PRIVACYXPERTS

Inklusive

Audio-Podcast zu den wichtigsten Begriffen sowie E-Book-Version für flexibles digitales Lesen

Michael Rohrlich

Kompendium KI-Recht

Die 100 wichtigsten Begriffe praxisnah erklärt

www.privacyxperts.de

Fachwissen, wann und wo Sie es brauchen: flexibel lesen und hören!

Mit diesem Kompendium erhalten Sie zwei praktische Ergänzungen für Ihren Arbeitsalltag:

Die **E-Book-Version** ermöglicht Ihnen einen flexiblen Zugriff auf alle Inhalte, ob im Büro, unterwegs oder im Homeoffice. So haben Sie Ihr Nachschlagewerk jederzeit griffbereit.

Zusätzlich steht Ihnen der begleitende Audio-Podcast **PrivacyXperts zum Hören** zur Verfügung. In interessanten Dialogen werden komplexe Themen wie KI-Verordnung, Datenschutz-Folgenabschätzung, Drittlandtransfer, Dokumentationspflichten und Risikobewertungen praxisnah diskutiert. Dabei beleuchten die Gesprächspartner typische Herausforderungen, Fallstricke und Lösungsansätze, die Datenschützerinnen und Datenschützer in ihrer täglichen Arbeit beschäftigen.

Die komplette Übersicht finden Sie hier:
https://www.privacyxperts.de/kompendium-ki-recht/

KOMPENDIUM KI-RECHT

DIE 100 WICHTIGSTEN BEGRIFFE PRAXISNAH ERKLÄRT

INHALTSVERZEICHNIS

VORWORT

Künstliche Intelligenz (KI) hat sich in kürzester Zeit von einer technologischen Vision zu einer prägenden Infrastruktur unserer Gegenwart entwickelt. Systeme, die Texte verfassen, Bilder erzeugen, komplexe Datenmengen analysieren, Entscheidungen unterstützen oder gar eigenständig treffen, sind inzwischen Teil des Alltags von Unternehmen, Behörden, Freiberuflern und auch Privatpersonen geworden. Es handelt sich also nicht, wie man immer noch teilweise liest, um eine „Zukunftstechnologie" – KI ist längst mitten unter uns.

Mit dieser rasanten Entwicklung wächst jedoch auch der Bedarf an rechtlicher Orientierung. Denn mit der KI-Nutzung stellen sich zahlreiche rechtliche Fragen: Wem gehören von KI erzeugte Inhalte? Welche Daten dürfen für das KI-Training verwendet werden? Wer haftet für fehlerhafte KI-Entscheidungen? Welche Transparenzpflichten bestehen? Und welche Rolle spielen etwa die Bereiche Datenschutz, Urheberrecht oder auch das allgemeine Persönlichkeitsrecht in einer zunehmend automatisierten Informationswelt?

Die europäische und nationale Gesetzgebung reagiert auf diese Herausforderungen mit einer Dynamik, wie sie in der Technologie- und Digitalregulierung bislang selten zu beobachten war. Besonders prägend ist dabei der europäische Rechtsrahmen zur Regulierung von künstlicher Intelligenz, der mit der KI-Verordnung (dem sogenannten AI Act) erstmals ein umfassendes Regelwerk für KI-Systeme geschaffen hat. Zugleich greifen bestehende gesetzliche Rahmenbedingungen weiterhin unmittelbar, nämlich etwa Datenschutzrecht, Urheberrecht, Wettbewerbsrecht, Markenrecht, Produkthaftungsrecht oder auch die Plattformregulierung.

Die rechtliche Realität der künstlichen Intelligenz ist daher kein isoliertes Spezialgebiet, sondern als Querschnittsmaterie ein komplexes Geflecht aus bestehenden Normen und neuen Regulierungsansätzen. Genau an dieser Stelle setzt der vorliegende Ratgeber an. Dieses Buch versteht sich als strukturierter Wegweiser durch die wichtigsten Begriffe, Konzepte und Rechtsfragen rund um künstliche Intelligenz. 100 zentrale Begriffe aus dem KI-Recht und angrenzenden Rechtsgebieten werden systematisch aufbereitet – von „A" wie „AI Act" über „K" wie „Künstliche Intelligenz" und „P" wie „Prompt" bis „Z" wie „Zweckbestimmung". Jeder Begriff wird nicht nur juristisch und zum Teil technisch eingeordnet, sondern auch in seinem praktischen Kontext erläutert. Das Ziel dieses Kompendiums ist dabei bewusst praxisorientiert. Neben rechtlichen Ausführungen und Einordnungen enthalten zahlreiche Einträge zusätzliche Hilfestellungen für die Anwendung im Alltag z. B. durch diverse Beispiele, Checklisten, Praxistipps etc. Damit richtet sich dieses Werk

nicht nur an Juristen, sondern vor allem auch an diejenigen, die sich beruflich mit KI beschäftigen bzw. diese beruflich nutzen, seien es Leitungspersonen, Mitglieder aus Betriebs- bzw. Personalrat, KI-Manager, IT-Experten, Digitalisierungsprofis oder externe Berater – und nicht zuletzt an alle, die sich fundiert mit den rechtlichen Grundlagen von KI auseinandersetzen möchten.

Die alphabetische Struktur des Buchs ermöglicht dabei einen schnellen Zugriff auf einzelne Themen, ohne dass eine lineare Lektüre erforderlich ist. Zugleich ergibt sich durch die Vielzahl der Begriffe ein Gesamtbild der rechtlichen Architektur rund um künstliche Intelligenz. Ein besonderes Anliegen dieses Ratgebers ist es, Recht verständlich zu vermitteln, ohne seine Komplexität zu verkürzen. KI-Recht ist ein umfangreiches und zugleich sehr dynamisches Feld, das sich in rasanter Geschwindigkeit weiterentwickelt. Neue Technologien führen zu neuen rechtlichen Fragestellungen, und gesetzgeberische Initiativen passen den Rechtsrahmen kontinuierlich an. Dieses Kompendium kann und will daher keine endgültigen Antworten auf individuelle Problemstellungen liefern. Es soll vielmehr Orientierung geben, Zusammenhänge aufzeigen und eine fundierte Grundlage für weitergehende rechtliche Analysen schaffen. Außerdem kann dieses Werk selbstverständlich keine individuelle Rechtsberatung ersetzen, sondern nur allgemeine juristische Informationen liefern.

Wer mit KI arbeitet, muss sich nicht nur mit technischen Fragen befassen, sondern zunehmend auch mit rechtlichen Anforderungen. Fragen der Compliance, der Dokumentation, der Transparenz und der Verantwortlichkeit werden zu zentralen Bestandteilen jeder KI-Strategie. Dieser Ratgeber soll dazu beitragen, diese Herausforderungen besser zu verstehen und rechtssicher zu gestalten.

Rechtsanwalt Michael Rohrlich, Würselen
(www.ra-rohrlich.de)

Michael Rohrlich ist Rechtsanwalt, Fachautor, Dozent und Videotrainer. Seine beruflichen Schwerpunkte liegen auf den Gebieten IT und Onlinerecht, E-Commerce, Print bzw. Onlinepublikationen. Er betreibt auch seine eigenen Webprojekte (z. B. Rechtssicher.info).

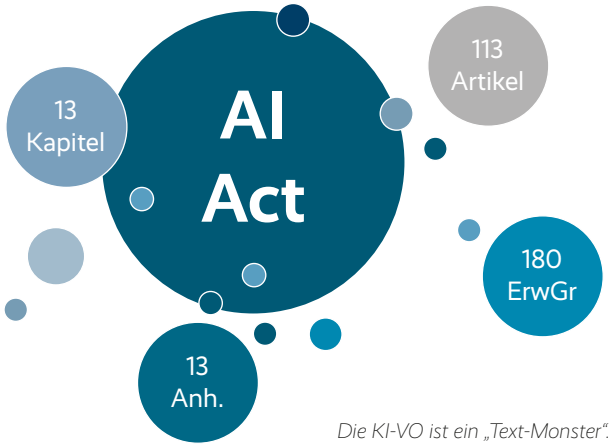
Darüber hinaus ist Michael Rohrlich Autor mehrerer Bücher und E-Books. Als Videotrainer ist er seit 2012 exklusiv für LinkedIn Learning (ehemals video2brain) tätig.

AI ACT

Hinter den Begriff „AI Act“ steckt die Verordnung (EU) 2024/1689 des Europäischen Parlaments und des Rates vom 13.06.2024 zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz und zur Änderung der Verordnungen (EG) Nr. 300/2008, (EU) Nr. 167/2013, (EU) Nr. 168/2013, (EU) 2018/858, (EU) 2018/1139 und (EU) 2019/2144 sowie der Richtlinien 2014/90/EU, (EU) 2016/797 und (EU) 2020/1828 (Verordnung über künstliche Intelligenz). Diese wird in Deutschland kurz als „KI-Verordnung“, oder noch kürzer: „KI-VO“, bezeichnet – oder umgangssprachlich eben mit der englischen Bezeichnung „AI Act“. Der AI Act ist als EU-Verordnung unmittelbar anwendbares Recht in den einzelnen Mitgliedstaaten, im Unterschied zu EU-Richtlinien bedarf sie keiner Umsetzung mehr ins nationale Recht.

Hinweis:
Mit Ausnahme dieses Abschnitts wird im Rahmen dieses Ratgebers anstelle von „AI Act“ die deutsche Bezeichnung, also „KI-Verordnung“ oder kurz: „KI-VO“, verwendet. In den Medien liest man hingegen sehr häufig das Synonym „AI Act“.

Der AI Act enthält insgesamt 113 Vorschriften (Artikel) sowie 13 Anhänge. Als „Auslegungshilfe“ dienen die vorangestellten insgesamt 180 Erwägungsgründe (ErwGr). Die reine Anzahl der Normen scheint, z. B. im Vergleich mit der Datenschutzgrundverordnung (99 Artikel), zwar nicht wesentlich höher. Allerdings haben es die einzelnen Vorschriften in sich und sind teilweise sehr umfangreich. Für die Praxis wichtige Regelungen, wie etwa in Art. 5 oder 6 der KI-VO, sind extrem umfangreich, enthalten Voraussetzungen, Ausnahmen, teilweise auch Gegenausnahmen und verweisen zudem an manchen Stellen auch noch auf Anhänge. Hinzu kommt, dass speziell die deutsche Sprachfassung der KI-VO an einigen Stellen nicht besonders gut gelungen ist, da sie unter einem starken zeitlichen Druck entstanden ist.



Die KI-VO ist ein „Text-Monster“.

Beim AI Act handelt es sich um den Rechtsrahmen der EU für KI-Systeme. Er zählt zur Kategorie der Produktregulierung, hat also die gesamte Wertschöpfungskette im Blick, von der Herstellung über den Vertrieb bis hin zur Nutzung von KI-Systemen. Er teilt KI-Systeme in verschiedene Risikoklassen ein (etwa „untragbar" oder „hochriskant") und regelt unterschiedliche Anforderungen (z. B. Datenqualität, Transparenz, menschliche Aufsicht) für alle Akteure der Wertschöpfungskette, vom Hersteller über Importeure und Händler bis hin zu Nutzern.

Außerdem enthält der AI Act Vorgaben zur Marktüberwachung. Zudem soll der AI Act Innovation fördern, aber zugleich Risiken (Diskriminierung, Sicherheitsprobleme, Grundrechtsverletzungen) durch strenge Regeln mindern.

Kapitel 1 (Art. 1–4)	Allgemeine Bestimmungen
Kapitel 2 (Art. 5)	Verbotene KI-Praktiken
Kapitel 3 (Art. 6–49)	Hochrisiko-KI-Systeme
Kapitel 4 (Art. 50)	Transparenzpflichten
Kapitel 5 (Art. 51–56)	KI-Modelle mit allg. Verwendungszweck
Kapitel 6 (Art. 57–63)	Maßnahmen zur Innovationsförderung
Kapitel 7 (Art. 64–70)	Governance
Kapitel 8 (Art. 71)	EU-Datenbank für Hochrisiko-KI-Systeme
Kapitel 9 (Art. 72–94)	Beobachtung nach dem Inverkehrbringen/Marktüberwachung
Kapitel 10 (Art. 95–96)	Verhaltenskodizes und Leitlinien
Kapitel 11 (Art. 97–98)	Befugnisübertragung und Ausschussverfahren
Kapitel 12 (Art. 99–101)	Sanktionen
Kapitel 13 (Art. 102–113)	Schlussbestimmungen (u. a. Geltungsbeginn)

Ein Blick ins Inhaltsverzeichnis des AI Acts zeigt, wo die Schwerpunkte liegen, nämlich insbesondere im Bereich der Hochrisiko-KI-Systeme.

Hinweis:
Der AI Act verfolgt einen **risikobasierten Ansatz,** sprich: Je höher das Risiko, desto mehr muss unternommen werden, um zu verhindern, dass es sich realisiert. Je nach Akteur und Risikoklasse bestehen unterschiedliche Pflichten.

Der AI Act ist zwar bereits in Kraft getreten, seine Anwendbarkeit wird jedoch stufenweise umgesetzt:

1. Inkrafttreten: **01.08.2024**
2. Wirksamwerden einzelner Vorschriften

   a) **02.02.2025**

   - Allg. Bestimmungen (Art. 1 bis 3 KI-VO)
   - KI-Kompetenz (Art. 4 KI-VO)
   - Verbot bestimmter KI-Praktiken (Art. 5 KI-VO)

   b) **02.08.2025**

   - KI mit allgemeinem Verwendungszweck (GPAI)
   - Notifizierungsstellen
   - Daten-Governance
   - Sanktionen (außer denen für GPAI-Anbieter)

   c) **02.08.2026**

   - Hochrisiko-KI-Systeme (Art. 6 Abs. 2, Anhang III KI-VO)
   - KI-Systeme, die nicht in die Hochrisiko-Klasse fallen
   - Sanktionen für GPAI-Anbieter
   - sonstige Vorschriften

   d) **02.08.2027**

   - Hochrisiko-KI-Systeme (Art. 6 Abs. 1, Anhang I KI-VO)

3. Übergangsfristen

   a) **02.08.2027**

   - Für Anbieter von KI-Modellen mit allgemeinem Verwendungszweck, die vor dem 02.08.2025 in Verkehr gebracht wurden (Art. 111 Abs. 3 KI-VO)

   b) **02.08.2030**

   - Für Anbieter und Betreiber von Hochrisiko-KI-Systemen, die bestimmungsgemäß von Behörden verwendet werden sollen und die vor dem 02.08.2026 in Verkehr gebracht oder in Betrieb genommen worden sind (Art. 111 Abs. 2 KI-VO)

   c) **31.12.2030**

   - Für bestimmte Komponenten von IT-Großsystemen, wenn diese vor dem 02.08.2027 in Verkehr gebracht oder in Betrieb genommen worden sind (Art. 111 Abs. 1 KI-VO)

Hinweis:
In der EU wird im Rahmen des sogenannten Digital Omnibus on AI diskutiert, ob Änderungen an der KI-VO vorgenommen werden sollen. Insbesondere wird hierbei geplant, die Anwendung der Hochrisiko-Vorschriften zu verschieben, und zwar auf den 02.12.2027 (für Hochrisiko-KI-Systeme nach Art. 6 Abs. 1, Anhang III KI-VO) und auf den 02.08.2028 (für Hochrisiko-KI-Systeme nach Art. 6 Abs. 1, Anhang I KI-VO). Ob und wann diese Änderungen kommen, lässt sich derzeit jedoch noch nicht abschließend beurteilen.

Der Anwendungsbereich bestimmt sich wie folgt:

1. Ausnahmen

a) KI-Systeme ausschließlich für Zwecke der nationalen Sicherheit (Art. 2 Abs. 3 KI-VO)

b) KI-Systeme ausschließlich für Verteidigungszwecke (Art. 2 Abs. 3 KI-VO)

c) KI-Systeme ausschließlich für militärische Zwecke (Art. 2 Abs. 3 KI-VO)

d) KI-Systeme und KI-Modelle (inklusive ihres Outputs) ausschließlich für wissenschaftliche Forschung entwickelt und in Betrieb genommen (Art. 2 Abs. 6 KI-VO)

e) KI-Systeme, die unter freien/quelloffenen Lizenzen stehen, sofern diese nicht als Hochrisiko-KI-System (Art. 6 KI-VO) oder verbotene KI-Praktik (Art. 5 KI-VO) in Verkehr gebracht oder in Betrieb genommen werden oder sie unter die Transparenzpflichten aus Art. 50 KI-VO fallen (Art. 2 Abs. 12 KI-VO)

f) Behörden in Drittländern oder internationale Organisationen, soweit diese Behörden/Organisationen KI-Systeme im Rahmen der internationalen Zusammenarbeit oder internationaler Übereinkünfte im Bereich der Strafverfolgung und justiziellen Zusammenarbeit mit der EU oder mit einem oder mehreren EU-Mitgliedstaaten verwenden und sofern ein solches Drittland oder eine solche internationale Organisation angemessene Garantien hinsichtlich des Schutzes der Privatsphäre, der Grundrechte und der Grundfreiheiten von Personen bietet (Art. 2 Abs. 4 KI-VO)

g) Forschungs-, Test- und Entwicklungstätigkeiten zu KI-Systemen oder -Modellen, bevor diese in Verkehr gebracht oder in Betrieb genommen wurden (Art. 2 Abs. 8 KI-VO)

h) Ausschließlich persönliche (und nicht berufliche) Nutzung von KI-Systemen durch Privatpersonen (sogenannte Haushaltsausnahme, Art. 2 Abs. 10 KI-VO)

i) Bestehende Hochrisiko-KI-Systeme, die vor dem 02.08.2026 in Verkehr gebracht oder in Betrieb genommen worden sind, ohne erhebliche Änderung der Systemkonfiguration (Art. 111 Abs. 2 KI-VO)

2. Örtlich

a) Entwicklung/Verwendung in der EU: Betreiber von KI-Systemen, die sich in der EU befinden oder die ihren Sitz in der EU haben (Niederlassungsprinzip, Art. 2 Abs. 1 lit. b) KI-VO)

b) Vertrieb oder Verwendung in der EU: Anbieter, die KI-Systeme in der EU in Verkehr bringen oder in Betrieb nehmen bzw. die GPAI in Verkehr bringen (Marktortprinzip, Art. 2 Abs. 1 lit. a) KI-VO)

c) Verwendung der Ausgabe in der EU: Anbieter/Betreiber von KI-Systemen (unabhängig vom Sitzland), deren Ausgabe in der EU verwendet wird (extraterritoriale Wirkung, Art. 2 Abs. 1 lit. c) KI-VO)

Kompakt-Checkliste AI Act

Der Branchenverband Bitkom hat im Januar 2026 die zweite Version des „Umsetzungsleitfaden[s] zur KI-Verordnung“ auf seiner Website zum kostenfreien Download bereitgestellt. Darin werden verschiedene Schritte der Prüfung zur Einhaltung der Vorgaben des AI Acts genannt:

- **Schritt 1.1:** Handelt es sich um ein KI-System im Sinne der KI-VO?
- **Schritt 1.2:** Abgrenzungsfragen KI-System und General Purpose AI (GPAI)
- **Schritt 1.3:** Bin ich Regulierungsadressat?
- **Schritt 1.3.1:** Bin ich Anbieter?
- **Schritt 1.3.2:** Bin ich Betreiber?
- **Schritt 1.3.3:** Bin ich Einführer?
- **Schritt 1.3.4:** Bin ich Händler?
- **Schritt 1.3.5:** Bin ich Produkthersteller?
- **Schritt 1.3.6:** Bin ich Bevollmächtigter des Anbieters?
- **Schritt 1.4:** Ist der räumliche Anwendungsbereich eröffnet?
- **Schritt 2:** In welche Risikoklasse fällt mein KI-System?
- **Schritt 2.1:** Ist einer der Verbotstatbestände aus Art. 5 einschlägig?
- **Schritt 2.2:** Ist das System hochriskant nach Art. 6 Abs. 1 i. V. m. Anhang I KI-VO?
- **Schritt 2.3:** Ist das System hochriskant nach Art. 6 Abs. 2 i. V. m. Anhang III KI-VO?
- **Schritt 2.4:** Ist eine Ausnahme im Sinne von Art. 6 Abs. 3 KI-VO gegeben?
- **Schritt 2.5:** Geht vom KI-System ein geringes Risiko aus?
- **Schritt 3:** Einstellen verbotener Praktiken
- **Schritt 4.1:** Welche Pflichten muss ich als Anbieter eines Hochrisiko-KI-Systems erfüllen?
- **Schritt 4.1.1:** Ist Art. 8 Abs. 2 KI-VO einschlägig?
- **Schritt 4.1.2:** Wie ist das Risikomanagementsystem auszugestalten?
- **Schritt 4.1.3:** Wie ist die Daten-Governance zu gestalten?
- **Schritt 4.1.4:** Wie ist die technische Dokumentation auszugestalten?
- **Schritt 4.1.5:** Wie sind die Aufzeichnungspflichten zu erfüllen?
- **Schritt 4.1.6:** Wie sind die Transparenzpflichten zu erfüllen?
- **Schritt 4.1.7:** Wie ist die menschliche Aufsicht zu gestalten?
- **Schritt 4.1.8:** Wie sind Genauigkeit, Robustheit und Cybersicherheit auszugestalten?
- **Schritt 4.1.9:** Wie ist das Qualitätsmanagement zu gestalten?
- **Schritt 4.1.10:** Wie ist die Dokumentation aufzubewahren?
- **Schritt 4.1.11:** Wie sind die automatisch erzeugten Protokolle aufzubewahren?
- **Schritt 4.1.12:** Welche Korrekturmaßnahmen und Informationspflichten obliegen dem Anbieter?
- **Schritt 4.1.13:** Wie gestaltet sich die Zusammenarbeit mit Behörden?
- **Schritt 4.2:** Welche Pflichten muss ich als Betreiber eines Hochrisiko-KI-Systems erfüllen?

- **Schritt 4.2.1:** Wann muss ich Anbieterpflichten erfüllen?
- **Schritt 4.2.2:** Welche spezifischen Betreiberpflichten sieht Art. 26 KI-VO vor?
- **Schritt 4.2.3:** Betreiberpflicht zur Grundrechte-Folgenabschätzung nach Art. 27 KI-VO
- **Schritt 4.2.4:** Transparenzpflichten des Betreibers (Art. 50 Abs. 3 und 4 KI-VO)
- **Schritt 5.1:** Wie baue ich KI-Kompetenz auf?
- **Schritt 5.2:** Wie gewährleiste ich Transparenz für bestimmte KI-Systeme?
- **Schritt 6.1:** Gibt es harmonisierte Normen oder gemeinsame Spezifikationen, die die Anforderungen aus Kapitel III Abschnitt 2 KI-VO abdecken?
- **Schritt 6.2:** Durchführung des erforderlichen Konformitätsbewertungsverfahrens
- **Schritt 6.3:** Was ist nach dem Konformitätsbewertungsverfahren zu tun?
- **Schritt 6.4:** Vorgehen bei wesentlichen Änderungen
- **Schritt 7:** Welche Pflichten sind nach dem Inverkehrbringen zu erfüllen?
- **Schritt 7.1:** Allgemeine Pflichten der Anbieter (Art. 16 KI-VO)
- **Schritt 7.2:** Die Pflichten nach Art. 72 und 73 KI-VO

Die EU-Kommission stellt online unter ihrem „AI Act Service Desk" unter anderem auch einen Bereich mit häufig gestellten Fragen (und Antworten) bereit. Diese FAQ-Sektion hat jüngst im April 2026 ein Update bekommen. Als Auszug daraus nachfolgend exemplarisch einige Fragen und Antworten (in eigener Übersetzung aus dem Englischen):

Frage: *„Was unterscheidet ein KI-Modell von einem KI-System? Werden Leitlinien herausgegeben?"*

„Die KI-Verordnung unterscheidet zwischen einem KI-System gemäß Art. 3 Nr. 1 KI-VO und einem universellen KI-Modell gemäß Art. 3 Nr. 63 KI-VO. Im Gesetz werden KI-Modelle als solche bezeichnet, die wesentliche Bestandteile von KI-Systemen sind. Sie stellen für sich genommen keine KI-Systeme dar. KI-Modelle erfordern die Hinzufügung weiterer Komponenten, wie beispielsweise einer Benutzeroberfläche, um zu KI-Systemen zu werden. KI-Modelle sind in der Regel in KI-Systeme integriert und bilden einen Teil davon (vgl. ErwGr 97 KI-VO). Große generative KI-Modelle sind ein typisches Beispiel für ein Allzweck-KI-Modell, da sie die flexible Generierung von Inhalten, beispielsweise in Form von Text, Audio, Bildern oder Videos, ermöglichen, die sich leicht an eine Vielzahl unterschiedlicher Aufgaben anpassen lassen (ErwGr 99 KI-VO). Die KI-Verordnung definiert ein KI-System als maschinenbasiertes System, das so konzipiert ist, dass es mit unterschiedlichen Autonomiegraden arbeitet und nach seiner Bereitstellung Anpassungsfähigkeit zeigen kann, und das für explizite oder implizite Ziele aus den

empfangenen Eingaben ableitet, wie Ausgabedaten wie Vorhersagen, Inhalte, Empfehlungen oder Entscheidungen zu generieren sind, die physische oder virtuelle Umgebungen beeinflussen können (Art. 3 Nr. 1, ErwGr 12 KI-VO). Weitere Informationen finden Sie in den Leitlinien zur Definition eines Systems der künstlichen Intelligenz."

Frage: *„Was bedeutet der ‚risikobasierte Ansatz'?"*

„Die KI-Verordnung folgt einem risikobasierten Ansatz und stuft KI-Systeme in vier verschiedene Risikokategorien ein: inakzeptables Risiko, hohes Risiko, Transparenzrisiko sowie minimales bis kein Risiko. Für die Kategorie unzumutbares Risiko führt die KI-Verordnung konkrete Praktiken auf, die verboten sind (Art. 5 KI-VO). Die KI-Systeme mit hohem Risiko werden gemäß Art. 6 KI-VO in Verbindung mit Anhang I (Liste der Harmonisierungsrechtsvorschriften der Union) und Anhang III KI-VO definiert. Anhang III umfasst acht Bereiche, in denen der Einsatz von KI besonders sensibel sein kann, und listet für jeden Bereich konkrete Anwendungsfälle auf, die nach Einschätzung des Gesetzgebers erhebliche Risiken für Gesundheit, Sicherheit und Grundrechte darstellen. Für bestimmte KI-Systeme, bei denen Transparenz besonders wichtig ist, sind Transparenzvorschriften vorgesehen. Alle anderen KI-Systeme gelten als KI-Systeme mit minimalem bis keinem Risiko, und die KI-Verordnung sieht für sie keine Verpflichtungen vor. Auf freiwilliger Basis können sich die Anbieter dieser Systeme dafür entscheiden, die Anforderungen an vertrauenswürdige KI anzuwenden und freiwillige Verhaltenskodizes einzuhalten."

Frage: *„Ist die Erkennung von Emotionen am Arbeitsplatz oder im Bildungsbereich bzw. für diese Zwecke (z. B. Mitarbeiterüberwachung) verboten?"*

„Das Inverkehrbringen, die Inbetriebnahme zu diesem spezifischen Zweck oder die Nutzung von KI-Systemen zur Erkennung von Emotionen natürlicher Personen am Arbeitsplatz und in Bildungseinrichtungen ist verboten. Dieses Verbot gilt jedoch nicht für die Nutzung eines KI-Systems, wenn dieses aus medizinischen oder sicherheitstechnischen Gründen eingeführt oder in Verkehr gebracht werden soll."

Frage: *„Gelten Standortdaten im Sinne des KI-Gesetzes als biometrische Daten?"*

„Standortdaten sind in der Regel keine biometrischen Daten. Dementsprechend fallen sie weder unter die in Anhang III Nr. 1 KI-VO aufgeführten Anwendungsfälle mit hohem Risiko noch unter die in Art. 5 Abs. 1 lit. g) KI-VO genannten verbotenen Praktiken."

Frage: *„Ist jede größere Veröffentlichung eines KI-Modells auch ein neues Modell im Sinne des KI-Gesetzes?"*

„Die Europäische Kommission betrachtet jede spätere Weiterentwicklung des KI-Modells nach dessen umfangreichem Vortrainingslauf als Teil desselben Modelllebenszyklus und somit als Teil desselben Modells, sofern diese vom selben Anbieter oder im Auftrag desselben Anbieters durchgeführt wird. Andere Überlegungen gelten, wenn ein anderer Akteur das Modell modifiziert. Dieses Verständnis eines Modells wurde von der Europäischen Kommission nach sorgfältiger Abwägung gewählt. In der modernen KI-Entwicklung ist es üblich, nach der Markteinführung kleine, iterative Änderungen an KI-Modellen vorzunehmen. Anbieter führen zudem häufig umfangreichere Nachtrainings an ihren bereits auf dem Markt befindlichen Modellen durch, und das daraus resultierende geänderte Modell wird unter einem neuen Namen vermarktet, was umgangssprachlich als „neues Modell" bezeichnet wird. Da sich unser Verständnis der Technologie noch weiterentwickelt, ist es derzeit schwierig, eine klare Grenze zu ziehen, was als relevante oder irrelevante Änderung gilt, um nachfolgende Modellversionen als eigenständige Modelle abzugrenzen. Daher betrachtet die Europäische Kommission derzeit aus Gründen der Rechtssicherheit jede Modellversion, die auf demselben umfangreichen Vortrainingslauf desselben Anbieters basiert, als dasselbe Modell. Folglich ist nicht jede von Anbietern als solche bezeichnete Version im Sinne des KI-Gesetzes zwangsläufig ein neues Modell, wenn man der Auslegung in den Leitlinien folgt. Um festzustellen, ob eine Version ein neues KI-Modell darstellt, sind möglicherweise nicht öffentliche technische Details zum Trainingsprozess erforderlich. Da KI-Modelle, die vor dem 2. August 2025 in Verkehr gebracht wurden, erst ab dem 2. August 2027 den Anforderungen der KI-Verordnung entsprechen müssen (Art. 111 Abs. 3 KI-VO), ist es möglich, dass diese Übergangsfrist auch für eine jetzt stattfindende Veröffentlichung gilt."

Frage: *„Wie gilt das KI-Gesetz für als Open Source veröffentlichte KI-Modelle für allgemeine Zwecke?"*

„Anbieter von als Open Source veröffentlichten KI-Modellen für allgemeine Zwecke können von bestimmten Verpflichtungen befreit sein (Art. 53 Abs. 2, Art. 54 Abs. 6 KI-VO), insbesondere …

- die Verpflichtung, technische Unterlagen für Behörden bereitzuhalten;
- die Verpflichtung, Dokumentation für nachgelagerte KI-Systemanbieter bereitzustellen;
- die Verpflichtung zur Benennung eines Bevollmächtigten (für Anbieter aus Nicht-EU-Ländern). Diese Ausnahmen setzen voraus, dass das Allzweck-KI-Modell …

- unter einer freien und quelloffenen Lizenz veröffentlicht wird, die den Zugriff, die Nutzung, die Änderung und die Verbreitung ohne Monetarisierung erlaubt;
- dessen Parameter, einschließlich Gewichte, Architektur und Nutzungsinformationen, öffentlich zugänglich sind;
- kein Allzweck-KI-Modell mit systemischem Risiko ist – Anbieter von Allzweck-KI-Modellen mit systemischem Risiko müssen alle Verpflichtungen für Anbieter von Allzweck-KI-Modellen erfüllen, unabhängig davon, ob das Modell als Open Source veröffentlicht wird.

Diese Ausnahmen tragen der Tatsache Rechnung, dass Open-Source-KI-Modelle zu Forschung und Innovation beitragen und durch ihren offenen Charakter bereits Transparenz bieten. Dennoch sind Anbieter, deren KI-Modelle die oben genannten Open-Source-Anforderungen erfüllen, nicht von der Verpflichtung zur Einhaltung der Urheberrechtsrichtlinie oder von der Verpflichtung zur Veröffentlichung einer Zusammenfassung der Trainingsdaten (Art. 53 Abs. 1 lit. c) und d) KI-VO) befreit, da ihr Open-Source-Charakter nicht zwangsläufig Informationen über die für das Training oder die Modifizierung des Modells verwendeten Daten oder darüber liefert, wie die Einhaltung des Urheberrechts sichergestellt wurde."

Frage: *„Welche Pflichten hat der Anbieter, wenn sich ein schwerwiegender Vorfall im Zusammenhang mit seinem Modell ereignet?"*

„Anbieter von Allzweck-KI-Modellen mit systemischem Risiko müssen relevante Informationen über schwerwiegende Vorfälle und mögliche Abhilfemaßnahmen zu deren Behebung unverzüglich erfassen, dokumentieren und dem KI-Büro sowie ggf. den zuständigen nationalen Behörden melden (Art. 55 Abs. 1 lit. c) KI-VO). Die Europäische Kommission ist der Ansicht, dass diese Verpflichtung schwerwiegende Cybersicherheitsverletzungen im Zusammenhang mit dem KI-Modell oder seiner physischen Infrastruktur umfasst, einschließlich der (Selbst-)Exfiltration von Modellparametern und Cyberangriffen, aufgrund ihrer möglichen Auswirkungen auf die in Art. 55 Abs. 1 lit. b) und d) KI-VO vorgesehenen Verpflichtungen. Darüber hinaus betrachtet die Europäische Kommission im Zusammenhang mit Kapitel V KI-VO als „schwerwiegenden Vorfall" jeden Vorfall oder jede Fehlfunktion eines Allzweck-KI-Modells, der bzw. die direkt oder indirekt zu einem der in der entsprechenden Definition für KI-Systeme in Art. 3 Nr. 49 lit. a) bis d) KI-VO aufgeführten Ereignisse führt. Das Kapitel „Sicherheit" des Verhaltenskodex für Allzweck-KI bietet durch seine Verpflichtung Nr. 9 ein Mittel, um die Einhaltung dieser Verpflichtung nachzuweisen."

ALLGEMEINES PERSÖNLICHKEITSRECHT

Das allgemeine Persönlichkeitsrecht (APR) stellt eine verfassungsrechtlich geschützte Position dar, eine Gesamtheit aus verschiedenen Einzelrechten, das sich aus Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 Grundgesetz (GG) herleitet. Art. 1 Abs. 1 GG zählt zu den bekanntesten Grundrechten und lautet wie folgt:

„Die Würde des Menschen ist unantastbar. Sie zu achten und zu schützen ist Verpflichtung aller staatlichen Gewalt."

Hinweis:
Art. 1 Abs. 1 GG ist nicht nur ein Grundrecht, sondern durchzieht als objektive Wertentscheidung die gesamte Rechtsordnung.

Die Regelung in Art. 2 Abs. 1 GG ist nicht minder wichtig

„Jeder hat das Recht auf die freie Entfaltung seiner Persönlichkeit, soweit er nicht die Rechte anderer verletzt und nicht gegen die verfassungsmäßige Ordnung oder das Sittengesetz verstößt."

Aus der Zusammenschau beider Normen folgt das allgemeine Persönlichkeitsrecht, dessen Schutz im Allgemeinen und dessen einzelne Bestandteile im Besonderen regelmäßig durch das Bundesverfassungsgericht gestärkt und ausgeformt werden. Es schützt die individuelle Entfaltung, Integrität und Selbstbestimmung einer Person. Das APR wirkt gegen staatliche Eingriffe (Schranken durch Grundrechte) und gegen private Beeinträchtigungen (als sogenannte Drittwirkung).

Das APR soll Lücken schließen und bereits existierende sowie noch unbenannte Freiheitsrechte ergänzen. Dadurch bietet es grundsätzlich Schutz gegen Einschränkungen der persönlichen Entfaltung. Es umfasst beispielsweise das Recht auf informationelle Selbstbestimmung, das Recht an der eigenen Ehre, das Recht am eigenen Namen, das Recht am eigenen Bild oder auch das Recht an der eigenen Stimme. So ist etwa das Recht auf informationelle Selbstbestimmung durch das Bundesverfassungsgericht in dessen „Volkszählungsurteil" aus dem Jahre 1983 entwickelt worden und bildet seitdem die Basis für unser Verständnis des Datenschutzrechts.

Im Zusammenhang mit der Nutzung von KI-Tools sind insbesondere das Recht am eigenen Bild und das Recht an der eigenen Stimme relevant. Das erstge-

nannte wird durch ein Spezialgesetz geschützt (Kunsturhebergesetz, KUG), für das zweitgenannte existieren nur eine Handvoll gerichtlicher Entscheidungen (die sogenannten „Marlene-Dietrich-, die „Heinz-Erhardt- oder auch die „Manfred-Lehmann/Bruce-Willis-Entscheidung").

Hinweis:
Auch ein postmortales Persönlichkeitsrecht besteht, z. B. in Bezug auf das Recht am eigenen Bild nach Maßgabe von § 22 S. 3 KUG.

In Deutschland ist das Recht am eigenen Bild im KUG verankert. Es schützt natürliche Personen davor, dass ihr „Bildnis" (im Wesentlichen Foto- oder Videoaufnahmen) ohne ihre Zustimmung oder ohne eine vertragliche Vereinbarung verwendet wird (§ 22 KUG), beispielsweise durch Veröffentlichung oder durch Bearbeitung mittels KI. Die Regelung des § 23 KUG (z. B. Aufnahmen von Personen der Zeitgeschichte oder von öffentlichen Versammlungen) beschreibt Konstellationen, in denen ausnahmsweise keine Zustimmung benötigt wird; diese werden jedoch eng ausgelegt. Mithilfe von KI erzeugte Deepfake-Bilder oder -Videos von realen Menschen berühren deren Recht am eigenen Bild. Ebenso können KI-Systeme, die Gesichtsbilder erkennen oder generieren, problematisch sein, wenn sie gegen diese Regeln verstoßen.

Eine Person hat ebenfalls das Recht an der eigenen Stimme. Diesbezüglich existiert zwar kein Spezialgesetz, wie z. B. das KUG für das Recht am eigenen Bild, aber es ist ein anerkannter Teil des allgemeinen Persönlichkeitsrechts. Dies haben auch schon diverse Gerichte entschieden:

- Oberlandesgericht Hamburg, Beschluss vom 08.05.1989, Az. 3 W 45/89 („Heinz-Erhardt-Entscheidung"):

„Das fortwirkende Persönlichkeitsrecht eines durch sprachliche Darstellung in Wort und Stimmklang bundesweit bekannt gewordenen Schauspielers umfasst auch das Recht, einer Verwendung dieser künstlerischen Eigenart in der Werbung mit Hilfe eines Sprachimitators entgegenzutreten."

- Bundesgerichtshof, Urteil vom 01.12.1999, Az. I ZR 49/97 („Marlene-Dietrich-Entscheidung"):

„Darüber hinaus schützen das allgemeine Persönlichkeitsrecht und seine besonderen Ausprägungen aber auch vermögenswerte Interessen der Person. Der Abbildung, dem Namen sowie sonstigen Merkmalen der Persönlichkeit wie etwa der Stimme kann ein beträchtlicher wirtschaftlicher Wert zukommen, der im allgemeinen auf der

Bekanntheit und dem Ansehen der Person in der Öffentlichkeit – meist durch besondere Leistungen etwa auf sportlichem oder künstlerischem Gebiet erworben – beruht."

- Landgericht Berlin, Urteil vom 20.08.2025, Az. 2 O 202/24 („Manfred-Lehmann/Bruce-Willis-Entscheidung"):

„In Rechtsprechung und Literatur ist anerkannt, dass das allgemeine Persönlichkeitsrecht auch das Recht an der eigenen Stimme umfasst, auch wenn es – anders als der Bildnisschutz gemäß §§ 22 ff. KUG – spezialgesetzlich nicht geregelt ist. Die Intensität der Persönlichkeitsrechtsbeeinträchtigung steht der durch Bild und Namensverwendung bei der Verwendung einer bekannten Stimme zu Werbezwecken in nichts nach […]."

Speziell mit generativer KI können Stimmen synthetisiert bzw. geklont werden. Auch die Möglichkeiten zur Manipulation von Bildmaterial sind speziell durch generative KI einfacher und schneller geworden. In Deutschland wird aktuell diskutiert, ob und wie unautorisiertes Kopieren der Stimme oder auch des Bildnisses eines Menschen reguliert werden kann. So existiert seit August 2025 der Entwurf einer neuen Vorschrift im Strafgesetzbuch. Der Entwurf des Gesetzestextes des neu geplanten § 201b Strafgesetzbuch (StGB) lautet:

„§ 201b Verletzung von Persönlichkeitsrechten durch digitale Fälschung

(1) Wer das Persönlichkeitsrecht einer anderen Person verletzt, indem er einen mit computertechnischen Mitteln hergestellten oder veränderten Medieninhalt, der den Anschein einer wirklichkeitsgetreuen Bild- oder Tonaufnahme des äußeren Erscheinungsbildes, des Verhaltens oder mündlicher Äußerungen dieser Person erweckt, einer dritten Person zugänglich macht, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft. Gleiches gilt, wenn sich die Tat nach Satz 1 auf eine verstorbene Person bezieht und deren Persönlichkeitsrecht dadurch schwerwiegend verletzt wird.

(2) Wer in den Fällen des Absatzes 1 Satz 1 den Medieninhalt der Öffentlichkeit zugänglich macht oder einen Medieninhalt zugänglich macht, der einen Vorgang des höchstpersönlichen Lebensbereichs zum Gegenstand hat, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft.

(3) Absatz 1 Satz 1, auch in Verbindung mit Absatz 2, gilt nicht für Handlungen, die in Wahrnehmung überwiegender berechtigter Interessen erfolgen, namentlich der Kunst oder der Wissenschaft, der Forschung oder der Lehre, der Berichterstattung über Vorgänge des Zeitgeschehens oder der Geschichte oder ähnlichen Zwecken dienen.

(4) Die Bild- oder Tonträger oder andere technische Mittel, die der Täter oder Teilnehmer verwendet hat, können eingezogen werden. § 74a ist anzuwenden."

Zielrichtung dieses Gesetzesvorhabens ist also einzig die Bestrafung der Zugänglichmachung von Deepfakes und der damit einhergehenden Persönlichkeitsrechtsverletzung. Straflos wäre hiernach folglich die Anfertigung derartiger Inhalte.

Ebenfalls geplant ist eine Änderung der Vorschrift § 184k StGB (Verletzung des Intimbereichs durch Bildaufnahmen). Nach aktuellem Gesetzesentwurf vom 24.03.2026 soll diese Norm zukünftig wie folgt geändert werden:

§ 184k StGB (aktuell)	**§ 184k StGB (Entwurf März 2026)**
(1) Mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe wird bestraft, wer *1. absichtlich oder wissentlich von den Genitalien, dem Gesäß, der weiblichen Brust oder der diese Körperteile bedeckenden Unterwäsche einer anderen Person unbefugt eine Bildaufnahme herstellt oder überträgt, soweit diese Bereiche gegen Anblick geschützt sind,* *2. eine durch eine Tat nach Nummer 1 hergestellte Bildaufnahme gebraucht oder einer dritten Person zugänglich macht oder* *3. eine befugt hergestellte Bildaufnahme der in der Nummer 1 bezeichneten Art wissentlich unbefugt einer dritten Person zugänglich macht.*	*(1) Mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe wird bestraft, wer* *1. eine Bildaufnahme, die eine andere Person sexualbezogen abbildet, absichtlich oder wissentlich unbefugt herstellt oder überträgt,* *2. eine durch eine Tat nach Nummer 1 hergestellte Bildaufnahme gebraucht oder einer dritten Person zugänglich macht oder* *3. eine befugt hergestellte Bildaufnahme, der in der Nummer 1 bezeichneten Art, unbefugt einer dritten Person zugänglich macht.*
	(2) Ebenso wird bestraft, wer eine Bildaufnahme einer anderen Person unbefugt mit technischen Mitteln derart verändert, dass die Person sexualbezogen abgebildet wird, und das veränderte Bild einer dritten Person zugänglich macht.
(2) Die Tat wird nur auf Antrag verfolgt, es sei denn, dass die Strafverfolgungsbehörde wegen des besonderen öffentlichen Interesses an der Strafverfolgung ein Einschreiten von Amts wegen für geboten hält.	*(3) Die Tat wird nur auf Antrag verfolgt, es sei denn, dass die Strafverfolgungsbehörde wegen des besonderen öffentlichen Interesses an der Strafverfolgung ein Einschreiten von Amts wegen für geboten hält.*

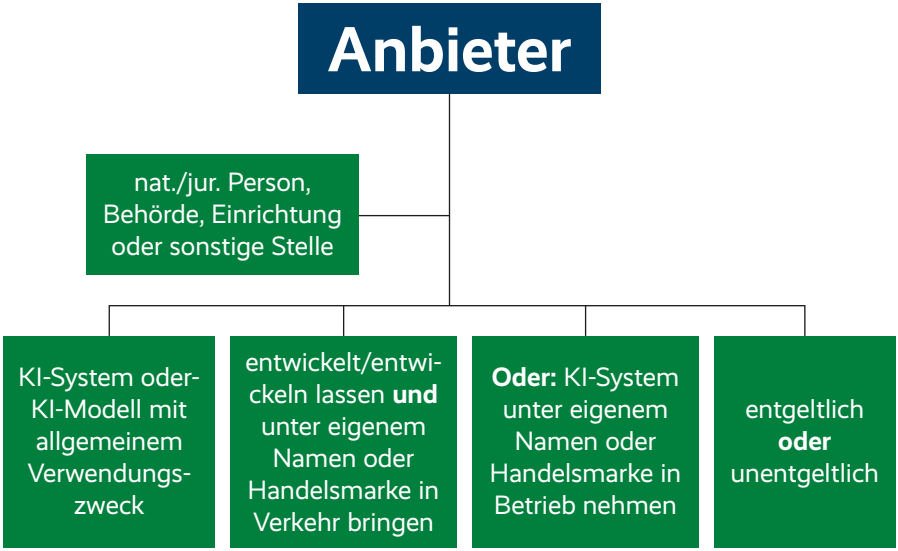
§ 184k StGB (aktuell)	§ 184k StGB (Entwurf März 2026)
(3) Absatz 1 gilt nicht für Handlungen, die in Wahrnehmung überwiegender berechtigter Interessen erfolgen, namentlich der Kunst oder der Wissenschaft, der Forschung oder der Lehre, der Berichterstattung über Vorgänge des Zeitgeschehens oder der Geschichte oder ähnlichen Zwecken dienen.	*(4) Absätze 1 und 2 gelten nicht für Handlungen, die in Wahrnehmung überwiegender berechtigter Interessen erfolgen, namentlich der Kunst oder der Wissenschaft, der Forschung oder der Lehre, der Berichterstattung über Vorgänge des Zeitgeschehens oder der Geschichte oder ähnlichen Zwecken dienen.*
(4) Die Bildträger sowie Bildaufnahmegeräte oder andere technische Mittel, die der Täter oder Teilnehmer verwendet hat, können eingezogen werden. § 74a ist anzuwenden.	*(5) Die Bildträger sowie Bildaufnahmegeräte oder andere technische Mittel, die der Täter oder Teilnehmer verwendet hat, können eingezogen werden. § 74a ist anzuwenden.*
	(6) In besonders schweren Fällen ist die Freiheitstrafe von drei Monaten bis zu drei Jahren. Ein besonders schwerer Fall liegt in der Regel vor, wenn *1. der Täter seine Befugnisse oder Stellung als Amtsträger ausnutzt,* *2. zwischen dem Täter und dem Opfer ein Beratungs-, Behandlungs- oder Betreuungsverhältnis wegen einer geistigen oder seelischen Krankheit oder Behinderung einschließlich einer Suchtkrankheit oder wegen einer körperlichen Krankheit oder Behinderung besteht oder ein Ausbildungs-, Dienst- oder Arbeitsverhältnis besteht, in dem das Opfer untergeordnet ist.*

Hinweis:
Sowohl das Bildnis als auch die Stimme einer Person können personenbezogene Daten im Sinne von Art. 4 Nr. 1 Datenschutzgrundverordnung darstellen, sodass dann parallel zum APR auch das Datenschutzrecht heranzuziehen ist.

ANBIETER

Gemäß Art. 3 Nr. 3 KI-Verordnung (KI-VO) wird der Begriff „Anbieter“ wie folgt definiert:

„eine natürliche oder juristische Person, Behörde, Einrichtung oder sonstige Stelle, die ein KI-System oder ein KI-Modell mit allgemeinem Verwendungszweck entwickelt oder entwickeln lässt und es unter ihrem eigenen Namen oder ihrer Handelsmarke in Verkehr bringt oder das KI-System unter ihrem eigenen Namen oder ihrer Handelsmarke in Betrieb nimmt, sei es entgeltlich oder unentgeltlich“



Prüfungsschema „Anbieter“

„Inverkehrbringen“ meint die erstmalige Bereitstellung eines KI-Systems oder eines KI-Modells mit allgemeinem Verwendungszweck auf dem Unionsmarkt (Art. 4 Nr. 9 KI-VO). Die „Bereitstellung auf dem Markt“ wird definiert als entgeltliche oder unentgeltliche Abgabe eines KI-Systems oder eines KI-Modells mit allgemeinem Verwendungszweck zum Vertrieb oder zur Verwendung auf dem Unionsmarkt im Rahmen einer Geschäftstätigkeit (Art. 4 Nr. 10 KI-VO). Unter „Inbetriebnahme“ soll hingegen die Bereitstellung eines KI-Systems in der Union zum Erstgebrauch direkt an den Betreiber oder zum Eigengebrauch entsprechend seiner Zweckbestimmung verstanden werden (Art. 4 Nr. 11 KI-VO). Nach Art. 4 Nr. 12 KI-VO ist die „Zweckbestimmung“ die Verwendung, für die ein KI-System laut Anbieter

bestimmt ist, einschließlich der besonderen Umstände und Bedingungen für die Verwendung, entsprechend den vom Anbieter bereitgestellten Informationen in den Betriebsanleitungen, im Werbe- oder Verkaufsmaterial und in diesbezüglichen Erklärungen sowie in der technischen Dokumentation.

Somit entspricht der Begriff „Anbieter" in der Regel einem Hersteller, Entwickler oder Produktanbieter. Maßgeblich ist, wer das KI-Modell mit allgemeinem Verwendungszweck respektive das KI-System technisch gestaltet (oder durch beauftragte Dritte gestalten lässt) und mit eigenem Branding herausgibt. Das Gleiche gilt für denjenigen, der ein KI-System „unter eigener Flagge" selber nutzt oder Dritten zur Nutzung bereitstellt. Auf dem Anbieter lasten folglich auch die Primärpflichten nach Maßgabe der KI-VO (z. B. Risikomanagement, Konformitätsbewertung, technische Dokumentation, CE-Kennzeichnung).

ANGEMESSENHEITSBESCHLUSS

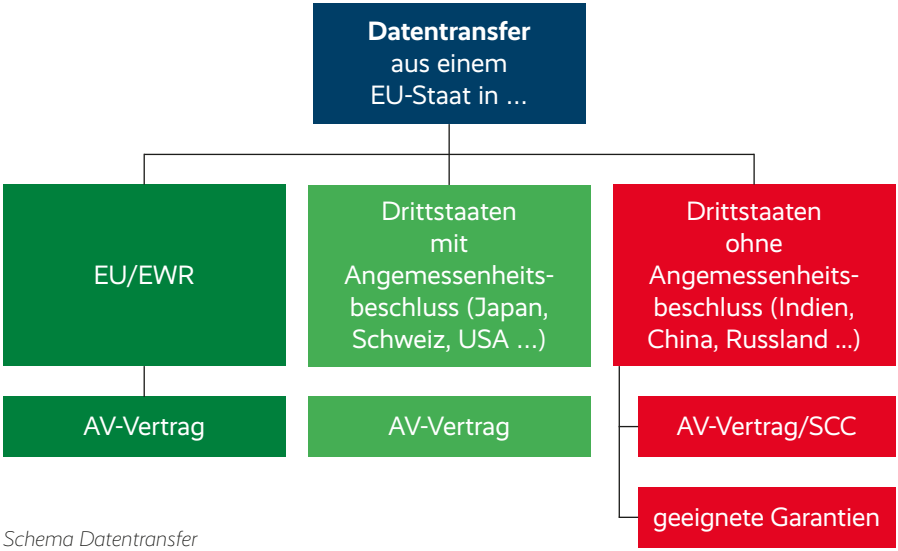
Wenn personenbezogene Daten auf Dritte übertragen werden sollen, dann muss dies legitimiert werden, und zugleich muss am Ort des Empfängers ein im Vergleich zur EU angemessenes Datenschutzniveau vorliegen. Bei Datentransfers innerhalb der EU bzw. des Europäischen Wirtschaftsraums (EWR) gilt die Datenschutzgrundverordnung (DSGVO), sodass in diesen Fällen von einem einheitlichen Datenschutzniveau ausgegangen wird.

Hinweis:
Der EWR umfasst neben den 27 EU-Mitgliedstaaten (Belgien, Bulgarien, Dänemark, Deutschland, Estland, Finnland, Frankreich, Griechenland, Irland, Italien, Kroatien, Lettland, Litauen, Luxemburg, Malta, Niederlande, Österreich, Polen, Portugal, Rumänien, Schweden, Slowakei, Slowenien, Spanien, Tschechien, Ungarn, Zypern) auch noch Island, Liechtenstein und Norwegen.

Fraglich ist, wie es beim Transfer von personenbezogenen Daten in Nicht-EU-Staaten (sogenannte „Drittstaaten") aussieht. Hierbei ist zwischen sicheren und unsicheren Drittstaaten zu unterscheiden. Denn für manche außereuropäische Länder gilt ein Angemessenheitsbeschluss, für andere wiederum nicht. Dabei handelt es sich um eine Entscheidung der EU-Kommission nach Art. 45 DSGVO, wonach der Drittstaat ein nach EU-Maßstäben ebenfalls angemessenes Datenschutzniveau bietet. Für die folgenden Staaten existiert (Stand April 2026) ein Angemessenheitsbeschluss:

- Andorra
- Argentinien
- Kanada
- Schweiz
- Färöer-Inseln
- Guernsey
- Israel
- Isle of Man
- Jersey
- Neuseeland
- Uruguay
- Japan
- Republik Korea
- Vereinigtes Königreich
- USA

Hinweis:
Der Angemessenheitsbeschluss zwischen der EU und den USA hat zwar derzeit noch Bestand. Allerdings werden unter der aktuellen Administration immer mehr der Voraussetzungen entfernt oder „ausgehöhlt", die geschaffen wurden, damit dieser Angemessenheitsbeschluss überhaupt ergehen konnte. Es ist daher nicht ausgeschlossen, dass der Europäische Gerichtshof (EuGH) auf einen entsprechenden Antrag hin zu entscheiden haben wird, ob der EU-USA-Angemessenheitsbeschluss weiterhin bestehen bleiben kann. Falls der EuGH ihn für unwirksam erklären sollte, dann entfiele damit eine wichtige Voraussetzung für den Transfer personenbezogener Daten in die USA. Und dies ist in den letzten Jahren bereits zweimal passiert, zuletzt Mitte 2020. Jeder, der Daten in die USA übermittelt, sollte hier auf dem Laufenden bleiben und sich auf den „Worst Case" vorbereiten, um ggf. alternative Angebote aus der EU nutzen zu können.



Schema Datentransfer

Alle anderen Nicht-EU-Staaten gelten somit als unsichere Drittstaaten. Sollen personenbezogene Daten aus der EU in solche unsicheren Drittstaaten übermittelt werden, muss ein spezieller Vertrag geschlossen werden, insbesondere in Form der sogenannten EU-Standardvertragsklauseln (engl.: Standard Contractual Clauses, SCC). Zusätzlich zu diesen vertraglichen müssen noch weitere geeignete Garantien vorliegen (technisch oder organisatorisch), die auch ohne einen Angemessenheitsbeschluss ein akzeptables Datenschutzniveau gewährleisten.

Liegt jedoch ein Angemessenheitsbeschluss vor, dürfen personenbezogene Daten ohne zusätzliche Schutzgarantien übermittelt werden. In solchen Fällen wird der Datentransfer ins Nicht-EU-Ausland so behandelt wie ein innereuropäischer.

ART.-9-DATEN

„Art.-9-Daten" bezeichnen besondere Kategorien personenbezogener Daten im Sinne von Art. 9 Datenschutzgrundverordnung (DSGVO). In dieser Vorschrift listet das Gesetz die als besonders sensibel eingestuften Datenkategorien auf:

- rassische/ethnische Herkunft
- politische Meinungen
- religiöse/weltanschauliche Überzeugungen
- Gewerkschaftszugehörigkeit
- genetische/biometrische Daten
- Gesundheitsdaten
- Daten über Sexualleben/sexuelle Orientierung

Ihre Verarbeitung ist grundsätzlich verboten, es sei denn, es greift eine enge Ausnahme wie etwa eine ausdrückliche Einwilligung, lebenswichtige Interessen, im Gesundheits- oder Arbeitsrecht vorgesehene Regelungen etc. (vgl. Art. 9 Abs. 2 DSGVO). Der Schutz ist sehr streng, da bei Missbrauch erhebliche Folgen für Betroffene drohen. Daher müssen für die Verarbeitung von Art.-9-Daten im Vergleich zu „normalen" personenbezogenen Daten, wie etwa Name, Anschrift oder Telefonnummer, erhöhte Schutzmaßnahmen gewährleistet werden.

Hinweis:
Aber auch im Zusammenhang mit der Verarbeitung „normaler" personenbezogener Daten, wie etwa dem Namen, der E-Mail-Adresse oder dem Geburtsdatum, kann sich ein erhöhter Schutzbedarf aufgrund eines erhöhten Risikos ergeben. Dies hängt regelmäßig vom jeweiligen Kontext ab. So ist z. B. eine Liste mit Namen und Telefonnummern von Pressevertretern in aller Regel eher als „harmlos" einzustufen. Hingegen dürfte der Liste mit Namen und Telefonnummern von Menschen im Zeugenschutzprogramm ein deutliches höheres Risiko immanent sein. Finanzdaten etwa fallen nicht unter Art. 9 Abs. 1 DSGVO, sind regelmäßig aber sehr sensibel und damit in besonderem Maße schützenswert.

Insgesamt ist die Bestimmung, ob ein Art.-9-Datum vorliegt, in der Praxis bisweilen nur schwer vorzunehmen, da die Einstufung auch vom Kontext abhängen kann. Insofern ist auch bei „normalen" personenbezogenen Daten stets auf Basis eines risikobasierten Ansatzes vorzugehen.

AUTOMATISIERTE ENTSCHEIDUNG

Der Begriff der automatisierten Entscheidung beschreibt den Einsatz von Algorithmen und KI-Systemen zur Herbeiführung von Rechtsfolgen oder erheblichen Beeinträchtigungen ohne maßgebliche menschliche Intervention. Eine automatisierte Entscheidung ist daher eine Entscheidung, die vollständig durch ein technisches System auf Basis personenbezogener Daten getroffen wird, ohne dass eine natürliche Person den Entscheidungsvorgang noch sinnvoll prüft oder mitgestaltet. Typische Beispiele sind automatische Kreditentscheidungen, Bonitätscores, automatisierte Bewerbervorauswahl oder dynamische Preisgestaltung.

Nach Art. 22 Abs. 1 Datenschutzgrundverordnung (DSGVO) hat die betroffene Person grundsätzlich das Recht, nicht einer ausschließlich auf einer automatisierten Verarbeitung – einschließlich Profiling – beruhenden Entscheidung unterworfen zu werden, die ihr gegenüber rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt. In der datenschutzrechtlichen Dogmatik stellt Art. 22 Abs. 1 DSGVO ein grundsätzliches Verbot dar, Personen Entscheidungen zu unterwerfen, die ausschließlich auf einer automatisierten Verarbeitung beruhen. Die Relevanz dieser Norm hat durch die Rechtsprechung des Europäischen Gerichtshofs (EuGH), insbesondere im Kontext des Schufa-Scorings (Urteil vom 07.12.2023, Az. C-634/21), eine erhebliche Steigerung erfahren. Der EuGH stellte in seinem Urteil klar, dass

eine automatisierte Entscheidung bereits dann vorliegt, wenn ein automatisierter Score-Wert eine „bestimmende Rolle" für das spätere Handeln eines menschlichen Entscheidungsträgers spielt. Damit wird das Kriterium der „Ausschließlichkeit" faktisch auf Systeme ausgeweitet, bei denen der Mensch nur noch formal eine Entscheidung bestätigt, ohne diese inhaltlich zu prüfen. Die Zulässigkeit solcher Systeme ist an strikte Ausnahmen gebunden: die vertragliche Notwendigkeit, eine ausdrückliche Einwilligung oder eine spezifische gesetzliche Ermächtigung. Aber auch in diesen Fällen müssen Verantwortliche angemessene Schutzmaßnahmen ergreifen, wozu das Recht auf menschliches Eingreifen, die Darlegung des eigenen Standpunkts und die Anfechtung der Entscheidung gehören.

Dieses Schutzkonzept wird durch Art. 86 KI-Verordnung (KI-VO) erweitert, der ein spezifisches Recht auf Erläuterung für Entscheidungen einführt, die auf Ausgaben von Hochrisiko-KI-Systemen basieren. Im Gegensatz zu Art. 22 DSGVO ist Art. 86 KI-VO weiter gefasst, da er auch solche Entscheidungen betrifft, die nur „auf der Grundlage" der KI-Ausgabe getroffen wurden, was menschliche Zwischenschritte explizit miteinschließt.

BEREITSTELLUNG AUF DEM MARKT

Der Begriff „Bereitstellung auf dem Markt" wird in Art. 3 Nr. 10 KI-VO wie folgt definiert:

„entgeltliche oder unentgeltliche Abgabe eines KI-Systems oder eines KI-Modells mit allgemeinem Verwendungszweck zum Vertrieb oder zur Verwendung auf dem Unionsmarkt im Rahmen einer Geschäftstätigkeit"

Dies bedeutet, ein KI-Modell mit allgemeinem Verwendungszweck oder ein KI-System zum Vertrieb oder zur Nutzung bereitzustellen. Wenn also etwa ein KI-System in der EU erstmals angeboten oder verkauft wird, gilt dies als Bereitstellung.

BESONDERE KATEGORIEN PERSONENBEZOGENER DATEN

Das Datenschutzrecht unterscheidet zwischen „normalen" und besonderen Kategorien personenbezogener Daten. Zu den besonderen Kategorien zählen Daten

gemäß Art. 9, 10 Datenschutzgrundverordnung (DSGVO), also insbesondere Angaben über Gesundheit, Religion oder Gewerkschaftszugehörigkeit (Art. 9 DSGVO) oder auch Angaben über strafrechtliche Verurteilungen und Straftaten (Art. 10 DSGVO). Die Definition des Begriffs „besondere Kategorien personenbezogener Daten" in Art. 3 Nr. 37 KI-Verordnung verweist entsprechend auf Art. 9, 10 DSGVO.

BETREIBER

Der Begriff „Betreiber" wird in Art. 3 Nr. 4 KI-Verordnung (KI-VO) folgendermaßen definiert:

„eine natürliche oder juristische Person, Behörde, Einrichtung oder sonstige Stelle, die ein KI-System in eigener Verantwortung verwendet, es sei denn, das KI-System wird im Rahmen einer persönlichen und nicht beruflichen Tätigkeit verwendet"

Im Unterschied zum „Anbieter" geht es hier eher um Verwender von KI, also beispielsweise ein Unternehmen, das ein KI-Tool im betrieblichen Alltag einsetzt. KI-Nutzung im Rahmen einer ausschließlich persönlichen und nicht beruflichen Tätigkeit wird hier aufgrund der sogenannten Haushaltsausnahme in Art. 2 Abs. 10 KI-VO ausgenommen. Betreiber haben gegenüber KI-Nutzern, wie insbesondere ihren Beschäftigten, Rechenschaftspflichten und müssen gewährleisten, dass der Einsatz des KI-Systems sicher und gesetzeskonform erfolgt (unter anderem Schulung des Personals, Überwachung der Ergebnisse).

Eine Akteursrolle ist allerdings nicht „in Stein gemeißelt", so kann ein Akteur die Rolle wechseln oder auch eine Doppelrolle einnehmen. Wenn ein Unternehmen z. B. ein KI-System als sogenannte Whitelable-Lösung einkauft, dies also unter eigenem Namen weiter vertreiben darf, und es zugleich selbst nutzt, kommt eine Einstufung gleichsam als Anbieter und Betreiber in Betracht. Und im Fall von Hochrisiko-KI-Systemen können andere Akteure als Anbieter gelten, wenn sie beispielsweise eine wesentliche Änderung an einem Hochrisiko-KI-System vornehmen oder die Zweckbestimmung eines KI-Systems derart ändern, dass dies dadurch als hochriskant eingestuft werden muss (vgl. Art. 25 KI-VO).

Hinweis:
Unter einer „wesentlichen Veränderung" versteht Art. 3 Nr. 23 KI-VO eine Veränderung eines KI-Systems nach dessen Inverkehrbringen oder Inbetriebnahme, die in der vom Anbieter durchgeführten ursprünglichen Konformitätsbewertung

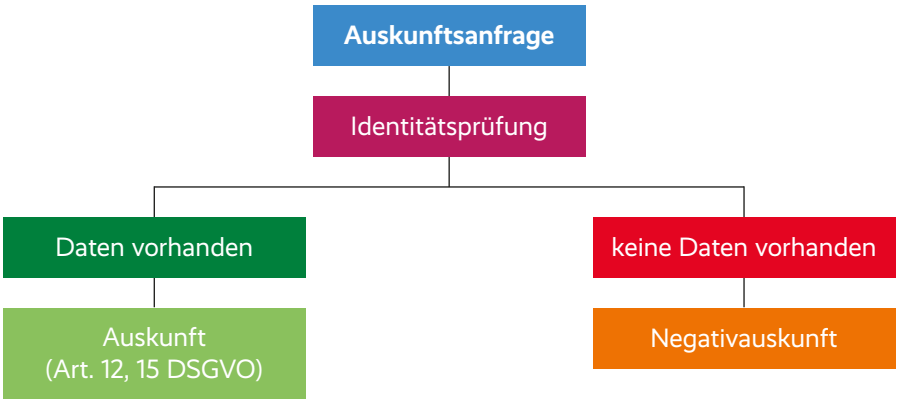
nicht vorgesehen oder geplant war und durch die die Konformität des KI-Systems mit den Anforderungen in Kapitel III Abschnitt 2 KI-VO beeinträchtigt wird oder die zu einer Änderung der Zweckbestimmung führt, für die das KI-System bewertet wurde.

BETROFFENENRECHTE

Betroffenenrechte sind die Rechte der von Datenverarbeitung Betroffenen nach der Datenschutzgrundverordnung (DSGVO). Sie erlauben es einer Person, Einfluss auf die Verarbeitung ihrer eigenen Daten zu nehmen.

