



11iE · PAPER

15.10.2026

BASISWISSEN MIT KRITISCHEN ANMERKUNGEN

Der EU AI Act. Was er regelt. Was offen bleibt.

Eine Einführung in die Regeln und ihre Folgen.
Mit persönlichen Anmerkungen zu Verantwortung,
Macht und Marktzugang.

Elfie Schürfeld-Todor

Kommunikationsstrategin, Autorin und Künstlerin

11iE.de

Inhalt

01 · Was reguliert wird und warum	3
02 · Was verboten ist	8
03 · Was hochreguliert ist	11
04 · Was transparent gemacht werden muss	14
05 · Wer das umsetzt	18
06 · Was offen bleibt	22
Quellen und weiterführende Lektüre	24
Über die Autorin	27

Wie dieses Paper gelesen werden kann

Die sechs Kapitel verbinden eine verständliche Einführung in die KI-Verordnung mit persönlichen Anmerkungen. Die farbigen Kästen zeigen meine Einordnung. Gesetzliche Aussagen werden vereinfacht zusammengefasst und über nummerierte, anklickbare Quellen belegt.

Grundlage ist die konsolidierte Fassung vom 27. Juli 2026. Der Quellenabgleich dieser überarbeiteten Ausgabe erfolgte am 15. Oktober 2026. Individuelle Anwendungen können weitere Voraussetzungen und Sonderregeln auslösen.

Die ursprüngliche Fassung entstand im Mai 2026, mit dem Kurs „EU AI Act Essentials“ des KI-Campus als thematischer Orientierung. Die vorliegende Ausgabe wurde inhaltlich aktualisiert und mit KI-Unterstützung redaktionell und gestalterisch überarbeitet. ^[18]

Hinweis: Keine Rechtsberatung

Ich bin keine Juristin. Dieses Paper dient der allgemeinen Information und meiner persönlichen Einordnung des EU AI Acts. Es stellt keine Rechtsberatung dar und ersetzt keine individuelle rechtliche Beratung durch eine Rechtsanwältin oder einen Rechtsanwalt.

01 · Was reguliert wird und warum

Risiko, Verantwortung und Marktzugang

Der EU AI Act legt Regeln für KI-Systeme und für bestimmte KI-Modelle fest. Er verbindet den Schutz von Gesundheit, Sicherheit und Grundrechten mit dem Anspruch, einen gemeinsamen europäischen Markt für vertrauenswürdige KI zu schaffen und Innovation zu unterstützen. ^[1]

Vier Ziele, eine anspruchsvolle Verbindung

Binnenmarkt, Vertrauen, Schutz und Innovation sollen zusammenpassen. Die Verordnung arbeitet dafür mit Verboten, Anforderungen an Hochrisiko-Systeme, Transparenzpflichten und eigenen Regeln für KI-Modelle mit allgemeinem Verwendungszweck. Welche Pflichten entstehen, hängt unter anderem von der Rolle eines Akteurs, dem System, dem Einsatz und dem jeweiligen Anwendungsdatum ab.

KI muss nicht ständig weiterlernen

Ein KI-System kann nach seiner Einführung anpassungsfähig sein. Das ist nach Artikel 3 Nr. 1 jedoch kein notwendiges Merkmal jedes erfassten Systems. Viele Modelle werden zunächst trainiert und bleiben im laufenden Einsatz technisch unverändert. Andere Systeme können später angepasst werden. Autonomie, Anpassung und die Fähigkeit, aus Eingaben Ausgaben abzuleiten, müssen deshalb auseinandergehalten werden. ^[2]

Das ist für die Regulierung relevant: Ein Produkt kann bereits ohne fortlaufendes Lernen erhebliche Risiken erzeugen. Umgekehrt macht Anpassungsfähigkeit ein System nicht automatisch zu einem Hochrisiko-System.

Regulatorische Fixkosten belasten kleinere Unternehmen häufig stärker. Dieser allgemeine Befund erlaubt noch keine Aussage darüber, welche Marktverschiebungen der AI Act bereits verursacht hat. ^[30]

Meine Einordnung · Gleiche Regeln sind nicht gleich schwer

Wer Schutzpflichten erfüllen soll, braucht die Mittel dazu. Ein kleines Team finanziert Dokumentation, Fachwissen und Prüfungen für ein Hochrisiko-System, bevor dieses Produkt Umsatz erzielt. Ein großer Anbieter kann vorhandene Strukturen nutzen und Kosten über viele Produkte verteilen. Gleiche Regeln können deshalb sehr ungleich wirken.

Zum Mitnehmen

- Die Verordnung verbindet Schutz und Innovationsförderung.
- Risiken und Pflichten hängen vom konkreten System, seinem Einsatz und der jeweiligen Rolle ab.
- Auch KI-Modelle selbst können reguliert sein.

01 · Was reguliert wird und warum

Wer angesprochen wird

Mehrere Rollen entlang einer Wertschöpfungskette

- **Anbieter** entwickeln KI-Systeme oder GPAI-Modelle oder lassen sie entwickeln und bringen sie unter eigenem Namen oder eigener Marke in Verkehr; bei KI-Systemen kann auch die Inbetriebnahme maßgeblich sein.
- **Betreiber** verwenden KI-Systeme in eigener Verantwortung. Eine rein persönliche, nicht berufliche Nutzung durch natürliche Personen ist von dieser Betreiberdefinition ausgenommen.
- **Importeure, Händler und Bevollmächtigte** haben eigene Aufgaben. Welche davon entstehen, hängt von ihrer Tätigkeit und dem erfassten System ab.
- **Produkthersteller** können ebenfalls in die Anbieterrolle fallen, wenn sie KI mit ihrem Produkt unter eigenem Namen auf den Markt bringen.
- **Betroffene Personen** sind Rechteinhaber. Ihre Rechte ergeben sich aus konkreten Vorschriften, etwa zum Beschweren oder zur Erklärung bestimmter Entscheidungen. Ein allgemeines Erklärungsrecht für jede KI-Ausgabe folgt daraus nicht. ^[1] ^[2]

EU-Bezug statt Unternehmenssitz allein

Auch Akteure außerhalb der EU können erfasst sein, beispielsweise wenn sie Systeme oder GPAI-Modelle auf dem EU-Markt anbieten oder die Ausgaben ihrer Systeme in der EU verwendet werden. Artikel 2 enthält zugleich Ausnahmen, unter anderem für bestimmte Forschungsaktivitäten und ausschließlich militärische, Verteidigungs- oder nationale Sicherheitszwecke. Diese Ausnahmen sind keine pauschale Freistellung jeder staatlichen KI-Nutzung. ^[1]

Meine Einordnung · Verantwortung muss erkennbar sein

Verantwortung lässt sich nur übernehmen, wenn die eigene Rolle erkennbar ist. In der Praxis greifen die Rollen ineinander: Ein Unternehmen kauft ein Modell ein, baut einen Dienst darauf und betreibt ihn selbst. Wer kleine Teams in die Pflicht nimmt, muss ihnen verständliche Informationen entlang dieser Kette zugänglich machen. Sonst wird aus einer klaren Zuordnung auf dem Papier eine weitere Hürde im Alltag.

Zum Mitnehmen

- Entwickeln, anbieten, importieren und nutzen sind unterschiedliche Tätigkeiten.
- Ein Unternehmen kann mehrere Rollen zugleich ausüben.
- Der konkrete Anwendungsbereich muss vor der Pflichtenprüfung geklärt werden.

