerberauswahl, Leistungsbewertung, Kündigungsvorbereitung), und schule genau diese Grenze. Bei Agenten gehört der zulässige Zweck in die Freigabe – siehe Copilot-Agenten in der Praxis.

Konformitätsbewertung: Anhang VI oder Anhang VII

Bevor ein Hochrisiko-System auf den Markt darf, muss der Anbieter die Konformität nachweisen. Die gute Nachricht, die in der öffentlichen Debatte regelmäßig untergeht: **Für die allermeisten Anhang-III-Systeme reicht die interne Kontrolle nach Anhang VI.** Keine Benannte Stelle, kein Gutachterhonorar, keine Wartezeit auf einen Prüftermin. Der Anbieter prüft sein QMS und seine technische Dokumentation selbst und steht mit seiner Unterschrift dafür ein.

Merkmal	Interne Kontrolle (Anhang VI)	Benannte Stelle (Anhang VII)	Sektorales Verfahren (Anhang I)

Merkmal	Interne Kontrolle (Anhang VI)	Benannte Stelle (Anhang VII)	Sektorales Verfahren (Anhang I)
Gilt für	Anhang III Nr. 2 bis 8 (Infrastruktur, Bildung, Personal, Kredit …)	Anhang III Nr. 1 Biometrie, wenn harmonisierte Normen nicht oder nur teilweise angewandt werden	KI in Medizinprodukten, Maschinen, Spielzeug usw.
Wer prüft	Anbieter selbst	externe, notifizierte Prüforganisation	die nach Sektorrecht zuständige Stelle
Prüfgegenstand	QMS und technische Dokumentation	QMS-Audit und Prüfung der Dokumentation	Produktprüfung inklusive KI-Anforderungen
Aufwand	intern, Personentage bis Personenmonate	zusätzlich Honorar und Terminvorlauf	fällt ohnehin an, wird um KI-Teil erweitert
Ergebnis	EU-Konformitätserklärung, CE	Bescheinigung, EU-Konformitätserklärung, CE	eine gemeinsame Erklärung für Produkt und KI

Für Anhang-I-Produkte bleibt es beim gewohnten Verfahren der Produktgesetzgebung. Die Omnibus-Verordnung stellt klar, dass ein Hersteller nicht allein deshalb in eine Drittprüfung gezwungen wird, weil sein Produkt eine Hochrisiko-KI-Komponente enthält, und sie schafft ein gemeinsames Antragsverfahren für Prüfstellen, die sowohl nach Sektorrecht als auch nach AI Act benannt werden wollen. Der Engpass sind die Benannten Stellen selbst: Es gibt schlicht zu wenige mit KI-Kompetenz, und wer schon einmal auf einen Termin bei einer Medizinprodukte-Prüfstelle gewartet hat, ahnt, wohin das führt.

CE-Kennzeichnung, Konformitätserklärung und EU-Datenbank

Am Ende der Bewertung stehen drei formale Schritte. Der Anbieter stellt eine **EU-Konformitätserklärung** nach Art. 47 aus und hält sie zehn Jahre bereit. Er bringt die **CE-Kennzeichnung** nach Art. 48 an – bei Software digital, etwa in der Oberfläche oder der Dokumentation. Und er **registriert** das System nach Art. 49 vor dem Inverkehrbringen in der EU-Datenbank, die die Kommission betreibt. Öffentliche Stellen registrieren zusätzlich ihre Nutzung als Betreiber. Systeme aus den Bereichen Strafverfolgung, Migration und Grenze landen in einem nicht öffentlichen Teil der Datenbank. Nach dem Marktstart folgen Marktbeobachtung nach Art. 72 und die Meldung schwerwiegender Vorfälle nach Art. 73.

General-Purpose-AI-Modelle und Open Source

Die großen Sprachmodelle – GPT, Claude, Gemini, Llama, Mistral und Co. – regelt der AI Act nicht als KI-System, sondern eine Ebene tiefer als **KI-Modell mit allgemeinem Verwendungszweck** (General Purpose AI, GPAI). Die Pflichten gelten seit 2. August 2025, die Durchsetzung durch das KI-Büro der Kommission mit Bußgeldern bis 15 Mio. Euro oder 3 % des Jahresumsatzes seit 2. August 2026. Modelle, die vor August 2025 auf dem Markt waren, haben bis 2. August 2027 Zeit. Welche Modelle gerade wo stehen, beschreibt das Q1-2026-Update der großen LLMs – Chancen, Risiken, Konsequenzen für Unternehmen.

Pflichten für alle GPAI-Anbieter

- **Technische Dokumentation** des Modells für das KI-Büro und die zuständigen Behörden (Anhang XI): Architektur, Training, Rechenaufwand, Energieverbrauch, Evaluierung.
- **Informationen für nachgelagerte Anbieter** (Anhang XII), damit die, die das Modell in ihre Systeme einbauen, ihre eigenen Pflichten erfüllen können.

- **Urheberrechts-Strategie:** Der Anbieter muss eine Policy zur Einhaltung des EU-Urheberrechts haben und insbesondere maschinenlesbare Nutzungsvorbehalte von Rechteinhabern gegen Text- und Data-Mining respektieren.
- **Zusammenfassung der Trainingsdaten:** öffentlich, nach einer Vorlage, die die Kommission im Juli 2025 veröffentlicht hat. Keine Liste aller Dateien, aber die wichtigsten Datensammlungen und Quellenarten.

