

EU-KI-Gesetz: Risikobasierter Regulierungsrahmen

Ein Leitfaden zu KI-Beschränkungen, Anforderungen und Verantwortlichkeiten

Welche Beschränkungen, Anforderungen und Verantwortlichkeiten sollten Sie verstehen, um KI-Tools in Ihren Geschäftsabläufen zu entwickeln, einzusetzen und zu nutzen?

Überblick: Das EU-KI-Gesetz

Als Mitarbeiter, der mit KI arbeitet, ist das **EU-KI-Gesetz** [tn500] (Verordnung (EU) 2024/1689) [1] der Rechtsrahmen, den Sie verstehen müssen. Es ist die weltweit erste umfassende Verordnung für **künstliche Intelligenz** [tn501] und **regelt** [te009] jedes KI-System, das Ihre Organisation entwickelt, einsetzt oder nutzt — durch einen risikobasierten Ansatz, der KI in Stufen basierend auf ihren potenziellen Auswirkungen auf Grundrechte und Sicherheit kategorisiert. Auf der höchsten Stufe sind bestimmte KI-Praktiken **höher eingestuft als** [te001] alle anderen und vollständig **verboten** [tn100] (Art. 5) — das Gesetz **verbietet** [te007] acht Kategorien inakzeptabler Praktiken, die verboten sind, mit engen Ausnahmen für die Strafverfolgung. Als **Hochrisiko** [tn200] eingestufte Systeme Ihrer Organisation (Art. 6, Anhang III) **müssen einhalten** [te002] strenge **Compliance-Anforderungen** [tn300] (Art. 8–15), bevor sie in Verkehr gebracht werden. Jeder Hochrisikobereich **fällt unter** [te005] spezifische Pflichten, die eine Konformitätsbewertung **erfordern** [te006]. Die Verordnung wird **durchgesetzt ab** [te003] einem **stufenweisen Durchsetzungszeitplan** [tn400] — die frühesten Verbote und KI-Kompetenzpflichten gelten bereits seit Februar 2025, **gefolgt von** [te008] weiteren Phasen, mit

vollständiger Durchsetzung bis August 2027. Das Gesetz **gilt für** [te004] **Anbieter** [tn502] (Organisationen, die KI entwickeln), **Betreiber** [tn503] (Organisationen, die KI einsetzen) sowie jede Stelle, deren KI-System-Ergebnisse Personen in der EU betreffen. Das Verständnis Ihrer Rolle in diesem Rahmen **ermöglicht** [te010] es Ihnen, KI verantwortungsvoll und konform in allen Mitgliedstaaten einzusetzen.

Verbotene Praktiken [tn100]: Art. 5 — Unannehmbares Risiko

Artikel 5 des KI-Gesetzes identifiziert KI-Praktiken mit einer **Risikostufe über** [te101] allen anderen Kategorien, die ein unannehmbares Risiko für die Grundrechte darstellen. Diese Praktiken sind vollständig verboten, mit engen Ausnahmen für die Strafverfolgung unter strengen richterlichen Sicherheitsvorkehrungen [1].

- **Unterschwellige Beeinflussung** [tn101]: KI-Systeme, die unterschwellige Techniken jenseits des Bewusstseins einer Person oder absichtlich manipulative oder täuschende Techniken einsetzen, mit dem Ziel oder der Wirkung, das Verhalten wesentlich zu verzerren und dadurch erheblichen Schaden zu verursachen oder vernunftgemäß wahrscheinlich zu verursachen
- **Ausnutzung von Schutzbedürftigkeit** [tn102]: KI-Systeme, die Schutzbedürftigkeiten aufgrund von Alter, Behinderung oder einer bestimmten sozialen oder wirtschaftlichen Situation ausnutzen, um Verhalten wesentlich zu verzerren und erheblichen Schaden zu verursachen
- **Sozialbewertung** [tn103]: KI-Systeme, die zur Bewertung oder Klassifizierung natürlicher Personen oder Gruppen auf der Grundlage ihres Sozialverhaltens oder bekannter, abgeleiteter oder vorhergesagter persönlicher Merkmale über einen bestimmten Zeitraum eingesetzt werden, wenn die resultierende Sozialbewertung zu nachteiliger oder ungünstiger Behandlung in sozialen Kontexten führt, die keinen Bezug zu den Kontexten haben, in denen die Daten ursprünglich erhoben

wurden, oder zu einer Behandlung, die in keinem Verhältnis zur Schwere des Sozialverhaltens steht

- **Prädiktive Polizeiarbeit** [tn104]: KI-Systeme, die Risikobewertungen einzelner natürlicher Personen vornehmen, um Straftaten ausschließlich auf der Grundlage von Profiling oder Persönlichkeitsmerkmalen vorherzusagen, es sei denn, sie unterstützen menschliche Bewertungen auf der Grundlage objektiver, überprüfbarer Fakten mit direktem Bezug zu kriminellen Aktivitäten
- **Ungezieltes Gesichtsdaten-Scraping** [tn105]: KI-Systeme, die Gesichtserkennungsdatenbanken durch ungezieltes Scraping von Gesichtsbildern aus dem Internet oder von Überwachungskameras aufbauen oder erweitern
- **Emotionserkennung am Arbeitsplatz und in der Bildung** [tn106]: KI-Systeme, die Emotionen natürlicher Personen am Arbeitsplatz und in Bildungseinrichtungen ableiten, außer wenn sie für medizinische oder sicherheitsrelevante Zwecke bestimmt sind
- **Biometrische Kategorisierung** [tn107]: KI-Systeme, die natürliche Personen einzeln auf der Grundlage biometrischer Daten kategorisieren, um Rasse, politische Meinungen, Gewerkschaftszugehörigkeit, religiöse oder philosophische Überzeugungen, Sexualleben oder sexuelle Orientierung abzuleiten, außer bei rechtmäßiger Kennzeichnung oder Filterung biometrischer Datensätze oder Kategorisierung durch Strafverfolgungsbehörden
- **Biometrische Echtzeit-Fernidentifizierung** [tn108]: Einsatz biometrischer Echtzeit-Fernidentifizierungssysteme in öffentlich zugänglichen Räumen für Strafverfolgungszwecke, außer unter engen Ausnahmen wie der gezielten Suche nach vermissten Personen, der Verhinderung unmittelbarer terroristischer Bedrohungen oder der Lokalisierung von Verdächtigen schwerer Straftaten, jeweils vorbehaltlich vorheriger richterlicher Genehmigung