01 · Was reguliert wird und warum

Vier Risikostufen als Orientierung

Die bekannte Einteilung in vier Stufen hilft beim Einstieg. Sie bildet die Rechtslage nicht vollständig ab: Pflichten können sich überlagern. Ein Hochrisiko-System kann beispielsweise zusätzlich Transparenzpflichten auslösen. Die Regeln für GPAI-Modelle kommen als eigener Bereich hinzu. ^[1]

Verbotene Praktiken

Artikel 5 verbietet bestimmte Anwendungen, etwa manipulative Praktiken oder bestimmte biometrische Verfahren. Voraussetzungen und Ausnahmen entscheiden. ^[4]

Hochrisiko-Systeme

Artikel 6 mit Anhängen I und III erfasst bestimmte Produkte und Verwendungen. Eine ganze Branche ist nicht automatisch hochriskant. ^[5]

Transparenzpflichten

Artikel 50 erfasst bestimmte Interaktionen und Inhalte. Diese Pflichten können zusätzlich zu Hochrisiko-Regeln gelten. ^[6]

Weitere Anwendungen

Ohne besondere Hochrisiko-Pflichten ist eine Anwendung nicht rechtsfrei. Datenschutz, Verbraucherschutz und weitere Regeln können gelten.

Eigener Regelungsbereich: GPAI-Modelle

Für Anbieter von Modellen mit allgemeinem Verwendungszweck gelten gesonderte Regeln. Sie sind keine fünfte Risikostufe.

Die vier Felder sind keine gegenseitig ausschließenden Schubladen. Ein Hochrisiko-System kann zusätzlich Transparenzpflichten auslösen. Für Anbieter von GPAI-Modellen gilt ein eigener Pflichtenrahmen; bei systemischem Risiko kommen weitere Anforderungen hinzu. ^[12]

Zum Mitnehmen

- Die Grafik dient der Orientierung, die Tatbestände bestimmen die Pflichten.
- Modell, System, Einsatz und Rolle müssen getrennt geprüft werden.

01 · Was reguliert wird und warum

Wann welche Regeln greifen

Inkrafttreten und Anwendbarkeit sind unterschiedliche Zeitpunkte. Die Verordnung trat am 1. August 2024 in Kraft. Der Digital-Omnibus zu KI hat 2026 unter anderem die Anwendungsfristen für zentrale Hochrisiko-Regeln geändert. Diese Übersicht folgt Artikel 113 in der konsolidierten Fassung vom 27. Juli 2026. ^[1] ^[3]

●	1. August 2024	Inkrafttreten der Verordnung
●	2. Februar 2025	Kapitel I, KI-Kompetenz und ursprüngliche Verbote
●	2. August 2025	Unter anderem GPAI-Regeln und Governance
●	2. August 2026	Allgemeines Anwendungsdatum, insbesondere Artikel 50
●	2. Dezember 2026	Neue Verbote zu sexualisierten Deepfakes ohne Einwilligung und Darstellungen sexuellen Kindesmissbrauchs; technische Kennzeichnung bestimmter Bestandssysteme
●	2. Dezember 2027	Zentrale Hochrisiko-Regeln für Anhang III
●	2. August 2028	Entsprechende Hochrisiko-Regeln für Anhang I

Für Artikel 50 Absatz 2 gilt eine konkrete Übergangsregel: Systeme, die bereits vor dem 2. August 2026 in Verkehr gebracht oder in Betrieb genommen wurden, müssen diese technischen Kennzeichnungspflichten ab dem 2. Dezember 2026 erfüllen. Das verschiebt nicht pauschal die übrigen Pflichten aus Artikel 50. Weitere Bestandsregeln: Artikel 111. ^[1] ^[23]

Meine Einordnung · Aufschub verteilt Zeit und Risiko

Übergangsfristen geben Unternehmen Zeit und verschieben zugleich Schutzpflichten. Bei Anhang III wurde der zentrale Termin vom 2. August 2026 auf den 2. Dezember 2027 verlegt, bei Anhang I vom 2. August 2027 auf den 2. August 2028. ^[1] ^[3] Wer bereits Ressourcen hat, kann diesen Vorsprung ausbauen. Ein Aufschub ist nur dann ein Gewinn, wenn die gewonnene Zeit eine bessere Umsetzung ermöglicht.

01 · Was reguliert wird und warum

Weitere Regeln und Sanktionen

Der AI Act steht nicht allein

Eine KI kann personenbezogene Daten verarbeiten, Teil eines Produkts sein und über eine Plattform angeboten werden. Je nach Fall greifen deshalb mehrere Rechtsgebiete: Datenschutzrecht, Verbraucherschutz und Lauterkeitsrecht, Plattformrecht wie der Digital Services Act, Produktsicherheits- und Produkthaftungsrecht sowie sektorale Regeln. Sie haben unterschiedliche Zwecke und Voraussetzungen. ^[1]

Die vorgeschlagene KI-Haftungsrichtlinie ist kein geltendes Recht. Die Kommission zog den Vorschlag COM(2022) 496 im Oktober 2025 zurück. Haftungsfragen verschwinden dadurch nicht; sie sind anhand der jeweils geltenden Regeln zu beurteilen. ^[16]

Geldbußen: Obergrenzen mit Differenzierung

- **Verbotene Praktiken:** bis zu 35 Millionen Euro oder bei Unternehmen bis zu 7 Prozent des weltweiten Jahresumsatzes des vorangegangenen Geschäftsjahres.
- **Bestimmte weitere Pflichtverstöße:** bis zu 15 Millionen Euro oder 3 Prozent.
- **Unrichtige, unvollständige oder irreführende Auskünfte auf behördliche Anfragen:** bis zu 7,5 Millionen Euro oder 1 Prozent. ^[11]

Bei Unternehmen gilt grundsätzlich die höhere der einschlägigen Obergrenzen. Für KMU einschließlich Start-ups gilt nach Artikel 99 Absatz 6 die niedrigere. Für kleine Midcaps gilt diese Erleichterung nach Absatz 6a bei den Verstößen aus Absätzen 4 und 5. Die konkrete Geldbuße hängt vom Einzelfall ab; die Höchstwerte sind keine automatischen Strafen. ^[11]

Meine Einordnung · Ein Nachweis erklärt noch keine Entscheidung

Dokumentation schafft einen Ausgangspunkt für Kontrolle. Sie macht eine Modellentscheidung noch nicht verständlich und ein Ergebnis noch nicht reproduzierbar. Diese Aufgaben brauchen jeweils Wissen, Zeit und geeignete Werkzeuge. Meine Kritik beginnt dort, wo formale Nachweise als ausreichender Schutz erscheinen, während die praktische Fähigkeit zur Prüfung fehlt.

Zum Mitnehmen

- Mehrere Rechtsgebiete können gleichzeitig relevant sein.
- Die KI-Haftungsrichtlinie wurde nicht verabschiedet.
- Die Bußgeldregeln berücksichtigen Unternehmensgröße und Umstände.

02 · Was verboten ist

Acht ursprüngliche Verbotsbereiche

Die seit Februar 2025 geltenden Tatbestände stehen in Artikel 5 Absatz 1 Buchstaben a bis h. Die folgende Übersicht benennt ihren Kern; entscheidend bleiben der vollständige Tatbestand und seine Ausnahmen. ^[4]

- **Manipulation:** bestimmte unterschwellige, gezielt manipulative oder täuschende Techniken, die Entscheidungen wesentlich verzerren und erheblichen Schaden verursachen oder wahrscheinlich machen.
- **Ausnutzung von Schutzbedürftigkeit:** bestimmte schädliche Verhaltensbeeinflussung durch Ausnutzung von Alter, Behinderung oder einer besonderen sozialen oder wirtschaftlichen Situation.
- **Social Scoring:** bestimmte soziale Bewertungen mit nachteiliger Behandlung in sachfremden Kontexten oder ungerechtfertigter beziehungsweise unverhältnismäßiger Benachteiligung.
- **Individuelle Kriminalitätsprognosen:** Risikobewertungen allein auf Grundlage von Profiling oder Persönlichkeitsmerkmalen. Die gesetzlich beschriebene Unterstützung menschlicher Beurteilung anhand objektiver, überprüfbarer Tatsachen ist davon zu unterscheiden.
- **Gesichtsdatenbanken:** Aufbau oder Erweiterung durch ungezieltes Sammeln von Gesichtsbildern aus dem Internet oder aus Videoüberwachung.
- **Emotionserkennung:** KI zur Ableitung von Emotionen am Arbeitsplatz und in Bildungseinrichtungen, mit Ausnahmen für medizinische oder Sicherheitszwecke.
- **Sensible biometrische Kategorisierung:** bestimmte Rückschlüsse etwa auf politische Überzeugungen, Religion oder sexuelle Orientierung anhand biometrischer Daten.
- **Biometrische Echtzeit-Fernidentifizierung:** Nutzung in öffentlich zugänglichen Räumen zu Strafverfolgungszwecken, vorbehaltlich eng geregelter Ausnahmen.

