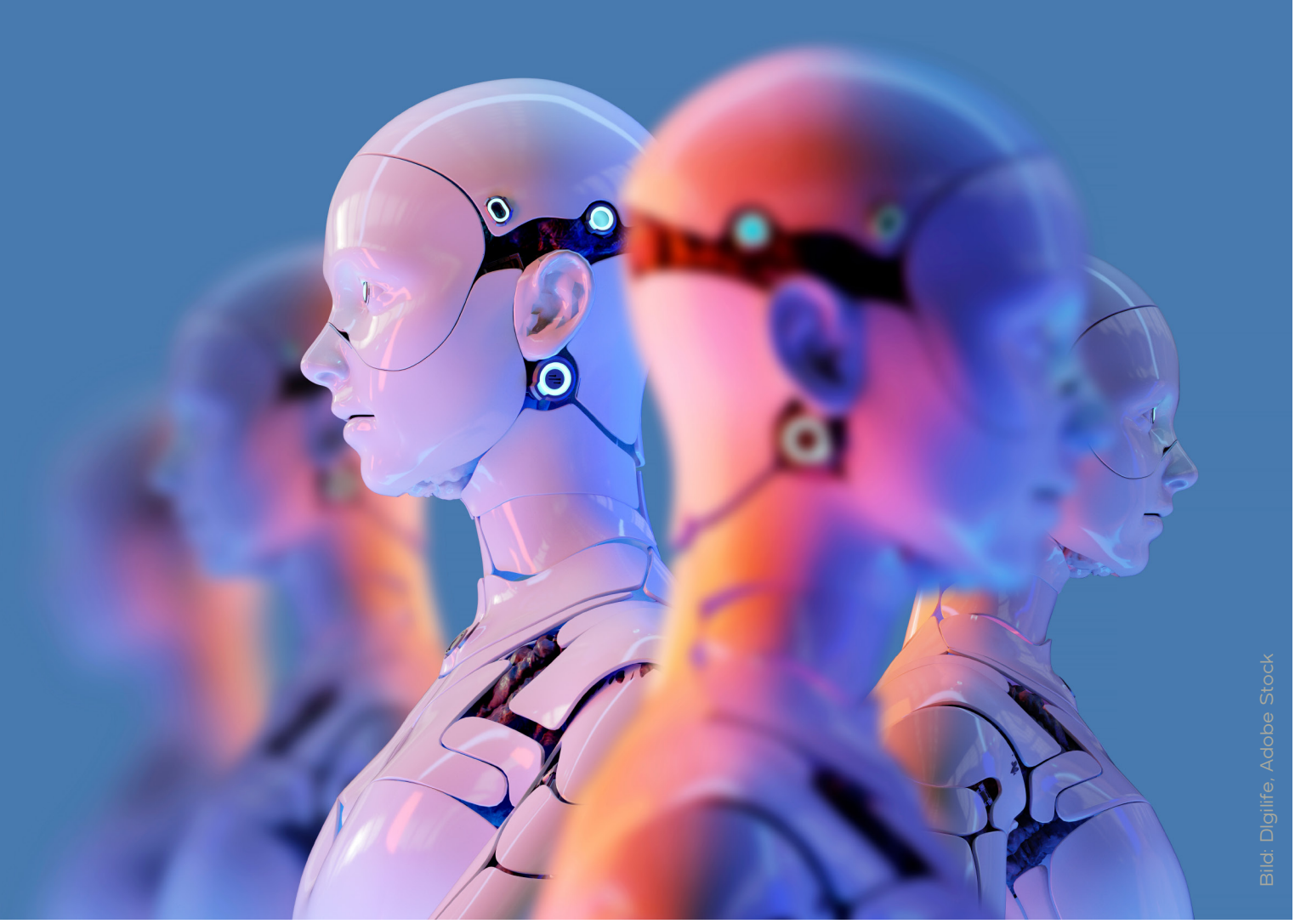


Bild: Digilife, Adobe Stock

Expertenwissen KI und Datenschutz

- KI-Verordnung
- DS-GVO
- KI-Kompetenz als Rechtspflicht

Schwartmann/Benedikt/Köhler

E-Book (PDF)

1. Auflage

DATAKONTEXT

1. KI-Kompetenz in zehn Kapiteln

Mit dieser Broschüre möchten wir Sie mit dem neuen Recht der künstlichen Intelligenz vornehmlich aus der Perspektive des betrieblichen Datenschutzes vertraut machen. Wir haben uns dazu entschieden, Sie in zehn Kapiteln mit unterschiedlichen Schwerpunkten über Fragen und Antworten behutsam und möglichst intuitiv mit der Materie vertraut zu machen. Den Kapiteln stellen wir diese Einleitung voran, um Ihnen das neue Recht zum einen Blick vorzustellen und Ihnen zugleich über Verweise in die Kapitel aufzuzeigen, wo Sie nähere Informationen finden.