Die Urheberrechtspflicht ist politisch der heißeste Teil. Sie verlangt keine Lizenz für jedes Trainingsdokument, aber sie zwingt Anbieter, Opt-outs von Verlagen und Plattformen technisch zu beachten und nachzuweisen, wie sie das tun. Wer einen Robots-Vorbehalt ignoriert, hat seit 2025 nicht nur ein Urheberrechts-, sondern auch ein AI-Act-Problem.

Systemisches Risiko: die Schwelle von 10 hoch 25

Ein GPAI-Modell gilt als Modell mit systemischem Risiko, wenn es Fähigkeiten mit hoher Wirkung hat. Vermutet wird das ab einem Trainingsaufwand von mehr als 10 hoch 25 Gleitkommaoperationen; die Kommission kann Modelle auch unterhalb der Schwelle anhand von Kriterien wie Reichweite und Fähigkeiten einstufen. Zusätzliche Pflichten nach Art. 55: Modellevaluierung nach dem Stand der Technik einschließlich Adversarial Testing, Bewertung und Minderung systemischer Risiken, Meldung schwerwiegender Vorfälle an das KI-Büro und angemessene Cybersicherheit für Modell und Infrastruktur. Das betrifft eine Handvoll Anbieter weltweit, nicht dein Unternehmen – es sei denn, du trainierst gerade dein eigenes Frontier-Modell. Dann hast du andere Sorgen.

Der Verhaltenskodex für GPAI

Weil harmonisierte Normen für Modelle fehlen, hat das KI-Büro mit Industrie, Wissenschaft und Zivilgesellschaft einen Verhaltenskodex erarbeitet, veröffentlicht im Juli 2025. Er hat drei Kapitel: Transparenz, Urheberrecht sowie Sicherheit und Schutz, letzteres nur für Modelle mit systemischem Risiko. Wer ihn unterzeichnet, kann damit die Erfüllung seiner Pflichten belegen; wer nicht unterzeichnet, muss gleichwertige Maßnahmen anders nachweisen und rechnet mit genauerer Prüfung. Unterzeichnet haben unter anderem Microsoft, Google, OpenAI, Anthropic, Amazon, IBM, Mistral und Aleph Alpha. Meta hat abgelehnt, xAI hat nur das Sicherheitskapitel unterschrieben.

Für dich als Betreiber ist das ein brauchbares Auswahlkriterium: Ein Modellanbieter, der den Kodex unterzeichnet hat, liefert in der Regel die Dokumentation, die du für deine eigene Einstufung brauchst. Wie sich die Plattformen in Datenschutz, Hosting und Vertragslage unterscheiden, steht im Überblick über generative KI-Plattformen.

Open-Source-Ausnahmen und ihre Grenzen

Der AI Act privilegiert freie und quelloffene Software an zwei Stellen. KI-Systeme unter freier Lizenz sind nach Art. 2 Abs. 12 grundsätzlich ausgenommen. GPAI-Modelle unter freier Lizenz, deren Gewichte, Architektur und Nutzungsinformationen öffentlich sind, sind nach Art. 53 Abs. 2 von der technischen Dokumentation und den Informationen für nachgelagerte Anbieter befreit. Klingt großzügig, hat aber Grenzen:

Situation	Ausnahme greift?	Was bleibt
Freies KI-System, minimales Risiko	ja	nichts aus dem AI Act; Urheber- und Datenschutzrecht gelten
Freies KI-System für Hochrisiko-Zweck	nein	volle Hochrisiko-Pflichten für den, der es in Verkehr

Situation	Ausnahme greift?	Was bleibt
		bringt
Freies KI-System mit verbotener Praktik	nein	Verbot
Freies KI-System mit Art.-50-Bezug (Chatbot, Generator)	nein	Transparenzpflichten
Freies GPAI-Modell ohne systemisches Risiko	teilweise	Urheberrechts-Policy und Trainingsdaten-Zusammenfassung bleiben Pflicht
Freies GPAI-Modell mit systemischem Risiko	nein	alle Pflichten inklusive Art. 55
Modell gegen Entgelt, mit Pflicht-Support oder Bezahlung durch Nutzerdaten	nein	gilt als monetarisiert, keine Open-Source-Privilegierung

Für Community-Projekte heißt das: Wer eine Bibliothek, ein Werkzeug oder ein kleines Modell veröffentlicht, ist weitgehend raus. Der AI Act schützt außerdem Entwicklerinnen und Entwickler freier Komponenten: Die Pflicht, nachgelagerten Anbietern Informationen zu liefern (Art. 25 Abs. 4), gilt nicht für freie Werkzeuge und Komponenten außer GPAI-Modellen. Die Pflichten treffen den, der aus freien Bausteinen ein Hochrisiko-Produkt macht – und das ist richtig so. Problematisch bleibt die Grauzone der Monetarisierung: Ein Projekt, das sich über kostenpflichtigen Enterprise-Support finanziert, kann die Privilegierung verlieren. Hier hätte der Gesetzgeber klarer sein können, und die Abschreckungswirkung auf kleine europäische Modellprojekte ist real, wenn auch kleiner als in vielen Kommentaren behauptet.