Ergänzung ab 2. Dezember 2026

Die 2026 eingefügten Buchstaben ba und bb betreffen bestimmte KI-Anwendungen für nicht einvernehmliche sexualisierte Darstellungen identifizierbarer Personen sowie Darstellungen sexuellen Kindesmissbrauchs. Für das Anbieten solcher Systeme und ihre konkrete Verwendung gelten eigene Voraussetzungen. Das Datum und die Reichweite dürfen nicht mit den ursprünglichen acht Tatbeständen vermischt werden. ^[3] ^[4]

02 · Was verboten ist

Wo die Grenzen verlaufen

Social Scoring: privat ist keine Ausnahme

Artikel 5 Absatz 1 Buchstabe c ist nicht auf Behörden beschränkt. Auch private Anbieter oder Betreiber können erfasst sein. Umgekehrt fällt nicht jede Bonitätsprüfung oder Risikobewertung automatisch unter dieses Verbot. Die Datengrundlage, der Kontext der Bewertung und die nachteilige Behandlung müssen am Tatbestand geprüft werden. ^[4]

Meine Einordnung · Bewertungen verteilen Chancen

Wer Menschen bewertet, beeinflusst ihren Zugang zu Chancen. Ob eine konkrete Praxis unter das Social-Scoring-Verbot fällt, beantwortet noch nicht, ob ihre Maßstäbe nachvollziehbar und anfechtbar sind. Auch eine zulässige Bonitätsprüfung kann tief in ein Leben eingreifen.

Strafverfolgung: unterschiedliche Regeln auseinanderhalten

Die Ausnahme für biometrische Echtzeit-Fernidentifizierung ist keine allgemeine Erlaubnis für Predictive Policing. Artikel 5 regelt individuelle Kriminalitätsprognosen und biometrische Identifizierung getrennt. Bei der Identifizierung sind unter anderem Zweckbindung, Notwendigkeit, Verhältnismäßigkeit und eine gerichtliche oder unabhängige behördliche Genehmigung relevant; für dringliche Fälle bestehen besondere Regeln. ^[4]

Emotionserkennung: Information ersetzt kein Verbot

Ein Hinweis auf eine Emotionsanalyse macht einen verbotenen Einsatz am Arbeitsplatz nicht zulässig. Zuerst muss geklärt werden, ob die Anwendung erlaubt ist. Erst danach stellt sich die Frage nach zusätzlichen Informationspflichten.

Meine Einordnung · Kontrolle reicht über das Werkzeug hinaus

Das Verbot bestimmter KI-gestützter Emotionserkennung begrenzt ein Werkzeug. Eine Führungskraft, die die Stimmung ihrer Beschäftigten selbst einschätzt, fällt dadurch nicht unter dieses spezielle KI-Verbot; andere rechtliche Grenzen bleiben bestehen. Die Grenze akzeptabler Kontrolle verläuft für mich nicht erst dort, wo KI ins Spiel kommt.

Zum Mitnehmen

- Private Akteure sind nicht pauschal vom Social-Scoring-Verbot ausgenommen.
- Ausnahmen gelten für bestimmte Tatbestände und Zwecke.
- Transparenz legalisiert keine verbotene Anwendung.

02 · Was verboten ist

Staatliche Macht und ihre Grenzen

Ausnahmen sind an Zwecke gebunden

Artikel 2 nimmt KI-Systeme aus, soweit sie ausschließlich für militärische, Verteidigungs- oder nationale Sicherheitszwecke eingesetzt werden. Die Ausnahme kann auch private Akteure erfassen. Sie ist keine allgemeine Freistellung staatlicher Nutzung. Eine zivile Verwendung muss gesondert geprüft werden. ^[1]

Strafverfolgung bleibt ein eigener Bereich

Für bestimmte biometrische Echtzeit-Fernidentifizierung zur Strafverfolgung verlangt Artikel 5 enge Voraussetzungen und grundsätzlich eine vorherige gerichtliche oder unabhängige behördliche Genehmigung. Dringliche Fälle haben besondere Regeln. Artikel 46 ermöglicht unter begrenzten Voraussetzungen Ausnahmen von der Konformitätsbewertung; er schafft keine allgemeine Befreiung vom AI Act. ^[1] ^[4]

Bestimmte Registrierungen für Strafverfolgung, Migration, Asyl und Grenzkontrolle erfolgen nach Artikel 49 in einem nicht öffentlichen Teil der EU-Datenbank. Artikel 99 Absatz 8 überlässt den Mitgliedstaaten die Entscheidung über Geldbußen gegen öffentliche Stellen. Diese Unterschiede verdienen eigene Aufmerksamkeit. ^[1]

Meine Einordnung · Kontrolle muss Macht begrenzen

Je mächtiger der Akteur, desto wichtiger ist unabhängige Kontrolle. Gerade staatliche KI kann Menschen treffen, die sich ihr nicht einfach entziehen können. Systeme für ausschließlich militärische, Verteidigungs- oder nationale Sicherheitszwecke fallen aus dem AI Act heraus, auch wenn private Unternehmen sie entwickeln. Die Schutzregeln im übrigen Anwendungsbereich setzen wirksame Gerichte und unabhängige Aufsicht voraus. Solche Regeln sind nur so stark wie die Institutionen, die sie durchsetzen. Die Systeme können weiterbestehen, wenn eine Regierung wechselt. Ein Gesetz, das den demokratischen Rechtsstaat voraussetzt, schützt nicht davor, dass er verloren geht.

03 · Was hochreguliert ist

Hochrisiko braucht eine konkrete Prüfung

Zwei Wege zur Einstufung

Artikel 6 Absatz 1 betrifft KI als Sicherheitsbauteil eines Produkts aus Anhang I oder als ein solches Produkt selbst. Zusätzlich muss das einschlägige Produktrecht eine Konformitätsbewertung durch Dritte verlangen. Die 2026 ergänzten Absätze 1a bis 1c präzisieren unter anderem die Abgrenzung sicherheitsrelevanter Funktionen. Nicht jede KI-Funktion eines regulierten Produkts ist dadurch automatisch hochriskant. ^[5]

Artikel 6 Absatz 2 verweist auf die Anwendungsfälle in Anhang III. Hierzu gehören bestimmte Anwendungen etwa in Bildung, Beschäftigung, kritischer Infrastruktur, Strafverfolgung, Migration oder Justiz. Maßgeblich ist die jeweils beschriebene Verwendung.

Für bestimmte Fälle aus Anhang III kann die Ausnahme aus Absatz 3 greifen, wenn kein erhebliches Risiko entsteht und eine der dort genannten Bedingungen erfüllt ist. Profiling natürlicher Personen bleibt innerhalb dieser Anhang-III-Prüfung hochriskant. Eine angenommene Ausnahme muss der Anbieter dokumentieren; hinzu kommt die gesetzlich vorgesehene Registrierung. ^[5]

Vier Fragen für die erste Einordnung

- **Was ist das System?** Funktion, Ausgaben und Zweck anhand der KI-Definition bestimmen.
- **Warum gilt EU-Recht?** Den Bezug zur EU und mögliche Ausnahmen prüfen.
- **Welche Tatbestände treffen zu?** Verbote, Hochrisiko-Einstufung und Transparenzpflichten getrennt betrachten. Bei GPAI-Modellen zusätzlich Kapitel V prüfen.
- **Welche Rolle und welches Datum?** Anbieter, Betreiber und weitere Rollen zuordnen und die anwendbaren Pflichten ermitteln.