Das Recht der künstlichen Intelligenz ist Produktrecht und insofern ganz anders aufgebaut und angelegt als etwa das Datenschutzrecht. Allerdings werden unter Verwendungen von KI-Systemen personenbezogene Daten verarbeitet und derselbe Lebenssachverhalt muss an den Regeln der KI-Verordnung und der DS-GVO gemessen werden. Um Ihnen das auch optisch deutlich zu machen haben wir uns dazu entschieden mit zwei Farben zu arbeiten. Alles, was von der KI-VO geregelt wird, weil es die Entwicklung und den Betrieb von KI-Modellen und KI-Systemen betrifft, ist orange markiert. Im Gegensatz dazu ist das, was den Einsatz von KI betrifft in blau dargestellt.

Insgesamt wollen wir Sie gerne über Fragen in die Materie einführen, die sich in Ihrer Praxis stellen und die wir im Anschluss beantworten. Wer wissen möchte, aus welchen Rechtsnormen die Antworten ableiten, kann das unter der Überschrift „Wo steht das?“ nachschauen.

Das KI-Recht nach der KI-VO (Kapitel 2)

Die **KI-VO** (Verordnung über Künstliche Intelligenz) ist seit dem 1. August 2024 geltendes Recht. Damit sich Staat, Gesellschaft und Wirtschaft an den neuen Rechtsrahmen gewöhnen können, wird er in Stufen wirksam. Die Berechnung aller Geltungsfristen hat am 2. August 2024 begonnen, Art. 113 UAbs. 2 KI-VO. Die KI-VO gilt für KI-Modelle und KI-Systeme. Im Fokus stehen derzeit Anwendungen, die wie ChatGPT Inhalte in menschlicher Sprache oder wie Dall-E Bilder hervorbringen, die man von menschlich erzeugten Inhalten von außen nicht mehr unterscheiden kann. Nach der Definition der KI-VO ist KI eine besondere, insbesondere **autonome und deshalb zwar in bestimmten Kontexten kontrollierbare, aber letztlich unbeherrschbare Technik**, die sich ohne menschliches Zutun verändern kann

Die juristische und rechtlich maßgebliche Definition der KI-VO stimmt zwar nicht in jedem Einzelfall mit den zahlreichen unterschiedlichen Begriffsbestimmungen überein, die zur Abgrenzung von KI und einfacher Software vorgeschlagen wurden. Im Kern geht es dem Rechtsakt aber um den Schutz natürlicher Personen vor den Risiken der Technologie, was die Anknüpfung an anderen besonders gefährlichen Merkmalen rechtfertigt. Oft ist die KI-VO gar nicht einschlägig, weil es nicht um KI im Sinne der KI-Verordnung geht. Manche Systeme gleichen nur Muster ab, ohne für autonomen Betrieb angelegt und anpassungsfähig zu sein. Gemeint ist damit Software, die sich nicht selbst verändern kann, die dem KI-Recht erst gar nicht unterfällt.

Die **KI-Verordnung gilt für jeden**, **der KI-Systeme beruflich in eigener Verantwortung einsetzt**. Sie regelt nämlich den Betrieb, sprich die Verwendung, von KI-Systemen und legt für „Betreiber“ Pflichten fest, z. B. nach Art. 50 Abs. 3 und 4 KI-VO. Wer als Handwerker seine Mitarbeiter- oder Kunden per Sprach-KI anspricht oder sich einen Werbeflyer von einer Bild-KI erzeugen lässt, ist Betreiber, denn er verwendet ein KI-System für berufliche Zwecke iSd Art. 3 Nr. 4 KI-VO.

