Bette Westenberger Brink

FAQ zur KI-Verordnung

KI-Systeme, KI–Modelle, Pflichten und Praxistipps

Mit der Verordnung (EU) 2024/1689 zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz (sog. „KI-Verordnung“, „KI-VO“ oder „AI-Act“) hat die Europäische Union (EU) erstmals einen umfassenden und unmittelbar geltenden Rechtsrahmen für den Einsatz von KI-Systemen und KI-Modellen geschaffen. Die Verordnung ist im August 2024 in Kraft getreten und verfolgt das Ziel, Innovation zu fördern und zugleich ein hohes Schutzniveau für Grundrechte, Sicherheit und öffentliche Interessen sicherzustellen.

Die Anwendung der Verordnung erfolgt stufenweise. Ein erheblicher Teil der Regelungen ist bereits umgesetzt. Ab dem 2. August 2026 werden die Vorschriften grundsätzlich in vollem Umfang anwendbar sein. Lediglich die Regelungen zu bestimmten Hochrisiko-KI-Systemen gelten erst ab dem 2. August 2027.

Für Unternehmen aller Branchen ergeben sich aus der KI-VO zahlreiche neue regulatorische Anforderungen. Diese betreffen nicht nur Entwickler von KI-Systemen, sondern auch Anbieter, Betreiber, Importeure und Händler sowie Unternehmen, die KI-Systeme in bestehende Produkte, Dienstleistungen oder Geschäftsprozesse integrieren oder deren Zweckbestimmung verändern. Insbesondere die Definition der eigenen Rolle, die Kategorisierung der jeweiligen KI-Systeme und die damit verbundenen Pflichten und Anforderungen an Governance, Dokumentation und Risikomanagement werfen in der Praxis vielfältige Auslegungs- und Umsetzungsfragen auf.

Vor diesem Hintergrund verfolgt dieses Whitepaper das Ziel, zentrale Fragen zur KI-Verordnung praxisnah zu beantworten. Es soll Unternehmen eine erste Orientierung über die wichtigsten Regelungsinhalte und Pflichten geben und dabei helfen, typische Fallstricke frühzeitig zu erkennen. Die dargestellten FAQs sollen als Grundlage für eine strukturierte Auseinandersetzung mit der KI-VO dienen und Unternehmen dabei unterstützen, ihre Compliance-Strategie im Bereich künstlicher Intelligenz rechtssicher und zukunftsorientiert auszurichten.

Inhalt

Was ist ein KI-System?

Nicht jede Software ist ein KI-System. Nach der Begriffsdefinition in Art. 3 Nr. 1 KI-VO müssen dafür insgesamt diese Voraussetzungen erfüllt sein:

„KI-System“ ist ein System, das...

... maschinengestützt ist:

Es muss sich um eine Software handeln, die nicht rein regelbasiert programmiert ist, sondern algorithmisch oder datenbasiert arbeitet.

... für einen in unterschiedlichem Grade autonomen Betrieb ausgelegt ist:

Das System ist kein „if-then-System“, sondern trifft teilautomatisiert bis vollständig autonome Entscheidungen ohne ständige menschliche Steuerung.

... nach seiner Betriebsaufnahme anpassungsfähig sein kann:

Das System ist lernfähig. Es hat die technische Möglichkeit zur Reaktion auf neue Eingaben. Es muss nur die potenzielle Fähigkeit zur Anpassung haben, zum Beispiel ein Feintuning auf Basis des Nutzerfeedbacks.

... die physische oder virtuelle Umgebung beeinflussen kann:

Das System „interagiert“, es hat reale Auswirkungen auf Menschen, Prozesse oder digitale Systeme.

... aus den erhaltenen Eingaben für explizite oder implizierte Ziele ableitet, wie Ausgaben (etwa Vorhersagen, Inhalte, Empfehlungen) oder Entscheidungen erstellt werden, die die Umgebung beeinflussen können:

Das System liefert Output, der für Handlungen genutzt wird oder diese direkt auslöst. Die Ableitungsfähigkeit ist die Fähigkeit, neue Inhalte auf Basis erlernter Muster zu erzeugen. Es werden Ergebnisse gewonnen und Schlussfolgerungen gezogen.

Ein KI-System nutzt daher Modelle, erkennt Muster, zieht eigenständig Schlüsse oder Prognosen und passt sein Verhalten datenbasiert an.

Die klassische Software arbeitet demgegenüber regelbasiert, führt vorab festgelegte „Wenn-Dann"-Anweisungen aus und verändert ihr Verhalten nicht selbstständig.

Beispiele:

Diese Software stellt beispielsweise kein KI-System dar:

- Buchhaltungssoftware, die nach festgelegten Regeln Rechnungen summiert und Mehrwertsteuer berechnet
- Die klassische SQL-Abfrage ohne adaptive Logik
- Ein medizinisches Diagnosetool, das „Wenn–Dann"-Regeln nutzt (z. B. „Wenn Fieber + Husten = Verdacht auf Grippe")
- Eine Industriesteuerung, die bei Überhitzung automatisch abschaltet

Was ist ein KI-Modell?

Die KI-VO enthält auch Regelungen für einige KI-Modelle.
Der Begriff des „KI-Modells“ wird in der KI-VO nicht definiert, allerdings formuliert ErwG 97, dass KI-Modelle „wesentliche Komponenten von KI-Systemen“ sind und für sich genommen keine KI-Systeme darstellen. KI-Modelle können danach auf verschiedene Weise in Verkehr gebracht werden, unter anderem über Bibliotheken, Anwendungsprogrammierschnittstellen (API), durch direktes Herunterladen oder als physische Kopie. Diese Modelle können weiter verändert oder zu neuen Modellen verfeinert werden. Damit KI-Modelle zu KI-Systemen werden, ist daher die Hinzufügung weiterer Komponenten, zum Beispiel einer Nutzerschnittstelle, erforderlich.