Tipp: Feinabstimmung macht dich nicht automatisch zum Modellanbieter

Wer ein offenes Modell mit eigenen Daten feinabstimmt, wird nach den GPAI-Leitlinien der Kommission erst dann selbst zum Anbieter eines GPAI-Modells, wenn die Änderung erheblich ist – als Richtwert gilt ein Rechenaufwand von mehr als einem Drittel des ursprünglichen Trainings. Ein LoRA-Adapter für deine Ticketklassifikation liegt Größenordnungen darunter. Deine Pflichten ergeben sich dann aus dem Zweck des Systems, das du daraus baust.

Kosten, KMU und die Frage nach Schaden und Nutzen

Kommen wir zum Titel. Ist der AI Act „viel Schaden, wenig Nutzen“? Um das zu beantworten, muss man die Zahlen anschauen, mit denen in der Debatte argumentiert wird. Und da wird es unangenehm – für beide Seiten.

Woher die Horrorzahlen kommen

Die meistzitierte Zahl lautet: Der AI Act verteuert KI-Projekte um 17 Prozent und kostet die europäische Wirtschaft rund 31 Mrd. Euro in fünf Jahren. Sie stammt aus einer Studie des Center for Data Innovation von 2021. Die Herleitung: Die Folgenabschätzung der Kommission rechnete für ein typisches Hochrisiko-System im Entwicklungswert von rund 170.000 Euro mit Compliance-Kosten, die sich auf bis zu etwa 17 Prozent dieses Werts summieren. Die Studie hat diesen Prozentsatz dann auf die gesamten KI-Investitionen in Europa angewandt.

Der Fehler ist offensichtlich, wenn man ihn einmal gesehen hat: Die Kommission ging davon aus, dass nur etwa 5 bis 15 Prozent aller KI-Anwendungen hochriskant sind. Für die übrigen 85 bis 95 Prozent fallen diese Kosten nicht an. Wer 17 Prozent auf den ganzen Markt rechnet, überschätzt die Gesamtbelastung grob um den Faktor sieben bis zwanzig. Das Brüsseler Forschungsinstitut CEPS, das an der Kostenstudie für die Kommission mitgearbeitet hatte, hat die Rechnung damals öffentlich zurückgewiesen.

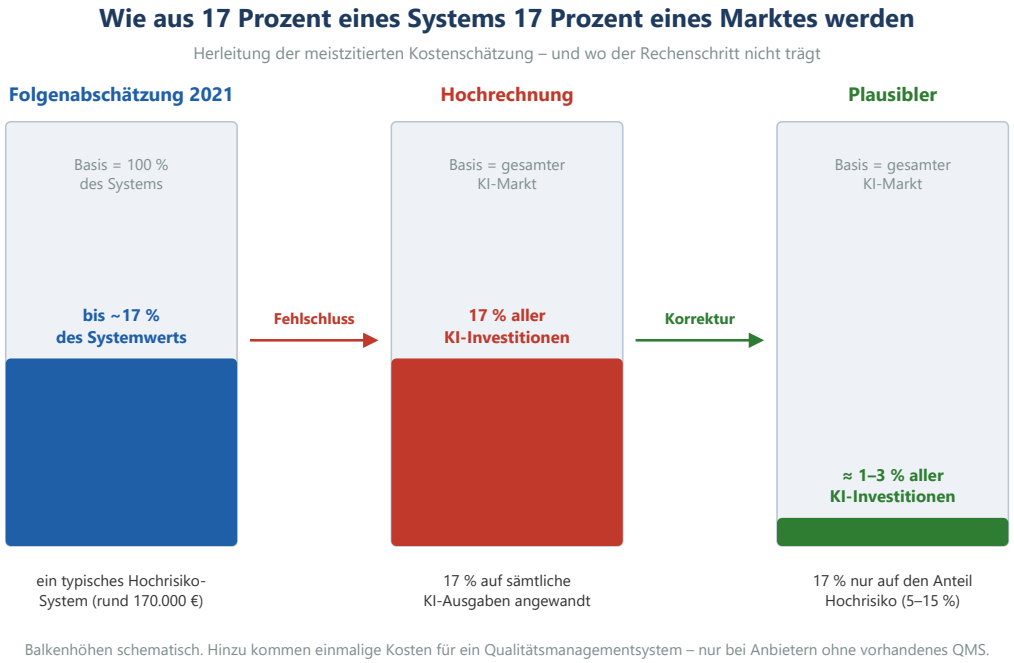


Abbildung 4: Der Rechenschritt hinter der 17-Prozent-Schätzung: richtig für ein einzelnes Hochrisiko-System, falsch als Aufschlag auf alle KI-Investitionen

Die zweite Zahl, die durch Präsentationen geistert: bis zu 400.000 Euro für ein Hochrisiko-System in einem KMU, angeblich rund 40 Prozent des Jahresgewinns. Sie setzt die einmaligen Kosten für den Aufbau eines Qualitätsmanagementsystems – in der Begleitstudie zur Folgenabschätzung mit rund 193.000 bis 330.000 Euro angesetzt – plus laufende Kosten in eine Rechnung, als müsste jedes Unternehmen sein QMS bei null beginnen und für jedes System neu aufbauen. Ein Medizintechnik-Hersteller hat sein QMS seit Jahren nach ISO 13485, ein Software-Haus mit ISO 27001 hat das Gerüst. Das QMS entsteht einmal pro Unternehmen, nicht einmal pro System.