Die KI-VO regelt **Ausnahmen von Ihrem Anwendungsbereich**. Das gilt insbesondere für **private Verwendung**. Wer KI für rein private Zwecke betreibt, ist in Einklang mit Art. 3 Nr. 4 KI-VO nicht Betreiber von KI. Für ihn gilt die KI-VO nicht. Allerdings muss man aufpassen. Lehrer, die ihren Schülern die Verwendung von ChatGPT zur Unterstützung bei den Hausaufgaben zur Verfügung stellen, sind Betreiber von KI-Systemen. Wer am Arbeitsplatz ein privat angeschafftes GPAI-System iSd Art. 3 Nr. 66 KI-VO verwendet, handelt beruflich und nicht privat. Das leuchtet ein, denn ein dienstlicher Text, der auf einem privaten Computer mit privater Software geschrieben wird, ist ja auch nicht privat. Derartige Verwendungen müssen zwischen Arbeitgeber und Be-

schäftigten abgestimmt sein. Betreiben ist dabei als Verwenden in eigener Verantwortung zu verstehen. Wer als Schreiner eine Sägemaschine verwendet, der betreibt sie im Rechtssinne. Wer bei der Arbeit ein KI-System verwendet, der betreibt es dementsprechend.

KI-Kompetenz: Rechtspflicht im Praxischeck (4. Kapitel)

Die KI-VO schreibt jedem, der ein KI-System wie ChatGPT beruflich in eigener Verantwortung verwendet, also betreibt, vor, KI-Kompetenz (Art. 4 KI-VO) zu besitzen und zu vermitteln. Da diese Pflicht für Betreiber, von KI-Systemen gilt, sind nicht nur Unternehmen und Behörden, sondern auch natürliche Personen verpflichtet, die ein KI-System wie ChatGPT nicht zu persönlichen Zwecken nutzen. Diese Pflicht muss im Februar 2025 umgesetzt sein, Art. 113 lit. a KI-VO. Konkrete Fragen, die jeder beim Umgang mit KI-Systemen wie ChatGPT mit Blick auf die KI-Kompetenz beantworten können sollte, lauten etwa wie folgt: Was ist ein KI-System? Was bedeutet Autonomie von KI? Warum kann KI nicht denken und trotzdem mit mir sprechen? Welche Nutzung von KI-Systemen ist gefahrlos möglich? Wo muss ich aufpassen? Was bedeutet „prompten" und wie geht das? Wie setze ich mich mit KI-Ergebnissen auseinander? Wie behalte ich als Mensch die Kontrolle über das Werkzeug KI? Was bedeutet der Einsatz von KI im beruflichen Alltag? Wo kann mir die Technik helfen, wo nicht? KI-Experten müssen das Wissen umsetzen. Ein Praxisscheck hilft bei der Einordnung des eigenen Kenntnisstandes.

Das Recht der KI-VO tritt neben das Datenschutzrecht (7., 8., 9. und 10. Kapitel)

Die KI-VO wählt einen rechtlichen Ansatz, der aus zwei Kernelementen besteht. Sie steckt zunächst einen gesetzlichen Rahmen für die Entwicklung und den Betrieb künstlicher Intelligenz ab und ordnet die Nutzung der Technik in Risikoklassen ein. Sodann löst die KI-VO das Problem der Übernahme von (menschlicher) Verantwortung bei maschineller Hilfe, indem sie den Menschen in die Pflicht nimmt, die autonome Technik selbstbestimmt zu stoppen, wenn es sein muss. Jenseits der Grenzen dieses Rechtsrahmens zum Schutz der Menschen und ihrer Rechte herrscht Freiheit zum Einsatz von KI, soweit nicht das von der KI-VO unberührte und unabhängig davon geltende sonstige Recht – etwa das Datenschutz- oder Urheberrecht – ohnehin Grenzen setzt. Wer KI-Systeme verwendet, der muss also nicht nur die Regeln der KI-VO einhalten. Da bei der Verwendung von KI-Systemen Texte und Bilder entstehen, deren Vorlagen geschützt sind und auf Inhalte zugegriffen wird, die geschützt sind, muss man etwa zusätzlich das Urheberrecht und das Markenrecht beachten. Das gilt bei der Verwendung von KI ohnehin und ebenso wie das Datenschutzrecht, wenn personenbezogene Daten verarbeitet werden (Art. 2 Abs. 7 KI-VO). Das Verbraucherschutzrecht, das Arbeitsrecht, das Schulrecht und das Jugendschutzrecht gelten ebenso. Diese Broschüre legt einen besonderen Schwerpunkt auf die Verknüpfung des KI-Rechts mit dem Datenschutzrecht, aber auch auf die Abgrenzung.