Hochrisiko-Klassifizierung [tn200]: Art. 6 und Anhang-III-Bereiche

Artikel 6 stuft KI-Systeme über zwei Wege als Hochrisiko ein ^[1]. Erstens sind KI-Systeme, die Sicherheitskomponenten von Produkten sind, die unter die in Anhang I aufgeführte EU-Harmonisierungsgesetzgebung fallen (wie Medizinprodukte, Maschinen, Spielzeug, Aufzüge und Fahrzeuge), Hochrisiko, wenn das Produkt eine Konformitätsbewertung durch Dritte erfordert (Art. 6(1)). Zweitens sind eigenständige KI-Systeme, die in den acht unten aufgeführten sensiblen Bereichen des Anhangs III eingesetzt werden, Hochrisiko (Art. 6(2)). In beiden Fällen **müssen** [te102] Systeme, die ein erhebliches Risiko für Gesundheit, Sicherheit oder Grundrechte darstellen, die vollständigen **Compliance-Anforderungen** [tn300] vor dem **Inverkehrbringen** [tn504] oder der Inbetriebnahme einhalten.

- **Biometrie** [tn201]: Biometrische Fernidentifizierung (nicht in Echtzeit), Emotionserkennungssysteme und biometrische Kategorisierung natürlicher Personen
- **Kritische Infrastruktur** [tn202]: KI als Sicherheitskomponenten bei der Verwaltung und dem Betrieb von Straßen-, Wasserversorgungs-, Gas-, Heizungs- und Strominfrastruktur
- **Bildung und Berufsausbildung** [tn203]: KI-Systeme zur Bestimmung des Zugangs zu oder der Zulassung zu Bildungseinrichtungen, zur Bewertung von Lernergebnissen, zur Überwachung von Prüfungen und zur Bewertung des angemessenen Bildungsniveaus für Einzelpersonen
- **Beschäftigung und Arbeitskräfteverwaltung** [tn204]: KI-Systeme in der Personalbeschaffung, Kandidatenauswahl, beschäftigungsbezogenen Entscheidungen, Aufgabenverteilung, Leistungs- und Verhaltensüberwachung von Arbeitnehmern
- **Wesentliche private und öffentliche Dienste** [tn205]: KI-Systeme zur Bewertung der Kreditwürdigkeit, Kreditscoring, Risikobewertung für Lebens- und Krankenversicherungspreise und Priorisierung der Einsatzleitung von Rettungsdiensten
- **Strafverfolgung** [tn206]: KI-Systeme für individuelle Risikobewertungen natürlicher Personen, polygraphenähnliche Instrumente und

Lügenerkennung, Bewertung der Zuverlässigkeit von Beweismitteln und Kriminalitätsanalyse einschließlich Profiling zur Vorhersage und Erkennung

- **Migration, Asyl und Grenzkontrolle** [tn207]: KI-Systeme zur Lügenerkennung in Asyl- und Visaverfahren, Risikobewertung von Bedrohungen durch irreguläre Migration und Überprüfung und Sicherheitsrisikobewertung natürlicher Personen
- **Rechtspflege und Demokratie** [tn208]: KI-Systeme zur Unterstützung von Justizbehörden bei der Erforschung und Auslegung von Tatsachen und Recht sowie bei der Rechtsanwendung, ebenso wie Systeme zur Beeinflussung des Ergebnisses von Wahlen oder Volksabstimmungen oder des Wahlverhaltens natürlicher Personen
- **Hochrisiko-Ausnahme** [tn209] (**Art. 6(3)**): Ein in Anhang III aufgeführtes KI-System wird NICHT als Hochrisiko angesehen, wenn es kein erhebliches Risiko für Gesundheit, Sicherheit oder Grundrechte darstellt, sofern es mindestens eine Bedingung erfüllt: (a) es führt eine eng begrenzte Verfahrensaufgabe aus, (b) es verbessert das Ergebnis einer zuvor abgeschlossenen menschlichen Tätigkeit, (c) es erkennt Entscheidungsmuster, ohne die menschliche Bewertung zu ersetzen, oder (d) es führt eine vorbereitende Aufgabe für eine Anhang-III-Bewertung durch. Ein Anhang-III-System, das ein Profiling natürlicher Personen durchführt, gilt jedoch stets als Hochrisiko ungeachtet dieser Bedingungen. Anbieter, die sich auf diese Ausnahme berufen, müssen ihre Bewertung dokumentieren und sich in der EU-Datenbank registrieren (Art. 49)

Compliance-Anforderungen [tn300] für Hochrisiko-KI-Systeme: Art. 8–15

Anbieter [tn502] von **Hochrisiko** [tn200]-KI-Systemen müssen acht zentrale Anforderungen vor dem **Inverkehrbringen** [tn504] erfüllen, die den gesamten

Lebenszyklus von der Konzeption über die Bereitstellung bis zur Marktüberwachung abdecken [1].