Ebenfalls oft zitiert: eine Umfrage der appliedAI-Initiative unter europäischen KI-Start-ups von Ende 2022. Rund die Hälfte erwartete eine Bremswirkung, 16 Prozent erwogen, ihre KI-Entwicklung einzustellen oder außerhalb der EU fortzuführen. Das ist ein ernstzunehmendes Stimmungsbild – aber es wurde zu einem Zeitpunkt erhoben, als ein erheblicher Teil der Befragten seine eigene Risikoklasse nicht kannte. Etwa ein Drittel ordnete sich damals selbst als hochriskant ein; nach der Systematik der finalen Verordnung wäre der Anteil deutlich kleiner gewesen.

Fakten: Was die Kostenschätzungen tatsächlich messen

- Kosten pro Hochrisiko-System: plausibel im mittleren fünfstelligen Bereich pro Jahr für Dokumentation, Aufsicht und Prüfung, wenn Grundstrukturen existieren.
- Einmalige QMS-Kosten: hoch, aber pro Unternehmen und nur bei Anbietern ohne bestehendes QMS.
- Betreiber ohne Hochrisiko-Systeme: im Wesentlichen Inventar, Schulung und

Transparenzhinweise – ein überschaubares Projekt, kein Prozent-Aufschlag auf das KI-Budget.

• Was keine Schätzung sauber erfasst: die Kosten der Unsicherheit, also Projekte, die nicht starten, weil niemand weiß, ob sie hochriskant sind. Das ist der eigentliche Schaden.

Was es wirklich kostet: drei Unternehmensprofile

Aus meinen Projekten lassen sich grobe Größenordnungen ableiten. Sie ersetzen keine Kalkulation, zeigen aber, wo das Geld tatsächlich hingeht – und dass Unternehmensgröße allein wenig aussagt. Entscheidend ist die Rolle.

Profil	Rolle und Risikoklasse	Typische Aufgaben	Größenordnung Aufwand
Mittelständler, 400 Personen, Copilot, Website-Chatbot, Rechnungserkennung	Betreiber, minimal und Transparenz	Inventar, Einstufung, Schulung nach Art. 4, Chatbot-Hinweis, Nutzungsrichtlinie	einige Personentage bis wenige Personenwochen, einmalig plus Pflege
Software-Start-up, 15 Personen, KI-gestütztes Bewerbermanagement	Anbieter, Hochrisiko Anhang III	QMS light, Risikomanagement, Datendokumentation, Bias-Tests, Logging, Gebrauchsanweisung, interne Konformitätsbewertung, Registrierung	mehrere Personenmonate im ersten Jahr, danach laufend ein relevanter Teil einer Stelle
Konzern, 8.000 Personen, mehrere eigene Systeme, davon zwei hochriskant	Anbieter und Betreiber, gemischt	KI-Governance-Gremium, Register, Integration in bestehendes QMS und ISMS, Lieferantenprüfung, Grundrechte-Folgenabschätzung	ein kleines Team; relativ zum Umsatz gering

Die Asymmetrie ist offensichtlich, und sie ist das stärkste Argument der Kritiker: Fixkosten treffen kleine Anbieter überproportional. Das Start-up aus Zeile zwei steckt einen spürbaren Teil seiner Entwicklungskapazität in Nachweise, der Konzern verbucht es unter Rauschen. Regulierung, die große Anbieter relativ begünstigt, ist ein bekanntes Muster – die DSGVO hat es vorgemacht.

KMU-Erleichterungen und Reallabore

Der AI Act und die Omnibus-Verordnung versuchen gegenzusteuern. Die Erleichterungen gelten für KMU nach der EU-Definition – weniger als 250 Personen und höchstens 50 Mio. Euro Umsatz oder 43 Mio. Euro Bilanzsumme – und seit der Omnibus-Verordnung in Teilen auch für **kleine Midcaps**, also Unternehmen bis 750 Personen und 150 Mio. Euro Umsatz oder 129 Mio. Euro Bilanzsumme.

Erleichterung	Rechtsgrundlage	Für wen	Was sie praktisch bringt
Vereinfachte technische Dokumentation	Art. 11	KMU, kleine Midcaps	Formular der Kommission statt freier Anhang-IV-Dokumentation
Vereinfachtes QMS	Art. 17, Art. 63	KMU ohne Partner- oder verbundene Unternehmen	Teile des QMS dürfen schlanker ausfallen
Bußgeld-Deckel	Art. 99	KMU, kleine Midcaps	jeweils der niedrigere Wert aus Festbetrag und Prozentsatz

Erleichterung	Rechtsgrundlage	Für wen	Was sie praktisch bringt
Vorrangiger und kostenloser Zugang zu Reallaboren	Art. 57 ff., Art. 62	KMU und Start-ups, teils kleine Midcaps	Test unter Aufsicht, Leitfäden, Ansprechpartner bei der Behörde
Test unter Realbedingungen	Art. 60, Art. 60a	Anbieter von Anhang-III- und Anhang-I-Systemen	Erprobung vor dem Marktstart mit Testplan und Einwilligung
Beratung und Informationskanäle	Art. 62, Art. 70	KMU, kleine Midcaps	Anlaufstellen und Schulungsangebote der Behörden

Die **KI-Reallabore** (Sandboxes) nach Art. 57 ff. sind das interessanteste Instrument. Jeder Mitgliedstaat muss nach der Omnibus-Verordnung bis 2. August 2027 mindestens eines betreiben; zusätzlich kann das KI-Büro ein Reallabor auf EU-Ebene für Systeme einrichten, die es selbst beaufsichtigt. Wer im Reallabor nach einem vereinbarten Plan arbeitet und sich an die Vorgaben der Behörde hält, wird für Verstöße gegen den AI Act während der Erprobung nicht mit Bußgeldern belegt. Die Dokumentation aus dem Reallabor kann später in die Konformitätsbewertung einfließen. In Deutschland soll die Bundesnetzagentur nach dem KI-MIG mindestens ein solches Reallabor errichten.