Ein KI-System ist damit die funktionsfähige KI-Anwendung in ihrer Gesamtheit, die dahinter stehende Technik, sozusagen der „technische Baustein“, ist dagegen das KI-Modell und beide sind durch eine Benutzeroberfläche verbunden.

Man kann sich das so vorstellen: Das KI-Modell ist das separate „Gehirn“, das nur dann kommunizieren und eingesetzt werden kann, wenn es in einen Kopf mit einer „Oberfläche“ mit Mund und Augen integriert ist. Erst beides zusammen wird zum KI-System.

Beispiele:

GPT oder Llama sind Modelle, die mit großen Textmengen trainiert sind, um Sprache zu verstehen und zu generieren. Sie werden in Chatbots, Übersetzungstools oder Textanalyse-Software integriert.

Für welche KI-Modelle gilt die KI-VO?

Die KI-VO enthält auch Regelungen für KI-Modelle: Es wird unterschieden zwischen KI-Modellen mit allgemeinem Verwendungszweck (General Purpose AI – GPAI, auch „Basismodelle“ oder „Allzweck-KI“) und KI-Modellen mit allgemeinem Verwendungszweck mit systemischem Risiko (GPAISR):

Ein KI-Modell mit allgemeinem Verwendungszweck ist nach der Begriffsbestimmung in Art. 3 Nr. 63 KI-VO im Wesentlichen ein KI-Modell, das eine erhebliche allgemeine Verwendbarkeit aufweist und in der Lage ist, unabhängig von der Art und Weise seines Inverkehrbringens ein breites Spektrum unterschiedlicher Aufgaben kompetent zu erfüllen. Es kann in eine Vielzahl nachgelagerter Systeme oder Anwendungen integriert werden.

Diese KI-Modelle werden daher nicht für eine spezifische Aufgabe oder Branche entwickelt, sondern können flexibel für verschiedene Anwendungen genutzt werden.

Beispiele:

- Große Sprachmodelle (LLMs) wie GPT, Claude oder DeepL
- Generative Bild-KI wie DALL-E oder Canva AI

Ein KI-Modell mit allgemeinem Verwendungszweck mit systemischem Risiko ist nach Art. 51 KI-VO ein KI-Modell, das darüber hinaus eine der folgenden Bedingungen erfüllt:

Es erreicht eine besonders hohe Rechenleistung, die in der KI-VO definiert ist:

Das KI-Modell verfügt über Fähigkeiten mit hohem Wirkungsgrad, die mithilfe geeigneter technischer Instrumente und Methoden, einschließlich Indikatoren und Benchmarks, bewertet werden (Art. 51 Abs. 1 a KI-VO). Der „hohe Wirkungsgrad“ wird nach Art. 51 Abs. 2 KI-VO erreicht, wenn die kumulierte Menge der für sein Training verwendeten Berechnungen, gemessen in Gleitkommaoperationen, mehr als 10^{25} Floating-Point Operations Per Second (FLOPS) beträgt.

Beispiele:

Modelle, die diesen Schwellenwert wahrscheinlich überschreiten:

- GPT-4
- Gemini

Es erreicht aufgrund seiner Wirkkraft ein systemisches Risiko:

Das KI-Modell verfügt unter Berücksichtigung der in Anhang XIII festgelegten Kriterien oder aufgrund einer Entscheidung des wissenschaftlichen Gremiums zufolge über Fähigkeiten oder eine Wirkung, die denen gemäß Art. 51 Abs. 1 a KI-VO entsprechen (Art. 51 Abs. 1 b KI-VO).

Kriterien sind danach u.a. die Anzahl der Parameter des Modells, die Qualität oder Größe des Datensatzes, die Menge der für das Trainieren des Modells verwendeten Berechnungen, gemessen in Gleitkommaoperationen oder anhand einer Kombination anderer Variablen, wie geschätzte Trainingskosten, geschätzter Zeitaufwand für das Trainieren oder geschätzter Energieverbrauch für das Trainieren, die Ein- und Ausgabemodalitäten des Modells, wie Text-Text (Große Sprachmodelle), Text-Bild, Multimodalität, die Benchmarks und Beurteilungen der Fähigkeiten des Modells, einschließlich unter Berücksichtigung der Zahl der Aufgaben ohne zusätzliches Training, der Anpassungsfähigkeit zum Erlernen neuer, unterschiedlicher Aufgaben, des Grades an Autonomie und Skalierbarkeit sowie der Instrumente, zu denen es Zugang hat, Reichweite auf den Binnenmarkt, Zahl der registrierten Endnutzer.

Für wen gelten die Pflichten nach der KI-VO?

Die KI-VO regelt in unterschiedlichem Maße Pflichten für diese Akteure:

Anbieter (Provider):

Jeder, der ein KI-System oder KI-Modell mit allgemeinem Verwendungszweck entwickelt oder entwickeln lässt und es in der EU unter eigenem Namen oder einer Handelsmarke in Verkehr bringt oder in Betrieb nimmt.

Betreiber (Deployer):

Jeder, der ein KI-System in eigener Verantwortung verwendet, es sei denn im Rahmen einer persönlichen und nicht beruflichen Tätigkeit.

Einführer (Importer):

Jeder, der in der Union ansässig oder niedergelassen ist und ein KI-System, das den Namen oder die Handelsmarke einer in einem Drittland niedergelassenen natürlichen oder juristischen Person trägt, in Verkehr bringt.

Händler (Distributor):

Jeder in der Lieferkette, der ein KI-System auf dem Unionsmarkt bereitstellt und nicht bereits Anbieter oder Einführer ist.

Produkthersteller (Product Manufacturer):

Jeder, der ein KI-System zusammen mit seinem Produkt unter seinem eigenen Namen oder seiner Handelsmarke in Verkehr bringt oder in Betrieb nimmt.

Gilt die KI-VO nur für europäische Unternehmen?

Nein, die KI-VO ist von Unternehmen immer dann zu beachten, sobald KI-Systeme in der EU in Verkehr gebracht oder genutzt werden. Damit gilt sie nicht nur, wenn Unternehmen ihren Sitz innerhalb der EU haben, sondern auch für Unternehmen mit Sitz in einem Drittstaat.