Meine Einordnung · Einordnung kostet bereits Ressourcen

Die erste Hürde liegt vor der Umsetzung: Ein kleines Team muss erkennen, welche Regeln überhaupt für sein Produkt gelten. Dafür braucht es technisches und rechtliches Verständnis. Eine gute Orientierung muss Entscheidungen erleichtern. Wenn sie vor allem zeigt, dass für jeden nächsten Schritt weitere Beratung nötig ist, bleibt der Marktzugang trotz verständlicher Checklisten ungleich.

03 · Was hochreguliert ist

Anforderungen über den Lebenszyklus

Für erfasste Hochrisiko-Systeme bilden die Artikel 8 bis 15 den zentralen Anforderungsrahmen. Die konkrete Ausgestaltung hängt vom System ab. Artikel 8 rahmt die Einhaltung; die folgenden Artikel beschreiben insbesondere sieben Themen. ^[1] ^[10]

- **Risikomanagement, Artikel 9:** Risiken über den Lebenszyklus ermitteln, bewerten und geeignete Maßnahmen vorsehen.
- **Daten und Daten-Governance, Artikel 10:** Anforderungen an Trainings-, Validierungs- und Testdaten erfüllen, soweit die Vorschrift für das System einschlägig ist.
- **Technische Dokumentation, Artikel 11:** die Erfüllung der Anforderungen vor dem Inverkehrbringen oder der Inbetriebnahme nachvollziehbar dokumentieren und aktuell halten.
- **Aufzeichnung, Artikel 12:** technische Möglichkeiten zur automatischen Protokollierung relevanter Ereignisse schaffen.
- **Transparenz gegenüber Betreibern, Artikel 13:** verständliche Informationen und Gebrauchsanweisungen zu Fähigkeiten, Grenzen und geeigneter Nutzung bereitstellen.
- **Menschliche Aufsicht, Artikel 14:** wirksame menschliche Kontrolle ermöglichen, einschließlich angemessener Eingriffsmöglichkeiten.
- **Genauigkeit, Robustheit und Cybersicherheit, Artikel 15:** ein angemessenes Niveau dieser Eigenschaften über den Lebenszyklus sicherstellen.

Konformität ist mehr als ein Dokument

Anbieterpflichten, Qualitätsmanagement, Konformitätsbewertung, EU-Konformitätserklärung und CE-Kennzeichnung stehen in weiteren Artikeln, insbesondere 16, 17, 43, 47 und 48. Sie lassen sich nicht allein aus der Liste der technischen Anforderungen ableiten. Für bestimmte Produktbereiche gelten zudem besondere Verknüpfungen mit dem sektoralen Recht. ^[1]

Meine Einordnung · Aufsicht braucht Handlungsmacht

Menschliche Aufsicht braucht Handlungsmacht. Ein Mensch kann nur wirksam beaufsichtigen, was er hinreichend versteht und tatsächlich beeinflussen darf. Eine formale Zuständigkeit reicht nicht. Zeit, Schulung, Handlungsspielraum und brauchbare Informationen entscheiden mit darüber, ob aus der vorgesehenen Aufsicht eine praktische Kontrolle wird.

Zum Mitnehmen

- Hochrisiko-Pflichten begleiten Entwicklung und Betrieb.
- Technische Anforderungen und organisatorische Anbieterpflichten greifen ineinander.
- Menschliche Aufsicht muss praktisch möglich sein.

03 · Was hochreguliert ist

Wenn Systeme sich verändern

Konformität ist kein einmaliger Haken

Der AI Act berücksichtigt Veränderungen über den Lebenszyklus. Bei einer wesentlichen Änderung kann nach Artikel 43 eine neue Konformitätsbewertung erforderlich werden. Vorab festgelegte und in der ursprünglichen Bewertung berücksichtigte Lernänderungen gelten nicht allein deshalb als wesentliche Änderung. Artikel 72 verlangt ein System zur fortlaufenden Beobachtung nach dem Inverkehrbringen. ^[28] ^[29]

Die Verordnung kennt also Veränderung. Ihr Werkzeug bleibt die Konformitätsbewertung aus dem europäischen Produktrecht. Derselbe gemeinsame Rechtsrahmen prägt auch Vorschriften für Aufzüge und Medizinprodukte; die konkreten Prüfverfahren unterscheiden sich. Bei Hochrisiko-KI muss der Anbieter beurteilen, ob neue Versionen, Daten oder Einsatzweisen von der bisherigen Bewertung gedeckt sind oder eine wesentliche Änderung darstellen. ^[28] ^[32]

Meine Einordnung · Produktlogik trifft auf schnelle Entwicklung

Der AI Act übernimmt für Hochrisiko-KI eine Produktlogik, die auch Aufzüge und Medizinprodukte prägt. Für mich ist eine erweiterte Produktprüfung noch keine überzeugende Antwort auf die Dynamik von KI. Ob eine neue Modellversion, neue Daten oder ein anderer Einsatz zur bisherigen Bewertung passen, muss der Anbieter erkennen und begründen. In kurzen Entwicklungszyklen wird daraus eine laufende Prüfaufgabe. Wer dafür ein eigenes Team hat, arbeitet unter anderen Bedingungen als ein kleiner Anbieter.

Was nachvollziehbar bleiben sollte

- Welche Änderung wurde vorgenommen und zu welchem Zweck?
- Welche Annahmen und Prüfungen der bisherigen Bewertung bleiben gültig?
- Welche neuen Risiken oder Grenzen wurden erkannt?
- Wer hat die Entscheidung getroffen und auf welcher Grundlage?

Diese Fragen sind meine praktische Orientierung. Welche Dokumente und Verfahren im Einzelfall vorgeschrieben sind, ergibt sich aus den jeweils einschlägigen Vorschriften.

04 · Was transparent gemacht werden muss

Vier unterschiedliche Pflichten

Artikel 50 unterscheidet nach Anwendung und Rolle. „KI muss gekennzeichnet werden“ ist dafür zu ungenau. Die folgenden vier Bereiche bilden die Grundstruktur. ^[6]

1. Direkte Interaktion mit KI

Anbieter müssen dafür sorgen, dass Menschen über die Interaktion mit einem KI-System informiert werden. Das entfällt, wenn die KI-Interaktion im jeweiligen Kontext für eine angemessen informierte, aufmerksame und verständige Person offensichtlich ist. Für gesetzlich zugelassene Strafverfolgungsanwendungen gelten gesonderte Voraussetzungen.

2. Technische Kennzeichnung synthetischer Inhalte

Anbieter von Systemen, die synthetische Audio-, Bild-, Video- oder Textinhalte erzeugen, müssen maschinenlesbare Kennzeichnung und Erkennbarkeit ermöglichen. Artikel 50 Absatz 2 berücksichtigt technische Machbarkeit und enthält unter anderem eine begrenzte Ausnahme für unterstützende Standardbearbeitung oder nicht wesentliche Veränderungen.

3. Emotionserkennung und biometrische Kategorisierung

Betreiber müssen die betroffenen Personen über den Einsatz informieren. Datenschutzrecht bleibt anwendbar. Diese Pflicht setzt voraus, dass der Einsatz überhaupt zulässig ist; ein Hinweis ersetzt keine Prüfung der Verbote aus Artikel 5.

4. Offenlegung gegenüber dem Publikum

Betreiber müssen bestimmte Deepfakes als künstlich erzeugt oder manipuliert offenlegen. Für KI-generierte oder manipulierte Texte zur Information der Öffentlichkeit über Angelegenheiten von öffentlichem Interesse gilt ebenfalls eine Offenlegungspflicht mit gesetzlichen Ausnahmen, unter anderem bei menschlicher Prüfung oder redaktioneller Kontrolle und übernommener redaktioneller Verantwortung.