Ehrlich gesagt: Ob das in der Praxis trägt, entscheidet sich an der Personalausstattung der Behörden. Ein Reallabor mit drei Stellen für ganz Deutschland ist eine Warteliste, kein Innovationsinstrument.

Wo die Kritik trifft – und wo nicht

Kritikpunkt	Berechtigt?	Einordnung
Fixkosten benachteiligen KMU und Start-ups	ja	Erleichterungen helfen, beseitigen die Asymmetrie aber nicht
Unklare Begriffe erzeugen Abwarten	ja	Normen fehlen, Leitlinien kommen spät; die Verschiebung hat die Unsicherheit eher verlängert
Ständig neue Fristen untergraben Planbarkeit	ja	Wer 2025 brav angefangen hat, fühlt sich 2026 bestraft; feste Termine sind jetzt immerhin gesetzt
Papier-Compliance statt echter Sicherheit	teilweise	Gilt für schlecht gemachte Umsetzung; Logging, Tests und Aufsicht sind echte Sicherheitsgewinne
Externe Prüfungen kosten bis zu einer Million	nein	Die meisten Anhang-III-Systeme brauchen keine Benannte Stelle
17 Prozent Aufschlag auf alle KI-Projekte	nein	Rechenfehler, siehe oben
Open Source wird abgewürgt	überwiegend nein	Weitgehende Ausnahmen; die Grauzone Monetarisierung ist das echte Problem
Ohne AI Act wäre Europa im KI-Rennen vorn	nein	Der Rückstand bei Kapital und Rechenzentren ist älter als jede Verordnung
Brüssel reguliert das Falsche	teilweise	Verbote und Hochrisiko-Kern sind gut begründbar; die Detailtiefe des Nachweises ist das Problem

Mein Fazit zur Titelfrage, ohne das Ende vorwegzunehmen: Der Schaden des AI Act liegt weniger in den Pflichten selbst als in der Unsicherheit, die drei Jahre Hin und Her erzeugt haben, und in der Asymmetrie zulasten kleiner Anbieter. Der Nutzen ist kleiner, als Brüssel behauptet, aber größer als null: Die Verbote verhindern Anwendungen, die niemand ernsthaft vermissen sollte, und für KI, die über Kredite, Jobs und Gesundheit mitentscheidet, ist ein Nachweis von Tests und Aufsicht keine Zumutung.

Verstoß	Höchstbetrag	Für KMU und kleine Midcaps
Verbotene Praktik (Art. 5)	35 Mio. Euro oder 7 % des weltweiten Jahresumsatzes, je nachdem was höher ist	der niedrigere der beiden Werte
Pflichten für Anbieter, Betreiber, Einführer, Händler, Transparenz (Art. 50)	15 Mio. Euro oder 3 %	der niedrigere der beiden Werte
Falsche oder irreführende Angaben gegenüber Behörden	7,5 Mio. Euro oder 1 %	der niedrigere der beiden Werte
GPAI-Anbieter (Art. 101, durch die Kommission)	15 Mio. Euro oder 3 %	keine Sonderregel

Praktische Umsetzung im Unternehmen – und das Zusammenspiel mit DSGVO und Haftung

Genug Theorie. So gehst du vor, wenn du nicht 80 Seiten Readiness-Analyse willst, sondern einen Stand, den du einer Prüferin oder einem Prüfer in einer Stunde erklären kannst.

Schritt 1: KI-Inventar

Du kannst nichts einstufen, was du nicht kennst. Das Inventar erfasst jedes KI-System, das im Unternehmen genutzt, gebaut oder eingekauft wird – inklusive der KI-Funktionen in Standardsoftware, die niemand bestellt hat, weil sie mit dem letzten Update einfach da waren. Quellen sind Einkauf und Verträge, das Software-Asset-Management, die Freigabelisten im Microsoft-365-Tenant für Copilot-Agenten und Apps sowie eine simple Abfrage in den Fachbereichen. Mindestfelder je Eintrag: Name, Anbieter, Zweck, Fachbereich, fachlicher Owner, Rolle (Anbieter oder Betreiber), verarbeitete Daten, betroffene Personengruppen, Status.

Wenn ihr Copilot-Agenten breit ausrollt, wächst das Inventar schneller als jede Tabelle. Dann gehört die Inventarisierung in die Agentenverwaltung selbst – wie das mit Microsoft-Bordmitteln geht, beschreibt Agent 365 – KI-Agenten als Steuerzentrale für Microsoft 365, Sicherheit und Automatisierung. Gleiches gilt für Automatisierungen mit KI-Schritten in Power Automate, n8n oder Make; welche Plattform welche Protokollierung mitbringt, zeigt Automatisierung mit KI in der Praxis – Power Automate, n8n, Zapier und Make im Vergleich.

