

VORLESUNGSSKRIPT

Die KI-Verordnung

Risikobasierte Regeln für Künstliche Intelligenz

MODUL

**Governance, Risk, Compliance & Ethics, Teil
2**

SEMESTER

WS 26/27

VERSION

1.0

Prof. Dr. Markus Oermann

Dozent

markus.oermann@thws.de

Technische Hochschule Würzburg-Schweinfurt

Stand: 23.07.2026

Inhalt

1 Hintergrund und Entstehungsgeschichte	3
1.1 Ein Rechtsrahmen für vertrauenswürdige KI	3
1.2 Vom Vorschlag zur geltenden Verordnung	3
2 Anwendungsbereich und Definitionen	4
2.1 Räumlich: ein breites Marktortprinzip	4
2.2 Sachliche Begrenzungen	4
2.3 Was ist ein „KI-System“?	4
3 Der risikobasierte Ansatz	5
4 Verbotene Praktiken (Art. 5 KI-VO)	6
4.1 Spezialfall: biometrische Echtzeit-Fernidentifizierung	6
5 Hochrisiko-KI (Art. 6 ff. KI-VO)	7
5.1 Zwei Wege in die Hochrisiko-Klasse	7
5.2 Das Korrektiv des Art. 6 Abs. 3	7
5.3 Anbieter und Betreiber	8
5.4 Die Pflichten der Anbieter (Art. 8–15 KI-VO)	8
5.5 Konformitätsbewertung und Pflichten nach Markteinführung	9
6 Begrenztes Risiko: Transparenzpflichten (Art. 50 KI-VO)	10
7 General Purpose AI und KI-Kompetenz	11
7.1 GPAI-Modelle (Art. 53–55 KI-VO)	11
7.2 KI-Kompetenz (Art. 4 KI-VO)	11
8 Governance und Zeitleiste	12
8.1 Wer wacht über die KI-VO?	12
8.2 Die gestaffelte Anwendbarkeit (Art. 113 KI-VO)	12
9 Individualrechte, Sanktionen und Haftungsausblick	13
9.1 Zwei Individualrechte	13
9.2 Sanktionen (Art. 99 KI-VO)	13
9.3 Haftungsausblick: PLD und AILD	14
10 Von der Ethik zum Recht	15
11 Quellen	16
11.1 Literatur	16
11.2 Normen & Standards	16

In der vorigen Einheit haben wir das Informationssicherheitsrecht entlang seiner zentralen Rechtsquellen kennengelernt: die Resilienz kritischer Einrichtungen (CER-Richtlinie und KRITIS-Dachgesetz), die Cybersicherheit nach NIS2-Richtlinie und BSI-Gesetz sowie die strafrechtliche Flanke der §§ 202a ff. StGB. Diese Regelwerke schützen die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen. Sie fragen aber nicht danach, *was* ein System inhaltlich tut. Genau hier setzt die KI-Verordnung an: Sie reguliert eine Grundlagentechnologie der Digitalen Gesellschaft und ihre Anwendungen, und sie tut dies mit Blick auf Sicherheit, Gesundheit und Grundrechte.

01

KAPITEL

Hintergrund und Entstehungsgeschichte

1.1 Ein Rechtsrahmen für vertrauenswürdige KI

Die KI-Verordnung (KI-VO), die oft nach ihrem englischsprachigen Titel auch als **AI Act** bezeichnet wird, ist Teil eines größeren Pakets der EU-Kommission zur Unterstützung *vertrauenswürdiger* künstlicher Intelligenz. Neben der Verordnung selbst gehören dazu das KI-Innovationspaket für KMU und Start-ups sowie der Koordinierte Plan für KI. Die Kommission bewirbt die KI-VO selbstbewusst als den **ersten umfassenden Rechtsrahmen für KI weltweit** (auch wenn die Verordnung selbst einige sehr zentrale Fragen offen lässt). Diese Vorreiterrolle ist Programm: Die EU möchte global Standards setzen.

Wichtig ist eine doppelte Abgrenzung. Die KI-VO enthält **keine** Regelungen zur zivilrechtlichen Haftung für die Ergebnisse von KI und auch keine substanziellen immaterialgüterrechtlichen Vorgaben. Sie ist Produktsicherheits- und Grundrechtsschutzrecht, kein zivilrechtliches Haftungsrecht. Wer durch eine KI geschädigt wird, findet seine Ansprüche also nicht hier, sondern, wie wir am Ende sehen, im allgemeinen und im spezielleren Haftungsrecht.

1.2 Vom Vorschlag zur geltenden Verordnung

Die Entstehung zog sich über mehr als drei Jahre. Am **21. April 2021** legte die Kommission den Vorschlag vor; das Vorhaben galt als eines der wichtigsten Regulierungsprojekte der Amtszeit 2019–2024. Nach der Verabschiedung in Parlament (März 2024) und Rat (Mai 2024) erfolgte am **12. Juli 2024** die Veröffentlichung im Amtsblatt. **In Kraft getreten** ist die KI-VO am **1. August 2024 als Verordnung (EU) 2024/1689**.

02

KAPITEL

Anwendungsbereich und Definitionen

2.1 Räumlich: ein breites Markortprinzip

Der räumliche Anwendungsbereich ist bewusst weit gezogen (Art. 2 KI-VO). Die Verordnung gilt für **alle Anbieter, Betreiber, Hersteller, Importeure und Händler**, die KI-Modelle, KI-Systeme oder KI-basierte Dienste in der Union in Verkehr bringen oder in ihre Produkte integrieren, und zwar **unabhängig von ihrem Standort und vom Standort der Server**. Maßgeblich ist also nicht, wo das Unternehmen sitzt, sondern wo das Ergebnis auf den Markt trifft (Markortprinzip). Erklärtes Ziel ist der **Brüssel-Effekt**, die globale Ausstrahlungswirkung des EU-Rechts. Das erzeugt eine Spannungslage insbesondere im Verhältnis zu den USA, deren Regulierungsphilosophie (jedenfalls aus Bundesebene) deutlich zurückhaltender ist.