- **Risikomanagementsystem** [tn301] (**Art. 9**): Ein kontinuierlicher, iterativer Prozess, der während des gesamten Lebenszyklus des Hochrisiko-KI-Systems geplant und aufrechterhalten wird, mit systematischer Identifizierung, Analyse, Schätzung und Bewertung von Risiken sowie Ergreifung geeigneter und gezielter Risikomanagementmaßnahmen. Das Risikomanagementsystem **informiert** [te301] die nachfolgenden Daten-Governance-Praktiken
- **Daten und Daten-Governance** [tn302] (**Art. 10**): Trainings-, Validierungs- und Testdatensätze müssen Qualitätskriterien erfüllen, einschließlich Relevanz, Repräsentativität, Vollständigkeit und statistischer Eigenschaften, die dem Verwendungszweck angemessen sind, mit Governance-Praktiken für Datenerhebung, -aufbereitung und Bias-Prüfung. Diese Praktiken werden in der technischen Dokumentation **dokumentiert in** [te302]
- **Technische Dokumentation** [tn303] (**Art. 11**): Umfassende technische Dokumentation, die vor dem Inverkehrbringen oder der Inbetriebnahme des Systems erstellt, auf dem neuesten Stand gehalten und den nationalen zuständigen Behörden auf Anfrage zur Verfügung gestellt wird, um die Konformität nachzuweisen
- **Protokollierung** [tn304] (**Art. 12**): Hochrisiko-KI-Systeme müssen so konzipiert sein, dass sie die automatische Aufzeichnung von Ereignissen («Logs») über ihre Lebensdauer ermöglichen, um die Rückverfolgbarkeit der Funktionsweise des Systems zu gewährleisten und die Marktüberwachung zu erleichtern
- **Transparenz und Informationsbereitstellung** [tn305] (**Art. 13**): Hochrisiko-KI-Systeme müssen so konzipiert sein, dass sie mit ausreichender Transparenz arbeiten, damit Betreiber die Ausgabe des Systems interpretieren und angemessen nutzen können, begleitet von klaren und angemessenen Gebrauchsanweisungen. Transparenz **ermöglicht** [te303] eine wirksame menschliche Aufsicht
- **Menschliche Aufsicht** [tn306] (**Art. 14**): Hochrisiko-KI-Systeme müssen mit geeigneten Mensch-Maschine-Schnittstellenwerkzeugen

ausgestattet sein, damit sie während der Nutzung wirksam von natürlichen Personen überwacht werden können, einschließlich der Fähigkeit, Leistungsfähigkeit und Grenzen zu verstehen, den Betrieb zu überwachen und in das System einzugreifen oder es zu unterbrechen

- **Genauigkeit, Robustheit und Cybersicherheit** ^[tn307] (**Art. 15**): Hochrisiko-KI-Systeme müssen während ihres gesamten Lebenszyklus ein angemessenes Maß an Genauigkeit, Robustheit und Cybersicherheit erreichen, mit Widerstandsfähigkeit gegenüber Fehlern, Störungen, Inkonsistenzen und adversarialen Angriffen einschließlich Datenvergiftung und Modellmanipulation. Diese Eigenschaften werden **validiert durch** ^[te304] die Gesamtkonformitätsbewertung
- **Gesamtkonformität** ^[tn308] (**Art. 8**): Hochrisiko-KI-Systeme müssen alle in den Artikeln 9–15 festgelegten Anforderungen erfüllen, unter Berücksichtigung des allgemein anerkannten Stands der Technik, des Verwendungszwecks des Systems und relevanter harmonisierter Normen oder gemeinsamer Spezifikationen, gefolgt von einem Konformitätsbewertungsverfahren vor dem Inverkehrbringen

Pflichten bei begrenztem Risiko ^[tn550]: Art. 50 — Transparenzanforderungen

Artikel 50 legt Transparenzpflichten für KI-Systeme fest, die direkt mit natürlichen Personen interagieren oder synthetische Inhalte erzeugen. Diese **gelten für** ^[te550] bestimmte Kategorien von KI-Systemen — unabhängig von ihrer Risikoeinstufung — die Risiken der Täuschung oder Manipulation bergen. Als Mitarbeiter ist das Verständnis dieser Pflichten entscheidend beim Einsatz von Chatbots, Inhaltsgenerierungstools oder biometrischen Systemen in kundenorientierten oder internen Abläufen ^[1].

- **Offenlegung menschlicher Interaktion** ^[tn551]: Anbieter müssen sicherstellen, dass KI-Systeme, die für die direkte Interaktion mit natürlichen Personen bestimmt sind (wie Chatbots), so gestaltet sind,

dass die betroffenen Personen darüber informiert werden, dass sie mit einem KI-System interagieren, es sei denn, dies ist aus den Umständen und dem Nutzungskontext offensichtlich. Dies **erfordert Offenlegung durch** [te551] den Anbieter beim ersten Kontakt

- **Kennzeichnung synthetischer Inhalte** [tn552]: Anbieter von KI-Systemen, die synthetische Audio-, Bild-, Video- oder Textinhalte erzeugen, müssen sicherstellen, dass die Ausgaben in einem maschinenlesbaren Format gekennzeichnet und als künstlich erzeugt oder manipuliert erkennbar sind. Dies schließt KI-Systeme mit allgemeinem Verwendungszweck ein. Die technischen Lösungen müssen wirksam, interoperabel, robust und zuverlässig sein. Diese Pflicht gilt nicht für KI-Systeme, die eine unterstützende Funktion für die Standardbearbeitung ausüben oder die die vom Betreiber bereitgestellten Eingabedaten nicht wesentlich verändern
- **Offenlegung von Emotionserkennung und Biometrie** [tn553]: Betreiber von Emotionserkennungssystemen oder biometrischen Kategorisierungssystemen müssen die betroffenen natürlichen Personen über den Betrieb des Systems informieren und personenbezogene Daten gemäß der DSGVO und verwandten Datenschutzvorschriften verarbeiten. Diese Pflicht gilt nicht für KI-Systeme, die für die Strafverfolgung eingesetzt werden
- **Deep-Fake-Offenlegung** [tn554]: Betreiber von KI-Systemen, die Bild-, Audio- oder Videoinhalte erzeugen oder manipulieren, die einen Deep Fake darstellen, müssen offenlegen, dass der Inhalt künstlich erzeugt oder manipuliert wurde. Dies **erstreckt sich auf** [te552] Texte, die zu Angelegenheiten von öffentlichem Interesse veröffentlicht werden und ebenfalls als KI-generiert gekennzeichnet werden müssen, es sei denn, der Inhalt wurde redaktionell überprüft

KI-Modelle mit allgemeinem Verwendungszweck [tn600]: Art. 51–56 —

GPAI-Modellpflichten

Kapitel V führt ein eigenes Regulierungsregime für KI-Modelle mit allgemeinem Verwendungszweck (GPAI) ein — großangelegte Modelle, die auf breiten Daten trainiert werden und verschiedene nachgelagerte Aufgaben bedienen können, wie große Sprachmodelle. Diese Regeln **gelten unabhängig von** [te600] der risikobasierten Klassifizierung für KI-Systeme und erkennen an, dass GPAI-Modelle **vielen nachgelagerten KI-Systemen zugrunde liegen** [te601]. Als Mitarbeiter müssen Sie, wenn Ihre Organisation Basismodelle entwickelt, einsetzt oder integriert, sowohl die Grundpflichten als auch die zusätzlichen Anforderungen bei systemischem Risiko verstehen [1].