Schritt 2: Einstufung mit Begründung

Für jeden Eintrag gehst du die Prüfreihenfolge aus Abbildung 1 durch und schreibst das Ergebnis mit zwei, drei Sätzen Begründung auf. Mehr braucht es bei minimalem Risiko nicht. Bei allem, was in die Nähe von Anhang III kommt, schreibst du ausführlicher: Welche Ausnahme nach Art. 6 Abs. 3 greift, warum kein Profiling vorliegt, welcher Mensch die eigentliche Entscheidung trifft. Diese Begründung ist dein Schutzschild, wenn die Bundesnetzagentur fragt.

Tipp: Diese Vorhaben gehen ohne Hochrisiko-Einstufung

- Copilot und Chat-Assistenten für Texte, Zusammenfassungen, Recherche, Übersetzung und Code.
- Wissensassistenten auf Handbüchern, Richtlinien, Produktdokumentation.
- Klassifikation und Weiterleitung von E-Mails, Tickets und Rechnungen.
- Prognosen für Absatz, Lager, Energie und Wartung, solange keine Personen bewertet werden.
- Qualitätskontrolle per Bilderkennung ohne Sicherheitsfunktion.
- Betrugserkennung im Zahlungsverkehr (in Anhang III ausdrücklich ausgenommen).
- Recruiting-Hilfen, die nur formulieren, übersetzen oder Termine koordinieren – nicht bewerten.

Schritt 3: KI-Kompetenz nach Art. 4

Art. 4 gilt für jedes Unternehmen, das KI einsetzt, seit Februar 2025. Die Omnibus-Verordnung hat die Pflicht neu gefasst: Anbieter und Betreiber müssen Maßnahmen ergreifen, um die KI-Kompetenz ihres Personals und der Personen, die in ihrem Auftrag mit KI arbeiten, zu fördern. Ein bestimmtes Kompetenzniveau jeder einzelnen Person schuldest du nicht. Einen eigenen Bußgeldtatbestand in Art. 99 gibt es für Art. 4 nicht – wer aber nach einem Schaden nicht belegen kann, dass er seine Leute befähigt hat, steht in jeder Haftungs- und Aufsichtsdiskussion schlecht da.

Praktisch heißt das: eine Basisschulung für alle, die KI nutzen (Funktionsweise, typische Fehler, Halluzinationen, was nicht in Prompts gehört, Kennzeichnung), vertiefte Module für Rollen mit Aufsichtsfunktion, Entwicklung oder Einkauf, und ein Nachweis, wer wann was absolviert hat. Wie du das in einen Einführungsplan einbettest, steht im KI im Unternehmen erfolgreich einführen – Praxisleitfaden.

Schritt 4: Risikoregister und Modelldokumentation

Für Systeme, die du selbst baust oder wesentlich anpasst, brauchst du zwei schlanke Artefakte, die auch ohne Hochrisiko-Einstufung sinnvoll sind und im Ernstfall der Kern deiner technischen Dokumentation werden:

Artefakt	Inhalt	Wer pflegt	Wann aktualisieren
Risikoregister	Risiko, betroffene Gruppe, Eintrittswahrscheinlichkeit, Auswirkung, Maßnahme, Restrisiko, Owner	fachlicher Owner mit IT und Datenschutz	bei jeder Änderung von Zweck, Modell, Daten; mindestens jährlich
Modellkarte	Zweck und ausgeschlossene Zwecke, Modell und Version, Datenquellen, Metriken, bekannte Grenzen, Aufsichtskonzept	Entwicklungsteam	bei jedem Release
Änderungsprotokoll	Was wurde wann warum geändert, wer hat freigegeben	Entwicklungsteam	laufend, automatisiert aus der Pipeline
Einstufungsvermerk	Ergebnis der Prüfreihenfolge mit Begründung	KI-Verantwortung im Unternehmen	bei Zweckänderung

Der Trick ist, diese Artefakte aus der Arbeit heraus entstehen zu lassen: Modellkarte als Datei im Repository, Änderungsprotokoll aus den Commits, Logs aus der Plattform. Dokumentation, die erst vor dem Audit geschrieben wird, sieht man an – sie ist zu glatt.

DSGVO: dieselben Daten, zwei Regelwerke

Der AI Act lässt die DSGVO unberührt. Sobald ein KI-System personenbezogene Daten verarbeitet, gelten beide nebeneinander, und die Pflichten überlappen sich: Die Datenschutz-Folgenabschätzung nach Art. 35 DSGVO und die Grundrechte-Folgenabschätzung nach Art. 27 AI Act fragen ähnliche Dinge, die Omnibus-Verordnung erlaubt ausdrücklich, aufeinander zu verweisen. Art. 22 DSGVO zu automatisierten Einzelentscheidungen und die menschliche Aufsicht nach Art. 14 AI Act ziehen in dieselbe Richtung. Neu ist Art. 4a AI Act: Er erlaubt Anbietern von Hochrisiko-Systemen und unter engen Voraussetzungen auch anderen Anbietern und Betreibern, besondere Kategorien personenbezogener Daten ausnahmsweise zur Erkennung und Korrektur von Verzerrungen zu verarbeiten – mit Pseudonymisierung, Zugriffsbeschränkung und Löschpflicht. Wie du Datenschutz und Leitplanken für Copilot konkret aufsetzt, beschreibt Microsoft Copilot-Governance – Grundlagen, Umsetzung, Praxis.