Im Einzelnen gilt die KI-VO für

- Anbieter, die in der EU KI-Systeme in Verkehr bringen oder in Betrieb nehmen oder KI-Modelle mit allgemeinem Verwendungszweck in Verkehr bringen, unabhängig davon, ob diese Anbieter in der Union oder in einem Drittland niedergelassen sind
- Betreiber von KI-Systemen, die ihren Sitz in der Union haben oder in der Union befinden
- Anbieter und Betreiber von KI-Systemen, die ihren Sitz in einem Drittland haben oder sich in einem Drittland befinden, wenn die vom KI-System hervorgebrachte Ausgabe in der Union verwendet wird
- Einführer und Händler von KI-Systemen
- Produkthersteller, die KI-Systeme zusammen mit ihrem Produkt unter ihrem eigenen Namen oder ihrer Handelsmarke in Verkehr bringen oder in Betrieb nehmen
- Bevollmächtigte von Anbietern, die nicht in der Union niedergelassen sind
- betroffene Personen, die sich in der Union befinden

Beispiel:

Ein US-amerikanisches Unternehmen entwickelt eine KI-Software, die Bewerbungen automatisch vorsortiert. Die Software wird über eine Online-Plattform auch den HR-Abteilungen europäischer Unternehmen angeboten. Folge: Das US-amerikanische Unternehmen muss sich als Anbieter bzw. Betreiber an die Vorgaben der KI-VO halten und unter anderem etwa eine Risikoklassifizierung und Konformitätsbewertung vornehmen und für die CE-Kennzeichnung sorgen, Dokumentationspflichten erfüllen und einen EU-Bevollmächtigten benennen.

Welche KI-Systeme gibt es?

Die KI-VO kategorisiert KI-Systeme in insgesamt vier Gruppen, die davon abhängig ist, welches Risiko von einem KI-System ausgeht. Das sind die Risikogruppen:

1. KI-Systeme mit unzulässigem Risiko

Diese KI-Systeme sind von vornherein verboten.

Art. 5 KI-VO verbietet bestimmte KI-Systeme, da sie ein unzulässiges Risiko für die Gesundheit, die Sicherheit oder Grundrechte mit sich bringen. Dazu gehört beispielsweise das Inverkehrbringen, die Inbetriebnahme oder die Verwendung von KI-Systemen, die manipulative oder täuschende Techniken einsetzen, die die Schutzbedürftigkeit von Personen aufgrund ihres Alters, einer Behinderung oder einer bestimmten sozialen oder wirtschaftlichen Situation ausnutzen oder die soziale Bewertungen von Personen (Social Scoring) vornehmen.

Kurz gesagt: Verboten sind KI-Systeme, die psychologisch manipulieren, schutzbedürftige Menschen ausnutzen, soziales Verhalten überwachen oder bewerten, biometrische Überwachung ohne enge Voraussetzungen betreiben oder emotionale oder verhaltensbezogene Bewertungen in sensiblen Kontexten vornehmen.

i

Beispiele:

- Eine App, die durch psychologische Manipulation Nutzer dazu bringt, gefährliche Entscheidungen zu treffen (z. B. übermäßiges Glücksspiel)
- Algorithmen in Sozialen Medien, die gezielt emotionale Schwächen ausnutzen, um Kaufentscheidungen zu befördern
- Spielzeug mit KI-Sprachassistenten, das Kinder zu riskantem Verhalten anstiftet
- Ein „Social Credit System“, das Bürger nach ihrem Verhalten im Alltag bewertet und Zugang zu öffentlichen Diensten einschränkt (ähnlich wie in China)

2. KI-Systeme mit hohem Risiko

Diese KI-Systeme sind erlaubt, bringen aber eine Fülle an Anforderungen und einen umfangreichen Pflichtenkatalog in Bezug auf Dokumentation, Risikomanagement, Qualitätsmanagement u.a. mit sich.

Art. 6 ff. KI-VO betrifft KI-Systeme mit hohem Risiko (High-Risk AI-Systems – HRAIS) für die Gesundheit, die Sicherheit oder Grundrechte. Diese KI-Systeme sind zwar zulässig, ihr Inverkehrbringen oder ihre Inbetriebnahme ist allerdings an weitreichende Anforderungen geknüpft. Art. 6 und 7 KI-VO regeln zunächst die Klassifizierung und Einordnung eines KI-Systems als Hochrisiko-KI-System. Danach liegt ein Hochrisiko-KI-System vor, wenn eine der nachfolgenden Anforderungen erfüllt ist:

Das KI-System wird als Sicherheitskomponente für ein Produkt verwendet, das unter die in Anhang I der KI-VO aufgeführten EU-Harmonisierungsrechtsvorschriften fällt oder das KI-System ist selbst ein solches Produkt (gilt ab 2. August 2027).

Das Produkt, dessen Sicherheitskomponente das KI-System ist oder das KI-System muss selbst als Produkt bereits einer Konformitätsbewertung durch Dritte gemäß den in Anhang I aufgeführten EU-Harmonisierungsrechtsvorschriften unterzogen werden (gilt ab 2. August 2027).

Das KI-System ist ein System nach Anhang III der KI-VO. Eine Ausnahme kann für diese KI-Systeme bestehen, wenn es kein erhebliches Risiko für die Gesundheit, Sicherheit oder Grundrechte natürlicher Personen birgt, indem es unter anderem nicht das Ergebnis der Entscheidungsfindung wesentlich beeinflusst (gilt ab 02.08.2026).

Im Prinzip werden danach solche KI-Systeme als Hochrisiko-KI-Systeme qualifiziert, die Menschen z. B. in Bezug auf Zugang zu Bildung, Arbeit, Kredite und Justiz direkt betreffen, die öffentliche Sicherheit oder Grundrechte berühren oder Teil eines sicherheitsrelevanten Produkts, wie z. B. von Autos oder Medizingeräten sind.