- **Klassifizierung systemischer Risiken** [tn601] (**Art. 51**): Ein GPAI-Modell wird als systemisches Risiko eingestuft, wenn es hochgradig wirkungsvolle Fähigkeiten besitzt (bewertet durch Benchmarks) oder wenn die Kommission es anhand der Kriterien in Anhang XIII einstuft. Ein Modell wird als hochgradig wirkungsvoll angenommen, wenn die kumulative Rechenleistung für das Training 10^{25} Gleitkommaoperationen übersteigt. Diese Klassifizierung **löst zusätzliche Pflichten gemäß** [te602] Artikel 55 aus
- **Technische Dokumentation** [tn602] (**Art. 53**): Anbieter von GPAI-Modellen müssen technische Dokumentation erstellen und pflegen, einschließlich Trainings- und Testprozesse sowie Bewertungsergebnisse, und diese dem KI-Büro und den nationalen zuständigen Behörden auf Anfrage zur Verfügung stellen
- **Informationen für nachgelagerte Anbieter** [tn603] (**Art. 53**): Anbieter von GPAI-Modellen müssen nachgelagerten Anbietern, die das Modell in KI-Systeme integrieren, Informationen und Dokumentation zur Verfügung stellen, damit diese die Fähigkeiten, Einschränkungen und ihre eigenen Compliance-Pflichten verstehen können. Diese Informationen müssen mindestens die in Anhang XII aufgeführten Elemente enthalten
- **Urheberrechtskonformität** [tn604] (**Art. 53**): Anbieter von GPAI-Modellen müssen eine Richtlinie zur Einhaltung des EU-Urheberrechts einführen, einschließlich der Identifizierung und Einhaltung von Rechtsvorbehalten

gemäß der Urheberrechtsrichtlinie (EU) 2019/790, und eine ausreichend detaillierte Zusammenfassung der Trainingsdateninhalte veröffentlichen

- **Pflichten bei systemischem Risiko** [tn605] (**Art. 55**): Anbieter von GPAI-Modellen mit systemischem Risiko müssen zusätzlich Modellbewertungen einschließlich adversarialer Tests durchführen, systemische Risiken auf Unionsebene bewerten und mindern, schwerwiegende Vorfälle nachverfolgen und dem KI-Büro melden sowie einen angemessenen Cybersicherheitsschutz für das Modell und seine Infrastruktur gewährleisten. Diese Pflichten **gehen über** [te603] die Grundanforderungen von Artikel 53 hinaus
- **Praxisleitfäden** [tn606] (**Art. 56**): Das KI-Büro fördert Praxisleitfäden auf Unionsebene zum Nachweis der Einhaltung der GPAI-Pflichten. Diese Praxisleitfäden umfassen Standards für technische Dokumentation, Zusammenfassungen der Trainingsdaten, Identifizierung systemischer Risiken und Risikobewertungsverfahren. Praxisleitfäden müssen bis zum 2. Mai 2025 fertig sein, und die Einhaltung genehmigter Praxisleitfäden **begründet die Konformitätsvermutung mit** [te604] den Artikeln 53 und 55 bis zur Veröffentlichung harmonisierter Normen
- **Open-Source-Ausnahme** [tn607]: GPAI-Modelle, die unter freien und Open-Source-Lizenzen veröffentlicht werden und deren Parameter, Architektur und Nutzungsinformationen öffentlich zugänglich sind, **sind befreit von** [te906] den Pflichten zur technischen Dokumentation und den nachgelagerten Informationspflichten (Art. 53(1)(a)-(b)). Diese Ausnahme gilt jedoch nicht für GPAI-Modelle mit systemischem Risiko — diese müssen ungeachtet der Lizenzierung alle Pflichten erfüllen

Pflichten nach Rolle [tn700]: Art. 16–27 — Wer muss was tun

Das KI-Gesetz weist jedem Akteur in der KI-Wertschöpfungskette eigene Pflichten zu. Als Mitarbeiter hängen Ihre Verantwortlichkeiten davon ab, ob Ihre Organisation **als** [te700] Anbieter, Betreiber, Einführer oder Händler von Hochrisiko-KI-Systemen

handelt. Das Verständnis Ihrer Rolle bestimmt, welche Compliance-Anforderungen für Ihre tägliche Arbeit gelten ^[1].

- **Anbieterpflichten** ^[tn701] (**Art. 16–21**): Anbieter tragen die schwersten Pflichten: Einhaltung aller Anforderungen (Art. 8–15), Einführung eines Qualitätsmanagementsystems (Art. 17), Aufbewahrung der technischen Dokumentation für 10 Jahre (Art. 18), Führung automatisch erzeugter Protokolle (Art. 19), Ergreifung von Korrekturmaßnahmen bei nicht konformen Systemen (Art. 20), **Zusammenarbeit mit** ^[te701] nationalen zuständigen Behörden (Art. 21), Anbringung der **CE-Kennzeichnung** ^[tn509] (Art. 48), Einrichtung einer **Beobachtung nach dem Inverkehrbringen** ^[tn507] (Art. 72) und Durchführung der Konformitätsbewertung vor dem Inverkehrbringen
- **Betreiberpflichten** ^[tn702] (**Art. 26**): Betreiber müssen KI-Systeme gemäß den Gebrauchsanweisungen nutzen, die menschliche Aufsicht kompetenten Personen zuweisen, sicherstellen, dass Eingabedaten relevant und repräsentativ sind, den Betrieb überwachen und Risiken an Anbieter melden, Protokolle mindestens sechs Monate aufbewahren, jeden **schwerwiegenden Vorfall** ^[tn508] der Marktüberwachungsbehörde melden (Art. 73), Arbeitnehmervertretungen vor dem Einsatz am Arbeitsplatz informieren, betroffene Personen über KI-gestützte Entscheidungsfindung informieren und **eine Grundrechte-Folgenabschätzung durchführen** ^[te702] (Art. 27) beim Einsatz als öffentliche Stelle oder im Bereich wesentlicher Dienste
- **Pflichten der Einführer** ^[tn703] (**Art. 23**): Einführer müssen überprüfen, dass der Anbieter die Konformitätsbewertung durchgeführt hat, die technische Dokumentation existiert, die CE-Kennzeichnung angebracht ist und ein Bevollmächtigter benannt wurde. Einführer dürfen nicht konforme Systeme nicht in Verkehr bringen, müssen Dokumentation 10 Jahre aufbewahren und mit den zuständigen Behörden zusammenarbeiten
- **Händlerpflichten** ^[tn704] (**Art. 24**): Händler müssen CE-Kennzeichnung, EU-Konformitätserklärung und Gebrauchsanweisungen überprüfen, bevor sie ein System bereitstellen. Sie dürfen nicht konforme Systeme