Produkthaftung und die zurückgezogene KI-Haftungsrichtlinie

Die Haftungsseite hat sich verschoben, und zwar in eine Richtung, die im AI-Act-Getöse untergeht. Die neue Produkthaftungsrichtlinie (EU) 2024/2853 behandelt Software ausdrücklich als Produkt – KI-Systeme eingeschlossen, ob lokal installiert oder als Cloud-Dienst. Die Mitgliedstaaten müssen sie bis 9. Dezember 2026 umsetzen; sie gilt für Produkte, die danach in Verkehr gebracht werden. Haftung ohne Verschulden, Offenlegungspflichten für Beweismittel und Vermutungsregeln zugunsten geschädigter Personen bei technischer Komplexität. Wer gegen verbindliche Sicherheitsanforderungen verstößt – und dazu zählen die Pflichten des AI Act –, gegen den wird die Fehlerhaftigkeit vermutet. Spätestens hier wird die Dokumentation aus Schritt 4 zur Verteidigung.

Die geplante KI-Haftungsrichtlinie dagegen ist vom Tisch. Die Kommission hat den Vorschlag in ihrem Arbeitsprogramm vom Februar 2025 mangels absehbarer Einigung zur Rücknahme vorgesehen und anschließend zurückgezogen. Damit bleibt es für verschuldensabhängige Ansprüche bei nationalem Deliktsrecht – in Deutschland also § 823 BGB mit allen Beweisproblemen, die geschädigte Personen bei einer Blackbox haben. Für Unternehmen ist das kurzfristig bequem und langfristig unklar; einen neuen Anlauf hat sich die Kommission ausdrücklich offengehalten.

Regelwerk	Schwerpunkt	Überschneidung mit dem AI Act	Stand
DSGVO	personenbezogene Daten	Folgenabschätzungen, Transparenz, automatisierte Entscheidungen, Bias-Daten nach Art. 4a	gilt seit 2018
Produkthaftungsrichtlinie 2024/2853	verschuldensunabhängige Haftung für fehlerhafte Produkte inklusive Software	Verstoß gegen AI-Act-Pflichten begründet Fehlervermutung	Umsetzung bis 9.12.2026
KI-Haftungsrichtlinie	Beweiserleichterungen bei Verschuldenshaftung	sollte AI-Act-Verstöße mit Kausalitätsvermutung verknüpfen	von der Kommission zurückgezogen
Cyber Resilience Act	Cybersicherheit von Produkten mit digitalen Elementen	Erfüllung gilt als Nachweis für Art. 15 AI Act	gestaffelt ab 2026/2027

Regelwerk	Schwerpunkt	Überschneidung mit dem AI Act	Stand
KI-MIG (Deutschland)	Behörden, Verfahren, Reallabore	Durchführung des AI Act, Bundesnetzagentur als Marktüberwachung	in Kraft seit 29.7.2026

Aufsicht in Deutschland

Das KI-MIG wurde vom Bundestag am 11. Juni 2026 beschlossen, vom Bundesrat im Juli gebilligt und gilt seit 29. Juli 2026. Die Bundesnetzagentur ist zentrale Marktüberwachungsbehörde für verbotene Praktiken, Hochrisiko-Systeme und Transparenzpflichten; für bestimmte Hochrisiko-Anwendungen richtet sie eine eigene KI-Marktüberwachungskammer ein, dazu ein Koordinierungs- und Kompetenzzentrum. Für KI in regulierten Produkten bleiben die sektoralen Behörden zuständig, für KI-Systeme öffentlicher Stellen der Länder und Kommunen ist die Bundesnetzagentur ausdrücklich nicht zuständig. Für GPAI-Modelle und Systeme auf Basis eigener GPAI-Modelle desselben Anbieters ist seit der Omnibus-Verordnung weitgehend das KI-Büro in Brüssel allein zuständig.

Weiterlesen: Passende Beiträge zur Umsetzung

› KI im Unternehmen erfolgreich einführen – Praxisleitfaden
› Microsoft Copilot-Governance – Grundlagen, Umsetzung, Praxis
› Agent 365 – KI-Agenten als Steuerzentrale für Microsoft 365, Sicherheit und Automatisierung
› Überblick über generative KI-Plattformen

Fazit: Viel Aufwand an der falschen Stelle, wenig Schaden für die meisten

Der EU AI Act ist kein Innovationskiller für das typische Unternehmen, das KI einsetzt. Wer Copilot, Chatbots und Automatisierungen betreibt, kommt mit Inventar, Einstufung, Schulung und ein paar Transparenzhinweisen aus. Wer das mit einem sechsstelligen Beratungsprojekt erledigt, hat sich verkaufen lassen.

Viel Schaden richtet der AI Act dort an, wo er am meisten Nutzen stiften soll: bei Anbietern von Hochrisiko-KI, besonders kleinen. Nicht wegen der Anforderungen an sich – Risikomanagement, Tests und Aufsicht sind gutes Engineering –, sondern wegen fehlender Normen, später Leitlinien, verschobener Fristen und einer Nachweistiefe, die Fixkosten erzeugt, die nur Große locker tragen. Die Omnibus-Verordnung hat Luft verschafft und einige Erleichterungen gebracht, die Grundstruktur aber nicht verändert. Und die Haftungsseite wird mit der neuen Produkthaftungsrichtlinie schärfer, während die KI-Haftungsrichtlinie verschwunden ist.

Meine Empfehlung: Nutze die Zeit bis Dezember 2027 nicht zum Abwarten, sondern zum Aufräumen. Inventar aufbauen, jede Einstufung begründen, Schulungen nachweisbar machen, Zwecke von Allzweck-Assistenten begrenzen, Modellkarten und Logs aus der laufenden Arbeit entstehen lassen. Wer das jetzt mit Augenmaß macht, hat in einem Jahr eine dünne Akte, die trägt – statt einer dicken, die niemand gelesen hat.