Beispiele:

- Software zur Zugangskontrolle per Gesichtserkennung
- KI zur automatischen Prüfung oder Bewertung von Bewerbungen
- KI zur Kreditwürdigkeitsprüfung (z. B. Scoring-Systeme bei Banken)
- Software in PKWs zum autonomem Fahren

3. KI-Systeme mit Transparenzrisiko

Hier interagieren KI-Systeme direkt mit Menschen, die auf diesen Umstand transparent hingewiesen werden müssen, damit sie nicht getäuscht werden können.

Für KI-Systeme, die für die Interaktion mit Menschen bestimmt sind, sieht Art. 50 KI-VO bestimmte Transparenzpflichten vor. Diese KI-Systeme sind so zu konzipieren, dass die betreffenden natürlichen Personen darüber informiert werden, dass sie mit einem KI-System interagieren (gilt ab 02.08.2026).

Diese KI-Systeme können gleichzeitig auch Hochrisiko-KI-Systeme oder KI-Systeme mit allgemeinem Verwendungszweck usw. sein, je nachdem, ob das System die entsprechenden Interaktionsmöglichkeiten bietet oder nicht.

Beispiele:

- Chatbots
- Sprachassistenten (z. B. Alexa, Siri)
- ChatGPT, wenn es als Kundenkommunikations-Servicetool eingesetzt wird
- Deepfakes (= KI-generierte Bild-, Audio- und Videoinhalte, die wirklichen Personen, Gegenständen, Orten, Einrichtungen oder Ereignissen ähneln und einer Person fälschlicherweise als echt oder wahrheitsgemäß erscheinen würden)

4. KI-Systeme mit minimalem oder keinem Risiko

Diese KI-Systeme fallen zwar in den Anwendungsbereich der KI-VO, unterliegen aber keinen besonderen Anforderungen oder Pflichten. Die EU-Kommission schätzt, dass etwa 80–90 % aller aktuellen KI-Anwendungen in diese niedrigste Risikoklasse fallen.

Diese KI-Systeme bleiben unreguliert und dürfen ohne die Erfüllung besonderer Anforderungen in Verkehr gebracht, in Betrieb genommen oder verwendet werden. Anderes gilt nur, wenn diese KI-Systeme gleichzeitig wegen ihrer Interaktionsmöglichkeiten ein KI-System mit Transparenzrisiko darstellen. Dann sind die Transparenzpflichten auch hier zu erfüllen.

Beispiele:

- Empfehlungssysteme auf Netflix, Spotify oder YouTube
- Übersetzungstools (z. B. DeepL, Google Translate)
- Spam-Filter
- Personalisierte Produktempfehlungen im Onlinehandel
- Heizungs- oder Lichtsteuerung im Smart Home
- Legal Tech AI
- KI in Videospielen (z. B. Gegnerverhalten, Story-Generierung)

Welche Pflichten gelten für die KI-Systeme der unterschiedlichen Risikostufen?

Ist die Klassifizierung des jeweiligen KI-Systems oder KI-Modells im Einzelfall erfolgt, sieht die KI-VO danach jeweils einen bestimmten Pflichtenkatalog für die unterschiedlichen Akteure vor:

1. KI-Kompetenz und Schulungen

Für Anbieter und Betreiber von KI-Systemen besteht grundsätzlich die Pflicht zur Sicherstellung der KI-Kompetenz aus Art. 4 KI-VO, und zwar unabhängig davon, in welche Risikoklasse das betreffende KI-System fällt. Danach ist dafür zu sorgen, dass das Personal und andere Personen, die mit dem Betrieb und der Nutzung von KISystemen befasst sind, über ein ausreichendes Maß an KI-Kompetenz verfügen. Zu berücksichtigen sind dabei deren technischen Kenntnisse, Erfahrung, Ausbildung und Schulung und der Kontext, in dem die KI-Systeme eingesetzt werden.

Die KI-Kompetenz zielt nach ErwG 20 darauf ab, die genannten Personen mit dem notwendigen Wissen auszustatten, um fundierte Entscheidungen über KI-Systeme zu treffen und ggf. Gefahren für sich und andere Personen zu erkennen.

Praxistipp:

Erstellen Sie eine Kompetenzmatrix dazu, wer im Unternehmen mit welchem Einsatzgebiet mit KI in Berührung kommt und welche Fachkompetenzen dazu erforderlich sind. Erstellen Sie auf dieser Basis ein Schulungskonzept, mit dem Ihre Mitarbeiter regelmäßig entsprechend ihrem jeweiligen Einsatzgebiet in Bezug auf allgemeine Grundsätze der KI-VO, Risikomanagement, Transparenz, Cybersicherheit usw. geschult werden.

2. Anforderungen und Pflichten bei Hochrisiko-KI-Systemen

Für Hochrisiko-KI-Systeme gilt zunächst der generelle Anforderungskatalog nach Art. 8 – 15 KI-VO, der bereits vor deren Inverkehrbringen und Inbetriebnahme erfüllt sein muss und zumeist Pflichten für den Anbieter während der Entwicklungsphase betrifft. Dazu gehören Anforderungen wie die

- Einrichtung und Unterhaltung eines Risikomanagementsystems
- Einhaltung bestimmter Anforderungen an die Daten-Governance
- Erstellung und Pflege einer technischen Dokumentation
- Protokollierung von Ereignissen während des Lebenszyklus des Systems
- Transparenzpflichten und Informationspflichten gegenüber Betreibern (Betriebsanleitung)
- Ermöglichung einer menschlichen Aufsicht
- Gewährleistung eines angemessenen Maßes an Genauigkeit, Robustheit und Cybersicherheit

1

Für **Anbieter** von Hochrisiko-KI-Systemen kommen zusätzlich die Pflichten aus Art. 16 ff. und Art. 43, 47 ff. KI-VO hinzu. Dazu zählen u.a.:

- Kennzeichnungspflichten: Angabe des Namens, des Handelsnamens bzw. der Handelsmarke und der Kontaktanschrift des Anbieters
- Einrichtung und Unterhaltung eines Qualitätsmanagementsystems
- Umfassende Dokumentationspflichten für 10 Jahre ab Inverkehrbringen oder Inbetriebnahme des KI-Systems
- Aufbewahrung der automatisch erzeugten Protokolle
- Umsetzung von Korrekturmaßnahmen und Informationspflicht gegenüber der Marktüberwachungsbehörde, wenn Grund zu der Annahme besteht, dass das KI-System nicht (mehr) den Anforderungen der KI-VO entspricht
- Zusammenarbeit mit den zuständigen Behörden

- Benennung eines EU-Bevollmächtigten, wenn der Anbieter in einem Drittland niedergelassen ist
- Durchführung eines Konformitätsbewertungsverfahrens
- Ausstellung einer EU-Konformitätserklärung
- Anbringen der CE-Kennzeichnung
- Registrierung in der EU-Datenbank

Betreiber von Hochrisiko-KI-Systemen müssen die Pflichten nach Art. 26 und 27 KI-VO erfüllen. Dazu zählen u.a.:

2

- Treffen geeigneter technischer und organisatorischer Maßnahmen zur Sicherstellung, dass das KI-System entsprechend der Betriebsanleitung des Anbieters verwendet wird
- Aussetzung des Betriebs, wenn die Anwendung gemäß Betriebsanleitung dazu führen kann, dass ein Risiko für die Gesundheit, Sicherheit oder die Grundrechte von Personen besteht
- Übertragung der menschlichen Aufsicht über das KI-System an natürliche Personen mit KI-Kompetenz
- Kontrolle, dass die Eingabedaten der Zweckbestimmung des KI-Systems entsprechen und ausreichend repräsentativ sind
- Ggf. Information an Arbeitnehmer und Arbeitnehmervertreter vor Inbetriebnahme oder Verwendung von Hochrisiko-Systemen im Beschäftigtenkontext
- Informationspflichten gegenüber Personen, sobald ein KI-System sie betreffende Entscheidungen trifft
- Information an Anbieter oder Händler des KI-Systems sowie der Marktüberwachungsbehörde, sobald Grund zu der Annahme für das Bestehen eines Risikos für die Gesundheit, Sicherheit oder die Grundrechte von Personen besteht
- Information an Anbieter und Händler/Einführer des KI-Systems sowie der Marktüberwachungsbehörde, sobald ein schwerwiegender Vorfall festgestellt wurde

- Aufbewahrung der automatisch erzeugten Protokolle über die Ereignisse während des gesamten Lebenszyklus des Systems für mindestens 6 Monate
- Ggf. Registrierung in der EU-Datenbank (gilt für Organe, Einrichtungen und sonstige Stellen der EU)
- Ggf. Durchführung einer Datenschutz-Folgeabschätzung (die Pflicht dürfte sich beim Betrieb eines Hochrisiko-Systems in der Regel bereits nach Art. 35 Datenschutzgrundverordnung - DSGVO ergeben) auf der Grundlage der vom Anbieter zur Verfügung gestellten Betriebsanleitung
- Ggf. Durchführung einer Grundrechte-Folgeabschätzung (gilt für Einrichtungen des öffentlichen Rechts und oder private Einrichtungen, die öffentliche Dienste erbringen sowie für Betreiber von Hochrisiko-Systemen zur Kreditwürdigkeits- und Bonitätsprüfung oder zur Risikobewertung und Preisbildung bei Lebens- und Krankenversicherungen)
- Kooperation mit den zuständigen Behörden

Einführer von Hochrisiko-KI-Systemen müssen zusätzlich die Pflichten nach Art. 23 KI-VO erfüllen. Dazu zählen u.a.:

3

- Prüfung, ob der Anbieter des Systems das Konformitätsbewertungsverfahren durchgeführt hat
- Prüfung, ob der Anbieter die technische Dokumentation erstellt hat
- Prüfung, ob das System mit der erforderlichen CE-Kennzeichnung versehen ist
- Prüfung, ob dem KI-System die EU-Konformitätserklärung und Betriebsanleitung beigefügt sind
- Prüfung, ob der Anbieter den ggf. erforderlichen EU-Bevollmächtigten benannt hat
- Information des Anbieters, der Bevollmächtigten und der Marktüberwachungsbehörden, wenn hinreichender Grund zu der Annahme besteht, dass das System ein Risiko für die Gesundheit, Sicherheit oder die Grundrechte von Personen birgt
- Angabe des Namens, des Handelsnamens oder der Handelsmarke und Anschrift
- Sicherstellung von ordnungsgemäßen Lagerungs- oder Transportbedingungen zur Gewährleistung der Konformität des KI-Systems

- Aufbewahrung eines Exemplars der von der notifizierten Stelle ausgestellten Bescheinigung, ggf. der Betriebsanleitung und der EU- Konformitätserklärung für 10 Jahre
- Nachweis der Konformität des KI-Systems auf begründete Anfrage einer zuständigen Behörde
- Zusammenarbeit mit den zuständigen Behörden

Hat ein Einführer hinreichenden Grund zu der Annahme, dass ein Hochrisiko-KI-System nicht den Anforderungen der KI-VO entspricht, darf er das System erst in Verkehr bringen, nachdem dessen Konformität hergestellt wurde. Er informiert den Anbieter bzw. die Bevollmächtigten und die Marktüberwachungsbehörden entsprechend.