nicht bereitstellen und müssen den Anbieter oder Einführer über festgestellte Nichtkonformitäten oder Risiken informieren

- **Verantwortlichkeiten in der Wertschöpfungskette [tn705] (Art. 25):**
Jeder Händler, Einführer, Betreiber oder Dritte **wird zum Anbieter [te703]** (und übernimmt alle Anbieterpflichten), wenn er: seinen Namen oder seine Marke auf ein Hochrisiko-KI-System setzt, eine wesentliche Änderung vornimmt oder den Verwendungszweck so ändert, dass es als Hochrisiko eingestuft wird. Dies verhindert Compliance-Lücken durch Umkennzeichnung oder Modifikation
- **Grundrechte-Folgenabschätzung [tn706] (Art. 27):** Öffentliche Betreiber und private Einrichtungen, die wesentliche Dienste erbringen, müssen vor dem Einsatz von Hochrisiko-KI-Systemen eine Folgenabschätzung für die Grundrechte durchführen. Die Bewertung umfasst: Beschreibung der Prozesse, Zeitraum und Häufigkeit der Nutzung, Kategorien betroffener Personen, spezifische Schadensrisiken, Maßnahmen zur menschlichen Aufsicht und **Governance-Mechanismen für [te704]** die Beschwerdebehandlung. Die Ergebnisse müssen der Marktüberwachungsbehörde mitgeteilt werden
- **Bevollmächtigter [tn707] (Art. 22):** In Drittländern (außerhalb der EU) ansässige Anbieter von Hochrisiko-KI-Systemen müssen vor der Bereitstellung ihrer Systeme auf dem EU-Markt durch schriftliches Mandat einen in der Union ansässigen Bevollmächtigten bestellen. Der Bevollmächtigte überprüft, dass die EU-Konformitätserklärung und die technische Dokumentation erstellt wurden, bewahrt Kopien 10 Jahre lang für die Behörden auf und arbeitet mit dem KI-Büro und den zuständigen Behörden im Auftrag des Anbieters zusammen

Querschnittsbestimmungen [tn800]: Pflichten und freiwillige Maßnahmen für alle KI

Bestimmte Pflichten **gelten für alle Risikostufen** [te800], unabhängig davon, ob ein KI-System als verboten, hochriskant, mit begrenztem Risiko oder mit minimalem Risiko eingestuft wird. Diese Querschnittsbestimmungen — teils verpflichtend, teils freiwillig — bilden den breiteren Kontext, den jeder mit KI arbeitende Mitarbeiter verstehen muss [1]. Beachten Sie, dass die überwiegende Mehrheit der im täglichen Geschäftsbetrieb eingesetzten KI-Systeme (wie Spam-Filter, Bestandsoptimierung oder Empfehlungssysteme) in die Kategorie minimales Risiko fällt und keinen verpflichtenden Auflagen unterliegt, die über die KI-Kompetenz hinausgehen — sie können freiwillig Verhaltenskodizes übernehmen (Art. 95).

- **KI-Kompetenz** [tn801] (**Art. 4**): Anbieter und Betreiber müssen im bestmöglichen Umfang ein ausreichendes Maß an KI-Kompetenz ihres Personals und anderer Personen sicherstellen, die in ihrem Auftrag mit dem Betrieb und der Nutzung von KI-Systemen befasst sind. Diese Pflicht **berücksichtigt** [te801] die technischen Kenntnisse, die Erfahrung, die Ausbildung und die Schulung der betreffenden Personen sowie den Kontext, in dem die KI-Systeme eingesetzt werden sollen. KI-Kompetenz gilt ab dem 2. Februar 2025 — sie gehört zu den frühesten Pflichten, die in Kraft treten
- **DSGVO und Datenschutz** [tn802]: Das KI-Gesetz gilt unbeschadet der DSGVO (Verordnung 2016/679), der LED (Richtlinie 2016/680) und der ePrivacy-Richtlinie (2002/58/EG). Jedes KI-System, das personenbezogene Daten verarbeitet, muss neben den Anforderungen des KI-Gesetzes auch die bestehenden Datenschutzgesetze einhalten. Datenschutz-Folgenabschätzungen gemäß Art. 35 DSGVO ergänzen die Grundrechte-Folgenabschätzungen gemäß Art. 27 des KI-Gesetzes
- **Nichtdiskriminierung** [tn803]: KI-Systeme müssen in Übereinstimmung mit dem EU-Antidiskriminierungsrecht entwickelt und eingesetzt werden. Verzerrungen in Trainingsdaten, Modelldesign oder Einsatz können zu diskriminierenden Ergebnissen gegen geschützte Gruppen aufgrund von Rasse, Geschlecht, Behinderung, Alter oder anderen Merkmalen führen. Anbieter von Hochrisiko-Systemen müssen Datensätze gezielt auf mögliche Verzerrungen untersuchen (Art. 10(2)(f)) und Maßnahmen zu deren Erkennung, Prävention und Minderung ergreifen
- **Freiwillige Verhaltenskodizes** [tn804]: Anbieter von nicht-hochriskanten KI-Systemen werden ermutigt, **freiwillig die** [te802] verpflichtenden

Anforderungen für Hochrisiko-Systeme anzuwenden, einschließlich der Erstellung von Verhaltenskodizes zu KI-Kompetenz, Umweltverträglichkeit, inklusivem Design, Diversität in Entwicklungsteams und Barrierefreiheit. Diese freiwilligen Verpflichtungen sollten auf klaren Zielen und messbaren Indikatoren basieren