2.2 Sachliche Begrenzungen

So weit der räumliche Zugriff ist, so weit sind auch die sachlichen Ausnahmen (Art. 2 KI-VO). Ausgenommen sind KI für **militärische, Verteidigungs- oder nationale Sicherheitszwecke** (Abs. 3), KI der Sicherheitsbehörden von Drittstaaten (Abs. 4), KI ausschließlich für **wissenschaftliche Zwecke** (Abs. 6) sowie reine Forschungs-, Test- und Entwicklungstätigkeiten vor dem Inverkehrbringen (Abs. 8). Ebenfalls außen vor bleibt der Betrieb von KI im Rahmen **persönlicher, nicht-beruflicher Tätigkeiten** (Abs. 10); die Verordnung adressiert also nicht den privaten Endnutzer. Open-Source-KI ist privilegiert, allerdings nicht, soweit es um verbotene, Hochrisiko- oder generative Systeme geht (Abs. 12).

ÜBUNG · BEGRIFFE

Das **Markortprinzip** knüpft an den Ort der Marktwirkung an, nicht an den Sitz des Anbieters; eine rein **persönliche, nicht-berufliche** KI-Nutzung fällt aus dem Anwendungsbereich.

2.3 Was ist ein „KI-System“?

Die Schlüsseldefinition steht in Art. 3 Nr. 1 KI-VO. Ein **KI-System** ist danach ein *maschinengestütztes System*, das für einen *in unterschiedlichem Grade autonomen Betrieb* ausgelegt ist, nach der Betriebsaufnahme *anpassungsfähig* sein kann und aus den erhaltenen Eingaben für *explizite oder implizite Ziele* ableitet, wie es Ausgaben (Vorhersagen, Inhalte, Empfehlungen oder Entscheidungen) erzeugt, die physische oder virtuelle Umgebungen beeinflussen. Drei Merkmale tragen die Definition: **Autonomiegrad**, **Anpassungsfähigkeit** und die **Ableitung von Ausgaben** aus Eingaben. Klassische, deterministisch programmierte Software fällt damit nicht unter den Begriff.

Die Formulierung orientiert sich bewusst an der **OECD-Definition von KI-Systemen**, um internationale Anschlussfähigkeit herzustellen. Zur Auslegung hat das KI-Büro der EU-Kommission am 6. Februar 2025 Leitlinien veröffentlicht.

03

KAPITEL

Der risikobasierte Ansatz

Das Grundkonzept der KI-VO ist einfach: Statt jede KI gleich zu behandeln, staffelt die Verordnung die Anforderungen nach dem angenommenen **Risiko** für Sicherheit, Leben und Grundrechte. Daraus ergibt sich eine Pyramide aus vier Stufen.

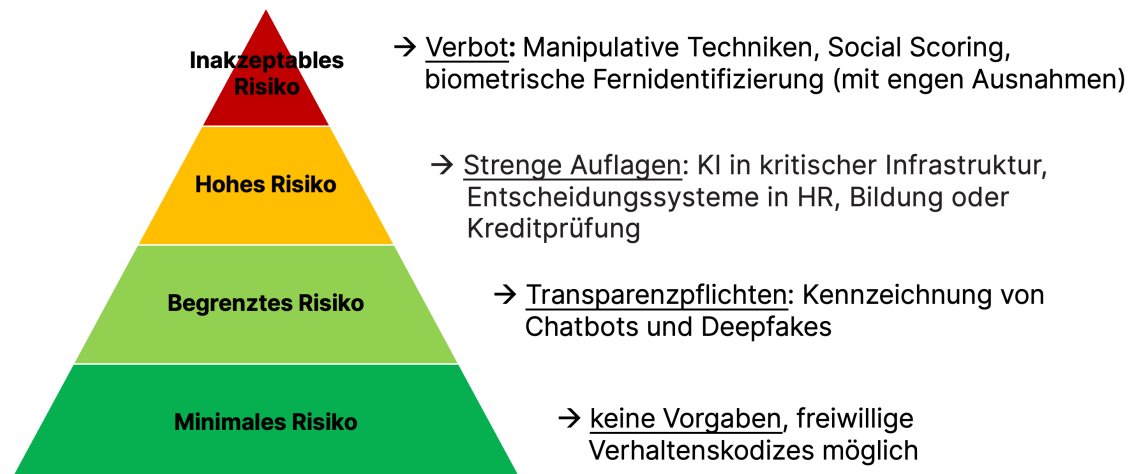


Abbildung 1: Die Risikopyramide der KI-VO: Mit steigendem Risiko für Sicherheit, Leben und Grundrechte verdichten sich die Pflichten: vom Verbot über strenge Auflagen und Transparenzpflichten bis zu unregulierter Minimalrisiko-KI (eigene Darstellung).

Je höher das Risiko, desto dichter die Pflichten; die ganz große Masse alltäglicher KI bleibt unreguliert. Erproben Sie diese Logik im folgenden Widget, indem Sie konkrete Anwendungsfälle einsortieren:

04

KAPITEL

Verbotene Praktiken (Art. 5 KI-VO)

An der Spitze der Pyramide stehen die (etwas plakativ so genannten) „Todsünden“. Art. 5 Abs. 1 KI-VO verbietet KI-Praktiken, die als Bedrohung für Sicherheit, Leben und Grundrechte gelten. Dazu zählen insbesondere:

- **manipulative KI**, die durch unterschwellige Techniken einen erheblichen Schaden verursacht (lit. a);
- KI, die **Vulnerabilitäten** (etwa wegen Alter, Behinderung oder wirtschaftlicher Lage) zur Verhaltensbeeinflussung ausnutzt (lit. b);
- umfassendes, kontextübergreifendes **Social Scoring** (lit. c);
- **Predictive Policing**, das allein auf personenbezogene Profile gestützt Straftaten vorhersagt (lit. d);
- **Emotionserkennung** am Arbeitsplatz und in Bildungseinrichtungen (lit. f);
- bestimmte Formen **biometrischer Kategorisierung** sowie das **ungezielte Scraping** von Gesichtsbildern zum Aufbau von Datenbanken.