Möglichkeiten und Risken beim Einsatz von KI (4. und 5. Kapitel)

KI soll in der EU eingesetzt werden und in den meisten Fällen bietet der Einsatz viele Möglichkeiten. Wie jedes komplexe Werkzeug, kann KI aber auch Risiken bergen. Für die Frage, ob die Verwendung von KI riskant ist, kommt es auf den konkreten Verwendungszweck an. Von diesem macht die KI-VO auch die rechtlichen Grenzen des Einsatzes abhängig. Und den bestimmt derjenige, der die KI verwendet. Die KI-VO stuft die von KI ausgehenden möglichen Risiken in drei Kategorien ein. Sie lauten wie in einer Pyramide erstens risikoarm und erlaubt (Art. 51 ff. KI-VO), zweitens hochriskant (Art. 6 ff. KI-VO) und nur unter strengen Voraussetzungen zulässig und drittens verboten (Art. 5 KI-VO). Ist der Einsatzzweck hochriskant, gelten sehr strenge und spezifische Pflichten für den Betrieb eines KI-Systems nach Art. 26 KI-VO. Ein Verstoß gegen Pflichten der KI-VO kann nach dieser mit enormen Bußgeldern in der Spitze in Höhe von vielen Millionen Euro belegt werden (vgl. Art. 99 und 101 KI-VO). Nach Art. 99 Abs. 1 KI-VO erlassen die Mitgliedstaaten nach den Vorgaben der KI-VO Vorschriften für Sanktionen bei Verstößen. Da zahlreiche Normen der KI-VO dem Schutz der Menschen dienen, die von den Anwendungen betroffen sind, kann zudem die Haftung der Betreiber nach dem Schadensersatzrecht des Bürgerlichen

Gesetzbuches eintreten, wenn diese gegen Normen der KI-VO verstoßen. Da dieselben Handlungen mit Datenverarbeitungen verbunden sind, dürfte zusätzlich auch an die Haftung auf Schadensersatz nach der DS-GVO (Art. 82 DS-GVO) zu denken sein.

In den meisten Fällen ist KI nicht hochriskant

KI-Systeme mit allgemeinem Verwendungszweck (engl. general purpose Artificial Intelligence, kurz GPAI-Systeme) sind etwas Besonders. Sie haben gem. Art. 3 Nr. 66 KI-VO keinen spezifischen Verwendungszweck. Man kann sie – wie ChatGPT – für beliebige und damit auch riskante Zwecke nutzen. Auch GPAI ist von der KI-VO in Art. 51 ff. erfasst. Sie ist aber von der besonderen und spezifischen Regulierung für KI freigestellt, wenn sie für einen Zweck verwendet wird, den die KI-VO nicht als hochriskant klassifiziert. In diesem Fall darf man KI verwenden, ohne dass die KI-VO dafür besondere Regeln aufstellt. Das liegt daran, dass diese Nutzung kein oder nur ein geringes Risiko für Rechte und Freiheiten der Menschen beinhaltet. Da man GPAI für allgemeine und beliebige Zwecke verwenden kann, verlangt der Einsatz dieser KI jedem, der sie verwendet, eine schwierige Entscheidung ab: Es muss festgestellt werden, ob die Verwendung von GPAI im konkreten Fall hochriskant ist. Das hängt allein vom Zweck der Verwendung ab. Setzt man als Arbeitgeber oder als Beschäftigter unter Missachtung betrieblicher Anweisungen GPAI ein, dann muss man genau auf die Verwendungszwecke achten. Die KI-VO besagt nämlich, dass jeder, der GPAI eigenmächtig zu einem Zweck einsetzt, der als hochriskant einzustufen ist, „Anbieter“ von KI wird, Art. 25 Abs. 1 lit. c KI-VO. Er muss dann die komplexen, auf die Hersteller zugeschnittenen Pflichten aus Art. 16 KI-VO erfüllen. Dazu zählt etwa, die Anforderungen an ein Risikomanagementsystem (Art. 9 KI-VO), an Daten-Governance (Art. 10 KI-VO), Technische Dokumentationen und Aufzeichnungen (Art. 11 KI-VO) sowie Transparenzanforderungen (Art. 13 KI-VO) zu erfüllen. Diese sind für einfache Verwender aber kaum zu stemmen. Achtung: Wenn Anbieter, also Hersteller von KI-Modellen und KI-Systemen wie Open AI bei ChatGPT diese nur für beliebige und allgemeine Zwecke anbieten, dann sind sie nicht für konkrete Anwendungen der Betreiber verantwortlich.