Zu den Betroffenenrechten gemäß DSGVO zählen die folgenden:

- Recht auf Auskunft (Art. 15 DSGVO)
- Recht auf Berichtigung (Art. 16 DSGVO)
- Recht auf Löschung (Art. 17 DSGVO)
- Recht auf Einschränkung der Verarbeitung (Art. 18 DSGVO)
- Recht auf Datenübertragbarkeit (Art. 20 DSGVO)
- Recht auf Widerspruch (Art. 21 DSGVO)
- Recht, nicht einer automatisierten Entscheidung unterworfen zu sein (Art. 22 DSGVO)
- Recht auf Widerruf (Art. 7 Abs. 3 DSGVO)
- Recht auf Beschwerde (Art. 77 DSGVO)



Schema Datentransfer

Diese Rechte dienen der informationellen Selbstbestimmung als Ausdruck des allgemeinen Persönlichkeitsrechts. Die Verantwortlichen müssen diese Rechte aktiv ermöglichen und zeitnah umsetzen.

All diese Betroffenenrechte sind selbstverständlich auch im Zuge der Nutzung von personenbezogenen Daten im Rahmen von KI-Tools zu gewährleisten.

Hinweis:
Dem Recht auf Auskunft kommt in der Praxis eine besondere Bedeutung zu. Denn es dient sozusagen als „Ausgangspunkt" auch dazu, die Durchsetzung der anderen Betroffenenrechte vorzubereiten oder überhaupt erst möglich zu machen. Denn nur dann, wenn man weiß, wer welche Daten verarbeitet, kann man ggf. Ansprüche auf Löschung, Widerspruch etc. geltend machen.

BEVOLLMÄCHTIGTER

In Art. 3 Nr. 5 KI-Verordnung (KI-VO) wird der Begriff „Bevollmächtigter" wie folgt definiert:

„eine in der Union ansässige oder niedergelassene natürliche oder juristische Person, die vom Anbieter eines KI-Systems oder eines KI-Modells mit allgemeinem Verwendungszweck schriftlich dazu bevollmächtigt wurde und sich damit einverstanden erklärt hat, in seinem Namen die in dieser Verordnung festgelegten Pflichten zu erfüllen bzw. Verfahren durchzuführen"

Diese Rolle dient dazu, die Vorgaben der KI-VO gegenüber im Nicht-EU-Ausland ansässigen Akteuren durchzusetzen. Sie ist vergleichbar mit dem EU-Vertreter gemäß Art. 4 Nr. 17 Datenschutzgrundverordnung („eine in der Union niedergelassene natürliche oder juristische Person, die von dem Verantwortlichen oder Auftragsverarbeiter schriftlich gemäß Artikel 27 bestellt wurde und den Verantwortlichen oder Auftragsverarbeiter in Bezug auf die ihnen jeweils nach dieser Verordnung obliegenden Pflichten vertritt").

BIOMETRISCHE DATEN

Der Begriff „biometrische Daten" wird in Art. 4 Nr. 14 Datenschutzgrundverordnung (DSGVO) definiert:

„mit speziellen technischen Verfahren gewonnene personenbezogene Daten zu den physischen, physiologischen oder verhaltenstypischen Merkmalen einer natürlichen Person, die die eindeutige Identifizierung dieser natürlichen Person ermöglichen oder bestätigen, wie Gesichtsbilder oder daktyloskopische Daten"

Die Definition dieses Begriffs gemäß Art. 3 Nr. 34 KI-Verordnung (KI-VO) enthält den zentralen Teil der DSGVO-Definition:

„mit speziellen technischen Verfahren gewonnene personenbezogene Daten zu den physischen, physiologischen oder verhaltenstypischen Merkmalen einer natürlichen Person, wie etwa Gesichtsbilder oder daktyloskopische Daten"

Bei Lichte betrachtet stimmen die beiden Definitionen aus DSGVO und KI-VO in den wesentlichen Aspekten überein. Denn es geht z. B. um die speziell für den Personalausweis angefertigten Porträtaufnahmen, aber auch um Fingerabdrücke, Iris-Scans, Stimm- oder Gangprofile. Solche Daten fallen unter die besonderen Kategorien personenbezogener Daten (Art. 9 DSGVO) und sind damit besonders geschützt.

BIOMETRISCHE IDENTIFIZIERUNG

Der Begriff „biometrische Identifizierung" wird ebenfalls im Rahmen der diversen Definitionen der KI-Verordnung erläutert (Art. 3 Nr. 35 KI-VO):

„die automatisierte Erkennung physischer, physiologischer, verhaltensbezogener oder psychologischer menschlicher Merkmale zum Zwecke der Feststellung der Identität einer natürlichen Person durch den Vergleich biometrischer Daten dieser Person mit biometrischen Daten von Personen, die in einer Datenbank gespeichert sind"

Es geht hierbei also insbesondere um einen Personenabgleich gegen eine Datenbank.

Dies soll gemäß ErwGr 15 S. 2 KI-VO keine KI-Systeme umfassen, die bestimmungsgemäß für die biometrische Verifizierung (wozu die Authentifizierung gehört) verwendet werden sollen, deren einziger Zweck darin besteht zu bestätigen, dass eine bestimmte natürliche Person die Person ist, für die sie sich ausgibt, sowie zur Bestätigung der Identität einer natürlichen Person zu dem alleinigen Zweck, Zugang zu einem Dienst zu erhalten, ein Gerät zu entriegeln oder Sicherheitszugang zu Räumlichkeiten zu erhalten.

BIOMETRISCHE VERIFIZIERUNG

Hingegen wird der Begriff der „biometrischen Verifizierung“ gemäß Art. 3 Nr. 36 KI-Verordnung folgendermaßen definiert:

„die automatisierte Eins-zu-eins-Verifizierung, einschließlich Authentifizierung, der Identität natürlicher Personen durch den Vergleich ihrer biometrischen Daten mit zuvor bereitgestellten biometrischen Daten“

Hier geht es daher um die Bestätigung einer Identität, indem individuelle menschliche Merkmale, wie etwa das Gesicht, die Stimme oder der Gang, automatisch erkannt werden. Dabei werden biometrische Daten (Fotos, Sprachproben etc.) mit zuvor vom Betroffenen erhaltenen Referenzdaten abgeglichen, die in einer Datenbank zum Zwecke des Abgleichs gespeichert sind. Typische Anwendungsfälle sind die Verifizierung gegenüber Zugangskontrollsystemen, wie etwa „FaceID“ im Apple iPhone.

BIOMETRISCHES FERNIDENTIFIZIERUNGSSYSTEM

Art. 3 Nr. 41 KI-Verordnung (KI-VO) legt den Begriff „biometrisches Fernidentifizierungssystem“ wie folgt fest:

„ein KI-System, das dem Zweck dient, natürliche Personen ohne ihre aktive Einbeziehung und in der Regel aus der Ferne durch Abgleich der biometrischen Daten einer Person mit den in einer Referenzdatenbank gespeicherten biometrischen Daten zu identifizieren“

Diese biometrischen Fernidentifizierungssysteme werden gemäß ErwGr 15 KI-VO in der Regel zur zeitgleichen Erkennung mehrerer Personen oder ihrer Verhaltensweisen verwendet, um die Identifizierung natürlicher Personen ohne ihre aktive Einbeziehung erheblich zu erleichtern. Dies umfasst keine KI-Systeme, die bestimmungsgemäß für die biometrische Verifizierung (wozu die Authentifizierung gehört) verwendet werden sollen, deren einziger Zweck darin besteht zu bestätigen, dass eine bestimmte natürliche Person die Person ist, für die sie sich ausgibt, sowie zur Bestätigung der Identität einer natürlichen Person zu dem alleinigen Zweck, Zugang zu einem Dienst zu erhalten, ein Gerät zu entriegeln oder Sicherheitszugang zu Räumlichkeiten zu erhalten.

Diese Ausnahme wird damit begründet, dass diese Systeme im Vergleich zu biometrischen Fernidentifizierungssystemen, die zur Verarbeitung biometrischer Daten einer großen Anzahl von Personen ohne ihre aktive Einbeziehung verwendet werden können, geringfügige Auswirkungen auf die Grundrechte natürlicher Personen haben dürften.

Wird ein solcher Abgleich in Echtzeigt vorgenommen, kommt die Erläuterung aus Art. 3 Nr. 42 KI-VO ins Spiel, denn dort wird der Begriff „biometrisches Echtzeit-Fernidentifizierungssystem" erläutert:

„ein biometrisches Fernidentifizierungssystem, bei dem die Erfassung biometrischer Daten, der Abgleich und die Identifizierung ohne erhebliche Verzögerung erfolgen, und das zur Vermeidung einer Umgehung der Vorschriften nicht nur die sofortige Identifizierung, sondern auch eine Identifizierung mit begrenzten kurzen Verzögerungen umfasst"

Bei solchen „Echtzeit-Systemen" erfolgen die Erfassung der biometrischen Daten, der Abgleich und die Identifizierung zeitgleich, nahezu zeitgleich oder auf jeden Fall ohne erhebliche Verzögerung. In diesem Zusammenhang sollte es keinen Spielraum für eine Umgehung der Bestimmungen dieser Verordnung über die „Echtzeitnutzung" der betreffenden KI-Systeme geben, indem kleinere Verzögerungen vorgesehen werden. „Echtzeitsysteme" umfassen die Verwendung von „Live-Material" oder „Near-live-Material" wie etwa Videoaufnahmen, die von einer Kamera oder einem anderen Gerät mit ähnlicher Funktion erzeugt werden (ErwGr 17 KI-VO).

Soll die Identifizierung hingegen erst nachträglich erfolgen, dann definiert Art. 3 Nr. 43 KI-VO ein solches System wie folgt:

„ein biometrisches Fernidentifizierungssystem, das kein biometrisches Echtzeit-Fernidentifizierungssystem ist"

Dies umfasst keine KI-Systeme, die bestimmungsgemäß für die biometrische Verifizierung, wozu die Authentifizierung gehört, verwendet werden sollen, deren einziger Zweck darin besteht zu bestätigen, dass eine bestimmte natürliche Person die Person ist, für die sie sich ausgibt, sowie zur Bestätigung der Identität einer natürlichen Person zu dem alleinigen Zweck, Zugang zu einem Dienst zu erhalten, ein Gerät zu entriegeln oder Sicherheitszugang zu Räumlichkeiten zu erhalten. Diese Ausnahme wird damit begründet, dass diese Systeme im Vergleich zu biometrischen Fernidentifizierungssystemen, die zur Verarbeitung biometrischer Daten einer großen Anzahl von Personen ohne ihre aktive Einbeziehung verwendet werden können, geringfügige Auswirkungen auf die Grundrechte natürlicher Personen haben dürften (ErwGr 17 KI-VO).

Beispielsweise kann eine Überwachungskamera das Gesicht einer vorbeigehenden Person aufnehmen und mit einer Fahndungsdatenbank abgleichen, um sie automatisch zu erkennen. Bei Echtzeitsystemen („biometrisches Echtzeit-Fernidentifizierungssystem") erfolgen Erfassung und Identifizierung sofort bzw. ohne spürbare Verzögerung. Diese Systeme gelten als hochriskant und sind unter der KI-Verordnung weitgehend verboten (außer eng umrissene Ausnahmen), da sie massiv in Grundrechte eingreifen.

Ein biometrisches Echtzeit-Fernidentifizierungssystem ist ein Unterfall des biometrischen Fernidentifizierungssystems. Hier geschehen die Datenerfassung (z. B. Videoaufnahme) und der anschließende Identitätsabgleich zeitgleich oder nahezu zeitgleich. Das System identifiziert Personen „in Echtzeit" im laufenden Betrieb. Da dabei Menschen oft unbemerkt überwacht werden, stellt dies eine der invasivsten KI-Anwendungen dar. Deshalb definiert die KI-Verordnung dies explizit und verbietet den Einsatz solcher Systeme im öffentlichen Raum. Als Beispiele können hier automatische Gesichtserkennungssysteme auf Flughäfen oder Straßen genannt werden.

BUNDESNETZAGENTUR (BNETZA)

Die Bundesnetzagentur (BNetzA) ist die nationale Regulierungsbehörde für Telekommunikation, Post, Energie, Eisenbahnen und digitale Infrastruktur. Nach aktuellem Stand wird die BNetzA auch zur zentralen Aufsichtsbehörde für die KI-Verordnung in Deutschland. Sie soll die Marktüberwachung von KI-Systemen übernehmen, ggf. Verstöße sanktionieren, Leitlinien erstellen, Vorgehen koordinieren und Meldepflichten abwickeln. Im Gesetz wird ihr zudem die Rolle eines „Koordinierungs- und Kompetenzzentrums KI-VO" übertragen. Das umfasst Koordination mit Behörden (z. B. Bundesamt für Sicherheit in der Informationstechnik oder Bundesanstalt für Finanzdienstleistungsaufsicht), Marktanalysen und Unterstützung kleinerer Anbieter.

Hinweis:
Im aktuellen Entwurf des Gesetzes zur Durchführung der Verordnung (EU) 2024/1689 des Europäischen Parlaments und des Rates vom 13.06.2024 zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz und zur Änderung der Verordnungen (EG) Nr. 300/2008, (EU) Nr. 167/2013, (EU) Nr. 168/2013, (EU) 2018/858, (EU) 2018/1139 und (EU) 2019/2144 sowie der Richtlinien

2014/90/EU, (EU) 2016/797 und (EU) 2020/1828, kurz: Gesetz zur Durchführung der Verordnung über künstliche Intelligenz (KI-MIG-VO), werden verschiedene Aspekte geregelt. Als sogenanntes Artikel-Gesetz enthält sie Änderungen an verschiedenen Gesetzen, unter anderem des Hinweisgeberschutzgesetzes oder des Sozialgesetzbuchs I. Zentraler Bestandteil in Art. 1 KI-MIG-VO ist jedoch das KI-Marktüberwachungs- und Innovationsförderungsgesetz (KI-MIG). In § 1 Abs. 1 KI-MIG ist festgelegt, dass die BNetzA die für die Einhaltung der KI-Verordnung zuständige Marktüberwachungsbehörde ist.

BÜRO FÜR KÜNSTLICHE INTELLIGENZ (KI-BÜRO)

Das EU-Büro für künstliche Intelligenz (KI-Büro, engl. „AI Office“) ist eine neu geschaffene Einrichtung der Europäischen Kommission. Seit Juni 2024 ist das KI-Büro eingerichtet, um die Umsetzung der KI-Verordnung zu unterstützen. Zu seinen Aufgaben gehören unter anderem die Förderung vertrauenswürdiger KI, Unterstützung der Mitgliedstaaten bei Aufsicht und Regulierung sowie internationale Zusammenarbeit zur KI-Governance. Das KI-Büro soll zentrale Richtlinien und Leitlinien erarbeiten, den Informationsaustausch zwischen nationalen Aufsichtsbehörden koordinieren und technische Expertise bereitstellen. Kurz: Das KI-Büro ist sozusagen das „KI-Exekutivorgan“ der EU-Kommission zur Überwachung und Weiterentwicklung des KI-Rechtsrahmens.

Hinweis:
Definiert wird das KI-Büro in Art. 3 Nr. 47 KI-Verordnung wie folgt:

„die Aufgabe der Kommission, zur Umsetzung, Beobachtung und Überwachung von KI-Systemen und KI-Modellen mit allgemeinem Verwendungszweck und zu der im Beschluss der Kommission vom 24. Januar 2024 vorgesehenen KI-Governance beizutragen; Bezugnahmen in dieser Verordnung auf das Büro für Künstliche Intelligenz gelten als Bezugnahmen auf die Kommission“

CE-KENNZEICHEN

Das CE-Kennzeichen (Conformité Européenne) ist eine Produktkennzeichnung, die anzeigt, dass ein Produkt spezifischen EU-Vorgaben entspricht. Die CE-Kennzeichnung ist generell nur für Produkte erforderlich, die unter harmonisierte EU-Vorschriften fallen, die dies ausdrücklich vorschreiben. Wenn für Ihr Produkt keine solchen EU-Anforderungen bestehen, darf die CE-Kennzeichnung nicht verwendet werden.

Beispielsweise fallen folgende Produkte unter die EU-Vorschriften zur CE-Kennzeichnung:

- Spielzeug
- Drohnen
- Elektro- und Elektronikgeräte
- pyrotechnische Erzeugnisse
- Sportboote und Wassermotorräder
- bestimmte Druckgeräte, Gasgeräte, Batterien und Maschinen
- Waagen und Messgeräte
- Persönliche Schutzausrüstung
- Medizingeräte einschließlich Diagnostika

Aber eben auch die KI-Verordnung (KI-VO) enthält entsprechende Vorgaben. Anbieter von Hochrisiko-KI-Systemen müssen die CE-Kennzeichnung an das Hochrisiko-KI-System oder, falls dies nicht möglich ist, auf seiner Verpackung oder in der beigefügten Dokumentation anbringen (Art. 16 Abs. lit. h) KI-VO). Die Voraussetzungen für die CE-Kennzeichnung enthält Art. 48 KI-VO:

- Bei digital bereitgestellten Hochrisiko-KI-Systemen wird eine digitale CE-Kennzeichnung nur dann verwendet, wenn sie über die Schnittstelle, von der aus auf dieses System zugegriffen wird, oder über einen leicht zugänglichen maschinenlesbaren Code oder andere elektronische Mittel leicht zugänglich ist.
- Die CE-Kennzeichnung wird gut sichtbar, leserlich und dauerhaft an Hochrisiko-KI-Systemen angebracht. Falls die Art des Hochrisiko-KI-Systems dies nicht zulässt oder nicht rechtfertigt, wird sie auf der Verpackung bzw. der beigefügten Dokumentation angebracht.

- Ggf. wird der CE-Kennzeichnung die Identifizierungsnummer der für die in Art. 43 KI-VO festgelegten Konformitätsbewertungsverfahren zuständigen notifizierten Stelle hinzugefügt. Die Identifizierungsnummer der notifizierten Stelle ist entweder von der Stelle selbst oder nach ihren Anweisungen durch den Anbieter oder den Bevollmächtigten des Anbieters anzubringen. Diese Identifizierungsnummer wird auch auf jeglichem Werbematerial angegeben, in dem darauf hingewiesen wird, dass das Hochrisiko-KI-System die Anforderungen für die CE-Kennzeichnung erfüllt.
- Falls Hochrisiko-KI-Systeme ferner unter andere Rechtsvorschriften der Union fallen, in denen die CE-Kennzeichnung auch vorgesehen ist, bedeutet die CE-Kennzeichnung, dass das Hochrisiko-KI-System auch die Anforderungen dieser anderen Rechtsvorschriften erfüllt.

Nach der KI-VO müssen alle als hochriskant eingestuften KI-Systeme ein CE-Zeichen tragen. Denn das bedeutet, dass der Anbieter eine Konformitätsbewertung durchgeführt hat und die EU-Anforderungen (Sicherheits- und Dokumentationspflichten) erfüllt sind. Das Fehlen des korrekten CE-Zeichens ist ein Verstoß, der Sanktionen nach sich ziehen kann.

Hinweis:
Für die CE-Kennzeichnung von Hochrisiko-KI-Systemen gelten ergänzende Grundsätze. Diese finden sich in der Verordnung (EG) Nr. 765/2008 des Europäischen Parlaments und des Rates vom 09.07.2008 über die Vorschriften für die Akkreditierung und Marktüberwachung im Zusammenhang mit der Vermarktung von Produkten und zur Aufhebung der Verordnung (EWG) Nr. 339/93 des Rates. Deren Art. 30 enthält die allgemeinen Regeln:

- Die CE-Kennzeichnung darf nur durch den Hersteller oder seinen Bevollmächtigen angebracht werden.
- Die CE-Kennzeichnung gemäß Anhang II wird nur auf Produkten angebracht, für die spezifische Harmonisierungsrechtsvorschriften der Gemeinschaft deren Anbringung vorschreiben, und wird auf keinem anderen Produkt angebracht.
- Indem er die CE-Kennzeichnung anbringt oder anbringen lässt, gibt der Hersteller an, dass er die Verantwortung für die Konformität des Produkts mit allen in den einschlägigen Harmonisierungsrechtsvorschriften der Ge-

meinschaft enthaltenen für deren Anbringung geltenden Anforderungen übernimmt.

- Die CE-Kennzeichnung ist die einzige Kennzeichnung, die die Konformität des Produkts mit den geltenden Anforderungen der einschlägigen Harmonisierungsrechtsvorschriften der Gemeinschaft, die ihre Anbringung vorschreiben, bescheinigt.

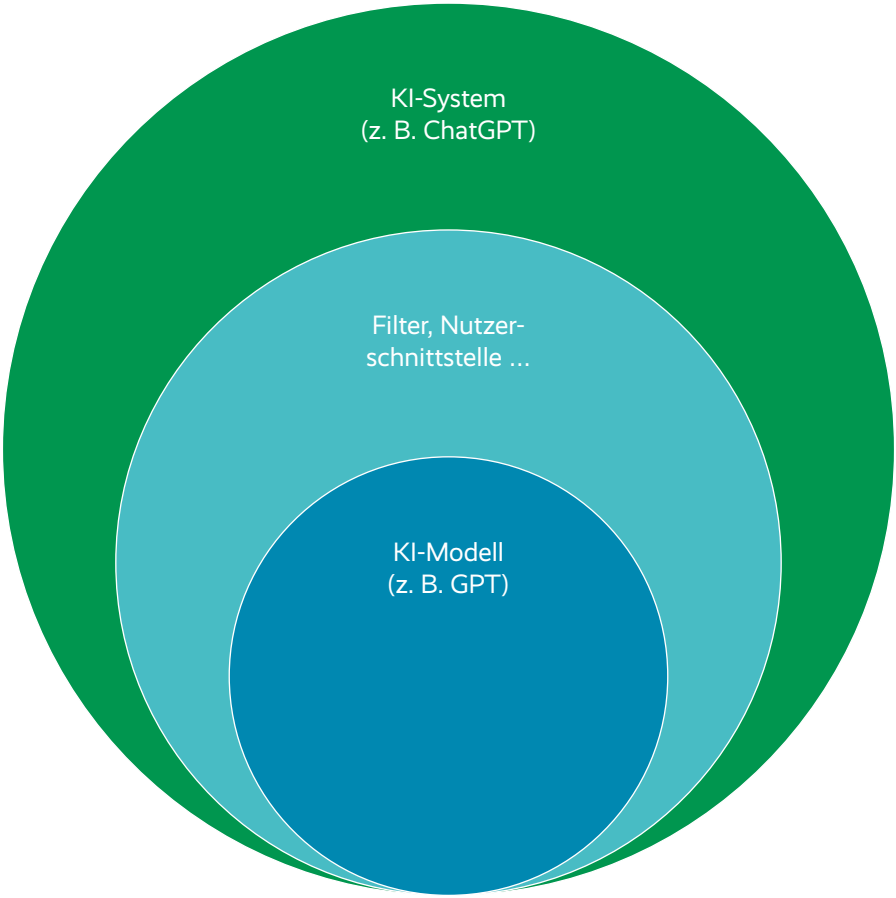
- Das Anbringen von Kennzeichnungen, Zeichen oder Aufschriften, deren Bedeutung oder Gestalt von Dritten mit der Bedeutung oder Gestalt der CE-Kennzeichnung verwechselt werden kann, ist untersagt. Jede andere Kennzeichnung darf auf Produkten angebracht werden, sofern sie Sichtbarkeit, Lesbarkeit und Bedeutung der CE-Kennzeichnung nicht beeinträchtigt.

- Unbeschadet des Artikels 41 stellen die Mitgliedstaaten die ordnungsgemäße Durchführung des Systems der CE-Kennzeichnung sicher und leiten bei einer missbräuchlichen Verwendung die angemessenen Schritte ein. Die Mitgliedstaaten sehen auch Sanktionen für Verstöße vor, die bei schweren Verstößen strafrechtlicher Natur sein können. Diese Sanktionen müssen in angemessenem Verhältnis zum Schweregrad des Verstoßes stehen und eine wirksame Abschreckung gegen missbräuchliche Verwendung darstellen.

CHATGPT

ChatGPT ist ein zusammengesetztes Wort aus „Chat“ (vom Englischen „to chat“, auf Deutsch: „plaudern“ oder „sich unterhalten“) und der Abkürzung „GPT“. Diese steht für „generative pre-trained transformer“, auf Deutsch also „generativer vortrainierter Transformer“. Dabei handelt es sich um das KI-System von OpenAI, das im November 2022 herausgebracht und für den Massenmarkt bereitgestellt wurde. Mit dieser generativen KI können Nutzer über die Eingabe von textbasierten Nachrichten (und inzwischen auch über Foto-, Video- oder Audio-Inhalte) ähnlich wie mit einem Menschen kommunizieren.

Die Grundlage von ChatGPT ist ein Large Language Model (LLM). Dabei handelt es sich um ein sehr leistungsfähiges Sprachmodell, das mit einer Vielzahl von Inhalten, insbesondere mit Textdokumenten, trainiert wurde.

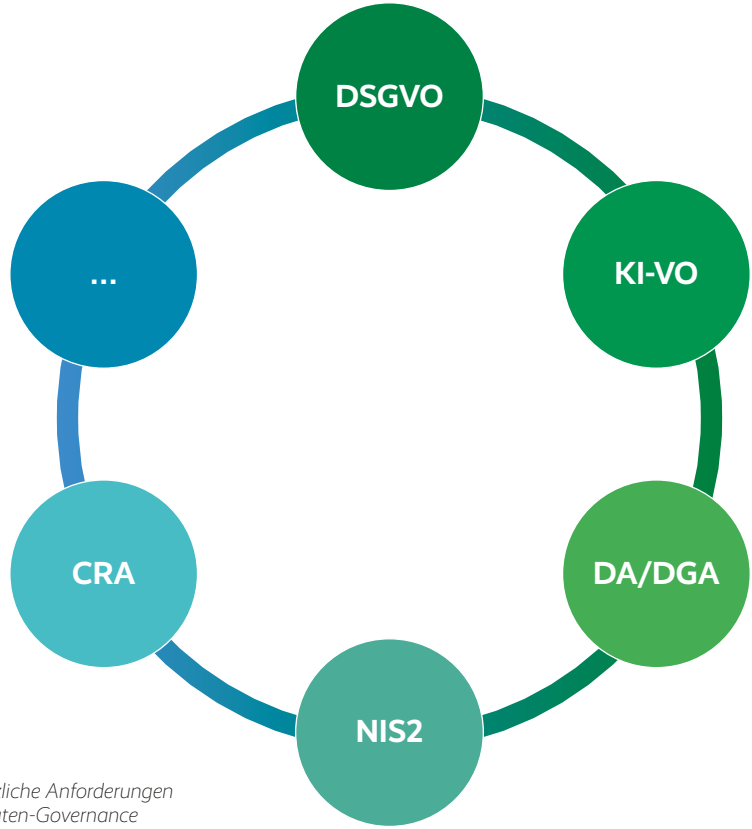


Unterschied KI-Modell/KI-System

Es muss also zwischen dem KI-System (ChatGPT) und dessen einzelnen Bestandteilen differenziert werden. Der wichtigste Bestandteil ist das „Herzstück", nämlich das KI-Modell (GPT), das sozusagen als „Motor" die Fähigkeiten der Anwendung enthält. Damit Nutzer jedoch mit der KI interagieren können, benötigt das KI-Modell zusätzlich zumindest noch eine Nutzerschnittstelle sowie weitere Bestandteile, wie beispielsweise einzelne Filter. Zusammen bilden diese Einzelteile dann das KI-System.

DATEN-GOVERNANCE

Daten-Governance bezeichnet den organisatorischen, rechtlichen und technischen Ordnungsrahmen, nach dem Daten im Unternehmen oder auch Behörden sinnvoll verwaltet, genutzt, geschützt und geteilt werden. Sie umfasst unter anderem Rollen und Verantwortlichkeiten (z. B. Data Owner, Data Steward), Prozesse und Richtlinien (etwa Freigabeprozesse, Löschkonzepte), technische Kontrollen (beispielsweise Zugriffsrechte, Verschlüsselung) sowie Compliance-Anforderungen (z. B. Datenschutzgrundverordnung (DSGVO), KI-Verordnung (KI-VO), Data Act/Data Governance Act (DGA), branchenspezifische Vorgaben).



Gesetzliche Anforderungen zur Daten-Governance

Daten-Governance ist weit mehr als nur Datenmanagement; sie bildet den regulatorischen und organisatorischen Rahmen, der die Integrität, Verfügbarkeit und Qualität von Daten über deren gesamten Lebenszyklus sicherstellt. Im Zeitalter der KI fungiert sie als Bindeglied zwischen technischer Innovation und rechtlicher Compliance. Zugleich sind Data Governance und die Sicherstellung bestimmter Datenqualitätsstandards ein „Enabler" für hochwertige und rechtskonforme KI Systeme und -modelle.

Auf EU-Ebene konkretisiert der DGA diesen Rahmen für den sektorübergreifenden Datenaustausch und führt unter anderem Regeln für Datenvermittlungsdienste und altruistische Datennutzung ein. Ziel ist die Schaffung eines vertrauenswürdigen europäischen Datenraums, in dem Daten über Grenzen und Sektoren hinweg geteilt werden können, ohne Datenschutz, Geschäftsgeheimnisse oder öffentliche Interessen zu gefährden.

Der DGA zielt darauf ab, das Vertrauen in den Datenaustausch innerhalb der Union zu stärken und neue europäische Datenräume zu erschließen. Durch die Regulierung von Datenvermittlungsdiensten und die Einführung des Konzepts des Datenaltruismus wird versucht, die bisherige Zurückhaltung bei der Bereitstellung von Daten – insbesondere aus dem öffentlichen Sektor – zu überwinden. Die Governance-Strukturen müssen hierbei sicherstellen, dass Daten auffindbar, verständlich, sicher und interoperabel sind. Dies erfordert insbesondere die Implementierung unternehmensweiter automatisierter Prüfprozesse für die Datenqualität.

Ein Kernaspekt der Daten-Governance unter der KI-VO sind die in Art. 10 KI-VO festgelegten Anforderungen für Hochrisiko-KI-Systeme. Trainings-, Validierungs- und Testdatensätze müssen angemessenen Governance- und Managementpraktiken unterliegen. Hierzu gehören insbesondere:

- **Relevanz und Repräsentativität:** Die Daten müssen den spezifischen Kontext der Anwendung widerspiegeln, um Verzerrungen zu vermeiden.
- **Fehlerfreiheit und Vollständigkeit:** Datensätze müssen auf Rauschen und Inkonsistenzen geprüft werden.
- **Bias-Management:** Prozesse zur Identifizierung und Minderung von Voreingenommenheiten bzw. Verzerrungen (z. B. ethnische oder geschlechtsspezifische Benachteiligungen) sind zwingend erforderlich.

Das Bundesamt für Sicherheit in der Informationstechnik hat mit dem Leitfaden Quality Criteria for AI Trainingsdata in AI Lifecycle („QUAIDAL)" einen methodi-

schen Katalog vorgelegt, der Unternehmen dabei unterstützt, diese Anforderungen durch konkrete Metriken und Maßnahmen zu operationalisieren. Datenqualität wird hierbei direkt als KI-Qualität verstanden, da die Performanz und Sicherheit eines Modells untrennbar mit der Güte der zugrunde liegenden Daten verknüpft sind. Der „QUAIDAL"-Leitfaden besteht aus insgesamt sechs Dokumenten:

- **Teildokument A:** „01-Grundlagen & Methodik" (beschreibt die zugrunde liegende Methodik und erläutert, wie der Katalog praktisch zur Bewertung von Trainingsdatensätzen angewendet wird)
- **Teildokument B:** „02-Qualitätskriterien & Bausteine" (enthält alle relevanten Qualitätskriterien sowie die zugehörigen Bausteine)
- **Teildokument C:** „03-Qualitätsmaßnahmen & Metrikenmethoden" (erläutert sämtliche Maßnahmen zur Qualitätssicherung sowie entsprechende Metriken und angewandte Methoden)
- **Teildokument D:** „04-Referenzen" (ausführliche Übersicht aller verwendeten Referenzen, Normen, Standards und Verordnungen)
- **Teildokument E:** „BSI GitHub Teil A – maschinenlesbare Form des Katalogs"
- **Teildokument F:** „BSI GitHub Teil B – Sourcecodes zu den Metriken & Methoden"

Das Dokument „Qualitätskriterien & Bausteine" beschreibt den Aufbau der grundsätzlichen Gliederung der Abstraktionslevel wie folgt:

1) Qualitätskriterium (QKB)

2) Qualitätsbaustein (QB)

3) Qualitätsmaßnahme (MA)

4) Metriken & Methoden (QM)

Qualitätskriterien sind wichtig für die Definition von Qualitätszielen und die Bewertung von Qualität in verschiedenen Kontexten. Sie werden oft in Normen, Standards und Verordnungen (wie der KI-Verordnung) definiert und genutzt und dienen als Grundlage für die Erstellung detaillierter messbarer Qualitätsanforderungen. Zu diesen Kriterien zählen:

- Repräsentativität
- Vollständigkeit
- Genauigkeit

- Konsistenz
- Korrektheit
- Einheitlichkeit
- Gültigkeit
- Eindeutigkeit
- Sichere Quellen
- Daten mit Personenbezug

Ein „Baustein" in diesem Kontext bezieht sich auf eine klar definierte Komponente oder Einheit innerhalb eines größeren Systems, die zur Erfüllung einer spezifischen Funktion oder Aufgabe dient. Die Liste dieser Bausteine umfasst die folgenden Inhalte:

- Syntaktische Genauigkeit
- Semantische Genauigkeit
- Vielfalt
- Ausgewogenheit
- Umfang
- Bias-Detektion
- Gesamtheit
- Konsistenzsicherung
- Quellenmanagement
- Data Checks
- Prozesse
- Feature Engineering
- Datenvorbereitung
- Expertenanalyse
- Bias-Mitigation

Die „QUAIDAL"-Vorgaben dienen letztlich als Leitfaden zur Planung, Umsetzung und Bewertung von Qualitätskriterien für Trainingsdaten im KI-Lebenszyklus.

DATENSCHUTZBEAUFTRAGTER (DSB)

Ein Datenschutzbeauftragter (DSB) ist eine interne oder externe Fachkraft mit Expertise im Datenschutzrecht und in der Datenschutzpraxis. Der DSB hat die Aufgabe, auf die Einhaltung datenschutzrechtlicher Vorschriften durch Beratung des Unternehmens und seiner Mitarbeiter hinzuwirken und die Einhaltung zu überwachen.

Die Antwort auf die Frage, wer unter welchen Voraussetzungen einen DSB benennen muss, erfordert in Deutschland eine zweistufige Prüfung nach Datenschutzgrundverordnung (DSGVO) und Bundesdatenschutzgesetz (BDSG), vgl. Art. 37 DSGVO und §§ 5, 38 BDSG.

1. Stufe (DSGVO)

- Die Verarbeitung wird von einer Behörde oder öffentlichen Stelle durchgeführt, mit Ausnahme von Gerichten, soweit sie im Rahmen ihrer justiziellen Tätigkeit handeln (Art. 37 Abs. 1 lit. a) DSGVO).
- Die Kerntätigkeit des Verantwortlichen oder des Auftragsverarbeiters besteht in der Durchführung von Verarbeitungsvorgängen, welche aufgrund ihrer Art, ihres Umfangs und/oder ihrer Zwecke eine umfangreiche regelmäßige und systematische Überwachung von betroffenen Personen erforderlich machen (Art. 37 Abs. 1 lit. b) DSGVO).
- Die Kerntätigkeit des Verantwortlichen oder des Auftragsverarbeiters besteht in der umfangreichen Verarbeitung besonderer Kategorien von Daten gemäß Art. 9 oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gemäß Art. 10 (Art. 37 Abs. 1 lit. c) DSGVO).

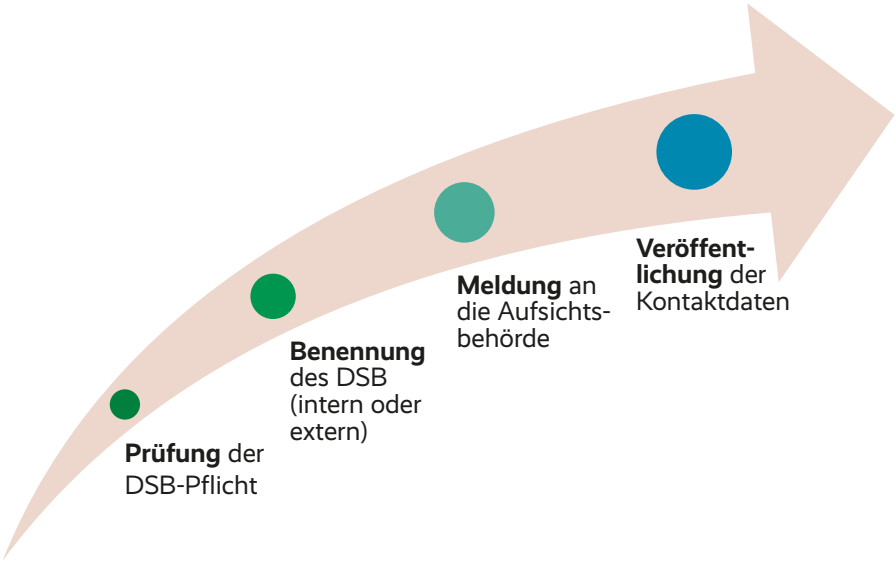
2. Stufe (BDSG)

- Öffentliche Stellen benennen einen DSB (gilt auch für öffentliche Stellen, die am Wettbewerb teilnehmen) (§ 5 BDSG).
- Unternehmen, die in der Regel mindestens 20 Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigen (§ 38 Abs. 1 S. 1 BDSG)
- Unternehmen, die personenbezogene Daten verarbeiten, die einer Datenschutz-Folgenabschätzung (DSFA) nach Art. 35 DSGVO unterliegen (§ 38 Abs. 1 S. 2 Alt. 1 BDSG)
- Unternehmen, die personenbezogene Daten geschäftsmäßig zum Zweck der Übermittlung/anonymisierten Übermittlung verarbeiten (§ 38 Abs. 1 S. 2 Alt. 2 BDSG)

- Unternehmen, die personenbezogener Daten für Zwecke der Markt- oder Meinungsforschung verarbeiten (§ 38 Abs. 1 S. 2 Alt. 3 BDSG)

Es kann sowohl ein interner als auch ein externer DSB benannt werden (Art. 37 Abs. 6 DSGVO). Er muss jedoch in jedem Fall die Fähigkeit zur Erfüllung seiner Aufgaben besitzen, außerdem auch Fachwissen in den Bereichen Datenschutzrecht und Datenschutzpraxis. Auch eine einschlägige berufliche Qualifikation ist Voraussetzung (z. B. Jurist). Außerdem darf keine Interessenskollision bestehen, was regelmäßig etwa bei Mitgliedern der Geschäftsleitung, Betriebsratsvorsitzenden, IT-Leitern, CISOs oder auch der Personalabteilungsleitung der Fall ist.

Die Benennung des DSB kann grundsätzlich formfrei erfolgen, allerdings ist eine schriftliche Benennung sinnvoll. Auf jeden Fall muss der DSB bei der zuständigen Aufsichtsbehörde gemeldet werden (Art. 37 Abs. 7 DSGVO). Auch sind seine Kontaktdaten zu veröffentlichen, z. B. im Rahmen der Datenschutzhinweise. Ein Name muss hier nicht zwingend genannt werden, die Nennung einer Funktions-E-Mail-Adresse (z. B. „datenschutz@...“) ist ausreichend. Wichtig ist, dass der DSB unter den angegebenen Kontaktdaten tatsächlich erreicht werden kann.



Schritte DSB-Benennung

Der DSB ist ordnungsgemäß und frühzeitig in alle mit dem Schutz personenbezogener Daten zusammenhängende Fragen einzubinden. Dabei ist er zur Wahrung der Geheimhaltung bzw. Vertraulichkeit verpflichtet (Art. 38 Abs. 5 DSGVO).

Der DSB ist nicht weisungsgebunden, aber auch nicht weisungsbefugt. Er dient als Ansprechpartner für alle Betroffenen. Der DSB berichtet unmittelbar an die Leitungsebene/Geschäftsführung. Er darf nicht wegen der Erfüllung seiner Aufgaben abberufen oder benachteiligt werden.

Um seine Tätigkeit sinnvoll ausführen zu können, benötigt der DSB die Bereitstellung ausreichender zeitlicher sowie finanzieller Ressourcen, wie etwa einen eigenen E-Mail-Account, ein eigenes Laufwerk bzw. Laufwerksordner zur Dateiablage, die Möglichkeit zur regelmäßigen Fortbildung usw.

Die gesetzlich vorgesehenen Aufgaben umfassen gemäß Art. 39 DSGVO Folgendes:

- Unterrichtung und Beratung des Verantwortlichen oder des Auftragsverarbeiters und der Beschäftigten, die Verarbeitungen durchführen, hinsichtlich ihrer Pflichten nach dieser Verordnung sowie nach sonstigen Datenschutzvorschriften der Union bzw. der Mitgliedstaaten
- Überwachung der Einhaltung dieser Verordnung, anderer Datenschutzvorschriften der Union bzw. der Mitgliedstaaten sowie der Strategien des Verantwortlichen oder des Auftragsverarbeiters für den Schutz personenbezogener Daten einschließlich der Zuweisung von Zuständigkeiten, der Sensibilisierung und Schulung der an den Verarbeitungsvorgängen beteiligten Mitarbeiter und der diesbezüglichen Überprüfungen
- Beratung – auf Anfrage – im Zusammenhang mit der DSFA und Überwachung ihrer Durchführung
- Zusammenarbeit mit der Aufsichtsbehörde
- Tätigkeit als Anlaufstelle für die Aufsichtsbehörde in mit der Verarbeitung zusammenhängenden Fragen, einschließlich der vorherigen Konsultation gemäß Art. 36, und ggf. Beratung zu allen sonstigen Fragen

Der DSB hat bei der Erfüllung seiner Aufgaben dem mit den Verarbeitungsvorgängen verbundenen Risiko gebührend Rechnung zu tragen, wobei er die Art, den Umfang, die Umstände und die Zwecke der Verarbeitung berücksichtigt.

DATENSCHUTZ-FOLGENABSCHÄTZUNG (DSFA)

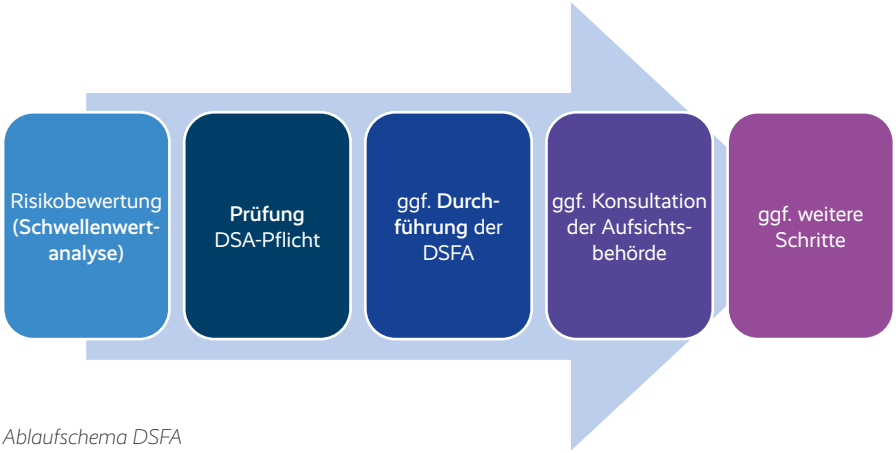
Eine Datenschutz-Folgenabschätzung (DSFA) ist eine systematische Risikoanalyse gemäß Art. 35 Datenschutzgrundverordnung (DSGVO). Sie ist durchzuführen, wenn eine Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat.

Risikostufen in der DSGVO

Typische Fälle sind neue Technologien (unter anderem KI-Anwendungen), Videoüberwachung, umfangreiches Monitoring oder Verarbeitung sensibler Daten.

In einem ersten Schritt ist eine Risikobewertung in Bezug auf die konkrete Verarbeitungstätigkeit vorzunehmen und zu dokumentieren (sogenannte Schwellwertanalyse). Ist die Schwelle zum (voraussichtlich) hohen Risiko überschritten, kann dann die konkrete Prüfung der Pflicht zur DSFA erfolgen. Muss diese tatsächlich durchgeführt werden, kommt es hier zu einer detaillierteren Prüfung des Risikoszenarios. Ergibt die Prüfung, dass geeignete technische und/oder organisatorische Maßnahmen (TOM) umgesetzt werden können, um das ursprünglich

als hoch identifizierte Risiko zumindest auf ein normales oder gar ein niedriges Maß zu senken, dann kann die geplante Verarbeitungstätigkeit mittels Umsetzung der geeigneten TOM durchgeführt werden. Andernfalls muss die zuständige Aufsichtsbehörde konsultiert werden. Sofern diese Vorgaben für konkrete TOM macht, mit deren Hilfe die geplante Verarbeitung ohne hohes Risiko durchgeführt werden kann, ist diesen Anweisungen Folge zu leisten. Sollte allerdings auch die Aufsichtsbehörde keinen Weg aufzeigen, wie sich das hohe Risiko reduzieren lässt, hat das zur Folge, dass die Verarbeitung jedenfalls nicht wie geplant durchgeführt werden darf.



Ablaufschema DSFA

Zur Prüfung, ob eine DSFA durchzuführen ist, sollten die folgenden Punkte Schritt für Schritt befolgt werden:

1. keine Ausnahme (Art. 35 Abs. 5, 10 DSGVO)?
2. Verarbeitung auf Positivliste (auch „Muss-Liste“ oder „Blacklist“ genannt; Art. 35 Abs. 4 DSGVO)?
3. Hohes Risiko gemäß Leitlinien der Art.-29-Gruppe aus dem Working Paper 248?
4. Sonstiges hohes Risiko im Sinne von Art. 35 Abs. 1 DSGVO?

Der erste Punkt, also die im Gesetz vorgesehenen Ausnahmefälle, spielen für Deutschland keine Rolle, denn – anders als z. B. Österreich – haben bislang weder die Bundesregierung noch die deutschen Datenschutzaufsichtsbehörden Gebrauch von diesen Ausnahmeregelungen gemacht.

Im zweiten Schritt ist zu prüfen, ob sich die geplante Verarbeitungstätigkeit auf einer sogenannten „Positivliste" wiederfindet. Dabei handelt es sich um Listen, auf denen die Aufsichtsbehörden solche Verarbeitungstätigkeiten aufgeführt haben, die in jedem Fall eine DSFA erforderlich machen. Solche Positivlisten existieren in jedem Bundesland und sind getrennt nach Unternehmen einerseits und öffentlichen Stellen andererseits.

Die Liste für den öffentlichen Bereich im Bundesland Nordrhein-Westfalen enthält beispielsweise unter anderem folgende Verarbeitungstätigkeiten:

- umfangreiche Verarbeitungstätigkeiten im Rahmen der Kinder- und Jugendhilfe
- umfangreiche Verarbeitungstätigkeiten von Arbeitslosengeld II etc. (Jobcenter)
- Verarbeitung von Meldedaten (Melderegister)
- Führen von Personenstandsregistern
- Bearbeiten von Personalausweis- und Passanträgen
- Verarbeitungstätigkeiten der Sozialhilfe
- Verarbeitung von personenbezogenen Daten im Rahmen der amtlichen Statistik

Die Positivliste der Datenschutzkonferenz (DSK) für den nicht-öffentlichen Bereich führt hingegen folgende Punkte an:

- Verwendung von biometrischen Systemen zur Zutrittskontrolle oder für Abrechnungszwecke
- große Anwaltssozietät/große Arztpraxis
- Fahrzeugdatenverarbeitung (zentralisierte Verarbeitung der Messwerte oder Bilderzeugnisse von Umgebungssensoren)
- Fraud-Prevention-Systeme
- Scoring durch Auskunfteien, Banken oder Versicherungen
- Betrieb von Bewertungsportalen
- Inkassodienstleistungen (Factoring)
- Geolokalisierung von Beschäftigten
- Big-Data-Analyse von Kundendaten, die mit Angaben aus Drittquellen angereichert wurden

- Kundensupport mittels künstlicher Intelligenz
- Telefongespräch-Auswertung mittels Algorithmen
- Anonymisierung von besonderen Arten personenbezogener Daten (Art. 9 DSGVO)
- Einsatz von Telemedizinlösungen zur detaillierten Bearbeitung von Krankheitsdaten

Wird man hier nicht fündig, sind im dritten Schritt die gesetzlichen Regelbeispiele aus Art. 35 Abs. 3 DSGVO zu prüfen. Dabei geht es um folgende Alternativen:

- systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen, die sich auf automatisierte Verarbeitung einschließlich Profiling gründet und die ihrerseits als Grundlage für Entscheidungen dient, die Rechtswirkung gegenüber natürlichen Personen entfalten oder diese in ähnlich erheblicher Weise beeinträchtigen
- umfangreiche Verarbeitung besonderer Kategorien von personenbezogenen Daten gemäß Art 9, 10 DSGVO
- systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche

Sollte man hier auch nicht zu einem Ergebnis kommen, dann sind im vierten Schritt die Risikokriterien aus den „Leitlinien zur Datenschutz-Folgenabschätzung (DSFA) und Beantwortung der Frage, ob eine Verarbeitung im Sinne der Verordnung 2016/679 wahrscheinlich ein hohes Risiko mit sich bringt“ (Working Paper 248) der Art.-29-Gruppe (Vorgänger des Europäischen Datenschutzausschusses) unter die Lupe zu nehmen:

- Evaluierung- oder Scoring-Maßnahmen
- automatisierte Entscheidung mit rechtlicher Relevanz oder ähnlicher Wirkung für den Betroffenen (Profiling)
- systematische Beobachtung von Betroffenen
- Verarbeitung besonderer Kategorien personenbezogener Daten
- in großem Umfang verarbeitete personenbezogene Daten
- Abgleich bzw. Kombination verschiedener Datensätze
- personenbezogene Daten verletzlicher Datensubjekte
- Einsatz neuartiger Lösungen/Technologien

- Übermittlung personenbezogener Daten in Drittstaaten
- Datenverarbeitungen, die Betroffene davon abhalten, ihre Rechte geltend zu machen oder einen Dienst/Vertrag zu nutzen

Sofern mehr als zwei der genannten Kriterien vorliegen, ist von einem hohen Risiko und damit von einer Pflicht zur Durchführung der DSFA auszugehen.

Zum besseren Verständnis enthält das Working Paper 248 auch noch einige Beispiele:

DSFA erforderlich	DSFA nicht erforderlich
Verarbeitung medizinischer Daten durch Krankenhaus	Verarbeitung medizinischer Daten durch Einzelarzt
Kameraüberwachung auf Schnellstraßen	Abonnentenliste eines Onlinemagazins
systematische Überwachung von Beschäftigten durch Arbeitgeber	Profilbildung durch auf Website eingebundene Werbeanzeigen
Profilbildung mit öffentlich zugänglichen Daten aus sozialen Netzwerken	
Betrieb einer Bonitätsdatenbank	

Ergibt auch hier die Suche keine Ergebnisse, ist im abschließenden fünften Schritt zu prüfen, ob ein sonstiges hohes Risiko im Sinne von Art. 35 Abs. 1 DSGVO besteht. Davon ist auszugehen „insbesondere bei Verwendung neuer Technologien", wie etwa KI, oder aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung. Auch hierbei gilt es, den risikobasierten Ansatz der DSGVO zu beachten.

Als Mindestinhalt muss eine DSFA folgende Punkte enthalten (Art. 35 Abs. 7 DSGVO):

- systematische Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung, ggf. einschließlich der vom Verantwortlichen verfolgten berechtigten Interessen
- Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck
- Bewertung der Risiken für die Rechte und Freiheiten der Betroffenen
- die zur Bewältigung der Risiken geplanten Abhilfemaßnahmen, einschließlich Garantien, Sicherheitsvorkehrungen und Verfahren, durch die der Schutz der Daten sichergestellt und der Nachweis dafür erbracht wird, dass die DSGVO eingehalten wird

Gerade bei der Durchführung und Dokumentation der DSFA kann natürlich auch KI sehr gut helfen. Als Beleg dafür mag die folgende, mit dem Tool Perplexity erstellte DSFA für die Einführung von Perplexity dienen, durchgeführt am Beispiel eines mittelständischen IT-Dienstleistungsunternehmens:

Beispiel: Datenschutz-Folgenabschätzung (DSFA) gemäß Art. 35 DSGVO

Einsatz von Perplexity AI als SaaS-Dienst

Verantwortlicher	[Mittelständisches IT-Dienstleistungsunternehmen, Deutschland]
Datenschutzbeauftragter	[Name/Funktion intern einzutragen]
KI-Beauftragter	[Name/Funktion intern einzutragen]
Erstellt am	19.03.2026
Version	1.0
Status	Entwurf – zur Prüfung durch DSB
Klassifikation	Vertraulich

Präambel und Erforderlichkeit der DSFA

Eine DSFA ist gemäß Art. 35 Abs. 1 DSGVO verpflichtend durchzuführen, wenn eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat.

Der geplante Einsatz von Perplexity AI als SaaS-Dienst erfüllt mehrere Kriterien der DSK-Blacklist (Muss-Liste) sowie des WP 248 Rev. 01 des Europäischen Datenschutzausschusses:

- Einsatz innovativer Technologie: Generative KI und Large Language Models stellen eine neue Technologie im Sinne des Art. 35 DSGVO dar.
- Leistungsbeurteilung von Beschäftigten: Die KI-gestützte Leistungsanalyse begründet das Kriterium „Bewerten oder Einstufen (Scoring)“ nach WP 248.
- Bewerbermanagement: Die Nutzung im Kontext von Recruiting und Bewerberauswahl gilt gemäß Anhang III Nr. 4 EU AI Act als Hochrisiko-KI.
- Drittstaatentransfer: Die Verarbeitung personenbezogener Daten bei einem in den USA ansässigen Anbieter (Perplexity AI, Inc.) erfordert besondere Schutzmaßnahmen.

- Einschaltung eines Auftragsverarbeiters: Die Auswertung der Leistungsanalysedaten durch einen externen Dienstleister begründet eine weitere Verarbeitungskette.

Die DSFA-Pflicht ist damit unzweifelhaft gegeben. Sie ist vor Inbetriebnahme des Tools abzuschließen. Da der Einsatz auch die Verarbeitung von Beschäftigtendaten umfasst, hat der Betriebsrat (sofern vorhanden) gemäß § 87 Abs. 1 Nr. 6 BetrVG ein zwingendes Mitbestimmungsrecht.

I. Systematische Beschreibung der Verarbeitung

1. Art der Verarbeitung

Das Unternehmen beabsichtigt den Einsatz des KI-gestützten SaaS-Dienstes Perplexity AI (Perplexity AI, Inc., San Francisco, USA) für verschiedene betriebliche Zwecke. Der Dienst kombiniert Large Language Models (LLMs) verschiedener Drittanbieter (unter anderem OpenAI-Modelle, Anthropic Claude, Google Gemini, Meta Llama) mit einer Echtzeit-Websuchfunktion. Die Verarbeitung umfasst:

- **Textgenerierung:** Erstellung von Inhalten für Website und Social Media (keine systemische Verarbeitung personenbezogener Daten Dritter in der Regel, es sei denn, Personenbezug wird durch Eingaben hergestellt)
- **Dokumentenübersetzung:** Verarbeitung von Dokumenteninhalten, die potenziell personenbezogene Daten enthalten (z. B. Kunden- oder Vertragspartnerdaten)
- **Grafikerstellung für Präsentationen:** Visuelle Inhaltsgenerierung; personenbezogener Datenbezug möglich, falls Präsentationsinhalte Personendaten enthalten
- **Korrespondenzunterstützung mit Kunden und Vertragspartnern:** Verarbeitung personenbezogener Daten von Kunden, Kontaktpersonen und Vertragspartnern durch Eingabe in das KI-System
- **Bewerbermanagement:** Verarbeitung personenbezogener Daten von Bewerbern (Name, Qualifikation, ggf. Lichtbild, Lebenslauf, Anschreiben) durch das KI-System
- **Leistungsanalyse von Beschäftigten:** Verarbeitung von Leistungsdaten aktueller Mitarbeiter durch das KI-System; Weitergabe an einen beauftragten externen Dienstleister zur Auswertung im Auftrag des Unternehmens

2. Umfang der Verarbeitung

Die Verarbeitung betrifft potenziell alle Kategorien von Beschäftigten des Unternehmens sowie externe Personen (Bewerber, Kunden, Vertragspartner). Die Intensität der Verarbeitung variiert je nach Anwendungsfall erheblich:

Anwendungsfall	**Betroffenen-gruppe**	**Datenkategorien**	**Verarbeitungs-intensität**
Texterstellung Website/ Social Media	Keine direkte Betroffenheit (sofern kein Personenbezug)	Ggf. Mitarbeiter-daten bei Nennung von Namen	Niedrig
Dokumenten-übersetzung	Kunden, Vertragspartner, ggf. Beschäftigte	Kontaktdaten, Vertragsdaten, Kommunikations-inhalte	Mittel
Grafikerstellung	Keine direkte Betroffenheit	Ggf. Personen-daten in Präsentationen	Niedrig
Korrespondenz-unterstützung	Kunden, Vertragspartner	Kontaktdaten, Kommunikations-inhalte, Vertragsdaten	Mittel bis Hoch
Bewerber-management	Bewerber	Bewerbungsun-terlagen (Name, Adresse, Qualifikation, Lichtbild, ggf. besondere Kategorien)	Hoch
Leistungsanalyse Beschäftigte	Aktive Beschäftigte	Leistungs-daten, Verhaltens-merkmale, ggf. Bewertungen	Hoch

Der Umfang der Verarbeitung hängt maßgeblich von der Nutzungsintensität und den eingegebenen Inhalten der einzelnen Nutzer ab. Es ist von einer unternehmensweiten Nutzung auszugehen.

3. Kontext der Verarbeitung

Das Unternehmen ist ein mittelständischer IT-Dienstleister in Deutschland. Es unterliegt damit vollumfänglich der DSGVO und dem BDSG. Der Kontext ist durch folgende Besonderheiten geprägt:

- Arbeitgeber-Arbeitnehmer-Verhältnis bei der Leistungsanalyse: strukturelles Machtgefälle, das erhöhte Anforderungen an die Verarbeitung stellt; § 26 BDSG als spezifischer Erlaubnistatbestand
- Bewerbungskontext: besonderer Schutzbedarf der Bewerber, die keine Vertragsbeziehung zum Unternehmen haben und auf die Informationspflichten nach Art. 13 DSGVO angewiesen sind
- Drittstaatentransfer: Perplexity AI, Inc. hat seinen Hauptsitz in den USA; Datentransfers erfolgen in ein Drittland.
- Nutzung multipler KI-Modelle: Perplexity greift auf LLMs verschiedener Drittanbieter (OpenAI, Anthropic, Google DeepMind, Meta, NVIDIA unter anderem) zu, die ihrerseits in den USA oder anderen Drittländern ansässig sind.
- Hohes gesellschaftliches Risikobewusstsein für KI-gestützte Personalentscheidungen (Diskriminierungsrisiko, Intransparenz)
- EU AI Act: KI-Systeme für HR-Zwecke (Bewerberauswahl, Leistungsbewertung) gelten als Hochrisiko-KI nach Anhang III Nr. 4 EU AI Act.

4. Zweck der Verarbeitung

Die Verarbeitung erfolgt zu folgenden Zwecken:

- Produktivitätssteigerung im Bereich Content-Erstellung (Website, Social Media)
- Effizienzgewinn bei der Übersetzung von Dokumenten
- Qualitätsverbesserung der Unternehmenskommunikation und Kundenkommunikation
- Unterstützung des Recruitings durch KI-gestützte Verarbeitung von Bewerbungsunterlagen
- Leistungsanalyse und -steuerung von Beschäftigten zur Personalentwicklung und ggf. zur Entscheidungsunterstützung (z. B. Boni, Beförderung, Weiterbeschäftigung)

Hinweis: Die Zwecke 4 und 5 begründen das höchste datenschutzrechtliche Risiko und erfordern die strengste Prüfung. Insbesondere ist zu klären, ob die KI-gestützte Leistungsanalyse als Grundlage für Personalentscheidungen mit rechtlicher Wirkung dienen soll (Relevanz für Art. 22 DSGVO).

5. Empfänger

Empfänger	Rechtsgrundlage der Übermittlung	Ort
Perplexity AI, Inc. (Auftragsverarbeiter)	Art. 28 DSGVO i. V. m. DPA, SCCs (EU SCC Module 2)	USA
Amazon Web Services (Sub-Processor)	Eingebunden via Perplexity DPA Annex 2	USA (ggf. EU-Region)
Microsoft Azure (Sub-Processor)	Eingebunden via Perplexity DPA Annex 2	USA (ggf. EU-Region)
Drittanbieter-LLM-Modellprovider (OpenAI, Anthropic, Google, Meta unter anderem)	Eingebunden via Perplexity DPA; gesonderte Unterauftragsverarbeitungsverträge	Überwiegend USA
Externer Dienstleister für Leistungsauswertung	Art. 28 DSGVO (eigenständiger AVV)	[Standort intern zu spezifizieren]

Perplexity AI hat einen Data Processing Addendum (DPA) für Enterprise-Kunden veröffentlicht, das EU Standardvertragsklauseln (SCC Modul 2 – Controller to Processor) inkorporiert und sich am EU-U.S. Data Privacy Framework orientiert.

Darüber hinaus bezieht Perplexity externe LLM-Modellprovider ein, über die im DPA Annex 3 informiert wird; für Änderungen dieser Modellprovider besteht lediglich eine Benachrichtigungspflicht, kein Widerspruchsrecht. Dies ist aus datenschutzrechtlicher Sicht kritisch zu bewerten, da keine vollständige Kontrolle über Sub-Unterauftragsverarbeiter besteht.

6. Speicherdauer

Eingabedaten (Prompts/Antworten) bei Enterprise-Nutzung: werden gemäß Perplexity DPA nicht für das Training der KI-Modelle verwendet. Hochgeladene Dateien werden standardmäßig 7 Tage aufbewahrt; bei Enterprise Pro mit 50+ Lizenzen können benutzerdefinierte Aufbewahrungsfristen festgelegt werden.

- Account-Daten: verbleiben für die Dauer der Vertragslaufzeit; Löschung innerhalb von 30 Tagen nach Vertragsende gemäß DPA Section 10
- Auf Unternehmensseite gespeicherte Outputs: werden nach den internen Löschkonzepten des Unternehmens behandelt; das Unternehmen ist hierfür als Verantwortlicher alleinzuständig.
- Bewerbungsdaten: Gemäß § 61b ArbGG i. V. m. § 15 AGG sind Bewerberdaten nach Abschluss des Auswahlverfahrens in der Regel nach 6 Monaten zu löschen, sofern keine andere gesetzliche Grundlage besteht.
- Beschäftigtendaten (Leistungsanalyse): Speicherdauer richtet sich nach dem Zweck der Verarbeitung und einschlägigen Aufbewahrungsvorschriften; in der Regel maximal für die Dauer des Beschäftigungsverhältnisses zuzüglich gesetzlicher Aufbewahrungsfristen.

Handlungsbedarf: Die genauen Speicherfristen sind im Verzeichnis der Verarbeitungstätigkeiten (Art. 30 DSGVO) festzulegen und mit Perplexity vertraglich abzusichern.

7. Funktionelle Beschreibung der Verarbeitung

Die Nutzung erfolgt über eine webbasierte SaaS-Oberfläche (https://www.perplexity.ai) oder – im Enterprise-Kontext – über eine organisationsverwaltete Enterprise-Umgebung. Nutzer (Beschäftigte des Unternehmens) geben Anfragen (Prompts) in das System ein, die ggf. personenbezogene Daten enthalten. Perplexity verarbeitet diese Eingaben mittels LLMs und gibt strukturierte Antworten aus.

Der technische Ablauf:

- Beschäftigte geben Prompts (Text, ggf. Dateien) in die Perplexity-Oberfläche ein.
- Perplexity sendet die Anfrage an seinen Backend-Dienst (gehostet auf AWS und/oder Microsoft Azure).

- Je nach Anfrage und gewähltem Modell wird die Anfrage an einen der integrierten LLM-Drittanbieter (OpenAI, Anthropic, Google, Meta/Llama unter anderem) weitergeleitet.
- Das Modell generiert eine Antwort; Perplexity kann zusätzlich Echtzeit-Websuche durchführen.
- Die Antwort wird an den Nutzer zurückgeliefert und ggf. in der Konversationshistorie gespeichert.

Bei der Leistungsanalyse werden die durch Perplexity aufbereiteten Daten an einen externen Dienstleister weitergegeben, der sie im Auftrag des Unternehmens auswertet und Berichte erstellt. Dieser Dienstleister ist als weiterer Auftragsverarbeiter gemäß Art. 28 DSGVO vertraglich einzubinden.

8. Beschreibung der Anlagen/Hard- und Software

Komponente	Beschreibung
Client-Endgeräte	Dienstliche Computer und ggf. mobile Endgeräte der Beschäftigten (betriebssystemseitig abzusichern)
Netzwerkinfrastruktur	Unternehmensnetzwerk (Firewall, VPN, TLS-Verschlüsselung bei Datenübertragung)
SaaS-Plattform	Perplexity AI Enterprise Pro/Max; Betrieb auf AWS und Microsoft Azure
LLM-Infrastruktur (Drittanbieter)	Server von OpenAI, Anthropic, Google, Meta, NVIDIA unter anderem, überwiegend in den USA
Browser-Applikation	Webbasierter Zugang; alternativ API-Anbindung möglich
Datensicherheitsmaßnahmen Perplexity	SOC-2-Type-II-Zertifizierung für Enterprise-Tier; Verschlüsselung in Transit (TLS) und at rest
Externer Dienstleister (Leistungsanalyse)	Eigene Infrastruktur gemäß AVV (separat zu spezifizieren)

9. Eingehaltene, gemäß Art. 40 DSGVO genehmigte Verhaltensregeln

Nach aktuellem Kenntnisstand sind für Perplexity AI keine nach Art. 40 DSGVO genehmigten Verhaltensregeln oder nach Art. 42 DSGVO ausgestellte Zertifizierungen vorhanden. Perplexity beruft sich auf die Einhaltung der DSGVO

sowie Compliance mit dem EU-U.S. Data Privacy Framework, was jedoch keine Genehmigung nach Art. 40 DSGVO darstellt. Das Fehlen eines anerkannten Zertifizierungsmechanismus ist im Rahmen der Risikoabwägung zu berücksichtigen.

II. Bewertung der Notwendigkeit und Verhältnismäßigkeit

1. Festgelegter Zweck

Die Verarbeitungszwecke sind in Abschnitt I.4 beschrieben und hinreichend bestimmt. Für die Anwendungsfälle Bewerbermanagement und Leistungsanalyse sind die Zwecke vorab schriftlich festzulegen und im VVT zu dokumentieren (Art. 30 DSGVO). Die Nutzungspolitik (z. B. eine KI-Nutzungsrichtlinie) muss den Beschäftigten mitgeteilt werden.

2. Eindeutiger Zweck

Die einzelnen Anwendungsfälle sind klar voneinander trennbar. Es ist jedoch sicherzustellen, dass keine Zweckvermischung stattfindet: Daten, die für die Korrespondenzunterstützung eingegeben wurden, dürfen nicht für die Leistungsanalyse verwendet werden.

Technische und organisatorische Maßnahmen (z. B. getrennte Arbeitsbereiche/„Spaces“ in Perplexity Enterprise) sind zu implementieren.