Auch zur Auslegung dieser Verbote hat das KI-Büro Leitlinien vom 4. Februar 2025 vorgelegt.

Der **2026 politisch vereinbarte AI Omnibus** (siehe Vertiefung weiter unten) ergänzt den Katalog um ein weiteres Verbot: KI-Systeme, die **nicht-einvernehmliche intime Aufnahmen („Nudifier“)** oder **Missbrauchsdarstellungen von Kindern** erzeugen oder manipulieren, mit einer Übergangsfrist bis zum **2. Dezember 2026**.

4.1 Spezialfall: biometrische Echtzeit-Fernidentifizierung

Der heikelste Punkt war die **biometrische Live-Gesichtserkennung zur Strafverfolgung**. Hier prallten die Positionen frontal aufeinander: Das Parlament wollte ein generelles Verbot, der Rat war dagegen. Das Ergebnis ist ein **Kompromiss** (Art. 5 Abs. 1 lit. h, Abs. 2–5 KI-VO). Die **Echtzeit-Fernidentifizierung in öffentlich zugänglichen Räumen zu Strafverfolgungszwecken ist grundsätzlich verboten**, aber unter Genehmigungsvorbehalt in engen Ausnahmen zulässig: zur Suche nach einer vermissten Person, zur Abwehr einer konkreten und unmittelbaren terroristischen Bedrohung sowie zur Verfolgung von Tätern oder Verdächtigen schwerer Straftaten. Außerhalb dieser Ausnahmen werden biometrische Fernerkennungssysteme als hochriskant eingestuft und entsprechend streng reguliert.

QUICK-CHECK

Eine Schulsoftware soll während des Unterrichts die Emotionen der Lernenden auswerten, um die „Aufmerksamkeit“ zu messen. Wie ist das nach der KI-VO einzuordnen?

Hochrisiko-KI mit Konformitätsbewertung

Verbotene Praktik (Emotionserkennung in Bildungseinrichtungen)

Begrenztes Risiko mit Transparenzpflicht

Minimales Risiko ohne besondere Vorgaben

05

KAPITEL

Hochrisiko-KI (Art. 6 ff. KI-VO)

Unterhalb der Verbotsschwelle schließt sich das eigentliche Herzstück der Verordnung an. Die Regelungen zu Hochrisiko-KI haben ihre Wurzeln im **Produktsicherheitsrecht** und übertragen dessen Logik auf KI.

5.1 Zwei Wege in die Hochrisiko-Klasse

Art. 6 KI-VO kennt zwei Anknüpfungspunkte. Nach **Absatz 1** ist ein System hochriskant, wenn es als **Sicherheitsbauteil** in einem Produkt eingesetzt wird, das ohnehin dem EU-Sicherheitsrecht unterliegt und eine **Konformitätsbewertung durch Dritte** erfordert (Anhang I, z. B. Verkehrsmittel, Aufzüge, Spielzeug, Medizinprodukte). Nach **Absatz 2** ist es hochriskant, wenn sein Verwendungszweck in **Anhang III** gelistet ist und es nach einer **Einzelfallbewertung** Risiken für Gesundheit, Sicherheit oder Grundrechte birgt. Anhang III nennt unter anderem kritische Infrastrukturen, Bildung (etwa Prüfungsbewertung), Beschäftigung (etwa **Lebenslauf-Sortierung** im Recruiting), wesentliche Dienstleistungen (etwa **Kreditwürdigkeitsprüfung**), Strafverfolgung, Migration sowie Rechtspflege und demokratische Prozesse.

5.2 Das Korrektiv des Art. 6 Abs. 3

Damit nicht jede triviale Anwendung in einem Anhang-III-Feld zur Hochrisiko-KI wird, enthält **Art. 6 Abs. 3 KI-VO** ein Korrektiv: Ein gelistetes System ist *nicht* hochriskant, wenn es **kein erhebliches Risiko** für Gesundheit, Sicherheit oder Grundrechte birgt: insbesondere, weil es **das Ergebnis der Entscheidungsfindung nicht wesentlich beeinflusst**. Ausgeschlossen sind also Systeme, die menschliche Entscheidungen nur *unterstützen*, sie aber nicht übernehmen oder maßgeblich prägen. Die Anbieter müssen ihre Bewertung jedoch **dokumentieren** und das System registrieren (Art. 6 Abs. 4); die Kommission soll dazu Leitlinien bereitstellen.

5.3 Anbieter und Betreiber

Wer wie reguliert wird, hängt von der Rolle in der Wertschöpfungskette ab. Der **Anbieter** ist die Person, die ein KI-System oder -Modell entwickelt oder entwickeln lässt und in Verkehr bringt (also in Alltagssprache: der Hersteller).

Der **Betreiber** hingegen verwendet das System (nur) in eigener Verantwortung (jenseits rein privater Nutzung).

Der Anbieter bestimmt originär den Verwendungszweck und kann unerwünschte Verwendungen ausschließen. Entscheidend ist die **Umwidmungsregel** des Art. 25 KI-VO: Wer ein System unter eigenem Namen vertreibt, es wesentlich verändert oder durch tatsächliche Nutzung zu einem Hochrisiko-Zweck einsetzt, **tritt rechtlich an die Stelle des Anbieters** und übernimmt dessen Pflichten.

Die Klärung der eigenen Rolle ist deshalb der erste Compliance-Schritt überhaupt.