Hochriskante KI ist erlaubt – es gelten aber besondere Anforderungen und Pflichten für Betreiber

Wann KI hochriskant ist, bestimmt das Recht selbst und benennt dafür konkrete Bereiche, vgl. Art. 6 Abs. 1 und Abs. 2 iVm Anhang III KI-VO. So ist etwa KI, die die Bedingungen von Arbeitsverhältnissen beeinflussen kann, oder die für die Bewertung von Lernergebnissen im Bildungsbereich, also bei Schülern, Auszubildenden oder Studierenden verwendet wird, hochriskant. Weitere hochriskante Bereiche sind unter anderem Gesundheit und Justiz. Oft kann man Hochriskantes und nicht Hochriskantes nur schwer auseinanderhalten. Als Faustformel kann man aber festhalten: Immer dann, wenn der Einsatz der KI einen Menschen in Rechten betreffen kann, also etwa bei der Bewertung in Beruf oder Schule oder bei der Erbringung öffentlicher Leistungen, sollte man zurückhaltend sein (vgl. Anhang III KI-VO). Sich von der KI eine Geschichte erzählen oder einen Reisetipp geben zu lassen, ist demgegenüber unproblematisch. Wenn man KI verwendet, die als hochriskant eingestuft ist, dann muss man die **strengen Pflichten einhalten**, die die KI-VO daran knüpft. Diese bestehen nach Art. 26 KI-VO etwa darin, passende Eingabedaten auszuwählen (Abs. 4), den Betrieb des KI-Systems zu überwachen (Abs. 5), von dem System erzeugte Protokolle aufzubewahren (Abs. 6) und von der Verwendung des Systems betroffene Arbeitnehmer zu informieren (Abs. 7). Zudem muss eine menschliche Aufsicht installiert werden (Abs. 2). Behörden müssen sich schließlich mit der Frage auseinandersetzen, wie der Einsatz des KI-Systems die Grundrechte der betroffenen Personen beeinflusst (sog. Grundrechte-Folgenabschätzung gem. Art. 27 KI-VO). Das Gesetz enthält **Ausnahmen von der Einstufung als hochriskant**. Das ist dann der Fall, wenn die KI nur unmaßgebliche Hilfsaufgaben übernimmt und ein zuvor gefundenes menschliches Ergebnis optimiert, aber nicht beeinflusst.

Verbotene KI kennen und meiden

Die verbotenen Zwecke legt die KI-VO ebenso fest wie die hochriskanten Zwecke. Verbotene Praktiken sind in Art. 5 KI-VO normiert. Dazu zählt etwa sog. Social Scoring, bei dem Menschen per KI manipuliert und klassifiziert werden und von dieser Klassifizierung deren staatliche Behandlung abhängig gemacht wird, Art. 5 Abs. 1 lit. c KI-VO.

2. Anwendungsbereich

Was ist vom sachlichen Anwendungsbereich der KI-VO umfasst?

In sachlicher Hinsicht erfasst die KI-VO KI-Systeme und KI-Modelle.

Wo steht es?

Art. 2 Abs. 1 KI-VO

Was genau unter einem **KI-System** zu verstehen ist, war im Entstehungsprozess der Verordnung lange umstritten. Insbesondere die Abgrenzung zu einfacher Software, die nach Einschätzung des europäischen Gesetzgebers nicht spezifisch regulierungsbedürftig ist, sorgte für zahlreiche, intensiv geführte Debatten. Schließlich einigten sich EU-Kommission, Parlament und Rat auf eine Begriffsbestimmung, die im Wesentlichen auf einen Vorschlag der OECD zur Definition von KI zurückgeht.