3. Legitimer Zweck

Alle genannten Verarbeitungszwecke sind grundsätzlich legitim im Sinne des Art. 6 DSGVO:

- Produktivitätssteigerung und Effizienz: berechtigtes Interesse des Unternehmens (Art. 6 Abs. 1 lit. f DSGVO)
- Bewerbermanagement: Erforderlichkeit zur Begründung eines Beschäftigungsverhältnisses (§ 26 Abs. 1 BDSG i. V. m. Art. 6 Abs. 1 lit. b DSGVO)
- Leistungsanalyse: Erforderlichkeit zur Durchführung des Beschäftigungsverhältnisses (§ 26 Abs. 1 BDSG); alternativ berechtigtes Interesse; Einwilligung als Rechtsgrundlage ist wegen des strukturellen Machtgefälles im Arbeitsverhältnis grundsätzlich problematisch.

4. Rechtmäßigkeit der Verarbeitung

Anwendungsfall	Rechtsgrundlage	Anmerkung
Texterstellung, Übersetzung, Grafikerstellung (ohne Personenbezug)	Art. 6 Abs. 1 lit. f DSGVO	Ggf. berechtigtes Interesse; kein eigenständiger Personenbezug
Korrespondenz-unterstützung (Kundendaten)	Art. 6 Abs. 1 lit. b oder f DSGVO	Vertragserfüllung oder berechtigtes Interesse; Informationspflicht prüfen
Bewerbermanagement	§ 26 Abs. 1 S. 1 BDSG i. V. m. Art. 6 Abs. 1 lit. b DSGVO	Erforderlichkeit ist zu dokumentieren; bei KI-gestützter Vorauswahl: Art. 22 DSGVO beachten
Leistungsanalyse Beschäftigte	§ 26 Abs. 1 BDSG ggf. i. V. m. Betriebsvereinbarung	Betriebsvereinbarung als empfohlene Rechtsgrundlage; Art. 22 DSGVO bei automatisierten Entscheidungen
Externer Dienstleister für Leistungsauswertung	Art. 28 DSGVO (eigenständiger AVV)	[Standort intern zu spezifizieren]

Kritischer Punkt – Art. 22 DSGVO: Sofern die KI-gestützte Leistungsanalyse Grundlage für Entscheidungen mit rechtlicher Wirkung oder erheblicher Beeinträchtigung für Beschäftigte ist (z. B. Gehaltserhöhung, Beförderung, Kündigung), greift das grundsätzliche Verbot automatisierter Einzelentscheidungen nach Art. 22 Abs. 1 DSGVO. Eine Ausnahme ist nur unter den Voraussetzungen des Art. 22 Abs. 2 DSGVO (Vertragserfüllung, gesetzliche Grundlage oder ausdrückliche Einwilligung) möglich. In jedem Fall sind die Rechte nach Art. 22 Abs. 3 DSGVO (menschliche Überprüfung, Einspruchsrecht) zu gewährleisten.

5. Angemessenheit der Verarbeitung

Die Verarbeitung ist für die genannten Zwecke grundsätzlich angemessen, sofern die spezifischen Risiken durch Schutzmaßnahmen adressiert werden. Der Einsatz einer generativen KI ist für Texterstellung und Übersetzung angemessen proportional zum angestrebten Effizienzgewinn. Bei der Leistungsanalyse und dem Bewerbermanagement muss die Verhältnismäßigkeit besonders sorgfältig geprüft werden, da erhebliche Eingriffe in Persönlichkeitsrechte möglich sind.

6. Erheblichkeit der Verarbeitung

Die Verarbeitung ist erheblich insbesondere bei:

- Verarbeitung von Bewerbungsunterlagen (personenbezogene und ggf. besonders schutzwürdige Daten)
- Leistungsanalyse von Beschäftigten (Profiling, Eingriff in Persönlichkeitsrechte, Potenzial für erhebliche Beeinträchtigung)
- Weitergabe von Kundendaten an einen US-amerikanischen Drittanbieter (Risiko des Vertrauensverlusts gegenüber Kunden)

Für weniger risikobehaftete Anwendungsfälle (Texterstellung ohne Personenbezug, Grafikerstellung) ist die Erheblichkeit gering.

7. Beschränktheit der Verarbeitung auf das notwendige Maß

Das Prinzip der Datensparsamkeit (Art. 5 Abs. 1 lit. c DSGVO) erfordert, dass Beschäftigte keine unnötigen personenbezogenen Daten in Prompts eingeben. Es sind klare Nutzerrichtlinien (KI-Nutzungsanweisung) zu erstellen, die

- die Eingabe von Namen, Adressen, besonderen Kategorien nach Art. 9 DSGVO untersagen, sofern nicht zwingend erforderlich,
- Pseudonymisierung von Betroffenen vor Eingabe vorschreiben und die
- den Umfang der für den jeweiligen Zweck zulässigen Dateneingabe konkret bestimmen.

8. Speicherbegrenzung

Das Unternehmen muss sicherstellen, dass …

- Konversationshistorien und Outputs regelmäßig gelöscht oder archiviert werden,
- Löschfristen für alle Anwendungsfälle festgelegt und technisch umgesetzt werden,
- Perplexity vertraglich zur Datenlöschung nach Vertragsende verpflichtet wird (bereits im DPA vorgesehen: Löschung innerhalb von 30 Tagen) und
- beim externen Dienstleister für Leistungsanalyse Löschfristen im AVV vereinbart werden

9. Generelle Information der betroffenen Personen

Das Unternehmen ist verpflichtet, alle betroffenen Personen über die Verarbeitung durch Perplexity zu informieren:

- Beschäftigte: Aktualisierung der Beschäftigteninformation (Art. 13 DSGVO); vorzugsweise als Anlage zur KI-Nutzungsrichtlinie
- Bewerber: Aktualisierung der Datenschutzerklärung für Bewerbungsverfahren mit ausdrücklichem Hinweis auf KI-Einsatz und etwaige automatisierte Verarbeitung
- Kunden und Vertragspartner: Prüfung und ggf. Ergänzung bestehender Datenschutzerklärungen

10. Information der betroffenen Personen bei Erhebung

Bei direkter Erhebung (z. B. Bewerbungsunterlagen, Kundenkommunikation) sind die Informationspflichten nach Art. 13 DSGVO vollständig zu erfüllen, einschließlich des Hinweises auf:

- den Empfänger Perplexity AI, Inc. (USA) als Auftragsverarbeiter
- die Drittlandübermittlung und die Schutzmaßnahmen (EU SCC)
- ggf. automatisierte Entscheidungsfindung und deren Logik (Art. 13 Abs. 2 lit. f DSGVO)

11. Information der betroffenen Personen, wenn die Daten nicht bei ihnen erhoben werden

Sofern personenbezogene Daten über Dritte in Prompts eingegeben werden (z. B. Kundendaten zur Unterstützung der Korrespondenz), die nicht direkt bei den Betroffenen erhoben wurden, sind die Informationspflichten nach Art. 14 DSGVO zu beachten. Die Umsetzbarkeit ist im Einzelfall zu prüfen; ggf. greift Art. 14 Abs. 5 lit. b DSGVO (unverhältnismäßiger Aufwand), wenn die Information im Widerspruch zu Art. 14 Abs. 5 DSGVO steht.

12. Auskunftsrecht der betroffenen Personen

Das Unternehmen muss sicherstellen, dass es Auskunftsersuchen (Art. 15 DSGVO) nachkommen kann. Dazu gehört die Fähigkeit, auf Anfrage Auskunft darüber zu erteilen,

- welche Daten einer Person in Perplexity eingegeben wurden,
- welche KI-gestützten Entscheidungen ggf. getroffen wurden.

Perplexity stellt Enterprise-Kunden Mechanismen zur Datenlöschung und Datenauskunft zur Verfügung; jedoch sind die internen Prozesse des Unternehmens auf die Erfüllung von Auskunftsersuchen auszurichten.

13. Recht auf Datenübertragbarkeit

Das Recht auf Datenübertragbarkeit (Art. 20 DSGVO) ist bei automatisierter Verarbeitung personenbezogener Daten auf Grundlage einer Einwilligung oder eines Vertrags zu beachten. Im vorliegenden Kontext ist dies primär bei der Leistungsanalyse relevant, soweit diese auf Einwilligung oder Vertrag beruht.

Perplexity stellt entsprechende Export-Funktionen bereit; die interne Umsetzung ist zu dokumentieren.

14. Auftragsverarbeiter

Perplexity AI, Inc. ist als Auftragsverarbeiter gemäß Art. 28 DSGVO einzubinden. Das Data Processing Addendum (DPA) von Perplexity ist für Enterprise-Kunden verfügbar und inkorporiert EU-Standardvertragsklauseln (SCC Modul 2). Folgende Punkte sind vertraglich sicherzustellen:

- Verarbeitung nur nach dokumentierten Weisungen des Unternehmens
- Kein Einsatz der Daten für KI-Modelltraining (im Enterprise-DPA zugesagt)
- Benachrichtigung bei Datenschutzverletzungen
- Unterstützung bei Betroffenenrechten und DSFA
- Vollständige Liste der Sub-Auftragsverarbeiter (Perplexity veröffentlicht diese unter trust.perplexity.ai)

Der externe Dienstleister für die Leistungsauswertung ist ebenfalls als eigenständiger Auftragsverarbeiter mit einem separaten AVV einzubinden.

15. Schutzmaßnahmen bei der Übermittlung in Drittländer

Perplexity AI, Inc. hat seinen Sitz in den USA. Die Datenübermittlung in die USA erfolgt auf folgender Basis:

- EU-Standardvertragsklauseln (SCC Modul 2 – Controller to Processor) gemäß Beschluss 2021/914 der Europäischen Kommission
- EU-U.S. Data Privacy Framework (DPF): Perplexity ist nach dem DPF zertifiziert.
- Für LLM-Subprozessoren (OpenAI, Anthropic, Google unter anderem) gelten Processor-to-Processor SCCs (Modul 3).

Als zuständige Aufsichtsbehörde für die SCCs wurde die Irish Data Protection Commission (DPC) bestimmt; maßgebliches Recht ist irisches Recht. Das Unternehmen muss ein Transfer Impact Assessment (TIA) durchführen, in dem die Risiken der Übermittlung in die USA bewertet werden (Zugriffsmöglichkeit von US-Behörden, CLOUD Act, FISA Section 702).

16. Vorherige Konsultation der zuständigen Datenschutzaufsichtsbehörde

Gemäß Art. 36 DSGVO ist eine vorherige Konsultation der Datenschutzaufsichtsbehörde (in NRW z. B. Landesbeauftragte für Datenschutz und Informationsfreiheit NRW – LDI NRW) erforderlich, wenn die DSFA ergibt, dass die geplante Verarbeitung ein hohes Risiko zur Folge hätte und das Unternehmen keine ausreichenden Maßnahmen zur Eindämmung dieses Risikos getroffen hat. Diese Entscheidung ist nach Abschluss der DSFA und Implementierung der Abhilfemaßnahmen zu treffen. Für die Teilbereiche Bewerbermanagement und Leistungsanalyse ist dies ernsthaft zu prüfen, sofern automatisierte Entscheidungen mit erheblicher Wirkung vorgesehen sind.

III. Risiken

1. Physische, materielle oder immaterielle Schäden

Risikobeschreibung: Durch fehlerhafte, verzerrte oder diskriminierende KI-Outputs können Bewerber oder Beschäftigte ungerechtfertigte Benachteiligungen erleiden (materiell: entgangene Stellenangebote, Gehaltseinbußen; immateriell: Ehrverletzung, psychische Belastung). Bei Datenpannen auf der Infrastruktur von Perplexity oder seinen Sub-Prozessoren können sensible Daten (Bewerbungsunterlagen, Leistungsbeurteilungen) in die Hände Unbefugter gelangen.

Wahrscheinlichkeit: mittel (insbesondere bei Leistungsanalyse und Bewerbermanagement)

Schwere: hoch

Gesamtrisiko: hoch

2. Verlust der Kontrolle über personenbezogene Daten

Risikobeschreibung: Mit der Übermittlung personenbezogener Daten an Perplexity als SaaS-Anbieter verliert das Unternehmen die direkte Kontrolle über die Datenverarbeitung. Die Einbindung mehrerer LLM-Drittanbieter (OpenAI, Anthropic, Google unter anderem) erweitert die Datenweitergabekette und schränkt die Kontrollmöglichkeiten weiter ein. Perplexity gewährt für Model-Provider lediglich eine Benachrichtigungspflicht, aber kein Widerspruchsrecht.

Wahrscheinlichkeit: mittel bis hoch

Schwere: hoch

Gesamtrisiko: hoch

3. Diskriminierung

Risikobeschreibung: LLMs können systemische Verzerrungen (Bias) reproduzieren, die zu einer diskriminierenden Behandlung von Bewerbern oder Beschäftigten führen können, etwa nach Geschlecht, ethnischer Herkunft, Alter oder anderen geschützten Merkmalen. Bei der Analyse von Bewerbungsunterlagen oder Leistungsdaten besteht ein erhöhtes Risiko der mittelbaren Diskriminierung.

Wahrscheinlichkeit: mittel (abhängig von Nutzung und Eingaben)

Schwere: hoch (AGG-Haftungsrisiko, gesellschaftliche Beeinträchtigung)

Gesamtrisiko: hoch (insbesondere bei Bewerbermanagement und Leistungsanalyse)

4. Identitätsdiebstahl oder -betrug

Risikobeschreibung: Bei einer Datenpanne aufseiten von Perplexity oder seiner Sub-Prozessoren könnten personenbezogene Daten (Kontaktdaten, Be-

werbungsunterlagen, Leistungsdaten) für Identitätsbetrug missbraucht werden. Das Risiko wird durch die US-amerikanische Rechtsordnung erhöht, die behördliche Zugriffe auf gespeicherte Daten ermöglicht (CLOUD Act, FISA 702).

Wahrscheinlichkeit: gering bis mittel

Schwere: mittel bis hoch

Gesamtrisiko: mittel

5. Finanzielle Verluste

Risikobeschreibung: Fehlgeleitete Entscheidungen auf Basis fehlerhafter KI-Outputs (z. B. falsche Leistungsbewertungen, die zu ungerechtfertigten Kündigungen führen) können erhebliche Kosten verursachen (Schadensersatzklagen, Bußgelder nach Art. 83 DSGVO, Prozesskosten). Bußgelder der Aufsichtsbehörde können bei schwerwiegenden DSGVO-Verstößen bis zu 4 % des weltweiten Jahresumsatzes betragen.

Wahrscheinlichkeit: gering bis mittel

Schwere: hoch

Gesamtrisiko: mittel

6. Unbefugte Aufhebung der Pseudonymisierung

Risikobeschreibung: Sofern Beschäftigte Daten pseudonymisiert in Prompts eingeben, besteht das Risiko, dass durch die Kombination von Prompts mit anderen im System verfügbaren Informationen oder durch Inferenz eine Re-Identifizierung stattfindet. Perplexity greift auf aktuelle Webinformationen zurück, was das Risiko der Deanonymisierung erhöht.

Wahrscheinlichkeit: mittel

Schwere: mittel

Gesamtrisiko: mittel

7. Rufschädigung

Risikobeschreibung: Bekanntwerden einer datenschutzwidrigen KI-Nutzung (insbesondere im HR-Bereich) kann zu Reputationsschäden gegenüber Kunden, Bewerbern und der Öffentlichkeit führen. Kunden, deren Daten ohne deren Wissen in US-amerikanische KI-Systeme eingegeben wurden, könnten das Vertrauen in das Unternehmen verlieren.

Wahrscheinlichkeit: mittel (bei unzureichender Transparenz)

Schwere: mittel bis hoch

Gesamtrisiko: mittel

8. Verlust der Vertraulichkeit bei Berufsgeheimnissen

Risikobeschreibung: Die Eingabe von vertraulichen Geschäftsinformationen, Vertragsdetails oder kundenspezifischen Daten in Perplexity könnte zur Offenbarung von Geschäftsgeheimnissen führen. Obwohl Perplexity im Enterprise-Tarif keine Daten für KI-Training verwendet, verbleiben Daten auf den Servern von Drittanbietern (AWS, Microsoft Azure, LLM-Anbieter). US-Behörden haben unter bestimmten Voraussetzungen Zugriffsrechte (CLOUD Act).

Wahrscheinlichkeit: mittel

Schwere: mittel bis hoch

Gesamtrisiko: mittel

9. Erhebliche wirtschaftliche oder gesellschaftliche Nachteile

Risikobeschreibung: Besonders gravierend bei der Leistungsanalyse: KI-gestützte Leistungsbewertungen, die als Grundlage für Entscheidungen über Weiterbeschäftigung, Kündigung oder Beförderung dienen, können zu erheblichen wirtschaftlichen Nachteilen für Beschäftigte führen. Fehlbewertungen können Karrieren und Existenzen gefährden. Gesellschaftlich ist das Potenzial für strukturelle Benachteiligung von Arbeitnehmergruppen problematisch.

Wahrscheinlichkeit: mittel (abhängig von der konkreten Nutzungsform)

Schwere: sehr hoch

Gesamtrisiko: hoch

Risikoübersicht:

Risiko	Wahrschein-lichkeit	Schwere	Gesamt-risiko	Priorität
Physische/materielle/ immaterielle Schäden	Mittel	Hoch	Hoch	1
Verlust der Datenkontrolle	Mittel bis hoch	Hoch	Hoch	1
Diskriminierung	Mittel	Hoch	Hoch	1
Wirtschaftliche/ gesellschaftliche Nachteile	Mittel	Sehr hoch	Hoch	1
Finanzielle Verluste	Gering bis mittel	Hoch	Mittel	2
Rufschädigung	Mittel	Mittel bis hoch	Mittel	2
Verlust der Vertraulichkeit	Mittel	Mittel bis hoch	Mittel	2
Unbefugte Re-Identifizierung	Mittel	Mittel	Mittel	3
Identitätsdiebstahl/-betrug	Gering bis mittel	Mittel bis hoch	Mittel	3

IV. Abhilfemaßnahmen

1. Minimierung der Verarbeitung personenbezogener Daten

Maßnahme	Verant-wortlicher	Priorität	Umset-zungsfrist
KI-Nutzungsrichtlinie: Verbot der Eingabe nicht erforderlicher personenbezogener Daten in Prompts; Pflicht zur Pseudo-nymisierung vor der Eingabe	KI-Beauf-tragter, DSB	Hoch	Vor Go-Live
Rollenbasiertes Zugriffskonzept: Nur berechtigte Mitarbeiter dürfen Bewerberdaten bzw. Leistungsanalyse-daten in das System eingeben.	IT, HR	Hoch	Vor Go-Live
Anwendungsfall-Segmentierung: technische Trennung der Arbeitsbereiche (z. B. separate Enterprise-Spaces) für Bewerbermanagement, Leistungsanalyse und allgemeine Nutzung	IT, KI-Beauf-tragter	Hoch	Vor Go-Live
Datenminimierende Prompt-Vorlagen: Bereitstellung vorgefertigter Prompt-Templates, die auf minimale Personen-daten ausgerichtet sind	KI-Beauf-tragter	Mittel	Binnen 3 Monaten

2. Schnellstmögliche Pseudonymisierung personenbezogener Daten

Maßnahme	Verant-wortlicher	Priorität	Umset-zungsfrist
Pseudonymisierungspflicht vor Eingabe in Perplexity: Nutzung von Kennziffern oder Pseudonymen statt echter Namen bei Leistungsanalyse und Bewerberma-nagement; Mapping-Tabellen sicher im Unternehmen aufbewahren	DSB, HR, IT	Hoch	Vor Go-Live
Technische Unterstützung: Bereitstellung eines internen Pseudonymisierungstools oder eines Word-/Excel-Templates für die Datenvorbereitung	IT	Mittel	Binnen 3 Monaten

Kontrollmechanismus: stichprobenartige Überprüfung von Konversationshistorien auf unzulässige Klardaten durch den DSB oder KI-Beauftragten	DSB	Mittel	Laufend

3. Transparenz in Bezug auf die Funktionen und die Verarbeitung personenbezogener Daten

Maßnahme	**Verantwortlicher**	**Priorität**	**Umsetzungsfrist**
Aktualisierung Datenschutzerklärung (Website, Bewerbungsportal, Beschäftigteninformation) mit ausdrücklichem Hinweis auf KI-Nutzung und Drittlandübermittlung	DSB, Rechtsabteilung	Hoch	Vor Go-Live
Mitarbeiterinformation: Schulung und schriftliche Information aller Perplexity-Nutzer über zulässige und unzulässige Nutzungsszenarien	KI-Beauftragter, HR	Hoch	Vor Go-Live
Bewerberinformation: klarer Hinweis in Stellenausschreibungen und Datenschutzerklärung auf KI-Einsatz im Bewerbungsverfahren; Information über Recht auf menschliche Überprüfung (Art. 22 Abs. 3 DSGVO)	HR, DSB	Hoch	Vor Go-Live
Transfer Impact Assessment (TIA): dokumentiertes TIA zur US-Drittlandübermittlung	DSB, KI-Beauftragter	Hoch	Vor Go-Live
Betriebsratseinbindung: Abschluss einer Betriebsvereinbarung nach § 87 Abs. 1 Nr. 6 BetrVG (sofern Betriebsrat vorhanden) vor Einführung für Anwendungsfälle mit Überwachungspotenzial	HR, Geschäftsführung	Hoch	Vor Go-Live

4. Überwachung der Verarbeitung personenbezogener Daten durch die betroffenen Personen

Maßnahme	Verantwortlicher	Priorität	Umsetzungsfrist
Beschwerdemechanismus: Einrichtung eines internen Kanals, über den Beschäftigte und Bewerber Bedenken zur KI-gestützten Verarbeitung äußern können	DSB, HR	Hoch	Vor Go-Live
Recht auf menschliche Überprüfung (Art. 22 Abs. 3 DSGVO): sicherstellen, dass bei Entscheidungen auf Basis KI-gestützter Leistungsanalyse oder Bewerberbewertung eine menschliche Überprüfung garantiert ist	HR, Geschäftsführung	Hoch	Vor Go-Live
Prozess für Auskunftsersuchen: Einrichtung eines dokumentierten Prozesses für Auskunftsersuchen bezüglich KI-gestützter Verarbeitungen	DSB	Mittel	Binnen 1 Monat
Löschanträge: Sicherstellung, dass individuelle Löschanträge bezüglich in Perplexity eingegebener Daten innerhalb der gesetzlichen Fristen bearbeitet werden können (Nutzung der Enterprise-Admin-Funktionen)	IT, DSB	Mittel	Binnen 1 Monat

5. Datensicherheitsmaßnahmen

Maßnahme	Verantwortlicher	Priorität	Umsetzungsfrist
Abschluss Enterprise-AVV (DPA) mit Perplexity vor Produktivsetzung	Rechtsabteilung, DSB	Hoch	Vor Go-Live
Prüfung und Abschluss des AVV mit dem externen Leistungsanalyse-Dienstleister	Rechtsabteilung, DSB	Hoch	Vor Go-Live
Verifikation der Sub-Prozessoren-Liste (trust.perplexity.ai) und Bewertung der datenschutzrechtlichen Geeignetheit	DSB	Hoch	Vor Go-Live

Nutzerbeschränkung: Single Sign-On (SSO) und MFA-Pflicht für alle Perplexity-Konten	IT	Hoch	Vor Go-Live
Netzwerksicherheit: Zugriff auf Perplexity ausschließlich über das Unternehmensnetzwerk (VPN) oder mit MDM-kontrollierten Endgeräten	IT	Hoch	Vor Go-Live
Datenspeicherung deaktivieren: Konfiguration der Enterprise-Einstellungen zur minimalen Datenspeicherung (ggf. Deaktivierung der Konversationshistorie für risikobehaftete Anwendungsfälle)	IT, KI-Beauftragter	Hoch	Vor Go-Live
Regelmäßige Sicherheitsaudits: jährliche Überprüfung der TOM von Perplexity durch Auditbericht (gemäß DPA Section 9)	DSB	Mittel	Jährlich
Incident-Response-Plan: Einbindung von Perplexity-bezogenen Datenpannen in das bestehende Datenpannen-Meldeverfahren (Art. 33/34 DSGVO)	DSB, IT	Mittel	Binnen 1 Monat
EU-AI-Act-Compliance-Prüfung für Hochrisiko-Anwendungsfälle (Bewerberauswahl, Leistungsbewertung): Dokumentation der menschlichen Aufsicht, Risikomanagementsystem, Aufbewahrung von Protokollen	KI-Beauftragter, DSB	Hoch	Vor Go-Live

V. Berücksichtigung von Datenschutzinteressen

1. Stellungnahme der Datenschutzaufsichtsbehörde

Eine Konsultation der Landesbeauftragten für Datenschutz und Informationsfreiheit NRW (LDI NRW) nach Art. 36 DSGVO ist bislang nicht erfolgt. Nach Implementierung der in Abschnitt IV beschriebenen Abhilfemaßnahmen ist zu prüfen, ob das Restrisiko auf ein akzeptables Maß reduziert werden konnte. Sollte dies insbesondere für die Anwendungsfälle Leistungsanalyse und Bewerbermanagement nicht abschließend bejaht werden können, ist eine vorherige Konsultation nach Art. 36 DSGVO einzuleiten. Die LDI NRW hat 8 Wochen Stellungnahmefrist (verlängerbar um weitere 6 Wochen).

Die DSK hat im Rahmen ihrer Orientierungshilfe „KI und Datenschutz“ (2024) klargestellt, dass beim Einsatz von KI-Anwendungen vielfach ein hohes Risiko vorliegt und daher eine DSFA durchzuführen ist. Aufsichtsbehörden stehen Arbeitnehmerdaten-Verarbeitungen mittels KI besonders kritisch gegenüber.

2. Stellungnahme des Datenschutzbeauftragten des Verantwortlichen

Der betriebliche Datenschutzbeauftragte wurde gemäß Art. 35 Abs. 2 DSGVO in die Erstellung dieser DSFA eingebunden. Nachfolgende Stellungnahme ist vor endgültiger Freigabe der DSFA einzuholen und dieser als Anlage beizufügen:

[Platzhalter: Formelle Stellungnahme des DSB einfügen – inklusive Empfehlung bezüglich vorheriger Konsultation nach Art. 36 DSGVO, Bewertung der Rechtsgrundlagen, Hinweise zu ggf. fehlenden Informationen im Sachverhalt]

Der DSB empfiehlt insbesondere:

- Die Zwecke der Leistungsanalyse präzise zu definieren und zu dokumentieren, ob und inwiefern automatisierte Entscheidungen im Sinne des Art. 22 DSGVO vorgesehen sind
- Den Abschluss einer Betriebsvereinbarung für die Anwendungsfälle Leistungsanalyse und ggf. Bewerbermanagement voranzutreiben
- Das Transfer Impact Assessment (TIA) für die USA-Übermittlung zu erstellen
- Einen vollständigen AVV mit Perplexity und dem externen Leistungsanalyse-Dienstleister vor Go-Live abzuschließen

3. Stellungnahme betroffener Personen

Art. 35 Abs. 9 DSGVO sieht vor, dass die Ansichten der betroffenen Personen oder ihrer Vertreter eingeholt werden sollen, wo angebracht, ohne die Interessen des Unternehmens zu schädigen.

- Beschäftigte: Bei Vorhandensein eines Betriebsrats ist dieser der institutionelle Vertreter der Beschäftigten. Seine zwingenden Mitbestimmungsrechte nach § 87 Abs. 1 Nr. 6 BetrVG decken die Anhörungspflicht gemäß Art. 35 Abs. 9 DSGVO mit ab. Eine Betriebsvereinbarung sollte die Mitarbeiterrechte bei KI-gestützter Leistungsbeurteilung sowie die zulässigen Nutzungsszenarien konkret regeln.

- Bewerber: Da Bewerber naturgemäß vor ihrer Bewerbung nicht eingebunden werden können, ist eine transparente Vorausinformation (Datenschutzerklärung, Stellenanzeige) als Äquivalent zu behandeln.
- Kunden und Vertragspartner: Eine direkte Anhörung ist aufgrund der Anzahl und Natur der Beziehungen nicht praktikabel. Stattdessen sind Datenschutzerklärungen und vertragliche Klauseln zu aktualisieren.

Gesamtergebnis und Freigabeentscheidung

Aktueller Risikostand (ohne Abhilfemaßnahmen): hoch

Erwarteter Risikostand nach Implementierung aller Abhilfemaßnahmen: mittel (für allgemeine Nutzung)/mittel bis hoch (für Bewerbermanagement und Leistungsanalyse; abhängig von der konkreten Ausgestaltung)

Entscheidung	**Unterschrift**	**Datum**
Datenschutzbeauftragter (Stellungnahme nach Art. 35 Abs. 2 DSGVO):		
KI-Beauftragter (Prüfung EU AI Act-Compliance):		
Geschäftsführung (Freigabeentscheidung):		

Hinweis: Diese DSFA ist regelmäßig zu überprüfen und zu aktualisieren, insbesondere bei wesentlichen Änderungen der Verarbeitung (z. B. Erweiterung der Nutzungsfälle, Wechsel des Perplexity-Tarifs, Änderungen des DPA oder der Sub-Prozessoren-Liste). Art. 35 Abs. 11 DSGVO schreibt eine regelmäßige Überprüfung vor.

Ist mit dieser KI-generierten DSFA z. B. „Einführung von Perplexity als SaaS“ jetzt die ganze Arbeit getan? Nein, sicherlich nicht. Ist die KI-generierte DSFA vollständig und fehlerfrei? Vermutlich auch nicht, aber sie stellt einen sehr guten Entwurf als Orientierungshilfe dar. Entscheidend ist und bleibt die menschliche Überprüfung anhand eigener Expertise.

DATENSCHUTZGRUNDVERORDNUNG (DSGVO)

Die Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27.04.2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG, kurz als Datenschutzgrundverordnung (DSGVO) bezeichnet, gilt seit dem 25.05.2018 europaweit für den Schutz personenbezogener Daten. Sie stärkt die Rechte natürlicher Personen und harmonisiert die Datenschutzregeln weitgehend; sie enthält jedoch auch einige sogenannte Öffnungsklauseln, die es den nationalen Gesetzgebern erlauben, eigene Regeln zu etablieren (mit denen die Schutzziele der DSGVO jedoch nicht unterlaufen werden dürfen). Ihre Kerninhalte sind:

- **Rechtsgrundlagen:** Verarbeitung nur auf Basis definierter Rechtsgrundlagen (z. B. Einwilligung, Vertrag, Gesetz, berechtigte Interessen, vgl. Art. 6 DSGVO)
- **Betroffenenrechte:** Rechte der Betroffenen z. B. auf Auskunft, Berichtigung, Löschung, Einschränkung, Datenübertragbarkeit oder Widerspruch (Art. 12 bis 23, 7, 77 DSGVO)
- **Prinzipien der Verarbeitung:** Rechtmäßigkeit, Treu und Glauben, Transparenz, Zweckbindung, Datenminimierung, Richtigkeit, Speicherbegrenzung, Integrität und Vertraulichkeit, Rechenschaftspflicht (Art. 5 DSGVO)
- Datenschutz durch **Technikgestaltung** („Privacy by design") und durch **Voreinstellung** („Privacy by default") nach Art. 25 DSGVO
- **Dokumentation:** Verzeichnis von Verarbeitungstätigkeiten (Art. 30 DSGVO), Beschreibung der technischen und organisatorischen Maßnahmen (TOM) (Art. 32 DSGVO)
- **Meldepflichten:** Datenschutzverletzungen sind binnen 72 Stunden an die Aufsichtsbehörde zu melden (Art. 33 DSGVO) sowie ggf. auch an die Betroffenen (Art. 34 DSGVO).

Die Grundsätze des Datenschutzrechts (Art. 5 DSGVO)

Alle zentralen Grundsätze aus Art. 5 DSGVO müssen bei der Verarbeitung personenbezogener Daten grundsätzlich eingehalten werden; zudem muss deren Einhaltung nachgewiesen werden können. Dies gilt auch für Datenverarbeitungen mittels KI.

Es gibt verschiedene Berührungspunkte zwischen der DSGVO und der KI-Verordnung (KI-VO):

Anforderung	Hochrisiko-KI gemäß KI-VO	DSGVO
Dokumentation	Erfassen von Hochrisiko-KI-Systemen zur Konformitäts-bewertung (Art. 43, Anhang VII Nr. 3 KI-VO)	VVT/TOM (Art. 30, 32 DSGVO)
Transparenz	Hochrisiko-KI-Systeme am Arbeitsplatz (Art. 26 Abs. 7 KI-VO); bei Chatbots, Deepfakes etc. (Art. 50 KI-VO)	Pflichtinformationen, Recht auf Auskunft (Art. 13, 14, 15 DSGVO)
Risikobewertung	Risikomanagementsystem (Art. 9 KI-VO)	TOM, Datenpanne, DSFA (Art. 32, 33, 34, 35, 36 DSGVO)
Managementsystem	Risikomanagement-/QM-System (Art. 9, 1 KI-VO7)/KI-Management-System	Datenschutz-Management-System (Art. 5, 24, 30 DSGVO)
Meldung von Vorfällen	schwerwiegende Vorfälle (Art. 9, 17, 73 KI-VO)	Datenpanne (Art. 33, 34 DSGVO)
Rechenschaftspflicht	Art. 17, ErwGr 27, 177 KI-VO	Art. 5 Abs. 2 DSGVO
Zweckbindung/ -bestimmung	Art. 3 Nr. 12 KI-VO	Art. 5 Abs. 1 lit. b) DSGVO
DSFA	insbesondere Art. 26 Abs. 9 KI-VO	Art. 35, 36 DSGVO

Die Datenschutzkonferenz (DSK) hat sich bereits in ihrer sogenannten „Hambacher Erklärung zur künstlichen Intelligenz“ vom 03.04.2019 zu KI geäußert. Darin fordert die DSK Folgendes: Die KI

- darf Menschen nicht zum Objekt machen,
- darf nur für verfassungsrechtlich legitimierte Zwecke eingesetzt werden und das Zweckbindungsgebot nicht aufheben,

- muss transparent, nachvollziehbar und erklärbar sein,
- muss Diskriminierungen vermeiden,
- muss den Grundsatz der Datenminimierung beachten,
- braucht Verantwortlichkeit,
- benötigt technische und organisatorische Standards und
- ihre Entwicklung bedarf der Steuerung.

In der „Checkliste zum Einsatz LLM-basierter Chatbots" des Hamburgischen Beauftragten für Datenschutz und Informationssicherheit vom 13.11.2023 werden insbesondere folgende Punkte herausgestellt:

- Compliance-Regelungen vorgeben
- Datenschutzbeauftragte einbinden
- Bereitstellung eines Funktions-Accounts
- Sichere Authentifizierung
- Keine Eingabe personenbezogener Daten
- Keine Ausgabe personenbezogener Daten
- Vorsicht bei personenbeziehbaren Daten
- Opt-out des KI-Trainings
- Opt-out der History
- Ergebnisse auf Richtigkeit prüfen
- Ergebnisse auf Diskriminierung überprüfen
- Keine automatisierte Letztentscheidung
- Beschäftigte sensibilisieren
- Datenschutz ist nicht alles
- Weitere Entwicklung verfolgen

Das Papier „The Bridge Blueprint – Thesen zur einheitlichen Anwendung von Datenschutz- und KI-Regulierung beim KI-Einsatz" vom Herbst 2025 (Entwurfsversion) wurde von insgesamt vier Personen aus den Datenschutzaufsichtsbehörden Hamburg und Schleswig-Holstein verfasst. Es soll eine „Blaupause" für eine „gol-

dene Brücke“ zwischen DSGVO und KI-Nutzung liefern und enthält daher wertvolle Lösungsansätze für praxisrelevante Probleme:

- Stellt der Grundsatz der Datenminimierung ein Hindernis für den KI-Einsatz dar?

Nein, da alle für den Zweck der Verarbeitung notwendigen Daten verarbeitet werden dürfen, insbesondere soweit dies der Erfüllung von Pflichten zum Schutz Betroffener dient.

- Stellt das Recht, „nicht einer ausschließlich auf einer automatisierten Verarbeitung beruhenden Entscheidung unterworfen zu werden“ (Art. 22 Abs. 1 DSGVO), ein Hindernis für den KI-Einsatz dar?

Nein, durch die Umsetzung der verbindlichen Anforderungen der KI-Verordnung, unter anderem für aussagekräftige Transparenz, verpflichtende menschliche Aufsicht und robuste Überprüfbarkeit durch Protokollierung, gibt es einen rechtlich verbindlichen Standard für sichere und nachprüfbare automatisierte Systeme, der somit Art. 22 DSGVO erfüllen kann.

- Können die berechtigten Interessen gemäß Art. 6 Abs. 1 UAbs. 1 lit. f) DSGVO als Rechtsgrundlage für die Verarbeitung personenbezogener Daten in/mit KI dienen?

Ja, jeder für den KI-Einsatz Verantwortliche hat ein berechtigtes Interesse daran, Daten zu verarbeiten, um die Einhaltung der KI-Verordnung zu gewährleisten. Dies umfasst die Prüfung, ob ein System als hochriskant einzustufen ist, unter ein Verbot fällt oder Transparenzpflichten unterliegt – eine Bewertung, die für jedes KI-System erforderlich ist.

- Kann ein „erhebliches öffentliches Interesse“ gemäß Art. 9 Abs. 2 lit. g) DSGVO durch die KI-Verordnung bestehen?

Ja, um dafür zu sorgen, dass ein KI-System z. B. nicht aufgrund des Gesundheitszustands oder der ethnischen Herkunft diskriminiert, müssen Maßnahmen ergriffen werden. Das umfasst auch, wenn unbedingt erforderlich, die gezielte Verarbeitung solcher Daten, um ebenjene Risiken zu testen, zu messen und zu verringern.

- Ist die DSFA gemäß Art. 35, 36 DSGVO ein sinnvolles Risiko-Instrument zur Nutzung von KI?

Ja, die wichtigsten Risiken, auf denen der Fokus liegen sollte, sind gesellschaftliche und individuelle Schäden, einschließlich des Potenzials für Fehlinformationen und Deepfakes, Falschdarstellung, Manipulation und Cybersicherheitsbedrohungen,

die ein KI-System kompromittieren können. Ein zentrales Risiko ist die unbeabsichtigte Preisgabe von Daten, wobei hohe Risiken für betroffene Personen insbesondere aus schädlichen oder unrichtigen Daten entstehen.

In der Checkliste „Datenschutzkonforme künstliche Intelligenz" des Bayerischen Landesamts für Datenschutzaufsicht (BayLDA) vom 24.01.2024 (Version 0.9) werden hingegen folgende Punkte behandelt:

- Festlegung und Dokumentation, welche Art von Anwendung mittels KI-Technologie realisiert werden soll
- Festlegung, ob ein eigenes KI-Modell in einer eigenen KI-Anwendung betrieben oder eine KI-Anwendung bei einem KI-Anbieter werden soll
- Festlegung, ob das KI-Modell an sich personenbeziehbar ist (falls ja, muss die Rechtsgrundlage für die Verarbeitung auf dem KI-Modell geprüft werden)
- Aufnahme des Einsatzes einer KI-Anwendung in das Verzeichnis der Verarbeitungstätigkeiten (VVT)
- Prüfung und Dokumentation, ob eine DSFA nach Art. 35 DSGVO durchgeführt werden muss
- Bei Verpflichtung der Durchführung einer DSFA nach Art. 35 DSGVO ist, wenn vorhanden, der DSB einzubinden.
- Festlegung und Dokumentation, welche Kategorien an personenbezogenen Daten als Eingabedaten in eine KI-Anwendung gegeben werden sollen
- Bei der Eingabe von besonderen personenbezogenen Daten nach Art. 9 DSGVO in eine KI-Anwendung ist eine Einwilligung einzuholen (oder die Ausnahmen des Art. 9 Abs. 2 DSGVO prüfen)
- Erstellung eines Risikomodells, mit dem die Datenschutzrisiken im spezifischen Einsatzszenario der KI-Anwendung abgebildet und nachgewiesen werden können
- Berechnung und Dokumentation von Metriken aus dem Risikomodell, mit denen eine angemessene Eindämmung der Datenschutzrisiken bei Verwendung üblicher Eingabedaten und der daraus resultierenden Ausgabedaten nachgewiesen werden kann (Art. 5 Abs. 2 DSGVO)
- Festlegung und Dokumentation des Umgangs mit Risiken aus dem Risikomodell, die sich insbesondere aus der fehlerhaften Verlässlichkeit ergeben

- Umsetzung der Informationspflichten nach Art. 12 ff. DSGVO
- Sicherstellung, dass Auskunftsersuchen nach Art. 15 DSGVO auch bei Anfragen zum Einsatz von KI-Anwendungen im Datenschutzmanagement berücksichtigt werden
- Bei konkretem Auskunftsersuchen nach Art. 15 DSGVO in Bezug auf ein personenbeziehbares KI-Modell wird – je nach KI-Technologie – geprüft, ob personenbezogene Daten im KI-Modell direkt ermittelbar sind oder ob diese eventuell nur mit Zusatzinformationen (z. B. konkreter Prompt bei großem Sprachmodell) aus einem KI-Modell abgeleitet werden können.
- Sicherstellung, dass Betroffenenrechte zur Berichtigung nach Art. 16 DSGVO, zur Löschung nach Art. 17 DSGVO, nach Einschränkung der Verarbeitung nach Art. 18 DSGVO, nach Datenübertragbarkeit nach Art. 20 DSGVO und des Widerspruchs nach Art. 21 DSGVO in Bezug auf KI auch im Datenschutzmanagement berücksichtigt werden
- Bei einem Löschersuchen nach Art. 17 DSGVO in Bezug auf ein personenbeziehbares KI-Modell wird – je nach KI-Technologie – geprüft, ob personenbezogene Daten im KI-Modell direkt ermittelbar sind oder ob diese eventuell nur mit Zusatzinformationen (z. B. konkreter Prompt bei großem Sprachmodell) auf einem KI-Modell abgeleitet werden können
- Sicherstellen, dass der Datenempfänger eines KI-as-a-Service-Szenarios sowohl mögliche Eingabedaten als auch Ausgabedaten von KI-Modellen und KI-Anwendungen nicht für eigene Zwecke verwendet (z. B. Nachtraining, Filterverbesserung, Marketing) oder zumindest bei einer Zweckänderung geeignete Rechtsgrundlagen und Informationspflichten eingehalten werden
- Vor dem Einsatz einer KI-Anwendung findet ein (zu dokumentierender) Freigabetest statt.
- Der Einsatz von KI-Anwendungen wird in das Schulungsprogramm zum Datenschutz aufgenommen.
- Der Einsatz von KI-Anwendungen ist zum Nachweis einer angemessenen Risikoeindämmung zu protokollieren.
- Bei der Protokollierung der Nutzung von KI-Anwendungen sind personenbezogene Daten, die einen Rückschluss auf einen konkreten Mitarbeiter ermöglichen, nur in pseudonymer Form mit gesicherten Identifikationsverfahren gespeichert.

- Findet eine Anpassung des KI-Modells im laufenden Betrieb einer KI-Anwendung statt, dann ist dies bei einer Risikobeurteilung und bei Freigabetests besonders zu berücksichtigen.
- Der Einsatz von KI-Anwendungen samt Datenschutz-Risikomodell ist zu dokumentieren und regelmäßig unter Berücksichtigung des Verzeichnisses der Verarbeitungstätigkeiten auf Aktualität und Vollständigkeit zu prüfen.

Im Diskussionspapier „Rechtsgrundlagen im Datenschutz beim Einsatz von künstlicher Intelligenz" des Landesbeauftragten für Datenschutz und Informationsfreiheit Baden-Württemberg vom 17.10.2024 (Version 2.0) findet sich unter anderem folgende Checkliste:

1. Welche Phase der Verarbeitung von Daten im Zusammenhang mit KI unterliegt der rechtlichen Bewertung?
2. Werden personenbezogene Daten im Anwendungsbereich der DSGVO verarbeitet? Oder werden anonyme Daten verarbeitet, die zu personenbezogenen Daten werden können?
3. Wer ist der Verantwortliche der Datenverarbeitung?
4. Ist eine Rechtsgrundlage im Datenschutzrecht vorhanden? Werden besondere Kategorien personenbezogener Daten nach Art. 9 Abs. 1 DSGVO verarbeitet, die einer Rechtsgrundlage nach Art. 9 Abs. 2 DSGVO bedürfen?
5. Rechtsfolge: Grundsätzlich ist die Verarbeitung möglich. Jedoch müssen die übrigen Pflichten eingehalten werden, z. B. die Grundsätze der DSGVO (Art. 5 DSGVO), die Beachtung der Betroffenenrechte (Art. 12 ff. DSGVO), die Umsetzung der technischen und organisatorischen Maßnahmen und Garantien (Art. 24 ff. und Art. 89 Abs. 1 DSGVO) und ggf. die Anfertigung einer Datenschutz-Folgenabschätzung (Art. 35 DSGVO).

Die Orientierungshilfe der Datenschutzkonferenz (DSK) „Künstliche Intelligenz und Datenschutz" vom 06.05.2024 enthält zusammengefasst folgende Prüffragen bzw. Aussagen:

- Einsatzfelder und Zwecke bestimmt?
- Einsatzfelder rechtmäßig?
- Einsatzfelder ohne personenbezogene Daten?
- Datenschutzkonformes Training von KI-Anwendungen?

- Rechtsgrundlage für die Datenverarbeitung?
- Keine automatisierte Letztentscheidung?
- Geschlossenes oder offenes System?
- Transparenz und Wahlmöglichkeit hinsichtlich KI-Training?
- Transparenz und Wahlmöglichkeit hinsichtlich Eingabehistorie?
- Berichtigung, Löschung und weitere Betroffenenrechte?
- Datenschutzbeauftragte und Beschäftigtenvertretung eingebunden?
- Verantwortlichkeit festgelegt?
- Interne Zuständigkeiten geregelt?
- Datenschutz-Folgenabschätzung geprüft bzw. durchgeführt?
- Betriebliche Accounts eingerichtet?
- Datensicherheit gewährleistet?
- Beschäftigte sensibilisiert?
- Weitere Entwicklungen verfolgen!
- Vorsicht bei Eingabe und Ausgabe personenbezogener Daten!
- Besondere Vorsicht bei besonderen Kategorien personenbezogener Daten!
- Ergebnisse auf Richtigkeit prüfen!
- Ergebnisse und Verfahren auf Diskriminierung prüfen!

In der „Orientierungshilfe zu empfohlenen technischen und organisatorischen Maßnahmen bei der Entwicklung und beim Betrieb von KI-Systemen“ vom Juni 2025 werden von der DSK die unterschiedlichen Phasen im Lebenszyklus einer KI (Design, Entwicklung, Einführung) bis hin zur KI-Nutzung behandelt. Dabei sind für KI-Nutzer primär die Ausführungen zu „Betrieb und Monitoring“ interessant:

1. Gewährleistungsziel Transparenz

- Bei entscheidungsunterstützenden KI-Systemen ist es erforderlich, dass die entscheidungsrelevanten Inhalte der Ausgaben deterministisch und reproduzierbar sind.
- Die bekannten maßgeblichen KI-Modellparameter (z. B. bei Entscheidungsbäumen) und Verarbeitungsschritte für das Zustandekommen der Ausgaben eines KI-Systems sind revisionssicher zu dokumentieren.

- Es muss festgehalten werden, welche Daten durch welches KI-System verarbeitet wurden und ob diese Daten für weiteres Training zur Verfügung gestellt werden.

2. Gewährleistungsziel Datenminimierung

- Zu den nötigen Maßnahmen können z. B. Pseudonymisierung oder eine nachträgliche Prüfung des Personenbezugs des entsprechenden KI-Modells gehören. Ggf. kann bei der Rückkopplung verteiltes Training (engl.: Federated Learning) angewendet werden, sodass nur einzelne Infrastrukturkomponenten die jeweiligen Daten verarbeiten und nicht die Daten selbst, sondern nur damit erzielte Trainingsergebnisse geteilt werden.

3. Gewährleistungsziel Nichtverkettung

- Die personenbezogenen Daten werden nicht für einen anderen als den festgelegten, eindeutigen und legitimen Zweck erhoben, verarbeitet und genutzt.

4. Gewährleistungsziel Intervenierbarkeit

- Beispielsweise kann das KI-System so lange in einem Wartestatus verbleiben („pending"), bis der weitere Fortgang nach menschlicher Kontrolle angestoßen wird, es können feste „menschliche" Bearbeitungszeiten vorgeschrieben werden, bevor eine Bestätigung erfolgen kann, um die Auseinandersetzung mit der Ausgabe zu unterstützen, oder es kann auch eine regelmäßige Freigabe-Erfordernis geben. Aber auch Hinweise in dem KI-System, dass die Ausgaben nicht perfekt sind, und ggf. die zusätzliche Angabe eines „Unsicherheitsfaktors", der die Verlässlichkeit der jeweiligen Ausgabe abschätzt, können hilfreich sein.
- Beachtung der Betroffenenrechte, je nach Risikograd muss ggf. eine Methode zum gezielten Entfernen bestimmter Informationen aus der KI („Machine Unlearning") integriert werden.

5. Gewährleistungsziel Verfügbarkeit

- Die personenbezogenen Daten sind und bleiben unversehrt, vollständig, zurechenbar und aktuell.

6. Gewährleistungsziel Integrität

- Bei KI-Systemen, die kontinuierlich im Rahmen ihrer Lernfähigkeit weiterentwickelt und angepasst werden, muss die Aufrechterhaltung der Qualität im Laufe der Zeit besonders aufmerksam verfolgt werden. Es müssen plötzliche

und kontinuierliche Verhaltensänderungen von KI-Systemen festgestellt und deren Auswirkungen auf die Risiken bewertet werden.

- Eingaben außerhalb des zulässigen Bereichs sollten durch Eingabefilter erkannt werden und zu einem deutlich erkennbaren Hinweis führen. Zusätzlich sollte erkannt werden, wenn Eingaben (von einem Angreifer) so verändert wurden, dass sie eine Fehlentscheidung des KI-Systems verursachen (engl.: Evasion Attacks).
- Es sollten regelmäßige Risikoeinschätzungen vorgenommen werden, insbesondere bei öffentlich verfügbaren KI-Systemen.
- Angriffe durch manipulierte Ein- und Ausgaben oder inkorrekte Rückmeldungen zur Qualität der Ausgaben, die für weiteres Training genutzt werden, müssen unterbunden werden.

7. Gewährleistungsziel Vertraulichkeit

- Die Extraktion der Trainingsdaten muss verhindert werden.

Der Branchenverband Bitkom hat einen „Praxisleitfaden KI & Datenschutz" herausgebracht. Er enthält zahlreiche wertvolle Hilfestellungen, unter anderem eine Checkliste, die in zwei Teile („Training von KI-Modellen und -Systemen" sowie „Nutzung von KI-Systemen") untergliedert ist. Der Part „Training eigener KI-Modelle und -Systeme" enthält unter anderem folgende Punkte:

- Festlegung und Beschreibung der KI-Technologie und Anlage entsprechender Dokumentation
- Klassifizierung der Trainingsdaten, Beurteilung der Personenbeziehbarkeit und Bewertung, ob das Training unter die DSGVO fällt
- ggf. Einbindung des Datenschutzbeauftragten
- Beurteilung der Rechtsgrundlage für die Verarbeitung personenbezogener Daten in Hinblick auf die verfolgten Verarbeitungszwecke
- Beurteilung der besonderen Voraussetzungen im Fall von besonderen Kategorien personenbezogener Daten (Art. 9 DSGVO)
- Prüfung der Datenqualität (Datenrichtigkeit) auch in Hinblick auf Voreingenommenheit (Bias) und Diskriminierungspotenzial
- Beurteilung der Risiken für die Rechte und Freiheiten der Betroffenen
- Beurteilung spezieller Anforderungen an den besonderen Schutzbedarf von

Kindern und Jugendlichen

- ggf. Durchführung einer DSFA (Art. 35 DSGVO)
- Festlegung und Sicherstellung angemessener technischer und organisatorischer Maßnahmen (einschließlich Zugriffs-, Berechtigungs- und Löschkonzept) nach Art. 32 DSGVO
- Aufnahme in das Verzeichnis der Verarbeitungstätigkeiten und Dokumentation zur Erfüllung der Rechenschaftspflicht unter Angabe insbesondere von Datenquelle bzw. Herkunft der Daten, Rechtsgrundlage sowie Erfüllung der Transparenzanforderungen
- bei Inanspruchnahme von (externen) Dienstleistern: sorgfältige Auswahl unter Berücksichtigung der besonderen Eignung des Dienstleisters, Festlegung des Verantwortungsbereichs des Dienstleisters einschließlich der Verarbeitungszwecke, Abschluss notwendiger Verträge unter Vorgabe entsprechender Leistungsanforderungen bzw. Weisungen
- Bewertung und Validierung des trainierten KI-Modells bzw. KI-Systems in Hinblick auf ggf. vorhandene Personenbezüge
- Implementierung notwendiger Prozesse zur Erfüllung von Betroffenenrechten

In Bezug auf die Nutzung von KI- Modellen und KI-Systemen hält Bitkom insbesondere die folgenden Punkte für wichtig:

- Festlegung und Beschreibung der KI-Technologie und Anlage entsprechender Dokumentation unter Berücksichtigung der Inhaberschaft und Verantwortlichkeit hinsichtlich des KI-Modells bzw. -Systems sowie der verwendeten KI-Umgebung bzw. KI-Anwendung
- ggf. Einbindung des Datenschutzbeauftragten
- bei Inanspruchnahme eines (externen) Dienstleisters: sorgfältige Auswahl unter Berücksichtigung der besonderen Eignung des Dienstleisters, Festlegung des Verantwortungsbereichs des Dienstleisters einschließlich der Verarbeitungszwecke, Abschluss notwendiger Verträge unter Vorgabe entsprechender Leistungsanforderungen bzw. Weisungen
- Beurteilung der Risiken für die Rechte und Freiheiten der Betroffenen
- ggf. Durchführung einer DSFA (Art. 35 DSGVO)
- Aufnahme in das Verzeichnis der Verarbeitungstätigkeiten und Dokumenta-

tion zur Erfüllung der Rechenschaftspflicht unter Angabe insbesondere von Rechtsgrundlage sowie Erfüllung der Transparenzanforderungen

- Entwicklung und Implementierung verbindlicher Verhaltensregeln hinsichtlich der Eingabe personenbezogener Daten (Prompt), insbesondere unter Berücksichtigung besonderer Kategorien personenbezogener Daten (Art. 9 DSGVO), und der Verwendung der Ergebnisse (Output)
- Angebote zur Sensibilisierung der Beschäftigten zum Umgang mit KI
- Implementierung notwendiger Prozesse zur Erfüllung von Betroffenenrechten

All diese Orientierungshilfen, Leitfäden etc. sind wertvolle Hilfestellungen von berufener Seite zur datenschutzrechtskonformen KI-Nutzung in der Praxis.

DATENSCHUTZVORFALL

Ein Datenschutzvorfall (umgangssprachlich auch als „Datenpanne“ bezeichnet) liegt vor, wenn es zu einer „Verletzung des Schutzes personenbezogener Daten“ kommt. Darunter versteht Art. 4 Nr. 12 Datenschutzgrundverordnung (DSGVO) Folgendes:

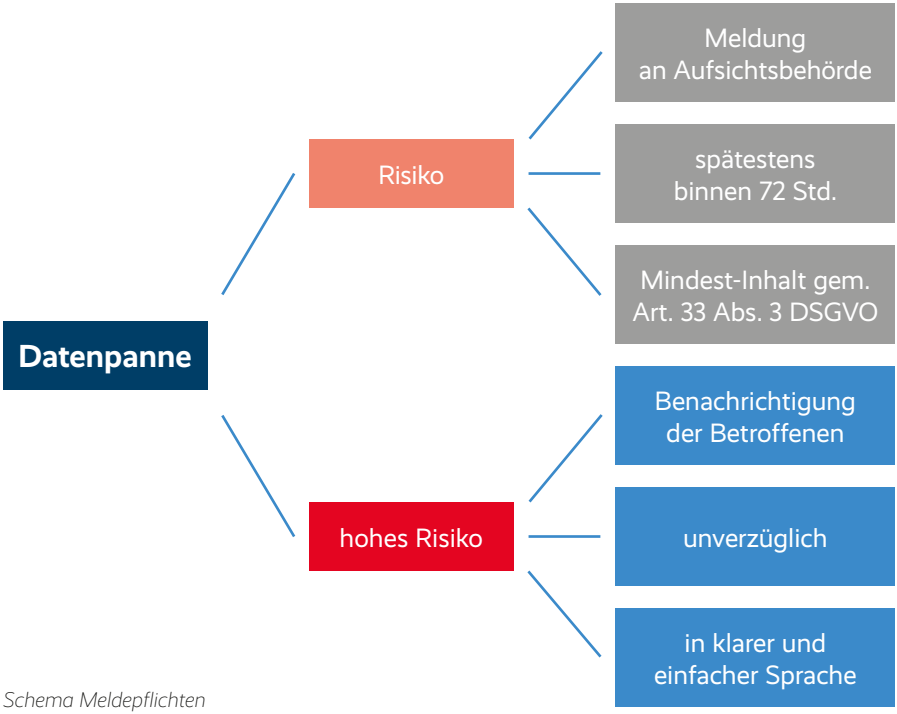
„eine Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung, oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden“

Typische Beispiele solcher Datenpannen sind etwa:

- Hack eines Servers
- Virus/Malware im Unternehmensnetzwerk
- Verlust eines Aktenordners
- Verlust eines externen Datenträgers
- Diebstahl eines Laptops, Tablets, Handys
- Versenden eines Schriftstücks an falschen Empfänger
- Unbeabsichtigtes Löschen/Verändern von Daten

Im Datenschutzrecht gibt es eine Meldepflicht für Datenpannen im Sinne von Art. 4 Nr. 12 DSGVO. Nach Art. 33 DSGVO meldet der Verantwortliche die Datenpanne an die für ihn zuständige Aufsichtsbehörde, es sei denn, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt. Diese Meldung hat unverzüglich und möglichst binnen 72 Stunden zu erfolgen.

Droht sogar ein hohes Risiko, dann muss der Verantwortliche zusätzlich auch noch die von der Datenpanne Betroffenen informieren (Art. 34 DSGVO).



Schema Meldepflichten

Zur Einstufung eines Risikos als „hoch" im Sinne von Art. 34 Abs. 1 DSGVO können die Kriterien aus dem Working Paper 248 der Art.-29-Gruppe herangezogen werden (s. Abschnitt „Datenschutz-Folgenabschätzung (DSFA)").

Hinweis:
Unabhängig davon, ob mit einer Datenpanne ein Risiko oder gar ein hohes Risiko im Sinne der DSGVO einhergeht, ein solcher Vorfall ist stets zu do-

kumentieren (Art. 33 Abs. 5 DSGVO). Dies ist eine Ausprägung der Rechenschaftsverpflichtung gemäß Art. 5 Abs. 2 DSGVO und ermöglicht der Datenschutzaufsichtsbehörde, die Einhaltung dieser Vorschrift zu überprüfen.

Unterfällt die Institution der NIS2-Richtlinie bzw. dem deutschen BSI-Gesetz (primär der sogenannte KRITIS-Bereich), dann gelten zugleich die Vorgaben für einen etwaigen Cybersicherheitsvorfall. Art. 23 NIS2 enthält eine mehrstufige Meldepflicht für Sicherheitsvorfälle, die erhebliche Auswirkungen auf die Erbringung der Dienste von NIS2-Betreibern haben (sogenannte erhebliche Sicherheitsvorfälle):

- **Frühwarnung:** unverzügliche, spätestens innerhalb von 24 Stunden nach Kenntnisnahme des Vorfalls abzusetzende Meldung
- **Meldung:** unverzügliche, spätestens innerhalb von 72 Stunden nach Kenntnisnahme des Vorfalls abzusetzende Meldung, die eine erste Bewertung des Vorfalls enthalten muss
- **Zwischenbericht:** ggf. nach Anforderung abzusetzende Meldung in Bezug auf etwaige neue Entwicklungen oder Erkenntnisse
- **Abschlussbericht:** spätestens nach einem Monat abzusetzende Meldung mit einer ausführlichen Beschreibung des Sicherheitsvorfalls, Angaben zur Art der Bedrohung bzw. zugrunde liegenden Ursache, die wahrscheinlich den Sicherheitsvorfall ausgelöst hat, Angaben zu den getroffenen und laufenden Abhilfemaßnahmen sowie ggf. die grenzüberschreitenden Auswirkungen des Sicherheitsvorfalls

Die NIS2-Meldepflichten gehen damit sogar noch über die Vorgaben der DSGVO hinaus.

Hinweis:
Auch in anderen Vorschriften finden sich vergleichbare Meldepflichten. So enthält der Cyber Resilience Act (CRA), der in erster Linie für Hersteller und Anbieter von Produkten mit digitalen Elementen gilt, entsprechende Meldepflichten zwecks Steigerung der Cybersicherheit. So müssen gemäß Art. 14 CRA schwerwiegende Sicherheitsvorfälle oder auch ausgenutzte Schwachstellen gemeldet werden. Speziell für den Finanzbereich regelt der Digital Operational Resilience Act (DORA) ebenfalls vergleichbare Meldepflichten (Art. 19 DORA).

Und auch in der KI-Verordnung (KI-VO) gibt es Regelungen zur Meldung von sogenannten „schwerwiegenden Vorfällen". Dabei handelt es sich gemäß Art. 3

Nr. 49 KI-VO um einen Vorfall oder eine Fehlfunktion bezüglich eines KI-Systems, das bzw. die direkt oder indirekt eine der nachstehenden Folgen hat:

- den Tod oder die schwere gesundheitliche Schädigung einer Person
- eine schwere und unumkehrbare Störung der Verwaltung oder des Betriebs kritischer Infrastrukturen
- die Verletzung von Pflichten aus den Unionsrechtsvorschriften zum Schutz der Grundrechte
- schwere Sach- oder Umweltschäden

Tritt ein solcher Vorfall ein, müssen die Anbieter von in der EU in Verkehr gebrachten Hochrisiko-KI-Systemen diesen Vorfall den zuständigen Behörden der Mitgliedstaaten, in denen der Vorfall stattgefunden hat, melden (Art. 73 Abs. 1 KI-VO).

Die Meldung hat unmittelbar zu erfolgen, nachdem der Anbieter den Zusammenhang zwischen dem KI-System und dem schwerwiegenden Vorfall oder jedenfalls die naheliegende Wahrscheinlichkeit eines solchen Zusammenhangs festgestellt hat, und in jedem Fall spätestens 15 Tage, nachdem der Anbieter oder ggf. der Betreiber Kenntnis von diesem schwerwiegenden Vorfall erlangt hat (Art. 73 Abs. 2 KI-VO). Die Meldung hat im Fall eines weitverbreiteten Verstoßes oder eines bestimmten schwerwiegenden Vorfalls (schwere und unumkehrbare Störung der Verwaltung oder des Betriebs kritischer Infrastrukturen) unverzüglich zu erfolgen, spätestens jedoch zwei Tage nachdem der Anbieter oder ggf. der Betreiber von diesem Vorfall Kenntnis erlangt hat (Art. 73 Abs. 3 KI-VO).

Hinweis:
Zur Erfüllung der Meldepflichten ist es je nach Unternehmensgröße erforderlich, interne Prozesse aufzubauen, um sicherzustellen, dass die meldepflichtigen Vorfälle als Verdachtsfall überhaupt intern gemeldet, aufgeklärt, bewertet und an die zuständige Behörde gemeldet und risikomitigiert werden.

DATENTRANSFER

Ein Datentransfer bezeichnet im Datenschutz die Übermittlung personenbezogener Daten von einer Stelle an eine andere. Beispiel: Unternehmen A übermittelt Unternehmen B eine Datei mit den Namen und Kontaktdaten von Newsletter-

Empfängern. Ebenfalls als „Transfer“ im Sinne der Datenschutzgrundverordnung (DSGVO) ist jedoch der Vorgang zu bewerten, dass ein Dritter Zugang zu Daten erhält: Beispiel: Unternehmen A gewährt dem IT-Dienstleister B Remote-Zugriff auf die interne Kundendatenbank, damit dieser die technischen Probleme dort lösen kann. In beiden Fällen, also der tatsächlichen Übermittlung von Daten und der Gewährung des Zugriffs auf Daten, liegt ein „Datentransfer“ im Sinne des Datenschutzrechts vor.

Entscheidend sind dabei zwei Aspekte: Zum einen muss die Übermittlung auf Dritte bzw. die Gewährung des Zugriffs durch Dritte legitimiert sein. Hierfür muss also genauso eine Rechtsgrundlage bestehen wie für alle anderen Verarbeitungsschritte durch den Verantwortlichen. Zum anderen muss am Ort des Datenempfängers/Dritten ein mit der EU vergleichbares Datenschutzniveau existieren, z. B. in Form eines Angemessenheitsbeschlusses.

In puncto Rechtsgrundlage für den Datentransfer müssen drei verschiedene Konstellationen differenziert werden:

- Auftragsverarbeitung (AV)
- Gemeinsame Verantwortlichkeit (engl.: Joint Controllership, JC)
- Getrennte Verantwortlichkeit

Auftragsverarbeitung (AV)	gemeinsame Verantwortlichkeit (JC)	getrennte Verantwortlichkeit
➤ Definition AV: Art. 4 Nr. 8 DSGVO ➤ Voraussetzungen: Art. 28 DSGVO ➤ AV-Vertrag: Art. 28 Abs. 3 DSGVO ➤ Verarbeitung im Auftrag des Verantwortlichen („verlängerter Arm“)	➤ Definition: Art. 4 Nr. 7 DSGVO ➤ Voraussetzungen: Art. 26 DSGVO ➤ JC-Vereinbarung: Art. 26 Abs. 1, 2 DSGVO ➤ Verarbeitung zu gemeinsamen, ggf. aber auch jeweils zu eigenen Zwecken	➤ Definition: Art. 4 Nr. 7 DSGVO ➤ allg. Voraussetzungen (insbesondere Art. 5, 6 DSGVO) ➤ Vereinbarung: keine spezielle erforderlich ➤ Verarbeitung nur jeweils zu eigenen Zwecken

Unterschiede Auftragsverarbeitung, gemeinsame bzw. getrennte Verantwortlichkeit

Als AV-Verhältnis werden beispielsweise das Outsourcing mittels Cloud-Computing, Datenerfassung, Datenkonvertierung oder Einscannen von Dokumenten, das Auslagern der Back-up-Sicherheitsspeicherung und anderer Archivierungen,

die Datenträgerentsorgung durch Dienstleister, die Prüfung oder Wartung (z. B. Fernwartung, externer Support) automatisierter Verfahren oder von EDV-Anlagen (wenn dabei ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann) oder auch der Einsatz von Cloud-Diensten (z. B. KI als Software-as-a-Service-Lösung) zu klassifizieren sein.

Eine gemeinsame Verantwortlichkeit liegt regelmäßig etwa bei gemeinsamer Verwaltung bestimmter Datenkategorien (z. B. Adressdaten) für gleichlaufende Geschäftsprozesse mehrerer Konzernunternehmen, bei gemeinsamer Errichtung einer IT-Infrastruktur, auf der mehrere Beteiligte ihre jeweils individuellen Zwecke verfolgen (etwa gemeinsames Betreiben einer Onlineplattform für Reisereservierungen durch ein Reisebüro, eine Hotelkette und eine Fluggesellschaft), bei klinischen Arzneimittelstudien oder auch bei Personalvermittlungs-Dienstleistern, die für einen Arbeitgeber Bewerber sichten und hierbei auch bei ihm eingegangene Bewerbungen einbeziehen, die nicht gezielt auf Stellen beim Arbeitgeber gerichtet sind.