Für **Händler** von Hochrisiko-KI-Systemen gelten die Pflichten nach Art. 24 KI-VO. Zu den Pflichten zählen u.a.:

4

- Prüfung, ob das System mit der erforderlichen CE-Kennzeichnung versehen ist
- Prüfung, ob dem KI-System die EU-Konformitätserklärung und Betriebsanleitung beigefügt sind
- Prüfung, ob der Anbieter des KI-Systems das Konformitätsbewertungsverfahren durchgeführt hat
- Prüfung, ob der Anbieter die technische Dokumentation erstellt hat
- Prüfung, ob der Anbieter und gegebenenfalls der Einführer des KI-Systems ihre Pflichten zur Anbieterkennzeichnung erfüllt haben und der Anbieter über ein Qualitätsmanagementsystem verfügt
- Sicherstellung von ordnungsgemäßen Lagerungs- oder Transportbedingungen zur Gewährleistung der Konformität des KI-Systems
- Information des Anbieters oder des Einführers sowie der zuständigen Behörden, sobald Grund zu der Annahme für das Bestehen eines Risikos für die Gesundheit, Sicherheit oder die Grundrechte von Personen besteht

- Nachweis der Konformität des KI-Systems auf begründete Anfrage einer zuständigen Behörde

- Zusammenarbeit mit den zuständigen Behörden

Auch hier gilt: Hat ein Händler hinreichenden Grund zu der Annahme, dass ein Hochrisiko-KI-System nicht den Anforderungen der KI-VO entspricht, darf er das System erst in Verkehr bringen, nachdem dessen Konformität hergestellt wurde. Er informiert den Anbieter bzw. den Einführer des Systems entsprechend.

Praxistipp:

Bereits zu Beginn des Projekts ist zu prüfen, ob das KI-System als hochriskant zu qualifizieren ist und welche Pflichten Sie konkret zu erfüllen haben. Entwickeln Sie ein KI-Compliance-System, um sicherzustellen, dass Sie laufend alle Pflichten nach der KI-VO erfüllen.

3. Pflichten bei KI-Systemen mit Transparenzrisiko

Für KI-Systeme mit Transparenzrisiko regelt Art. 50 KI-VO die sog. Transparenzpflichten.

Anbieter haben das KI-System so zu konzipieren und zu entwickeln, dass die betreffenden natürlichen Personen informiert werden, dass sie mit einem KI-System interagieren. Die erzeugten Ausgaben an Audio-, Bild-, Video- oder Textinhalten des KI-Systems müssen gekennzeichnet und als künstlich erzeugt oder manipuliert erkennbar sein.

Beispiel:

Der Anbieter eines KI-Systems zur Integration von Chatbots in Webseiten stellt technisch sicher, dass der Chatbot die Kommunikation mit dem Hinweis, „Hallo, ich bin ein KI-Assistent…“ eröffnet oder bringt einen entsprechenden Hinweis am Chat-Fenster an.

Anbieter haben damit technisch sicherzustellen, dass die synthetischen Inhalte maschinenlesbar als KI-generiert gekennzeichnet sind – und zwar so, dass die Kennzeichnung wirksam, systemübergreifend lesbar, manipulationsresistent und konsistent ist.

Betreiber eines KI-Systems, das Deepfakes erzeugt oder manipuliert, haben ebenfalls entsprechende Kennzeichnungspflichten: Sie müssen offenlegen, dass die Inhalte künstlich erzeugt oder manipuliert wurden (Art. 50 Abs. 4 KI-VO).

Beispiel:

Auf einer Webseite wird ein Deepfake-Werbevideo mit einer Person veröffentlicht, die einer prominenten Person zum Verwechseln ähnlich sieht. Im Video ist ein Hinweis „KI-generiert“ eingefügt.

Ein Textbeitrag in einem Social-Media-Kanal ist mit „KI-generiert“ gekennzeichnet.

Für **Betreiber** eines Emotionserkennungssystems oder eines Systems zur biometrischen Kategorisierung sind gesonderte Pflichten geregelt (vgl. Art. 50 Abs. 3 KI-VO): Der Betreiber muss die davon betroffenen natürlichen Personen über den Betrieb des Systems informieren; er muss sicherstellen, dass die Verarbeitung der personenbezogenen Daten mit der Datenschutzgrundverordnung (DSGVO) im Einklang steht.

Es gibt eine Ausnahme: Diese Pflicht gilt nicht, wenn das System gesetzlich zur Aufdeckung, Verhütung oder Ermittlung von Straftaten zugelassen ist und im Einklang mit dem Unionsrecht betrieben wird – vorausgesetzt, geeignete Schutzvorkehrungen für Rechte und Freiheiten Dritter bestehen.

Beispiel:

Eine Kundenservice-Kamera erkennt Gesichtsausdrücke, wie z. B. Lächeln oder Stirnrunzeln und ordnet sie emotionalen Zuständen, wie Ärger, Frustration oder Desinteresse zu, um den Service zu verbessern. Dann müssten die Kunden zu Beginn informiert werden, z.B. mit dem Hinweis: „Diese Kamera nutzt KI zur Emotionserkennung."

Für **Anbieter** und **Betreiber** gilt gleichermaßen: Nach Art. 50 Abs. 5 KI-VO müssen die Hinweise den betreffenden Personen spätestens zum Zeitpunkt der ersten Interaktion oder Aussetzung in klarer und eindeutiger Weise gegeben werden. Die Informationen müssen außerdem den geltenden Barrierefreiheitsanforderungen entsprechen.

4. Verhaltenskodizes bei KI-Systemen mit minimalem oder keinem Risiko

Für diese KI-Systeme gelten keine spezifischen Pflichten. Die KI-VO sieht aber in Art. 95 die Option vor, dass zukünftig freiwillig bestimmte Verhaltensweisen und Anforderungen eingehalten werden können.

Das Büro für künstliche Intelligenz der Europäischen Kommission (EU AI Office) und die Mitgliedstaaten sollen die Erstellung von entsprechenden Verhaltenskodizes fördern und erleichtern, damit KI-Systeme mit minimalem oder keinem Risiko zumindest einige grundlegende Anforderungen freiwillig erfüllen. Die Kodizes können sich auch auf ethische Leitlinien, Umweltnachhaltigkeit, KI-Kompetenz, Inklusivität, Vielfalt oder den Schutz vulnerabler Gruppen beziehen.

Gibt es Pflichten für KI-Modelle?