Meine Einordnung · Ein Zeichen ist noch keine Erklärung

Ein Zeichen macht die Beteiligung von KI sichtbar. Es erklärt noch nicht, wer recherchiert, Ideen entwickelt, ausgewählt und Verantwortung übernommen hat. Eine technische Markierung und ein verständlicher Hinweis leisten zudem unterschiedliche Dinge.

Transparenz muss sichtbar machen, wer welchen Beitrag geleistet hat und wer für den Inhalt entsteht.

Zur Umsetzung liegen der freiwillige Transparenzkodex vom 10. Juni 2026 und Leitlinien der Kommission vom 20. Juli 2026 vor. Die gesetzlichen Pflichten folgen aus der Verordnung. ^{[21] [22]}

04 · Was transparent gemacht werden muss

Deepfakes, Kunst und offene Fragen

Realistisch kann auch eine erfundene Person wirken

Die Deepfake-Definition betrifft KI-generierte oder manipulierte Bild-, Ton- oder Videoinhalte, die wirklichen Personen, Gegenständen, Orten, Einrichtungen oder Ereignissen ähneln und fälschlich echt oder wahrheitsgemäß erscheinen würden. Reiner Text fällt nicht darunter. ^[2] ^[6]

Die Leitlinien und FAQ erläutern, dass auch plausibel existierende oder früher existiert habende Personen und Situationen relevant sein können. Ein fotorealistisches Bild einer erfundenen Frau kann deshalb erfasst sein. Dass die konkrete Person nicht existiert, nimmt den Inhalt nicht automatisch aus der Prüfung. Fotorealismus allein beantwortet die Rechtsfrage aber ebenfalls nicht: Aussage, Verwendungskontext und Erwartungen des Publikums sind mitzuberücksichtigen. ^[22] ^[23]

Kunst verändert die Form der Offenlegung

Für offensichtlich künstlerische, kreative, satirische, fiktionale oder vergleichbare Werke sieht Artikel 50 Absatz 4 eine angemessene Offenlegung vor, die Darstellung oder Genuss des Werks nicht beeinträchtigt. Das ist keine vollständige Kennzeichnungsfreiheit. Andere Rechtsvorschriften bleiben anwendbar. ^[6] ^[23]

Bearbeitung und Offenlegung sind getrennt zu prüfen

Die begrenzte Ausnahme für unterstützende Standardbearbeitung in Artikel 50 Absatz 2 betrifft die technische Anbieterpflicht. Sie ist keine pauschale Ausnahme von sämtlichen Betreiberpflichten. Umgekehrt macht nicht jede Retusche ein Foto automatisch zu einem kennzeichnungspflichtigen Deepfake. ^[6] ^[23]

Meine Einordnung · Ein Hinweis ersetzt kein Urteil

Ein Werk kann künstlich sein und etwas Wahres ausdrücken. Ein dokumentarisch wirkender Inhalt kann falsch sein, obwohl seine Herkunft offengelegt wurde. Die Kennzeichnung ordnet die Entstehung ein. Die Bewertung des Inhalts bleibt eine weitere Aufgabe. Ein Herkunftshinweis nimmt uns dieses Urteil nicht ab.

04 · Was transparent gemacht werden muss

Mein Betrachter-Test

Ich beginne bei der Wahrnehmung: **Kann dieses Bild oder ein naheliegender Ausschnitt davon für eine echte Aufnahme gehalten werden?** Mit dieser Frage habe ich auf LinkedIn KI-generierte und KI-bearbeitete Bilder betrachtet. ^[31]

Mein Betrachter-Test ist eine redaktionelle Orientierung. Er ersetzt keine rechtliche Prüfung. Für die Einordnung nach Artikel 50 sind zusätzlich Inhalt, Nutzungskontext und Publikum relevant. Ein Ausschnitt kann die Wahrnehmung verändern, ist aber nicht in jedem Fall der alleinige rechtliche Maßstab. ^{[22] [23]}

Ein Label erzählt nicht die ganze Entstehung

Die freiwilligen EU-Symbole unterscheiden unter anderem vollständig KI-generierte und teilweise KI-veränderte Inhalte. Es gibt auch ein Basissymbol; ergänzende Informationen können hinzukommen. Bezeichnungen wie „AI Generated“ oder „AI Modified“ ordnen die Produktion grob ein. Sie beziffern nicht den Anteil menschlicher Ideen, Recherche, Auswahl oder Verantwortung. ^[24]

Meine Einordnung · Die KI wird sichtbar. Wo bleibt der Mensch?

In diesem Paper stecken mein Kurs zum EU AI Act, meine Notizen, meine Fragen und meine Auswahl von Quellen. Ich habe mit Claude und ChatGPT diskutiert, Einordnungen entwickelt, widersprochen und Texte überarbeitet. Ein pauschales KI-Label erzählt diese Arbeit nicht. Es zeigt den Einsatz eines Werkzeugs, aber nicht, was ein Mensch inhaltlich eingebracht hat. Zur Transparenz gehört für mich auch, wie ein Inhalt entstanden ist und wer dafür einsteht. Menschliche Arbeit muss sichtbar bleiben.

Zum Mitnehmen

- Wahrnehmung und Entstehungsprozess sind verschiedene Fragen.
- Kennzeichnung ersetzt keine Information über menschliche Beiträge.
- Die Beschreibung der eigenen Arbeitsweise macht Verantwortung greifbarer.

04 · Was transparent gemacht werden muss

Wasserzeichen: Wer kann sie prüfen?

„Verschlüsselt“ ist für Text-Wasserzeichen oft missverständlich. Die hier beschriebenen Verfahren verschlüsseln nicht den Text. Sie beeinflussen die Auswahl von Wörtern oder Tokens nach einem geheimen Muster. Ein passender Detektor kann daraus ein statistisches Signal ableiten. ^[25] ^[26]

OpenAI: Zugang für ausgewählte Prüfende

OpenAI beschreibt mit textGrain ein solches Verfahren. Zum hier geprüften Stand ist die Text-Erkennung zunächst ausgewählten Forschenden und Fachorganisationen zugänglich. Der allgemeine öffentliche Zugang ist damit nicht gegeben. Öffentliche Prüfangebote für Bild oder Audio sind nicht automatisch Text-Detektoren. Die Abdeckung hängt außerdem vom Produkt, Modell und Einführungsstand ab. ^[25]

Anthropic: Erkennung in einer privaten Vorschau

Anthropic beschreibt eine Variante von SynthID-Text mit einem privaten Schlüssel. Eine Erkennungs-API wird in einer privaten Vorschau für zugelassene Organisationen angeboten, unter anderem aus Aufsicht, Forschung, Medien und Faktenprüfung. Zugang zur Prüfung bedeutet nicht, dass der geheime Schlüssel veröffentlicht wird. Ein gewöhnlicher KI-Textdetektor kann dieses Muster nicht ohne Weiteres auslesen. ^[26]

Was das Signal nicht aussagt

Ein Treffer beweist weder die Identität der schreibenden Person noch den Anteil ihrer Gedanken. Er bewertet auch nicht den Wahrheitsgehalt. Fehler und verlorene Signale sind möglich; ein fehlendes Signal beweist keine menschliche Entstehung. Die Angaben oben stammen von den Herstellern und sind keine unabhängige Prüfung ihrer Zuverlässigkeit. ^[25] ^[26]

Meine Einordnung · Transparenz braucht Zugang zur Prüfung

Wer markiert, entscheidet hier auch über den Zugang zur Erkennung. Die betroffene Person kann einen behaupteten Treffer nicht unbedingt selbst überprüfen. Für mich bleibt die Transparenz unvollständig, solange unabhängige Nachprüfung, verständliche Fehlergrenzen und Möglichkeiten zum Widerspruch fehlen. Ein technisches Signal darf nicht an die Stelle eines Urteils über Urheberschaft, Leistung oder Glaubwürdigkeit treten.