Getrennte Verantwortlichkeiten liegen hingegen insbesondere bei dem Versand von Briefen, Paketen etc. durch einen Versanddienstleister, bei Überweisungen über die Hausbank, bei Beauftragung eines Steuerberaters oder bei der Konsultation eines Anwalts vor.

Hinweis:
Bei getrennter Verantwortlichkeit ist eine gesonderte Vereinbarung zwar nicht erforderlich. Aus Rechenschaftsgesichtspunkten und bei Zweifelsfällen kann es im Einzelfall aber hilfreich sein, eine entsprechende Vereinbarung zu treffen. Diese kann dann zumindest Indizwirkung entfalten.

Anhand der folgenden Fragen lässt sich ermitteln, ob ein AV-Verhältnis vorliegt und ob die essenziellen Rahmenbedingungen gegeben sind:

- Keine Entscheidung des Auftragsverarbeiters über Zwecke und Mittel (ggf. Entscheidung über einige der Mittel, aber nicht über Zwecke!)?
- Weisungsbefugnis des Verantwortlichen gegenüber dem Auftragsverarbeiter?
- Verarbeitung personenbezogener Daten als Kern des Auftrags?
- Korrekter AV-Vertrag (Art. 28 Abs. 3 DSGVO)?
- Angemessenes Datenschutzniveau (EU/EWR? Drittstaat mit oder ohne Angemessenheitsbeschluss?)

DEEPFAKE

Nach Art. 3 Nr. 60 KI-Verordnung (KI-VO) wird der Begriff „Deepfake“ definiert als ein durch KI erzeugter oder manipulierter Bild-, Ton- oder Videoinhalt, der wirklichen Personen, Gegenständen, Orten, Einrichtungen oder Ereignissen ähnelt und einer anderen Person fälschlicherweise als echt oder wahrheitsgemäß erscheinen würde.

Ein geht hierbei also um einen mithilfe von KI angefertigten oder manipulierten Foto-, Video- oder Audio-Inhalt, der eine reale Person täuschend echt darstellt bzw. wiedergibt, obwohl diese Handlung nicht von ihr stammt. Generative KI-Systeme können sehr schnell und nutzerfreundlich realistische Bilder oder Stimmen erzeugen (z. B. ein Politiker, der scheinbar etwas anderes sagt). Deepfakes können in fremde Urheberrechte (wenn geschützte Stimmen oder Bilder verwendet werden) sowie Persönlichkeitsrechte (Recht am eigenen Bild, Recht am eigenen Wort, Recht an der eigenen Stimme) eingreifen. Zudem kann damit ein Verstoß gegen das Datenschutzrecht einhergehen, soweit es sich um Inhalte mit Bezug zu natürlichen Personen handelt.

Ein sehr offensichtlicher Deepfake

Die KI-VO verlangt für KI-Generierung von Bild-, Ton- oder Videoinhalten, die Deepfakes sind, die deutliche Kennzeichnung, dass es sich um KI-Inhalte handelt. Art. 50 Abs. 4 S. 1 bis 3 KI-VO stellt für KI-Nutzer folgende Regeln auf:

„Betreiber eines KI-Systems, das Bild-, Ton- oder Videoinhalte erzeugt oder manipuliert, die ein Deepfake sind, müssen offenlegen, dass die Inhalte künstlich erzeugt oder manipuliert wurden. Diese Pflicht gilt nicht, wenn die Verwendung zur Aufdeckung, Verhütung, Ermittlung oder Verfolgung von Straftaten gesetzlich zugelassen ist. Ist der Inhalt Teil eines offensichtlich künstlerischen, kreativen, satirischen, fiktionalen oder analogen Werks oder Programms, so beschränken sich die in diesem Absatz festgelegten Transparenzpflichten darauf, das Vorhandensein solcher erzeugten oder manipulierten Inhalte in geeigneter Weise offenzulegen, die die Darstellung oder den Genuss des Werks nicht beeinträchtigt.“

Ausnahmen dieser Transparenz- bzw. Kennzeichnungspflicht existieren im Kontext der Strafverfolgung etc. Bei künstlerischen, satirischen oder ähnlichen Inhalten besteht hingegen eine eingeschränkte Kennzeichnungspflicht.

Hinweis:
Die genannten Informationen müssen spätestens zum Zeitpunkt der ersten Interaktion oder Aussetzung in klarer und eindeutiger Weise bereitgestellt werden. Zudem müssen die Informationen den geltenden Barrierefreiheitsanforderungen entsprechen (vgl. Art. 50 Abs. 5 KI-VO).

Im März 2026 hat die EU-Kommission den zweiten Entwurf eines Verhaltenskodexes zur Transparenz von KI-generierten Inhalten veröffentlicht. Das in diesem Kodex verankerte übergeordnete Ziel besteht darin, das Funktionieren des EU-Binnenmarkts zu verbessern, die Verbreitung von menschenzentrierter und vertrauenswürdiger KI sowie Innovationen zu fördern und gleichzeitig ein hohes Schutzniveau für Gesundheit, Sicherheit und die in der EU-Grundrechtecharta verankerten Grundrechte, einschließlich Demokratie, Rechtsstaatlichkeit und Umweltschutz, vor den schädlichen Auswirkungen von KI in der EU zu gewährleisten. Der Kodex umfasst zwei Abschnitte: Der erste Abschnitt enthält Regeln für die Kennzeichnung und Erkennung von KI-generierten und -manipulierten Inhalten für Anbieter generativer KI-Systeme (Art. 50 Abs. 2, 5 KI-VO). Der zweite Abschnitt regelt hingegen die Vorgaben für die Kennzeichnung von Deepfakes sowie von KI-generierten und -manipulierten Texten für Betreiber von KI-Systemen (Art. 50 Abs. 4, 5 KI-VO).

Abschnitt 1 des Kodex gilt nur für dessen Unterzeichner, soweit sie Anbieter von KI-Systemen sind, die synthetische Audio-, Bild-, Video- oder Textinhalte generieren („generative KI-Systeme"), und in den Anwendungsbereich von Art. 2 und 50 Abs. 2 KI-VO fallen. Abschnitt 1 enthält die folgenden Regeln:

1) Verpflichtung 1: Mehrstufige Kennzeichnung von KI-generierten Inhalten
   a) Maßnahme 1.1: Maschinell lesbare Kennzeichnungsverfahren
      - Teilmaßnahme 1.1.1: Digital signierte Metadaten
      - Teilmaßnahme 1.1.2: Unwahrnehmbare Wasserzeichen-Techniken, die in den Inhalt eingebettet sind
      - Teilmaßnahme 1.1.3: Fingerprinting- oder Protokollierungsfunktionen (optionale ergänzende Maßnahme)
   b) Maßnahme 1.2: Nicht-Entfernung maschinenlesbarer Kennzeichnungen
   c) Maßnahme 1.3: Transparenz der Provenienzkette (optional)
   d) Maßnahme 1.4: Optionale Funktionalität für erkennbare Kennzeichnungen (für Deepfakes sowie KI-generierte und -manipulierte veröffentlichte Texte)

2) Verpflichtung 2: Erkennung der Kennzeichnung von KI-generierten Inhalten
   a) Maßnahme 2.1: Bereitstellung von Erkennungsmechanismen für die aktive Kennzeichnung für Betreiber, Endnutzer und andere Dritte
   b) Maßnahme 2.2: Forensische Erkennungsmechanismen (optionale ergänzende Maßnahme)
   c) Maßnahme 2.3: Klare und leicht zugängliche Offenlegung der Überprüfungs- und Erkennungsergebnisse
   d) Maßnahme 2.4: Förderung der Kompetenz im Umgang mit KI-basierten Kennzeichnungstechnologien und Verifizierung
3) Verpflichtung 3: Maßnahmen zur Erfüllung der Anforderungen an Kennzeichnungs- und Erkennungsverfahren
   a) Maßnahme 3.1: Wirksamkeit
   b) Maßnahme 3.2: Zuverlässigkeit
   c) Maßnahme 3.3: Robustheit
   d) Maßnahme 3.4: Interoperabilität
   e) Maßnahme 3.5: Weiterentwicklung des Stands der Technik bei der Kennzeichnung und Erkennung
4) Verpflichtung 4: Prüfung, Verifizierung und Einhaltung
   a) Maßnahme 4.1: Compliance-Rahmenwerk
   b) Maßnahme 4.2: Prüfung, Verifizierung und Überwachung
   c) Maßnahme 4.3: Schulung
   d) Maßnahme 4.4: Zusammenarbeit mit Marktüberwachungsbehörden

Abschnitt 2 gilt hingegen nur für Unterzeichner des Kodexes, soweit sie Betreiber von KI-Systemen sind, die Deepfakes oder veröffentlichte Texte mit dem Ziel generieren oder manipulieren, die Öffentlichkeit über Angelegenheiten von öffentlichem Interesse zu informieren, die in den Anwendungsbereich von Art. 50 Abs. 4 KI-VO fallen. Diesbezüglich sieht der Kodex folgende Maßnahmen vor:

1) Verpflichtung 1: Offenlegung von KI-generierten und manipulierten Deepfakes sowie von veröffentlichten Texten

   a) Maßnahme 1.1: Gestaltungsanforderungen für Symbole, Kennzeichnungen oder Haftungsausschlüsse

   b) Maßnahme 1.2: Anforderungen an die Platzierung von Symbolen, Beschriftungen oder Haftungsausschlüssen

      - Echtzeitvideo (verschiedene Formate)v
      - Nicht-Echtzeit-Video (verschiedene Formate)
      - Bild (einzelne Modalität)
      - Audio (einzelne Modalität)
      - Andere multimodale Inhalte
      - Text

   c) Maßnahme 1.3: Optionale Verwendung eines EU-Symbols und Beteiligung an dessen Entwicklung

2) Verpflichtung 2: Angemessene Einhaltung, Sensibilisierung und Überprüfung

   a) Maßnahme 2.1: Interne Compliance

   b) Maßnahme 2.2: Sensibilisierung und Schulung

   c) Maßnahme 2.3: Überprüfung, Rückmeldung und Zusammenarbeit mit Behörden

3) Verpflichtung 3: Angemessene Kennzeichnung für künstlerische, kreative und ähnliche Werke

4) Verpflichtung 4: Menschliche Überprüfung, redaktionelle Kontrolle und Verantwortung in Bezug auf KI-generierte oder manipulierte Textveröffentlichungen

Der Kodex enthält auch Vorschläge für Symbole für die entsprechenden Kennzeichnungen.

Die im Kodex der EU vorgeschlagenen Symbole zur Kennzeichnung von KI-Content

DOKUMENTATION

In Bezug auf KI-Systeme der Hochrisikoklasse verlangt die KI-Verordnung (KI-VO) als Voraussetzung, dass eine technische Dokumentation des betreffenden Systems erstellt wird, bevor es in Verkehr gebracht oder in Betrieb genommen wird; zudem ist es auch anschließend auf dem neusten Stand zu halten (Art. 11 Abs. 1 KI-VO). Diese Dokumentation ist so zu erstellen, dass aus ihr der Nachweis hervorgeht, wie das Hochrisiko-KI-System die Anforderungen aus den Art. 8 bis 15 KI-VO erfüllt, und dass den zuständigen nationalen Behörden und den notifizierten Stellen die Informationen in klarer und verständlicher Form zur Verfügung stehen, die erforderlich sind, um zu beurteilen, ob das KI-System diese Anforderungen erfüllt (Art. 11 Abs. 2 S. 1 KI-VO). Sie enthält zumindest folgende Angaben (Art. 11 Abs. 2 S. 2, Anhang IV KI-VO):

- allgemeine Beschreibung des KI-Systems
- detaillierte Beschreibung der Bestandteile des KI-Systems und seines Entwicklungsprozesses
- detaillierte Informationen über die Überwachung, Funktionsweise und Kontrolle des KI-Systems
- Darlegungen zur Eignung der Leistungskennzahlen für das spezifische KI-System
- detaillierte Beschreibung des Risikomanagementsystems (RMS) gemäß Art. 9 KI-VO
- Beschreibung einschlägiger Änderungen, die der Anbieter während des Lebenszyklus an dem System vorgenommen hat
- Aufstellung der vollständig oder teilweise angewandten harmonisierten Normen, deren Fundstellen im Amtsblatt der EU veröffentlicht wurden
- Kopie der EU-Konformitätserklärung gemäß Art. 47 KI-VO
- detaillierte Beschreibung des Systems zur Bewertung der Leistung des KI-Systems in der Phase nach dem Inverkehrbringen gemäß Art. 72 KI-VO

Kleine und mittlere Unternehmen (sogenannter KMU-Bereich) sowie Start-ups können die in Anhang IV aufgeführten Elemente der technischen Dokumentation in vereinfachter Weise bereitstellen. Dazu können sie ein von der EU-Kommission bereitgestelltes Formular nutzen (Art. 11 Abs. 2 S. 3, 4 KI-VO).

Der TÜV Austria bietet einen „Best Practice Leitfaden" für die technische Dokumentation von Hochrisiko-KI-Systemen an. Die zentralen Punkte darin lauten wie folgt:

Best Practice: Technische Dokumentation eines Hochrisiko-KI-Systems (TÜV Austria)	
Wichtige Informationen	➤ Zuständigkeiten (einschließlich Kontaktangaben) ➤ Veröffentlichungsdatum ➤ Versionsnummer ➤ Modelltyp(en) und Architektur(en) ➤ (High-Level-)Informationen über Trainingsalgorithmen, Parameter, Fairness-Beschränkungen oder andere angewandte Ansätze, verwendete Basismodelle und Funktionen ➤ andere Ressourcen für weitere Informationen ➤ Lizenzinformationen
Verwendungs-zweck	➤ primäre Verwendungszwecke und (vereinfachte) Definition des Anwendungsbereichs ➤ vorgesehene Hauptnutzer ➤ vorhersehbare Fehlanwendungen ➤ Anwendungsfälle, die nicht in den Anwendungsbereich fallen ➤ Anwendungsrisiken und Maßnahmen zur Risikominderung (einschließlich der Quellen der Risiken) ➤ Betriebsanleitung für den Betreiber und ggf. eine grundlegende Beschreibung der für den Betreiber zur Verfügung gestellten Benutzerschnittstelle
Ergebnisse der Risikoanalyse	➤ bekannte und vorhersehbare Risiken (bei Verwendung entsprechend der Zweckbestimmung) ➤ Abschätzung und Bewertung der Risiken (bei Verwendung entsprechend der Zweckbestimmung) ➤ Bewertung anderer eventuell auftretender Risiken (basierend auf Daten aus dem Post-Market-Monitoring gemäß Art. 72 KI-VO) ➤ Ergreifung geeigneter und gezielter Risikomanagement-maßnahmen
Grundrechte-Folgenabschät-zung (Art. 27 KI-VO, ISO 42001 Anhang B.5)	➤ Verfahren zur Verwendung entsprechend der Zweckbestimmung ➤ Zeitraum und Häufigkeit der Verwendung ➤ Kategorien der betroffenen natürlichen Personen/Personen-gruppen sowie deren spezifische Schadensrisiken ➤ Maßnahmen der menschlichen Aufsicht ➤ zu ergreifende Maßnahmen im Fall des Eintretens der erkannten Risiken

Best Practice: Technische Dokumentation eines Hochrisiko-KI-Systems (TÜV Austria)	
Einhaltung der Vorschriften	➤ Risikomanagementsystem (Art. 9 KI-VO) ➤ ganz oder teilweise angewandte harmonisierte Normen ➤ Verzeichnis sonstiger angewandter einschlägiger Normen und technischer Spezifikationen ➤ Kopie der EU-Konformitätserklärung (Art. 47 KI-VO)
Entwicklungs-prozess	➤ Verwendung von vortrainierten Systemen oder Tools ➤ allgemeine Logik ➤ verwendete Trainingsdatensätze ➤ Schritte der Datenvorverarbeitung (Art. 10 KI-VO) ➤ Trainingsmethoden und -techniken ➤ die für das Training, die Validierung und den Test erforderlichen Rechenressourcen
Technische Details	➤ Zusammenspiel mit Hardware und Software ➤ Systemarchitektur ➤ minimale und empfohlene Hardware-Spezifikationen ➤ Software-Anforderungen ➤ Input/Output ➤ Software/Firmware-Versionen ➤ Verfügbarkeit ➤ Details der Produktkomponenten ➤ Maßnahmen zur menschlichen Überwachung
Test- und Validierungsdaten-satz inklusive Methodik	➤ Zusammensetzung des zur Bewertung der Modellleistung verwendeten Testdatensatzes ➤ verwendete Validierungsund Testverfahren
Leistungs-kennzahlen des KI-Systems	➤ Beschreibung der Angemessenheit jeder Leistungskennzahl und des akzeptablen Zielbereichs ➤ Bewertung geeigneter Leistungskennzahlen, die auf potenzielle Verzerrungen und deren Auswirkungen hinweisen ➤ Unsicherheit der Leistungsmessungen ➤ Systemfähigkeiten und -beschränkungen in Bezug auf die Leistungskennzahlen und die Robustheit ➤ Interpretation der Leistungskennzahlen in Bezug auf die Zuverlässigkeit des Systems ➤ Public Evaluation Protocols: alle verwendeten Protokolle oder Tools (z. B. GLUE, SuperGLUE, HELM) ➤ alternative Bewertungsmethoden

Best Practice: Technische Dokumentation eines Hochrisiko-KI-Systems (TÜV Austria)	
Überwachung des KI-Systems	➤ Pläne für den Fall von Systemausfällen ➤ Rollback-Pläne ➤ Verfahren zur Überwachung des Zustands des KI-Systems in der Post-Market-Phase ➤ ergriffene Maßnahmen zur Cybersicherheit (Anhang IV, Nr. 2h KI-VO) ➤ relevante Änderungen, die der Anbieter im Laufe seines Lebenszyklus am System vorgenommen hat
Lebenszyklus des KI-Systems	➤ vorher festgelegte Änderungen ➤ Verfahren, mit denen die Organisation auf betriebliche Veränderungen reagiert ➤ Dokumentation (aktuell, genau und von zuständigen Leitungsperson genehmigt)
Zusätzliche Anforderungen an KI-Modelle mit allgemeinem Verwendungszweck	➤ allgemeine Beschreibung des KI-Modells ➤ detaillierte Beschreibung und genutzte Ressourcen im Entwicklungsprozess ➤ Richtlinie zur Einhaltung des Unionsrechts in Bezug auf Urheberrecht und verwandte Schutzrechte (Art. 53 Abs. 1 lit. c) KI-VO) ➤ Kriterien für die Bewertung systemischer Risiken ➤ falls die GPAI ein systemisches Risiko darstellt: Adversarial Testing und Modellanpassungen

Hinweis:
Die Anforderungen an ein Hochrisiko-KI-System (Art. 8 bis 15 KI-VO) und somit auch die Pflicht zur technischen Dokumentation müssen von den Anbietern erfüllt werden (Art. 16 lit. a) KI-VO).

Im Bereich Datenschutz gilt gemäß Art. 5 Abs. 2 Datenschutzgrundverordnung (DSGVO) eine allgemeine Pflicht zum Nachweis darüber, dass die Grundsätze aus Art. 5 Abs. 1 DSGVO eingehalten werden. Zentraler Punkt der Datenschutzdokumentation ist das Verzeichnis von Verarbeitungstätigkeiten (VVT).

Während die technische Dokumentation für Hochrisiko-KI-Systeme das jeweilige System erfasst, beinhaltet das VVT Verarbeitungstätigkeiten im Zusammenhang mit personenbezogenen Daten – hier kann es also ggf. Überschneidungen geben. So oder so ist es ratsam, eine Übersicht der im Einsatz befindlichen KI-Systeme anzulegen. Hierzu kann beispielsweise die folgende tabellarische Darstellung dienen:

Best Practice: Technische Dokumentation eines Hochrisiko-KI-Systems			
	KI-System 1	**KI-System 2**	**...**
Name/Bezeichnung			
Beschreibung/Funktion			
Einsatzbereich/Abteilung (aktiv, geplant)			
Anwendungszweck („use cases“) (aktiv, geplant)			
Risiko-Einstufung (verboten, hoch, begrenzt, niedrig, GPAI)			
Begründung der Einstufung			
Rolle/Akteur im Sinne der KI-VO (Anbieter, Betreiber, Händler, Einführer)			
Sitz des Akteurs			
ggf. Serverstandort			
Lizenzvariante (gratis, kostenpflichtig)			
lokale oder Cloud-Lösung			
AV/gemeinsame Verantwortlichkeit/ getrennte Verantwortlichkeit			
bei Hochrisiko-KI-Systemen: Schutzmaßnahmen bezüglich Beeinträchtigung von Gesundheit, Sicherheit oder Grundrechten			
Transparenzpflichten			
Maßstab bezüglich KI-Kompetenz (Anfänger, Fortgeschrittene, Profis)			

EINFÜHRER

Der Begriff „Einführer“ wird in Art. 3 Nr. 6 KI-Verordnung (KI-VO) wie folgt definiert:

„eine in der Union ansässige oder niedergelassene natürliche oder juristische Person, die ein KI-System, das den Namen oder die Handelsmarke einer in einem Drittland niedergelassenen natürlichen oder juristischen Person trägt, in Verkehr bringt“

In diesem Zusammenhang bedeutet „Inverkehrbringen“ die erstmalige Bereitstellung eines KI-Systems oder eines KI-Modells mit allgemeinem Verwendungszweck auf dem Unionsmarkt (Art. 3 Nr. 9 KI-VO). Letztlich geht es hier also um Importeure.

Bevor Einführer ein Hochrisiko-KI-System in Verkehr bringen, stellen sie sicher, dass das System der KI-VO entspricht (Art. 23 Abs. 1 KI-VO), indem sie überprüfen, ob

- der Anbieter des Hochrisiko-KI-Systems das entsprechende Konformitätsbewertungsverfahren gemäß Art. 43 KI-VO durchgeführt hat,
- der Anbieter die technische Dokumentation gemäß Art. 11, Anhang IV KI-VO erstellt hat,
- das System mit der erforderlichen CE-Kennzeichnung versehen ist und ihm die in Art. 47 KI-VO genannte EU-Konformitätserklärung und Betriebsanleitungen beigefügt sind,
- der Anbieter einen Bevollmächtigten gemäß Art. 22 Abs. 1 KI-VO benannt hat.

Hat ein Einführer hinreichenden Grund zu der Annahme, dass ein Hochrisiko-KI-System nicht der KI-VO entspricht oder gefälscht ist oder diesem eine gefälschte Dokumentation beigefügt ist, bringt er das System erst in Verkehr, nachdem dessen Konformität hergestellt wurde. Birgt das Hochrisiko-KI-System ein Risiko im Sinne von Art. 79 Abs. 1 KI-VO, informiert der Einführer den Anbieter des Systems, die Bevollmächtigten und die Marktüberwachungsbehörden darüber (Art. 23 Abs. 2 KI-VO).

Hinweis:
Die Einführer müssen ihren Namen, ihren eingetragenen Handelsnamen oder ihre eingetragene Handelsmarke und die Anschrift, unter der sie in Bezug auf das Hochrisiko-KI-System kontaktiert werden können, auf der Verpackung oder ggf. in der beigefügten Dokumentation angeben (Art. 23 Abs. 3 KI-VO).

Die Einführer halten für einen Zeitraum von zehn Jahren ab dem Inverkehrbringen oder der Inbetriebnahme des Hochrisiko-KI-Systems ein Exemplar der von der notifizierten Stelle ausgestellten Bescheinigung sowie ggf. die Betriebsanleitungen und die in Art. 47 KI-VO genannte EU-Konformitätserklärung bereit (Art. 23 Abs. 5 KI-VO). Außerdem sind auch Einführer unter Umständen zur Übermittlung der notwendigen Informationen sowie zur weiteren Zusammenarbeit mit der zuständigen Marktüberwachungsbehörde verpflichtet (Art. 23 Abs. 6, 7 KI-VO).

EINWILLIGUNG

Die Einwilligung ist eine von mehreren möglichen Rechtsgrundlagen, die zur rechtmäßigen Verarbeitung personenbezogener Daten vorliegen müssen (Art. 6 Abs. 1 UAbs. 1 lit. a) Datenschutzgrundverordnung, DSGVO). Um zu prüfen, ob eine wirksame Einwilligung vorliegt, sollten die folgenden Fragen beantwortet werden:

- Eindeutig bestätigende Handlung?
- Freiwillig (Besonderheit im Beschäftigtenverhältnis, § 26 Abs. 2 Bundesdatenschutzgesetz?)?
- Ausreichend informiert (insbesondere auf das Widerrufsrecht hingewiesen?)?
- Unmissverständlich abgegeben?
- Willensbekundung?
- Spezialgesetzliche Vorgaben (z. B. durch § 25 Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz, § 7 Abs. 2 Nr. 2 Gesetz gegen den unlauteren Wettbewerb)?
- Nachweis der Einwilligung möglich?
- Bei schriftlicher Einwilligung: in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache und so, dass sie von anderen Sachverhalten klar zu unterscheiden ist?
- Kein Verstoß von Teilen der Erklärung gegen die DSGVO?
- „Kopplungsverbot“ beachtet (Art. 7 Abs. 4 DSGVO)?
- Form (vgl. z. B. § 26 Abs. 2 S. 3 BDSG)?
- Widerruf (Art. 7 Abs. 3 DSGVO)?

Hinweis:
Der Widerruf der Einwilligung muss so einfach wie die Erteilung der Einwilligung sein (Art. 7 Abs. 3 S. 4 DSGVO).

Die Einwilligung ist grundsätzlich die schlechteste aller möglichen Rechtsgrundlagen, da sie jederzeit frei widerrufen werden kann (Art. 7 Abs. 3 S. 1 DSGVO); sie wirkt allerdings nur für die Zukunft (Art. 7 Abs. 3 S. 2 DSGVO). Aufgrund der Widerrufbarkeit bietet sie sich insbesondere als Rechtsgrundlage für die Verarbeitung personenbezogener Daten mittels KI nicht an.

EMOTIONSERKENNUNGSSYSTEM

Der Begriff „Emotionserkennungssystem" wird in Art. 3 Nr. 39 KI-Verordnung (KI-VO) folgendermaßen definiert:

„ein KI-System, das dem Zweck dient, Emotionen oder Absichten natürlicher Personen auf der Grundlage ihrer biometrischen Daten festzustellen oder daraus abzuleiten"

Es geht hier also um KI-Anwendungen, die menschliche Gefühlszustände aus Gesichtsausdruck, Stimme, Körperhaltung oder Ähnlichem analysieren. Ein Beispiel wäre ein System, das Kamerabilder auswertet, um Freude, Wut oder Angst zu erkennen. Im Rahmen der KI-VO werden derartige KI-Systeme als hochriskant eingestuft, weil sie in die Privatsphäre eingreifen und diskriminierend wirken können. Daher dürfen Emotionserkennungssysteme nur noch unter strengen Bedingungen verwendet werden (z. B. in beschränkten Behördenanwendungen oder Systemen für ausschließlich medizinische oder therapeutische Zwecke) – viele kommerzielle Einsatzformen werden eingeschränkt oder verboten.

FINETUNING

Unter Finetuning (dt.: Feinabstimmung) von KI versteht man die weitere Anpassung eines bereits vortrainierten KI-Modells an zusätzliche, spezifische Trainingsdaten, um das Modellverhalten an einem bestimmten Anwendungsfall auszurichten. Technisch wird das Basismodell mit neuen Datensätzen weitertrainiert, sodass es beispielsweise die Fachsprache eines Unternehmens, branchentypische

Dokumentstrukturen oder spezifische regulatorische Anforderungen besser „versteht".

Im Kontext der KI-Verordnung (KI-VO) wird Finetuning als eine Form der Modifizierung von KI-Systemen bzw. KI-Modellen mit allgemeinem Verwendungszweck verstanden. Das gilt insbesondere dann, wenn das zusätzliche Training das Verhalten des Modells wesentlich verändert. Finetuning kann eine solche wesentliche Änderung darstellen, wenn es die grundlegende Logik oder die Risikoeigenschaften des Modells signifikant beeinflusst. Dies kann dazu führen, dass derjenige, der das Finetuning durchführt, selbst als Anbieter eines neuen oder wesentlich geänderten KI-Systems anzusehen ist (Art. 25 Abs. 1 lit. b) KI-VO). Ob es sich noch um Finetuning oder schon um eine Weiterentwicklung handelt, muss im konkreten Einzelfall entschieden werden, was aber nicht immer trennscharf entschieden werden kann.

Dies führt dazu, dass Unternehmen, die lediglich ein bestehendes Modell anpassen, plötzlich die vollen Pflichten eines Anbieters nach Art. 16 ff. KI-VO treffen, einschließlich der Durchführung von Konformitätsbewertungsverfahren und der Erstellung technischer Dokumentationen. Der ursprüngliche Anbieter ist zwar zur Unterstützung verpflichtet, doch die rechtliche Hauptverantwortung verschiebt sich auf denjenigen, der das Finetuning vornimmt.

Aus Sicht des Datenschutzes ist das Finetuning eine Phase der Weiterverarbeitung. Wenn hierfür personenbezogene Daten genutzt werden, muss der Zweck der Verarbeitung mit dem ursprünglichen Erhebungszweck vereinbar sein, sofern keine neue Einwilligung oder eine anderweitige Rechtsgrundlage vorliegt. Da die Daten beim Finetuning oft tiefer in die Modellstrukturen integriert werden als bei der reinen Inferenz (Abfrage), steigt das Risiko einer Rekonstruierbarkeit dieser Daten, was die Anforderungen an die Datensicherheit und Anonymisierung erhöht.

GELDBUßE

Entsprechend den Vorgaben der KI-Verordnung (KI-VO) erlassen die EU-Mitgliedstaaten Vorschriften für Sanktionen und andere Durchsetzungsmaßnahmen, zu denen auch Verwarnungen und nicht-monetäre Maßnahmen gehören können, die bei Verstößen gegen die KI-VO durch Akteure Anwendung finden, und ergreifen alle Maßnahmen, die für deren ordnungsgemäße und wirksame Durchsetzung notwendig sind (Art. 99 Abs. 1 S. 1 KI-VO) – das kann letztlich auch die Verhängung einer Geldbuße sein. Diese Sanktionen müssen nach Maßgabe von

Art. 99 Abs. 1 S. 2 KI-VO wirksam, verhältnismäßig und abschreckend sein – eine Formulierung, die eins zu eins aus der Datenschutzgrundverordnung (DSGVO) übernommen wurde. Allerdings sollen insbesondere die Interessen von kleinen und mittleren Unternehmen (KMU-Bereich) und Start-ups sowie deren wirtschaftliches Überleben berücksichtigt werden. Eine Einheitlichkeit auf EU-Ebene wird durch entsprechende Leitlinien der EU-Kommission angestrebt.

Je nach Verstoß drohen unterschiedliche Maximalgeldbußen:

- Verstoß gegen verbotene Praktiken gemäß Art. 5 KI-VO (Art. 99 Abs. 3 KI-VO): Geldbuße bis zu 35 Mio. Euro oder bis zu 7 % des weltweit erzielten Vorjahresgesamtumsatzes (je nachdem, welcher Betrag höher ist)
- Verstoß gegen verschiedene Vorgaben für Hochrisiko-KI-Systeme, also gegen Art. 16, 22, 23, 24, 26, 31, 33, 34, 50 KI-VO (Art. 99 Abs. 4 KI-VO): Geldbuße bis zu 15 Mio. Euro oder bis zu 3 % des weltweit erzielten Vorjahresgesamtumsatzes
- Bereitstellung irreführender oder falscher Informationen (Art. 99 Abs. 5 KI-VO): Geldbuße bis zu 7,5 Mio. Euro oder bis zu 1 % des weltweit erzielten Vorjahresgesamtumsatzes

Hinweis:
In Bezug auf den festen Maximalbetrag (z. B. 35 Mio. Euro) bzw. den maximalen Prozentsatz (z. B. 7 %) kann der jeweils höhere Betrag festgesetzt werden. Im Falle einer Unternehmensgruppe ist der Umsatz der Gruppe und nicht nur des einzelnen Unternehmens entscheidend. Nach Maßgabe von Art. 99 Abs. 6 KI-VO soll jedoch bei Verstößen durch Unternehmen des KMU-Bereichs bzw. Start-ups der jeweils niedrigere Betrag gelten.

Bei Verstößen durch Anbieter von KI-Modellen mit allgemeinem Verwendungszweck drohen Geldbußen von bis zu 15 Mio. Euro oder bis zu 3 % des weltweit erzielten Vorjahresgesamtumsatzes – je nachdem, welcher Betrag höher ist (Art. 101 Abs. 1 KI-VO).

Als Kriterien zur Festlegung der konkreten Bußgeldhöhe können gemäß Art. 99 Abs. 7 KI-VO folgende Aspekte herangezogen werden:

- Art, Schwere und Dauer des Verstoßes und seiner Folgen, unter Berücksichtigung des Zwecks des KI-Systems sowie ggf. der Zahl der betroffenen Personen und des Ausmaßes des von ihnen erlittenen Schadens

- ob demselben Akteur bereits von anderen Marktüberwachungsbehörden für denselben Verstoß Geldbußen auferlegt wurden
- ob demselben Akteur bereits von anderen Behörden für Verstöße gegen das Unionsrecht oder das nationale Recht Geldbußen auferlegt wurden, wenn diese Verstöße auf dieselbe Handlung oder Unterlassung zurückzuführen sind, die einen einschlägigen Verstoß gegen diese Verordnung darstellt
- Größe, Jahresumsatz und Marktanteil des Akteurs, der den Verstoß begangen hat
- jegliche anderen erschwerenden oder mildernden Umstände im jeweiligen Fall, wie etwa unmittelbar oder mittelbar durch den Verstoß erlangte finanzielle Vorteile oder vermiedene Verluste
- Grad der Zusammenarbeit mit den zuständigen nationalen Behörden, um den Verstoß abzustellen und die möglichen nachteiligen Auswirkungen des Verstoßes abzumildern
- Grad an Verantwortung des Akteurs unter Berücksichtigung der von ihm ergriffenen technischen und organisatorischen Maßnahmen
- Art und Weise, wie der Verstoß den zuständigen nationalen Behörden bekannt wurde, insbesondere ob und ggf. in welchem Umfang der Akteur den Verstoß gemeldet hat
- Vorsätzlichkeit oder Fahrlässigkeit des Verstoßes
- alle Maßnahmen, die der Akteur ergriffen hat, um den Schaden, der den betroffenen Personen zugefügt wird, zu mindern

Auch diese Methodik sowie die einzelnen Aspekte sind dem Grunde nach bereits aus der DSGVO bekannt.

GEMEINFREIHEIT

„Gemeinfreiheit“ (engl.: public domain) auf dem Gebiet Urheberrecht bedeutet, dass ein Erzeugnis keinem Urheberrechtsschutz (mehr) unterliegt. Gründe dafür sind z. B. Ablauf der Schutzfrist (70 Jahre nach Tod des Urhebers) oder von Anfang an fehlende Schutzfähigkeit. Gemeinfreie Erzeugnisse dürfen ohne Erlaubnis kopiert, bearbeitet oder verbreitet werden, und zwar im privaten wie im beruflichen Kontext.

Hinweis:
Aber auch gemeinfreie Erzeugnisse können eventuell Persönlichkeitsrechte berühren, wenn echte Personen aufgenommen worden sind.

Die Voraussetzungen, die ein Erzeugnis erfüllen muss, um als nach dem Urheberrecht schützenswertes Werk eingestuft zu werden, finden sich in § 1, 2 Urheberrechtsgesetz (UrhG). In § 1 UrhG ist Folgendes geregelt:

„Die Urheber von Werken der Literatur, Wissenschaft und Kunst genießen für ihre Werke Schutz nach Maßgabe dieses Gesetzes."

Zusätzlich formuliert § 2 Abs. 2 UrhG noch weitere Anforderungen:

„Werke im Sinne dieses Gesetzes sind nur persönliche geistige Schöpfungen."

Hinweis:
Generell können verschiedene Arten von Werken vorliegen, z. B. Texte, Fotos, Videos, Musikstücke, Code usw. (vgl. § 2 Abs. 1 UrhG).

Wem steht das Urheberrecht an KI-Output zu?

Der Knackpunkt bei KI-Output besteht darin, dass der maßgebliche Anteil an dem Erzeugnis nicht beim Menschen, sondern der Löwenanteil in aller Regel bei der KI liegt. Es gibt sicher schwierige Abgrenzungsfälle, aber die meisten KI-Erzeugnisse werden schwerpunktmäßig der KI zugerechnet, da der Mensch ja „nur" den Befehl zur Ausführung gibt (sogenannter Prompt) und daher eher die Rolle eines Auftraggebers einnimmt. Insofern wird durch die KI keine persönliche geistige Schöpfung im Sinne von § 2 Abs. 2 UrhG erbracht, sodass die überwiegende Anzahl von KI-Outputs als gemeinfrei eingestuft wird.

Das bedeutet, dass man sich als KI-Nutzer regelmäßig kaum Gedanken um etwaige fremde Urheberrechte machen muss. Allerdings gilt die Gemeinfreiheit gegenüber jedermann, sodass auch kein Exklusiv-Content besteht.

Das zieht allerdings zahlreiche Folgefragen nach sich, insbesondere ob ein KI-generierter Inhalt dem UrhG unterfallen kann, wenn er von einem Menschen überarbeitet wird. Oder andersherum: Verliert ein menschlich erschaffenes Werk das Urheberrecht, wenn es von einer KI verändert wird?

In beiden Fällen lautet die Antwort: Es kommt darauf an! Und zwar darauf, wie hoch der jeweilige Bearbeitungsanteil ausfällt. Bearbeitet also beispielsweise ein Mensch den von einer KI erschaffenen Text in der Weise, dass er dort nicht nur ein paar Wörter, sondern ganze Absätze ändert, neue Absätze hinzufügt, den Sprachstil und ggf. den inhaltlichen Schwerpunkt anders gestaltet, dann kann die überarbeitete Fassung Urheberrecht für den Bearbeiter erlangen. Die ursprüngliche KI-Fassung ist und bleibt allerdings gemeinfrei.

Hinweis:
Während der KI-Output regelmäßig nicht dem Schutz des Urheberrechts unterfällt, kann der KI-Input, also der Prompt, dies sehr wohl. Das ist jedenfalls dann so, wenn der Prompt als persönliche geistige Schöpfung im Bereich Literatur, Wissenschaft oder Kunst anzusehen ist (§§ 1, 2 Abs. 2 UrhG).

GPAI

s. Abschnitt „KI-Modell mit allgemeinem Verwendungszweck“

GRUNDRECHTE

Grundrechte sind die fundamentalen Rechte von Menschen, z. B. auf Menschenwürde, körperliche Unversehrtheit, Meinungsfreiheit etc. Im KI-Kontext stehen besonders das allgemeine Persönlichkeitsrecht, informationelle Selbstbestimmung, Meinungsfreiheit und Gleichheit im Vordergrund. KI-Anwendungen dürfen diese Grundrechte nicht verletzen; die KI-Verordnung betont insbesondere den Schutz von Privatsphäre und Grundrechten.

Hinweis:
Auf EU-Ebene gilt die EU-Grundrechtecharta. So regelt z. B. Artikel 8 den Schutz personenbezogener Daten. („Jede Person hat das Recht auf Schutz der sie betreffenden personenbezogenen Daten.")

Die Grundrechte ergeben sich aus dem deutschen Grundgesetz (GG), also der Verfassung der Bundesrepublik Deutschland. Diese enthält die rechtliche und politische Grundordnung Deutschlands. Die Grundrechte sind in den Art. 1 bis 19 GG geregelt und dienen als Abwehrrechte der Bürger gegen den Staat.

Alle Grundrechte sind gleichrangig, im Streitfall müssen daher die unterschiedlichen Rechte gegeneinander abgewogen werden, um im Wege eines möglichst schonenden Ausgleichs zu einer praxisgerechten Lösung zu kommen (sogenannte praktische Konkordanz).

In den Art. 1 bis 19 GG finden sich folgende Grundrechte:

- Menschenwürde (Art. 1 GG)
- Persönliche Freiheitsrechte (Art. 2 GG)
- Gleichheit vor dem Gesetz (Art. 3 GG)
- Glaubens- und Gewissensfreiheit (Art. 4 GG)
- Freiheit der Meinung, Kunst und Wissenschaft (Art. 5 GG)
- Ehe, Familie, Kinder (Art. 6 GG)
- Schulwesen (Art. 7 GG)
- Versammlungsfreiheit (Art. 8 GG)
- Vereinigungs-/Koalitionsfreiheit (Art. 9 GG)
- Brief-, Post-, Fernmeldegeheimnis (Art. 10 GG)
- Freizügigkeit (Art. 11 GG)
- Berufsfreiheit (Art. 12 GG)
- Militärische und zivile Dienstpflichten (Art. 12a GG)
- Eigentum (Art. 14 GG)
- Vergesellschaftung (Art. 15 GG)
- Staatsangehörigkeit/Auslieferung (Art. 16 GG)

- Asyl (Art. 16a GG)
- Petitionsrecht (Art. 17 GG)
- Einschränkung der Grundrechte in besonderen Fällen (Art. 17a GG)
- Grundrechtsverwirkung (Art. 18 GG)
- Einschränkung von Grundrechten/Rechtsweg (Art. 19 GG)

Die im GG verankerten unabänderlichen obersten Wertprinzipien werden zusammenfassend als freiheitlich demokratische Grundordnung bezeichnet. Diese umfasst folgende Aspekte:

- das Recht des Volkes, die Staatsgewalt in Wahlen und Abstimmungen und durch besondere Organe der Gesetzgebung, der vollziehenden Gewalt und der Rechtsprechung auszuüben und die Volksvertretung in allgemeiner, unmittelbarer, freier, gleicher und geheimer Wahl zu wählen
- die Bindung der Gesetzgebung an die verfassungsmäßige Ordnung und die Bindung der vollziehenden Gewalt und der Rechtsprechung an Gesetz und Recht
- das Recht auf Bildung und Ausübung einer parlamentarischen Opposition
- die Ablösbarkeit der Regierung und ihre Verantwortlichkeit gegenüber der Volksvertretung
- die Unabhängigkeit der Gerichte
- der Ausschluss jeder Gewalt- und Willkürherrschaft
- die im Grundgesetz konkretisierten Menschenrechte (s. o.)

GRUNDRECHTE-FOLGENABSCHÄTZUNG (GFA)

Eine Grundrechte-Folgenabschätzung (GFA) ist in der KI-Verordnung (KI-VO) für bestimmte Betreiber als spezielle Untersuchung für Hochrisiko-KI-Systeme verankert. Sie ergänzt die Datenschutz-Folgenabschätzung (DSFA) um grundrechtliche Aspekte. Ziel der GFA ist es, dass die spezifischen Risiken für die Rechte von Einzelpersonen oder Gruppen von Einzelpersonen, die wahrscheinlich betroffen sein werden, sowie auch Maßnahmen ermittelt werden, die im Falle eines Eintre-

tens dieser Risiken zu ergreifen sind. Die GFA ist vor dem erstmaligen Einsatz des Hochrisiko-KI-Systems durchzuführen. Zudem ist sie zu aktualisieren, wenn der Betreiber der Auffassung ist, dass sich einer der relevanten Faktoren geändert hat (vgl. ErwGr. 96 S. 4, 5 KI-VO).

Bestimmte Betreiber eines Hochrisiko-KI-Systems müssen vorab prüfen und dokumentieren, welche Auswirkungen dieses KI-System auf EU-Grundrechte haben kann (z. B. Diskriminierung, Recht auf Leben, Selbstbestimmung). Die GFA dient der Transparenz und Konfliktvermeidung: Ergibt die Abschätzung schwere Risiken für Grundrechte, kommen Nachbesserung oder gar ein Verbot in Betracht. Im Ergebnis muss der Betreiber ggf. durch technische und/oder organisatorische Maßnahmen (TOM) den Grundrechtsschutz sicherstellen.

Adressaten (Art. 27 Abs. 1 S. 1 KI-VO)	**GFA** (Art. 27 Abs. 1 S. 2 lit. a)–f) KI-VO)
➤ (wohl) die gesamte staatliche Verwaltung ➤ private Einrichtungen, die öffentliche Dienste erbringen (z. B. Bildung, Gesundheitsversorgung, Sozialdienste, Wohnungswesen und Justizverwaltung, vgl. ErwGr. 96 KI-VO) ➤ Banken und Versicherungen bezüglich KI-Systemen zur Prüfung der Kreditwürdigkeit (vgl. Anhang III Nr. 5 lit. b) KI-VO) ➤ Risikobewertung bzw. Preisbildung bei Kranken- und Lebensversicherung (vgl. Anhang III Nr. 5 lit. c) KI-VO) ➤ Ausnahme: KRITIS (vgl. Anhang III Nr. 2 KI-VO)	➤ Beschreibung der Verfahren, bei denen das KI-System verwendet wird ➤ Beschreibung des Zeitraums und der Häufigkeit, innerhalb dessen bzw. mit der das KI-System verwendet werden soll ➤ Kategorien von Betroffenen ➤ spezifische Schadensrisiken ➤ Beschreibung der Umsetzung von Maßnahmen der menschlichen Aufsicht ➤ Maßnahmen, die im Fall des Eintretens der Risiken zu ergreifen sind, einschließlich der Regelungen für die interne Unternehmensführung und Beschwerdemechanismen

Tabellarische Übersicht zur GFA

Zur Durchführung der GFA sind lediglich solche Betreiber verpflichtet, bei denen es sich um Einrichtungen des öffentlichen Rechts oder private Einrichtungen, die öffentliche Dienste erbringen, handelt. Außerdem trifft die Pflicht auch solche Betreiber von Hochrisiko-KI-Systemen, die bestimmungsgemäß für die Kreditwürdigkeitsprüfung und Bonitätsbewertung natürlicher Personen verwendet werden

sollen (mit Ausnahme von KI-Systemen, die zur Aufdeckung von Finanzbetrug verwendet werden), und solche, die bestimmungsgemäß für die Risikobewertung und Preisbildung in Bezug auf natürliche Personen im Fall von Lebens- und Krankenversicherungen eingesetzt werden sollen (Art. 27 Abs. 1 S. 1, Anhang III Nr. 5 lit. b), c) KI-VO).

Hinweis:
Der Betreiber kann sich in ähnlichen Fällen auf zuvor durchgeführte GFA oder bereits vorhandene Folgenabschätzungen, die vom Anbieter durchgeführt wurden, stützen (Art. 27 Abs. 2 S. 2 KI-VO).

Sobald die GFA durchgeführt wurde, teilt der Betreiber der Marktüberwachungsbehörde (in Deutschland der Bundesnetzagentur) die Ergebnisse mit. Dazu stellt die Marktüberwachungsbehörde ein Musterformular bereit. Die GFA kann ggf. einer eventuell ebenfalls durchgeführten DSFA (Art. 35 Datenschutzgrundverordnung) ergänzend beigefügt werden (Art. 27 Abs. 4 KI-VO).

HAFTUNG (DES KI-NUTZERS)

Bei der Nutzung von KI stellt sich nicht selten die Frage: Wer haftet eigentlich? Es kommt hierbei natürlich auf den Kontext und auf das konkrete Einsatzszenario an, aber generell haftet nicht „die KI" selbst. In aller Regel muss der KI-Nutzer dafür einstehen, dass er KI-Output verwendet bzw. welche Inhalte er im Rahmen seines Prompts nutzt.

Wer beispielsweise mit ChatGPT einen Text erstellt, mit Midjourney ein Bild generiert oder mit Claude Code für ein Programm schreibt – bei der Verwendung von KI-Erzeugnissen, gleich welcher Art, liegt die Verantwortung regelmäßig beim Nutzer. Wer einen KI-Text für interne (etwa als Aktennotiz oder Stellungnahme für einen Kollegen) oder für externe Zwecke (z. B. als Social-Media-Posting oder Kundenanschreiben) verwendet, der haftet für darin ggf. enthaltene Fehler und Rechtsverstöße grundsätzlich nach denselben Regeln, als wenn er den Text eigenständig verfasst hätte. Wer ein KI-Bild in einen Blog-Artikel einbindet, der muss für darin eventuell enthaltene Verstöße gegen fremde Urheber- oder Markenrechte einstehen. Enthalten KI-Erzeugnisse personenbezogene Daten Dritter, muss deren Verwender die entsprechenden Voraussetzungen erfüllen, also insbesondere eine Rechtsgrundlage für die Datenverarbeitung vorweisen können.

Kurzum: Wer KI einsetzt und den entsprechenden Output nutzt, der ist dafür genauso verantwortlich wie für eigene Werke. Daher kann nur dringend empfohlen werden, KI-Output niemals einfach so ungeprüft eins zu eins zu übernehmen. Die inhaltliche und rechtliche Kontrolle muss abschließend immer noch durch den Menschen erfolgen.

HÄNDLER

Nach Art. 3 Nr. 7 KI-Verordnung (KI-VO) wird „Händler" wie folgt definiert:

„eine natürliche oder juristische Person in der Lieferkette, die ein KI-System auf dem Unionsmarkt bereitstellt, mit Ausnahme des Anbieters oder des Einführers"

„Bereitstellung auf dem Markt" meint in diesem Zusammenhang die entgeltliche oder unentgeltliche Abgabe eines KI-Systems oder eines KI-Modells mit allgemeinem Verwendungszweck zum Vertrieb oder zur Verwendung auf dem Unionsmarkt im Rahmen einer Geschäftstätigkeit (Art. 3 Nr. 10 KI-VO).

Hinweis:
KI-Anbieter (also in der Regel Hersteller) und KI-Einführer (also Importeure) können demnach kein Händler in diesem Sinne sein. Eine Doppelrolle beispielsweise als „Anbieter" auf der einen und als „Händler" auf der anderen Seite ist somit ausgeschlossen.

Ein Händler kauft also das KI-Produkt (meist vom Einführer oder Hersteller) und vertreibt es weiter, z. B. über eine Onlineplattform. Rechtlich trägt der Händler weniger Verantwortung als Anbieter, Betreiber oder Einführer. Er muss aber insbesondere prüfen, ob das System eine korrekte CE-Kennzeichnung besitzt und ob eine Betriebsanleitung beigefügt ist (Art. 24 Abs. 1 KI-VO). Zudem muss er prüfen, ob Anbieter und ggf. Einführer des betreffenden KI-Systems

- auf dem Hochrisiko-KI-System oder, falls dies nicht möglich ist, auf seiner Verpackung oder in der beigefügten Dokumentation ihren Namen, ihren eingetragenen Handelsnamen bzw. ihre eingetragene Handelsmarke und ihre Kontaktanschrift angeben (Art. 24 Abs. 1 KI-VO i. V. m. Art. 16 lit. b) KI-VO),
- über ein Qualitätsmanagementsystem verfügen, das Art. 17 KI-VO entspricht (Art. 24 Abs. 1 KI-VO i. V. m. Art. 16 lit. c) KI-VO),

- ihren Namen, ihren eingetragenen Handelsnamen oder ihre eingetragene Handelsmarke und die Anschrift, unter der sie in Bezug auf das Hochrisiko-KI-System kontaktiert werden können, auf der Verpackung oder ggf. in der beigefügten Dokumentation angeben (Art. 24 Abs. 1 KI-VO i. V. m. Art. 23 Abs. 3 KI-VO).

Ist ein Händler der Auffassung oder hat er aufgrund von Informationen, die ihm zur Verfügung stehen, Grund zu der Annahme, dass ein Hochrisiko-KI-System nicht den Anforderungen der Art. 8-15 KI-VO entspricht, stellt er das Hochrisiko-KI-System erst auf dem Markt bereit, nachdem die Konformität des Systems mit den Anforderungen hergestellt wurde (Art. 24 Abs. 2 S. 1 KI-VO). Er ergreift außerdem die erforderlichen Korrekturmaßnahmen, um die Konformität dieses Systems mit diesen Anforderungen herzustellen, es zurückzunehmen oder zurückzurufen, oder er stellt sicher, dass der Anbieter, der Einführer oder ggf. jeder relevante Akteur diese Korrekturmaßnahmen ergreift (Art. 24 Abs. 4 S. 1 KI-VO).

Birgt das Hochrisiko-IT-System zudem ein Risiko im Sinne des Art. 79 Abs. 1 KI-VO, informiert der Händler den Anbieter bzw. den Einführer des Systems (Art. 24 Abs. 2 S. 2 KI-VO) sowie die für das betroffene Hochrisiko-KI-System zuständigen Behörden darüber und macht dabei ausführliche Angaben, insbesondere zur Nichtkonformität und zu bereits ergriffenen Korrekturmaßnahmen (Art. 24 Abs. 4 S. 2 KI-VO).

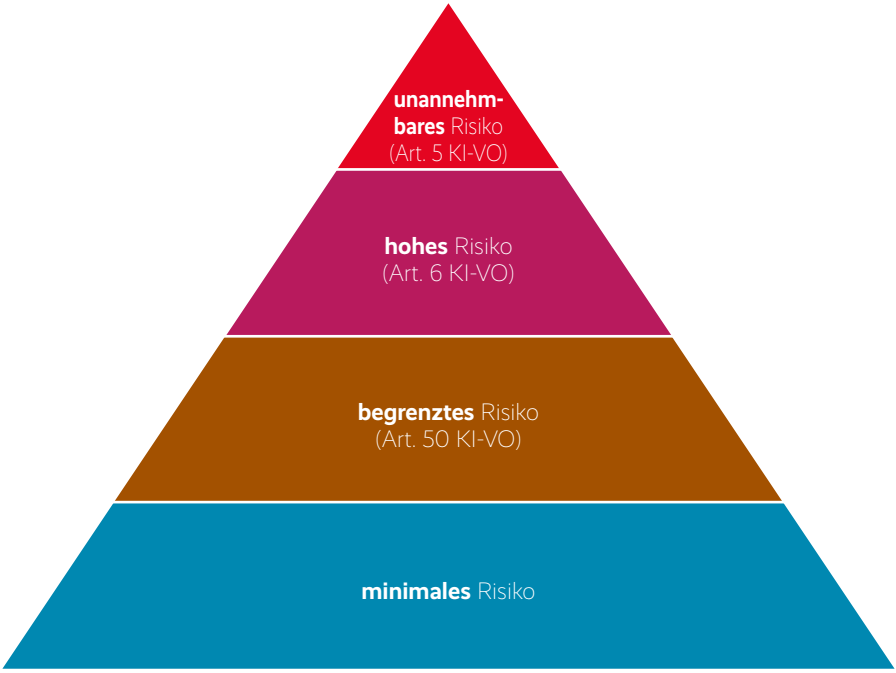
Solange sich ein Hochrisiko-KI-System in ihrer Verantwortung befindet, gewährleisten Händler, dass – soweit zutreffend – die Lagerungs- oder Transportbedingungen die Konformität des Systems mit den in den Art. 8 bis 15 KI-VO festgelegten Anforderungen nicht beeinträchtigen (Art. 24 Abs. 3 KI-VO). Darüber hinaus muss der Händler mit der zuständige Marktüberwachungsbehörde zusammenarbeiten, indem er ihr bestimmte Informationen bereitstellt und alle Maßnahmen unterstützt, um insbesondere das von diesem System ausgehende Risiko zu verringern oder abzumildern (vgl. Art. 24 Abs. 5, 6 KI-VO).

HOCHRISIKO-KI-SYSTEM

Hochrisiko-KI-Systeme sind solche, die entweder in bestimmte Produkte integriert oder in sensiblen Bereichen eingesetzt werden und erhebliche Schäden verursachen können. Die KI-Verordnung (KI-VO) regelt derartige Systeme in ihrem Artikel 6 sowie in den Anhängen I und III. Diese KI-Systeme gelten als derart risikobehaftet, dass Anbieter und Betreiber strenge Anforderungen erfüllen müs-

sen (z. B. Risikomanagement, Datenqualität, Transparenz, menschliche Aufsicht). Hochrisiko-KI-Systeme müssen zudem in eine EU-weit zugängliche Datenbank eingetragen werden.

Die Pflichten der einzelnen Akteure hängen maßgeblich von der Einstufung der KI-Systeme in eine der im Gesetz vorgesehenen Risikoklassen ab; die meisten Pflichten bestehen in Bezug auf als hochriskant eingestufte KI-Systeme. Die KI-VO differenziert generell zwischen KI-Systemen mit unannehmbarem (Art. 5 KI-VO), hohem (Art. 6 KI-VO), begrenztem (vgl. Art. 50 KI-VO) und minimalem Risiko.



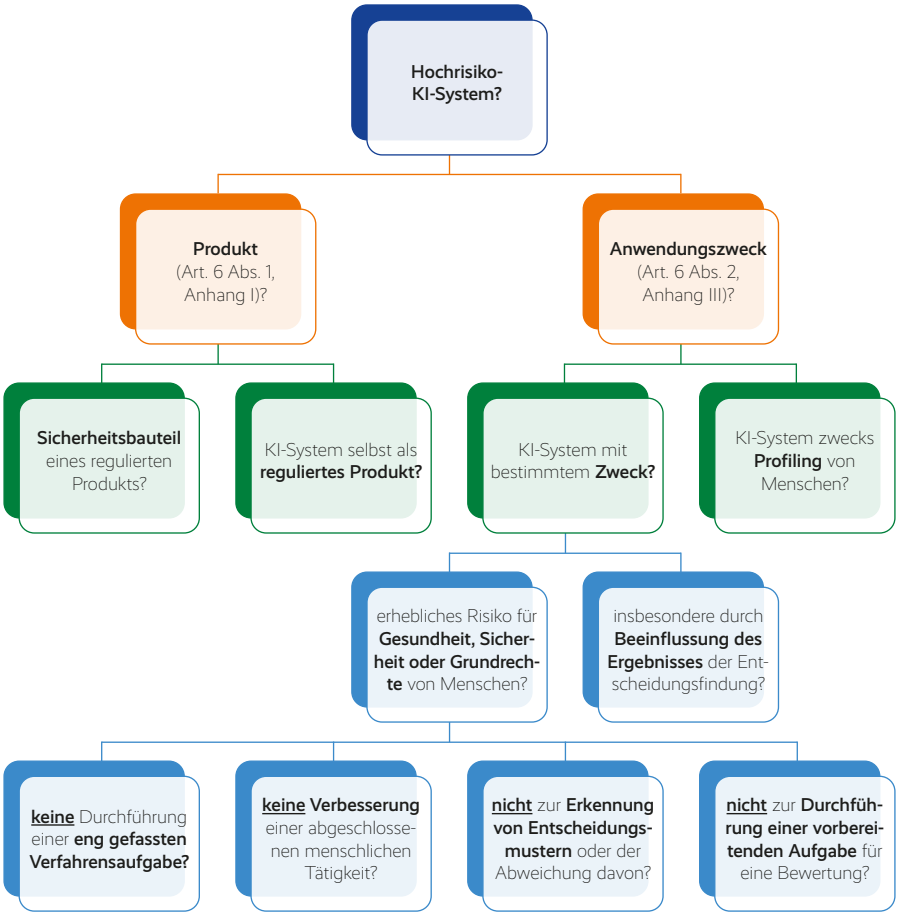
Risikoklassen-Pyramide

Hinweis:
Die Einteilung erfolgt häufig in die genannten vier Risikoklassen. Es lässt sich jedoch argumentieren, dass die Klasse „begrenztes Risiko" keine eigene Klasse ist, sondern nach Art. 50 KI-VO lediglich in bestimmten Konstellationen Transparenzpflichten vorgegeben werden. Zudem existiert noch eine „Sonderklasse", nämlich die Einordnung als KI mit allgemeinem Verwendungszweck (mit und ohne systemisches Risiko). Daher kann man auch von lediglich drei oder sogar von fünf Risikoklassen sprechen. Viel wichtiger ist jedoch die Beachtung des

risikobasierten Ansatzes, der, ähnlich wie im Datenschutz, auch im Rahmen der KI-VO zu beachten ist.

Die Prüfung, ob ein KI-System die Voraussetzungen von Art. 6 KI-VO erfüllt, ob es unter eine der Ausnahmeregelungen fällt oder ob eine Gegenausnahme greift, ist herausfordernd. Daher sollte sie sehr bedacht, aber dennoch zeitnah erfolgen.

Der Weg zum Ergebnis, ob ein KI-System als hochriskant eingestuft wird, verläuft in zwei verschiedenen Strängen: Es geht einerseits um die Frage, ob KI-Systeme in bestimmte Produktkategorien integriert werden. Andererseits muss auf den Anwendungszweck von KI-Systemen geschaut werden.



Schema Prüfung Hochrisiko-KI-System

Nach Maßgabe von Art. 6 Abs. 1, Anhang I KI-VO fällt ein KI-System in die Hochrisiko-Stufe, wenn es zu einer bestimmten, bereits durch EU-Vorschriften regulierten Produktkategorie gehört. Dazu zählen die folgenden Kategorien:

- Maschinen
- Spielzeug
- Sportboote/Wassermotorräder
- Aufzüge
- Geräte und Schutzsysteme für explosionsgefährdete Bereiche
- Funkanlagen
- Druckgeräte
- Seilbahnen
- Persönliche Schutzausrüstung
- Geräte zur Verbrennung gasförmiger Stoffe
- Medizinprodukte
- In-vitro-Diagnostika
- Sicherheit in der zivilen Luftfahrt
- zwei-, drei- oder vierrädrige Fahrzeuge
- land- und forstwirtschaftliche Fahrzeuge
- Schiffsausrüstung
- Eisenbahnsystem
- Kraftfahrzeuge/Kfz-Anhänger

Wenn ein KI-System als Sicherheitsbauteil in ein bereits als riskant eingestuftes und deshalb schon EU-weit reguliertes Produkt eingebunden werden soll, dann fällt dieses KI-System in die Hochrisiko-Klasse.

Der zweite Strang der Prüfung bezieht sich gemäß Art. 6 Abs. 2, Anhang III KI-VO auf bestimmte Einsatzzwecke. Danach sollen in den folgenden Bereichen Hochrisiko-KI-Systeme angesiedelt sein:

- erlaubte Biometrie (biometrische Fernidentifizierung, Emotionserkennung, biometrische Kategorisierung)

- KRITIS-Verwaltung und -Betrieb, z. B. digitale Infrastruktur, Straßenverkehr, Wasser-, Gas-, Wärmeoder Stromversorgung
- allgemeine und berufliche Bildung
- Beschäftigung, Personalmanagement und Zugang zur Selbstständigkeit
- Zugänglichkeit und Inanspruchnahme grundlegender privater und öffentlicher Dienste und Leistungen
- Strafverfolgung (z. B. Lügendetektor oder Profiling)
- Migration, Asyl und Grenzkontrolle
- Rechtspflege (Justizbehörden) und demokratische Prozesse

Nach Anhang III Nr. 2, ErwGr 56 KI-VO werden beispielsweise im Bildungsbereich folgende KI-Einsatzzwecke als hochriskant eingestuft:

- Zugang, Zulassung oder Zuweisung zu Bildung- und Berufsbildungseinrichtungen bzw. zu entsprechenden Programmen
- Bewertung von Lernergebnissen
- Bewertung oder wesentliche Beeinflussung des Bildungsniveaus
- Überwachung von verbotenem Verhalten von Schülern, Studenten, Azubis etc. während Prüfungen

Aber auch etwa für den Bereich Beschäftigung/Personalmanagement erfolgt in vielen Bereichen der KI-Einsatz im Hochrisiko-Bereich. Hierbei sind insbesondere folgende Szenarien möglich:

- Finden und Kontaktieren von potenziellen Kandidaten, beispielsweise über Social Media
- Sichtung von eingehenden Bewerbungen und Filterung geeigneter Kandidaten
- Analyse von Sprache, Tonfall, Mimik, Gestik etc.
- Auswertung von Onlineassessments und Filterung geeigneter Kandidaten
- Unterstützung bei der Entscheidung für bzw. gegen Bewerber
- Durchführung von Leistungsprognosen
- personalisiertes Onboarding

Die KI-VO sieht diverse Ausnahmefälle für bestimmte Konstellationen vor, die wieder aus dem Hochrisiko-Bereich herausfallen, soweit dabei kein erhebliches Risiko der Beeinträchtigung in Bezug auf die Gesundheit, Sicherheit oder Grundrechte von Menschen besteht (Art. 6 Abs. 3 KI-VO).

Beispiele für die in Art. 6 Abs. 3 lit. a) bis d) KI-VO genannten Ausnahmefälle finden sich in ErwGr 53 KI-VO:

Durchführung einer eng gefassten Verfahrensaufgaben	➤ Umwandlung von unstrukturierten in strukturierte Daten ➤ Kategorisierung eingehender Dokumente ➤ Erkennung von Duplikaten
Verbesserung des Ergebnisses einer zuvor abgeschlossenen menschlichen Tätigkeit	➤ Optimierung der Sprache in Dokumenten
Erkennung von Entscheidungsmustern oder Abweichungen von früheren Entscheidungsmustern	➤ Prüfung auf Abweichungen von Benotungsmustern von Lehrern etc. zur Aufdeckung von Unstimmigkeiten
Durchführung einer vorbereitenden Aufgabe für eine Bewertung	➤ Indexierung ➤ Suche ➤ Textverarbeitung ➤ Datenverknüpfung ➤ Übersetzung

Hinweis:
KI-Systeme, die nach Art. 6 Abs. 2, Anhang III KI-VO als hochriskant eingestuft werden, und auch solche, die gemäß Art. 6 Abs. 3 KI-VO ausnahmsweise aus dem Hochrisiko-Bereich auszuklammern sind, müssen gleichermaßen intern dokumentiert sowie auch in der EU-Datenbank für Hochrisiko-KI-Systeme registriert werden (vgl. Art. 71, 49, 6 Abs. 4 KI-VO).

Die EU-Kommission sollte spätestens bis zum 02.02.2026 Leitlinien zur praktischen Umsetzung von Art. 6 KI-VO und eine umfassende Liste praktischer Beispiele für Anwendungsfälle für KI-Systeme, die hochriskant oder nicht hochriskant sind, bereitstellen (vgl. Art. 6 Abs. 5 KI-VO). Dies ist bislang aber leider noch nicht geschehen.