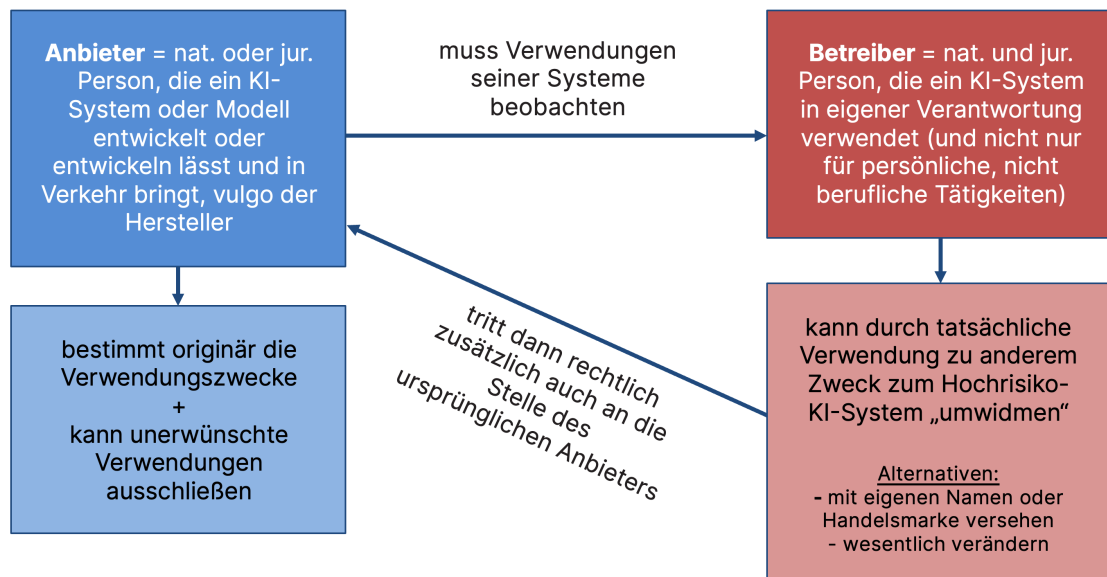


Abbildung 2: Anbieter und Betreiber im Überblick: Der Anbieter bestimmt originär den Verwendungszweck und beobachtet die Verwendung seiner Systeme; der Betreiber verwendet das System in eigener Verantwortung und kann durch Umwidmung, eigene Kennzeichnung oder wesentliche Veränderung selbst zum Anbieter werden (eigene Darstellung).

Testen Sie im folgenden Widget, welche Umstände einen Betreiber zum Anbieter werden lassen:

5.4 Die Pflichten der Anbieter (Art. 8–15 KI-VO)

Für Hochrisiko-Systeme gilt ein dichter Pflichtenkatalog, der den gesamten Lebenszyklus erfasst:

- **Risikomanagementsystem** mit Risikoanalyse und Milderungsmaßnahmen vor und nach Markteinführung (Art. 9);
- **Daten-Governance**: Training nur mit qualifizierten, repräsentativen Datensätzen (Art. 10);
- **technische Dokumentation** mit allen Informationen, die Behörden zur Prüfung benötigen (Art. 11);
- **Protokollierung** der Systemaktivitäten zur Rückverfolgbarkeit (Art. 12);

- **Transparenz** und klare Informationen für nachgelagerte Akteure, die „Bedienungsanleitung“ (Art. 13);
- **menschliche Aufsicht**, etwa durch eine Abschalteinrichtung (Art. 14);
- **Robustheit, Genauigkeit und Cybersicherheit** (Art. 15).

5.5 Konformitätsbewertung und Pflichten nach Markteinführung

Bevor ein Hochrisiko-System auf den Markt darf, durchläuft es die **Konformitätsbewertung** (Art. 43–49 KI-VO): Prüfung gegen die Anforderungen, Registrierung eigenständiger Anhang-III-Systeme in einer EU-Datenbank, Unterzeichnung einer Konformitätserklärung und schließlich die **CE-Kennzeichnung**. Bei wesentlichen Änderungen ist das Verfahren erneut zu durchlaufen.

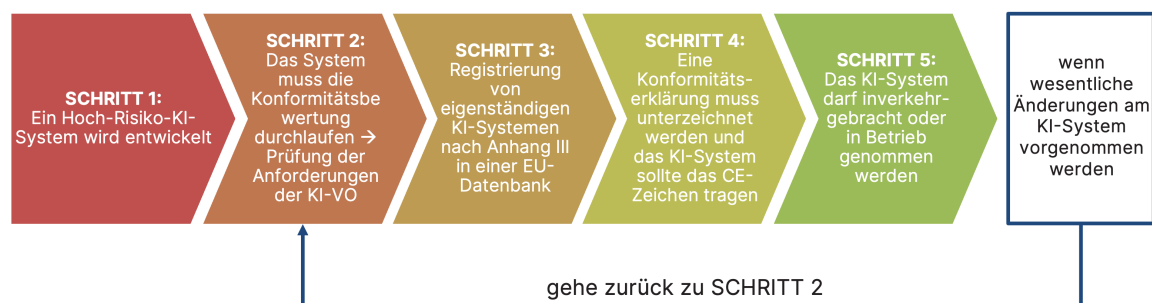


Abbildung 3: Der Weg eines Hochrisiko-KI-Systems zur Marktreife: von der Entwicklung über die Konformitätsbewertung, die Registrierung in der EU-Datenbank und die Konformitätserklärung bis zum Inverkehrbringen mit CE-Kennzeichnung. Wesentliche Änderungen führen zurück zu Schritt 2 (eigene Darstellung).

Nach der Markteinführung übernehmen die nationalen Marktüberwachungsbehörden die Aufsicht; **Betreiber** müssen die Verwendung nach Betriebsanleitung sicherstellen, Protokolle aufbewahren (Art. 26 KI-VO) und, als öffentliche Stellen sowie bestimmte private Betreiber von Anhang-III-Systemen, vor der Inbetriebnahme eine **Grundrechte-Folgenabschätzung** durchführen (Art. 27 KI-VO). **Anbieter** richten eine Beobachtung ihrer Systeme ein; beide melden schwerwiegende Vorfälle an die Behörden.