- **Recht auf Erklärung** [tn805]: Betroffene Personen haben das Recht, eine Erklärung zu erhalten, wenn eine Entscheidung eines Betreibers hauptsächlich auf der Ausgabe bestimmter Hochrisiko-KI-Systeme beruht und diese Entscheidung rechtliche Wirkungen entfaltet oder sie in ähnlich erheblicher Weise betrifft. Die Erklärung muss klar und aussagekräftig sein und **den betroffenen Personen ermöglichen** [te803], ihre Rechte auszuüben. Jede Person kann eine **Beschwerde** [tn807] bei einer Marktüberwachungsbehörde einreichen (Art. 85). Personen, die Verstöße melden, sind durch den **Hinweisgeberschutz** [tn806] (Richtlinie 2019/1937) geschützt. Diese Rechte gelten zusätzlich zu bestehenden Rechten gemäß Art. 22 DSGVO

Governance und Durchsetzung [tn900]: Institutioneller Rahmen und Sanktionen

Das KI-Gesetz schafft einen mehrstufigen Governance-Rahmen auf EU- und nationaler Ebene, mit dem **Büro für Künstliche Intelligenz** [tn901] im Zentrum. Die Durchsetzung erfolgt durch Marktüberwachungsbehörden in jedem Mitgliedstaat, mit gestaffelten Verwaltungsgeldbußen bei Nichtkonformität. Als Mitarbeiter hilft Ihnen das Verständnis der Governance-Struktur zu wissen, wer **die KI-Aktivitäten Ihrer Organisation überwacht** [te900] und welche Sanktionen gelten [1].

- **Büro für Künstliche Intelligenz** [tn901] (**Art. 64**): Das KI-Büro, eingerichtet bei der Europäischen Kommission, entwickelt Fachkompetenz und Kapazitäten der Union im Bereich KI. Es verfügt über die Befugnisse einer Marktüberwachungsbehörde für die Aufsicht

über GPAI-Modelle, kann Verstöße untersuchen, Dokumentation anfordern, Bewertungen durchführen und **die Compliance-Einhaltung durchsetzen für** [te901] Anbieter von KI-Modellen mit allgemeinem Verwendungszweck auf Unionsebene

- **Europäisches KI-Gremium** [tn902] (**Art. 65–66**): Das Europäische KI-Gremium, bestehend aus einem Vertreter je Mitgliedstaat, berät die Kommission und die Mitgliedstaaten zur einheitlichen und wirksamen Anwendung der Verordnung. Das KI-Gremium koordiniert zwischen nationalen Behörden, sammelt Fachexpertise, gibt Leitlinien zur GPAI-Durchsetzung und **unterstützt die Harmonisierung der** [te902] Verwaltungspraktiken in der gesamten Union. Er wird durch ein **Beratungsforum** [tn909] (Art. 67) aus Vertretern von Industrie, Zivilgesellschaft, Wissenschaft und KMU unterstützt
- **Nationale zuständige Behörden** [tn903] (**Art. 70**): Jeder Mitgliedstaat muss mindestens eine notifizierende Behörde und eine Marktüberwachungsbehörde benennen. Diese Behörden üben ihre Befugnisse unabhängig und unparteiisch aus, mit angemessener KI-Expertise, Datenschutzkenntnissen und Cybersicherheitskompetenz. Marktüberwachungsbehörden **führen die Durchsetzung auf** [te903] nationaler Ebene durch, einschließlich Inspektionen, Dokumentenanforderungen und Korrekturmaßnahmen. Alle Hochrisiko-KI-Systeme müssen in der **EU-Datenbank** [tn908] (Art. 71) registriert werden, bevor sie in Verkehr gebracht werden
- **Sanktionsstufe 1: Verbotene Praktiken** [tn904] (**Art. 99(3)**): Verstöße gegen das Verbot der in Artikel 5 genannten KI-Praktiken **bestraft Verstöße gegen** [te907] verbotene Praktiken, mit Geldbußen von bis zu 35 000 000 EUR oder bei Unternehmen bis zu 7 % des gesamten weltweiten Jahresumsatzes des vorangegangenen Geschäftsjahres, je nachdem, welcher Betrag höher ist. Für KMU und Start-ups ist die Geldbuße auf den niedrigeren der beiden Beträge begrenzt
- **Sanktionsstufe 2: Betreiberpflichten** [tn905] (**Art. 99(4)**): Verstöße gegen Betreiberpflichten (Anbieter Art. 16, Betreiber Art. 26, Einführer Art. 23, Händler Art. 24), Anforderungen an notifizierte Stellen oder Transparenzpflichten (Art. 50) werden mit Geldbußen von bis zu 15 000 000 EUR oder 3 % des gesamten weltweiten Jahresumsatzes belegt, je

nachdem, welcher Betrag höher ist. Diese Stufe **deckt die Mehrzahl der [te904]** alltäglichen Compliance-Verstöße ab

- **Sanktionsstufe 3: Falschinformationen [tn906] (Art. 99(5)):** Die Bereitstellung unrichtiger, unvollständiger oder irreführender Informationen an notifizierte Stellen oder nationale zuständige Behörden wird mit Geldbußen von bis zu 7 500 000 EUR oder 1 % des gesamten weltweiten Jahresumsatzes belegt, je nachdem, welcher Betrag höher ist. Dies gilt für Anfragen im Rahmen von Konformitätsbewertungen, Marktüberwachungsuntersuchungen oder jeder behördlichen Anfrage
- **GPAI-Modell-Geldbußen [tn907] (Art. 101):** Die Kommission kann Anbietern von GPAI-Modellen Geldbußen von bis zu 3 % des weltweiten Jahresumsatzes oder 15 000 000 EUR auferlegen, je nachdem, welcher Betrag höher ist, bei Verstoß gegen GPAI-Pflichten, Nichtbefolgung von Auskunftersuchen oder Verweigerung des Zugangs zum Modell für Bewertungen. Der Gerichtshof der EU hat **unbeschränkte Zuständigkeit zur Überprüfung der [te905]** Bußgeldentscheidungen der Kommission

Durchsetzungszeitplan [tn400]: Stufenweise Anwendung des KI-Gesetzes

Das KI-Gesetz trat am 1. August 2024 **in Kraft ab [te103]** diesem Datum und wird stufenweise über einen Zeitraum von drei Jahren angewandt ^[1]. Jede Phase bringt zusätzliche Bestimmungen in Kraft und gibt betroffenen Organisationen Zeit zur Erreichung der Konformität.