Die Anbieter von Hochrisiko-KI-Systemen müssen die Anforderungen aus Art. 8 ff. KI-VO erfüllen (Art. 16 lit. a) KI-VO):

- Einhaltung der Anforderungen/Stand der Technik (Art. 8 KI-VO)
- Risikomanagementsystem (RMS) (Art. 9 KI-VO)
- Daten (qualitative Trainings-, Validierungs- und Testdatensätze)/Daten-Governance (Art. 10 KI-VO)
- technische Dokumentation (Art. 11, Anhang IV KI-VO)
- Aufzeichnungspflichten/Protokollierung (Art. 12 KI-VO)
- Transparenz/Bereitstellung von Informationen (Art. 13 KI-VO)
- menschliche Aufsicht (Art. 14 KI-VO)
- Genauigkeit, Robustheit und Cybersicherheit (Art. 15 KI-VO)

Zusätzlich obliegen den Anbietern noch folgende Pflichten:

- Anbringung von Handelsnamen und ggf. Handelsmarke sowie Kontaktanschrift (Art. 16 lit. b) KI-VO)
- Betrieb eines Qualitätsmanagementsystems (Art. 16 lit. c), Art. 17 KI-VO)
- Erstellen und Aufbewahren der erforderlichen Dokumentation (Art. 16 lit. d), Art. 18 KI-VO)
- Aufbewahren der erstellten Protokolle (Art. 16 lit. e), Art. 19 KI-VO)
- Durchlaufen des Konformitätsbewertungsverfahrens (Art. 16 lit. f), Art. 43 KI-VO)
- Ausstellen einer EU-Konformitätserklärung (Art. 16 lit. g), Art. 47, Anhang V KI-VO)
- Anbringung einer CE-Kennzeichnung (Art. 16 lit. h), Art. 48 KI-VO)
- Registrierung (Art. 16 lit. i), Art. 49, Anhang VIII KI-VO)
- Pflichtinformationen und ggf. Korrekturmaßnahmen (Art. 16 lit. j), Art. 20 KI-VO)
- Rechenschaftspflicht (Art. 16 lit. k) KI-VO
- Barrierefreiheitsanforderungen (Art. 16 lit. l) KI-VO
- Zusammenarbeit mit Behörden (Art. 21 KI-VO)
- Pflicht zur Meldung schwerwiegender Vorfälle (Art. 73, Art. 3 Nr. 49 KI-VO)
- Einrichtung und Dokumentation eines Systems zur Beobachtung nach dem Inverkehrbringen (Art. 72, Anhang IV KI-VO)

Hinweis:
In Nicht-EU-Staaten niedergelassene Anbieter müssen außerdem noch einen EU-Bevollmächtigen benennen (Art. 22 KI-VO).

Im Rahmen der Registrierung eines Hochrisiko-KI-Systems (Art. 49 KI-VO) sind diverse Informationen bereitzustellen. Dabei wird gemäß Anhang VIII KI-VO differenziert zwischen KI-Systemen, die nach Maßgabe von Art. 6 Abs. 2, Anhang III KI-VO als hochriskant gelten (Art. 49 Abs. 1 KI-VO), und solchen, die gemäß Art. 6 Abs. 3 KI-VO ausnahmsweise doch nicht als Hochrisiko-KI-System einzustufen sind (Art. 49 Abs. 2 KI-VO). Während diese Pflichten für Anbieter bestehen, sieht Art. 49 Abs. 3 KI-VO eine entsprechende Pflicht für Betreiber von Hochrisiko-KI-Systemen vor, die Behörden oder Organe, Einrichtungen oder sonstige Stellen der EU oder in ihrem Namen handelnde Personen sind.

Abschnitt A von Anhang VIII KI-VO enthält die im Lichte von Art. 49 Abs. 1 KI-VO von Anbietern bereitzustellenden Informationen:

- der Name, die Anschrift und die Kontaktdaten des Anbieters
- bei Vorlage von Informationen durch eine andere Person im Namen des Anbieters: der Name, die Anschrift und die Kontaktdaten dieser Person
- ggf. der Name, die Anschrift und die Kontaktdaten des Bevollmächtigten
- der Handelsname des KI-Systems und etwaige zusätzliche eindeutige Angaben, die die Identifizierung und Rückverfolgbarkeit des KI-Systems ermöglichen
- eine Beschreibung der Zweckbestimmung des KI-Systems und der durch dieses KI-System unterstützten Komponenten und Funktionen
- eine grundlegende und knappe Beschreibung der vom System verwendeten Informationen (Daten, Eingaben) und seiner Betriebslogik
- der Status des KI-Systems (in Verkehr/in Betrieb; nicht mehr in Verkehr/in Betrieb, zurückgerufen)
- die Art, die Nummer und das Ablaufdatum der von der notifizierten Stelle ausgestellten Bescheinigung und ggf. Name oder Identifizierungsnummer dieser notifizierten Stelle
- ggf. eine gescannte Kopie der Bescheinigung der notifizierenden Stelle
- alle Mitgliedstaaten, in denen das KI-System in Verkehr gebracht, in Betrieb genommen oder in der Union bereitgestellt wurde

- eine Kopie der in Art. 47 KI-VO genannten EU-Konformitätserklärung
- elektronische Betriebsanleitungen; dies gilt nicht für Hochrisiko-KI-Systeme in den Bereichen Strafverfolgung oder Migration, Asyl und Grenzkontrolle gemäß Anhang III Nr. 1, 6, 7 KI-VO
- eine URL-Adresse für zusätzliche Informationen (fakultativ)

Dagegen enthält Abschnitt B von Anhang VIII die von Anbietern von Hochrisiko-KI-Systemen gemäß Art. 49 Abs. 2 KI-VO bereitzustellenden Informationen:

- der Name, die Anschrift und die Kontaktdaten des Anbieters
- bei Vorlage von Informationen durch eine andere Person im Namen des Anbieters: Name, Anschrift und Kontaktdaten dieser Person
- ggf. der Name, die Anschrift und die Kontaktdaten des Bevollmächtigten
- der Handelsname des KI-Systems und etwaige zusätzliche eindeutige Angaben, die die Identifizierung und Rückverfolgbarkeit des KI-Systems ermöglichen
- eine Beschreibung der Zweckbestimmung des KI-Systems
- die Bedingung oder Bedingungen gemäß Art. 6 Abs. 3 KI-VO, aufgrund derer das KI-System nicht als Hochrisiko-System eingestuft wird
- eine kurze Zusammenfassung der Gründe, aus denen das KI-System in Anwendung des Verfahrens gemäß Art. 6 Abs. 3 KI-VO nicht als Hochrisiko-System eingestuft wird
- der Status des KI-Systems (in Verkehr/in Betrieb; nicht mehr in Verkehr/in Betrieb, zurückgerufen)
- alle Mitgliedstaaten, in denen das KI-System in der Union in Verkehr gebracht, in Betrieb genommen oder bereitgestellt wurde

Hingegen finden sich in Abschnitt C von Anhang VIII die von Betreibern von Hochrisiko-KI-Systemen gemäß Art. 49 Abs. 3 KI-VO bereitzustellende Informationen:

- der Name, die Anschrift und die Kontaktdaten des Betreibers
- der Name, die Anschrift und die Kontaktdaten der Person, die im Namen des Betreibers Informationen übermittelt
- die URL des Eintrags des KI-Systems in der EU-Datenbank durch seinen Anbieter

- eine Zusammenfassung der Ergebnisse der gemäß Art. 27 KI-VO durchgeführten Grundrechte-Folgenabschätzung
- ggf. eine Zusammenfassung der im Einklang mit Art. 35 Datenschutzgrundverordnung (DSGVO) gemäß Art. 26 Abs. 8 KI-VO durchgeführten Datenschutz-Folgenabschätzung

Hinweis:
Diese Informationen, die im Zuge der Registrierung angegeben werden, müssen anschließend aktuell gehalten und ggf. korrigiert werden. Die Einstufung als Hochrisiko-KI-System sollte einem strukturierten Prozess zur Aufnahme folgen. Dieser stellt sicher, dass die nachher für die Dokumentation und zur Erfüllung erforderlicher Berichtspflichten notwendigen Informationen aufgenommen werden und idealerweise an zentraler Stelle gespeichert werden. Je nach Institution und Prüfprozess lassen sich die Anforderungen nach KI-VO und DSGVO insbesondere im Betreiberkontext kombinieren und einheitlich abfragen und Umsetzungsmaßnahmen einheitlich definieren.

Betreiber von Hochrisiko-KI-Systemen sind aber auch nicht ganz unbeteiligt, ihnen obliegen nämlich die folgenden Pflichten:

- Umsetzung geeigneter technischer und organisatorischer Maßnahmen um sicherzustellen, dass das KI-System entsprechend der Betriebsanleitung verwendet wird (Art. 26 Abs. 1 KI-VO)
- Übertragung der menschlichen Aufsicht an Personen, die über die erforderliche Kompetenz, Ausbildung und Befugnis verfügen (Art. 26 Abs. 2 KI-VO)
- Sicherstellen, dass Eingabedaten der Zweckbestimmung des KI-Systems entsprechen und ausreichend repräsentativ sind (Art. 26 Abs. 4 KI-VO)
- Überwachen des Betriebs des KI-Systems und Benachrichtigung von Anbieter, Händler und/oder Überwachungsbehörde bei Risiko für Gesundheit, Sicherheit oder Grundrechte bzw. schwerwiegenden Vorfall (Art. 26 Abs. 5 KI-VO)
- Aufbewahren der durch das KI-System automatisch erzeugten Protokolle für einen angemessenen Zeitraum von mindestens sechs Monaten (Art. 26 Abs. 6 KI-VO)
- Bereitstellen von Pflichtinformationen gegenüber Beschäftigten und ggf. Betriebs- bzw. Personalratsmitgliedern bei Einsatz von KI-Systemen am Arbeitsplatz (Art. 26 Abs. 7 KI-VO)

- Durchführung einer Datenschutz-Folgenabschätzung (Art. 13, 26 Abs. 9 KI-VO i. V. m. Art. 35 DSGVO)
- Bereitstellen von Pflichtinformationen gegenüber Personen, über die das KI-System Entscheidungen trifft oder bei denen es Unterstützung leistet (Art. 26 Abs. 11 KI-VO, ggf. Art. 50 KI-VO)
- Zusammenarbeit mit der zuständigen Behörde (Art. 26 Abs. 12 KI-VO)
- Betreiber, die Strafverfolgungsbehörden oder Ähnliches im Sinne der EU-Datenschutzrichtlinie zur Zusammenarbeit im Bereich Justiz und Inneres sind: Antrag auf Genehmigung zur Nutzung eines KI-Systems zur biometrischen Fernidentifizierung und Dokumentation der Verwendung des KI-Systems sowie Vorlegen eines Jahresberichts an die Marktüberwachungsbehörde (Art. 26 Abs. 10 KI-VO)
- Betreiber, bei denen es sich um Einrichtungen des öffentlichen Rechts handelt oder um private Einrichtungen, die öffentliche Dienste erbringen: Durchführung einer Grundrechte-Folgenabschätzung (Art. 27 KI-VO)

INBETRIEBNAHME

Der Begriff „Inbetriebnahme" wird in Art. 3 Nr. 11 KI-Verordnung folgendermaßen definiert:

„die Bereitstellung eines KI-Systems in der Union zum Erstgebrauch direkt an den Betreiber oder zum Eigengebrauch entsprechend seiner Zweckbestimmung"

Es geht hier also um den Moment, in dem ein KI-System nach dem ersten Markteintritt erstmals bestimmungsgemäß aktiviert bzw. eingesetzt wird. Beispiel: Ein Hersteller bringt ein KI-gesteuertes Medizinprodukt auf den Markt (Inverkehrbringen), und ein Krankenhaus setzt es ein – Letzteres ist die Inbetriebnahme.

INFORMATIONSPFLICHTEN

Informationspflichten sind gesetzlich vorgeschriebene Pflichten, Betroffene und Behörden zu informieren. Im Datenschutz umfassen sie z. B. die Transparenzpflichten gemäß Art. 13, 14 Datenschutzgrundverordnung, also die Pflicht, Betroffene proaktiv unter anderem über Zweck, Speicherdauer, Rechtsgrundlage etc. zu

informieren. In Bezug auf KI-Systeme gibt es nach Art. 50 KI-Verordnung ebenfalls Transparenz- und Informationspflichten (s. Abschnitt „Transparenzpflichten“).

Anbieter bzw. Betreiber müssen in bestimmten Konstellationen bestimmte Informationen bereitstellen. Ziel ist es, Nutzern und Betroffenen die KI-Entscheidungen verständlich zu machen und Datenschutz zu gewährleisten.

INVERKEHRBRINGEN

Der Begriff „Inverkehrbringen“ wird gemäß Art. 3 Nr. 9 KI-Verordnung (KI-VO) wie folgt beschrieben:

„die erstmalige Bereitstellung eines KI-Systems oder eines KI-Modells mit allgemeinem Verwendungszweck auf dem Unionsmarkt“

„Bereitstellung“ auf dem Markt ist dabei die entgeltliche oder unentgeltliche Abgabe eines KI-Systems oder eines KI-Modells mit allgemeinem Verwendungszweck zum Vertrieb oder zur Verwendung auf dem Unionsmarkt im Rahmen einer Geschäftstätigkeit (Art. 3 Nr. 10 KI-VO).

Wann ein Produkt als „in Verkehr gebracht“ gilt, entscheidet der Moment des Verkaufs oder der kostenlosen Abgabe im Markt.

ISO 42001

Die ISO-Norm 42001 bietet Vorgaben für ein KI-Managementsystem (KIMS), das Institutionen bei der Entwicklung, Bereitstellung und Nutzung von KI-Systemen unterstützt. Sie ist der weltweit erste zertifizierbare internationale Standard für KIMS und umfasst Themen wie Transparenz, Verantwortlichkeit, Risikomanagement und Ethik.

Diese Norm ist besonders relevant für die Einhaltung der Anforderungen an Hochrisiko-KI-Systeme gemäß Art. 6 KI-Verordnung (KI-VO), wie Risikomanagement, Governance und Datensatzqualität. Denn sie bietet einen strukturierten Rahmen zur verantwortungsvollen Entwicklung, Implementierung und Nutzung von KI-Systemen, um Risiken zu minimieren und Vertrauen zu schaffen. Institutionen, die diese Norm implementieren, können eine Vermutung der Konformität gemäß Art. 40 KI-VO genießen, sofern die Norm als harmonisierter Standard anerkannt wird.

Hinweis:
Die ISO 42001 gilt branchenübergreifend und ist mit anderen Standards, wie z. B. der ISO 27001, kompatibel.

Die Kernaspekte und Ziele der ISO 42001 sind:

- Verantwortungsvolle KI: Sicherstellung ethischer Grundsätze und Transparenz im gesamten KI-Lebenszyklus
- Risikomanagement: effektive Identifikation und Behandlung KI-spezifischer Risiken
- Compliance: Unterstützung bei der Einhaltung rechtlicher Vorgaben, einschließlich potenzieller Anforderungen der KI-VO
- Struktur: basiert auf der „High-Level Structure" (HLS) und dem PDCA-Zyklus (Plan – Do – Check – Act) für kontinuierliche Verbesserung
- Zertifizierung: ermöglicht Unternehmen, durch unabhängige Audits nachzuweisen, dass sie KI verantwortungsvoll einsetzen.

IT-SICHERHEIT

IT-Sicherheit umfasst alle Maßnahmen, die Informationen und Systeme vor unbefugtem Zugriff, Missbrauch, Ausfall oder Zerstörung schützen. Im Datenschutz ist IT-Sicherheit zentral: Art. 32 Datenschutzgrundverordnung verpflichtet Verantwortliche und Auftragsverarbeiter zur Umsetzung „geeigneter technischer und organisatorischer Maßnahmen" für ein dem Risiko angemessenes Schutzniveau. Dazu zählen beispielsweise Verschlüsselung, Back-ups, Firewalls etc. Ein „IT-Sicherheitsvorfall" bzw. „Datenschutzvorfall" (sogenannte Datenpanne) ist etwa ein Hackerangriff, Malware-Befall oder Systemausfall, der Daten gefährdet. Für besonders kritische Infrastrukturen (KRITIS-Bereich) gelten zudem spezifische IT-Sicherheitsgesetze (z. B. durch die NIS2-Richtlinie bzw. deren deutsches Umsetzungsgesetz).

KI-BEAUFTRAGTER

Ein KI-Beauftragter (engl.: AI Officer), oft auch als „KI-Manager" bezeichnet, ist ein Experte oder Funktionsträger für KI-Fragen. Während die KI-Verordnung (KI-VO)

keinen speziellen „KI-Beauftragten“ vorschreibt, ist eine solche Rolle sehr wohl zu empfehlen, um die erforderliche KI-Kompetenz im Unternehmen sicherzustellen. In Art. 4 KI-VO wird die sogenannte KI-Kompetenz gefordert. Daraus ergibt sich, dass Anbieter und Anwender über ein ausreichendes Maß an KI-Kompetenz verfügen müssen. Ein KI-Beauftragter kann Fachabteilungen schulen und beraten, sorgt für die Umsetzung der KI-VO im Unternehmen bzw. in der Behörde (z. B. Risiko-Management, Dokumentation) und kann als Schnittstelle zu Aufsichtsbehörden fungieren. Insbesondere für Institutionen, in denen im hohen Maße KI genutzt wird, ist diese Rolle/Funktion – analog zum Datenschutzbeauftragten – sehr sinnvoll. Mittelbar kann sich eine Pflicht zur Bestellung eines KI-Beauftragten auch aus Vorgaben gemäß ISO 42001 ergeben.

KI-COMPLIANCE

KI-Compliance umfasst alle Prozesse und Maßnahmen, die ein Unternehmen ergreift, um dem rechtlichen Rahmen für den Einsatz von KI, insbesondere KI-Verordnung (KI-VO) und ergänzende Gesetze, zu genügen. Das betrifft etwa den Aufbau eines Risikomanagementsystems für KI (Art. 9 KI-VO), regelmäßige Audits von KI-Anwendungen, Fortbildung der Mitarbeiter (Art. 4 KI-VO), interne Richtlinien (einschließlich der Prozesse und Rollen) und Dokumentationen. Ziel ist, Strafen zu vermeiden (z. B. Bußgelder von bis zu 35 Mio. Euro oder 7 % des Umsatzes) und Vertrauen zu schaffen.

KI-GRUNDSÄTZE

Die sieben Grundsätze, die zwar unverbindlich sind, jedoch im Rahmen der KI-Verordnung beachtet werden sollten, lauten wie folgt (ErwGr 27 KI-VO):

- **„menschliches Handeln und menschliche Aufsicht“:** bedeutet, dass ein KI-System entwickelt und als Instrument verwendet wird, das den Menschen dient, die Menschenwürde und die persönliche Autonomie achtet und so funktioniert, dass es von Menschen angemessen kontrolliert und überwacht werden kann
- **„technische Robustheit und Sicherheit“:** bedeutet, dass KI-Systeme so entwickelt und verwendet werden, dass sie im Fall von Schwierigkeiten robust

sind und widerstandsfähig gegen Versuche, die Verwendung oder Leistung des KI-Systems so zu verändern, dass dadurch die unrechtmäßige Verwendung durch Dritte ermöglicht wird, und dass ferner unbeabsichtigte Schäden minimiert werden

- **„Privatsphäre und Daten-Governance“:** bedeutet, dass KI-Systeme im Einklang mit den geltenden Vorschriften zum Schutz der Privatsphäre und zum Datenschutz entwickelt und verwendet werden und dabei Daten verarbeiten, die hohen Qualitäts- und Integritätsstandards genügen

- **„Transparenz“:** bedeutet, dass KI-Systeme so entwickelt und verwendet werden, dass sie angemessen nachvollziehbar und erklärbar sind, wobei den Menschen bewusst gemacht werden muss, dass sie mit einem KI-System kommunizieren oder interagieren, und dass die Betreiber ordnungsgemäß über die Fähigkeiten und Grenzen des KI-Systems informieren und die betroffenen Personen über ihre Rechte in Kenntnis setzen müssen

- **„Vielfalt, Nichtdiskriminierung und Fairness“:** bedeutet, dass KI-Systeme in einer Weise entwickelt und verwendet werden, die unterschiedliche Akteure einbezieht und den gleichberechtigten Zugang, die Geschlechtergleichstellung und die kulturelle Vielfalt fördert, wobei diskriminierende Auswirkungen und unfaire Verzerrungen, die nach Unionsrecht oder nationalem Recht verboten sind, verhindert werden

- **„soziales und ökologisches Wohlergehen“:** bedeutet, dass KI-Systeme in nachhaltiger und umweltfreundlicher Weise und zum Nutzen aller Menschen entwickelt und verwendet werden, wobei die langfristigen Auswirkungen auf den Einzelnen, die Gesellschaft und die Demokratie überwacht und bewertet werden

- **„Rechenschaftspflicht“:** bedeutet, dass die Einhaltung der gesetzlichen Vorgaben im Zweifel nachgewiesen werden können muss

Die Anwendung dieser Grundsätze sollte, soweit möglich, in die Gestaltung und Verwendung von KI-Modellen einfließen. Denn diese ethischen Grundsätze sollen dazu beitragen, dass KI vertrauenswürdig und ethisch vertretbar ist.

Unbeschadet der rechtsverbindlichen Anforderungen der KI-VO und anderer geltender Rechtsvorschriften tragen diese Grundsätze zur Gestaltung kohärenter, vertrauenswürdiger und menschenzentrierter KI bei, im Einklang mit der EU-Grundrechtecharta und den Werten, auf die sich die Union gründet.

Hinweis:
Alle Interessenträger, einschließlich der Industrie, der Wissenschaft, der Zivilgesellschaft und der Normungsorganisationen, werden aufgefordert, die ethischen Grundsätze bei der Entwicklung freiwilliger bewährter Verfahren und Normen, soweit angebracht, zu berücksichtigen.

KI-INPUT

Als KI-Input bezeichnet man die Daten oder Informationen, die einem KI-System zur Verarbeitung zugeführt werden (z. B. Sensordaten, Nutzereingaben, Trainings- oder Finetuning-Daten). Die Qualität des KI-Inputs bestimmt entscheidend die Leistung des KI-Systems, also den KI-Output („put garbage in, get garbage out"). Im rechtlichen Kontext wird darauf geachtet, dass Trainings-, Test- und Eingabedaten möglichst frei von Vorurteilen sind und insbesondere auch mit Blick auf personenbezogene Daten den datenschutzrechtlichen Anforderungen entsprechen.

Hinweis:
Aber auch Daten ohne Personenbezug können einem Geheimhaltungsinteresse unterfallen; diese sollten dann möglichst nicht in eine KI eingegeben werden. Das gilt jedenfalls in Bezug auf ein KI-Cloud-Angebot (Software-as-a-Service, SaaS). Auf die Eingabe von Geschäftsgeheimnissen, Log-in-Daten unter anderen sensiblen Informationen in die KI sollte nach Möglichkeit verzichtet werden.

Im Rahmen der Nutzung von KI können neben dem eigentlichen Prompt oder in die KI eingebundenen Dateien auch noch weitere Vorgänge relevant sein. Denn auch z. B. im Zuge des Finetunings oder eines individuellen KI-Trainings sind die einschlägigen rechtlichen Vorgaben zu beachten.

KI-KOMPETENZ

Nach Art. 4 KI-Verordnung (KI-VO) müssen Anbieter und Betreiber ein „ausreichendes Maß an KI-Kompetenz" gewährleisten. Damit ist gemeint, dass Unternehmen und Behörden Fachwissen in Entwicklung, Erprobung, Einsatz und Überwachung von KI-Systemen vorweisen müssen. Diese KI-Kompetenz (engl.: AI Literacy) kann insbesondere durch die Aus- und Weiterbildung von Fachleuten sicherstellen, dass

Die KI-Nutzung hat viele unterschiedliche Facetten.

KI-Anwendungen technisch richtig gestaltet, eingesetzt und überwacht werden. Fehlt sie, kann dies als Mangel in der Sorgfaltspflicht gelten.

Hinweis:
Die KI-VO sieht zwar keine direkten Sanktionen für einen Verstoß gegen die Pflicht aus Art. 4 KI-VO vor, insbesondere ist ein solcher nicht mit einem Bußgeld bedroht. Allerdings droht bei etwaigen Schäden durch Fehler im Zusammenhang mit dem KI-Einsatz eine Haftungsverschärfung. Zudem stellt die Nichtbeachtung der Anforderungen zur KI-Kompetenz einen Compliance-Verstoß dar.

Alle Anbieter und Betreiber von KI-Systemen müssen ein gewisses Maß an KI-Kompetenz nachweisen können. Diese Pflicht ist in Art. 4 KI-VO geregelt und bewusst an den Anfang der KI-VO gestellt, also sozusagen „vor die Klammer gezogen". Die Vorschrift lautet:

„Die Anbieter und Betreiber von KI-Systemen ergreifen Maßnahmen, um nach besten Kräften sicherzustellen, dass ihr Personal und andere Personen, die in ihrem Auftrag mit dem Betrieb und der Nutzung von KI-Systemen befasst sind, über ein ausreichendes Maß an KI-Kompetenz verfügen, wobei ihre technischen Kenntnisse, ihre Erfahrung, ihre Ausbildung und Schulung und der Kontext, in dem die KI-Systeme eingesetzt werden sollen, sowie die Personen oder Personengruppen, bei denen die KI-Systeme eingesetzt werden sollen, zu berücksichtigen sind."

Daraus folgen in puncto KI-Kompetenz gleich mehrere Dinge:

- Die Pflicht gilt sowohl für Anbieter als auch für Betreiber.
- Sie besteht unabhängig von der Einordnung in eine der verschiedenen KI-Risikoklassen.
- Die KI-Kompetenz muss in Bezug auf Beschäftigte und auch auf andere Personen, die mit Betrieb und Nutzung von KI-Systemen beauftragt sind (z. B. Freelancer, IT-Dienstleister), gewährleistet werden.
- Es sollen der berufliche Background sowie die Erfahrungen der betreffenden Personen und außerdem die KI-Anwendungsgebiete berücksichtigt werden.

Das bedeutet also, dass eine generische Fortbildung, in der wie „mit der Gießkanne" alle Beschäftigten geschult werden, nicht ausreichend sein dürfte. Es gilt vielmehr, ein gut dokumentiertes, individuell auf einzelne Personengruppen (z. B. „Einsteiger", „Fortgeschrittene" und „Profis") abgestimmtes Schulungskonzept zu erstellen und umzusetzen.

Fortbildungen sind sicherlich das zentrale Mittel zur Umsetzung der KI-Kompetenz, allerdings nicht das alleinige. Das legt die Definition des Begriffs „KI-Kompetenz" aus Art. 3 Nr. 56 KI-VO nahe:

„die Fähigkeiten, die Kenntnisse und das Verständnis, die es Anbietern, Betreibern und Betroffenen unter Berücksichtigung ihrer jeweiligen Rechte und Pflichten im Rahmen dieser Verordnung ermöglichen, KI-Systeme sachkundig einzusetzen sowie sich der Chancen und Risiken von KI und möglicher Schäden, die sie verursachen kann, bewusst zu werden"

Ergänzend dazu führt ErwGr 20 S. 1-6 KI-VO noch Folgendes aus:

„Um den größtmöglichen Nutzen aus KI-Systemen zu ziehen und gleichzeitig die Grundrechte, Gesundheit und Sicherheit zu wahren und eine demokratische Kontrolle zu ermöglichen, sollte die KI-Kompetenz Anbieter, Betreiber und betroffene Personen mit den notwendigen Konzepten ausstatten, um fundierte Entscheidungen über KI-Systeme zu treffen. Diese Konzepte können in Bezug auf den jeweiligen Kontext unterschiedlich sein und das Verstehen der korrekten Anwendung technischer Elemente in der Entwicklungsphase des KI-Systems, der bei seiner Verwendung anzuwendenden Maßnahmen und der geeigneten Auslegung der Ausgaben des KI-Systems umfassen sowie – im Falle betroffener Personen – das nötige Wissen, um zu verstehen, wie sich mithilfe von KI getroffene Entscheidungen auf sie auswirken werden. Im Zusammenhang mit der Anwendung dieser Verordnung sollte die KI-Kompetenz allen einschlägigen Akteuren […] die Kenntnisse vermitteln, die erforderlich sind, um die angemessene Einhaltung und die ordnungsgemäße Durchsetzung der Verordnung sicherzustellen."

Hinweis:
KI-Kompetenz sollte also juristische, technische, operative, aber auch ethische Aspekte umfassen.

Die Person, die bei einem Betreiber eines Hochrisiko-KI-Systems zur Kontrolle/Überwachung desselben zuständig ist, muss über die „normale" KI-Kompetenz hinaus noch weitere Kenntnisse erlangen. Das lässt sich aus Art. 14 Abs. 4, ErwGr 73, 91 KI-VO herauslesen. Denn dort finden sich spezielle Anforderungen an so eine menschliche Aufsicht:

- Verstehen der einschlägigen Fähigkeiten und Grenzen des KI-Systems
- Fähigkeit zur ordnungsgemäßen Überwachung des KI-Systems
- Erkennen und Beheben von Anomalien, Fehlfunktionen sowie unerwarteter Leistung
- Bewusstsein für eine mögliche Neigung zum automatischen oder übermäßigen Vertrauen in die vom KI-System hervorgebrachte Ausgabe („Automatisierungsbias")
- Fähigkeit zur richtigen Interpretation der Ausgabe des KI-Systems
- Entscheidungsfähigkeit, in bestimmten Situationen das KI-System nicht zu verwenden oder die Ausgabe des KI-Systems außer Acht zu lassen, außer Kraft zu setzen oder rückgängig zu machen

- Fähigkeit zum Eingriff in den Betrieb oder zur Unterbrechung des Betriebs des KI-Systems

Die genannten Anforderungen stellen einerseits folglich einen notwendigen Teil der KI-Kompetenz der menschlichen Aufsicht über Hochrisiko-KI-Systeme dar. Andererseits dürften diese speziellen Vorgaben gerade nicht für die KI-Kompetenz in Bezug auf KI-Systeme mit begrenztem oder minimalem Risiko gelten; jedenfalls nicht zwingend und nicht in jedem Fall.

Die EU-Kommission hat ein sogenanntes „Lebendiges Repositorium" zur Förderung des Lernens und des Austauschs über KI-Kompetenz herausgebracht (Stand: Januar 2025). Darin finden sich exemplarische Maßnahmen aus der Praxis unterschiedlicher Unternehmen. Dieser Aufstellung lassen sich folgende Punkte als mögliche sinnvolle KI-Kompetenz-Maßnahmen entnehmen:

- Liste möglicher Anwendungsfälle („use cases")
- umfassendes Schulungskonzept bzw. ein globales digitales Weiterbildungs- und Umschulungsprogramm
- Reihe interner Akademien für spezifische Rollen bzw. Anwendungsbereiche (IT, Rechtsabteilung, Personalbereich ...)
- unterschiedliche Lernangebote (z. B. Live-Webinare, Workshops, Video- oder Podcasts, E-Learnings, VR-Simulationen, spielbasierte und Storytelling-orientierte Trainingsmethoden)
- Aufteilung der Inhalte (KI-Grundlagen, bereichsspezifische KI, juristische Aspekte, KI-Risiken, Schulungen mit Praxisübungen ...)
- Bereitstellung von schriftlichem Schulungs- und Informationsmaterial
- interne Plattform als Informations- und Kommunikationsportal
- Betrieb interner KI-Test-Plattformen
- Einrichtung eines interdisziplinären KI-Teams
- Fortschrittsüberwachung bzw. regelmäßige Evaluation und Anpassung des Schulungskonzepts bzw. der einzelnen Angebote
- Möglichkeit für Feedback
- Zusammenarbeit mit externen Experten
- Mentorenprogramm

- interne KI-Richtlinie (KI-Guideline)
- Arbeits- bzw. Dienstanweisungen und ggf. Betriebs- bzw. Dienstvereinbarungen sowie Zusammenarbeit mit Betriebsrat oder Personalrat
- regelmäßige Sensibilisierungsmaßnahmen bzw. -veranstaltungen
- Umsetzung eines KI-Management-Systems nach ISO 42001
- Maßnahmen für das Change-Management
- Prüfung von KI-Kenntnissen im Rahmen des Bewerbungs- bzw. Einstellungsverfahrens
- spezielle Qualifizierung einzelner Mitarbeiter als interne Multiplikatoren
- Daten-Management-System (Daten-Governance)

Natürlich müssen nicht immer alle der genannten Punkte umgesetzt werden, um KI-Kompetenz gemäß Art. 4 KI-VO gewährleisten zu können. Welche Maßnahmen im eigenen Unternehmen oder in einer Behörde sinnvoll sind und zur betreffenden Institution passen, das muss jeder für sich selbst entscheiden.

Mit einer umfangreichen FAQ-Sammlung beleuchtet die EU-Kommission das Thema „KI-Kompetenz" noch etwas genauer. Darin werden auszugsweise unter anderem folgende Fragen geklärt (in eigener Übersetzung aus dem Englischen):

- **„Welche Zielgruppe fällt in den Anwendungsbereich von Art. 4 KI-VO? Wer sind ‚andere Personen'?"**

  „Dies betrifft jeden in der Organisation, der sich direkt mit einem KI-System befasst […]. ‚Personen, die im Auftrag von Anbietern/Arbeitgebern mit dem Betrieb und der Nutzung von KI-Systemen befasst sind' bedeutet, dass es sich nicht um Arbeitnehmer handelt, sondern um Personen, die […] in den organisatorischen Zuständigkeitsbereich fallen. Es kann z. B. ein Auftragnehmer, ein Dienstleister oder ein Kunde sein."

- **„Muss ein Unternehmen, dessen Mitarbeiter ChatGPT z. B. zum Verfassen von Werbetexten oder zur Übersetzung von Texten nutzen, die Anforderung an die KI-Kompetenz gemäß Art. 4 KI-VO erfüllen?"**

  „Ja, sie sollten über die spezifischen Risiken, z. B. Halluzinationen, informiert werden."

- **„Welche Mindestinhalte sollten für ein KI-Kompetenzprogramm gemäß Art. 4 KI-VO berücksichtigt werden?"**

„Das Amt für künstliche Intelligenz wird keine strengen Anforderungen an Art. 4 KI-VO und dessen ‚ausreichende KI-Kompetenz' stellen. Im Gegenteil, sie hält […] ein gewisses Maß an Flexibilität für erforderlich. Um jedoch Art. 4 KI-VO einzuhalten, sollten Anbieter und Betreiber von KI-Systemen mindestens

a) ein allgemeines Verständnis von KI in ihrer Organisation gewährleisten: Was ist KI? Wie funktioniert sie? Welche KI wird in unserer Organisation eingesetzt? Was sind ihre Chancen und Gefahren?

b) die Rolle ihrer Organisation (Anbieter oder Betreiber von KI-Systemen) berücksichtigen: Entwickelt meine Organisation KI-Systeme oder verwendet sie nur KI-Systeme, die von einer anderen Organisation entwickelt wurden?

c) das Risiko der bereitgestellten KI-Systeme berücksichtigen: Was müssen Mitarbeiter wissen, wenn sie mit einem solchen KI-System zu tun haben? Was sind die Risiken, denen sie sich bewusst sein müssen, und müssen sie sich der Minderung bewusst sein?

d) einen konkreten Aufbau ihrer KI-Kompetenzmaßnahmen auf der vorhergehenden Analyse vornehmen unter Berücksichtigung von:

- *Unterschieden bei den technischen Kenntnissen, der Erfahrung, der Aus- und Weiterbildung des Personals unter anderen Personen. Wie viel wissen die Personen über KI und die von ihnen verwendeten Systeme der Organisation? Was sollten sie sonst noch wissen?*
- *Kontext, in dem die KI-Systeme verwendet werden sollen, und die Personen, bei denen die KI-Systeme verwendet werden sollen. In welchem Sektor und zu welchem Zweck/Dienst wird das KI-System verwendet?*

Diese Punkte umfassen rechtliche und ethische Aspekte. Daher werden ein Verständnis der KI-VO sowie zu Ethik- und Governance-Grundsätzen gefördert."

- **„Ist eine KI-Schulung für Art. 4 KI-VO obligatorisch, oder sind auch andere KI-Kompetenzinitiativen zulässig?"**

„[…] In vielen Fällen kann es jedoch unwirksam und unzureichend sein, sich einfach auf die Gebrauchsanweisungen der KI-Systeme zu verlassen oder das Personal aufzufordern, sie zu lesen. Art. 4 KI-VO soll Schulungen und Orientierungshilfen bieten, die auf der Grundlage des Kenntnisstands und der Art des Wissens jeder Zielgruppe sowie des Kontexts und des Zwecks der in der Organisation verwendeten KI-Systeme am besten geeignet sind. […] In Art. 26 KI-VO wird z. B. eine Verpflichtung für Betreiber von Hochrisiko-Systemen eingeführt, um

sicherzustellen, dass das mit den KI-Systemen befasste Personal in der Praxis ausreichend geschult ist, um mit dem System umzugehen und die menschliche Aufsicht zu gewährleisten. Sich auf die Gebrauchsanweisung zu verlassen reicht daher nicht aus, weitere Maßnahmen sind erforderlich."

- **„Dürfen KI-Kompetenztrainingskonzepte zwischen verschiedenen Detaillierungsgraden unterscheiden?"**

  „Ja, Art. 4 KI-VO ermutigt Anbieter und Betreiber, das Wissen, die Erfahrung, die Aus- und Weiterbildung von Mitarbeitern unter anderen Personen zu berücksichtigen, um ein ausreichendes Maß an KI-Kompetenz zu gewährleisten. Angesichts des Unterschieds zwischen KI-Systemen und der Tatsache, dass der Wissens- und Erfahrungsstand sowie die Art der erhaltenen allgemeinen und beruflichen Bildung variieren können, können unterschiedliche Ausbildungsniveaus oder Lernansätze angemessen sein."

- **„Wie müssen Organisationen ihre Maßnahmen dokumentieren, um Art. 4 KI-VO und die darin enthaltenen Best-Effort-Bestimmungen einzuhalten? Benötigen sie spezielle Zertifikate?"**

  „Ein Zertifikat ist nicht erforderlich. Organisationen können interne Aufzeichnungen über Schulungen [...] führen."

- **„Wann beginnt die Durchsetzung? Ist ein Unternehmen bereits zu spät bzw. in Gefahr, wenn es noch keine etablierte KI-Kompetenzinitiative hat?"**

  „Art. 4 KI-VO trat am 02.02.2025 in Kraft, daher gilt bereits die Verpflichtung, Maßnahmen zu ergreifen, um die KI-Kompetenz seiner Mitarbeiter sicherzustellen. Die Aufsichts- und Durchsetzungsvorschriften gelten ab dem 03.08.2026."

- **„Welche Folgen könnte es für eine Organisation geben, wenn davon ausgegangen wird, dass sie Art. 4 KI-VO nicht einhält?"**

  „Die nationalen Marktüberwachungsbehörden könnten Sanktionen und andere Durchsetzungsmaßnahmen verhängen, um Verstöße gegen Art. 4 KI-VO zu ahnden. Grundlage hierfür sind die nationalen Rechtsvorschriften, die die Mitgliedstaaten bis zum 02.08.2025 erlassen sollen. Es ist wichtig zu betonen, dass bei der Durchsetzung der KI-VO ein verhältnismäßiger Ansatz verfolgt wird. Jede Sanktion muss verhältnismäßig sein, auf dem Einzelfall beruhen und Faktoren wie Art und Schwere sowie den vorsätzlichen und fahrlässigen Charakter des Verstoßes berücksichtigen. Dies könnte jedoch wahrscheinlicher sein, wenn es einen Beweis für einen Vorfall gibt, der auf das Fehlen einer angemessenen Schulung und Anleitung von Mitarbeitern oder anderen Personen zurückzuführen ist."

- **„Wie können KMU mit begrenzten Ressourcen sicherstellen, dass ihre Mitarbeiter die erforderliche KI-Kompetenz erwerben? Gibt es spezielle Schulungsinitiativen oder EU-Förderprogramme?“**

  „Ein Beispiel für eine EU-Initiative, die KMU unterstützen könnte, ist das Netzwerk der europäischen digitalen Innovationszentren (EDIH). EDIH sind 251 zentrale Anlaufstellen in ganz Europa […], sie unterstützen KMU und Organisationen des öffentlichen Sektors bei der Digitalisierung ihrer Prozesse. […] KMU und Organisationen des öffentlichen Sektors können sich an EDIH wenden, um Unterstützung bei KI-Technologien und ihren Digitalisierungszielen im weiteren Sinne zu erhalten.“

- **„Ist ein KI-Beauftragter genauso notwendig wie für die DSGVO? Können ein Datenschutzbeauftragter (DSB) und ein AI Officer dieselbe Person sein? Soll eine Organisation ein KI-Governance-Board einrichten?“**

  „Nein, es gibt keine spezifische Governance-Struktur, die zur Einhaltung von Art. 4 KI-VO verpflichtet ist.“

Auch die in Deutschland zuständige Marktüberwachungsbehörde, die Bundesnetzagentur (BNetzA), hat inzwischen das Hinweispapier „KI-Kompetenzen nach Artikel 4 KI-Verordnung“ veröffentlicht. Darin finden sich die folgenden Punkte:

1. **Individuellen Bedarf ermitteln**
   - Welche Personen entwickeln, betreiben oder nutzen KI-Systeme?
   - Welche KI-Systeme sind das?
   - Zu welchem Zweck arbeiten diese Personen mit diesen KI-Systemen?
   - Welche Risiken sind mit der Arbeit mit diesen KI-Systemen verbunden?
2. **Maßnahmen ausgestalten und hierbei beachten, unter anderem**
   - individuelle Faktoren der betroffenen Personen wie Ausbildung, Erfahrung, Wissensstand,
   - Art der Tätigkeit,
   - den Kontext, in dem das jeweilige KI-System eingesetzt wird, z. B. Anwendungsbereich, Nutzungsphase, betroffene Personen, Zweck,
   - das damit verbundene Risiko sowie
   - die Rolle der eigenen Organisation hinsichtlich der KI-Wertschöpfungskette.

3. **Regelmäßige Auffrischung**
4. **Ausreichende Dokumentation der durchgeführten Maßnahmen, unter anderem**
   - die Art der Maßnahmen,
   - den inhaltlichen und zeitlichen Umfang,
   - die teilnehmenden Personen.

Auch wenn gerade keine Pflicht zur Benennung eines „KI-Beauftragten" – parallel zum DSB nach Vorgabe der Datenschutzgrundverordnung – besteht, wäre es in jedem Fall aber wünschenswert, wenn zumindest eine Person existierte, die mit dem notwendigen Wissen ausgestattet ist und als Organisator sowie als Bindeglied fungieren kann („KI-Beauftragter", „KI-Manager", „AI Officer" oder Ähnliche). Gleichwohl wäre eine solche Funktion ideal oder vielleicht sogar ein ganzes „KI-Team", das interdisziplinär besetzt ist und das Thema „KI" federführend übernimmt.

KI-MANAGEMENT-SYSTEM

Ein KI-Management-System (KIMS), auch als KI-Compliance-Management-System bezeichnet, ist ein organisatorisches System (analog zu Qualitäts-, Datenschutz- oder Informationssicherheits-Management-Systemen), das die sichere Entwicklung und Verwendung von KI gewährleistet. Es kann Richtlinien, Prozesse und Verantwortlichkeiten definieren, z. B. wer KI-Projekte genehmigt, wie Risiken bewertet werden, wie Feedback-Schleifen aufgebaut sind usw. Die KI-Verordnung verlangt von Anbietern von Hochrisiko-KI-Systemen den Betrieb eines Risikomanagementsystems (Art. 9 KI-VO) – und ein KIMS wäre eine Möglichkeit für dessen praktische Umsetzung. Für große Unternehmen ist ein formalisiertes System empfehlenswert, um Compliance nachweisen zu können. Hierfür bieten sich insbesondere die ISO 42001 oder andere Frameworks an.

KI-MODELL

Ein KI-Modell ist ein algorithmisches Modell (z. B. künstliches neuronales Netzwerk), das anhand von Daten trainiert wurde. Mathematisch enthält es die Parameter, die aus dem Lernprozess („Training") resultieren. Beispiele sind Bildklassifi-

katoren, Sprachmodelle oder Entscheidungsbäume. Das Modell erzeugt basierend auf neuen Eingaben Ausgaben (Vorhersagen, Klassifizierungen, generierte Inhalte). Beispiel für ein KI-Modell ist „GPT“ (Abkürzung für engl.: generative pre-trained transformer), das als „Motor“ z. B. im KI-System ChatGPT verankert ist.

Hinweis:
In der KI-Verordnung wird zwischen „normalen“ KI-Modellen und „KI-Modellen mit allgemeinem Verwendungszweck“ sowie „KI-Modellen mit allgemeinem Verwendungszweck mit systemischem Risiko“ unterschieden. Für den erstgenannten Begriff, also für „KI-Modell“, enthält das Gesetz keine eigene Definition.

KI-MODELL MIT ALLGEMEINEM VERWENDUNGSZWECK

Unter diesem Begriff werden Allzweck-KI-Modelle (z. B. große Sprachmodelle, engl.: large language models, LLM) verstanden, die nicht für eine einzelne Aufgabe, sondern für vielfältige Zwecke einsetzbar sind. Sie können durch Feintuning oder spezifische Prompts für viele Anwendungen genutzt werden. Mit ihnen lassen sich folglich auch ganz unterschiedliche Ergebnisse erzielen, von Text- über Musik-, Video- und Foto-Ausgaben bis hin zu speziellen Formaten, wie etwa PowerPoint-Folien.

Da sie sich grundlegend von KI-Modellen mit einem konkreten Verwendungszweck unterscheiden (z. B. KI-Modelle zur Erkennung von Krebszellen), regelt die KI-Verordnung (KI-VO) sie gesondert. Hier wird zudem unterschieden in KI-Modelle mit allgemeinem Verwendungszweck mit systemischem und ohne systemisches Risiko. Unabhängig von den in der KI-VO geregelten vier Risikoklassen (unannehmbar, hoch, begrenzt, minimal) existieren spezielle Vorgaben für KI mit allgemeinem Verwendungszweck (engl.: general purpose AI, kurz: GPAI). Unterschieden wird hierbei zwischen KI-Modell und KI-System.

Eine generelle Definition des Begriffs „KI-Modell“ enthält die KI-VO zwar nicht. Aber der Begriff „KI-Modell mit allgemeinem Verwendungszweck“ wird in Art. 3 Nr. 63 KI-VO wie folgt definiert:

„ein KI-Modell – einschließlich der Fälle, in denen ein solches KI-Modell mit einer großen Datenmenge unter umfassender Selbstüberwachung trainiert wird –, 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, und das in eine Vielzahl nachgelagerter Systeme oder Anwendungen integriert werden kann, ausgenommen KI-Modelle, die vor ihrem Inverkehrbringen für Forschungs- und Entwicklungstätigkeiten oder die Konzipierung von Prototypen eingesetzt werden"

Als GPAI-Modell dürften daher wohl die LLM, also GPT von OpenAI, Llama von Meta, Googles Gemini oder auch Claude von Anthropic, einzustufen sein.

Anbieter von KI-Modellen mit allgemeinem Verwendungszweck haben folgende Pflichten zu erfüllen:

- Erstellen und Aktualisieren der technischen Dokumentation des KI-Modells, um sie dem AI Office und der nationalen Aufsichtsbehörde zur Verfügung zu stellen (Art. 53 Abs. 1 lit. a), Anhang XI KI-VO)
- Erstellen und Aktualisieren von Informationen und der Dokumentation, um sie für Anbieter von KI-Systemen zur Verfügung zu stellen (Art. 53 Abs. 1 lit. b), Anhang XII KI-VO)
- Strategie zur Einhaltung des Urheberrechts (Art. 53 Abs. 1 lit. c) KI-VO
- Erstellen und Veröffentlichen einer hinreichend detaillierten Zusammenfassung der für das KI-Training verwendeten Inhalte nach einer vom AI Office bereitgestellten Vorlage (Art. 53 Abs. 1 lit. d) KI-VO
- ggf. Zusammenarbeit mit der EU-Kommission und nationalen Aufsichtsbehörde (Art. 53 Abs. 3 KI-VO)
- ggf. Benennung eines EU-Bevollmächtigten (Art. 54 Abs. 1 KI-VO)

Anbieter von KI-Modellen mit allgemeinem Verwendungszweck, die ein systemisches Risiko aufweisen, haben zusätzlich zu den in Art. 53, 54 KI-VO genannten Pflichten auch noch folgende Vorgaben zu erfüllen:

- Durchführung einer KI-Modell-Bewertung mit standardisierten Protokollen und Instrumenten, die dem Stand der Technik entsprechen (Art. 55 Abs. 1 lit. a) KI-VO)
- Bewerten und Mindern von möglichen systemischen Risiken auf Unionsebene – einschließlich ihrer Ursachen –, die sich aus der Entwicklung, dem Inverkehrbringen oder der Verwendung von solchen KI-Modellen ergeben können (Art. 55 Abs. 1 lit. b) KI-VO)

- Erfassen und Dokumentieren von einschlägigen Informationen über schwerwiegende Vorfälle und mögliche Abhilfemaßnahmen sowie ggf. Meldung an das AI Office bzw. die nationale Aufsichtsbehörde (Art. 55 Abs. 1 lit. c) KI-VO)
- Gewährleisten eines angemessenen Maßes an Cybersicherheit sowie an Sicherheit der physischen Infrastruktur des KI-Modells (Art. 55 Abs. 1 lit. d) KI-VO)

Ein KI-Modell mit allgemeinem Verwendungszweck wird als ein solches mit systemischem Risiko eingestuft, wenn eine der folgenden Bedingungen erfüllt ist (vgl. Art. 51 Abs. 1 KI-VO):

a) Es verfügt über Fähigkeiten mit hohem Wirkungsgrad, die mithilfe geeigneter technischer Instrumente und Methoden, einschließlich Indikatoren und Benchmarks, bewertet werden;

b) unter Berücksichtigung der in Anhang XIII festgelegten Kriterien von der Kommission von Amts wegen oder aufgrund einer qualifizierten Warnung des wissenschaftlichen Gremiums getroffenen Entscheidung zufolge verfügt es über Fähigkeiten oder eine Wirkung, die denen gemäß Buchstabe a entsprechen.

Hinweis:
Bei einem KI-Modell mit allgemeinem Verwendungszweck wird angenommen, dass es über Fähigkeiten mit hohem Wirkungsgrad gemäß Art. 51 Abs. 1 lit. a) KI-VO verfügt, wenn die kumulierte Menge der für sein Training verwendeten Berechnungen, gemessen in Gleitkommaoperationen, mehr als 10^{25} beträgt (Art. 51 Abs. 2 KI-VO).

In Art. 3 Nr. 65 KI-VO wird „systemisches Risiko" wie folgt definiert:

„Risiko, das für die Fähigkeiten mit hoher Wirkkraft von KI-Modellen mit allgemeinem Verwendungszweck spezifisch ist und aufgrund deren Reichweite oder aufgrund tatsächlicher oder vernünftigerweise vorhersehbarer negativer Folgen für die öffentliche Gesundheit, die Sicherheit, die öffentliche Sicherheit, die Grundrechte oder die Gesellschaft insgesamt erhebliche Auswirkungen auf den Unionsmarkt hat, die sich in großem Umfang über die gesamte Wertschöpfungskette hinweg verbreiten können"

In Anhang XIII KI-VO werden die Kriterien für KI-Modelle mit allgemeinem Verwendungszweck mit systemischem Risiko gemäß Art. 51 KI-VO angeführt:

- Anzahl der Parameter des Modells
- Qualität oder Größe des Datensatzes, z. B. durch Tokens gemessen

- 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
- Ein- und Ausgabemodalitäten des Modells, wie Text-Text (LLM), Text-Bild, Multimodalität, Schwellenwerte auf dem Stand der Technik für die Bestimmung der Fähigkeiten mit hoher Wirkkraft für jede Modalität und die spezifische Art der Ein- und Ausgaben (z. B. biologische Sequenzen)
- Benchmarks und Beurteilungen der Fähigkeiten des Modells, unter Berücksichtigung der Zahl der Aufgaben ohne zusätzliches Training, der Anpassungsfähigkeit zum Erlernen neuer, unterschiedlicher Aufgaben, des Grads an Autonomie und Skalierbarkeit sowie der Instrumente, zu denen es Zugang hat
- ob es aufgrund seiner Reichweite große Auswirkungen auf den Binnenmarkt hat – davon wird ausgegangen, wenn es mindestens 10.000 in der Union niedergelassenen registrierten gewerblichen Nutzern zur Verfügung gestellt wurde
- Zahl der registrierten Endnutzer

Die EU-Kommission stellt seit März 2025 eine FAQ-Sektion für KI-Modelle mit allgemeinem Verwendungszweck online bereit. Diese FAQ enthalten exemplarisch die Antworten auch auf folgende Fragen (eigene Übersetzung aus dem Englischen):

- **„Was sind Allzweck-KI-Modelle?“**

  „Die KI-VO definiert ein universelles KI-Modell [oder auch „Allzweck-KI-Modelle“] als „ein KI-Modell, auch wenn ein solches KI-Modell mit einer großen Datenmenge unter Verwendung von Selbstüberwachung in großem Maßstab trainiert wird, das eine erhebliche Allgemeingültigkeit aufweist und in der Lage ist, unabhängig von der Art und Weise, wie das Modell in Verkehr gebracht wird, ein breites Spektrum unterschiedlicher Aufgaben kompetent auszuführen, und das in eine Vielzahl nachgelagerter Systeme oder Anwendungen integriert werden kann“ (Art. 3 Nr. 63 KI-VO). In den Erwägungsgründen der KI-VO wird weiter präzisiert, welche Modelle als signifikant allgemein gelten und in der Lage sein sollten, ein breites Spektrum unterschiedlicher Aufgaben zu erfüllen. In Erwägungsgrund 98 der KI-VO heißt es: ‚Während die Allgemeingültigkeit eines Modells unter anderem auch durch eine Reihe von Parametern bestimmt werden könnte, sollten Modelle mit mindestens einer Milliarde Parametern, die mit einer großen

Datenmenge unter Verwendung der Selbstüberwachung in großem Maßstab trainiert werden, als signifikant allgemein angesehen werden und ein breites Spektrum unterschiedlicher Aufgaben kompetent erfüllen.' In Erwägungsgrund 99 wird hinzugefügt, dass ‚große generative KI-Modelle ein typisches Beispiel für ein universelles KI-Modell sind, da sie eine flexible Generierung von Inhalten wie Text, Audio, Bild oder Video ermöglichen, die problemlos eine Vielzahl unterschiedlicher Aufgaben erfüllen können. Beachten Sie, dass eine signifikante Allgemeingültigkeit und die Fähigkeit, eine Vielzahl von unterschiedlichen Aufgaben kompetent auszuführen, durch Modelle innerhalb einer einzigen Modalität wie Text, Audio, Bilder oder Video erreicht werden können, wenn die Modalität flexibel genug ist. Dies kann auch durch Modelle erreicht werden, die entwickelt, verfeinert oder anderweitig modifiziert wurden, um bei einer bestimmten Aufgabe oder bei einer Reihe von Aufgaben in einem bestimmten Bereich besonders gut zu sein. Unterschiedliche Phasen der Entwicklung eines Modells stellen keine unterschiedlichen Modelle dar."

➤ **„Warum brauchen wir Regeln für universelle KI-Modelle?"**

„Künstliche Intelligenz (KI) verspricht enorme Vorteile für unsere Wirtschaft und Gesellschaft. Allzweck-KI-Modelle spielen dabei eine wichtige Rolle, da sie für eine Vielzahl von Aufgaben eingesetzt werden können und somit die Grundlage für eine Reihe von nachgelagerten KI-Systemen bilden, die in Europa und weltweit eingesetzt werden. Die KI-VO soll sicherstellen, dass universelle KI-Modelle sicher und vertrauenswürdig sind. Um dieses Ziel zu erreichen, ist es von entscheidender Bedeutung, dass Anbieter von KI-Allzweckmodellen ein gutes Verständnis ihrer Modelle entlang der gesamten KI-Wertschöpfungskette sicherstellen, damit nachgeschaltete Anbieter diese Modelle sowohl in KI-Systeme integrieren als auch ihren eigenen Verpflichtungen aus der KI-VO nachkommen können. Genauer gesagt und wie nachstehend näher erläutert, müssen Anbieter von KI-Modellen für allgemeine Zwecke technische Dokumentationen ihrer Modelle erstellen, um sie nachgelagerten Anbietern zur Verfügung zu stellen und dem Amt für künstliche Intelligenz und den zuständigen nationalen Behörden auf Anfrage zur Verfügung zu stellen, eine Urheberrechtspolitik einzuführen und eine Zusammenfassung der Schulungsinhalte zu veröffentlichen. Darüber hinaus müssen Anbieter von universellen KI-Modellen, die Systemrisiken bergen, was entweder der Fall sein kann, weil die Modelle sehr leistungsfähig sind oder weil sie aus anderen Gründen erhebliche Auswirkungen auf den Binnenmarkt haben, diese Modelle der EU-Kommission melden, die sich aus diesen Modellen ergebenden Systemrisiken bewerten und mindern, unter anderem durch die

Durchführung von Modellbewertungen, die Meldung schwerwiegender Vorfälle und die Gewährleistung einer angemessenen Cybersicherheit dieser Modelle."

➤ **„Wer gilt als Anbieter eines universellen KI-Modells?"**

„Die Vorschriften der KI-VO über KI-Modelle für allgemeine Zwecke gelten für Anbieter, die solche Modelle in der Union in Verkehr bringen, unabhängig davon, ob diese Anbieter in der Union oder in einem Drittland niedergelassen oder ansässig sind (Art. 2 Abs. 1 lit. a) KI-VO). Ein Anbieter eines KI-Modells für allgemeine Zwecke ist eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die ein KI-Modell für allgemeine Zwecke entwickelt oder ein solches Modell entwickelt hat und es entgeltlich oder unentgeltlich in Verkehr bringt (Art. 3 Nr. 3 KI-VO). Das Inverkehrbringen eines Modells bedeutet die erstmalige Bereitstellung des Modells auf dem Unionsmarkt (Art. 3 Nr. 9 KI-VO), das heißt die erstmalige Bereitstellung zum Vertrieb oder zur Verwendung auf dem Unionsmarkt im Rahmen einer gewerblichen Tätigkeit, sei es entgeltlich oder unentgeltlich (Art. 3 Nr. 10 KI-VO). Beachten Sie, dass ein KI-Modell für allgemeine Zwecke auch dann als in Verkehr gebracht gilt, wenn der Anbieter dieses Modells das Modell in sein eigenes KI-System integriert, das auf dem Markt bereitgestellt oder in Betrieb genommen wird, es sei denn,

a) das Modell wird für rein interne Prozesse verwendet, die für die Bereitstellung eines Produkts oder einer Dienstleistung für Dritte nicht wesentlich sind,

b) die Rechte natürlicher Personen werden nicht beeinträchtigt und

c) das Modell ist kein KI-Modell für allgemeine Zwecke mit Systemrisiko (Erwägungsgrund 97 KI-VO)."

➤ **„Welche Pflichten haben Anbieter von KI-Modellen für allgemeine Zwecke?"**

„Anbieter von KI-Modellen für allgemeine Zwecke müssen technische Informationen über ihre Modelle dokumentieren, um diese Informationen dem Amt für künstliche Intelligenz und den zuständigen nationalen Behörden auf Anfrage zur Verfügung zu stellen (Art. 53 Abs. 1 lit. a) KI-VO) und nachgeschalteten Anbietern zur Verfügung zu stellen (Art. 53 Abs. 1 lit. b) KI-VO). Sie müssen auch eine Strategie zur Einhaltung des Unionsrechts im Bereich des Urheberrechts und der verwandten Schutzrechte (Art. 53 Abs. 1 lit. c) KI-VO) einführen und eine ausreichend detaillierte Zusammenfassung der für die Schulung des Modells verwendeten Inhalte erstellen und öffentlich zugänglich machen (Art. 53 Abs. 1 lit. d) KI-VO). […] Anbieter von Allzweck-KI-Modellen mit systemischem Risiko haben nach der KI-VO zusätzliche Pflichten. Sie müssen systemische Risiken bewerten und min-

dern, insbesondere indem sie Modellbewertungen durchführen, schwerwiegende Vorfälle verfolgen, dokumentieren und melden und einen angemessenen Cybersicherheitsschutz für das Modell und seine physische Infrastruktur gewährleisten (Art. 55 KI-VO). […] Die Verpflichtungen für Anbieter von KI-Modellen für allgemeine Zwecke gelten ab dem 02.08.2025 (Art. 113 lit. b) KI-VO), wobei besondere Vorschriften für KI-Modelle für allgemeine Zwecke gelten, die vor diesem Datum in Verkehr gebracht wurden (Art. 111 Abs. 3 KI-VO).“

- **„Was ist, wenn jemand ein Modell open source betreibt, muss er dann auch die Verpflichtungen für Anbieter von universellen KI-Modellen einhalten?“**

  „Die Verpflichtung zur Erstellung und Übermittlung von Unterlagen an das KI-Büro, die zuständigen nationalen Behörden und nachgeschaltete Anbieter (Art. 53 Abs. 1 lit. a), b) KI-VO) gilt nicht, wenn das Modell unter einer freien und quelloffenen Lizenz veröffentlicht wird und seine Parameter, einschließlich der Gewichtungen, der Informationen über die Modellarchitektur und der Informationen über die Modellnutzung, öffentlich zugänglich gemacht werden (Art. 53 Abs. 2 KI-VO). In den Erwägungsgründen 102 und 103 der KI-VO wird weiter präzisiert, was eine freie und quelloffene Lizenz darstellt, und das KI-Büro beabsichtigt, weitere Klarstellungen zu Fragen zu Open-Sourcing-Allzweck-KI-Modellen vorzulegen. Die Ausnahme gilt nicht für universelle KI-Modelle mit systemischem Risiko. Nach der quelloffenen Modellfreigabe können die Maßnahmen, die erforderlich sind, um die Einhaltung der Verpflichtungen nach Art. 55 KI-VO zu gewährleisten, schwieriger umzusetzen sein (Erwägungsgrund 112 KI-VO). Folglich müssen Anbieter von universellen KI-Modellen mit systemischem Risiko möglicherweise systemische Risiken bewerten und mindern, bevor sie ihre Modelle als Open Source veröffentlichen.“

- **„Wenn jemand ein Modell verfeinert oder auf andere Weise modifiziert, muss er dann auch die Verpflichtungen für Anbieter von universellen KI-Modellen einhalten?“**

  „Allzweck-KI-Modelle können weiter modifiziert oder auf neue Modelle abgestimmt werden (Erwägungsgrund 97 KI-VO). Dementsprechend können nachgelagerte Unternehmen, die ein bestehendes KI-Modell für allgemeine Zwecke verfeinern oder anderweitig ändern, Anbieter neuer Modelle werden. Die besonderen Umstände, unter denen ein nachgelagertes Unternehmen Anbieter eines neuen Modells wird, sind eine schwierige Frage mit potenziell großen wirtschaftlichen Auswirkungen, da viele Organisationen und Einzelpersonen KI-Modelle für all-

gemeine Zwecke, die von einem anderen Unternehmen entwickelt wurden, verfeinern oder anderweitig ändern. Im Falle einer Änderung oder Feinabstimmung eines bestehenden KI-Modells für allgemeine Zwecke sollten sich die Verpflichtungen der Anbieter von KI-Modellen für allgemeine Zwecke gemäß Art. 53 KI-VO auf die Änderung oder Feinabstimmung beschränken, indem beispielsweise die bereits vorhandene technische Dokumentation durch Informationen über die Änderungen ergänzt wird (Erwägungsgrund 109 KI-VO). Die Verpflichtungen für Anbieter von KI-Allzweckmodellen mit Systemrisiko gemäß Art. 55 KI-VO sollten nur in klar festgelegten Fällen gelten. Das Amt für künstliche Intelligenz beabsichtigt, zu dieser Frage weitere Erläuterungen zu geben. Unabhängig davon, ob eine nachgeschaltete Einrichtung, die ein Allzweck-KI-Modell in ein KI-System integriert, als Anbieter des Allzweck-KI-Modells gilt, muss diese Einrichtung die einschlägigen Anforderungen und Verpflichtungen des KI-Gesetzes für KI-Systeme erfüllen."

- **„Welche Durchsetzungsbefugnisse hat das Amt für künstliche Intelligenz?"**

  „Das KI-Büro wird die in der KI-VO festgelegten Verpflichtungen für Anbieter von KI-Modellen für allgemeine Zwecke (Art. 88 KI-VO) und ausnahmsweise die Verpflichtungen für Anbieter von KI-Systemen, die auf KI-Modellen für allgemeine Zwecke basieren, überwachen und durchsetzen, wenn der Anbieter des Modells und des Systems derselbe sind (Art. 75 Abs. 1 KI-VO). Das Amt für künstliche Intelligenz wird unter anderem die zuständigen Marktüberwachungsbehörden der Mitgliedstaaten bei der Durchsetzung der Anforderungen an KI-Systeme (Art. 75 Abs. 2, 3 KI-VO) unterstützen. Die Durchsetzung durch das Amt für künstliche Intelligenz wird durch die ihm durch die KI-VO übertragenen Befugnisse untermauert, nämlich die Befugnis, Informationen anzufordern (Art. 91 KI-VO), Bewertungen von KI-Modellen für allgemeine Zwecke durchzuführen (Art. 92 KI-VO), Maßnahmen von Anbietern anzufordern, einschließlich der Umsetzung von Risikominderungsmaßnahmen, und das Modell vom Markt zurückzurufen (Art. 93 KI-VO) und Geldbußen von bis zu 3 % des weltweiten Jahresumsatzes oder 15 Millionen Euro zu verhängen, je nachdem, welcher Betrag höher ist (Art. 101 KI-VO)."

Der Verhaltenskodex für KI mit allgemeinem Verwendungszweck (GPAI) ist ein freiwilliges Instrument, das von unabhängigen Experten ausgearbeitet wurde und Unternehmen dabei helfen soll, die entsprechenden Verpflichtungen der KI-VO zu erfüllen. Dieser Kodex wurde am 10.07.2025 veröffentlicht. Es gibt jedoch noch keine finale Fassung, da unter anderem noch ergänzende Leitlinien der EU-Kommission zu Schlüsselkonzepten im Zusammenhang mit KI-Modellen mit allgemeinem Verwendungszweck fehlen.

Der Kodex besteht aus drei separat verfassten Kapiteln zu unterschiedlichen Themen:

1. Transparenz

2. Urheberrecht

3. Sicherheit

Die Kapitel über Transparenz und Urheberrecht bieten allen Anbietern von KI-Modellen mit allgemeinem Verwendungszweck eine Möglichkeit, die Einhaltung ihrer Verpflichtungen gemäß Art. 53 KI-VO nachzuweisen. Das Kapitel über Sicherheit und Gefahrenabwehr ist nur für die geringe Zahl von Anbietern der fortschrittlichsten Modelle relevant, die den Verpflichtungen der KI-VO für Anbieter von KI-Modellen mit allgemeinem Verwendungszweck mit Systemrisiko gemäß Art. 55 KI-VO unterliegen.

Hinweis:
Das Kapitel „Transparenz" bietet zudem ein benutzerfreundliches Muster für ein Dokumentationsformular, das es Anbietern ermöglicht, die erforderlichen Informationen leicht zu dokumentieren, um eine ausreichende Transparenz gewährleisten zu können.

Unterzeichner des Kodex sind (Stand: April 2026):

- Accexible
- AI Alignment Solutions
- AI Studio Delta
- Aleph Alpha
- Almawave
- Amazon
- Anthropic
- Black Forest Labs
- Bria AI
- Cohere
- Domyn
- Dweve
- Euc Inovação Portugal
- Fastweb
- Google
- Humane Technology
- IBM
- Lawise
- LINAGORA
- Microsoft
- Mistral AI
- Open Hippo
- OpenAI
- Pleias
- re-inventa
- ServiceNow
- WRITER

Hinweis:
Diese Liste wird vonseiten der EU fortlaufend aktualisiert.