FALLSTUDIE

CV-Sortierung im Recruiting: hochriskant oder doch nicht?

Ein mittelständisches Unternehmen führt eine KI ein, die eingehende Bewerbungen automatisch bewertet und eine Rangliste der Kandidatinnen und Kandidaten erstellt. Die Personalabteilung lädt nur die ersten zehn zum Gespräch ein. Wie ist das System einzuordnen, und was folgt daraus?

Lösung. Bewerbermanagement bei der Einstellung ist ein in **Anhang III** gelisteter Verwendungszweck (Beschäftigung). Das System ist damit **grundsätzlich Hochrisiko-KI** nach Art. 6 Abs. 2 KI-VO. Das Korrektiv des **Art. 6 Abs. 3** greift hier nicht, denn die KI beeinflusst das Ergebnis *wesentlich*: Wer nicht in den Top Ten landet, wird faktisch

aussortiert; das ist mehr als bloße Unterstützung. Folge: Es gelten die Pflichten der Art. 8–15 (u. a. Daten-Governance gegen Diskriminierung nach Art. 10, menschliche Aufsicht nach Art. 14), die Konformitätsbewertung mit CE-Kennzeichnung sowie die Betreiberpflichten nach Art. 26. Das Unternehmen ist hier zunächst Betreiber; würde es das System wesentlich verändern oder unter eigenem Namen vertreiben, würde es nach Art. 25 zum Anbieter und müsste dessen volle Pflichten tragen.

06

KAPITEL

Begrenztes Risiko: Transparenzpflichten (Art. 50 KI-VO)

Eine Stufe tiefer auf der Risikopyramide reguliert die KI-VO nicht das *Ob*, sondern nur das *Offenlegen*. Art. 50 KI-VO verlangt **Transparenz**, wo Menschen sonst über die Natur einer Interaktion oder eines Inhalts getäuscht werden könnten. Anbieter eines Systems, das mit Menschen **interagiert** (etwa ein Chatbot), müssen offenlegen, dass es sich um eine KI handelt (Abs. 1). Wer **synthetische Inhalte generiert**, muss diese maschinenlesbar kennzeichnen (Stichwort „**Watermarking**“, Abs. 2). Betreiber von Systemen zur **Emotionserkennung oder biometrischen Kategorisierung** informieren die Betroffenen (Abs. 3). Und wer **Deepfakes** oder Texte von öffentlichem Interesse erzeugt, muss sie als künstlich erzeugt **kennzeichnen** (Stichwort „**Labeling**“, Abs. 4). Die Inhalte selbst werden nicht geregelt; reguliert wird allein die Erkennbarkeit.

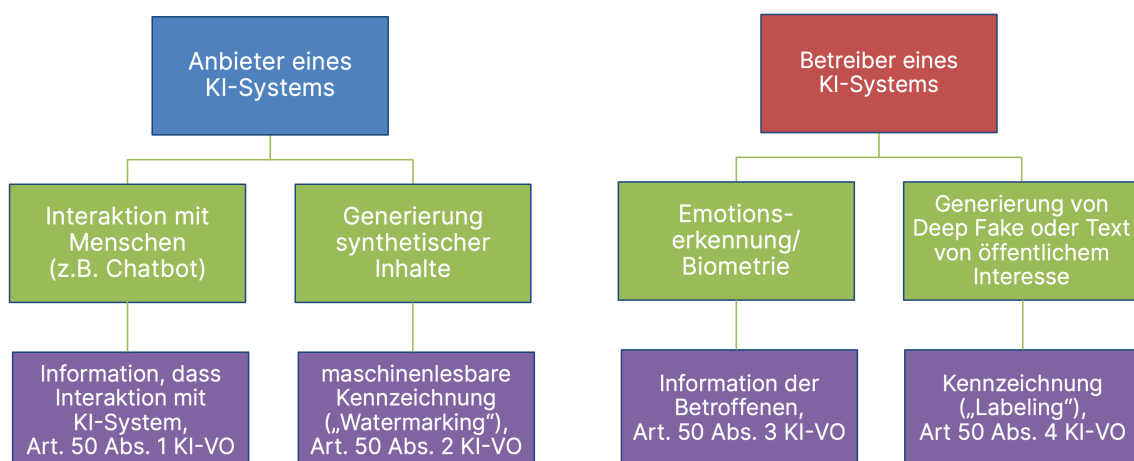


Abbildung 4: Die Transparenzpflichten des Art. 50 KI-VO im Überblick: Anbieter informieren bei Interaktion mit Menschen (Abs. 1) und kennzeichnen synthetische Inhalte maschinenlesbar (Abs. 2); Betreiber informieren Betroffene bei Emotionserkennung und biometrischer Kategorisierung (Abs. 3) und kennzeichnen Deepfakes sowie Texte von öffentlichem Interesse (Abs. 4) (eigene Darstellung).

07

KAPITEL

General Purpose AI und KI-Kompetenz

7.1 GPAI-Modelle (Art. 53–55 KI-VO)

Große Sprach- und Basismodelle passen schlecht in das anwendungsbezogene Risikoraster, weil ihre Verwendungszwecke offen sind. Die KI-VO adressiert sie deshalb gesondert als **KI-Modelle mit allgemeinem Verwendungszweck** (General Purpose AI, GPAI). Nach Art. 3 Nr. 63 KI-VO ist ein GPAI-Modell ein Modell, das (oft durch Training mit großen Datenmengen unter umfassender Selbstüberwachung) eine erhebliche **allgemeine Verwendbarkeit** aufweist, ein **breites Spektrum** unterschiedlicher Aufgaben kompetent erfüllt und in viele nachgelagerte Systeme integriert werden kann. Anbieter solcher Modelle müssen technische Dokumentation mit Fokus auf Trainingsverfahren und -daten bereitstellen, nachgelagerte Akteure informieren (Art. 53); in Drittstaaten ansässige Anbieter müssen zudem einen bevollmächtigten Vertreter in der EU benennen (Art. 54).