Ja, die KI-VO regelt auch diverse Pflichten für Anbieter von KI-Modellen.

Pflichten bei KI-Modellen mit allgemeinem Verwendungszweck

Anbieter von KI-Modellen mit allgemeinem Verwendungszweck haben die Pflichten nach Art. 53 KI-VO zu erfüllen:

- Erstellung und Aktualisierung einer technischen Dokumentation zum KI-Modell, die Trainings- und Testverfahren, die Ergebnisse seiner Bewertung und die Informationen nach Anhang XI der KI-VO enthält
- Zurverfügungstellung der technischen Dokumentation an die Anbieter, die die Integration des KI Modells in ihr KI-System beabsichtigen. Die Dokumentation muss Anbieter von KI-Systemen in die Lage versetzen, die Fähigkeiten und Grenzen des KI-Modells mit allgemeinem Verwendungszweck gut zu verstehen und ihren Pflichten gemäß dieser Verordnung nachzukommen und den Inhalt nach Anhang XII enthalten
- Umsetzung einer Copyright-Strategie: Strategie zur Einhaltung des Urheberrechts, insbesondere zur Ermittlung und Einhaltung eines gemäß Art. 4 Abs. 3 der DMS-Richtlinie geltend gemachten Rechtsvorbehalts (Nutzungsvorbehalt des Rechteinhabers beim Text- und Data Mining), auch durch modernste Technologien
- Erstellung und Veröffentlichung einer Zusammenfassung der für das Training des KI-Modells mit allgemeinem Verwendungszweck verwendeten Inhalte
- Zusammenarbeit mit den zuständigen Behörden
- Benennung eines EU-Bevollmächtigten, wenn der Anbieter in einem Drittland zugelassen ist

Pflichten bei KI-Modellen mit allgemeinem Verwendungszweck mit systemischem Risiko

Anbieter von KI-Modellen mit allgemeinem Verwendungszweck mit systemischem Risiko haben die Pflichten nach Art. 55 KI-VO zu erfüllen:

- Erfüllung der Pflichten nach Art. 53 und 54 KI-VO für ein KI-Modell mit allgemeinem Verwendungszweck
- Meldepflicht binnen 2 Wochen an die EU-Kommission, sobald ein KI-Modell die Anforderungen an ein systemisches Risiko erfüllt; es ist dann das Verfahren nach Artikel 52 Abs. 2 – 6 KI-VO einzuhalten
- Durchführung einer Modellbewertung mit standardisierten Protokollen und Instrumenten entsprechend dem Stand der Technik inklusive Durchführung und Dokumentation von Angriffstests, um systemische Risiken zu ermitteln und zu mindern
- Bewertung und Minderung von möglichen systemischen Risiken auf Unionsebene, einschließlich ihrer Ursachen, die sich aus der Entwicklung dem Inverkehrbringen oder der Verwendung von KI-Modellen mit allgemeinem Verwendungszweck mit systemischem Risiko ergeben können
- Erfassung und Dokumentation der einschlägigen Informationen über schwerwiegende Vorfälle und möglicher Abhilfemaßnahmen und unverzügliche Unterrichtung des EU-AI Office und der zuständigen nationalen Behörden
- Gewährleistung eines angemessenen Maßes an Cybersicherheit für das KI-Modell und dessen physische Infrastruktur

Welche Pflichten gelten, wenn ein KI-Modell in ein KI-System integriert wird?

Nach ErwG 97 Satz 9 gelten die spezifischen Vorschriften für KI-Modelle auch dann, wenn diese Modelle in ein KI-System integriert werden oder ein Teil davon sind. Die Pflichten für das jeweilige KI-Modell bleiben bestehen und sind dann von dem Anbieter, Betreiber usw. des KI-Systems mit zu erfüllen.

Beispiel:

Ein Unternehmen lizenziert verschiedene KI-Modelle (z. B. DeepSpeech, BERT, T5), die über APIs verbunden werden, um damit den Kundenservice zu automatisieren, so dass Anfragen per Text oder Sprache automatisch verstanden, beantwortet und an die richtige Abteilung weitergeleitet werden.

Das Unternehmen muss neben den Transparentpflichten des Anbieters und Betreibers zum KI-System aus Art.50 KI-VO zusätzlich die Pflichten nach Art.53 ff. KI-VO erfüllen: Erstellung einer technischen Dokumentation, Einhaltung der Urheberrechts-Compliance, Zusammenfassung der Trainingsinhalte usw.

Was gilt, wenn ein KI-Modell zu einem neuen KI-Modell modifiziert wird?

Die KI-VO enthält für diesen Fall keine Regelung. In den am 18.07.2025 veröffentlichen GPAI Leitlinien der EU-Kommission (Guidelines on the scope of the obligations for general-purpose AI models established by AI Act) stellt die EU-Kommission dazu jedoch unter Rn. 61 ff. klar:

> *„Nicht jede Änderung eines Allzweck-KI-Modells führt dazu, dass der nachgelagerte Modifikator als Anbieter des geänderten Allzweck-KI-Modells anzusehen ist. Stattdessen wird der nachgeschaltete Modifikator nur dann zum Anbieter des modifizierten Allzweck-KI-Modells, wenn die Modifikation zu einer erheblichen Änderung der Allgemeingültigkeit, der Fähigkeiten oder des systemischen Risikos des Modells führt. Indiz dafür, wann eine erhebliche Änderung vorliegt ist, dass die für die Modifikation verwendete Trainingsrechenleistung mehr als ein Drittel der Trainingsrechenleistung des ursprünglichen Modells beträgt. In diesen Fällen ist der Modifikator als Anbieter mit den entsprechenden Pflichten in Bezug auf das modifizierte, neue KI-Modell anzusehen.“*

Es kommt also bei der Frage, ob zusätzliche Pflichten zu erfüllen sind, auf die Abgrenzung zwischen „bloßer Anpassung“ und „erheblicher Modifikation“ des jeweiligen KI-Modells an.