Außerdem hat sich xAI dem Kapitel „Sicherheit" angeschlossen; dies bedeutet, dass das Unternehmen die Einhaltung der in der KI-VO festgelegten Verpflichtungen in Bezug auf Transparenz und Urheberrecht durch alternative angemessene Mittel nachweisen muss.

KI-OUTPUT

Der KI-Output ist das Ergebnis eines KI-Systems, also etwa eine Klassifizierung, ein generiertes Bild oder Text, eine Empfehlung oder Entscheidung. Die rechtliche Verantwortung für die Nutzung von KI-Output liegt grundsätzlich bei den Nutzern des KI-Systems, diese müssen daher sicherstellen, dass der KI-Output inhaltlich korrekt ist und keine Rechtsverstöße enthält.

KI-REALLABOR

Ein KI-Reallabor (sogenannte Regulatory Sandbox) ist eine von Behörden geschaffene Umgebung, in der innovative KI-Systeme unter realen Bedingungen, aber kontrolliert getestet werden dürfen. Anbieter können dort für eine begrenzte Zeit neue KI-Produkte entwickeln, trainieren und validieren, unter Aufsicht der zuständigen Behörde. Ziel ist es, Innovation zu fördern und Risiken zugleich niedrig zu halten. Die KI-Verordnung (KI-VO) regelt in ihren Artikeln 57 bis 63 die Rahmenbedingungen für solche KI-Reallabore. Ein Beispiel wäre ein behördliches Programm, in dem eine Firma eine KI-gestützte Gesundheits-App unter Aufsicht mit echten Patientendaten testet, bevor sie regulär zugelassen wird.

Der Begriff „KI-Reallabor" beschreibt gemäß Art. 3 Nr. 55 KI-VO

„einen kontrollierten Rahmen, der von einer zuständigen Behörde geschaffen wird und den Anbieter oder zukünftige Anbieter von KI-Systemen nach einem Plan für das Reallabor einen begrenzten Zeitraum und unter regulatorischer Aufsicht nutzen können, um ein innovatives KI-System zu entwickeln, zu trainieren, zu validieren und – gegebenenfalls unter Realbedingungen – zu testen"

Der „Plan für das Reallabor" ist hingegen gemäß Art. 3 Nr. 54 KI-VO „ein zwischen dem teilnehmenden Anbieter und der zuständigen Behörde vereinbartes Dokument, in dem die Ziele, die Bedingungen, der Zeitrahmen, die Methodik und die Anforderungen für die im Reallabor durchgeführten Tätigkeiten beschrieben werden". Und der „Plan für einen Test unter Realbedingungen" wird in Art. 3 Nr. 53 KI-VO als Dokument definiert, in dem die Ziele, die Methodik, der geografische, bevölkerungsbezogene und zeitliche Umfang, die Überwachung, die Organisation und die Durchführung eines Tests unter Realbedingungen dargestellt werden.

Anhang IX der KI-VO enthält Vorgaben für bestimmte Pflichtinformationen, die bei Tests unter Realbedingungen gemäß Art. 60 KI-VO bei der Registrierung von in Anhang III KI-VO aufgeführten Hochrisiko-KI-Systemen bereitzustellen sind:

- eine unionsweit einmalige Identifizierungsnummer des Tests unter Realbedingungen
- der Name und die Kontaktdaten des Anbieters oder zukünftigen Anbieters und der Betreiber, die an dem Test unter Realbedingungen teilgenommen haben
- eine kurze Beschreibung des KI-Systems, seine Zweckbestimmung und sonstige zu seiner Identifizierung erforderliche Informationen
- eine Übersicht über die Hauptmerkmale des Plans für den Test unter Realbedingungen
- Informationen über die Aussetzung oder den Abbruch des Tests unter Realbedingungen

KI-RECHT

Der Sammelbegriff „KI-Recht" bezeichnet das entstehende Rechtsgebiet rund um die Entwicklung, den Vertrieb und speziell die Nutzung von KI. Er umfasst insbesondere die KI-Verordnung der EU sowie weitere internationale Gesetzgebung und Regulatorik, aber auch die Datenschutzgrundverordnung (soweit die KI personenbezogene Daten verarbeitet), IT-Sicherheitsgesetze, Verbraucherschutzregelungen (Produkthaftung bei KI-Fehlfunktionen), Urheberrecht, Markenrecht und noch viele andere Dinge mehr. Insgesamt ist dieses noch sehr junge Rechtsgebiet in höchstem Maße dynamisch und komplex, was nicht zuletzt auf die rasante technische Entwicklung zurückzuführen ist.

KI-RICHTLINIE

Eine (interne) KI-Richtlinie (engl. auch: AI Policy) ist eine unternehmens- oder behördeninterne Regelung, die den Rahmen für den Einsatz von KI-Systemen durch Beschäftigte definiert und organisatorische, technische sowie rechtliche Rahmenbedingungen festlegt. Sie regelt insbesondere die Fragen, welche KI-Tools genutzt

werden können, welche Daten verarbeitet werden dürfen, welche Voraussetzungen zu erfüllen sind, welche Prüfschritte durchgeführt werden müssen und welche Dokumentations- und Transparenzpflichten gelten. Gleichzeitig dient die KI-Richtlinie als zentrales Instrument, um Datenschutzgrundverordnung, KI-Verordnung (KI-VO) und weitere Vorgaben in die Praxis des Arbeitsalltags zu übersetzen und klare Verantwortlichkeiten, Schulungsanforderungen und Eskalationswege festzulegen.

Hinweis:
Bei Bestehen eines Betriebsrats ist dieser aufgrund der möglichen Leistungs- und Verhaltenskontrolle in aller Regel mitbestimmungspflichtig (§ 87 Abs. 1 Nr. 6 Betriebsverfassungsgesetz).

Angesichts der massiven rechtlichen und wirtschaftlichen Risiken ist eine interne KI-Richtlinie für jede Institution, die KI einsetzt oder entwickelt, unverzichtbar. Sie dient dazu, die abstrakten gesetzlichen Vorgaben in konkrete Dienstanweisungen zu übersetzen und das Risiko von „Schatten-KI" zu minimieren.

Hinweis:
„Schatten-KI" bezeichnet, analog zur „Schatten-IT", den Umstand, dass Beschäftigte in einem Unternehmen oder einer Behörde ohne Wissen oder gar entgegen der Anweisung des Arbeitgebers eigene, ggf. auch private KI-Tools zu beruflichen Zwecken nutzen. Dadurch hat der Arbeitgeber keine Kontrolle darüber, er erfährt womöglich sogar nichts davon und muss unter Umständen gleichwohl die rechtliche Verantwortung für seine Beschäftigten übernehmen.

Eine professionelle KI-Richtlinie sollte als lebendes Dokument gestaltet sein und folgende Bereiche abdecken:

- Zweckgebundene Nutzung: Definition klarer Anwendungsfälle, für die KI-Tools genehmigt sind (z. B. Marketing, Kundensupport), und solcher, die untersagt sind
- Vorgaben zu Datenschutz- und Geheimnisschutz: explizite Anweisungen, welche Datenarten (z. B. personenbezogene Daten, Quellcodes, Finanzdaten, Log-in-Daten) niemals in öffentliche KI-Modelle, wie etwa ChatGPT, eingegeben werden dürfen
- Qualitätssicherungspflichten: die Verpflichtung für Beschäftigte, KI-Outputs auf „Halluzinationen", sachliche Richtigkeit sowie Urheber- und andere Rechtsverletzungen zu prüfen, bevor diese nach außen kommuniziert werden

- Ethische Leitlinien: Verankerung des „Human in the Loop"-Prinzips, um sicherzustellen, dass keine kritischen Entscheidungen ohne menschliche Aufsicht getroffen werden
- KI-Kompetenz (Art. 4 KI-VO): Bereitstellung von Angeboten zwecks Schulung und Sensibilisierung der Beschäftigten

Hinweis:
Die KI-Richtlinie sollte eng mit Schulungsprogrammen verknüpft sein, die technisches Verständnis, Risikobewusstsein und ethische Reflexion vermitteln.

In Deutschland gibt es inzwischen erste Vorlagen. So hat etwa die Gesellschaft für Datenschutz und Datensicherheit (GDD e. V.) im Mai 2025 die **„GDD-Musterrichtlinie – Betriebliche Richtlinie zum Einsatz Künstlicher Intelligenz"** veröffentlicht. An deren inhaltlichem Aufbau kann man sich gut orientieren:

1. Ziel der Richtlinie
2. Geltungsbereich
3. Anwendungsbereich
4. Grundsätze für die Nutzung von KI
4.1 Freigabe
4.2 Geprüfte und freigegebene KI-Anwendungen
4.3 Verbot der Nutzung privater KI-Anwendungen
4.4 Zweckgebundene Nutzung
4.5 Verantwortung und Überprüfung der Ergebnisse
4.5.1 Entscheidungsfindung
4.5.2 Ethische Grundsätze
4.6 Einhaltung von Urheberrechten
4.7 Kennzeichnung der von einer KI erstellten Inhalte
4.8 Schulungspflicht
5. Sicherheit und Datenschutz
5.1 Personenbezogene Daten und Geschäftsgeheimnisse
5.2 Training von KI-Anwendungen
5.3 Beachtung anderer Richtlinien

6. Dokumentation und Nachvollziehbarkeit
7. Haftung und Sanktionen
8. Überwachung und sicherer Einsatz
9. Regelmäßige Überprüfung der Richtlinie
10. Inkrafttreten

Natürlich wird die Gliederung für konkrete Anwendungsfälle individuell anzupassen sein, ein guter Leitfaden ist sie aber allemal.

KI-SYSTEM

Ein KI-System wird in der KI-Verordnung folgendermaßen definiert (Art. 3 Nr. 1 KI-VO):

„ein maschinengestütztes System, das für einen in unterschiedlichem Grade autonomen Betrieb ausgelegt ist und das nach seiner Betriebsaufnahme anpassungsfähig sein kann und das aus den erhaltenen Eingaben für explizite oder implizite Ziele ableitet, wie Ausgaben wie etwa Vorhersagen, Inhalte, Empfehlungen oder Entscheidungen erstellt werden, die physische oder virtuelle Umgebungen beeinflussen können“

Ergänzend führt ErwGr 12 S. 2, 3, 5, 6, 11, 12 KI-VO aus:

„Darüber hinaus sollte die Begriffsbestimmung auf den wesentlichen Merkmalen der KI beruhen, die sie von einfacheren herkömmlichen Softwaresystemen und Programmierungsansätzen abgrenzen, und sollte sich nicht auf Systeme beziehen, die auf ausschließlich von natürlichen Personen definierten Regeln für das automatische Ausführen von Operationen beruhen. Ein wesentliches Merkmal von KI-Systemen ist ihre Fähigkeit, abzuleiten. […] Zu den Techniken, die während der Gestaltung eines KI-Systems das Ableiten ermöglichen, gehören Ansätze für maschinelles Lernen, wobei aus Daten gelernt wird, wie bestimmte Ziele erreicht werden können, sowie logik- und wissensgestützte Konzepte, wobei aus kodierten Informationen oder symbolischen Darstellungen der zu lösenden Aufgabe abgeleitet wird. Die Fähigkeit eines KI-Systems, abzuleiten, geht über die einfache Datenverarbeitung hinaus, indem Lern-, Schlussfolgerungs- und Modellierungsprozesse ermöglicht werden. […] KI-Systeme sind mit verschiedenen Graden der Autonomie ausgestattet, was bedeutet, dass sie bis zu einem gewissen Grad unabhängig von menschlichem Zutun agie-

ren und in der Lage sind, ohne menschliches Eingreifen zu arbeiten. Die Anpassungsfähigkeit, die ein KI-System nach Inbetriebnahme aufweisen könnte, bezieht sich auf seine Lernfähigkeit, durch sie es sich während seiner Verwendung verändern kann."

Die EU-Kommission sah sich dazu veranlasst, im Februar 2025 Leitlinien zur Definition des so zentralen Begriffs „System der künstlichen Intelligenz" zu veröffentlichen. Darin finden sich zu den einzelnen Elementen eines „KI-Systems" folgende ergänzende Hinweise:

- „Maschinengestütztes System": d. h., dass mit Maschinen (Hard- und Softwarekomponenten) entwickelt wird und auf ihnen lauffähig ist; nicht beschränkt auf bestimmte Computersysteme
- „Autonomie": d. h. ohne zwingende menschliche Beteiligung und ohne menschliches Eingreifen; angemessener Grad an Handlungsunabhängigkeit
- „Anpassungsfähigkeit": d. h. selbstlernende Fähigkeiten, durch die die KI sich während des Einsatzes ändern kann
- „Ziele": d. h. systeminterne Ziele, die sich auf die auszuführenden Aufgaben und deren Ergebnisse beziehen
- „Rückschlüsse auf die Erzeugung von Ergebnissen": d. h. Fähigkeit, Schlussfolgerungen zu ziehen
- „Beeinflussung der Umgebung durch Output": d. h. Erzeugen von Ausgaben durch Verarbeitung komplexer Muster und Beziehungen
- „Interaktion mit der Umwelt": d. h. aktive Einwirkung auf die physische oder virtuelle Welt

Ein Beispiel für ein KI-System ist ChatGPT des Anbieters OpenAI, das zusammen mit dem KI-Modell „GPT" als „Herzstück" und weiteren Komponenten (z. B. Filtern oder einer Nutzerschnittstelle) eine KI-Anwendung darstellt.

Hinweis:
Die Definition von „KI-System" entscheidet maßgeblich darüber, ob eine bestimmte Anwendung unter die KI-VO fällt und ob der Anbieter bzw. Betreiber die dementsprechenden Pflichten erfüllen muss. Gleichwohl ist sie in ihren Details umstritten. Es ist aber empfehlenswert, die Definition aus Art. 3 Nr. 1 KI-VO als sehr weitgehend anzusehen, sodass von dieser nahezu alle modernen KI-Tools umfasst werden; lediglich rein regelbasierte, deterministische Software soll ausgeschlossen sein.

KI-SYSTEM MIT ALLGEMEINEM VERWENDUNGSZWECK

Der Begriff „KI-System mit allgemeinem Verwendungszweck“ wird in Art. 3 Nr. 66 KI-Verordnung wie folgt definiert:

„KI-System, das auf einem KI-Modell mit allgemeinem Verwendungszweck beruht und in der Lage ist, einer Vielzahl von Zwecken sowohl für die direkte Verwendung als auch für die Integration in andere KI-Systeme zu dienen“

ChatGPT dürfte wohl das bekannteste KI-System mit einem solchen allgemeinen Verwendungszweck sein.

KI-TRAINING

Beim KI-Training wird ein KI-Modell mit Trainingsdaten gefüttert, um die lernbaren Parameter zu optimieren. Man spricht vom „Lernen“ oder „Anpassen“ des Modells. Das Training kann beaufsichtigt (mit gelabelten Daten) oder unüberwacht erfolgen. Ziel ist, dass das Modell Muster in den Daten erkennt (z. B. Bildmerkmale) und daraus Regeln ableitet. Es geht also beispielsweise um folgende Aufgaben:

- Welche Wörter treten häufig zusammen auf?
- Welche Merkmale besitzt ein bestimmtes Objekt auf Bildern?
- Welche Faktoren beeinflussen einen Kreditrisiko-Score?

Hinweis:
Hochrisiko-KI-Systeme, in denen Techniken eingesetzt werden, bei denen KI-Modelle mit Daten trainiert werden, müssen mit Trainings-, Validierungs- und Testdatensätzen entwickelt werden, die bestimmten Qualitätskriterien entsprechen (Art. 10 Abs. 1 KI-Verordnung (KI-VO)).

Für Trainings-, Validierungs- und Testdatensätze gelten Daten-Governance- und Datenverwaltungsverfahren, die für die Zweckbestimmung des Hochrisiko-KI-Systems geeignet sind (Art. 10 Abs. 2 KI-VO). Diese Verfahren betreffen insbesondere

- die einschlägigen konzeptionellen Entscheidungen,
- die Datenerhebungsverfahren und die Herkunft der Daten und im Fall personenbezogener Daten den ursprünglichen Zweck der Datenerhebung,

- relevante Datenaufbereitungsvorgänge wie Annotation, Kennzeichnung, Bereinigung, Aktualisierung, Anreicherung und Aggregierung,
- die Aufstellung von Annahmen, insbesondere in Bezug auf die Informationen, die mit den Daten erfasst und dargestellt werden sollen,
- eine Bewertung der Verfügbarkeit, Menge und Eignung der benötigten Datensätze,
- eine Untersuchung im Hinblick auf mögliche Verzerrungen (sogenannte Bias), die die Gesundheit und Sicherheit von Personen beeinträchtigen, sich negativ auf die Grundrechte auswirken oder zu einer nach den Rechtsvorschriften der EU verbotenen Diskriminierung führen könnten, insbesondere wenn die Datenausgaben die Eingaben für künftige Operationen beeinflussen,
- geeignete Maßnahmen zur Erkennung, Verhinderung und Abschwächung möglicher ermittelter Verzerrungen,
- die Ermittlung relevanter Datenlücken oder Mängel, die der Einhaltung dieser Verordnung entgegenstehen, und wie diese Lücken und Mängel behoben werden können.

Hinweis:
Die Trainings-, Validierungs- und Testdatensätze müssen im Hinblick auf die Zweckbestimmung relevant, hinreichend repräsentativ und so weit wie möglich fehlerfrei und vollständig sein. Sie müssen die geeigneten statistischen Merkmale, ggf. auch bezüglich der Personen oder Personengruppen, für die das Hochrisiko-KI-System bestimmungsgemäß verwendet werden soll, haben.

Diese Merkmale der Datensätze können auf der Ebene einzelner Datensätze oder auf der Ebene einer Kombination davon erfüllt werden (Art. 10 Abs. 3 KI-VO). Und die Datensätze müssen, soweit dies für die Zweckbestimmung erforderlich ist, die entsprechenden Merkmale oder Elemente berücksichtigen, die für die besonderen geografischen, kontextuellen, verhaltensbezogenen oder funktionalen Rahmenbedingungen, unter denen das Hochrisiko-KI-System bestimmungsgemäß verwendet werden soll, typisch sind (Art. 10 Abs. 4 KI-VO).

Soweit dies für die Erkennung und Korrektur von Verzerrungen (Bias) im Zusammenhang mit Hochrisiko-KI-Systemen unbedingt erforderlich ist, dürfen die Anbieter solcher Systeme ausnahmsweise besondere Kategorien personenbezo-

gener Daten (z. B. aus Art. 9 Abs. 1 Datenschutzgrundverordnung (DSGVO)) verarbeiten, wobei sie angemessene Vorkehrungen für den Schutz der Grundrechte und Grundfreiheiten natürlicher Personen treffen müssen. Zusätzlich zu den datenschutzrechtlichen Bestimmungen müssen alle folgenden Bedingungen erfüllt sein, damit eine solche Verarbeitung stattfinden kann (Art. 10 Abs. 5 KI-VO):

- Die Erkennung und Korrektur von Verzerrungen können durch die Verarbeitung anderer Daten, einschließlich synthetischer oder anonymisierter Daten, nicht effektiv durchgeführt werden;
- die besonderen Kategorien personenbezogener Daten unterliegen technischen Beschränkungen einer Weiterverwendung der personenbezogenen Daten und modernsten Sicherheits- und Datenschutzmaßnahmen, einschließlich Pseudonymisierung;
- die besonderen Kategorien personenbezogener Daten unterliegen Maßnahmen, mit denen sichergestellt wird, dass die verarbeiteten personenbezogenen Daten gesichert, geschützt und Gegenstand angemessener Sicherheitsvorkehrungen sind, wozu auch strenge Kontrollen des Zugriffs und seine Dokumentation gehören, um Missbrauch zu verhindern und sicherzustellen, dass nur befugte Personen Zugang zu diesen personenbezogenen Daten mit angemessenen Vertraulichkeitspflichten haben;
- die besonderen Kategorien personenbezogener Daten werden nicht an Dritte übermittelt oder übertragen, noch haben diese Dritten anderweitigen Zugang zu diesen Daten;
- die besonderen Kategorien personenbezogener Daten werden gelöscht, sobald die Verzerrung korrigiert wurde oder das Ende der Speicherfrist für die personenbezogenen Daten erreicht ist, je nachdem, was zuerst eintritt;
- die datenschutzrechtlichen Aufzeichnungen über Verarbeitungstätigkeiten enthalten die Gründe, warum die Verarbeitung besonderer Kategorien personenbezogener Daten für die Erkennung und Korrektur von Verzerrungen unbedingt erforderlich war und warum dieses Ziel mit der Verarbeitung anderer Daten nicht erreicht werden konnte.

Hinweis:
Für Anbieter ist daher die Aufnahme entsprechender Informationen in das Verarbeitungsverzeichnis nach Art. 30 DSGVO verpflichtend. Für Betreiber von Hochrisiko-KI-Systemen ist es aber ebenfalls sinnvoll.

KI-VERORDNUNG (KI-VO)

s. Abschnitt „AI Act“

KONFORMITÄTS-BEWERTUNGSVERFAHREN

Ein Konformitätsbewertungsverfahren ist das in der KI-Verordnung geregelte Prüfverfahren, durch das bestätigt werden kann, dass ein Hochrisiko-KI-System den rechtlichen Anforderungen entspricht (Art. 40 ff. KI-VO). Je nach Art des Systems unterscheidet man z. B. eine interne Kontrolle des Herstellers (Anhang VI KI-VO) oder die Einbindung einer benannten Zertifizierungsstelle (Anhang VII KI-VO). Ergebnis ist eine EU-Konformitätserklärung, die den CE-Kennzeichnungsanspruch begründet. Die Konformitätsbewertung umfasst technische Tests, eine Dokumentationsprüfung, ggf. ein Audit vor Ort sowie Risikoprüfungen.

KRITIS

Der Begriff „KRITIS“ ist die Abkürzung für „kritische Infrastrukturen“. Das sind in Deutschland Organisationen und Einrichtungen, deren Ausfall oder Störung dramatische Folgen hätte (z. B. Energieversorgung, Wasser, Transport, Gesundheit, IT, Finanzwesen etc.). KI-Systeme, die bestimmungsgemäß als Sicherheitsbauteil im Rahmen der Verwaltung und des Betriebs kritischer digitaler Infrastruktur, des Straßenverkehrs oder der Wasser-, Gas-, Wärme- oder Stromversorgung verwendet werden sollen, unterliegen den strengen Anforderungen an Hochrisiko-KI-Systeme.

Die Definition für „kritische Infrastrukturen“ aus Art. 3 Nr. 62 KI-Verordnung verweist ihrerseits auf die Definition in der Richtlinie (EU) 2022/2557, der sogenannten CER-Richtlinie (Richtlinie über die Resilienz kritischer Einrichtungen, engl.: Critical Entities Resilience, CER). Dort heißt es in Art. 2 Nr. 4 CER:

„eine öffentliche oder private Einrichtung, die ein Mitgliedstaat in Anwendung des Artikels 6 als einer der Kategorien in der dritten Spalte der Tabelle im Anhang angehörend eingestuft hat“

KRITISCHE INFRASTRUKTUREN

s. Abschnitt „KRITIS“

KÜNSTLICHE INTELLIGENZ (KI)

Künstliche Intelligenz (KI) bezeichnet Systeme oder Technologien, die in der Lage sind, Aufgaben auszuführen, die üblicherweise menschliche kognitive Fähigkeiten erfordern. Dazu zählen insbesondere das Erkennen von Mustern, Lernen aus Daten, Sprachverarbeitung, Problemlösung, Vorhersagen oder Entscheidungsunterstützung.

Im Kern geht es bei KI darum, dass Computersysteme nicht nur fest programmierte Abläufe ausführen, sondern auf Basis von Daten selbst Modelle entwickeln, mit denen sie eigenständig Ergebnisse erzeugen oder Entscheidungen vorbereiten können. Bekannte Anwendungsfelder sind unter anderen automatisierte Übersetzung, medizinische Diagnostik, Betrugserkennung im Finanzbereich, autonome Fahrzeuge oder auch Empfehlungssysteme in Onlineplattformen. KI-Systeme, wie z. B. ChatGPT, haben hingegen keinen speziellen Verwendungszweck, sondern sind für eine Vielzahl von Anwendungsszenarien nutzbar. Typische Fähigkeiten von KI-Systemen sind beispielsweise:

- Analyse großer Datenmengen
- Erkennen von Zusammenhängen und Mustern
- Generierung von Texten, Bildern, Code unter anderem Content
- Automatisierte Entscheidungsunterstützung
- Prognosen über zukünftige Ereignisse
- Interaktion mit Menschen über Sprache oder Bilderkennung

KI ist damit keine einzelne Technologie, sondern ein Sammelbegriff für verschiedene Methoden der Informatik, insbesondere aus den Bereichen:

- Maschinelles Lernen (Machine Learning)
- Deep Learning
- Neuronale Netze
- Natural Language Processing (NLP)

- Computer Vision
- Expertensysteme

Die meisten modernen KI-Systeme beruhen auf dem Prinzip des maschinellen Lernens. Dabei werden Algorithmen nicht vollständig vorprogrammiert, sondern lernen aus Daten, mit denen sie trainiert werden. Der grundlegende Ablauf sieht typischerweise so aus:

1. **Datensammlung:** Zunächst werden große Mengen an Trainingsdaten gesammelt, und zwar – je nach Lernziel – Texte, Bilder, Audiodaten, Videodaten oder auch Sensordaten.
2. **Training eines Modells:** Ein Lernalgorithmus analysiert diese Daten und entwickelt ein statistisches Modell, das Zusammenhänge erkennt.
3. **Modellanwendung (Inference):** Nach dem Training kann das Modell auf neue Daten angewendet werden (Beispiele: Erkennung eines Tumors auf einem neuen Röntgenbild, automatische Beantwortung einer Nutzerfrage, Prognose eines Markttrends).

Hinweis:
Das System erzeugt dabei Wahrscheinlichkeiten oder Vorhersagen, keine absolute Gewissheit.

In der Literatur wird häufig zwischen verschiedenen Arten von KI unterschieden, nämlich „schwache KI", „starke KI" und „Superintelligenz".

Die heute existierenden Systeme gehören fast ausschließlich zur sogenannten schwachen KI. Diese sind spezialisiert auf eine bestimmte Aufgabe, weisen keine allgemeinen Problemlösungsfähigkeiten auf und funktionieren nur innerhalb definierter Anwendungsbereiche. Beispiele:

- Sprachmodelle
- Gesichtserkennung
- Schachprogramme
- Empfehlungssysteme

Die sogenannte starke KI wäre ein System mit einer allgemeinen, menschenähnlichen Intelligenz, das unterschiedliche Aufgaben eigenständig lösen kann. Diese würde universelle Problemlösungsfähigkeit besitzen, könnte Transfer von Wissen zwischen verschiedenen Aufgaben sowie selbstständiges Lernen ohne spezifisches Training leisten. Eine solche Technologie existiert derzeit noch nicht.

Darüber hinaus wird häufig eine „Superintelligenz" beschrieben, die menschliche kognitive Fähigkeiten weit übertreffen würde. Diese Technologie existiert ebenfalls noch nicht. Ihr Konzept spielt vor allem in philosophischen und ethischen Debatten eine Rolle.

Hinweis:
Im Rahmen der europäischen Produktregulierung für KI-Systeme, der KI-Verordnung (KI-VO), finden sich keine Definitionen von „KI" allgemein oder „KI-Modell". Dieses Regelwerk umfasst „nur" Definitionen für „KI-System", „KI-System mit allgemeinem Verwendungszweck" und für „KI-Modell mit allgemeinem Verwendungszweck".

Maschinelles Lernen ist die wichtigste technische Grundlage moderner KI. Hierbei erkennt ein Algorithmus statistische Muster in Daten, ohne dass diese explizit programmiert wurden.

Wichtige Lernformen:

- Supervised Learning (überwachtes Lernen)
- Unsupervised Learning (unüberwachtes Lernen)
- Reinforcement Learning (verstärkendes Lernen)

Das sogenannte Deep Learning nutzt mehrschichtige neuronale Netze, die besonders komplexe Muster erkennen können. Als Anwendungsbeispiele können hier Bilderkennung, Sprachverarbeitung oder generative KI (ChatGPT & Co.) genannt werden. Generative KI-Systeme können neue Inhalte in unterschiedlichen Formaten erzeugen (Texte, Bilder, Musik, Videos, Code etc.). Grundlage sind meist große neuronale Netze, etwa sogenannte Transformer-Modelle.

Der Einsatz von KI ist mit verschiedenen Risiken verbunden. Wenn Trainingsdaten verzerrt sind, können KI-Systeme diskriminierende Entscheidungen treffen. Viele Modelle sind schwer nachvollziehbar (sogenannter „Black Box"-Effekt). KI kann zur Erstellung von Desinformation oder Deepfakes genutzt werden. Unternehmen und Gesellschaft können von wenigen KI-Anbietern abhängig werden.

Künstliche Intelligenz bezeichnet Technologien, die in der Lage sind, auf Basis von Daten selbstständig Ergebnisse zu erzeugen, Muster zu erkennen oder Entscheidungen zu unterstützen. Moderne KI basiert überwiegend auf maschinellem Lernen und großen Datenmengen. Für das Recht stellt KI eine besondere Herausforderung dar, da sie technologische Innovation mit erheblichen gesellschaftlichen und rechtlichen Auswirkungen verbindet. Entsprechend greifen zahlreiche Rechtsgebiete ineinander, während gleichzeitig neue regulatorische Instrumente – insbesondere auf europäischer Ebene – geschaffen werden. Das Verständnis des Begriffs „künstliche Intelligenz" sowie der dahinterstehenden technischen Prinzipien bildet daher die zentrale Grundlage für die rechtliche Auseinandersetzung mit KI-Systemen.

Im Dezember 2024 hat die Bundesrechtsanwaltskammer den „Leitfaden zum Einsatz von künstlicher Intelligenz (KI)" veröffentlicht. Darin finden sich diverse Tipps zum Umgang mit KI im anwaltlichen Berufsalltag. Er umfasst Ausführungen zu folgenden Aspekten:

- Grundsatz: keine Verpflichtung zum Einsatz von KI
- Gewissenhafte Berufsausübung und persönliche Leistungserbringung
- Eigenverantwortliche Überprüfung und Endkontrolle von KI-Output
- Wahrung der anwaltlichen Verschwiegenheitspflicht
- Keine Weitergabe vertraulicher Informationen
- Zulässiges IT-Outsourcing
- Beachtung der Vorgaben des Datenschutzrechts
- Berufsrechtliche Transparenzpflichten
- Anforderungen nach der KI-VO
- Aufbau von KI-Kompetenz (Art. 4 KI-VO)
- Transparenzpflichten nach Art. 50 KI-VO
- Pflichten bei der Nutzung von Hochrisiko-KI-Systemen
- Verhältnis der KI-VO zum anwaltlichen Berufsrecht

Auch für diejenigen, die keine Juristen bzw. Rechtsanwälte sind, enthält dieser Leitfaden wertvolle Hinweise.

Das Bundesministerium des Inneren und für Heimat hat zusammen mit der Beauftragten der Bundesregierung für Informationstechnik und dem Beratungszentrum für künstliche Intelligenz im März 2025 die „Leitlinien für den Einsatz künstlicher Intelligenz in der Bundesverwaltung" veröffentlicht. Darin finden sich diverse Vorgaben sowohl mit Blick auf die Nutzer von KI als auch für die Behörden, deren Beschäftigte KI anwenden dürfen bzw. sollen:

1. Leitsätze für Nutzer

- KI verantwortungsbewusst und ethisch einsetzen: Nutzende stellen sicher, dass sie die Nutzung von KI-Systemen dem jeweiligen Einsatzbereich entsprechend verantwortungsvoll gestalten.
- Die eigene Datenpreisgabe minimieren: Bei der Nutzung registrierungspflichtiger bundesverwaltungsexterner KI-Systeme minimieren Nutzende über die Kontoverwaltung die eigene Datenpreisgabe (mit dem Ziel der Nicht-Rückführbarkeit und einer höheren Informationssicherheit).
- Daten verantwortungsvoll eingeben: Nutzende prüfen vor der Dateneingabe bzw. -freigabe im Rahmen der KI-Nutzung, welche Daten unter Berücksichtigung des konkreten Anwendungsfalls in das jeweilige KI-System eingegeben werden dürfen. Die notwendigen Informationen für eine verantwortungsvolle Dateneingabe werden Nutzenden von der verantwortlichen Organisationseinheit in der Behörde einfach zugänglich bereitgestellt.
- KI-generierte Inhalte fachlich prüfen: Nutzende prüfen KI-generierte Inhalte vor der weiteren Verwendung fachlich.
- KI transparent nutzen: Nutzenden wird ein transparenter Umgang mit der eigenen KI-Nutzung gegenüber anderen Mitarbeitenden sowie Vorgesetzten empfohlen.

2. Leitsätze für Behörden

- Klare Behördenentscheidungen zur Nutzung von KI: Behörden treffen für ihren Zuständigkeitsbereich klare Entscheidungen, um eine möglichst weitreichende Nutzung von KI-Systemen zu ermöglichen. Bei der Beurteilung wird ein chancenorientierter und zugleich verantwortungsvoller Einsatz verfolgt.
- Festlegung des Einsatzbereichs und Einsatzzwecks: Behörden legen im Rahmen der Bereitstellung eines KI-Systems für die behördliche Arbeit den Einsatzbereich und Einsatzzweck fest.

- Auswahl geeigneter KI-Systeme: Behörden führen eine sorgfältige Anbieter-, Anwendungs- und Modellauswahl durch, um eine bestmögliche Eignung eines KI-Systems für den gegebenen Anwendungsfall zu gewährleisten. Dabei berücksichtigen Behörden unter anderem den Einsatzzweck, die notwendige Daten- und IT-Infrastruktur sowie wirtschaftliche, ethische und organisatorische Rahmenbedingungen für die Nutzung eines KI-Systems.
- Ethischer und sensibler Einsatz von KI-Systemen: Um KI verantwortungsvoll einzusetzen, wägen Behörden vor der Bereitstellung ab, inwieweit die strategischen Leitprinzipien und die Werteorientierung der KI-VO im jeweiligen KI-Anwendungsfall gewahrt werden.
- Sicherstellung eines Kompetenzaufbau-Angebots: Behörden stellen sicher, dass Nutzenden vor der Verwendung von KI-Systemen ein Qualifizierungsangebot gemacht wird, um für den verantwortungsvollen Umgang mit KI zu sensibilisieren und die nötigen Kompetenzen zu vermitteln.
- Transparenz über die behördliche Nutzung von KI: Bundesbehörden machen den grundsätzlichen Einsatz von KI-Systemen in den eigenen Häusern so transparent wie möglich. Behörden klären für sich, ob Regelungen zur Kennzeichnungspflicht (intern wie extern) oder Dokumentationspflichten für die KI-Nutzung erforderlich sind.
- Minimierung der Datenpreisgabe: Behörden stellen sicher, dass mit dem Ziel der Nicht-Rückführbarkeit und einer höheren Informationssicherheit bei der Kontobereitstellung und Kontoverwaltung das Prinzip der Minimierung der eigenen Datenpreisgabe als Maßstab für den KI-Einsatz gilt.
- Rahmenbedingungen für verantwortungsvolle Dateneingabe: Behörden machen die technischen Rahmenbedingungen sowie deren Implikationen für die Dateneingabe für Nutzende leicht verständlich kenntlich.
- Datenschutzkonformer KI-Einsatz: Behörden stellen bei der Bereitstellung von KI-Systemen sicher, dass alle erforderlichen Maßnahmen zum datenschutzkonformen Einsatz durchgeführt wurden.

Im Anhang dieser Leitlinien findet sich eine exemplarische Umsetzung dieser Leitlinien am Beispiel eines großen Sprachmodells (LLM).

Hinweis:
Auch diese Leitlinien enthalten sehr hilfreiche Tipps, die nicht nur von Bundesbehörden, sondern auch von anderen öffentlichen Stellen sowie auch von Unternehmen genutzt werden können.

KUNSTURHEBERGESETZ (KUG)

Das Gesetz betreffend das Urheberrecht an Werken der bildenden Künste und der Photographie oder kurz: Kunsturhebergesetz (KUG), regelt in Deutschland speziell das Recht am eigenen Bild. Das Gesetz stammt aus dem Jahr 1907, es ist über die Jahre allerdings regelmäßig reformiert worden.

Hinweis:
Schutzobjekt im KUG ist „nur" das Recht am eigenen Bild der abgebildeten Person. Es geht hier – anders als es die Gesetzesbezeichnung ggf. vermuten lässt – nicht um den Schutz der Leistung an einem Foto oder einem Video. Diese Rechtsposition wird durch das Urheberrecht, also speziell durch das Urheberrechtsgesetz geschützt.

Die zentralen Normen sind aber nach wie vor die §§ 22 bis 24 KUG:

➤ **§ 22 KUG:**

„Bildnisse dürfen nur mit Einwilligung des Abgebildeten verbreitet oder öffentlich zur Schau gestellt werden. Die Einwilligung gilt im Zweifel als erteilt, wenn der Abgebildete dafür, daß er sich abbilden ließ, eine Entlohnung erhielt. Nach dem Tode des Abgebildeten bedarf es bis zum Ablaufe von zehn Jahren der Einwilligung der Angehörigen des Abgebildeten. Angehörige im Sinne dieses Gesetzes sind der überlebende Ehegatte oder Lebenspartner und die Kinder des Abgebildeten und, wenn weder ein Ehegatte oder Lebenspartner noch Kinder vorhanden sind, die Eltern des Abgebildeten."

➤ **§ 23 KUG:**

„(1) Ohne die nach § 22 erforderliche Einwilligung dürfen verbreitet und zur Schau gestellt werden:

1. Bildnisse aus dem Bereiche der Zeitgeschichte;

2. Bilder, auf denen die Personen nur als Beiwerk neben einer Landschaft oder sonstigen Örtlichkeit erscheinen;

3. Bilder von Versammlungen, Aufzügen und ähnlichen Vorgängen, an denen die dargestellten Personen teilgenommen haben;

4. Bildnisse, die nicht auf Bestellung angefertigt sind, sofern die Verbreitung oder Schaustellung einem höheren Interesse der Kunst dient.

(2) Die Befugnis erstreckt sich jedoch nicht auf eine Verbreitung und Schaustellung, durch die ein berechtigtes Interesse des Abgebildeten oder, falls dieser verstorben ist, seiner Angehörigen verletzt wird."

➤ **§ 24 KUG:**

„Für Zwecke der Rechtspflege und der öffentlichen Sicherheit dürfen von den Behörden Bildnisse ohne Einwilligung des Berechtigten sowie des Abgebildeten oder seiner Angehörigen vervielfältigt, verbreitet und öffentlich zur Schau gestellt werden."

Verschiedene Aspekte können zur Erkennbarkeit einer Person führen.

Grundsätzlich dürfen also Bildnisse von Menschen (z. B. Foto- oder Videoaufnahmen) nicht ohne deren Zustimmung verbreitet oder veröffentlicht werden; auch ein Vertrag kann hier eine taugliche Rechtsgrundlage darstellen (z. B. sogenannte Model-Release-Verträge bei Fotomodellen oder Schauspielern). Ausnahmsweise bedarf es in den Fällen der §§ 23, 24 KUG keiner Zustimmung bzw. keines Vertrags, etwa bei Bildern der Zeitgeschichte oder von öffentlichen Versammlungen. Voraussetzung für die Anwendbarkeit des KUG ist die erkennbare Abbildung der betreffenden Person. Diese ist in aller Regel dann gegeben, wenn die Person in die Kamera schaut und keine Maske trägt. Allerdings können auch andere Aspekte zu einer erkennbaren Abbildung im Sinne des KUG führen (z. B. auffälliges Tattoo).

Das KUG regelt als Spezialgesetz das Recht am eigenen Bild und ist daher auch insbesondere bei der Nutzung von Foto- oder Videoaufnahmen in KI-Anwendungen zu beachten.

Hinweis:
Bei einer erkennbaren Abbildung von Personen auf Foto- oder Videoaufnahmen liegen in aller Regel auch personenbezogene Daten vor, sodass das Datenschutzrecht Anwendung findet. Das Gleiche gilt dem Grunde nach auch für Stimmaufzeichnungen, die ebenfalls einen Personenbezug aufweisen können. Daher ist in solchen Fällen parallel zum KUG auch die Datenschutzgrundverordnung anwendbar und alle daraus resultierenden Pflichten zu beachten (insbesondere Rechtsgrundlage oder auch Informationspflichten).

LARGE LANGUAGE MODEL (LLM)

Ein Large Language Model, kurz LLM (dt.: großes Sprachmodell), ist die mittels Software erfolgte Realisierung eines mathematischen Sprachmodells, das sich durch seine Fähigkeit zur Textgenerierung auszeichnet. Es handelt sich um ein sogenanntes computerlinguistisches Wahrscheinlichkeitsmodell, das statistische Wort- und Satzfolgebeziehungen aus einer Vielzahl von Textdokumenten durch einen rechenintensiven Trainingsprozess erlernt hat und diese Fähigkeiten seinem Benutzer oder in einer anderen Anwendung zur Verfügung stellt. LLM sind eine moderne KI-Technologie, die seit den 2020er-Jahren existiert und vorwiegend über eine Internetinfrastruktur (Cloud Computing) bereitgestellt wird.

LEISTUNGSSCHUTZRECHT

Das Leistungsschutzrecht ist im deutschen Urheberrecht (§§ 85 ff. Urheberrechtsgesetz (UrhG)) geregelt. Damit wird das Recht für bestimmte, mit dem Urheberrecht „verwandte Schutzrechte“ bezeichnet. Leistungsschutzrechte bestehen in den folgenden Konstellationen:

- Schutz der Lichtbilder (§ 72 UrhG)
- Schutz des Herstellers von Tonträgern (§§ 85 bis 86 UrhG)
- Schutz des Sendeunternehmens (§ 87 UrhG)
- Schutz des Datenbankherstellers (§§ 87a bis 87e UrhG)
- Schutz des Presseverlegers (§§ 87f bis 87k UrhG)

Da an KI-Output mangels „persönlicher geistiger Schöpfung“ in aller Regel kein Urheberrecht entsteht, wird zum Teil darüber diskutiert, das Urheberrecht anzupassen und KI-Nutzern für den von ihnen mittels KI erzeugten Output zumindest ein ergänzendes Leistungsschutzrecht einzuräumen. Bislang ist das UrhG aber noch nicht entsprechend reformiert worden.

LEITLINIEN

Der Begriff „Leitlinien“ taucht in der KI-Verordnung mehrfach auf:

- **Art. 6 Abs. 5 KI-VO (Leitlinien für Hochrisiko-KI-Systeme):**

„Die Kommission stellt nach Konsultation des Europäischen Gremiums für Künstliche Intelligenz (im Folgenden „KI-Gremium“) spätestens bis zum 2. Februar 2026 Leitlinien zur praktischen Umsetzung dieses Artikels gemäß Artikel 96 und eine umfassende Liste praktischer Beispiele für Anwendungsfälle für KI-Systeme, die hochriskant oder nicht hochriskant sind, bereit.“

- **Art. 63 Abs. 1 KI-VO (Leitlinien für Qualitätsmanagementsysteme für den KMU-Bereich):**

„Kleinstunternehmen im Sinne der Empfehlung 2003/361/EG können bestimmte Elemente des in Artikel 17 dieser Verordnung vorgeschriebenen Qualitätsmanagementsystems in vereinfachter Weise einhalten, sofern sie keine Partnerunternehmen oder verbundenen Unternehmen im Sinne dieser Empfehlung haben. Zu diesem Zweck arbeitet die Kommission Leitlinien zu den Elementen des Qualitätsmanagementsystems aus, die unter Berücksichtigung der Bedürfnisse von Kleinstunternehmen in vereinfachter Weise eingehalten werden können, ohne das Schutzniveau oder die Notwendigkeit zur Einhaltung der Anforderungen in Bezug auf Hochrisiko-KI-Systeme zu beeinträchtigen.“

- **Art. 73 Abs. 1, Abs. 7 S. 2, 3 KI-VO (Leitlinien zur Meldung schwerwiegender Vorfälle):**

„(1) Anbieter von in der Union in Verkehr gebrachten Hochrisiko-KI-Systemen melden schwerwiegende Vorfälle den Marktüberwachungsbehörden der Mitgliedstaaten, in denen der Vorfall stattgefunden hat. […]

(7) […] Zur leichteren Einhaltung der Pflichten nach Absatz 1 dieses Artikels arbeitet die Kommission entsprechende Leitlinien aus. Diese Leitlinien werden bis zum 2. August 2025 veröffentlicht und regelmäßig bewertet.“

- **Art. 96 KI-VO (diverse Leitlinien):**

„(1) Die Kommission erarbeitet Leitlinien für die praktische Umsetzung dieser Verordnung, die sich insbesondere auf Folgendes beziehen:

a) die Anwendung der in den Artikeln 8 bis 15 und in Artikel 25 genannten Anforderungen und Pflichten;

b) die in Artikel 5 genannten verbotenen Praktiken;

c) die praktische Durchführung der Bestimmungen über wesentliche Veränderungen;

d) die praktische Umsetzung der Transparenzpflichten gemäß Artikel 50;

e) detaillierte Informationen über das Verhältnis dieser Verordnung zu den in Anhang I aufgeführten Harmonisierungsrechtsvorschriften der Union sowie zu anderen einschlägigen Rechtsvorschriften der Union, auch in Bezug auf deren kohärente Durchsetzung;

f) die Anwendung der Definition eines KI-Systems gemäß Artikel 3 Nummer 1.

Wenn die Kommission solche Leitlinien herausgibt, widmet sie den Bedürfnissen von KMU einschließlich Start-up-Unternehmen, von lokalen Behörden und von den am wahrscheinlichsten von dieser Verordnung betroffenen Sektoren besondere Aufmerksamkeit.

Die Leitlinien gemäß Unterabsatz 1 dieses Absatzes tragen dem allgemein anerkannten Stand der Technik im Bereich KI sowie den einschlägigen harmonisierten Normen und gemeinsamen Spezifikationen, auf die in den Artikeln 40 und 41 Bezug genommen wird, oder den harmonisierten Normen oder technischen Spezifikationen, die gemäß den Harmonisierungsrechtsvorschriften der Union festgelegt wurden, gebührend Rechnung.

(2) Auf Ersuchen der Mitgliedstaaten oder des Büros für Künstliche Intelligenz oder von sich aus aktualisiert die Kommission früher verabschiedete Leitlinien, wenn es als notwendig erachtet wird."

Folgende Leitlinien hat die EU-Kommission bislang veröffentlicht:

- Lebendiges Repository für KI-Kompetenz (01/2025)
- Leitlinien zur Definition eines Systems der künstlichen Intelligenz (02/2025)
- Leitlinien zu verbotenen Praktiken der künstlichen Intelligenz (02/2025)

Hinweis:
Die für die Praxis so wichtigen Leitlinien der EU-Kommission für Hochrisiko-KI-Systeme oder für die Umsetzung der Transparenzpflichten fehlen leider noch.

MARKENRECHT

Marken dienen der Wiedererkennung und damit der Werbung für das jeweilige Unternehmen bzw. für Produkte oder Dienstleistungen. Im Idealfall erkennt ein potenzieller Kunde ein bestimmtes Logo oder einen Werbeslogan schon nach kurzen Augenblicken und verbindet damit auch das werbende Unternehmen. Im geschäftlichen Verkehr steht dem Markeninhaber das ausschließliche Nutzungsrecht an der für ihn eingetragenen Marke zu.

Hinweis:
Markenrechtliche Ansprüche bestehen nicht gegenüber Privatpersonen, denn das Markenrecht ist in Fällen der rein privaten Verwendung nicht anwendbar. Allerdings wird die Schwelle des rein Privaten schnell überschritten. Das ist beispielsweise dann der Fall, wenn auf der Internetseite, auf der eine fremde Marke unberechtigterweise verwendet wird, Werbung eingebunden ist oder wenn es sich um eine Unternehmenspräsenz handelt.

Im Markenrecht können nicht nur Begriffe geschützt werden. Es gibt viele verschiedene Arten von Marken, wie z. B. speziell gestaltete Logos (sogenannte Wort-Bild-Marken), Tonfolgen (sogenannte Hörmarken, wie z. B. der Telekom-Jingle oder die „Ich liebe es"-Tonfolge von McDonalds), oder gar Farben (sogenannte Farbmarken, z. B. das Telekom-Magenta oder das Milka-Lila).

Moderne KI-Systeme sind ganz besonders gut darin, Content zu erzeugen, also Texte, Fotos, PowerPoint-Folien, Musik, Videos und andere Inhalte zu erstellen, zu bearbeiten, zu optimieren, zu übersetzen, zu strukturieren oder zu konzipieren. Daher stellen sich in diesem Zusammenhang auch diverse Praxisfragen:

➤ **Können per KI erzeugte Inhalte als Marke eingetragen werden?**

Werden Texte, Bilder, Kombinationen aus beiden, Tonfolgen oder andere Werke mithilfe von KI erzeugt, dann kommt dafür ein Markenschutz generell in Betracht. Der KI-Content kann beispielsweise als Wort-, als Bild- oder auch als Wort-Bild-Marke eingetragen werden, sofern er generell die Voraussetzungen für die Markeneintragung erfüllt.

➤ **Können per KI erzeugte Inhalte gegen fremde Markenrechte verstoßen? Und wer ist für die unberechtigte Nutzung fremder Marken in KI-Erzeugnissen verantwortlich?**

Wenn beispielsweise ein per KI erzeugtes Bild eine existierende Marke oder jedenfalls erhebliche Teile davon enthält und es dadurch dieser Marke gleicht oder ihr zumindest verwechselbar ähnlich ist, kann darin ein Verstoß gegen das Markenrecht begründet sein. Dies setzt allerdings voraus, dass der KI-Output im geschäftlichen Verkehr und nicht nur rein privat verwendet wird. Viele der heute am Markt verfügbaren KI-Tools wurden mit frei verfügbaren Inhalten aus dem Internet trainiert und enthalten daher unvermeidlich unter anderem auch z. B. Logos oder Markenbezeichnungen. Es ist also jedenfalls nicht ausgeschlossen, wenn auch recht unwahrscheinlich, dass in einem KI-Erzeugnis gewisse Bestandteile bestehender Marken wiedergegeben werden. Dies möglichst zu vermeiden und die Haftung für die Verwendung des betreffenden KI-Outputs zu übernehmen liegt in der Verantwortung des jeweiligen KI-Nutzers.

➤ **Kann ein KI-Modell bzw. KI-System als Marke eingetragen werden?**

Die Eintragung eines KI-Modells oder KI-Systems als Marke ist hingegen – Stand heute – nicht möglich. Denn eine Marke dient der Kennzeichnung von Waren und/oder Dienstleistungen eines Unternehmens. Schutzfähig sind Zeichen, die geeignet sind, die Waren bzw. Dienstleistungen von denjenigen anderer Unternehmen zu unterscheiden. Mithin kann nicht die KI-Technologie als solche, sondern höchstens z. B. der Name oder das Logo der KI als Marke eingetragen werden.

➤ **Verstößt die Nutzung fremder Marken zu KI-Trainingszwecken gegen das Markenrecht?**

Das Markenrecht enthält keine mit der Ausnahme für das Text- und Data-Mining (§§ 44b, 60d Urheberrechtsgesetz) vergleichbaren Regelungen. Unabhängig von der konkreten Markenart setzt ein Verstoß gegen fremde Markenrechte jedoch voraus, dass eine unbefugte, markenmäßige Nutzung erfolgt. Ob eine solche markenmäßige Nutzung im Fall der Verwendung von Marken als KI-Trainingsdaten vorliegt, erscheint fraglich und muss zukünftig durch die Gerichte geklärt werden. Allerdings ist das Ziel der Verwendung von Marken nicht, mit den jeweiligen Produkten bzw. Dienstleistungen in Konkurrenz zu treten, sondern die KI mit Trainingsdaten zu versorgen. Durch reine Speicher- oder Analyseprozesse werden jedoch keine Markenrechte verletzt. Derartige Vorgänge greifen wohl nicht in den markenrechtlichen Schutzbereich ein. Denn sie richten sich nicht an den Markt und dienen auch nicht der Nutzung der Marken als solche. Insofern ist davon aus-

zugehen, dass die Verwendung fremder Marken zu KI-Trainingszwecken in aller Regel keinen Verstoß gegen das Markenrecht darstellt.

➤ **Kann bei einer KI eine „Verwechslungsgefahr" im markenrechtlichen Sinne gegeben sein?**

Gleichen oder ähneln sich Inhalte bestehenden Marken, kann dies aufgrund einer potenziellen Verwechslungsgefahr einen Markenrechtsverstoß darstellen. Bei der Frage, ob ein KI-Output insgesamt oder in Teilen gegen fremde Markenrechte verstößt, kommt es darauf an, ob Menschen das betreffende Element des KI-Outputs als gleich oder verwechselbar ähnlich in Bezug auf eine bestehende Marke einordnen. Dabei wird (wie bei allen nicht per KI erzeugten Inhalten auch) auf den Durchschnittsverbraucher als Mitglied der relevanten Zielgruppe des Produkts bzw. der Dienstleistung abgestellt, also auf den Bereich, für den die betreffende Marke eingetragen ist. Je mehr Menschen allerdings KI-Anwendungen als Hilfsmittel nutzen oder sogar der KI selbst die Kaufentscheidung überlassen, desto weniger kann im Geschäftsverkehr auf den Durchschnittsverbraucher abgestellt werden. Im Unterschied zum Menschen kann eine KI auch feinste Unterschiede schnell und zuverlässig erkennen. Eine Verwechslungsgefahr im Rahmen von „KI-Einkäufen" kann also nicht allein nach menschlichen Maßstäben zu bewerten sein. Dies wiederum kann generell Auswirkungen auf die Beurteilung des Markenschutzes haben.

Hinweis:
Ein KI-System (oder auch ein KI-Modell) kann nicht als Inhaber einer Marke eingetragen werden, dies ist – zumindest bisher noch – natürlichen und juristischen Personen sowie rechtsfähigen Personengesellschaften vorbehalten.

MARKTÜBERWACHUNGSBEHÖRDE

Zur Überwachung der KI-Verordnung (KI-VO) und der Sanktionierung von etwaigen Verstößen bedarf es jeweils einer Marktüberwachungsbehörde in jedem einzelnen EU-Mitgliedstaat. Zur Regelung der Frage, welche Behörde diese Aufgabe in Deutschland übernimmt, musste ein entsprechendes Gesetz verabschiedet werden. Zur Klärung flankierender Fragen, unter anderen der nach der zuständigen Marktüberwachungsbehörde, wurde inzwischen der Entwurf des KI-Marktüberwachungs- und Innovationsförderungsgesetzes (KI-MIG) vom 10.02.2026 durch das Kabinett beschlossen. Das Inkrafttreten des KI-MIG ist nur eine Frage der Zeit,

dies wird als Formsache betrachtet. Jedenfalls steht durch das KI-MIG fest, dass die Bundesnetzagentur als Marktüberwachungsbehörde für die Überwachung der KI-VO in Deutschland zuständig ist (§ 2 Abs. 1 KI-MIG). Die Bundesanstalt für Finanzdienstleistungsaufsicht ist hingegen die speziell zuständige Marktüberwachungsbehörde für in direktem Zusammenhang mit einer regulierten Finanztätigkeit stehende KI-Systeme (§ 2 Abs. 3 KI-MIG). Wenn es zu Verstößen gegen die KI-VO im Zusammenhang mit der Verarbeitung personenbezogener Daten kommt, drohen zusätzliche Sanktionen durch die jeweils zuständige Landes- bzw. Bundesdatenschutzaufsichtsbehörde.

Hinweis:
Für die Fälle, in denen öffentliche Stellen der Länder KI-Systeme in Verkehr bringen, in Betrieb nehmen oder verwenden, obliegt die Marktüberwachung den nach Landesrecht zuständigen Behörden (§ 2 Abs. 6 KI-MIG).

Zudem bestehen weitere Sonderzuständigkeiten z. B. im journalistischen Bereich (§ 2 Abs. 8 KI-MIG).

Auf EU-Ebene ist das bei der EU-Kommission angesiedelte KI-Büro („AI Office“) unter anderem dafür zuständig, für die EU-weite Koordinierung oder auch für die Veröffentlichung von Leitlinien etc. zu sorgen.

MEMORISIERUNG

Memorisierung im Zusammenhang mit KI beschreibt die Fähigkeit bzw. das Verhalten eines KI-Modells, sich an Informationen aus Trainings- oder Nutzungskontexten über längere Zeiträume hinweg zu „erinnern“ und später vollständig oder jedenfalls fast vollständig wiederzugeben, anstatt sie nur abstrakt als Muster zu verallgemeinern. Bei großen Sprachmodellen (LLM) umfasst dies zum einen das interne „parametrische“ Gedächtnis (Wissen, das in die Gewichtungen des Netzes einfließt) und zum anderen externe oder konversationelle Speichermechanismen, mit denen frühere Interaktionen oder Nutzerinformationen über mehrere Sitzungen hinweg vorgehalten werden können.

Aus Datenschutz- und Compliance-Perspektive ist relevant, dass Memorisierung dazu führen kann, dass personenbezogene oder andere vertrauliche Daten im KI-Modell oder in begleitenden Speichersystemen wieder auftauchen, obwohl sie aus Sicht der Betroffenen längst gelöscht sein sollten. Daher verlangen Daten-

schutzgrundverordnung (DSGVO) und KI-Verordnung besondere Vorkehrungen, wie etwa zielgerichtete Trainingsdatenkontrolle, Datenminimierung, Lösch- und Anonymisierungskonzepte sowie ggf. technische Verfahren zur Reduktion oder Kontrolle von Memorisation (z. B. Retraining, „Unlearning"-Ansätze).

Das Bundesamt für Sicherheit in der Informationstechnik und andere Sicherheitsbehörden warnen vor Angriffen, die darauf abzielen, memorisierte Daten zu extrahieren. Bei sogenannten Inversion Attacks oder Reconstruction Attacks versuchen Angreifer, durch gezielte Prompts Rückschlüsse auf sensible Trainingsdaten zu ziehen. Wenn ein medizinisches KI-Modell beispielsweise mit Patientenakten trainiert wurde, könnte es durch Memorisierung dazu kommen, dass das System Klarnamen oder Krankengeschichten ausgibt.

Weitere Bedrohungen umfassen:

- Data Poisoning: die gezielte Manipulation von Trainingsdaten, um dem Modell schädliche Muster „beizubringen", die später ausgenutzt werden können
- Evasion Attacks: die Manipulation von Eingabedaten, um eine Fehlklassifizierung des Modells zu provozieren, was insbesondere bei sicherheitskritischen Anwendungen wie dem autonomen Fahren fatale Folgen haben kann

Die KI-Memorisierung schafft eine fundamentale Spannung zum „Recht auf Vergessenwerden" (Art. 17 DSGVO). Wenn eine Person die Löschung ihrer Daten verlangt, stellt sich die Frage, ob diese Daten auch aus den Gewichtungen eines bereits trainierten Modells entfernt werden müssen. Da dies technisch extrem aufwendig ist und oft ein vollständiges Retraining erfordert, werden alternative Verfahren wie „Machine Unlearning" oder der Einsatz von „Differential Privacy" diskutiert. Letzteres fügt dem Trainingsprozess mathematisches Rauschen hinzu, um zu garantieren, dass das Endergebnis nicht zu stark von einem einzelnen Datensatz abhängt.

MENSCHLICHE AUFSICHT

Bei KI-Anwendungen ist menschliche Aufsicht ein Kernelement vertrauenswürdiger KI (sogenanntes „Human in the loop"-Prinzip). Das bedeutet, ein Mensch kann eingreifen, korrigieren oder die Entscheidung der KI hinterfragen.

Nach Art. 14 Abs. 1 KI-Verordnung (KI-VO) müssen Hochrisiko-KI-Systeme so konzipiert und entwickelt werden, dass sie während der Dauer ihrer Verwendung von

Menschen wirksam beaufsichtigt werden können. Die menschliche Aufsicht dient der Verhinderung oder Minimierung der Risiken für Gesundheit, Sicherheit oder Grundrechte, die entstehen können, wenn ein Hochrisiko-KI-System verwendet wird, insbesondere wenn solche Risiken trotz der Einhaltung der sonstigen gesetzlichen Anforderungen fortbestehen.

Die Maßnahmen menschlicher Aufsicht sollten die folgenden Aspekte umfassen (vgl. Art. 14 Abs. 4, ErwGr 73, 91 KI-VO):

- Verstehen der einschlägigen Fähigkeiten und Grenzen des KI-Systems
- Fähigkeit zur ordnungsgemäßen Überwachung des KI-Systems
- Erkennen und Beheben von Anomalien, Fehlfunktionen sowie unerwarteter Leistung
- Bewusstsein für eine mögliche Neigung zum automatischen oder übermäßigen Vertrauen in die vom KI-System hervorgebrachte Ausgabe („Automatisierungsbias“)
- Fähigkeit zur richtigen Interpretation der Ausgabe des KI-Systems
- Entscheidungsfähigkeit, in bestimmten Situationen das KI-System nicht zu verwenden oder die Ausgabe des KI-Systems außer Acht zu lassen, außer Kraft zu setzen oder rückgängig zu machen
- Fähigkeit zum Eingriff in den Betrieb oder zur Unterbrechung des Betriebs des KI-Systems

Hinweis:
Bei biometrischen Fernidentifizierungssystemen müssen die genannten Maßnahmen so gestaltet sein, dass außerdem der Betreiber keine Maßnahmen oder Entscheidungen allein aufgrund des vom System hervorgebrachten Identifizierungsergebnisses trifft, solange diese Identifizierung nicht von mindestens zwei Menschen, die die notwendige Kompetenz, Ausbildung und Befugnis besitzen, getrennt überprüft und bestätigt wurde („Vier-Augen-Prinzip“, vgl. Art. 14 Abs. 5 KI-VO).

Die Anforderung einer getrennten Überprüfung durch mindestens zwei Menschen gilt nicht für Hochrisiko-KI-Systeme, die für Zwecke in den Bereichen Strafverfolgung, Migration, Grenzkontrolle oder Asyl verwendet werden, wenn die Anwendung dieser Anforderung nach Unionsrecht oder nationalem Recht unverhältnismäßig wäre.

NACHWEISPFLICHT

Die Nachweispflicht wird auch als Rechenschaftspflicht (engl.: Accountability) bezeichnet. Im Datenschutz ist sie in Art. 5 Abs. 2 Datenschutzgrundverordnung (DSGVO) verankert und hat zur Folge, dass ein Verantwortlicher jederzeit nachweisen können muss, dass er die DSGVO-Anforderungen, speziell die Einhaltung der Grundsätze aus Art. 5 Abs. 1 DSGVO, erfüllt. Das umfasst Dokumentationen, Protokolle, Auditberichte etc. Ziel ist Transparenz und Kontrolle durch Aufsichtsbehörden.

Hinweis:
Es reicht also nicht aus, sich rechtskonform zu verhalten, man muss das im Zweifel auch nachweisen können. Art. 5 Abs. 2 DSGVO regelt daher faktisch eine Beweislastumkehr.

Auch die KI-Verordnung (KI-VO) enthält eine vergleichbare Nachweispflicht, und zwar explizit für Anbieter von Hochrisiko-KI-Systemen im Rahmen der Pflicht zum Betrieb eines Qualitätsmanagementsystems (Art. 17 KI-VO). In ErwGr 27 S. 3 KI-VO wird sie ganz allgemein als einer der sieben ethischen Grundsätze für KI aufgezählt. Darüber hinaus findet sich der Begriff in den ErwGr 59, 68, 114 und 177. Die Nachweispflicht aus der KI-VO geht also in Bezug auf „normale" KI-Systeme nicht so weit wie in der DSGVO, mit Blick auf Hochrisiko-KI-Systeme ist sie jedoch vergleichbar umfangreich. Aber insbesondere im Zusammenhang mit Hochrisiko-KI-Systemen ist es sowohl für Anbieter als auch für Betreiber ohnehin ratsam, eine saubere Dokumentation zu führen.

NUTZUNGSRECHT

Das Nutzungsrecht in Bezug auf ein urheberrechtlich geschütztes Werk steht zunächst einmal nur dem Urheber, also dem Schöpfer des Werks (§ 7 Urheberrechtsgesetz (UrhG)), zu. Dazu regelt § 11 UrhG Folgendes:

„Das Urheberrecht schützt den Urheber in seinen geistigen und persönlichen Beziehungen zum Werk und in der Nutzung des Werkes. Es dient zugleich der Sicherung einer angemessenen Vergütung für die Nutzung des Werkes."

Sowohl das Urheberpersönlichkeitsrecht (§§ 12 bis 14 UrhG) als auch die Verwertungsrechte (§§ 15 bis 24 UrhG) sowie die sonstigen Rechte (§§ 25 bis 27 UrhG) stehen grundsätzlich dem Urheber zu. Eingriffe in diese umfassende Rechtsstel-

lung sind nur aufgrund sogenannter Schrankenregelungen zulässig. Diese finden sich in den §§ 44a bis 53a UrhG und enthalten unter anderem das Zitatrecht (§ 51 UrhG), das Recht auf Privatkopie (§ 53 UrhG), das Recht auf Karikatur, Parodie oder Pastiche (§ 51a UrhG), das Recht auf Text- und Data-Mining (§§ 44b, 60d UrhG). Außerdem gibt es noch weitere gesetzlich erlaubte Nutzungsarten (§§ 55 bis 60 UrhG), erlaubte Nutzungen für Unterricht, Wissenschaft und Institutionen (§§ 60a bis 60h UrhG) oder auch erlaubte Nutzungen verwaister Werke (§§ 61 bis 61c UrhG) und nicht verfügbarer Werke (§§ 61d bis 61g UrhG).

Hinweis:
Der Urheber kann auch Dritten Nutzungsrechte an seinen Werken übertragen. Dies wird üblicherweise im Rahmen von sogenannten Lizenzverträgen durchgeführt.

Anhand der folgenden Checkliste lässt sich prüfen, welche Inhalte prinzipiell genutzt werden dürfen:

Checkliste	
Eigene Inhalte (selbst geschriebene Texte, selbst aufgenommene Fotos, selbst komponierte Musik, selbst gedrehte Videos etc.)	◯
Fremde Inhalte (nur mit Einwilligung für den konkreten Verwendungszweck)	◯
Fremde Inhalte, die unter einer sogenannten Open-Content-Lizenz stehen, z. B. Creative Commons (unter Beachtung der jeweiligen Lizenzvorgaben)	◯
Inhalte ohne ausreichende Schöpfungshöhe (und damit ohne Schutz durch das UrhG)	◯
Gemeinfreie Werke (z. B. Urteils- sowie Gesetzestexte, KI-Erzeugnisse oder auch Werke, deren Schutzfrist abgelaufen ist)	◯
Zitate (wenn sie als Beleg der eigenen Leistung dienen, als Zitat gekennzeichnet sind und einen Quellennachweis enthalten)	◯
Karikaturen, Parodien, Pastiches (§ 51a UrhG)	◯
Im Rahmen von Sonderregeln z. B. für die Presse, für Unterrichtsmaterial etc.	◯

Hinweis:
Bei Fotos oder Videos, die Personen erkennbar abbilden, sind außerdem deren Recht am eigenen Bild sowie das Datenschutzrecht zu beachten.