Verschärfte Pflichten treffen GPAI-Modelle mit **systemischem Risiko** (Art. 55 KI-VO): eigene Risikoanalyse und Minderungsmaßnahmen, Modellevaluation, Meldung schwerwiegender Vorfälle und Cybersicherheitsvorkehrungen. Das systemische Risiko wird grundsätzlich am **Rechenaufwand für das Training** festgemacht, derzeit bei mehr als 10^{25} FLOP (Art. 51 KI-VO), ergänzt um weitere Kriterien.

7.2 KI-Kompetenz (Art. 4 KI-VO)

Quer zu allen Risikostufen steht eine Pflicht, die jeden Einsatz betrifft. Nach **Art. 4 KI-VO** müssen Anbieter *und* Betreiber sicherstellen, dass ihr Personal und beauftragte Personen über ausreichende **KI-Kompetenz** verfügen: Fähigkeiten, Kenntnisse und ein Verständnis für den sachkundigen Einsatz von KI sowie ein Bewusstsein für Chancen, Risiken und mögliche Schäden (Art. 3 Nr. 56). Dabei sind technische Vorkenntnisse, Erfahrung, Ausbildung und Einsatzkontext zu berücksichtigen. Diese Pflicht gilt bereits **seit dem 2. Februar 2025** und betrifft praktisch jede Organisation, die KI nutzt. Der AI Omnibus schwächt sie 2026 redaktionell ab: Anbieter und Betreiber müssen die KI-Kompetenz ihres Personals nur noch **fördern**, statt sie im Ergebnis zu **gewährleisten**.

DEFINITION

GPAI vs. Hochrisiko-KI

Hochrisiko-Pflichten knüpfen an einen konkreten, riskanten *Verwendungszweck* an; GPAI-Pflichten knüpfen an das *Modell* selbst an, dessen Zwecke offen sind.

08

KAPITEL

Governance und Zeitleiste

8.1 Wer wacht über die KI-VO?

Die Durchsetzung ruht auf einem **mehrstufigen Governance-Gefüge** (vgl. Novelli et al. 2024). Auf supranationaler Ebene steht das bei der Kommission angesiedelte **KI-Büro (AI Office, DG CNECT)**, das insbesondere die GPAI-Anbieter beaufsichtigt; flankiert wird es vom **KI-Ausschuss (AI Board)**, einem beratenden **Forum** und einem **wissenschaftlichen Gremium (Scientific Panel)**. Auf nationaler Ebene benennen die Mitgliedstaaten **Notifizierungs- und Marktüberwachungsbehörden**; die Konformität prüfen unabhängige **notifizierte Stellen**.

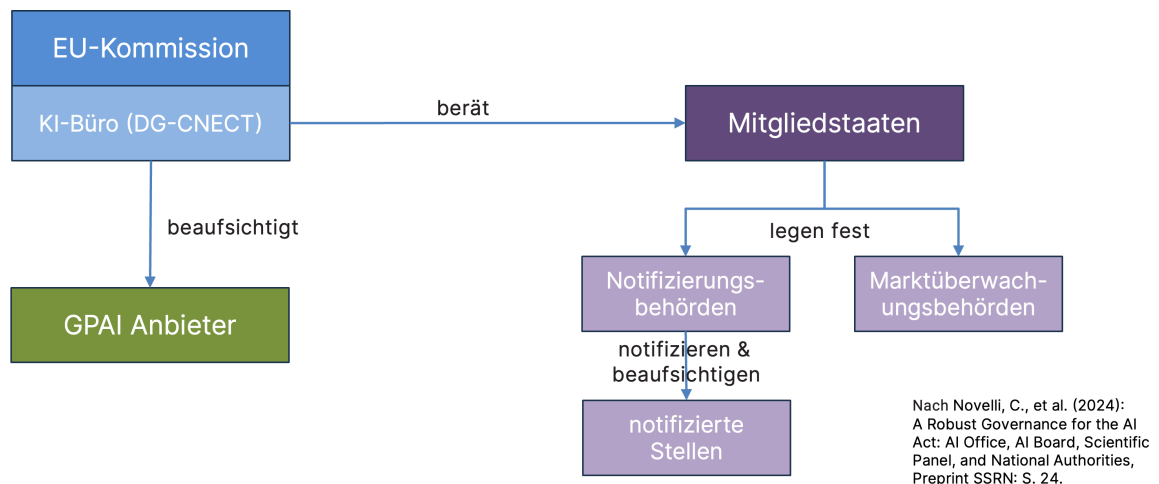


Abbildung 5: Governancestruktur der KI-VO (vereinfacht): Das KI-Büro der EU-Kommission beaufsichtigt die GPAI-Anbieter und berät die Mitgliedstaaten, die ihrerseits Notifizierungs- und Marktüberwachungsbehörden benennen; die Notifizierungsbehörden notifizierte Stellen und beaufsichtigen diese (eigene Darstellung, in Anlehnung an Novelli et al. 2024, S. 24).