Häufige Fragen zum EU AI Act

Gilt der EU AI Act auch für Unternehmen, die KI nur nutzen?

Ja. Als Betreiber hast du seit Februar 2025 die Pflicht zur Förderung der KI-Kompetenz nach Art. 4 und darfst keine verbotenen Praktiken einsetzen. Seit August 2026 kommen Transparenzpflichten, etwa für Deepfakes, dazu. Die umfangreichen Betreiberpflichten nach Art. 26 treffen dich nur bei Hochrisiko-Systemen, ab 2. Dezember 2027.

Ist Microsoft 365 Copilot ein Hochrisiko-System?

Nein. Copilot ist ein allgemeiner Assistent auf Basis von GPAI-Modellen und fällt im normalen Büroeinsatz unter minimales Risiko. Hochriskant wird es erst, wenn du es für einen Zweck aus Anhang III einsetzt, etwa zum Bewerten von Bewerbungen. Dann wirst du nach Art. 25 möglicherweise selbst zum Anbieter.

Wann gelten die Hochrisiko-Pflichten nach der Verschiebung?

Für eigenständige Systeme nach Anhang III ab 2. Dezember 2027, für KI in regulierten Produkten nach Anhang I ab 2. August 2028. Festgelegt hat das die Omnibus-Verordnung (EU) 2026/1744, die seit 27. Juli 2026 in Kraft ist.

Wer entscheidet, ob ein KI-System hochriskant ist?

Der Anbieter in eigener Verantwortung, ohne Vorabgenehmigung. Der Betreiber prüft, ob sein Einsatzzweck zur Einstufung passt. Die Marktüberwachung, in Deutschland die Bundesnetzagentur, kann die Einstufung überprüfen und korrigieren.

Brauche ich für Hochrisiko-KI immer eine Benannte Stelle?

Nein. Für die meisten Anhang-III-Systeme reicht die interne Kontrolle nach Anhang VI. Eine Benannte Stelle nach Anhang VII ist im Wesentlichen bei biometrischen Systemen ohne vollständige Anwendung harmonisierter Normen nötig. KI in Produkten nach Anhang I folgt dem jeweiligen Sektorverfahren.

Was muss ich zur KI-Kompetenz nach Art. 4 konkret tun?

Maßnahmen ergreifen, die die KI-Kompetenz deiner Leute fördern – passend zu Vorwissen, Rolle und Einsatz. Bewährt haben sich eine Basisschulung für alle Nutzerinnen und Nutzer, vertiefte Module für Rollen mit Aufsicht oder Entwicklung und ein Nachweis über Teilnahme und Inhalte.

Sind Open-Source-Modelle vom AI Act ausgenommen?

Teilweise. Freie KI-Systeme sind ausgenommen, solange sie nicht hochriskant, verboten oder transparenzpflichtig sind. Freie GPAI-Modelle sind von Teilen der Dokumentationspflichten befreit, müssen aber Urheberrechts-Policy und Trainingsdaten-Zusammenfassung liefern. Bei systemischem Risiko oder Monetarisierung entfällt die Ausnahme.

Was kostet die Umsetzung des AI Act wirklich?

Für Betreiber ohne Hochrisiko-Systeme meist wenige Personentage bis Personenwochen. Für Anbieter von Hochrisiko-KI mehrere Personenmonate im ersten Jahr, plus QMS-Aufbau, falls keines existiert. Die oft zitierten 17 Prozent Aufschlag auf alle KI-Projekte beruhen auf einer fehlerhaften Hochrechnung.

Welche Bußgelder drohen?

Bis 35 Mio. Euro oder 7 % des weltweiten Jahresumsatzes bei verbotenen Praktiken, bis 15 Mio. Euro oder 3 % bei den meisten anderen Pflichten, bis 7,5 Mio. Euro oder 1 % bei falschen Angaben. Für KMU und kleine Midcaps gilt der jeweils niedrigere Wert.

Wie verhält sich der AI Act zur DSGVO?

Beide gelten nebeneinander. Der AI Act ersetzt keine Rechtsgrundlage nach DSGVO. Datenschutz- und Grundrechte-Folgenabschätzung dürfen aufeinander verweisen, und Art. 4a AI Act erlaubt unter engen Bedingungen die Verarbeitung sensibler Daten zur Bias-Korrektur.

Gibt es noch eine KI-Haftungsrichtlinie?

Nein. Die Kommission hat den Vorschlag zurückgezogen. Relevant ist stattdessen die neue Produkthaftungsrichtlinie (EU) 2024/2853, die Software und KI als Produkt erfasst, bis 9. Dezember 2026 umzusetzen ist und bei Verstößen gegen AI-Act-Pflichten eine Fehlervermutung vorsieht.

Welche KI-Vorhaben kann ich ohne Hochrisiko-Einstufung umsetzen?

Alles, was nicht über Menschen in den Bereichen aus Anhang III entscheidet und kein Sicherheitsbauteil eines regulierten Produkts ist: Assistenten für Text und Code, Wissenssuche, Ticket- und Rechnungsklassifikation, Prognosen ohne Personenbezug, Qualitätskontrolle ohne Sicherheitsfunktion und Betrugserkennung im Zahlungsverkehr.