Praxischeck: Voraussetzungen für das Vorliegen eines KI-Systems

1. **maschinengestütztes** System,
2. das für einen in unterschiedlichem Grade **autonomen** Betrieb ausgelegt ist und
3. das nach seiner Betriebsaufnahme **anpassungsfähig** sein kann und
4. das aus den erhaltenen Eingaben für **explizite oder implizite Ziele**
5. **ableitet**, wie Ausgaben wie etwa Vorhersagen, Inhalt, Empfehlungen oder Entscheidungen erstellt werden,
6. die **physische oder virtuelle Umgebungen** beeinflussen können

Die Mehrzahl der genannten Tatbestandsvoraussetzungen ist nicht geeignet, um eine trennscharfe und rechtssichere Abgrenzung zu gewährleisten. Deutlich wird dies bei den Merkmalen der expliziten oder impliziten Ziele und der physischen oder virtuellen Umgebungen, die im Ergebnis alle Ziele und Umgebungen abdecken. Die Anpassungsfähigkeit des Systems ist darüber hinaus nach dem Gesetzeswortlaut eine rein fakultative Eigenschaft eines KI-Systems. Maschinengestützt bedeutet lediglich, dass das System auf einem Computer läuft, was ebenfalls keine Abgrenzung zu herkömmlicher Software ermöglicht. Schließlich liefert auch die Auslegung auf einen in unterschiedlichem Grade autonomen Betrieb kein Abgrenzungsmerkmal, da grundsätzlich jeder Grad der autonomen Aufgabenerfüllung erfasst ist.

Praxistipp:

Nach der derzeit vorherrschenden Meinung ist deshalb die Ableitungsfähigkeit die zentrale Voraussetzung eines KI-Systems. Diese ermöglicht es dem System, Ausgaben zu generieren, die sich so nicht explizit in seinen Trainingsdaten wiederfinden. Vielmehr leitet das System aus Daten Muster und Regeln ab, auf deren Basis es dann neue Inhalte erzeugt.

Diese Fähigkeit geht einher mit der besonderen Regulierungsbedürftigkeit von KI-Systemen. Denn aus ihr folgt, dass das System Teile der Handlungsanweisungen, auf deren Grundlage es die ihm zugewiesenen Aufgaben erfüllt, selbst schreibt. Nicht einmal der Entwickler des Systems hat deshalb einen Einblick in die Regeln, nach denen ein KI-System arbeitet. Diese Eigenschaft wird auch als Opazität bezeichnet, die Systeme werden in Abgrenzung zu explizit von einem

menschlichen Entwickler programmierten Systemen **autonome Systeme** genannt. Unter Autonomie ist dabei allein die autonome Erstellung von Handlungsanweisungen durch die Systeme zu verstehen. Die autonome Aufgabenübernahme, wie sie in der Begriffsbestimmung der KI-VO angelegt ist, liefert dagegen kein überzeugendes Abgrenzungskriterium.

Abb. : Hat ausschließlich ein menschlicher Programmierer dem Programm seine Handlungsanweisungen explizit vorgegeben, spricht einiges dafür, dass es sich bei dem Programm um herkömmliche Software handelt. Hat das Programm dagegen einige oder alle Handlungsanweisungen selbstständig aus Eingabedaten abgeleitet, handelt es sich regelmäßig um eine KI im SInne der KI-VO.

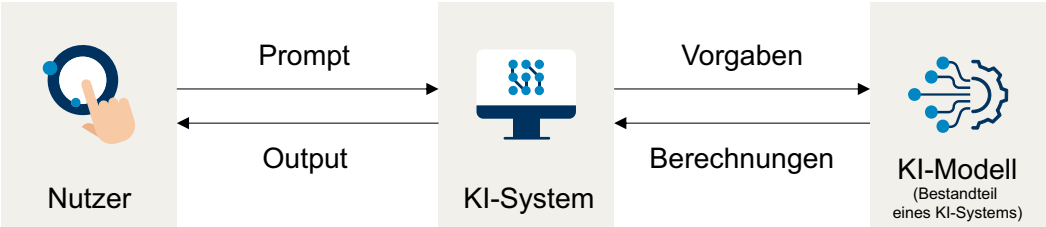
Die EU-Kommission hat den Auftrag, bis Ende 2024 Leitlinien für die praktische Anwendung der Definition von KI-Systemen zu erarbeiten. Es ist zu hoffen, dass darin einige der bisher unpraktikablen Tatbestandsmerkmale konkretisiert werden.

Wo steht es?