8.2 Die gestaffelte Anwendbarkeit (Art. 113 KI-VO)

Die KI-VO gilt nicht auf einen Schlag, sondern in Etappen (Art. 113). Ursprünglich waren dafür vier Stufen vorgesehen; der **AI Omnibus** (siehe Vertiefung unten) hat zwei davon um über ein Jahr nach hinten verschoben. Die nach der politischen Einigung vom Mai 2026 maßgebliche Zeitleiste:

- **2. Februar 2025:** die **Verbote** (Kapitel I und II) sowie die KI-Kompetenz-Pflicht werden anwendbar (Letztere durch den Omnibus abgeschwächt; neu hinzu tritt das Verbot von „Nudifiern“ und KI-generiertem Missbrauchsmaterial, das ab **2. Dezember 2026** greift);
- **2. August 2025:** die Regeln zu **GPAI-Modellen**, zu den Behörden, zur **Governance** und zu den **Sanktionen** — hiervon rührt der Omnibus nicht;

- **2. August 2026:** die **Transparenzpflichten** des Art. 50 (Chatbot-Hinweis, Deepfake-Kennzeichnung); für die Kennzeichnungspflicht nach Abs. 2 gilt bei bereits im Verkehr befindlichen Systemen eine Übergangsfrist bis **2. Dezember 2026**;
- **2. August 2027:** die Frist der Mitgliedstaaten zur Einrichtung von **Reallaboren** (Art. 57), ursprünglich 2026;
- **2. Dezember 2027:** die eigenständigen **Anhang-III-Hochrisikosysteme** (Art. 6 Abs. 2), ursprünglich 2. August 2026;
- **2. August 2028:** die **produktbezogenen** Hochrisiko-Systeme (Art. 6 Abs. 1), ursprünglich 2. August 2027.

■ DEEP DIVE Vertiefung: Warum erst 2028 für Art. 6 Abs. 1?

Die produktbezogenen Hochrisiko-Systeme (Tor 1) bekommen nach wie vor die längste Schonfrist, weil sie in bestehende Konformitätsverfahren des sektoralen Produktsicherheitsrechts (Anhang I, z. B. Maschinen, Medizinprodukte) eingebettet werden müssen. Diese Verzahnung mit etablierten Prüfrezimes und notifizierten Stellen brauchte offenbar mehr Vorlauf als ursprünglich veranschlagt: Der AI Omnibus verschiebt beide Fristen um mehr als ein Jahr, ohne an der Grundlogik etwas zu ändern. Die eigenständigen Anhang-III-Anwendungsfälle (Tor 2) laufen nun ab dem 2. Dezember 2027 an, gut acht Monate vor den produktintegrierten Systemen.

09

KAPITEL

Individualrechte, Sanktionen und Haftungsausblick

9.1 Zwei Individualrechte

Auf Drängen des Parlaments geht die KI-VO über das im Produktsicherheitsrecht Übliche hinaus und gewährt zwei **Individualrechte**. Das **Recht auf Beschwerde** bei einer Marktüberwachungsbehörde besteht bei Verdacht eines Verstoßes und setzt keine eigene Betroffenheit voraus (Art. 85). Das **Recht auf Erläuterung** steht Betroffenen zu, deren Entscheidungen unter Beteiligung eines Anhang-III-Hochrisiko-Systems ergehen (Art. 86).

9.2 Sanktionen (Art. 99 KI-VO)

Die Mitgliedstaaten müssen wirksame Sanktionen vorsehen. Der Rahmen ist gestaffelt: Verstöße gegen die **verbotenen Praktiken** können mit bis zu **35 Mio. € oder 7 %** des weltweiten Jahresumsatzes geahndet werden; Verstöße gegen sonstige Pflichten (auch für GPAI) mit bis zu 15 Mio. € oder 3 %; fehlerhafte Auskünfte mit bis zu 7,5 Mio. € oder 1,5 % (jeweils der höhere Wert).

9.3 Haftungsausblick: PLD und AILD

Die von der KI-VO bewusst ausgelassene zivilrechtliche Haftung für KI-Schäden sollte durch zwei flankierende Richtlinienvorschläge der Kommission vom 28. September 2022 geschlossen werden. Die **KI-Haftungsrichtlinie (AILD)** wollte die Beweisführung für Geschädigte erleichtern, unter anderem durch einen Anspruch auf Offenlegung der nach der KI-VO dokumentierten Informationen und eine widerlegbare Kausalitätsvermutung mit Beweislastumkehr. Dieser Vorschlag ist Anfang 2025 jedoch **gescheitert**. Verabschiedet wurde dagegen die **reformierte Produkthaftungsrichtlinie (EU) 2024/2853**: Sie erstreckt die verschuldensunabhängige Herstellerhaftung, die nicht an ein schuldhaftes Verhalten, sondern an die geschaffene Gefahrenquelle anknüpft, ausdrücklich auf Software und damit auf KI-Systeme. Sie ist bis zum 9. Dezember 2026 in deutsches Recht umzusetzen.

Wohin führt das im Einzelfall? Das folgende Widget führt durch die Haftungslogik je nach Schadensart:

FALLSTUDIE

Wenn die KI Schaden anrichtet

Ein autonom navigierender Lagerroboter mit eingebauter KI verletzt eine Mitarbeiterin. Sie möchte Schadensersatz. Findet sie ihren Anspruch in der KI-VO?

Lösung. Nein. Die KI-VO regelt Bedingungen für den Marktzugang, Risikomanagement und Aufsicht, aber **keine Haftungsansprüche** für KI-Schäden. Den Anspruch sucht die Geschädigte im Haftungsrecht: nach der reformierten **Produkthaftungsrichtlinie (EU) 2024/2853**, die als verschuldensunabhängige Haftung an die vom Hersteller geschaffene Gefahrenquelle anknüpft und nun auch Software erfasst, sowie im allgemeinen Deliktsrecht. Die ursprünglich vorgesehene **KI-Haftungsrichtlinie** mit ihren Beweiserleichterungen hätte ihr geholfen; sie ist aber Anfang 2025 gescheitert, sodass die beweisrechtliche Lage anspruchsvoll bleibt. Die KI-VO wirkt hier nur *mittelbar*: Verletzt der Hersteller ihre Pflichten, kann das die Fehlerhaftigkeit des Produkts und damit die Haftung begründen.