05 · Wer das umsetzt

Anbieter, Betreiber und Rollenwechsel

Anbieter und Betreiber haben unterschiedliche Pflichten. Ein Unternehmen kann beide Rollen einnehmen. Die Anbieterdefinition erfasst auch GPAI-Modelle; Betreiber verwenden KI-Systeme in eigener Verantwortung. ^[2]

Wann ein Betreiber zum Anbieter werden kann

Artikel 25 nennt für Hochrisiko-Systeme bestimmte Fälle: eigenes Branding eines bereits angebotenen Hochrisiko-Systems, eine wesentliche Veränderung bei fortbestehender Hochrisiko-Einstufung oder eine Änderung des Verwendungszwecks, durch die ein bisher nicht hochriskantes System hochriskant wird. Fine-Tuning allein ist deshalb kein automatischer Rollenwechsel. ^[7]

„Wesentliche Veränderung“ ist in Artikel 3 Nr. 23 definiert. Maßgeblich sind unter anderem Änderungen, die bei der ursprünglichen Konformitätsbewertung nicht vorgesehen waren und die Einhaltung der Anforderungen berühren oder den vorgesehenen Zweck verändern. Die Anwendung auf einen konkreten Eingriff bleibt eine fachliche Prüfung. ^[2]

Was Anbieter von Hochrisiko-Systemen organisieren müssen

- Erfüllung der einschlägigen Anforderungen und ein Qualitätsmanagementsystem.
- Technische Dokumentation, passende Konformitätsbewertung, EU-Konformitätserklärung und CE-Kennzeichnung.
- Registrierung, soweit vorgeschrieben, sowie Zusammenarbeit mit Behörden.
- Korrektur- und Informationsmaßnahmen, wenn Voraussetzungen dafür vorliegen.
- Aufbewahrung automatisch erzeugter Protokolle, soweit sie unter eigener Kontrolle stehen, für einen angemessenen Zeitraum von mindestens sechs Monaten, sofern anwendbares Recht nichts anderes vorsieht. ^{[1] [10]}

Meine Einordnung · Veränderung verschiebt Verantwortung

Wer ein System verändert, kann neue Verantwortung übernehmen. Die Grenze muss vor dem Eingriff erkennbar sein. Für kleine Teams ist dafür entscheidend, welche Informationen der ursprüngliche Anbieter zugänglich macht. Verantwortung ohne Zugang zum nötigen Wissen ist keine tragfähige Arbeitsteilung.

Zum Mitnehmen

- Fine-Tuning allein macht noch nicht zum Anbieter.
- Rollenwechsel hängen an konkreten Voraussetzungen.
- Die Pflichten für Hochrisiko-Systeme gelten nicht pauschal für jeden KI-Anbieter.

05 · Wer das umsetzt

Betreiberpflichten und Verantwortung

Artikel 26 richtet sich an Betreiber von Hochrisiko-Systemen. Zu den Pflichten zählen die Nutzung nach Gebrauchsanweisung, die Zuweisung menschlicher Aufsicht und die Überwachung des Betriebs. Soweit Betreiber die Eingabedaten kontrollieren, müssen diese für den vorgesehenen Zweck relevant und hinreichend repräsentativ sein. ^[8]

Bei bestimmten Risiken oder schwerwiegenden Vorfällen entstehen Informations- und Handlungspflichten. Automatisch erzeugte Protokolle unter eigener Kontrolle sind grundsätzlich mindestens sechs Monate aufzubewahren, soweit einschlägiges Recht keine andere Regel vorsieht. Vor einem Einsatz am Arbeitsplatz sind Arbeitnehmervertretung und betroffene Beschäftigte zu informieren. Absatz 11 betrifft die Information von Personen bei bestimmten Entscheidungen; die Zusammenarbeit mit Behörden steht in Absatz 12. ^[8]

Ein Chatbot-Fall aus dem Wettbewerbsrecht

Das OLG Hamm entschied am 12. Mai 2026 im Verfahren I-4 UKI 3/25 über unzutreffende Qualifikationsangaben des Chatbots einer ästhetischen Praxis. Das Gericht rechnete die Angaben dem Unternehmen zu. Fragen nach ärztlichen Qualifikationen waren vorhersehbar; die Antworten hätten kontrolliert werden können. ^[14]

Die Entscheidung beruht auf dem Lauterkeitsrecht, nicht auf Artikel 26 des AI Act. Sie belegt keine allgemeine Haftungsregel für jede KI-Ausgabe. Das OLG ließ die Revision zu. Diese Rechtsmittelmöglichkeit ist vom späteren Verfahrensstand zu unterscheiden: Die Verbraucherzentrale führt das Urteil zum 1. Juni 2026 als rechtskräftig. Der Grund für den Eintritt der Rechtskraft wird in den hier verwendeten Quellen nicht erläutert. ^{[14] [15]}

Meine Einordnung · Verantwortung wird tägliche Arbeit

Die Verantwortung für einen eingesetzten Chatbot lässt sich nicht einfach an dessen vermeintliche Eigenständigkeit abgeben. Kontrolle wird tägliche Arbeit. Ein Konzern kann dafür eigene Zuständigkeiten schaffen. In einem kleinen Betrieb landet dieselbe Aufgabe häufig bei wenigen Menschen, die bereits andere Aufgaben tragen. Die Verteilung dieser Arbeit entscheidet mit darüber, wer sich den Einsatz von KI leisten kann.

Zum Mitnehmen

- Artikel 26 adressiert Hochrisiko-Systeme.
- Die konkrete Rolle, Kontrolle über Daten und besondere Rechtsregeln zählen.
- Bestehendes Recht kann KI-Aussagen unabhängig vom AI Act erfassen.

05 · Wer das umsetzt

KI-Kompetenz ist eine laufende Aufgabe

Artikel 4 verpflichtet Anbieter und Betreiber zu Maßnahmen, die die KI-Kompetenz ihres Personals und anderer in ihrem Auftrag tätiger Personen fördern. Wissen, Erfahrung, Ausbildung, Einsatzkontext und betroffene Menschen sind zu berücksichtigen. Die aktuelle Fassung verlangt nicht, ein bestimmtes Kompetenzniveau jeder einzelnen Person zu garantieren. Zugleich sieht sie Unterstützung durch Kommission und Mitgliedstaaten vor. ^[9]

Drei Lernbereiche als Orientierung dieses Papers

Die folgenden Bereiche sind ein didaktisches Modell. Sie sind keine gesetzlich vorgeschriebenen Stufen und keine Zertifizierung.

- **Grundverständnis:** Was kann KI leisten, wo liegen typische Grenzen und welche Folgen kann ihr Einsatz für Menschen haben? Dazu gehören ein Bewusstsein für Datenschutz, Fehler und die eigene Verantwortung.
- **Anwendungskompetenz:** Das konkret eingesetzte System verstehen, Ergebnisse im Fachkontext beurteilen, Grenzen erkennen und wissen, wann geprüft, eingegriffen oder eskaliert werden muss.
- **Technische und organisatorische Vertiefung:** Je nach Rolle Kenntnisse über Entwicklung, Tests, Daten, Systemänderungen, Risikomanagement und Governance. Nicht jede Person braucht dafür Zugriff auf Modellarchitektur oder Code.

Meine Einordnung · Eine Schulung erledigt die Aufgabe nicht

KI-Kompetenz lässt sich nicht mit einem einmaligen Kurs abhaken. Systeme und Einsatzmöglichkeiten verändern sich, während die Verantwortung im Team bleibt. Wirksames Lernen braucht Zeit im Arbeitsalltag, konkrete Fälle und die Möglichkeit, Ergebnisse zu hinterfragen. Eine Schulungsbescheinigung kann diese Praxis dokumentieren, aber nicht ersetzen.