Art. 3 Nr. 1 KI-VO

KI-Modelle sind statistische Modelle, die die Basis zahlreicher KI-Systeme bilden. Die Modelle werden mit einer großen Zahl an Daten trainiert und passen dabei ihre Parameter an, um auf dieser Grundlage das wahrscheinlich treffendste Ergebnis für eine konkrete Anfrage des Nutzers zu ermitteln. KI-Sprachmodelle wie GPT berechnen beispielsweise wahrscheinliche Wortfolgen. Andere KI-Modelle generieren Bilder oder Videos.

Das KI-Modell ist eine Komponente des KI-Systems. Das System ist typischerweise mit einer Benutzeroberfläche ausgestattet. Außerdem übersetzt es die Eingabe des menschlichen Nutzers in die vom Modell verarbeitbaren Parameter und das Ergebnis des Modells zurück in natürliche Sprache.



Einige KI-Modelle weisen eine erhebliche allgemeine Verwendbarkeit auf und sind in der Lage, ein breites Spektrum unterschiedlicher Aufgaben kompetent zu erfüllen. Diese **KI-Modelle mit allgemeinem Verwendungszweck** können in eine Vielzahl nachgelagerter Systeme integriert werden. Da eine Unzulänglichkeit des Modells Auswirkungen auf alle nachgelagerten Systeme hat, werden KI-Modelle mit allgemeinem Verwendungszweck in der KI-VO gesondert reguliert.

Wo steht es?

Art. 3 Nr. 63 KI-VO

Gilt die KI-VO für jede KI?

Grundsätzlich gilt die KI-VO für jede KI. Allerdings sind einige besondere KI-Systeme vom Anwendungsbereich der KI-VO **ausgenommen**. Dies gilt für

1. KI-Systeme für militärische Zwecke, Verteidigungszwecke oder Zwecke der nationalen Sicherheit,
2. KI-Systeme und KI-Modelle für den alleinigen Zweck der wissenschaftlichen Forschung und Entwicklung und
3. KI-Systeme, die unter freien und quelloffenen Lizenzen bereitgestellt werden.

Wo steht es?

Art. 2 Abs. 3, 6 und 12 KI-VO

Die KI-VO ist in ihrem Kern Produktsicherheitsrecht. Der darin typische **Bestandsschutz** für bereits in Verkehr gebrachte oder in Betrieb genommene Produkte gilt auch für KI. Für die Praxis von besonderer Relevanz ist der Schutz von hochriskanten KI-Systemen, die vor dem 2. August 2026 in Verkehr gebracht oder in Betrieb genommen wurden. Private Akteure müssen die in der KI-VO vorgesehenen Pflichten im Umgang mit diesen Systemen nur erfüllen, wenn deren Konzeption nach dem Stichtag erheblich verändert wurde.

Praxischeck: Voraussetzungen für eine Befreiung von den Pflichten der KI-VO

1. Vorliegen eines KI-Systems
2. Kein verbotenes KI-System
3. Keine Komponente eines besonderen IT-Großsystems
4. Privater Akteur
5. Inverkehrbringen oder Inbetriebnahme vor dem 2. August 2026
6. Keine erhebliche Veränderung der Konzeption

Was genau unter einer **erheblichen Veränderung** zu verstehen ist, lässt der Gesetzgeber offen. Es dürfte mehr zu verlangen sein, als bei einer wesentlichen Veränderung, die in Art. 3 Nr. 23 KI-VO legaldefiniert ist. Ein einfaches Update genügt jedenfalls nicht, um eine erhebliche Veränderung des KI-Systems zu begründen. Die Befreiung gilt im Übrigen für **alle Akteure** der KI-VO, obwohl die Vorschrift ausdrücklich nur Betreiber in Bezug nimmt. Es handelt sich dabei um einen Übersetzungsfehler in der deutschen Fassung.

Wo steht es?

Art. 111 Abs. 2 KI-VO

Sind die Vorschriften der KI-VO im Umgang mit KI-Systemen immer zu beachten?

Die Vorschriften der KI-VO gelten grundsätzlich erst, wenn das KI-System in Verkehr gebracht oder in Betrieb genommen wird. Sofern ein KI-System mit diesem Ziel entwickelt wird, müssen

die Vorschriften aber bereits im Entwicklungsprozess berücksichtigt werden. Die Vorschriften der KI-VO sind daher regelmäßig bei **Entwicklung und Betrieb** von KI-Systemen zu beachten.