DEEP DIVE Vertiefung: Der „AI Omnibus“ – von der Ankündigung zur beschlossenen Fristverschiebung

Bereits kurz nach Geltungsbeginn kündigte die Kommission Anpassungen an. Am **19. November 2025** legte sie den **Digital Omnibus on AI** vor: vereinfachte Dokumentationspflichten (auch für Mid-Caps), eine klarere Rechtsgrundlage für die Verarbeitung besonderer Datenkategorien zur **Bias-Erkennung**, eine Stärkung des KI-Büros und vor allem eine Verschiebung einzelner Umsetzungsfristen.

Die Trilog-Verhandlungen waren zäh: Ein erster Anlauf am 28. April 2026 scheiterte an der Konformitätsbewertung für Anhang-I-Systeme. Am **7. Mai 2026** einigten sich Rat und Parlament vorläufig, der Rat bestätigte am 13. Mai, das Parlament stimmte am **16. Juni 2026** mit 423 zu 57 Stimmen (bei 174 Enthaltungen) zu, und der Rat gab am **29. Juni 2026** sein endgültiges Placet. Offen sind bei Redaktionsschluss dieses Kapitels nur noch

Unterzeichnung und Veröffentlichung im Amtsblatt, die vor dem 2. August 2026 erwartet wird; **erst damit werden die neuen Fristen rechtsverbindlich.**

Kern der Einigung sind die im vorigen Abschnitt dargestellten **Fristverschiebungen** für Anhang-III- (2. Dezember 2027) und Anhang-I-Systeme (2. August 2028) sowie für die Reallabore (2. August 2027). Hinzu kommen ein neues **Verbot von KI-„Nudifiern“ und KI-generiertem Missbrauchsmaterial** (Art. 5, Übergangsfrist bis 2. Dezember 2026), eine viermonatige Übergangsfrist für die **Kennzeichnungspflicht** des Art. 50 Abs. 2 bei Bestandssystemen, eine Ausdehnung der Rechtsgrundlage zur **Bias-Erkennung** auf alle KI-Systeme und GPAI-Modelle, eine Begrenzung doppelter Prüfpflichten für in Sektorrecht eingebettete Anhang-I-Systeme sowie die bereits erwähnte Abschwächung der KI-Kompetenz-Pflicht. Die **GPAI-Regeln** (Art. 51 ff.) und die übrigen Verbote des Art. 5 bleiben unangetastet. Der Vorgang zeigt exemplarisch: Die KI-VO ist kein abgeschlossenes Werk, sondern wird schon in ihrer Umsetzungsphase nachjustiert, hier durch eine Verlängerung der Vorlaufzeit, nicht durch eine Absenkung der materiellen Anforderungen.

QUICK-CHECK

Welche Aussage zur Durchsetzung der KI-VO trifft zu?

Die KI-VO enthält einen eigenständigen Schadensersatzanspruch gegen KI-Anbieter.

Verstöße gegen die verbotenen Praktiken können mit bis zu 35 Mio. € oder 7 % des Jahresumsatzes geahndet werden.

Die biometrische Echtzeit-Fernidentifizierung ist ausnahmslos verboten.

GPAI-Modelle unterliegen denselben Pflichten wie Hochrisiko-Systeme.

010

KAPITEL

Von der Ethik zum Recht

Damit schließt sich der Kreis dieses Kurses. In der ersten Einheit haben wir Sicherheit als ethischen **Wert** begründet, die Grenzen maschineller Verantwortung ausgelotet und mit Collingridge, Dignum und der IEEE-7000-Familie gefordert, ethische Anforderungen **von Anfang an** in den Entwicklungsprozess zu holen. Die KI-VO ist die rechtliche Antwort auf genau diese Forderung: Sie übersetzt abstrakte Prinzipien wie Transparenz, menschliche Aufsicht, Rechenschaft und Schutz der Grundrechte in durchsetzbare Pflichten über den gesamten Lebenszyklus eines Systems. Zwischen dem ethischen Anspruch der ersten und dem rechtlichen Rahmen dieser letzten Einheit liegt der eigentliche Gegenstand von Governance, Risk, Compliance & Ethics: aus Werten verbindliche, prüfbare und gelebte Praxis zu machen.

011

KAPITEL

Quellen

11.1 Literatur

- Novelli, C., Hacker, P., Morley, J., Trondal, J. & Floridi, L. (2024): A Robust Governance for the AI Act: AI Office, AI Board, Scientific Panel, and National Authorities. *European Journal of Risk Regulation* 16 (2), S. 566–590. <https://doi.org/10.1017/err.2024.57>

11.2 Normen & Standards

- Verordnung (EU) 2024/1689 des Europäischen Parlaments und des Rates vom 13. Juni 2024 zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz (KI-Verordnung). https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=OJ:L_202401689
- Richtlinie (EU) 2024/2853 des Europäischen Parlaments und des Rates vom 23. Oktober 2024 über die Haftung für fehlerhafte Produkte (Produkthaftungsrichtlinie). https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=OJ:L_202402853
- Vorschlag für eine Richtlinie über die Anpassung der Vorschriften über außervertragliche zivilrechtliche Haftung an künstliche Intelligenz (KI-Haftungsrichtlinie, AILD), COM(2022) 496 final, Anfang 2025 zurückgezogen.
- Vorschlag für eine Verordnung zur Änderung der KI-Verordnung im Hinblick auf bestimmte in Anhang III und IV festgelegte Anwendungsfristen für Anforderungen an Hochrisiko-KI-Systeme sowie zur Änderung weiterer Rechtsakte („Digital Omnibus on AI“), COM(2025) 897, vorgelegt am 19. November 2025; vorläufige Trilog-Einigung vom 7. Mai 2026, gebilligt durch das Europäische Parlament am 16. Juni 2026 und den Rat am 29. Juni 2026 (Veröffentlichung im Amtsblatt bei Redaktionsschluss ausstehend).
- Leitlinien des KI-Büros zum Begriff des KI-Systems (6. Februar 2025) sowie zu den verbotenen Praktiken (4. Februar 2025).