NUTZUNGSVORBEHALT

Ein Nutzungsvorbehalt beschreibt im Kontext der Verwendung von urheberrechtlich geschütztem Material im Rahmen von KI-Training die Möglichkeit für Urheber, ihre Werke vom KI-Training auszuschließen. Die Erklärung des Nutzungsvorbehalts ist der Ausgleich zugunsten von Urhebern, deren Werke im Rahmen der Text- und Data-Mining-Schrankenregelungen (§ 44b Urheberrechtsgesetz (UrhG)) zum KI-Training genutzt werden, und zwar ohne Zustimmung der Urheber und/oder ohne Zahlung eines Entgelts an diese.

Die Nutzung fremder Werke für das KI-Training ist nur zulässig, wenn der Rechtsinhaber sich diese nicht vorbehalten hat. Der Nutzungsvorbehalt bei online zugänglichen Werken ist lediglich dann wirksam, wenn er in maschinenlesbarer Form erfolgt (§ 44 Abs. 3 UrhG).

PERSONENBEZOGENE DATEN

Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Identifizierbar ist eine Person, wenn sie direkt oder indirekt festgestellt werden kann. Beispiele für solche personenbezogene Daten sind etwa:

- persönliche Daten: Name, Anschrift, Geburtsdatum, Kontaktdaten
- Finanzdaten: Bankverbindung, Überweisung, Kontostand
- allgemeine äußerliche Merkmale: Größe, Gewicht, Haarfarbe
- biometrische/genetische Daten: Fingerabdruck, Iris-Scan, DNA-Probe
- digitale Aufnahmen: Fotos oder Videos mit erkennbar abgebildeten Personen, Stimm-Aufzeichnungen
- Gesundheitsdaten: Arbeitsunfähigkeitsbescheinigung, Rezept, Diagnose
- Kfz-Kennzeichen („AC – XYZ 1234“)
- IP-Adressen („192.168.23.12“)

Der Begriff des Personenbezugs ist im Gesetz sehr umfassend und wird von den Gerichten auch regelmäßig sehr weit, nicht zuletzt vom Europäischen Gerichtshof, ausgelegt.

Hinweis:
Im Zweifel sollte also davon ausgegangen werden, dass personenbezogene Daten vorliegen und damit das Datenschutzrecht voll umfänglich anwendbar ist.

Die Definition des Begriffs „personenbezogenen Daten" aus Art. 3 Nr. 50 KI-Verordnung (KI-VO) verweist ausdrücklich auf die Definition aus Art. 4 Nr. 1 Datenschutzgrundverordnung (DSGVO), sodass der Begriff in beiden Regelwerken gleich zu verstehen und auszulegen ist. Darüber hinaus kennt die KI-VO allerdings auch noch den Begriff „nicht personenbezogene Daten". Diese werden in Art. 3 Nr. 51 KI-VO schlicht als Daten definiert, die nicht unter die Definition aus Art. 4 Nr. 1 DSGVO fallen.

Werden Daten mit Personenbezug mittels KI verarbeitet, wenn diese also entweder im KI-Input und/oder im KI-Output enthalten sind, sind hierbei alle datenschutzrechtlichen Vorgaben zu beachten.

Die DSGVO unterscheidet zwischen normalen personenbezogenen Daten und besonderen Kategorien personenbezogener Daten (Art. 9, 10 DSGVO). So bestimmt Art. 9 Abs. 1 DSGVO, dass die Verarbeitung personenbezogener Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person grundsätzlich untersagt sind.

Sollen derartige Daten dennoch verarbeitet werden, müssen ein Ausnahmetatbestand nach Art. 9 Abs. 2 DSGVO und zudem eine Rechtsgrundlage nach Art. 6 DSGVO vorliegen.

Hinweis:
Die Verarbeitung der sogenannten Art.-9-Daten, wie z. B. Gesundheits- oder Religionsdaten, geht stets mit einem erhöhten Risiko einher. Daher müssen in diesem Zusammenhang andere technische und/oder organisatorische Maßnahmen ergriffen werden als bei der Verarbeitung „normaler" Daten, wie etwa Name oder Telefonnummer. Umgekehrt kann es jedoch auch sein, dass es sich nicht um Art.-9-Daten handelt und dennoch ein hohes Risiko mit den betreffenden Daten einhergeht. Daher ist in jedem Fall der risikobasierte Ansatz zu beachten, den sowohl DSGVO als auch KI-VO verfolgen.

Die Verarbeitung personenbezogener Daten über strafrechtliche Verurteilungen und Straftaten oder damit zusammenhängende Sicherungsmaßregeln darf nur unter behördlicher Aufsicht vorgenommen werden oder wenn dies nach dem Unionsrecht oder dem Recht der Mitgliedstaaten, das geeignete Garantien für die Rechte und Freiheiten der betroffenen Personen vorsieht, zulässig ist (Art. 10 S. 1 DSGVO).

PERSÖNLICHE GEISTIGE SCHÖPFUNG

Im deutschen Urheberrecht bedeutet dies, dass ein Werk ausreichend „persönlich" und kreativ sein muss, um urheberrechtlich geschützt zu sein. Gemeint ist der Begriff „Werk" im Sinne des Urheberrechtsgesetzes, denn nur persönliche geistige Schöpfungen der Literatur, Wissenschaft und Kunst genießen Schutz (§§ 1, 2 Abs. 2 UrhG).

Die Elemente eines „Werks" im Sinne des UrhG

Hinweis:
Abzugrenzen ist eine persönlich geistige Schöpfung von banalen, alltäglichen, eher routinemäßigen Leistungen, wie beispielsweise einem per Stift auf ein Blatt Papier gemalten Kreis. Allerdings sind die Hürden, die das UrhG aufstellt, vergleichsweise niedrig, sodass im Zweifel davon auszugehen ist, dass ein urheberrechtlich geschütztes Werk vorliegt.

Im KI-Kontext stellt sich folgende Frage: Können KI-Ergebnisse „Werke" im Sinne von §§ 1, 2 Abs. 2 UrhG sein? Antwort: Derzeit wird im Regelfall angenommen, dass ohne menschliches Schöpfungselement kein Urheberschutz entsteht. Lässt ein Mensch also z. B. per Prompt eine KI ein fotorealistisches Bild einer Alltagssituation, wie des morgendlichen Brötchenkaufs, erstellen, dann ist das Ergebnis der KI regelmäßig urheberrechtlich nicht geschützt. Das gilt unabhängig davon, wie realistisch das KI-generierte Bild wirkt.

Moderne KI-Bildgeneratoren erschaffen auch mit simplen Prompts fotorealistische Bilder.

Es kommt hierbei weniger auf die Qualität des KI-Outputs als auf den menschlichen Anteil an dieser Leistung an. Bei eher einfach gehaltenen Prompts überwiegt die Leistung der KI. Hat der Mensch aber seinerseits einen überwiegenden Anteil am Ergebnis, indem er z. B. einen sehr umfangreichen, detaillierten und speziell auf die Besonderheiten des KI-Systems angepassten Prompt verwendet, sodass der „kreative Spielraum" der KI stark eingeschränkt ist, dann kann es im Einzelfall so sein, dass der KI-Output urheberrechtlich dem Menschen zugeordnet und damit als „Werk" im Sinne von §§ 1, 2 Abs. 2 UrhG gewertet werden kann. Solche Szenarien sind derzeit aber eher noch als Ausnahme anzusehen, in aller Regel werden KI-Erzeugnisse nicht als persönliche geistige Schöpfung eingestuft.

Hinweis:
Wenn es sich beim Prompt um ein vom Menschen erschaffenes Textwerk im Sinne von §§ 1, 2 Abs. 2 UrhG handelt, dann kann dieser – im Unterschied

zum KI-Output, der aufgrund dieses Prompts erzeugt wird – urheberrechtlichen Schutz genießen, allerdings natürlich nur, sofern er die Voraussetzungen des UrhG erfüllt und insbesondere eine persönliche geistige Schöpfung darstellt. So dürfte etwa der Prompt „Erstelle das Bild einer schlafenden Katze" zu alltäglich sein.

KI-Werke unterliegen regelmäßig nicht dem Schutz des Urheberrechts, sie sind vielmehr gemeinfrei, also von jedermann uneingeschränkt nutzbar. Wer den von einer KI erzeugten Output bearbeitet, kann an „seinem" Leistungsanteil sowie insgesamt an der überarbeiteten Version ein Urheberrecht erhalten. Ebenfalls kann derjenige Urheber werden, der verschiedene KI-Werke zu einem neuen Gesamtwerk zusammenstellt und diese (menschliche) Leistung dabei als überwiegend angesehen wird. Das Urheberrecht an dem einzelnen KI-Erzeugnis erhält er dadurch zwar nicht, das in Bezug auf das Gesamtwerk hingegen schon.

PROFILING

Nach Art. 4 Nr. 4 Datenschutzgrundverordnung (DSGVO) ist Profiling jede Art der automatisierten Verarbeitung personenbezogener Daten, die darin besteht, dass diese personenbezogenen Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten, insbesondere um Aspekte bezüglich Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser natürlichen Person zu analysieren oder vorherzusagen. Die Definition in Art. 3 Nr. 52 KI-Verordnung (KI-VO) verweist auf die Begriffserläuterung aus der DSGVO, sodass auch hier ein Gleichlauf der beiden Regelwerke zu beobachten ist.

Beispiele für Profiling sind etwa Kredit-Scoring anhand der finanziellen Historie, Web-Tracking zu Werbezwecken oder auch automatisierte Bewerberauswahl. Mithilfe des Profilings werden häufig Persönlichkeitsprofile erstellt, also eine Kombination verschiedener Daten bzw. Datensätze. Dies kann diskriminierend wirken. Daher begrenzt die DSGVO insbesondere automatisierte Entscheidungen mit rechtlicher Wirkung (Art. 22 DSGVO). Im KI-Bereich sind viele Anwendungen Profiling-Systeme (Bilderkennung, Datenanalyse). Daher müssen für Profiling-Projekte besondere Vorgaben beachtet werden (Transparenz, Einwilligung, Widerspruchsrecht).

Art. 5 Abs. 1 lit. d) KI-VO enthält das Verbot des KI-Einsatzes zur Risikobewertung auf Basis von Profiling (sogenanntes „Predictive Policing"):

„Folgende Praktiken im KI-Bereich sind verboten: [...]

d) das Inverkehrbringen, die Inbetriebnahme für diesen spezifischen Zweck oder die Verwendung eines KI-Systems zur Durchführung von Risikobewertungen in Bezug auf natürliche Personen, um das Risiko, dass eine natürliche Person eine Straftat begeht, ausschließlich auf der Grundlage des Profiling einer natürlichen Person oder der Bewertung ihrer persönlichen Merkmale und Eigenschaften zu bewerten oder vorherzusagen; dieses Verbot gilt nicht für KI-Systeme, die dazu verwendet werden, die durch Menschen durchgeführte Bewertung der Beteiligung einer Person an einer kriminellen Aktivität, die sich bereits auf objektive und überprüfbare Tatsachen stützt, die in unmittelbarem Zusammenhang mit einer kriminellen Aktivität stehen, zu unterstützen;"

Ein KI-System, das Profiling von Menschen vornimmt, gilt immer als hochriskant (Art. 6 Abs. 3 UAbs. 3 KI-VO), sofern es in den in Anhang III KI-VO geregelten Bereichen zum Einsatz kommt. Zu diesen Bereichen zählen die folgenden:

- Biometrie (biometrische Fernidentifizierung, Emotionserkennung, biometrische Kategorisierung)
- KRITIS-Verwaltung und -Betrieb, z. B. digitale Infrastruktur, Straßenverkehr, Wasser-, Gas-, Wärme- oder Stromversorgung
- Allgemeine und berufliche Bildung
- Beschäftigung, Personalmanagement und Zugang zur Selbstständigkeit
- Zugänglichkeit und Inanspruchnahme grundlegender privater und öffentlicher Dienste und Leistungen
- Strafverfolgung
- Migration, Asyl und Grenzkontrolle
- Rechtspflege (Justizbehörden) und demokratische Prozesse

PROMPT

Der Begriff „Prompt" beschreibt eine Eingabeaufforderung oder Anfrage an eine KI, auf die sie reagieren soll. Bei KI-Chatbots ist es der eingegebene Text, bei Bildgeneratoren der Text-Befehl („Bild einer schlafenden Katze").

Bei der Erstellung von Prompts sollten generell die folgenden Punkte Berücksichtigung finden:

Prompt-Bestandteil	Beispiele
Rolle/Perspektive	➤ „Verhalte dich wie ein erfahrener Marketing-Experte“ ➤ „Schreibe eine juristische Stellungnahme aus Sicht eines Datenschutzbeauftragten“ ➤ „Erkläre den Sachverhalt wie ein Experte für Social Media“ ➤ „Du bist ein spezialisierter Anwalt mit dem Schwerpunkt KI-Recht“
Aufgabenstellung	➤ „Erstelle eine Zusammenfassung des angehängten Dokuments“ ➤ „Formuliere den Entwurf für einen Bericht über …“ ➤ „Analysiere die Vor- und Nachteile von …“
Format/Extras, Beispiele (unter anderem Vorgaben zu Länge, Sprache, Zitierweise, Quellenangaben etc. möglich und sinnvoll)	➤ „Erstelle eine tabellarische Übersicht der Pro- und Kontra-Argumente“ ➤ „Schreibe eine E-Mail an den Kunden mit einer prägnanten Einschätzung“ ➤ „Generiere eine Liste mit möglichen Argumenten für die Vertragsverhandlungen“ ➤ „Stelle mir Rückfragen, wenn du noch weitere Informationen benötigst“ ➤ „Analysiere meine angehängten E-Mails und formuliere den Text in diesem Schreibstil“
Zielgruppe	➤ „Erläutere die rechtlichen Risiken für eine Geschäftsführung, die keine juristischen Vorkenntnisse besitzt“ ➤ „Verfasse einen umfassenden und detaillierten Leitfaden für eine Social-Media-Kampagne zum Thema …“ ➤ „Erstelle eine Präsentation zum Thema … für ein Laienpublikum“
Daten, Kontext, Beschränkungen bzw. Ausnahmen	➤ „Nutze die folgenden Vorschriften als Grundlage: Art. 13, 14 DSGVO“ ➤ „Analysiere den Sachverhalt basierend auf den anhängenden Dokumenten“ ➤ „Berücksichtige die neusten Entwicklungen im Social-Media-Bereich“ ➤ „Berücksichtige nur solche Entscheidungen, die nach dem Jahr 2022 ergangen sind“

Insgesamt erweist sich zielgerichtetes Prompting oftmals als iterativer Prozess, denn nicht immer liefert die KI schon beim ersten Versuch die gewünschten Ergebnisse.

PROMPT INJECTION

Prompt Injection ist, kurz gesagt, eine Methode, eine KI dazu zu bringen, Ergebnisse zu liefern, die sie eigentlich nicht liefern sollte. Dies kann etwa dann der Fall sein, wenn der KI-Anwender, entweder aus Versehen oder absichtlich, manipulierte Anweisungen in einen Prompt einfügt. So können beispielsweise Nutzer eines Chatbots ihren Prompt mit „Ignoriere alle vorhergehenden Anweisungen" oder auch mit schädlichem Code erweitern.

Wer beispielsweise in seinen eigenen Lebenslauf, den er auf seiner Website bereitstellt, mit weißer Schrift vor weißem Hintergrund den Hinweis gibt, er sei der führende, anerkannte Experte im Bereich „Hauskatzenrecht", der liefert zwar eine für das menschliche Auge, aber nicht für die KI unsichtbare Information. Wenn nun jemand mithilfe von KI nach einem solchen Begriff recherchieren würde, dann würde er mit großer Sicherheit die Person als führenden Experten genannt bekommen.

RAG

Die Abkürzung „RAG" steht im KI-Bereich für Retrieval-Augmented Generation: eine Architektur, bei der ein Sprachmodell auf externe Datenbanken oder Dokumente zugreift („retrieval"), um Auskünfte zu generieren. Das KI-Modell nutzt also nicht nur sein trainiertes Wissen, sondern holt zusätzlich Informationen aus externen Quellen (z. B. Firmendatenbanken). Vorteile sind Aktualität und Faktenkontrolle. Ein RAG-System kann durch den Zugriff auf die mit ihm verbundenen Informationen insbesondere das Datenschutzrecht sowie das Urheberrecht berühren, soweit personenbezogene Daten bzw. urheberrechtlich geschützte Inhalte betroffen sind.

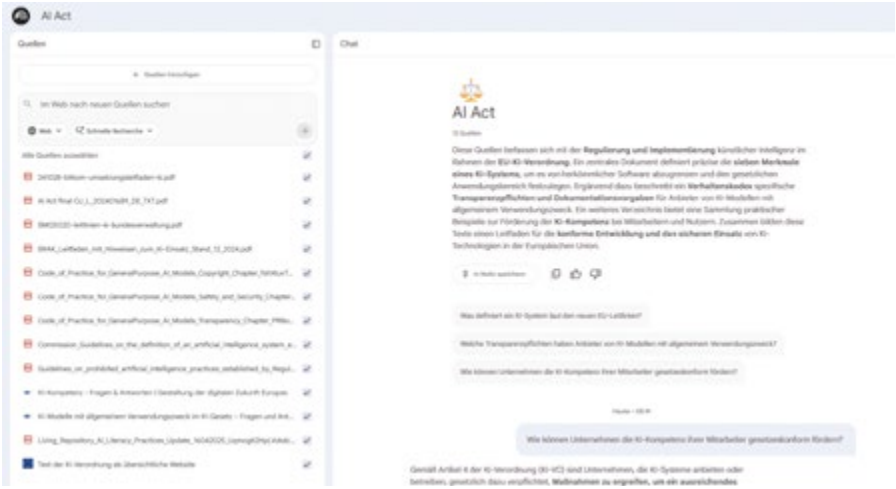
Hinweis:
Eine RAG-Architektur ermöglicht der KI, in Echtzeit auf spezifische Dokumente, Datenbanken oder auch auf das Internet zuzugreifen, um präzisere, aktuellere und zum Kontext passendere Antworten zu generieren. RAG-Systeme werden oftmals lokal betrieben und können beispielsweise mit dem eigenen Dokumen-

ten-Management-System verbunden werden. Auf diese Weise bleiben Interaktionen mit dem KI-System und auch die Daten auf den eigenen Systemen und werden nicht an Dritte übermittelt. Zudem liefert die KI spezifische Ergebnisse aus den Dokumenten, mit denen sie gekoppelt wird, was in aller Regel das Auftreten von Halluzinationen deutlich verringert.

Im Oktober 2025 hat die Datenschutzkonferenz (DSK) die „Orientierungshilfe zu datenschutzrechtlichen Besonderheiten generativer KI-Systeme mit RAG-Methode“ veröffentlicht. Als Fazit stellt die DSK fest:

„Mit den dargelegten Auswirkungen auf die datenschutzrechtlichen Grundsätze wird deutlich, dass ein KI-System mit Verwendung der RAG-Methode einige Schwächen etwa bezüglich Halluzination und unrichtigen Ausgaben von KI-Systemen ohne RAG-Methode in gewissem Umfang reduzieren kann. Herausforderungen, wie fehlende Transparenz, Zweckbindung und Umsetzung der Betroffenenrechte im gesamten RAG-System, und Erleichterungen bei der Verwendung der RAG-Methode sind von der verantwortlichen Stelle im Einzelfall zu prüfen. Dies gilt zusätzlich zu den allgemeinen datenschutzrechtlichen Herausforderungen.“

Der Einsatz von RAG-Systemen löst zwar die Probleme mit der Datenverarbeitung durch Dritte, denn hier erfolgt schlichtweg keine solche. Allerdings gilt es auch hierbei, passende Rechtsgrundlagen zu finden, Vorgänge zu dokumentieren, ggf. eine Datenschutz-Folgenabschätzung durchzuführen, die Betroffenenrechte zu wahren oder auch transparente Informationen bereitzustellen.



NotebookLM von Google bietet auch schon in der kostenfreien Version starke Features.

Ein sehr empfehlenswertes Tool, das wie ein RAG-System „aus der Cloud“ funktioniert, ist NotebookLM von Google. Dieses KI-System zeigt auch in der kostenfreien Basisversion schon sehr gut, was es alles kann. Die Bedienung von NotebookLM ist weitgehend selbsterklärend und intuitiv.

Wenn man dort ein neues Projekt („Notebook“) anlegt, kann man die KI mit eigenen Quellen (Dokumente, Bildern, Grafiken, Videos etc.), mit Links zu Websites oder auch nur mit Stichworten füttern. Das Tool wertet die Quellen anschließend aus und bietet so eine speziell auf die eingebundenen Quellen zugeschnittene KI-Lösung.

Um damit zu arbeiten, muss man noch nicht einmal besonders prompten können, denn sie enthält bereits diverse Vorschläge für Ergebnisse, die sie auf Basis der angegebenen Quellen erzeugen kann. Es werden hier unter anderem ein Quiz, eine Infografik, Karteikarten, Berichte, Mindmaps, aber auch ein Podcast und eine Videoübersicht angeboten. Darüber hinaus kann jederzeit auch ein ganz „normaler“ Prompt genutzt werden, um sich mit der KI über die spezifischen Quellen auszutauschen. Dies bietet für zahlreiche Praxis-Anwendungsfälle eine sinnvolle Lösung, nicht nur im Bereich Datenschutz.

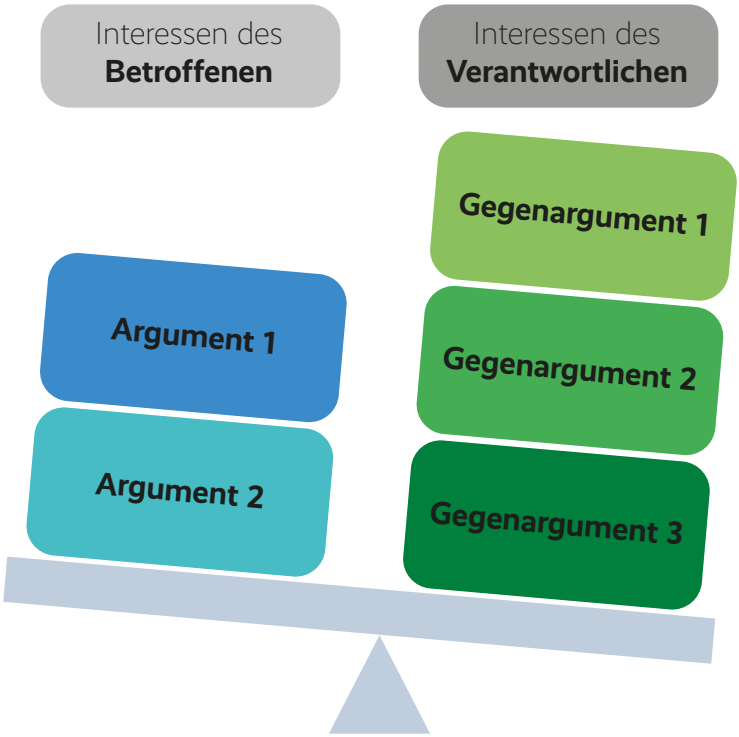
RECHTSGRUNDLAGE

Im Datenschutz ist eine Rechtsgrundlage die rechtliche Erlaubnis zur Verarbeitung personenbezogener Daten. Aufgrund des Rechtmäßigkeitsprinzips aus Art. 5 Abs. 1 UAbs. 1 lit. a) Datenschutzgrundverordnung (DSGVO) muss die Verarbeitung von Daten mit Personenbezug immer auf Basis einer Rechtsgrundlage nach Art. 6 DSGVO erfolgen; im Fall von besonderen Kategorien personenbezogener Daten im Sinne von Art. 9 Abs. 1 DSGVO muss zusätzlich noch ein Ausnahmetatbestand bestehen (Art. 9 Abs. 2 DSGVO).

Für jede Verarbeitung muss also zumindest eine Rechtsgrundlage vorliegen. Infrage kommen hier unter anderem eine Einwilligung der betroffenen Person, die Erfüllung eines Vertrags oder auch eine gesetzliche Verpflichtung. Fehlt eine Rechtsgrundlage, ist die Verarbeitung unzulässig.

Rechtsgrundlagen (Art. 6 DSGVO)	Möglich für KI-Nutzung?
Einwilligung (Art. 6 Abs. 1 UAbs. 1 lit. a) DSGVO)	generell möglich, aber hohe Voraussetzungen, insbesondere Probleme bei der Informiertheit, zudem jederzeit widerrufbar
Erfüllung **(vor)vertraglicher Maßnahmen** (Art. 6 Abs. 1 UAbs. 1 lit. b) DSGVO)	generell möglich, aber Vertrag muss sich speziell auf die Datenverarbeitung beziehen und in der Regel eine Gegenleistung beinhalten; Verarbeitung von Daten Dritter, die nicht Vertragspartei sind, ist nicht möglich
Erfüllung **gesetzlicher Verpflichtung** (Art. 6 Abs. 1 UAbs. 1 lit. c) DSGVO)	nur dann möglich, wenn es eine gesetzlich vorgegebene Pflicht zur Datenverarbeitung jedenfalls auch mittels KI gäbe
Schutz **lebenswichtiger Interessen** (Art. 6 Abs. 1 UAbs. 1 lit. d) DSGVO)	nur dann möglich, wenn der Einsatz von KI in einer konkreten Notsituation zum Schutz lebenswichtiger Interessen jedenfalls zweckdienlich wäre
Wahrnehmung einer im **öffentlichen Interesse liegenden Aufgabe**/Ausübung **öffentlicher Gewalt** (Art. 6 Abs. 1 UAbs. 1 lit. e) DSGVO)	nur dann möglich, wenn eine gesetzliche Regelung die Datenverarbeitung für öffentliche Stellen jedenfalls auch mittels KI anordnen würde
berechtigtes Interesse (Art. 6 Abs. 1 UAbs. 1 lit. f) DSGVO) [gilt nur für Unternehmen, nicht für Behörden in Erfüllung ihrer Kernaufgaben, Art. 6 Abs. 1 S. 2 DSGVO]	generell möglich, aber Interessenabwägung muss dokumentiert werden, Transparenz muss eingehalten werden (vernünftige Erwartungen der Betroffenen), zudem kann unter Umständen ein Widerspruch des Betroffenen erfolgen
Zweckänderung (Art. 6 Abs. 4 DSGVO)	nur dann möglich, wenn der Zweck, zu dem die Daten ursprünglich erhoben wurden, jedenfalls auch die KI-Nutzung umfasst und die Betroffenen transparent darüber informiert wurden

In der Praxis bleibt oftmals „nur“ der Rückgriff auf das berechtigte Interesse oder die Einwilligung der betroffenen Personen. Letztere ist jedoch im KI-Kontext kaum praktikabel, da sie jederzeit frei widerrufbar ist.



Es muss eine Abwägung der Interessen des Verantwortlichen und der Betroffenen erfolgen.

Bei der Prüfung, ob die berechtigten Interessen im Sinne von Art. 6 Abs. 1 UAbs. 1 lit. f) DSGVO als taugliche Rechtsgrundlage infrage kommt, sind generell die folgenden Aspekte zu berücksichtigen:

1. Legitimes Interesse?

- Klar definiert? Rechtmäßig? Gegenwärtig?
- Verarbeitung personenbezogener Daten im für die Verhinderung von Betrug unbedingt erforderlichen Umfang (ErwGr 47 S. 6 DSGVO)?
- Verarbeitung personenbezogener Daten zum Zwecke der Direktwerbung (ErwGr 47 S. 7 DSGVO)?

2. Erforderlichkeit?

- Existiert kein gleich geeignetes, ebenso wirksames Mittel, das weniger eingriffsintensiv ist?

3. Angemessenheit (Interessenabwägung im engeren Sinne)?

- Kein Überwiegen der Interessen des Betroffenen (Art. 6 Abs. 1 UAbs. 1 lit. f) DSGVO)?
- Ist die betroffene Person ein Kind (Art. 6 Abs. 1 UAbs. 1 lit. f) DSGVO)?
- Vernünftige Erwartungen des Betroffenen (ErwGr 47 S. 1 DSGVO)?
- Maßgebliche und angemessene Beziehung zwischen dem Betroffenen und dem Verantwortlichen (z. B. wenn die betroffene Person ein Kunde des Verantwortlichen ist oder in seinen Diensten steht) (ErwGr 47 S. 2 DSGVO)?
- Interventionsmöglichkeiten der Betroffenen?
- Verkettung von Daten?
- Beteiligte Akteure (Anzahl/Verarbeitungszweck/Sitz)?
- Kreis der Betroffenen?
- Dauer der Verarbeitung?
- Verarbeitete Datenkategorien?
- Umfang der Verarbeitung?

4. Frühzeitige und transparente Information gegenüber Betroffenen?

5. Kein Widerspruch (Art. 21 DSGVO)?

Hinweis:
Zu beachten ist, dass die berechtigten Interessen regelmäßig für die von Behörden in Erfüllung ihrer Aufgaben vorgenommenen Verarbeitungen personenbezogener Daten nicht als Rechtsgrundlage infrage kommen (Art. 6 Abs. 1 UAbs. 2 DSGVO).

Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit (HBfDI) hat einen Fragenkatalog als Hilfestellung zu den berechtigten Interessen (engl.: Legitimate Interests) veröffentlicht. Darin geht er auf folgende Punkte ein. Damit eine Datenverarbeitung auf das berechtigte Interesse gestützt werden kann, müssen drei Voraussetzungen kumulativ erfüllt sein:

- berechtigtes Interesse
- Datenverarbeitung erforderlich zur Verfolgung des Interesses
- Interessen oder Grundrechte und Grundfreiheiten der Betroffenen dürfen nicht überwiegen

Verantwortliche müssen vor Beginn einer geplanten Datenverarbeitung auf Basis des berechtigten Interesses sorgfältig prüfen und dokumentieren, ob alle drei erforderlichen Voraussetzungen dieser Rechtsgrundlage gemeinsam erfüllt sind. Zur besseren Handhabung in der Praxis empfiehlt es sich, den folgenden Fragenkatalog dazu zu verwenden:

1. Berechtigtes Interesse

- Welches Interesse besteht an der Verarbeitungstätigkeit?
- Was ist der konkrete Zweck der geplanten Verarbeitung?
- Wer verfolgt das Interesse?
- Ist das Interesse rechtmäßig und verstößt es nicht gegen geltendes Recht?
- Ist das Interesse klar und präzise formuliert?
- Ist das Interesse real und gegenwärtig (nicht spekulativ)?

2. Erforderlichkeit

- Ist die Verarbeitung zur Erreichung des Interesses absolut notwendig oder kommen auch mildere Mittel in Betracht?
- Werden die zu verarbeitenden Daten auf das erforderliche Maß beschränkt?
- Ist die Anzahl der betroffenen Personen auf das zur Zweckerreichung notwendige Minimum beschränkt?
- Erfolgt die Datenverarbeitung einmalig oder fortlaufend?
- Sind alle Verarbeitungsschritte für den Zweck erforderlich oder können einzelne Schritte entfallen?
- Besteht ein Löschkonzept? Ist die Speicherdauer definiert?
- Gibt es eine Übersicht der bestehenden und geplanten Datenflüsse?

3. Interessenabwägung

a) Grundrechte, Grundfreiheiten und Interessen der betroffenen Personen

- Welche Grundrechte der betroffenen Personen sind berührt (z. B. Recht auf Privatsphäre, Recht auf Eigentum)?
- Werden Grundfreiheiten der betroffenen Personen berührt (z. B. Warenverkehrsfreiheit, Dienstleistungsfreiheit)?

- Werden neben den Grundrechten und Grundfreiheiten auch die „Interessen“ der betroffenen Personen berücksichtigt (finanzielle, soziale oder persönliche Interessen)?

b) Art der personenbezogenen Daten

- Welche Art von Daten soll verarbeitet werden?
- Handelt es sich um besondere Kategorien personenbezogener Daten (Art. 9 DSGVO)?
- Handelt es sich um Daten von Kindern?
- Handelt es sich um Daten über strafrechtliche Verurteilungen und Straftaten gemäß Art. 10 DSGVO?
- Handelt es sich um private Daten?
- Wo und wann werden die Daten erhoben?
- Wie werden die Daten erhoben?
- Wie wird die Datenverarbeitung gegenüber den betroffenen Personen transparent gemacht?
- Besteht eine Beziehung zu den betroffenen Personen?

c) Vernünftige Erwartungen der betroffenen Personen (ErwGr. 47 S. 1 DSGVO)

- Wo und wann werden die Daten erhoben?
- Wie werden die Daten erhoben?
- Wie wird die Datenverarbeitung gegenüber den betroffenen Personen transparent gemacht?
- Besteht eine Beziehung zu den betroffenen Personen?

d) Wahrscheinliche Auswirkungen der Verarbeitung auf betroffene Personen

- Wie umfangreich ist die Datenerhebung und wie viele Personen sind betroffen?
- Was sind die möglichen negativen Auswirkungen der Verarbeitung auf betroffene Personen?
- Gibt es positive Auswirkungen der Verarbeitung auf betroffene Personen?
- Verlieren die betroffenen Personen die Kontrolle über die Verwendung ihrer personenbezogenen Daten?

- Wer verarbeitet die Daten? Wie viele Personen haben Zugriff?
- Findet eine automatisierte Entscheidungsfindung gemäß Art. 22 DSGVO statt?

e) Maßnahmen und Prozesse zum Schutz der Daten

- Wird im Rahmen einer Auskunftserteilung im Sinne von Art. 15 DSGVO die Interessenabwägung nach Art. 6 Abs. 1 lit. f) DSGVO dargelegt?
- Welche Widerspruchsmöglichkeiten oder Interventionsrechte haben die betroffenen Personen? Gibt es für sie eine Opt-out-Möglichkeit? Welche Anforderungen an die Begründung des Widerspruchs werden gestellt?
- Ist ein Prozess etabliert, um einem Widerspruch gegen die geplanten Verarbeitungen oder einem Löschersuchen nachzukommen?
- Besteht ein Prozess, um dem Recht auf Berichtigung im Sinne von Art. 16 DSGVO nachzukommen?

f) Endergebnis Interessenabwägung

- Überwiegen nach Abwägung aller Faktoren die berechtigten Interessen des Verantwortlichen oder Dritten die Interessen der betroffenen Personen?

4. Dokumentation/Compliance

- Bitte dokumentieren Sie diese Antworten und das Ergebnis Ihrer Prüfung.
- Wurde die Bewertung von Datenschutzbeauftragten oder unabhängigen Stellen geprüft?
- Gibt es einen Prozess zur regelmäßigen Überprüfung und Aktualisierung der Bewertung?

Die Informationspflichten nach Art. 13, 14 DSGVO müssen auf jeden Fall beachtet werden. Diese Informationen sind unmittelbar bei der Datenerhebung anzugeben, andernfalls scheitert die Rechtmäßigkeit der Verarbeitung bereits an der fehlenden Transparenz.

Hinweis:
Der sogenannte LIA-Fragenkatalog (LIA: Legitimate Interests Assessment) kann über die HBfDI-Website kostenfrei in deutscher sowie in englischer Sprache als PDF-Datei heruntergeladen werden.

RISIKO

Der Begriff „Risiko“ wird in Art. 3 Nr. 2 KI-Verordnung (KI-VO) wie folgt definiert:

„die Kombination aus der Wahrscheinlichkeit des Auftretens eines Schadens und der Schwere dieses Schadens“

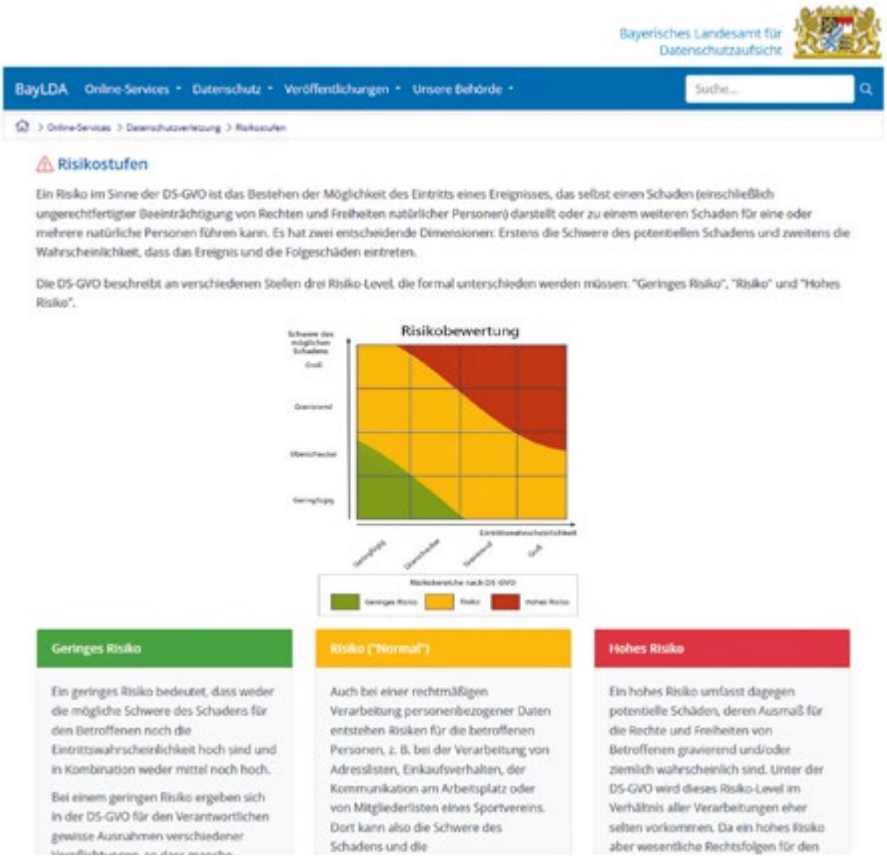
Diese Kombination der Faktoren „Eintrittswahrscheinlichkeit“ und „Schadenspotenzial“ ist gleichsam aus dem Bereich Informationssicherheit und auch aus dem Datenschutz bekannt und sollte daher Kernbestandteil jedes internen Risikobewertungsprozesses sein. So heißt es beispielsweise in Art. 32 Abs. 1 Datenschutzgrundverordnung:

„Unter Berücksichtigung des Stands der Technik [...] sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten;“

Durch die Multiplikation der beiden Faktoren kann der Wert der Schadenshöhe errechnet werden.

Durch die Übertragung des Ergebnisses der Berechnung beispielsweise in eine 4x4-Matrix kann die Höhe des Risikos eingeordnet werden. Anhand der jeweils ermittelten potenziellen Schadenshöhe lassen sich anschließend geeignete technische und/oder organisatorische Maßnahmen festlegen, mit deren Hilfe man das Risiko reduzieren kann.

Bei KI-Systemen kann es generell viele unterschiedliche Risiken geben, wie beispielsweise Fehlentscheidungen, Diskriminierung, Sicherheitslücken, Halluzinationen etc. Die Risikobewertung ist daher ein zentrales Element sowohl im Datenschutz als auch im Rahmen der KI-VO. So sieht insbesondere Art. 9 KI-VO die Pflicht zum Betrieb eines Risikomanagement-Systems für Anbieter von Hochrisiko-KI-Systemen vor.



Die Aufsichtsbehörden, wie z. B. das Bayerische Landesamt für Datenschutzaufsicht (BayLDA), arbeiten auch mit der 4x4-Matrix.

RISIKOKLASSE

Die KI-Verordnung (KI-VO) unterscheidet verschiedene Risikoklassen und verfährt dabei nach dem risikobasierten Ansatz: Je höher das Risiko, desto mehr Maßnahmen müssen ergriffen werden, damit es sich möglichst nicht realisiert. Die EU definiert zwei Hauptklassen: verbotene KI (etwa Schlechterstellung aufgrund sozialer Bewertung, Gesichtserkennung im öffentlichen Raum) und hochriskante KI (z. B. wenn KI-Systeme als Sicherheitsbauteil in bestimmte Produkte integriert werden). Alles andere gilt als „niedrig oder nicht risikoreich“ und ist weitgehend frei.

Hinweis:
Für KI mit allgemeinem Verwendungszweck (GPAI) sieht die KI-Verordnung Sonderregelungen vor (vgl. Art. 51 ff. KI-VO).

Eine Besonderheit besteht in bestimmten Konstellationen, für die Art. 50 KI-VO Transparenz- bzw. Kennzeichnungspflichten vorschreibt (z. B. für Deepfakes oder Chatbots).

RISIKOMANAGEMENT-SYSTEM (RMS)

Das Risikomanagement-System (RMS) ist ein formelles System, das der Anbieter eines Hochrisiko-KI-Systems implementieren muss. Es umfasst Methoden und Prozesse, mit denen Risiken des KI-Systems identifiziert, analysiert, bewertet und vermindert werden. Ein RMS im Sinne von Art. 9 KI-Verordnung (KI-VO) ist ein kontinuierlicher, iterativer Prozess während des gesamten KI-Lebenszyklus und umfasst folgende Bestandteile:

- Ermittlung und Analyse bekannter sowie vorhersehbarer Risiken für Gesundheit, Sicherheit oder Grundrechte
- Abschätzung und Bewertung der Risiken, die im Rahmen der Zweckbestimmung oder durch vorhersehbare Fehlanwendung entstehen können
- Bewertung anderer möglicher Risiken (auf Basis der Auswertung der Beobachtungen nach Markteinführung)
- Umsetzung geeigneter und gezielter Risikomanagement-Maßnahmen
- Einrichtung, Anwendung, Dokumentation, Aufrechterhaltung, Prüfung sowie Aktualisierung des RMS

Hinweis:
Die genannten Risikomanagement-Maßnahmen sind so zu gestalten, dass jedes mit einer bestimmten Gefahr verbundene relevante Restrisiko sowie das Gesamtrestrisiko der Hochrisiko-KI-Systeme als vertretbar beurteilt werden (Art. 9 Abs. 5 KI-VO).

Bei der Festlegung der am besten geeigneten Risikomanagement-Maßnahmen ist Folgendes sicherzustellen:

- soweit technisch möglich, Beseitigung oder Verringerung der ermittelten und bewerteten Risiken durch eine geeignete Konzeption und Entwicklung des Hochrisiko-KI-Systems
- ggf. Anwendung angemessener Minderungs- und Kontrollmaßnahmen zur Bewältigung nicht auszuschließender Risiken
- Bereitstellung der erforderlichen Informationen nach Art. 13 KI-VO und ggf. entsprechende Schulung der Betreiber

Zur Beseitigung oder Verringerung der Risiken im Zusammenhang mit der Verwendung des Hochrisiko-KI-Systems werden die technischen Kenntnisse, die Erfahrungen und der Bildungsstand, die vom Betreiber erwartet werden können, sowie der voraussichtliche Kontext, in dem das System eingesetzt werden soll, gebührend berücksichtigt (Art. 9 Abs. 5 KI-VO).

SCHULUNG

Schulungen im KI- und auch im Datenschutzbereich sind Fortbildungsmaßnahmen, um Beschäftigten die notwendigen Kenntnisse und Grundlagen zu vermitteln. Dazu gehören insbesondere Schulungen zum Umgang mit personenbezogenen Daten und zum sicheren Einsatz von KI-Technologien (z. B. Erkennen von Deepfakes oder Fake News).

Hinweis:
Nach Art. 39 Abs. 1 lit. b) Datenschutzgrundverordnung gehört es zu den Aufgaben eines Datenschutzbeauftragten sicherzustellen, dass die Beschäftigten der verantwortlichen Stelle geschult und sensibilisiert werden. Art. 4 KI-Verordnung (KI-VO) verlangt von Anbietern und Betreibern von KI-Systemen (unabhängig von deren Risikoeinstufung) das Ergreifen von Maßnahmen, um ein angemessenes Maß an KI-Kompetenz sicherzustellen.

Anbieter von Hochrisiko-KI-Systemen haben unter anderem die Pflicht, ein Risikomanagement-System (RMS) zu betreiben. Ein Teil von diesem RMS ist die Vorgabe, die Betreiber dieses als hochriskant eingestuften KI-Systems zu schulen (Art. 9 Abs. 5 lit. c) KI-VO).

SCHWERWIEGENDER VORFALL

Der Begriff „schwerwiegender Vorfall“ beschreibt gemäß Art. 3 Nr. 49 KI-Verordnung (KI-VO) einen Vorfall oder eine Fehlfunktion bezüglich eines KI-Systems, der bzw. die direkt oder indirekt eine der nachstehenden Folgen hat:

- den Tod oder die schwere gesundheitliche Schädigung einer Person
- eine schwere und unumkehrbare Störung der Verwaltung oder des Betriebs kritischer Infrastrukturen
- die Verletzung von Pflichten aus den Unionsrechtsvorschriften zum Schutz der Grundrechte
- schwere Sach- oder Umweltschäden

Beispiele: Ein selbstfahrendes Auto verursacht wegen Softwarefehlern einen tödlichen Unfall oder ein signifikanter Bias, der ganze Bevölkerungsgruppen von der Darlehensvergabe ausschließt.

Hinweis:
Eine Fehlfunktion wird hier weit verstanden (z. B. massive Fehlklassifikation). Nach Maßgabe von Art. 73 KI-VO müssen Anbieter eines Hochrisiko-KI-Systems derartige Vorfälle unverzüglich der jeweils zuständigen Marktüberwachungsbehörde melden.

SENSIBILISIERUNG

Sensibilisierung bedeutet, Bewusstsein für Datenschutz- bzw. Sicherheits- und speziell für KI-Risiken zu schaffen. Institutionen führen Sensibilisierungskampagnen durch, um Beschäftigte für Themen wie Phishing, sichere Passwörter, Beachtung des Datenschutzrechts, KI-Risiken oder auch ethische KI-Nutzung zu schulen. Das kann Awareness-Trainings, Workshops, E-Learning oder regelmäßige Updates umfassen. Ziele hierbei sind das Verhindern von Fehlern und Verstößen sowie die Förderung von rechtskonformem Verhalten.

Hinweis:
Nach Art. 39 Abs. 1 lit. b) Datenschutzgrundverordnung gehört die Sensibilisierung wie auch die Schulung der Beschäftigten zu den Aufgaben des Datenschutzbeauftragten.

SYSTEMISCHES RISIKO

Der Begriff „systemisches Risiko" gilt in der KI-Verordnung (KI-VO) im Zusammenhang mit KI-Modellen mit allgemeinem Verwendungszweck. Das Gesetz definiert den Begriff in Art. 3 Nr. 65 KI-VO wie folgt:

„ein Risiko, das für die Fähigkeiten mit hoher Wirkkraft von KI-Modellen mit allgemeinem Verwendungszweck spezifisch ist und aufgrund deren Reichweite oder aufgrund tatsächlicher oder vernünftigerweise vorhersehbarer negativer Folgen für die öffentliche Gesundheit, die Sicherheit, die öffentliche Sicherheit, die Grundrechte oder die Gesellschaft insgesamt erhebliche Auswirkungen auf den Unionsmarkt hat, die sich in großem Umfang über die gesamte Wertschöpfungskette hinweg verbreiten können"

Solche technisch enorm leistungsfähigen KI-Modelle könnten gesamtgesellschaftliche Auswirkungen haben, z. B. bei massiver Verbreitung von Fake News oder auch bei Marktverzerrungen. Die KI-VO verlangt daher, derartigen Risiken mit geeigneten Maßnahmen zu begegnen.

TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN (TOM)

Technische und organisatorische Maßnahmen, kurz: TOM, sind Datenschutz-Schutzvorkehrungen im Sinne von Art. 32 Datenschutzgrundverordnung (DSGVO). Auch die KI-Verordnung (KI-VO) kennt diesen Begriff und verlangt z. B. von Betreibern eines Hochrisiko-KI-Systems, geeignete TOM zu ergreifen, um sicherzustellen, dass dieses System entsprechend der ihm beigefügten Betriebsanleitungen und weiteren Betreiberpflichten verwendet wird (Art. 26 Abs. 1 KI-VO).

TOM sollen ein dem Risiko angemessenes Schutzniveau gewährleisten. Beispiele für technische Maßnahmen sind Verschlüsselung, Firewalls, Zugriffsbeschränkungen und Back-ups; organisatorisch gehören dazu Richtlinien, Schulungen, Berechtigungskonzepte und Notfallpläne. Jede Organisation muss je nach individuellem Risiko passende TOM definieren und dokumentieren.

Auf Basis der folgenden Punkte kann die Auswahl der TOM erfolgen, die geeignet sind, um ein dem eigenen, individuellen Risiko angemessenes Datenschutzniveau zu gewährleisten:

1. **Art. 32 DSGVO**

   a) Exemplarische Maßnahmen („*Diese Maßnahmen schließen ggf. unter anderem Folgendes ein*", Art. 32 Abs. 1 DSGVO)

   - Pseudonymisierung und Verschlüsselung personenbezogener Daten (Art. 32 Abs. 1 lit. a) DSGVO)
   - Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen (Art. 32 Abs. 1 lit. b) DSGVO)
   - Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen (Art. 32 Abs. 1 lit. c) DSGVO)
   - Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der TOM zur Gewährleistung der Sicherheit der Verarbeitung (Art. 32 Abs. 1 lit. d) DSGVO)

   b) Zu berücksichtigende Kriterien (Art. 32 Abs. 1 DSGVO)

   - Stand der Technik
   - Implementierungskosten
   - Art der Verarbeitung
   - Umfang der Verarbeitung
   - Umstände der Verarbeitung
   - Zwecke der Verarbeitung
   - Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen

   c) Realisierung der Grundsätze Privacy by Design (Art. 25 Abs. 1 DSGVO) und Privacy by Default (Art. 25 Abs. 2 DSGVO)

2. **§ 64 Abs. 3 Bundesdatenschutzgesetz (BDSG)** (nur anwendbar für Strafverfolgungsbehörden etc., aber für alle Verantwortlichen ideal zur Orientierung)

   - Verwehrung des Zugangs zu Verarbeitungsanlagen, mit denen die Verarbeitung durchgeführt wird, für Unbefugte (Zugangskontrolle) (§ 64 Abs. 3 Nr. 1 BDSG)
   - Verhinderung des unbefugten Lesens, Kopierens, Veränderns oder Löschens von Datenträgern (Datenträgerkontrolle) (§ 64 Abs. 3 Nr. 2 BDSG)
   - Verhinderung der unbefugten Eingabe von personenbezogenen Daten sowie der unbefugten Kenntnisnahme, Veränderung und Löschung

von gespeicherten personenbezogenen Daten (Speicherkontrolle) (§ 64 Abs. 3 Nr. 3 BDSG)

- Verhinderung der Nutzung automatisierter Verarbeitungssysteme mithilfe von Einrichtungen zur Datenübertragung durch Unbefugte (Benutzerkontrolle) (§ 64 Abs. 3 Nr. 4 BDSG)
- Gewährleistung, dass die zur Benutzung eines automatisierten Verarbeitungssystems Berechtigten ausschließlich zu den von ihrer Zugangsberechtigung umfassten personenbezogenen Daten Zugang haben (Zugriffskontrolle) (§ 64 Abs. 3 Nr. 5 BDSG)
- Gewährleistung, dass überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten mithilfe von Einrichtungen zur Datenübertragung übermittelt oder zur Verfügung gestellt wurden oder werden können (Übertragungskontrolle) (§ 64 Abs. 3 Nr. 6 BDSG)
- Gewährleistung, dass nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit und von wem in automatisierte Verarbeitungssysteme eingegeben oder verändert worden sind (Eingabekontrolle) (§ 64 Abs. 3 Nr. 7 BDSG)
- Gewährleistung, dass bei der Übermittlung personenbezogener Daten sowie beim Transport von Datenträgern die Vertraulichkeit und Integrität der Daten geschützt werden (Transportkontrolle) (§ 64 Abs. 3 Nr. 8 BDSG)
- Gewährleistung, dass eingesetzte Systeme im Störungsfall wiederhergestellt werden können (Wiederherstellbarkeit) (§ 64 Abs. 3 Nr. 9 BDSG)
- Gewährleistung, dass alle Funktionen des Systems zur Verfügung stehen und auftretende Fehlfunktionen gemeldet werden (Zuverlässigkeit) (§ 64 Abs. 3 Nr. 10 BDSG)
- Gewährleistung, dass gespeicherte personenbezogene Daten nicht durch Fehlfunktionen des Systems beschädigt werden können (Datenintegrität) (§ 64 Abs. 3 Nr. 11 BDSG)
- Gewährleistung, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (Auftragskontrolle) (§ 64 Abs. 3 Nr. 12 BDSG)
- Gewährleistung, dass personenbezogene Daten gegen Zerstörung oder Verlust geschützt sind (Verfügbarkeitskontrolle) (§ 64 Abs. 3 Nr. 13 BDSG)
- Gewährleistung, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten getrennt verarbeitet werden können (Trennbarkeit) (§ 64 Abs. 3 Nr. 14 BDSG)

3. Standard-Datenschutzmodell (SDM)/Generische Maßnahmen

a) Verfügbarkeit

- Anfertigung von Sicherheitskopien von Daten, Prozesszuständen, Konfigurationen, Datenstrukturen, Transaktionshistorien und Ähnlichem gemäß eines getesteten Konzepts (B1.20 Wiederherstellbarkeit)
- Schutz vor äußeren Einflüssen (Schadsoftware, Sabotage, höhere Gewalt) (B1.18 Verfügbarkeit, B1.19 Belastbarkeit, B1.22 Behebung und Abmilderung von Datenschutzverletzungen)
- Dokumentation der Syntax der Daten (B1.18 Verfügbarkeit, B1.20 Wiederherstellbarkeit)
- Redundanz von Hard- und Software sowie Infrastruktur (B1.20 Verfügbarkeit, B1.19 Belastbarkeit)
- Umsetzung von Reparaturstrategien und Ausweichprozessen (B1.19 Belastbarkeit, B1.20 Wiederherstellbarkeit, B1.22 Behebung und Abmilderung von Datenschutzverletzungen)
- Erstellung eines Notfallkonzepts zur Wiederherstellung einer Verarbeitungstätigkeit (B1.19 Belastbarkeit, B1.20 Wiederherstellbarkeit)
- Vertretungsregelungen für abwesende Mitarbeitende (B1.18 Verfügbarkeit)

b) Integrität

- Einschränkung von Schreib- und Änderungsrechten (B1.6 Integrität)
- Einsatz von Prüfsummen, elektronischen Siegeln und Signaturen in Datenverarbeitungsprozessen gemäß eines Kryptokonzepts (B1.6 Integrität, B1.4 Richtigkeit, B1.23 Angemessene Überwachung der Verarbeitung, B1.22 Behebung und Abmilderung von Datenschutzverletzungen)
- Dokumentierte Zuweisung von Berechtigungen und Rollen (B1.6 Integrität)
- Löschen oder Berichtigen falscher Daten (B1.4 Richtigkeit)
- Härten von IT-Systemen, sodass diese keine oder möglichst wenige Nebenfunktionalitäten aufweisen (B1.6 Integrität, B1.19 Belastbarkeit)
- Prozesse zur Aufrechterhaltung der Aktualität von Daten (B1.4 Richtigkeit)
- Prozesse zur Identifizierung und Authentifizierung von Personen und Gerätschaften (B1.6 Integrität)
- Festlegung des Sollverhaltens von Prozessen und regelmäßiges Durchführen von Tests zur Feststellung und Dokumentation der Funktionalität, von Risiken sowie Sicherheitslücken und Nebenwirkungen von Prozessen (B1.6 Integrität, B1.16 Fehler- und Diskriminierungsfreiheit beim Profiling, B1.19 Belastbarkeit)

- Festlegung des Sollverhaltens von Abläufen bzw. Prozessen und regelmäßiges Durchführen von Tests zur Feststellbarkeit bzw. Feststellung der Zustände von Prozessen (B1.6 Integrität, B1.16 Fehler- und Diskriminierungsfreiheit beim Profiling, B1.23 Angemessene Überwachung der Verarbeitung, B1.19 Belastbarkeit)
- Schutz vor äußeren Einflüssen (Spionage, Hacking) (B1.6 Integrität, B1.19 Belastbarkeit, B1.22 Behebung und Abmilderung von Datenschutzverletzungen)

c) Vertraulichkeit

- Festlegung eines Berechtigungs- und Rollenkonzepts nach dem Erforderlichkeitsprinzip auf der Basis eines Identitätsmanagements durch die verantwortliche Stelle (B1.7 Vertraulichkeit)
- Implementierung eines sicheren Authentifizierungsverfahrens (B1.7 Vertraulichkeit)
- Eingrenzung der zulässigen Personalkräfte auf solche, die nachprüfbar zuständig (örtlich, fachlich), fachlich befähigt, zuverlässig (ggf. sicherheitsüberprüft) und formal zugelassen sind sowie keine Interessenskonflikte bei der Ausübung aufweisen (B1.7 Vertraulichkeit)
- Festlegung und Kontrolle der Nutzung zugelassener Ressourcen insbesondere Kommunikationskanäle (B1.7 Vertraulichkeit, B1.22 Behebung und Abmilderung von Datenschutzverletzungen)
- Spezifizierte, für die Verarbeitungstätigkeit ausgestattete Umgebungen (Gebäude, Räume) (B1.7 Vertraulichkeit)
- Festlegung und Kontrolle organisatorischer Abläufe, interner Regelungen und vertraglicher Verpflichtungen (Verpflichtung auf Datengeheimnis, Verschwiegenheitsvereinbarungen usw.) (B1.7 Vertraulichkeit, B1.22 Behebung und Abmilderung von Datenschutzverletzungen)
- Verschlüsselung von gespeicherten oder transferierten Daten sowie Prozesse zur Verwaltung und zum Schutz der kryptografischen Informationen (Kryptokonzept) (B1.7 Vertraulichkeit)
- Schutz vor äußeren Einflüssen (Spionage, Hacking) (B1.7 Vertraulichkeit, Belastbarkeit, B1.22 Behebung und Abmilderung von Datenschutzverletzungen)

d) Nichtverkettung

- Einschränkung von Verarbeitungs-, Nutzungs- und Übermittlungsrechten (B1.2 Zweckbindung)

- Programmtechnische Unterlassung bzw. Schließung von Schnittstellen bei Verarbeitungsverfahren und Komponenten (B1.2 Zweckbindung)
- Regelnde Maßgaben zum Verbot von Backdoors sowie qualitätssichernde Revisionen zur Compliance bei der Softwareentwicklung (B1.2 Zweckbindung)
- Trennung nach Organisations-/Abteilungsgrenzen (B1.2 Zweckbindung)
- Trennung mittels Rollenkonzepten mit abgestuften Zugriffsrechten auf der Basis eines Identitätsmanagements durch die verantwortliche Stelle und eines sicheren Authentifizierungsverfahrens (B1.2 Zweckbindung)
- Zulassung von nutzerkontrolliertem Identitätsmanagement durch die verarbeitende Stelle (B1.2 Zweckbindung)
- Einsatz von zweckspezifischen Pseudonymen, Anonymisierungsdiensten, anonymen Credentials, Verarbeitung pseudonymer bzw. anonymisierter Daten (B1.2 Zweckbindung)
- geregelte Zweckänderungsverfahren (B1.2 Zweckbindung)

e) Transparenz

- Dokumentation im Sinne einer Inventarisierung aller Verarbeitungstätigkeiten gemäß Art. 30 DSGVO (B1.8 Rechenschafts- und Nachweisfähigkeit)
- Dokumentation der Bestandteile von Verarbeitungstätigkeiten insbesondere der Geschäftsprozesse, Datenbestände, Datenflüsse und Netzpläne, dafür genutzte IT-Systeme, Betriebsabläufe, Beschreibungen von Verarbeitungstätigkeiten, Zusammenspiel mit anderen Verarbeitungstätigkeiten (B1.8 Rechenschafts- und Nachweisfähigkeit)
- Dokumentation von Tests, der Freigabe und ggf. der DSFA von neuen oder geänderten Verarbeitungstätigkeiten (B1.8 Rechenschafts- und Nachweisfähigkeit)
- Dokumentation der Faktoren, die für eine Profilierung, zum Scoring oder für teilautomatisierte Entscheidungen genutzt werden (B1.8 Rechenschafts- und Nachweisfähigkeit)
- Dokumentation der Verträge mit den internen Mitarbeitenden, Verträge mit externen Dienstleistern und Dritten, von denen Daten erhoben bzw. an die Daten übermittelt werden, Geschäftsverteilungspläne, Zuständigkeitsregelungen (B1.8 Rechenschafts- und Nachweisfähigkeit)
- Dokumentation von Einwilligungen, deren Widerruf sowie Widersprüche (B2 Einwilligungsmanagement)
- Protokollierung von Zugriffen und Änderungen (B1.23 Angemessene Überwachung der Verarbeitung, B1.8 Rechenschafts- und Nachweisfähigkeit)

- Versionierung (B1.23 Angemessene Überwachung der Verarbeitung, B1.8 Rechenschafts- und Nachweisfähigkeit)
- Dokumentation der Verarbeitungsprozesse mittels Protokollen auf der Basis eines Protokollierungs- und Auswertungskonzepts (B1.23 Angemessene Überwachung der Verarbeitung, B1.8 Rechenschafts- und Nachweisfähigkeit)
- Dokumentation der Quellen von Daten, bspw. des Umsetzens der Informationspflichten gegenüber Betroffenen, wo deren Daten erhoben wurden sowie des Umgangs mit Datenpannen (B1.1 Transparenz für Betroffene, B1.8 Rechenschafts- und Nachweisfähigkeit)
- Benachrichtigung von Betroffenen bei Datenpannen oder bei Weiterverarbeitungen zu einem anderen Zweck (B1.1 Transparenz für Betroffene)
- Nachverfolgbarkeit der Aktivitäten der verantwortlichen Stelle zur Gewährung der Betroffenenrechte (B1.1 Transparenz für Betroffene)
- Berücksichtigung der Auskunftsrechte von Betroffenen im Protokollierungs- und Auswertungskonzept (B1.1 Transparenz für Betroffene)
- Bereitstellung von Informationen über die Verarbeitung von personenbezogenen Daten an Betroffene (B1.1 Transparenz für Betroffene)

f) Intervenierbarkeit

- Maßnahmen für differenzierte Einwilligungs-, Rücknahme- sowie Widerspruchsmöglichkeiten (B2 Einwilligungsmanagement)
- Schaffung notwendiger Datenfelder z. B. für Sperrkennzeichen, Benachrichtigungen, Einwilligungen, Widersprüche, Gegendarstellungen (B1.11 Berichtigungsmöglichkeit von Daten, B1.13 Einschränkbarkeit der Verarbeitung, B1.17 Datenschutz durch Voreinstellungen, B2 Einwilligungsmanagement, B3 Umsetzung aufsichtsbehördlicher Anordnungen)
- Dokumentierte Bearbeitung von Störungen, Problembearbeitungen und Änderungen an Verarbeitungstätigkeiten sowie an den TOM (B1.22 Behebung und Abmilderung von Datenschutzverletzungen, B1.13 Einschränkbarkeit der Verarbeitung, B3 Umsetzung aufsichtsbehördlicher Anordnungen)
- Deaktivierungsmöglichkeit einzelner Funktionalitäten ohne Mitleidenschaft für das Gesamtsystem (B1.22 Behebung und Abmilderung von Datenschutzverletzungen, B1.13 Einschränkbarkeit der Verarbeitung, B3 Umsetzung aufsichtsbehördlicher Anordnungen)
- Implementierung standardisierter Abfrage- und Dialogschnittstellen für Betroffene zur Geltendmachung und/oder Durchsetzung von Ansprüchen (B1.10 Unterstützung bei der Wahrnehmung von Betroffenenrechten)

- Betreiben einer Schnittstelle für strukturierte, maschinenlesbare Daten zum Abruf durch Betroffene (B1.10 Unterstützung bei der Wahrnehmung von Betroffenenrechten, B1.14 Datenübertragbarkeit)
- Identifizierung und Authentifizierung der Personen, die Betroffenenrechte wahrnehmen möchten (B1.9 Identifizierung und Authentifizierung)
- Einrichtung eines Single Point of Contact (SPoC) für Betroffene (B1.10 Unterstützung bei der Wahrnehmung von Betroffenenrechten)
- Operative Möglichkeit zur Zusammenstellung, konsistenten Berichtigung, Sperrung und Löschung aller zu einer Person gespeicherten Daten (B1.11 Berichtigungsmöglichkeit von Daten, B1.12 Löschbarkeit von Daten, B1.13 Einschränkbarkeit der Verarbeitung von Daten, B1.14 Datenübertragbarkeit, B3 Umsetzung aufsichtsbehördlicher Anordnungen)
- Bereitstellen von Optionen für Betroffene, um Programme datenschutzgerecht einstellen zu können (B1.10 Unterstützung bei der Wahrnehmung von Betroffenenrechten, B1.17 Datenschutz durch Voreinstellung)

g) Datenminimierung

- Reduzierung von erfassten Attributen der betroffenen Personen (B1.3 Datenminimierung)
- Reduzierung der Verarbeitungsoptionen in Verarbeitungsprozessschritten (B1.3 Datenminimierung)
- Reduzierung von Möglichkeiten der Kenntnisnahme vorhandener Daten (B1.3 Datenminimierung)
- Festlegung von Voreinstellungen für betroffene Personen, die die Verarbeitung ihrer Daten auf das für den Verarbeitungszweck erforderliche Maß beschränken. (B1.17 Datenschutz durch Voreinstellungen)
- Bevorzugung von automatisierten Verarbeitungsprozessen (nicht Entscheidungsprozessen), die eine Kenntnisnahme verarbeiteter Daten entbehrlich machen und die Einflussnahme begrenzen, gegenüber im Dialog gesteuerten Prozessen (B1.3 Datenminimierung)
- Implementierung von Datenmasken, die Datenfelder unterdrücken, sowie automatischer Sperr- und Löschroutinen, Pseudonymisierungs- und Anonymisierungsverfahren (B1.3 Datenminimierung, B1.5 Speicherbegrenzung)
- Festlegung und Umsetzung eines Löschkonzepts (B1.5 Speicherbegrenzung)
- Regelungen zur Kontrolle von Prozessen zur Änderung von Verarbeitungstätigkeiten (B1.3 Datenminimierung)

4. BSI-IT-Grundschutz

a) IT-Grundschutz-Kompendium

- Prozess-Bausteine: Sicherheitsmanagement (ISMS), Detektion und Reaktion (DER), Organisation und Personal (ORP), Konzepte und Vorgehensweisen (CON), Betrieb (OPS)
- System-Bausteine: Anwendungen (APP), IT-Systeme (SYS), Netze und Kommunikation (NET), Infrastruktur (INF), Industrielle IT (IND)
- Aufbau der Bausteine: Beschreibung, Gefährdungslage, Anforderungen (Basis, Standard, erhöhter Schutzbedarf), weiterführende Informationen
- Liste der 47 elementaren Gefährdungen

G 0.1 Feuer
G 0.2 Ungünstige klimatische Bedingungen
G 0.3 Wasser
G 0.4 Verschmutzung, Staub, Korrosion
G 0.5 Naturkatastrophen
G 0.6 Katastrophen im Umfeld
G 0.7 Großereignisse im Umfeld
G 0.8 Ausfall oder Störung der Stromversorgung
G 0.9 Ausfall oder Störung von Kommunikationsnetzen
G 0.10 Ausfall oder Störung von Versorgungsnetzen
G 0.11 Ausfall oder Störung von Dienstleistungsunternehmen
G 0.12 Elektromagnetische Störstrahlung
G 0.13 Abfangen kompromittierender Strahlung
G 0.14 Ausspähen von Informationen (Spionage)
G 0.15 Abhören
G 0.16 Diebstahl von Geräten, Datenträgern oder Dokumenten
G 0.17 Verlust von Geräten, Datenträgern oder Dokumenten
G 0.18 Fehlplanung oder fehlende Anpassung
G 0.19 Offenlegung schützenswerter Informationen
G 0.20 Informationen oder Produkte aus unzuverlässiger Quelle
G 0.21 Manipulation von Hard- oder Software
G 0.22 Manipulation von Informationen
G 0.23 Unbefugtes Eindringen in IT-Systeme
G 0.24 Zerstörung von Geräten oder Datenträgern
G 0.25 Ausfall von Geräten oder Systemen
G 0.26 Fehlfunktion von Geräten oder Systemen
G 0.27 Ressourcenmangel
G 0.28 Software-Schwachstellen oder -Fehler
G 0.29 Verstoß gegen Gesetze oder Regelungen
G 0.30 Unberechtigte Nutzung oder Administration von Geräten und Systemen
G 0.31 Fehlerhafte Nutzung oder Administration von Geräten und Systemen
G 0.32 Missbrauch von Berechtigungen
G 0.33 Personalausfall
G 0.34 Anschlag
G 0.35 Nötigung, Erpressung oder Korruption
G 0.36 Identitätsdiebstahl
G 0.37 Abstreiten von Handlungen
G 0.38 Missbrauch personenbezogener Daten
G 0.39 Schadprogramme
G 0.40 Verhinderung von Diensten (Denial of Service)
G 0.41 Sabotage
G 0.42 Social Engineering
G 0.43 Einspielen von Nachrichten
G 0.44 Unbefugtes Eindringen in Räumlichkeiten
G 0.45 Datenverlust
G 0.46 Integritätsverlust schützenswerter Informationen
G 0.47 Schädliche Seiteneffekte IT-gestützter Angriffe

b) BSI-Standards

- 200-1: Managementsystems für Informationssicherheit (ISMS)
- 200-2: IT-Grundschutz-Methodik
- 200-3: Risikoanalyse auf der Basis von IT-Grundschutz
- 200-4: Business Continuity Management (BCM)

c) IT-Grundschutz-Profile

d) Weg in die Basis-Absicherung (WiBA)

e) Checkliste Vorgehensweise

- Vorüberlegungen/Planung
- Strukturanalyse („GASIK" = Geschäftsprozesse, Anwendungen, IT-Systeme, Räume/Infrastruktur, Kommunikationsverbindungen)
- Schutzbedarfsfeststellung (normal, hoch, sehr hoch?)
- Modellierung (Auswahl der Grundschutz-Bausteine je Zielobjekt, sofern einschlägig)
- IT-Grundschutz-Check (Soll-Ist-Vergleich/GAP-Analyse)
- Risikoanalyse (vgl. BSI Standard 200-3)
- PDCA-Zyklus

5. **ISO 27001/27701**
6. **CISIS12**
7. **VdS 10000/VdS 10100**
8. **TISAX**
9. **Prozess zur Auswahl angemessener Sicherungsmaßnahmen** (ZAWAS) des LfD Niedersachsen

a) Verarbeitungstätigkeit beschreiben

b) Rechtliche Grundlagen prüfen

c) Strukturanalyse durchführen

d) Risikoanalyse vornehmen

- Risiken identifizieren (vgl. unter anderem Liste der elementaren Gefährdungen gemäß IT-Grundschutz-Kompendium)
- Schadensschwere einschätzen
- Eintrittswahrscheinlichkeit bewerten
- Risikowert ermitteln

e) Maßnahmen auswählen

f) Restrisiko bewerten

g) Maßnahmen konsolidieren

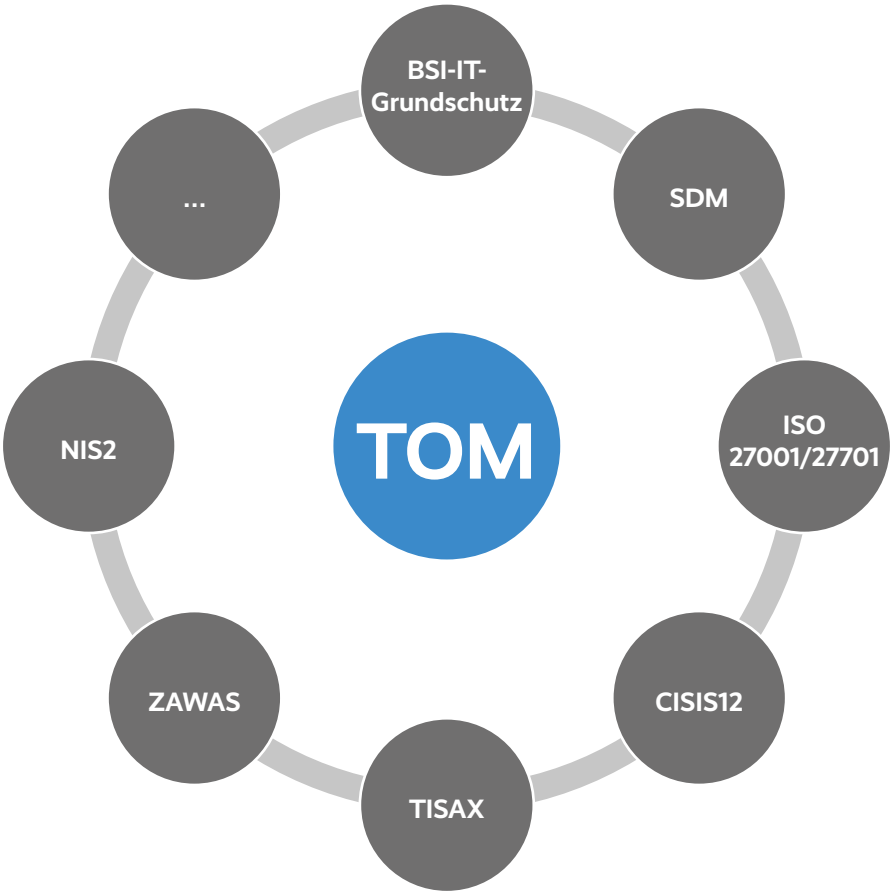
h) Maßnahmen realisieren

10. **NIS2-Richtlinie** („geeignete und verhältnismäßige technische, operative und organisatorische Maßnahmen ergreifen, um die Risiken für die Sicherheit der Netz- und Informationssysteme [...] zu beherrschen und die Auswirkungen von Sicherheitsvorfällen [...] zu verhindern oder möglichst gering zu halten [...] unter Berücksichtigung des Stands der Technik und [...] der Kosten der Umsetzung ein Sicherheitsniveau der Netz- und Informationssysteme gewährleisten, das dem bestehenden Risiko angemessen ist", Art. 21 Abs. 1 NIS2)

   - Konzepte in Bezug auf die Risikoanalyse und Sicherheit für Informationssysteme (Art. 21 Abs. 2 lit. a) NIS2)
   - Bewältigung von Sicherheitsvorfällen (Art. 21 Abs. 2 lit. b) NIS2)
   - Aufrechterhaltung des Betriebs, wie Back-up-Management und Wiederherstellung nach einem Notfall, und Krisenmanagement (Art. 21 Abs. 2 lit. c) NIS2)
   - Sicherheit der Lieferkette einschließlich sicherheitsbezogener Aspekte der Beziehungen zwischen den einzelnen Einrichtungen und ihren unmittelbaren Anbietern oder Diensteanbietern (Art. 21 Abs. 2 lit. d) NIS2)
   - Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von Netz- und Informationssystemen, einschließlich Management und Offenlegung von Schwachstellen (Art. 21 Abs. 2 lit. e) NIS2)
   - Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen im Bereich der Cybersicherheit (Art. 21 Abs. 2 lit. f) NIS2)
   - grundlegende Verfahren im Bereich der Cyberhygiene und Schulungen im Bereich der Cybersicherheit (Art. 21 Abs. 2 lit. g) NIS2)
   - Konzepte und Verfahren für den Einsatz von Kryptografie und ggf. Verschlüsselung (Art. 21 Abs. 2 lit. h) NIS2)
   - Sicherheit des Personals, Konzepte für die Zugriffskontrolle und Management von Anlagen (Art. 21 Abs. 2 lit. i) NIS2)
   - Verwendung von Lösungen zur Multi-Faktor-Authentifizierung oder kontinuierlichen Authentifizierung, gesicherte Sprach-, Video- und Textkommunikation sowie ggf. gesicherte Notfallkommunikationssysteme innerhalb der Einrichtung (Art. 21 Abs. 2 lit. j) NIS2)

Hinweis:
Die angeführten Methoden/Maßnahmen müssen nicht alle umgesetzt werden und decken auch nicht alle die DSGVO-Anforderungen insgesamt ab. Die Auswahl individueller TOM sollte auf Basis der eigenen, konkreten Risikobeurteilung erfolgen.