Was eine sinnvolle Lernpraxis für mich ausmacht

Aus meiner Sicht helfen konkrete Beispiele aus der eigenen Arbeit mehr als eine pauschale Schulung für alle. Wer Kunden informiert, braucht anderes Wissen als jemand, der ein Modell integriert oder Daten auswählt. Der Lernbedarf sollte sich deshalb mit Aufgaben und Systemen weiterentwickeln.

Zum Mitnehmen

- Artikel 4 gibt keine drei festen Kompetenzstufen vor.
- Maßnahmen sollen zu Rolle und Einsatz passen.
- Die Frage nach wirksamem Lernen bleibt auch nach einer Schulung offen.

05 · Wer das umsetzt

Deutsche Aufsicht und europäische Ebene

Das KI-MIG gilt seit 29. Juli 2026

Mit dem Inkrafttreten des KI-Marktüberwachungs- und Innovationsförderungsgesetzes hat die Bundesnetzagentur eine zentrale Rolle bei der Umsetzung der KI-Verordnung übernommen. Sie ist in ihren Zuständigkeitsbereichen Marktüberwachungsbehörde und fungiert als zentrale Anlauf- und Beschwerdestelle. ^[13]

Das Koordinierungs- und Kompetenzzentrum bei der Bundesnetzagentur unterstützt zuständige Stellen bei komplexen Entscheidungen und koordiniert ihre Zusammenarbeit. Fachaufsichten bleiben je nach Produktbereich und Zuständigkeit beteiligt. Die konkrete Aufsicht folgt daher nicht allein dem Sitz eines Unternehmens oder dem Schlagwort „KI“.

Unterstützung und Reallabore

Die Bundesnetzagentur beschreibt ein KI-Reallabor als Instrument zur begleiteten Entwicklung und Erprobung, insbesondere für KMU und Start-ups. Hinzu kommen Informationsangebote und der europäische AI Act Service Desk. Die Verordnung sieht eigene Unterstützungsmaßnahmen für kleinere Unternehmen vor. ^[13] ^[20]

Das AI Office gehört zum Gesamtbild

Auf EU-Ebene hat das AI Office Aufgaben bei GPAI-Modellen und, nach der geänderten Zuständigkeitsordnung, auch bei bestimmten KI-Systemen. Nationale Aufsicht und europäische Zuständigkeit müssen deshalb gemeinsam betrachtet werden. Artikel 74 und 75 enthalten dazu konkrete Regeln und Ausnahmen. ^[1]

Meine Einordnung · Beratung nimmt die Umsetzung nicht ab

Unterstützung ist vorgesehen, und sie kann hilfreich sein. Eine Anlaufstelle übernimmt aber weder die tägliche Prüfung noch automatisch die Kosten eines Unternehmens.

Zum Mitnehmen

- Das KI-MIG gilt, die Bundesnetzagentur ist zentrale Anlaufstelle.
- Zentrale Koordinierung und sektorale Zuständigkeiten bestehen nebeneinander.
- Europäische Zuständigkeiten sind zusätzlich zu beachten.

06 · Was offen bleibt

Drei mögliche Vorteile und ihre Kosten

Gute KI-Governance kann praktische Vorteile haben. Drei davon sind für mich entscheidend. Sie entstehen durch funktionierende Abläufe, nicht allein durch das Vorhandensein von Unterlagen.

- **Risiken früher erkennen:** Annahmen, Tests und Grenzen prüfen, bevor ein Problem Menschen betrifft.
- **Verantwortung nachvollziehbar machen:** Zuständigkeiten, Entscheidungen und Eingriffe so festhalten, dass sie geprüft werden können.
- **Wiederkehrende Arbeit erleichtern:** Wissen und brauchbare Verfahren aufbauen, statt jede Frage von vorn zu lösen.

Meine Einordnung · Die Kosten entstehen vorher

Der spätere Umsatz finanziert die Vorleistung nicht. Ein kleines Unternehmen muss Zeit, Fachwissen und Geld bereitstellen, bevor sein Hochrisiko-Produkt Umsatz erzielt. Ein großer Anbieter verteilt ähnliche Aufgaben auf bestehende Abteilungen und viele Produkte. Diese ungleichen Voraussetzungen verschwinden nicht dadurch, dass die Regeln für alle gelten.

Hilfe ist mehr als ein Verweis auf eine Anlaufstelle

Artikel 62 sieht Unterstützung für kleinere Unternehmen vor. Hinzu kommen bestimmte vereinfachte Dokumentationsmöglichkeiten und differenzierte Bußgeldobergrenzen. Es wäre falsch, diese Hilfen zu verschweigen. Ebenso wenig wäre es richtig, daraus eine Übernahme der gesamten Umsetzungsarbeit oder ihrer Kosten abzuleiten. ^[1] ^[11] ^[20]

Meine Frage an die Umsetzung ist konkret: Welche Kosten und welcher Zeitaufwand bleiben nach der Unterstützung übrig? Erst dann lässt sich beurteilen, ob ein kleines Team die Anforderungen tatsächlich tragen kann.

Zum Mitnehmen

- Schutz entsteht durch wirksame Praxis.
- Unterstützung muss die verbleibende Belastung spürbar verringern.
- Tragfähigkeit gehört für mich zur Qualität von Regulierung.

06 · Was offen bleibt

Wer an der Ausgestaltung beteiligt ist

OpenAI, Anthropic und Google waren an der Erarbeitung des Transparenzkodex zu Artikel 50 beteiligt. Die offizielle Teilnehmerliste vom 8. Dezember 2025 nennt Anthropic Ireland und Google in Arbeitsgruppe 1 zur technischen Kennzeichnung und Erkennung. OpenAI ist zusätzlich in Arbeitsgruppe 2 zur Offenlegung durch Betreiber aufgeführt. Auch weitere Unternehmen, Forschung und Zivilgesellschaft nahmen teil. ^[27]

Die Kommission beschreibt einen von unabhängigen Vorsitzenden geleiteten Prozess, den das AI Office unterstützte. Der freiwillige Kodex konkretisiert die Umsetzung bestehender Pflichten. ^[21]

Meine Einordnung · Mitwirkung ist auch eine Ressourcenfrage

Wer Personal, technisches Wissen und Zeit in solche Prozesse einbringen kann, hat Möglichkeiten zur Mitgestaltung. Kleine Teams müssen die für sie relevanten Ergebnisse später verstehen und umsetzen, können aber nicht im gleichen Umfang an jedem Tisch sitzen. Wer am Tisch sitzt, schreibt mit, wie Pflichten in der Praxis aussehen. Darin sehe ich eine Machtfrage.

Marktbewegungen sind noch kein Wirkungsnachweis

Cohere und Aleph Alpha meldeten am 16. September 2026 eine verbindliche Vereinbarung. Laut Unternehmensmitteilung stand der Vollzug unter behördlichem Genehmigungsvorbehalt. Aus einer solchen Ankündigung folgt weder eine bereits vollzogene Übernahme noch ein Beleg dafür, dass der AI Act diese Marktbewegung verursacht hat. ^[17]

Der AI Act regelt Pflichten. Ob daraus Schutz, faire Chancen und nachvollziehbare Verantwortung werden, entscheidet sich in der Praxis. Diese Folgen möchte ich weiter beobachten und an konkreten Fällen prüfen.

**Bleibt meine Frage: Schützt der AI Act eine europäische Wirtschaft, die mithalten kann?
Oder schützt er Nutzer in einer Wirtschaft, die zuschauen muss?**

Quellen und weiterführende Lektüre

Quellen zum Nachlesen

[1] KI-Verordnung, konsolidierte Fassung vom 27.07.2026

EUR-Lex. Verordnung (EU) 2024/1689 in der durch den Digital-Omnibus geänderten Fassung.