Beispiel:

Ein KI-Modell wird auf Basis eines Finetunings für einen bestimmten Anwendungsfall abgestimmt: Ein Unternehmen nutzt ein großes Sprachmodell und nimmt ein Finetuning mit internen Vertragsmustern, FAQs und branchenspezifischem Vokabular vor. Die Trainingsrechenleistung dazu beträgt ca. 5–10 % des ursprünglichen Trainings. Damit bleibt die Allgemeingültigkeit erhalten, die Fähigkeiten werden nur spezialisiert und nicht erweitert und es entsteht kein neues systemisches Risiko. Das Unternehmen erhält nicht den Anbieterstatus.

Wann gelten Betreiber, Händler, Einführer oder sonstige Dritte als Anbieter?

Die KI-VO enthält nur in Bezug auf Hochrisiko-KI-Systeme dazu eine Reglung: Nach Art. 25 KI-VO werden Händler, Einführer, Betreiber oder sonstige Dritte zu Anbietern eines Hochrisiko-KI-Systems mit den entsprechenden Anbieterpflichten, wenn sie

- ein bereits in Verkehr gebrachtes oder in Betrieb genommenes Hochrisiko-KI-System mit ihrem Namen oder ihrer Handelsmarke versehen, auch wenn vertragliche Vereinbarungen eine andere Aufteilung der Pflichten vorsehen

- eine wesentliche Veränderung eines Hochrisiko-KI-Systems, das bereits in Verkehr gebracht oder in Betrieb genommen wurde, so vornehmen, dass es weiterhin ein Hochrisiko-KI-System bleibt

- die Zweckbestimmung eines KI-Systems, einschließlich eines KI-Systems mit allgemeinem Verwendungszweck, das nicht als hochriskant eingestuft wurde und bereits in Verkehr gebracht oder in Betrieb genommen wurde, so verändern, dass das betreffende KI-System zu einem Hochrisiko-KI-System wird

Der bisherige Anbieter wird von seinen Pflichten befreit, bleibt allerdings u.a. verpflichtet, mit dem neuen Anbieter zusammen zu arbeiten und ihm alle erforderlichen Informationen zur Verfügung zu stellen.

Praxistipp:

Prüfen Sie vor jeder eigenen Markteinführung, Umbenennung oder Integration, ob Sie rechtlich als Anbieter gelten – auch dann, wenn Sie die KI nicht selbst entwickelt haben. Warnsignale sind: Re-Branding, White-Label-Modelle, OEM-Produkte.

Zu jeder technischen oder funktionalen Änderung sollte vorab geprüft werden, ob sich Leistung, Zweck, Entscheidungslogik oder Risikoprofil des KI-Systems ändert. Insbesondere Zweckänderungen bergen ein hohes Risiko für Compliance-Fallen:
Ein Chatbot wird zur Personalauswahl, ein Analyse-Tool zur Kreditwürdigkeitsprüfung oder eine Bildanalyse zur Zugangskontrolle eingesetzt und macht ein Tool zum Hochrisiko-KI-System.

Ihre Ansprechpartner

Wir beraten Sie gern zu allen Fragen rund um die KI-VO

SABINE HEUKRODT-BAUER

Rechtsanwältin, Partnerin
Fachanwältin für IT-Recht
Fachanwältin für Gewerblichen Rechtsschutz
Zertifizierte KI-Beauftragte (TÜV)

+49 6131 28770 80
sabine.heukrodt-bauer@bette.legal

FLORIAN DECKER

Rechtsanwalt, Partner
Fachanwalt für IT-Recht
Zertifizierter KI-Beauftragter (TÜV)

+49 6131 28770 81
florian.decker@bette.legal

Was wir für Sie tun können

Wir unterstützen Sie dabei, KI rechtssicher einzusetzen und Risiken vorzeitig zu steuern, ohne Innovationen auszubremsen:

- Identifizierung Ihrer konkreten Pflichten
- Prüfung der Schnittstellen zu datenschutzrechtlichen Pflichten nach DSGVO
- Prüfung der Schnittstellen zu urheberrechtlichen Pflichten
- Risikoklassifizierung zur Einordnung von KI-Modellen und KI-Systemen
- Risikofolgeabschätzungen
- Compliance-Beratung und KI-Governance
- Erstellung von Schulungskonzepten, Durchführung von Schulungen
- Erstellen von Verträgen mit KI-Entwicklern
- Lizensierung von KI-Modellen und KI-Systemen
- Erstellen von Verträgen KI as a Service (KIaaS)

Über Bette Westenberger Brink

Wir sehen uns als partnerschaftliche Unternehmensberater. Und als solche sprechen wir nicht nur „fließend juristisch“, sondern vor allem verständlich und auf Augenhöhe. Nicht von Anwalt zu Mandant. Sondern von Mensch zu Mensch.

Unsere Anwälte helfen mittelständischen Unternehmen, öffentlichen Stellen und Finanzierern in diesen Praxisgruppen, nachhaltig erfolgreich zu sein:

Unternehmen & Compliance

Arbeit & Personal

Digitalisierung & Datenschutz

Verwaltung & Vergabe

Bau & Immobilien

Bitte beachten Sie, dass es sich bei den Informationen in diesem Whitepaper um eine vereinfachte Darstellung der Rechtslage handelt. Wir stellen Ihnen die vorliegenden Informationen nur unter Ausschluss jeglicher Haftung zur Verfügung. Eine Haftung für die Richtigkeit und Vollständigkeit der Informationen wird nicht übernommen. Die Nutzung der Informationen kann eine auf den Einzelfall abgestimmte, anwaltliche Rechtsberatung nicht ersetzen.

Bette Westenberger Brink

Sie haben noch Fragen?
Kontaktieren Sie uns.

Mainz

+49 6131 28770 0
+49 6131 28770 99
mainz@bette.legal

Große Langgasse 1a
D-55116 Mainz

Erfurt

+49 361 34740 0
+49 361 34740 99
erfurt@bette.legal

Anger 10
D-99084 Erfurt