Die KI-VO sieht eine Bereichsausnahme für die **private Nutzung** von KI-Systemen vor. Diese greift, wenn die KI im Rahmen einer ausschließlich privaten und nicht beruflichen Tätigkeit verwendet wird. Die Nutzung darf also in keinem Bezug zu einer beruflichen Tätigkeit stehen. Die Bereichsausnahme greift nicht, wenn die KI zu beruflichen Zwecken auf einem privaten Gerät verwendet wird.

Praxisbeispiele:

Beispiele für eine private Nutzung	Beispiele für eine berufliche Nutzung
⇨ Verfassen eines Textes für eine Geburtstagskarte ⇨ Planung einer privaten Reise ⇨ private Nutzung als Ersatz für eine klassische Suchmaschine	⇨ Generieren eines Lebenslaufs für eine Bewerbung ⇨ Erfüllen einer beruflichen Aufgabe auf einem privaten Endgerät ⇨ sprachliche Überarbeitung einer beruflichen E-Mail

Wo steht es?

Art. 2 Abs. 10 KI-VO

In welchem Verhältnis stehen KI-VO und DS-GVO zueinander?

Grundsätzlich berührt die KI-VO nicht die Vorschriften der DS-GVO. So eindeutig diese Unberührtheitsklausel auch klingt, das konkrete Verhältnis von KI-VO und DS-GVO ist in einigen Fällen unklar. Die folgende Übersicht soll einige zentrale Berührungspunkte der beiden Rechtsakte sichtbar machen:

Praxischeck:

DS-GVO	KI-VO	Erläuterung
Art. 9 Abs. 2 Buchst. g	Art. 10 Abs. 5	neue Rechtsgrundlage für die Verarbeitung besonderer Kategorien personenbezogener Daten (dazu 7.1)
Art. 6 Abs. 4	Art. 59 Abs. 1	neue Rechtsgrundlage für die Weiterverarbeitung personenbezogener Daten zur Entwicklung bestimmter KI-Systeme im öffentlichen Interesse im KI-Reallabor (dazu 7.1)
Art. 17 Abs. 1	Art. 26 Abs. 10 UAbs. 2 Art. 60 Abs. 4 Buchst. i und Abs. 5 S. 1	neue Löschpflichten im Rahmen des Betriebs von KI-Systemen zur nachträglichen biometrischen Fernidentifizierung und des Testens von KI-Systemen unter Realbedingungen

Praxischeck:		
DS-GVO	**KI-VO**	**Erläuterung**
Art. 22 Abs. 1	Art. 2 Abs. 7 S. 2	keine neue Rechtsgrundlage für automatisierte Entscheidungen im Einzelfall einschließlich Profiling (dazu 7.4)

Enthält ein großes KI-Sprachmodell personenbezogene Informationen?

Große KI-Sprachmodelle (engl.: Large Language Model, LLM) lernen im Trainingsprozess, welche Wortbestandteile typischerweise aufeinanderfolgen. Das verleiht ihnen die Fähigkeit, im Betrieb wahrscheinliche Wortfolgen auf eine konkrete Eingabe des Nutzers zu generieren.

LLM simulieren also, wie die menschliche Sprache funktioniert. In diesem Kontext lassen sich Sprache und Information aber nicht sinnvoll trennen. Da das LLM die Funktionsweise menschlicher Sprache simuliert, speichert es zwangsläufig Informationen über die Umwelt und insbesondere über natürliche Personen, die mit dieser Sprache beschrieben werden. Für die betroffene Person ist es nicht relevant, ob eine sie betreffende Information im Wege einer binären Zuordnung oder durch Wahrscheinlichkeitsverteilungen hinterlegt und abrufbar ist. Deshalb ist auf die Beurteilung des Personenbezugs von LLM die aus der Rechtssache Breyer bekannte Rechtsprechung des EuGH übertragbar. Ob ein LLM personenbezogene Daten speichert ist damit eine Frage des Einzelfalls.

Praxistipp:

Ein großes KI-Sprachmodell speichert personenbezogene Daten, wenn der Abruf von Informationen über natürliche Personen erlaubt und praktisch durchführbar ist. Entscheidend wäre dann ob die Informationen mit einem verhältnismäßigen Aufwand an Zeit, Kosten und Arbeitskräften durchführbar ist.