- **2. Februar 2025 [tn401]:** Verbote inakzeptabler KI-Praktiken (Kapitel II, Art. 5) treten in Kraft. KI-Kompetenzpflichten (Art. 4) verlangen von Anbietern und Betreibern die Sicherstellung ausreichender KI-Kompetenz bei ihrem Personal. Diese Phase wird **gefolgt von [te401]** den GPAI-Regeln im August 2025

- **2. Mai 2025** [tn910]: Frist für GPAI-Praxisleitfäden (Art. 56). Das Büro für Künstliche Intelligenz muss endgültige Praxisleitfäden veröffentlichen, auf die sich GPAI-Modellanbieter zum Nachweis der Einhaltung ihrer Pflichten stützen können. Dies wird **gefolgt von** [te908] den GPAI-Modellpflichten im August 2025
- **2. August 2025** [tn402]: Regeln für KI-Modelle mit allgemeinem Verwendungszweck (GPAI) gelten, einschließlich Transparenzpflichten und Bestimmungen für systemische Risiken. Die Governance-Struktur und der Sanktionsrahmen (einschließlich Geldbußen bis zu 35 Millionen EUR oder 7 % des weltweiten Umsatzes) werden anwendbar. Dies wird **gefolgt von** [te402] den Hochrisiko-Pflichten im August 2026
- **2. August 2026** [tn403]: Der Großteil der Verordnung tritt in Kraft, mit **vollen Pflichten ab** [te104] diesem Datum für Hochrisiko-KI-Systeme (Art. 6–27, Art. 40–49), einschließlich Risikomanagement, Daten-Governance, Transparenz, menschliche Aufsicht und Konformitätsbewertungsverfahren für Anbieter und Betreiber. Jeder Mitgliedstaat muss bis zu diesem Datum auch einen **KI-Reallabor** [tn506] (Art. 57) betriebsbereit haben. Wichtig: KI-Systeme, die vor diesem Datum bereits in Verkehr gebracht oder in Betrieb genommen wurden, unterliegen dem Gesetz nur, wenn sie nach dem 2. August 2026 wesentliche Änderungen in ihrer Gestaltung oder ihrem Verwendungszweck erfahren. Dies wird **gefolgt von** [te403] der vollständigen Durchsetzung im August 2027
- **2. August 2027** [tn404]: **Vollständige Durchsetzung ab** [te105] diesem Datum: Pflichten gelten für KI-Systeme, die Bestandteile großangelegter IT-Systeme der EU in den Bereichen Freiheit, Sicherheit und Justiz nach Anhang X sind (einschließlich SIS, VIS, Eurodac, ETIAS, ECRIS-TCN)

Referenzen

1. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). *Official Journal of the European Union*, L series. [\[Source\]](#)

2. Corrigendum to Regulation (EU) 2024/1689 of 13 June 2024 (AI Act). *Official Journal of the European Union*, L 2024/1689. [\[Source\]](#)
3. European Commission. AI Act — Shaping Europe's digital future: regulatory framework for AI. [\[Source\]](#)
4. European AI Office. General-Purpose AI Code of Practice — First Draft. [\[Source\]](#)
5. EUR-Lex. Annex III to Regulation (EU) 2024/1689: High-Risk AI Systems referred to in Article 6(2). [\[Source\]](#)

Häufig gestellte Fragen

F: Was ist das EU-KI-Gesetz?

A: Das **EU-KI-Gesetz** [\[tn500\]](#) (Verordnung (EU) 2024/1689) ist der weltweit erste umfassende Rechtsrahmen speziell für die Regulierung **künstlicher Intelligenz** [\[tn501\]](#). Es legt harmonisierte Regeln für die Entwicklung, das **Inverkehrbringen** [\[tn504\]](#), die Inbetriebnahme und die Nutzung von KI-Systemen in der Europäischen Union fest und verfolgt einen risikobasierten Ansatz, der von **verbotenen Praktiken** [\[tn100\]](#) bis zu Transparenzanforderungen mit minimalem Risiko reicht.

F: Für wen gilt das KI-Gesetz?

A: Das KI-Gesetz gilt für **Anbieter** [\[tn502\]](#) (die KI-Systeme entwickeln oder in Auftrag geben und unter eigenem Namen oder eigener Marke in Verkehr bringen), **Betreiber** [\[tn503\]](#) (die KI-Systeme unter ihrer Verantwortung einsetzen), Einführer, Händler und Produkthersteller. Es erfasst Unternehmen mit Sitz in der EU, aber auch solche außerhalb der EU, wenn die Ergebnisse ihres KI-Systems in der Union verwendet werden.

F: Welche KI-Praktiken sind nach dem Gesetz verboten?

A: Artikel 5 verbietet acht Kategorien von KI-Praktiken, die als unannehmbares Risiko gelten, darunter **unterschwellige Manipulation** [\[tn101\]](#), **Ausnutzung von Schutzbedürftigkeit** [\[tn102\]](#), **Sozialbewertung** [\[tn103\]](#), **prädiktive Polizeiarbeit** [\[tn104\]](#) auf alleiniger Grundlage von Profiling, **ungezieltes Gesichtsdaten-Scraping** [\[tn105\]](#), **Emotionserkennung am Arbeitsplatz und in der Bildung** [\[tn106\]](#), diskriminierende **biometrische Kategorisierung** [\[tn107\]](#) und **biometrische Echtzeit-**

Fernidentifizierung [tn108] in öffentlichen Räumen für die Strafverfolgung (mit engen Ausnahmen).

F: Was sind Hochrisiko-KI-Systeme und welche Anforderungen müssen sie erfüllen?