[2] Anwendungsbereich und Begriffe

Europäische Kommission, AI Act Service Desk. Artikel 2 und 3; weiterführende Artikel über die Navigation.

[3] Anwendungsfristen

Europäische Kommission, AI Act Service Desk. Artikel 113, konsolidierter Stand 27.07.2026.

[4] Verbotene KI-Praktiken

Europäische Kommission, AI Act Service Desk. Artikel 5 mit Voraussetzungen und Ausnahmen.

[5] Einstufung von Hochrisiko-Systemen

Europäische Kommission, AI Act Service Desk. Artikel 6; Anhänge I und III sind über die Navigation erreichbar.

[6] Transparenzpflichten

Europäische Kommission, AI Act Service Desk. Artikel 50 zu Interaktion, synthetischen Inhalten, Biometrie und Deepfakes.

[7] Verantwortung entlang der Wertschöpfungskette

Europäische Kommission, AI Act Service Desk. Artikel 25 zum Wechsel in die Anbieterrolle.

[8] Pflichten der Betreiber von Hochrisiko-Systemen

Europäische Kommission, AI Act Service Desk. Artikel 26.

[9] KI-Kompetenz

Europäische Kommission, AI Act Service Desk. Artikel 4, geändert durch den Digital-Omnibus.

[10] Pflichten der Anbieter von Hochrisiko-Systemen

Europäische Kommission, AI Act Service Desk. Artikel 16; weitere Anforderungen in Artikeln 8 bis 21, 43, 47 und 48.

[11] Geldbußen und Verhältnismäßigkeit

Europäische Kommission, AI Act Service Desk. Artikel 99 einschließlich der Regeln für KMU und kleine Midcaps.

Quellen und weiterführende Lektüre

Quellen und Einordnung

[12] Modelle mit allgemeinem Verwendungszweck

Europäische Kommission, AI Act Service Desk. Artikel 53 zu den Grundpflichten von GPAI-Anbietern.

[13] KI-MIG und deutsche Aufsicht

Bundesnetzagentur, 29.07.2026: Bundesnetzagentur übernimmt zentrale Rolle bei der Umsetzung der KI-Verordnung.

[14] Chatbot-Angaben vor dem OLG Hamm

Justiz NRW, Pressemitteilung vom 12.05.2026. Verfahren I-4 UKI 3/25, Verbraucherzentrale NRW gegen Aesthetify GmbH.

[15] Verfahrensstand zum Urteil des OLG Hamm

Verbraucherzentrale NRW, Stand 01.06.2026. Bericht der klagenden Organisation, die das Urteil als rechtskräftig führt.

[16] Rücknahme der KI-Haftungsrichtlinie

Europäische Kommission, Amtsblatt C/2025/5423 vom 06.10.2025. Zurückgezogen: COM(2022) 496, Verfahren 2022/0303(COD).

[17] Cohere und Aleph Alpha

Unternehmensmitteilung vom 16.09.2026 zur verbindlichen Vereinbarung. Der angekündigte Vollzug steht unter Genehmigungsvorbehalt.

[18] EU AI Act Essentials

KI-Campus. Kurs von appliedAI Institute for Europe und Technischer Universität München. Thematische Orientierung der ursprünglichen Fassung.

[19] GPAI Code of Practice

Europäische Kommission. Freiwilliger Kodex zur Unterstützung des Nachweises der Erfüllung gesetzlicher GPAI-Pflichten.

[20] Unterstützung kleiner Unternehmen

Europäische Kommission, AI Act Service Desk. Artikel 62 zu KMU, Start-ups und weiteren erfassten kleinen Unternehmen.

[21] Transparenzkodex für KI-generierte Inhalte

Europäische Kommission. Endfassung vom 10.06.2026; freiwillige Umsetzungshilfe zu Artikel 50.

[22] Leitlinien zu Artikel 50

Europäische Kommission, 20.07.2026. Auslegung der Transparenzpflichten für Anbieter und Betreiber.

Quellen und weiterführende Lektüre

Quellen und Einordnung

[23] Fragen und Antworten zu Artikel 50

Europäische Kommission, Stand 24.07.2026. Deepfake-Begriff, Kontext, Ausnahmen und Übergangsfrist.

[24] EU-Symbole für die Kennzeichnung

Europäische Kommission, Stand 13.10.2026. Freiwillige Kennzeichnungshilfen für erzeugte oder veränderte Inhalte.

[25] Text-Wasserzeichen bei OpenAI

OpenAI, 05.10.2026: Our approach to EU text provenance rules. Herstellerangaben zu textGrain und beschränktem Detektorzugang.

[26] Text-Wasserzeichen bei Anthropic

Anthropic, 14.08.2026, aktualisiert 01.09.2026: How Claude's text watermark works. Herstellerangaben zur Erkennung; Veröffentlichungsdatum direkt an der Quelle geprüft.

[27] Teilnehmende am Transparenzkodex

Europäische Kommission, Liste vom 08.12.2025. OpenAI: Arbeitsgruppen 1 und 2; Anthropic Ireland und Google: Arbeitsgruppe 1.

[28] Konformität bei wesentlichen Änderungen

Europäische Kommission, AI Act Service Desk. Artikel 43, insbesondere Absatz 4.

[29] Beobachtung nach dem Inverkehrbringen

Europäische Kommission, AI Act Service Desk. Artikel 72 zur fortlaufenden Überwachung von Hochrisiko-Systemen.

[30] Regulierungsaufwand und Unternehmensgröße

OECD: Smart Regulations, Strong Business, Kapitel zu Treibern regulatorischer Belastung. Allgemeine Einordnung, kein Wirkungsnachweis zum AI Act.

[31] Der Betrachter-Test

Elfie Schürfeld-Todor, LinkedIn. Eigene redaktionelle Orientierung zur Wahrnehmung KI-generierter und KI-bearbeiteter Bilder.

[32] Gemeinsamer Rahmen des europäischen Produktrechts

Europäische Kommission: New Legislative Framework. Gemeinsamer Rechtsrahmen unter anderem für Aufzüge, Medizinprodukte und den AI Act; keine identischen Prüfverfahren.

Rechtsverbindlich sind die amtlich veröffentlichten Rechtsakte. Der AI Act Service Desk bietet eine gut zugängliche Lesefassung. Unternehmensmitteilungen sind als solche ausgewiesen; persönliche Bewertungen im Paper sind keine Aussagen dieser Quellen.

Über die Autorin



Mit KI bearbeitet

Elfie Schürfeld-Todor

Ich bin Kommunikationsstrategin, Autorin und AI Search Strategist & Project Manager bei duwerk. Auf 11iE schreibe ich über KI, Kommunikation und Gesellschaft. Meine Kunst veröffentliche ich als Euphemia Stokefield.

KI ist mein Sparringspartner. Die Gedanken und die Verantwortung für die Inhalte liegen bei mir.

[Über mich](#) · [Fakten & Quellen](#) · [LinkedIn](#)

Zur Entstehung

Dieses Paper begann mit meinem Kurs zum EU AI Act und meinen eigenen Notizen. Ich habe Fragen entwickelt, Quellen ausgewählt und meine Positionen im Austausch mit Claude und ChatGPT weiter ausgearbeitet. Die KI unterstützte Recherche, Formulierung und Gestaltung. Ich habe die Entwürfe diskutiert, korrigiert und überarbeitet.

Die persönlichen Einordnungen, die Auswahl dessen, was ich veröffentliche, und die Verantwortung für den Inhalt liegen bei mir. Welche Primärquellen die rechtlichen Aussagen stützen, ist über die nummerierten Links nachvollziehbar.

Ausgabe vom 15.10.2026, redaktionell überarbeitet am 18.10.2026. Die Erstfassung stammt vom 21.05.2026. Quellen und Inhaltsverzeichnis sind anklickbar. Dieses Paper bietet allgemeine Information und persönliche Einordnung, keine Rechtsberatung.

Bleib neugierig. Bleib menschlich.