A: **Hochrisiko** [tn200]-KI-Systeme sind solche, die in sensiblen Bereichen gemäß Anhang III eingesetzt werden, wie **Biometrie** [tn201], **kritische Infrastruktur** [tn202], **Bildung** [tn203] und **Beschäftigung** [tn204]. Sie müssen Anforderungen erfüllen, darunter ein **Risikomanagementsystem** [tn301], **Daten-Governance** [tn302], **technische Dokumentation** [tn303], **Transparenz** [tn305] und **menschliche Aufsicht** [tn306], und müssen vor dem Inverkehrbringen eine **Konformitätsbewertung** [tn505] durchlaufen.

F: Wie stelle ich fest, ob mein KI-System ein Hochrisikosystem ist?

A: Folgen Sie diesem Entscheidungsbaum. Prüfen Sie zunächst, ob Ihr KI-System eine Sicherheitskomponente eines Produkts ist, das unter die in Anhang I aufgeführte EU-Harmonisierungsgesetzgebung fällt (wie Medizinprodukte, Maschinen oder Fahrzeuge) — wenn ja und das Produkt eine Konformitätsbewertung durch Dritte erfordert, ist Ihr System **Hochrisiko** [tn200]. Prüfen Sie zweitens, ob Ihr System in einen der acht Bereiche des Anhangs III fällt. Wenn ja, prüfen Sie, ob die **Hochrisiko-Ausnahme** [tn209] (Art. 6(3)) gilt: Das System ist NICHT Hochrisiko, wenn es eine eng begrenzte Verfahrensaufgabe ausführt, das Ergebnis einer zuvor abgeschlossenen menschlichen Tätigkeit verbessert, Entscheidungsmuster erkennt, ohne menschliches Urteil zu ersetzen, oder eine vorbereitende Bewertungsaufgabe durchführt — es sei denn, es führt ein Profiling natürlicher Personen durch, dann gilt es stets als Hochrisiko. Wenn keine dieser Ausnahmen greift, ist Ihr System Hochrisiko und muss alle **Compliance-Anforderungen** [tn300] der Art. 8–15 erfüllen. Dokumentieren Sie Ihre Klassifizierungsbegründung und registrieren Sie sich in der **EU-Datenbank** [tn908] (Art. 49).

F: Wann tritt das KI-Gesetz in Kraft?

A: Das KI-Gesetz gilt in Phasen: **verbotene Praktiken** [tn100] und KI-Kompetenz ab dem **2. Februar 2025** [tn401]; GPAI-Modellregeln und Governance ab dem **2. August 2025** [tn402]; Pflichten für **Hochrisiko** [tn200]-KI-Systeme ab dem **2. August 2026** [tn403]; und vollständige Durchsetzung für Komponenten großangelegter IT-Systeme ab dem **2. August 2027** [tn404].

F: Welche Strafen drohen bei Nichtkonformität?

A: Die Sanktionen sind nach Schwere des Verstoßes gestaffelt. Die schwerwiegendsten Verstöße (die **verbotene Praktiken** [tn100] betreffen) können zu Geldbußen von bis zu 35 Millionen EUR oder 7 % des gesamten weltweiten Jahresumsatzes führen, je nachdem, welcher Betrag höher ist. Verstöße gegen Pflichten für **Hochrisiko** [tn200]-Systeme werden mit Geldbußen von bis zu 15 Millionen EUR oder 3 % des Umsatzes belegt. Die Angabe unrichtiger Informationen gegenüber Behörden kann zu Geldbußen von bis zu 7,5 Millionen EUR oder 1 % des Umsatzes führen. Für KMU und Start-ups gelten reduzierte Obergrenzen.

F: Was bedeutet das KI-Gesetz für mich als Mitarbeiter?

A: Das KI-Gesetz betrifft Sie je nach Rolle auf verschiedene Weisen. Erstens verlangt **KI-Kompetenz** [tn801] (Art. 4), dass Ihre Organisation sicherstellt, dass Sie die KI-Systeme, mit denen Sie arbeiten, ausreichend verstehen — diese Pflicht gilt ab dem 2. Februar 2025. Zweitens müssen Sie, wenn Sie an der Entwicklung von KI beteiligt sind (**Anbieterpflichten** [tn701]), die Einhaltung von Anforderungen wie Risikomanagement, Daten-Governance und Dokumentation sicherstellen. Wenn Sie KI-Tools einsetzen (**Betreiberpflichten** [tn702]), müssen Sie die Gebrauchsanweisungen befolgen, menschliche Aufsicht zuweisen und betroffene Personen informieren. Selbst die Nutzung eines Chatbots oder KI-Inhaltsgenerators löst **Transparenzpflichten bei begrenztem Risiko** [tn550] aus.

F: Was sind KI-Modelle mit allgemeinem Verwendungszweck und warum sind sie wichtig?

A: **KI-Modelle mit allgemeinem Verwendungszweck** [tn600] (GPAI) sind großangelegte Modelle, die auf breiten Daten trainiert werden und eine Vielzahl von Aufgaben ausführen können — wie große Sprachmodelle und multimodale Basismodelle. Das KI-Gesetz reguliert diese separat, weil sie **vielen nachgelagerten KI-Systemen zugrunde liegen** [te601]. Wenn Ihre Organisation ein GPAI-Modell nutzt oder integriert, sollten Sie die Pflichten des Anbieters in Bezug auf technische Dokumentation, Urheberrechtskonformität und — falls das Modell ein **systemisches Risiko** [tn601] aufweist — zusätzliche Bewertungs- und Cybersicherheitsanforderungen verstehen.

F: Wer setzt das KI-Gesetz durch und an wen sollte ich mich bei Fragen wenden?

A: Die Durchsetzung erfolgt auf zwei Ebenen. Das **Büro für Künstliche Intelligenz** [tn901] (Art. 64) überwacht GPAI-Modellanbieter auf Unionsebene. Auf nationaler Ebene benennt jeder Mitgliedstaat **nationale zuständige Behörden** [tn903] (Art. 70)

— insbesondere Marktüberwachungsbehörden — die Inspektionen durchführen, Beschwerden bearbeiten und Sanktionen verhängen. Das **Europäische KI-Gremium** [tn902] (Art. 65) koordiniert zwischen diesen nationalen Behörden. Innerhalb Ihrer Organisation sollte Ihre Compliance-, Rechts- oder KI-Governance-Abteilung Ihre erste Anlaufstelle sein.