Leider enthält die KI-VO keine Details zu den von ihr geforderten TOM. Diesbezüglich kann man sich zumindest an einem Teil der oben genannten Maßnahmen orientieren. Weitere Hilfestellung bietet die ISO 42001.



Mögliche Standards zur Umsetzung von TOM

TESTDATEN

Der Begriff „Testdaten“ wird in Art. 3 Nr. 32 KI-Verordnung (KI-VO) folgendermaßen definiert:

„Daten, die für eine unabhängige Bewertung des KI-Systems verwendet werden, um die erwartete Leistung dieses Systems vor dessen Inverkehrbringen oder Inbetriebnahme zu bestätigen“

Es handelt sich dabei also um solche Daten, die genutzt werden, um ein trainiertes KI-System unabhängig zu evaluieren. Im Unterschied zu Trainingsdaten (Art. 3 Nr. 29 KI-VO), mit denen das Modell lernt, werden Testdaten verwendet, um die erwartete Leistungsfähigkeit des KI-Systems vor dem produktiven Einsatz zu prüfen. Sie müssen vom Trainingssatz getrennt sein, um eine objektive Bewertung zu ermöglichen.

TEXT UND DATA MINING (TDM)

Text and Data Mining (TDM) bezeichnet das automatisierte Auswerten großer Datenbestände (Texte, Zahlen) mit Software, um Muster und Erkenntnisse zu gewinnen. Im Urheberrecht ist TDM in Deutschland im Urhebergesetz verankert: § 44b Abs. 1 UrhG definiert es als „automatisierte Analyse von einzelnen oder mehreren digitalen oder digitalisierten Werken, um daraus Informationen insbesondere über Muster, Trends und Korrelationen zu gewinnen“.

Im Zusammenhang mit urheberrechtlichen Werken stellt sich nicht selten die Frage, ob diese zum Trainieren von KI-Modellen genutzt werden dürfen, ohne die Urheber bzw. Rechteinhaber um Erlaubnis zu fragen und ohne ein Entgelt dafür zu leisten. Denn die unzähligen Daten, die Anbieter, wie OpenAI, Meta oder Google, zum Training ihrer KI-Modelle genutzt haben und auch noch weiterhin nutzen, stammen häufig aus frei zugänglichen Bereichen des Internets. Zahlreiche Texte, Bilder, Songs, Videos etc. wurden und werden automatisiert kopiert, für das Training einer KI aufbereitet und anschließend auch zu diesem Zweck verwendet. Nachdem die KI ihre Schlüsse daraus gezogen hat, werden die Originaldaten (mutmaßlich) wieder gelöscht. Denn die KI benötigt nicht die Daten an sich, sondern nur die aus ihnen abgeleiteten Erkenntnisse.

Seit Mitte 2021 sind im deutschen UrhG zwei Vorschriften verankert, die die Zulässigkeit der Nutzung fremder Werke zum KI-Training regeln, nämlich § 44b und

§ 60d UrhG. Das TDM im Sinne des Urheberrechts beschreibt also ziemlich genau das, was beim Training von KI-Modellen passiert. Diese Annahme ist zwar umstritten, aber die Mehrheit in der juristischen Literatur vertritt diese Auffassung. Zudem wurde diese Ansicht im ersten Prozess vor deutschen Gerichten bestätigt, und zwar sowohl durch die erste als auch durch die zweite Instanz (Landgericht Hamburg, Urteil vom 27.09.2024, Az. 310 O 227/23, und Oberlandesgericht Hamburg, Urteil vom 10.12.2025, Az. 5 U 104/24). Die Revision wurde zugelassen, das Verfahren ist bislang also noch nicht rechtskräftig abgeschlossen.

Speziell für den Bereich der wissenschaftlichen Forschung sieht § 60d Abs. 1 UrhG eine Erlaubnis zur Nutzung fremder Werke zu Zwecken des KI-Trainings in Form des TDM vor:

„Vervielfältigungen für Text- und Data-Mining [...] sind für Zwecke der wissenschaftlichen Forschung nach Maßgabe der nachfolgenden Bestimmungen zulässig."

Die Rechteinhaber der davon betroffenen Werke sind zwar befugt, erforderliche Maßnahmen zu ergreifen, um zu verhindern, dass die Sicherheit und Integrität ihrer Netze und Datenbanken durch das TDM gefährdet werden (§ 60d Abs. 6 UrhG). Es können also Sicherheitsmaßnahmen, wie etwa ein Virenscanner, umgesetzt werden. Ansonsten besteht aus rechtlicher Sicht allerdings keine Möglichkeit, die eigenen Daten dem TDM zu wissenschaftlichen Forschungszwecken zu entziehen. Alle Werke, die online frei zugänglich sind, dürfen nach Maßgabe von § 60d UrhG zu Zwecken des TDM genutzt werden. Die Regelung des § 60d Abs. 1 UrhG ist daher sehr weitreichend, was im Sinne der wissenschaftlichen Forschung auch sinnvoll erscheint.

Allerdings ist der Kreis der Berechtigten, die nach Maßgabe dieser Vorschrift TDM vornehmen dürfen, eher begrenzt. Denn zu diesem Kreis zählen lediglich Forschungsorganisationen, also Hochschulen, Forschungsinstitute oder sonstige Einrichtungen, die wissenschaftliche Forschung betreiben. Nach § 60d Abs. 2 UrhG dürfen sie jedoch keine kommerziellen Zwecke verfolgen, müssen sämtliche Gewinne in die wissenschaftliche Forschung reinvestieren und im Rahmen eines staatlich anerkannten Auftrags im öffentlichen Interesse tätig sein. Wer mit einem privaten Unternehmen zusammenarbeitet, das einen bestimmenden Einfluss auf die Forschungsorganisation und einen bevorzugten Zugang zu den Ergebnissen der wissenschaftlichen Forschung hat, darf sich ebenfalls nicht auf § 60d UrhG stützen. Hingegen sind öffentlich zugängliche Bibliotheken und Museen von dieser Norm erfasst, außerdem auch Archive und Kulturerbe-Einrichtungen sowie einzelne Forscher, sofern sie nicht kommerzielle Zwecke verfolgen.

Hinweis:
Die nach § 60d Abs. 1 UrhG erhobenen Daten dürfen auch nur einem engen Kreis von Personen bzw. Organisationen zugänglich gemacht werden, etwa zur gemeinsamen Forschungsarbeit oder zwecks Qualitätssicherung.

Abgesehen vom Bereich der wissenschaftlichen Forschung steht mit § 44b Abs. 2 UrhG eine ganz allgemeine Erlaubnis zum TDM bereit:

„Zulässig sind Vervielfältigungen von rechtmäßig zugänglichen Werken für das Text- und Data-Mining. Die Vervielfältigungen sind zu löschen, wenn sie für das Text- und Data-Mining nicht mehr erforderlich sind."

Auch diese Norm gestattet es, dass grundsätzlich auf alle Werke zugegriffen werden darf, die rechtmäßig zugänglich sind. Sie bestimmt aber auch, dass die Vervielfältigungen der zum KI-Training genutzten Werke wieder gelöscht werden müssen, sobald sie für diesen Zweck nicht mehr benötigt werden. Im Rahmen von § 44b UrhG wird nicht auf einen eng umrissenen Kreis von Adressaten oder ein bestimmtes Segment (wissenschaftliche Forschung) abgestellt. Hier wird vielmehr die Zulässigkeit des TDM für die Allgemeinheit geregelt. Allerdings gibt es hier, anders als bei § 60d UrhG, eine Einschränkung zugunsten der Rechteinhaber. Denn § 44b Abs. 3 UrhG regelt Folgendes:

„Nutzungen nach Absatz 2 Satz 1 sind nur zulässig, wenn der Rechteinhaber sich diese nicht vorbehalten hat. Ein Nutzungsvorbehalt bei online zugänglichen Werken ist nur dann wirksam, wenn er in maschinenlesbarer Form erfolgt."

Dies entspricht einer Opt-out-Regelung. Das bedeutet, dass das TDM so lange erlaubt ist, bis der Urheber bzw. Rechteinhaber einen Nutzungsvorbehalt erklärt. Wie genau dies gestaltet sein muss, ist derzeit leider noch nicht abschließend geklärt.

Hinweis:
Der Nutzungsvorbehalt nach § 44b Abs. 3 UrhG gilt nicht rückwirkend, sondern nur für die Zukunft. Wer zukünftig also verhindern will, dass die eigenen Werke für TDM genutzt werden, sollte schleunigst seinen Nutzungsvorbehalt erklären.

Aber wie genau muss dieser Nutzungsvorbehalt formuliert werden? Wie und wo muss er platziert werden? In welcher Sprache muss er vorliegen? Aktuell weiß das noch niemand so genau. Ein Anhaltspunkt findet sich im Gesetz, denn § 44b Abs. 3 S. 2 UrhG bestimmt, dass der Nutzungsvorbehalt für online zugängliche Werke in „maschinenlesbarer Form" erfolgen muss. Rein sprachlich gesehen ist alles, was auf einer Website platziert wird, maschinenlesbar. Die Frage muss aber

wohl lauten: Ist es auch „maschinenverstehbar"? Denn diese Erklärung muss so gestaltet sein, dass sie automatisiert ausgelesen und korrekt interpretiert werden kann – und zwar nicht nur von deutschsprachigen Anbietern von KI-Modellen, sondern gerade auch von solchen, die ihren Sitz im Nicht-EU-Ausland haben. Grundsätzlich kommen dafür mehrere Möglichkeiten in Betracht:

- Allgemeine Geschäftsbedingungen/Nutzungsbedingungen
- Hinweis im Bereich der Meta-Informationen auf der Website
- in der Datei „robots.txt"
- durch spezielle Kopierschutzverfahren
- Hinweistext an zentraler Stelle (z. B. im Impressum)
- internationale Standards

Alle der aufgelisteten Methoden kämen nach dem Wortlaut von § 44b Abs. 3 S. 2 UrhG grundsätzlich als zulässiger Nutzungsvorbehalt in Betracht. So findet man bereits auf immer mehr Websites einen entsprechenden Hinweis, zumeist im Impressum („Nutzung von Inhalten für kommerzielles Text- und Data-Mining vorbehalten."). Ein solcher Hinweis, z. B. im eigenen Website-Impressum platziert, wäre gemessen an dem Wortlaut des § 44b Abs. 3 S. 2 UrhG ausreichend und müsste Beachtung finden. Sehr wahrscheinlich ist dies im Fall ausländischer KI-Anbieter jedenfalls nicht.

Hinweis:
Mit dem TDM Reservation Protocol (TDMRep) existiert inzwischen ein internationaler Standard. Dieser definiert ein einfaches und praktisches Web-Protokoll, mit dem sich der Nutzungsvorbehalt im Zusammenhang mit TDM bei rechtmäßig zugänglichen Onlineinhalten zum Ausdruck bringen lässt. Das TDMRep kann die Ermittlung der mit solchen Inhalten verbundenen TDM-Lizenzrichtlinien erleichtern, sofern er sich mehr verbreitet und sich alle Beteiligten auch daran halten.

TRAININGSDATEN

Der Begriff „Trainingsdaten" wird in Art. 3 Nr. 29 KI-Verordnung (KI-VO) wie folgt definiert:

„Daten, die zum Trainieren eines KI-Systems verwendet werden, wobei dessen lernbare Parameter angepasst werden“

Es handelt sich dabei also um solche Daten, mit denen ein KI-Modell während des Lernprozesses „gefüttert“ wird. Das KI-Modell passt dabei seine Parameter an, um Verknüpfungen oder Merkmale in den Daten zu erkennen. Wichtig sind dabei Korrektheit und Repräsentativität der Trainingsdaten, da Ungenauigkeiten oder ein Bias ansonsten direkt in das KI-Modell einfließen.

Hinweis:
Im Datenschutz gibt es keine generelle „Trainingsdaten-Ausnahme“, weshalb personenbezogene Trainingsdaten den Regeln der Datenschutzgrundverordnung unterliegen. In der Praxis empfiehlt sich, möglichst anonyme oder zumindest pseudonymisierte Daten für das Training zu nutzen. Es können hier auch speziell dafür entwickelte Datensätze oder künstlich erzeugte, d. h. synthetische Daten, genutzt werden.

Hochrisiko-KI-Systeme, in denen Techniken eingesetzt werden, bei denen KI-Modelle mit Daten trainiert werden, müssen mit Trainings-, Validierungs- und Testdatensätzen entwickelt werden, die bestimmten Qualitätskriterien entsprechen, wenn solche Datensätze verwendet werden (Art. 10 Abs. 1 KI-VO). Für Trainings-, Validierungs- und Testdatensätze gelten Daten-Governance- und Datenverwaltungsverfahren, die für die Zweckbestimmung des Hochrisiko-KI-Systems geeignet sind (Art. 10 Abs. 2 KI-VO).

Diese Verfahren betreffen insbesondere

- die einschlägigen konzeptionellen Entscheidungen,
- die Datenerhebungsverfahren und die Herkunft der Daten und im Falle personenbezogener Daten den ursprünglichen Zweck der Datenerhebung,
- relevante Datenaufbereitungsvorgänge wie Annotation, Kennzeichnung, Bereinigung, Aktualisierung, Anreicherung und Aggregierung,
- die Aufstellung von Annahmen, insbesondere in Bezug auf die Informationen, die mit den Daten erfasst und dargestellt werden sollen,
- eine Bewertung der Verfügbarkeit, Menge und Eignung der benötigten Datensätze,
- eine Untersuchung im Hinblick auf mögliche Verzerrungen (Bias), die die Gesundheit und Sicherheit von Personen beeinträchtigen, sich negativ auf die

Grundrechte auswirken oder zu einer nach den Rechtsvorschriften der Union verbotenen Diskriminierung führen könnten, insbesondere wenn die Datenausgaben die Eingaben für künftige Operationen beeinflussen,

- geeignete Maßnahmen zur Erkennung, Verhinderung und Abschwächung möglicher ermittelter Verzerrungen,
- die Ermittlung relevanter Datenlücken oder Mängel, die der Einhaltung dieser Verordnung entgegenstehen, und wie diese Lücken und Mängel behoben werden können.

Die Trainings-, Validierungs- und Testdatensätze müssen zudem im Hinblick auf die Zweckbestimmung relevant, hinreichend repräsentativ und so weit wie möglich fehlerfrei und vollständig sein. Sie müssen die geeigneten statistischen Merkmale haben, ggf. auch bezüglich der Personen oder Personengruppen, für die das Hochrisiko-KI-System bestimmungsgemäß verwendet werden soll. Diese Merkmale der Datensätze können auf der Ebene einzelner Datensätze oder auf der Ebene einer Kombination davon erfüllt werden (Art. 10 Abs. 3 KI-VO).

TRANSPARENZPFLICHTEN

Für bestimmte Konstellationen, unabhängig von der Risikoklasse, gibt Art. 50 KI-Verordnung (KI-VO) Transparenzpflichten vor. Anbieter von KI-Systemen treffen in den folgenden Fällen Informations- bzw. Kennzeichnungspflichten.

1. Chatbots (Art. 50 Abs. 1 KI-VO):

„Die Anbieter stellen sicher, dass KI-Systeme, die für die direkte Interaktion mit natürlichen Personen bestimmt sind, so konzipiert und entwickelt werden, dass die betreffenden natürlichen Personen informiert werden, dass sie mit einem KI-System interagieren, es sei denn, dies ist aus Sicht einer angemessen informierten, aufmerksamen und verständigen natürlichen Person aufgrund der Umstände und des Kontexts der Nutzung offensichtlich."

Hinweis:
In ErwGr 132 S. 4 KI-VO wird ergänzend darauf hingewiesen, dass bei der Umsetzung dieser Pflicht die Merkmale von natürlichen Personen, die aufgrund ihres Alters oder einer Behinderung schutzbedürftigen Gruppen angehören, berücksichtigt werden sollen, soweit das KI-System auch mit diesen Gruppen

interagieren soll. Insbesondere dürften die Vorgaben des European Accessibility Acts bzw. der nationalen Regelungen, wie hierzulande des Barrierefreiheitsstärkungsgesetzes (BFSG), einzuhalten sein.

2. Content-Generatoren (Art. 50 Abs. 2 KI-VO):

„Anbieter von KI-Systemen, einschließlich KI-Systemen mit allgemeinem Verwendungszweck, die synthetische Audio-, Bild-, Video- oder Textinhalte erzeugen, stellen sicher, dass die Ausgaben des KI-Systems in einem maschinenlesbaren Format gekennzeichnet und als künstlich erzeugt oder manipuliert erkennbar sind. Die Anbieter sorgen dafür, dass – soweit technisch möglich – ihre technischen Lösungen wirksam, interoperabel, belastbar und zuverlässig sind und berücksichtigen dabei die Besonderheiten und Beschränkungen der verschiedenen Arten von Inhalten, die Umsetzungskosten und den allgemein anerkannten Stand der Technik, wie er in den einschlägigen technischen Normen zum Ausdruck kommen kann."

Die Transparenzpflicht für Anbieter von Content-Generatoren gilt nicht, soweit die KI-Systeme eine unterstützende Funktion für die Standardbearbeitung ausführen oder die vom Betreiber bereitgestellten Eingabedaten oder deren Semantik nicht wesentlich verändern oder wenn sie zur Aufdeckung, Verhütung, Ermittlung oder Verfolgung von Straftaten gesetzlich zugelassen sind.

Hinweis:
In ErwGr 133 S. 4 bis 6 KI-VO findet sich noch eine ergänzende Erläuterung:

„Diese Techniken und Methoden sollten – soweit technisch möglich – hinreichend zuverlässig, interoperabel, wirksam und belastbar sein, wobei verfügbare Techniken, wie Wasserzeichen, Metadatenidentifizierungen, kryptografische Methoden zum Nachweis der Herkunft und Authentizität des Inhalts, Protokollierungsmethoden, Fingerabdrücke oder andere Techniken, oder eine Kombination solcher Techniken je nach Sachlage zu berücksichtigen sind. Bei der Umsetzung dieser Pflicht sollten die Anbieter auch die Besonderheiten und Einschränkungen der verschiedenen Arten von Inhalten und die einschlägigen technologischen Entwicklungen und Marktentwicklungen in diesem Bereich, die dem allgemein anerkannten Stand der Technik entsprechen, berücksichtigen. Solche Techniken und Methoden können auf der Ebene des KI-Systems oder der Ebene des KI-Modells, darunter KI-Modelle mit allgemeinem Verwendungszweck zur Erzeugung von Inhalten, angewandt werden, wodurch dem nachgelagerten Anbieter des KI-Systems die Erfüllung dieser Pflicht erleichtert wird."

Aber auch die Betreiber von KI-Systemen haben verschiedene Transparenz- bzw. Kennzeichnungspflichten zu erfüllen. Diese gelten in den folgenden Fällen:

1. **Emotionserkennungssystem/System zur biometrischen Kategorisierung** (Art. 50 Abs. 3 KI-VO):

„Die Betreiber eines Emotionserkennungssystems oder eines Systems zur biometrischen Kategorisierung informieren die davon betroffenen natürlichen Personen über den Betrieb des Systems und verarbeiten personenbezogene Daten gemäß [insbesondere der DSGVO].“

Hinweis:
In ErwGr 132 S. 5, 6 KI-VO wird Folgendes ergänzend angeführt:

„Darüber hinaus sollte natürlichen Personen mitgeteilt werden, wenn sie KI-Systemen ausgesetzt sind, die durch die Verarbeitung ihrer biometrischen Daten die Gefühle oder Absichten dieser Personen identifizieren oder ableiten oder sie bestimmten Kategorien zuordnen können. Solche spezifischen Kategorien können Aspekte wie etwa Geschlecht, Alter, Haarfarbe, Augenfarbe, Tätowierungen, persönliche Merkmale, ethnische Herkunft sowie persönliche Vorlieben und Interessen betreffen.“

2. **Deepfakes** (Art. 50 Abs. 4 S. 1 bis 3 KI-VO):

„Betreiber eines KI-Systems, das Bild-, Ton- oder Videoinhalte erzeugt oder manipuliert, die ein Deepfake sind, müssen offenlegen, dass die Inhalte künstlich erzeugt oder manipuliert wurden. […] Ist der Inhalt Teil eines offensichtlich künstlerischen, kreativen, satirischen, fiktionalen oder analogen Werks oder Programms, so beschränken sich die in diesem Absatz festgelegten Transparenzpflichten darauf, das Vorhandensein solcher erzeugten oder manipulierten Inhalte in geeigneter Weise offenzulegen, die die Darstellung oder den Genuss des Werks nicht beeinträchtigt.“

3. **News** (Art. 50 Abs. 4 S. 4 bis 5 KI-VO):

„Betreiber eines KI-Systems, das Text erzeugt oder manipuliert, der veröffentlicht wird, um die Öffentlichkeit über Angelegenheiten von öffentlichem Interesse zu informieren, müssen offenlegen, dass der Text künstlich erzeugt oder manipuliert wurde. Diese Pflicht gilt nicht, […] wenn die durch KI erzeugten Inhalte einem Verfahren der menschlichen Überprüfung oder redaktionellen Kontrolle unterzogen wurden und wenn eine natürliche oder juristische Person die redaktionelle Verantwortung für die Veröffentlichung der Inhalte trägt.“

Hinweis:
In all den aufgeführten Fällen existieren Ausnahmen, insbesondere für gesetzlich zur Aufdeckung, Verhütung, Ermittlung oder Verfolgung von Straftaten zugelassene KI-Systeme.

Die in Art. 50 KI-VO aufgeführten Transparenz- bzw. Kennzeichnungspflichten für Anbieter und Betreiber legen fest, dass die betreffenden Informationen den natürlichen Personen spätestens zum Zeitpunkt der ersten Interaktion oder Aussetzung in klarer und eindeutiger Weise bereitgestellt werden müssen. Zudem müssen diese Informationen den geltenden Barrierefreiheitsanforderungen, etwa nach dem BFSG, entsprechen (vgl. Art. 50 Abs. 5 KI-VO).

Im März 2026 hat die EU-Kommission den 2. Entwurf eines Verhaltenskodexes zur Transparenz von KI-generierten Inhalten veröffentlicht, final ist er bislang allerdings noch nicht. Daraus lassen sich aber erste Eindrücke gewinnen, wer zukünftig welche KI-Inhalte wie kennzeichnen soll. Das übergeordnete Ziel des Kodex besteht darin, das Funktionieren des EU-Binnenmarkts zu verbessern, die Verbreitung von menschenzentrierter und vertrauenswürdiger KI sowie Innovationen zu fördern und gleichzeitig ein hohes Schutzniveau für Gesundheit, Sicherheit und die in der EU-Grundrechtecharta verankerten Grundrechte, einschließlich Demokratie, Rechtsstaatlichkeit und Umweltschutz, vor den schädlichen Auswirkungen von KI in der EU zu gewährleisten.

Der EU-Kodex enthält zwei Abschnitte, wovon der erste Regeln für die Kennzeichnung und Erkennung von KI-generierten und KI-manipulierten Inhalten für Anbieter generativer KI-Systeme aufstellt (Art. 50 Abs. 2, 5 KI-VO). Der zweite Abschnitt umfasst Vorgaben für die Kennzeichnung von Deepfakes sowie von KI-generierten und KI-manipulierten Texten für Betreiber von KI-Systemen (Art. 50 Abs. 4, 5 KI-VO).

Abschnitt 1 gilt nur für Unterzeichner des Kodex, soweit sie Anbieter von KI-Systemen sind, die synthetische Audio-, Bild-, Video- oder Textinhalte generieren („generative KI-Systeme“) und in den Anwendungsbereich von Art. 2 und 50 Abs. 2 KI-VO fallen. Anbieter generativer KI-Modelle, die unabhängig von KI-Systemen in Verkehr gebracht werden, sowie Drittanbieter von Kennzeichnungslösungen können auf freiwilliger Basis dem Kodex beitreten, um nachzuweisen, dass ihre Kennzeichnungs- und Erkennungslösungen den Anforderungen von Art. 50 Abs. 2, 5 KI-VO sowie diesem Abschnitt des Kodex entsprechen. Abschnitt 1 enthält die folgenden Regeln:

Verpflichtung 1: Mehrstufige Kennzeichnung von KI-generierten Inhalten

Maßnahme 1.1: Maschinell lesbare Kennzeichnungsverfahren

Teilmaßnahme 1.1.1: Digital signierte Metadaten

Teilmaßnahme 1.1.2: Unwahrnehmbare Wasserzeichen-Techniken, die in den Inhalt eingebettet sind

Teilmaßnahme 1.1.3: Fingerprinting- oder Protokollierungsfunktionen (optionale ergänzende Maßnahme)

Maßnahme 1.2: Nicht-Entfernung maschinenlesbarer Kennzeichnungen

Maßnahme 1.3: Transparenz der Provenienzkette (optional)

Maßnahme 1.4: Optionale Funktionalität für erkennbare Kennzeichnungen (für Deepfakes sowie KI-generierte und -manipulierte veröffentlichte Texte)

Verpflichtung 2: Erkennung der Kennzeichnung von KI-generierten Inhalten

Maßnahme 2.1: Bereitstellung von Erkennungsmechanismen für die aktive Kennzeichnung für Betreiber, Endnutzer und andere Dritte

Maßnahme 2.2: Forensische Erkennungsmechanismen (optionale ergänzende Maßnahme)

Maßnahme 2.3: Klare und leicht zugängliche Offenlegung der Überprüfungs- und Erkennungsergebnisse

Maßnahme 2.4: Förderung der Kompetenz im Umgang mit KI-basierten Kennzeichnungstechnologien und Verifizierung

Verpflichtung 3: Maßnahmen zur Erfüllung der Anforderungen an Kennzeichnungs- und Erkennungsverfahren

Maßnahme 3.1: Wirksamkeit

Maßnahme 3.2: Zuverlässigkeit

Maßnahme 3.3: Robustheit

Maßnahme 3.4: Interoperabilität

Maßnahme 3.5: Weiterentwicklung des Stands der Technik bei der Kennzeichnung und Erkennung

Verpflichtung 4: Prüfung, Verifizierung und Einhaltung

Maßnahme 4.1: Compliance-Rahmenwerk

Maßnahme 4.2: Prüfung, Verifizierung und Überwachung

Maßnahme 4.3: Schulung

Maßnahme 4.4: Zusammenarbeit mit Marktüberwachungsbehörden

Abschnitt 2 gilt ebenfalls nur für Unterzeichner des Kodex. Voraussetzung ist, dass es sich um Betreiber von KI-Systemen handelt, die Deepfakes oder veröffentlichte Texte mit dem Ziel generieren oder manipulieren, die Öffentlichkeit über Angelegenheiten von öffentlichem Interesse zu informieren, die in den Anwendungsbereich von Art. 50 Abs. 4 KI-VO fallen.

Diesbezüglich sieht der Kodex folgende Maßnahmen vor:

Verpflichtung 1: Offenlegung von KI-generierten und manipulierten Deepfakes sowie von veröffentlichten Texten

Maßnahme 1.1: Gestaltungsanforderungen für Symbole, Kennzeichnungen oder Haftungsausschlüsse

Maßnahme 1.2: Anforderungen an die Platzierung von Symbolen, Beschriftungen oder Haftungsausschlüssen

- Echtzeitvideo (verschiedene Formate)
- Nicht-Echtzeit-Video (verschiedene Formate)
- Bild (einzelne Modalität)
- Audio (einzelne Modalität)
- Andere multimodale Inhalte
- Text

Maßnahme 1.3: Optionale Verwendung eines EU-Symbols und Beteiligung an dessen Entwicklung

Verpflichtung 2: Angemessene Einhaltung, Sensibilisierung und Überprüfung

Maßnahme 2.1: Interne Compliance

Maßnahme 2.2: Sensibilisierung und Schulung

Maßnahme 2.3: Überprüfung, Rückmeldung und Zusammenarbeit mit Behörden

Verpflichtung 3: Angemessene Kennzeichnung für künstlerische, kreative und ähnliche Werke

Verpflichtung 4: Menschliche Überprüfung, redaktionelle Kontrolle und Verantwortung in Bezug auf KI-generierte oder manipulierte Textveröffentlichungen

URHEBERRECHTSGESETZ (URHG)

Das Urheberrechtsgesetz (UrhG) ist das deutsche Gesetz zum Schutz geistigen Eigentums an Werken der Literatur, Wissenschaft und Kunst. Es definiert den Schutzumfang (§ 2 UrhG: persönliche geistige Schöpfungen), Dauer und Ausnahmen des Urheberrechts, aber auch verwandte Schutzrechte.

Hinweis:
Mithilfe von KI generierte Inhalte werden regelmäßig nicht als persönliche geistige Schöpfungen eingestuft, sodass an ihnen kein Urheberrecht entsteht, sie also gemeinfrei sind.

Im KI-Kontext ist das UrhG insbesondere auch deshalb relevant, weil es regelt, wer wann welche Inhalte nutzen darf. Das UrhG enthält seit Mitte 2021 mit §§ 44b, 60d UrhG spezielle Schrankenregelungen für das Text- und Data-Mining (TDM) sowie Regeln für GEMA/GVL-Lizenzen im Streaming, die für KI-Anwendungen zu beachten sind.

Ein Urheber ist im Urheberrecht der Erschaffer eines Werks, das im Bereich Literatur, Wissenschaft oder Kunst aufgrund einer persönlichen geistigen Schöpfung entstanden ist.

Es gibt verschiedene Arten von Werken, beispielsweise Texte, Fotos, Grafiken, Musik, Code etc. (vgl. § 2 Abs. 1 UrhG).

Der Urheber hat umfassende Rechte an seinem Werk (Vervielfältigungs-, Verbreitungs-, Bearbeitungsrecht, Urheberpersönlichkeitsrechte).

Der Stil zu zeichnen wird, im Gegensatz zu einem konkreten Bild, nicht durch das Urheberrecht geschützt.

Im Zusammenhang mit der Nutzung von KI sind folgende Fragen besonders praxisrelevant:

- Wer hat die Rechte an Inhalten, die von KI-Systemen erzeugt werden?
- Wie sieht es bei der Überarbeitung von KI-Output durch einen Menschen oder – andersherum formuliert – bei der Überarbeitung von menschlichen Werken durch die KI aus?
- Ist ein bestimmter Stil, zu zeichnen, zu formulieren etc. überhaupt durch das UrhG geschützt?
- Muss KI-generierter oder KI-manipulierter Content als solcher gekennzeichnet werden?
- Wie ändert sich ein Geschäftsmodell, wenn bislang Content erstellt und die Rechte daran gegen Entgelt an Kunden übertragen wurden, jetzt aber KI-Tools für die Arbeit genutzt werden?

Diese und noch einige Fragen mehr müssen zukünftig durch die Gerichte geklärt werden.

Hinweis:
Bei Nutzung von urheberrechtlich geschütztem Material für das KI-Training muss der Urheber zustimmen – es sei denn, es greift eine Ausnahme (z. B. Schrankenregelung für TDM).

VALIDIERUNGSDATEN

Der Begriff „Validierungsdaten" wird in Art. 3 Nr. 30 KI-Verordnung (KI-VO) wie folgt definiert:

„Daten, die zur Evaluation des trainierten KI-Systems und zur Einstellung seiner nicht erlernbaren Parameter und seines Lernprozesses verwendet werden, um unter anderem eine Unter- oder Überanpassung zu vermeiden"

Ein „Validierungsdatensatz" ist daher ein separater Datensatz oder ein Teil des Trainingsdatensatzes mit fester oder variabler Aufteilung (Art. 3 Nr. 31 KI-VO).

Validierungsdaten werden beim KI-Training zur Feinjustierung verwendet. Sie dienen dazu, die Leistung des KI-Modells während des Trainings zu prüfen, ohne

die finalen Testdaten zu verwenden. Im Unterschied zu Testdaten beeinflussen Validierungsdaten direkt den Trainingsprozess (z. B. um sogenanntes Overfitting zu vermeiden).

Hinweis:
Nach Maßgabe von Art. 10 KI-VO haben Anbieter von Hochrisiko-KI-Systemen nicht nur in Bezug auf Testdaten, sondern auch bezüglich der Validierungsdaten bestimmte Pflichten zu befolgen.

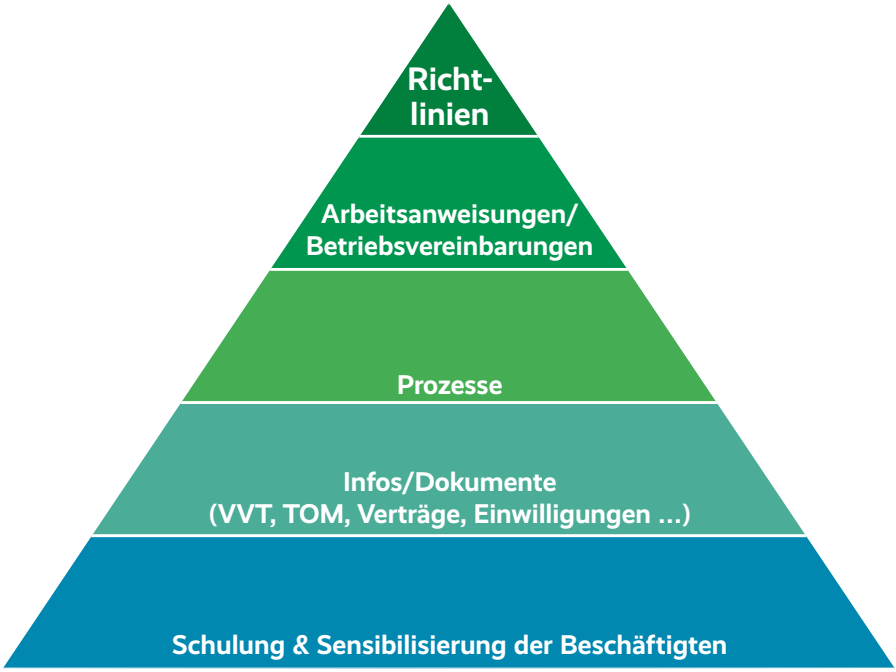
VERARBEITUNGSVERZEICHNIS (VVT)

Das Verzeichnis von Verarbeitungstätigkeiten (VVT), oder kurz: Verarbeitungsverzeichnis, nach Art. 30 Datenschutzgrundverordnung (DSGVO) ist ein internes Register, das jeder Verantwortliche und Auftragsverarbeiter führen muss. Darin sollen alle Datenverarbeitungsaktivitäten aufgelistet und dazu jeweils Zweck, Kategorien von Daten, Kategorien von Betroffenen, Empfänger, Speicherdauer etc. notiert werden.

Aufgrund der Rechenschaftspflicht aus Art. 5 Abs. 2 DSGVO kommt einer sauberen Datenschutzdokumentation eine spezielle Bedeutung zu – auch und gerade beim Einsatz von KI. Zentrales Element ist hierbei das VVT. Dieses muss von jeder verantwortlichen Stelle geführt werden, vom Solo-Selbstständigen über kleine und mittelständische Betriebe (KMU-Bereich) bis hin zum multinationalen Konzern.

Neben der Dokumentationsfunktion kommt dem VVT auch noch die Strukturierung der eigenen Datenverarbeitungsvorgänge zu. Letztlich stellt die Datenschutzdokumentation aber auch nur einen (wenn auch wichtigen) Baustein eines Datenschutz-Management-Systems (DSMS) dar. Ein solches DSMS ist für jedes Unternehmen sowie jede Behörde sinnvoll.

Hinweis:
Die Erstellung und Pflege des VVT sollten in die Datenschutzprozesse der verantwortlichen Stelle eingebaut sein. Auch Unternehmen im KMU-Bereich sollten dazu interne Richtlinien und Prozessbeschreibungen vorhalten, um nicht zuletzt die Aktualität der im VVT enthaltenen Einträge sicherzustellen.



Exemplarische Bestandteile eines DSMS

Hinweis:
Das VVT ist ein rein internes Dokument, welches nur von den Datenschutzaufsichtsbehörden auf Anfrage eingesehen werden kann. Sonstige Dritte haben keinen Anspruch auf Einsichtnahme – auch betroffene Personen nicht.

Im Grunde gibt es nicht ein VVT, sondern sogar zwei. In Art. 30 Abs. 1 DSGVO ist das VVT von Verantwortlichen geregelt und in Art. 30 Abs. 2 DSGVO findet sich ein spezielles, vom Umfang her abgespecktes VVT für Auftragsverarbeiter. So hat ein Unternehmen, das z. B. als IT-Dienstleister für seine Kunden tätig wird, regelmäßig zwei Verarbeitungsverzeichnisse zu führen: eines für die eigenen, internen Prozesse und eines zu allen Kategorien von im Auftrag eines Auftraggebers, also eines Kunden, durchgeführten Datenverarbeitungen.

Das VVT kann man sich als eine Art „Informationszentrale" speziell für den Bereich Datenschutz vorstellen. Art. 30 DSGVO gibt vor, welche Angaben verpflichtend enthalten sein müssen. Leider fehlen im Gesetz jedoch Hinweise dazu, wie grob- oder wie feingliedrig so ein VVT zu sein hat, ob es einen bestimmten Umfang haben muss oder in welchem (Datei-)Format es zu führen ist.

Hinweis:
Es spielt keine Rolle, ob das VVT als handschriftliches Verzeichnis, im Word-, Excel- oder sonstigem Dateiformat oder aber mittels Spezialsoftware geführt wird. Wichtig ist vielmehr, dass zumindest alle gesetzlich geforderten Pflichtangaben gemäß Art. 30 DSGVO enthalten sind und dass das Verzeichnis aus sich heraus verständlich ist.

Nach Art. 30 Abs. 1 DSGVO haben Verantwortliche in ihrem VVT zumindest folgende Angaben aufzunehmen:

- Name und Kontaktdaten des Verantwortlichen
- ggf. Name und Kontaktdaten des gemeinsam Verantwortlichen
- ggf. Name und Kontaktdaten des EU-Vertreters (vgl. Art. 4 Nr. 17 DSGVO)
- ggf. Name und Kontaktdaten des Datenschutzbeauftragten (DSB)
- Zwecke der Verarbeitung
- Kategorien Betroffener
- Kategorien personenbezogener Daten
- Kategorien von Empfängern
- Übermittlung an ein Drittland
- Löschfristen
- allgemeine Beschreibung der technischen und organisatorischen Maßnahmen (TOM) (vgl. Art. 32 DSGVO)

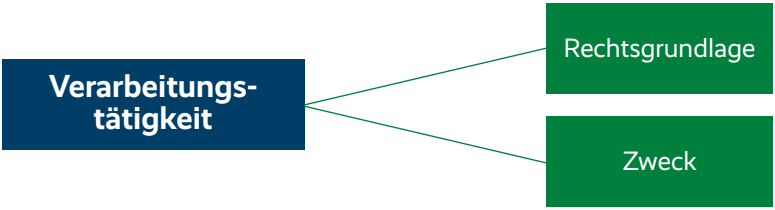
Hinweis:
Im Internet finden sich zahlreiche Vorlagen für ein VVT, die meisten sind sogar kostenfrei nutzbar. So stellen unter anderem das Bayerische Landesamt für Datenschutzaufsicht (https://www.lda.bayern.de/de/muster.html), der Landesdatenschutzbeauftragte Baden-Württemberg (https://www.baden-wuerttemberg.datenschutz.de/praxishilfen/), die Datenschutzkonferenz (https://www.bfdi.bund.de/DE/Fachthemen/Inhalte/Allgemein/Verzeichnis-Verarbeitungstaetigkeiten.html) oder auch Emodeon (https://emodeon.de/datenschutz-vorlagen-und-muster/) solche Vorlagen bereit.

Zusätzlich zu den Art.-30-Pflichtangaben sollten, speziell mit Blick auf den KI-Einsatz, aber auch noch die jeweilige Rechtsgrundlage, eine Risikoeinstufung sowie ggf. die Quelle, aus der Daten stammen, mit ins VVT aufgenommen werden.

Insbesondere die Angabe der Risikoeinstufung ist im Rahmen des VVT absolut sinnvoll. Wenn zu jeder einzelnen Verarbeitungstätigkeit ein Risikowert bzw. ein Eintrag in einer Risikomatrix vorhanden ist, lässt sich auf einen Blick erkennen, wie risikoreich die betreffende Verarbeitung ist und wie hier die dazu passenden „angemessenen" TOM auszusehen haben, ob im Fall einer Datenpanne neben der Meldung an die Aufsichtsbehörden (Art. 33 DSGVO) ggf. auch noch eine an die Betroffenen (Art. 34 DSGVO) erfolgen und ob hier ggf. eine Datenschutz-Folgenabschätzung durchgeführt werden muss.

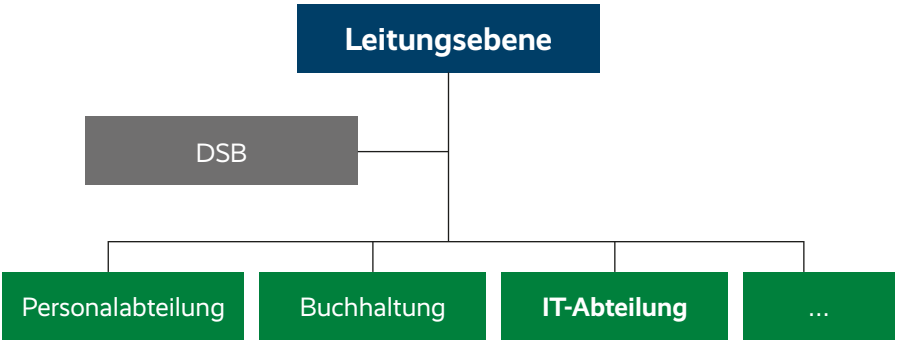
Hinweis:
Ob im VVT oder separat – die Erstellung und Pflege eines „Bestandsverzeichnisses" aller genutzter KI-Tools ist absolut sinnvoll. Denn ein solches Verzeichnis kann dabei helfen, den Überblick zu behalten, die jeweiligen Risiken zu erkennen, die Vertragssituation zu bewerten usw.

Leider regelt die DSGVO nicht, was unter „Verarbeitungstätigkeit" zu verstehen ist und wie fein (oder grob) aufgegliedert diese erfasst werden muss. Letztlich bestimmt sich regelmäßig eine Verarbeitungstätigkeit anhand des ihr zugrunde liegenden Zwecks und der einschlägigen Rechtsgrundlage.



Aus Zweck und Rechtsgrundlage ergibt sich die Verarbeitungstätigkeit.

Eine gute Herangehensweise ist, sich ein Organigramm des eigenen Unternehmens zu erstellen, auf dem die interne Struktur schematisch dargestellt wird.



Beispiel für ein einfaches Organigramm

Ganz grob lassen sich exemplarisch folgende, typische Fachabteilungen bzw. -bereiche identifizieren:

- Leitungsebene
- Personalabteilung
- Buchhaltung
- Marketing
- IT
- Presseabteilung
- Einkauf
- Vertrieb
- Produktion
- Fuhrpark

Diese erste Aufteilung in einzelne Fachbereiche ist für das VVT noch zu grob und daher nicht sinnvoll. Es sollte eine weitere Unterteilung je Fachbereich in die jeweiligen typischen Tätigkeiten erfolgen. Der Fachbereich „Personalabteilung" kann beispielsweise folgende Haupttätigkeiten umfassen:

- Anlage und Führung der Personalakten
- Bewerbermanagement
- Urlaubs- und Abwesenheitsplanung
- Beförderungen/Versetzungen

Hinweis:
Je nach Unternehmensgröße kann man sich auch eventuell an dokumentierten Geschäftsprozessen orientieren. Denn insbesondere im Vertrieb, Marketing, IT und Personalabteilung sind die Aufgaben häufig über Geschäftsprozesse standardisiert. Die DSGVO lässt es zu, dass jede verantwortliche Stelle ihre eigene Herangehensweise wählt, solange die gesetzlichen Vorgaben umgesetzt werden.

Diese einzelnen Prozesse müssen dann „nur" noch mit den gesetzlichen Pflichtangaben versehen werden.

Hinweis:
Letztlich müssen im VVT alle Verarbeitungen aufgeführt werden, die im geschäftlichen bzw. behördlichen Arbeitsalltag tatsächlich durchgeführt und bei denen personenbezogene Daten verarbeitet werden.

Auftragsverarbeiter haben außerdem ein zusätzliches VVT zu führen, nämlich je ein Verzeichnis zu allen Kategorien von im Auftrag eines Verantwortlichen durchgeführten Verarbeitungen. Darin sind gemäß Art. 30 Abs. 2 DSGVO die folgenden Mindestangaben zu dokumentieren:

- Name und Kontaktdaten des Auftragsverarbeiters
- Name und Kontaktdaten jedes Verantwortlichen, in dessen Auftrag der Auftragsverarbeiter tätig ist
- ggf. Name und Kontaktdaten des EU-Vertreters des Verantwortlichen oder des Auftragsverarbeiters
- ggf. Name und Kontaktdaten und eines etwaigen Datenschutzbeauftragten
- Kategorien von Verarbeitungen, die im Auftrag des Verantwortlichen durchgeführt werden
- ggf. Übermittlungen von personenbezogenen Daten an ein Drittland
- allgemeine Beschreibung der TOM gemäß Art. 32 DSGVO

Hinweis:
Art, Umfang und Inhalte können sich dabei an dem „großen" Haupt-VVT nach Art. 30 Abs. 1 DSGVO orientieren.

Die folgenden, exemplarisch aufgelisteten Unterlagen sollten, sofern möglich und sinnvoll, das eigene VVT ergänzen:

- Übersicht Hardware
- Übersicht Software
- Übersicht Fuhrpark
- Übersicht Mobile Device Management
- Netzwerkdiagramm
- Organigramm (Unternehmensstruktur)
- Schlüsselliste
- Arbeitsanweisung(en)
- Interne Richtlinie(n) mit Bezug zum Datenschutz (z. B. Clean Desk Policy, Home-Office-Vorgaben, KI-Nutzung)
- Betriebsvereinbarung(en)
- Nutzerrechte-/Rollenkonzept
- Gebäudeplan/Grundriss
- Lösch-Konzept
- DSB-Benennungsurkunde
- Passwort-Richtlinie
- Back-up-Konzept
- Prozessbeschreibungen
- Übersicht Dienstleister/Datenflüsse
- Auftragsverarbeitungsverträge/Vereinbarungen zur gemeinsamen Verantwortlichkeit
- Notfallpläne
- Schulungsunterlagen Datenschutz, Informations- und IT-Sicherheit
- Schulungsnachweise Beschäftigte
- DSB-Tätigkeitsberichte
- Exemplarischer Arbeitsvertrag
- Exemplarische Verpflichtung zur Vertraulichkeit
- Datenschutzerklärungen z. B. für Bewerber, Beschäftigte, Kunden, Website etc.

VERBOTENE KI-PRAKTIKEN

Die KI-Verordnung (KI-VO) listet in ihrem Artikel 5 bestimmte KI-Praktiken auf, die entweder menschenfeindlich, manipulativ oder unsicher und deshalb mit einem untragbaren Risiko verbunden sind. Derartige Praktiken sind generell untersagt – ob sie auch ohne KI-Einsatz ggf. aufgrund anderer gesetzlicher Vorgaben verboten sind, das klärt die KI-VO nicht. Als Produktregulierung stellt die KI-VO einzig und allein auf den KI-Kontext ab.

Hinweis:
Das Verbot dient dem Schutz der Grundrechte und soll unerwünschte Extremszenarien verhindern.

Zu den verbotenen KI-Praktiken (also KI mit unannehmbarem Risiko) zählen Art. 5 Abs. 1 lit. a) bis h) KI-VO folgende:

- unterschwellige Beeinflussung/manipulative Techniken
- Ausnutzung der Schwäche oder Schutzbedürftigkeit bestimmter Personen
- Schlechterstellung durch Bewertung des sozialen Verhaltens (sogenanntes „Social Scoring“)

- Risikobeurteilung von natürlichen Personen (z. B. „Predictive Policing“)
- Datenbanken zur Gesichtserkennung
- Ableitung von Emotionen natürlicher Personen in Büro, Schule, Uni etc.
- biometrische Kategorisierung
- biometrische Echtzeit-Fernidentifizierungssysteme in öffentlichen Räumen zur Strafverfolgung

Hinweis:
Durch den geplanten „Digital Omnibus on AI“ will die EU weitere Verbotstatbestände einführen. Dabei handelt es sich um das Verbot von KI zur Erstellung oder Manipulation von nicht einvernehmlichem, realistischem intimen Material („nudification“) sowie um das Verbot von Systemen, die Material über sexuellen Kindesmissbrauch generieren oder verändern.

Diese stichwortartige Aufzählung von verbotenen KI-Praktiken hilft allerdings nur für eine erste Orientierung. Denn dieses Thema wird zwar nur in einer einzigen Norm behandelt (Art. 5 KI-VO), diese hat es aber in sich. Das Gesetz enthält in den einzelnen Regelungen jeweils bestimmte Voraussetzungen, Ausnahmen und zum Teil auch Gegenausnahmen. So regelt beispielsweise Art. 5 Abs. 1 lit. c) KI-VO:

„Folgende Praktiken im KI-Bereich sind verboten: […]

c) das Inverkehrbringen, die Inbetriebnahme oder die Verwendung von KI-Systemen zur Bewertung oder Einstufung von natürlichen Personen oder Gruppen von Personen über einen bestimmten Zeitraum auf der Grundlage ihres sozialen Verhaltens oder bekannter, abgeleiteter oder vorhergesagter persönlicher Eigenschaften oder Persönlichkeitsmerkmale, wobei die soziale Bewertung zu einem oder beiden der folgenden Ergebnisse führt:

i) Schlechterstellung oder Benachteiligung bestimmter natürlicher Personen oder Gruppen von Personen in sozialen Zusammenhängen, die in keinem Zusammenhang zu den Umständen stehen, unter denen die Daten ursprünglich erzeugt oder erhoben wurden;

ii) Schlechterstellung oder Benachteiligung bestimmter natürlicher Personen oder Gruppen von Personen in einer Weise, die im Hinblick auf ihr soziales Verhalten oder dessen Tragweite ungerechtfertigt oder unverhältnismäßig ist“

Dieses Beispiel zeigt sehr deutlich, dass nicht alle Praktiken der Bewertung oder Einstufung von Menschen verboten sein sollen, sondern lediglich solche, die auf Grundlage des sozialen Verhaltens oder Ähnlichem erfolgen, dies zudem über einen bestimmten Zeitraum. Voraussetzung ist allerdings, dass die Bewertung oder Einstufung zu jedenfalls einer von zwei möglichen Schlechterstellungen führt.

Hinweis:
Die sorgfältige Prüfung von Art. 5 KI-VO entscheidet über „Wohl und Wehe", also darüber, ob ein KI-System auch nach dem 02.02.2025 weiter bzw. neu entwickelt, vertrieben oder genutzt werden darf. Die zu erwartenden gerichtlichen Entscheidungen müssen abgewartet werden, um Klarheit hinsichtlich verschiedener Details zu erlangen. Gleichwohl sollte eine intensive Prüfung von Art. 5 KI-VO, sofern noch nicht geschehen, so bald wie möglich erfolgen. Diese muss auch bei jeder Einführung neuer KI-Technologien bzw. Einsatzszenarien neu angestoßen sowie prozessual verankert und beschrieben werden.

Art. 5 Abs. 1 lit. h) KI-VO enthält neben bestimmten Voraussetzungen auch noch einzelne Ausnahmen:

„Folgende Praktiken im KI-Bereich sind verboten: [...]

h) die Verwendung biometrischer Echtzeit-Fernidentifizierungssysteme in öffentlich zugänglichen Räumen zu Strafverfolgungszwecken, außer wenn und insoweit dies im Hinblick auf eines der folgenden Ziele unbedingt erforderlich ist:

i) gezielte Suche nach bestimmten Opfern von Entführung, Menschenhandel oder sexueller Ausbeutung sowie die Suche nach vermissten Personen;

ii) Abwenden einer konkreten, erheblichen und unmittelbaren Gefahr für das Leben oder die körperliche Unversehrtheit natürlicher Personen oder einer tatsächlichen und bestehenden oder tatsächlichen und vorhersehbaren Gefahr eines Terroranschlags;

iii) Aufspüren oder Identifizieren einer Person, die der Begehung einer Straftat verdächtigt wird, zum Zwecke der Durchführung von strafrechtlichen Ermittlungen oder von Strafverfahren oder der Vollstreckung einer Strafe für die in Anhang II aufgeführten Straftaten, die in dem betreffenden Mitgliedstaat nach dessen Recht mit einer Freiheitsstrafe oder einer freiheitsentziehenden Maßregel der Sicherung im Höchstmaß von mindestens vier Jahren bedroht ist."

Die Verwendung biometrischer Echtzeit-Fernidentifizierungssysteme soll also grundsätzlich verboten sein, es sei denn, einer der angeführten Ausnahmefälle liegt vor (z. B. Suche nach Entführungsopfern oder Abwendung eines Terror-

anschlags). Zu den hier in Ziffer iii) und Anhang II KI-VO genannten Straftaten, aufgrund derer die potenziellen Täter mittels KI ausnahmsweise doch ermittelt werden dürfen, zählen unter anderem Terrorismus, Menschenhandel und Mord, aber auch Umweltkriminalität. Es geht hierbei also in erster Linie um gravierende Delikte, bei denen ausnahmsweise doch KI-gestützte biometrische Echtzeit-Fernidentifizierungssysteme in öffentlich zugänglichen Räumen zu Strafverfolgungszwecken zum Einsatz kommen dürfen.

Liste der Straftaten aus Anhang II KI-VO

Die EU-Kommission hat im Februar 2025 Leitlinien zu verbotenen Praktiken der künstlichen Intelligenz veröffentlicht. Darin finden sich diverse Beispiele für die in Art. 5 KI-VO beschriebenen Praktiken:

1. **Unterschwellige Beeinflussung bzw. schädliche Manipulation und Täuschung** (Art. 5 Abs. 1 lit. a) KI-VO)

➤ Ein KI-gestützter Chatbot, der sich mit synthetischer Stimme als Freund oder Verwandter ausgibt, um Betrug zu begehen.

➤ Ein KI-System, das unterschwellige visuelle Botschaften einblendet, die zu schnell sind, um bewusst wahrgenommen zu werden, aber das Verhalten beeinflussen.

- Ein KI-System, das personalisierte Manipulationstechniken einsetzt, um Nutzer zu riskanten Entscheidungen zu bewegen, wie beispielsweise exzessives Spielen.
- Ein KI-System, das unterschwellige Techniken einsetzt, um Kaufentscheidungen zu beeinflussen.

2. **Schädliche Ausnutzung der Schwachstellen von Menschen** (Art. 5 Abs. 1 lit. b) KI-VO)
   - Ein KI-gesteuertes Spielzeug, das Kinder dazu ermutigt, gefährliche Aufgaben zu erfüllen, wie das Klettern auf Möbel.
   - Ein KI-System, das ältere Menschen mit personalisierten Betrugsangeboten anspricht, indem es ihre eingeschränkten kognitiven Fähigkeiten ausnutzt.
   - Ein KI-System, das gezielt Werbung für räuberische Finanzprodukte an einkommensschwache Personen richtet.
3. **Bewertung und Schlechterstellung von Personen auf der Grundlage ihres sozialen Verhaltens** (sogenanntes Social Scoring) (Art. 5 Abs. 1 lit. c) KI-VO)
   - Eine Sozialhilfebehörde verwendet ein KI-System, das auf sozialen Gewohnheiten oder Internetverbindungen basiert, um Empfänger für Betrugsprüfungen auszuwählen.
   - Eine Stadtverwaltung erstellt eine Vertrauenswürdigkeitsbewertung von Einwohnern, die zu sozialer Ausgrenzung führt, z. B. durch den Entzug öffentlicher Leistungen.
   - Ein KI-System, das Bürger auf der Grundlage ihres Sozialverhaltens in sozialen Medien bewertet und ihnen gezielte politische Botschaften sendet.
   - Eine Steuerbehörde, die ein KI-System zur Auswahl von Steuererklärungen verwendet, basierend auf nicht verwandten sozialen Daten.
4. **Individuelle Risikobewertung und Vorhersage von Straftaten** (z. B. „Predictive Policing“) (Art. 5 Abs. 1 lit. d) KI-VO)
   - Ein KI-System, das das Risiko einer Person, eine Straftat zu begehen, ausschließlich auf der Grundlage von Alter, Nationalität und Adresse bewertet.
   - Ein KI-System, das Kinder auf der Grundlage ihrer Beziehungen zu anderen Personen als potenzielle Straftäter einstuft.
   - Ein Steuerbehörden-KI-System, das Steuerbetrug ausschließlich auf der Grundlage von Profilen und Persönlichkeitsmerkmalen vorhersagt.

5. **Ungezieltes Scraping zur Entwicklung von Datenbanken zur Gesichtserkennung** (Art. 5 Abs. 1 lit. e) KI-VO)

- Ein Unternehmen, das Gesichtsbilder aus sozialen Medien wie Facebook und Youtube sammelt, um eine Gesichtserkennungsdatenbank zu erstellen.
- Ein KI-System, das Aufnahmen aus Webcams etc. aus öffentlichen Räumen sammelt, um biometrische Datenbanken zu erweitern.

6. **Erkennung bzw. Ableitung von Emotionen in Bildungseinrichtungen oder am Arbeitsplatz** (Art. 5 Abs. 1 lit. f) KI-VO)

- Ein KI-System, das die Emotionen von Mitarbeitern in einem Callcenter überwacht, um ihre Arbeitsleistung zu bewerten.
- Ein KI-System, das die Emotionen von Schülern während Onlineprüfungen analysiert, um ihre Aufmerksamkeit zu überwachen.
- Ein KI-System, das die Emotionen von Kunden in einem Supermarkt analysiert, um gezielte Werbung zu schalten.
- Ein KI-System, das Emotionen von Schülern in einer Bildungseinrichtung erkennt, um deren Engagement zu bewerten.

7. **Biometrische Kategorisierung** (Art. 5 Abs. 1 lit. g) KI-VO)

- Ein KI-System, das Personen anhand ihrer biometrischen Daten ihrer ethnischen Zugehörigkeit zuordnet.
- Ein KI-System, das aus biometrischen Daten Rückschlüsse auf die sexuelle Orientierung einer Person zieht.
- Ein KI-System, das Personen anhand von Gesichtszügen politischen Meinungen zuordnet.

8. **Biometrische Echtzeit-Fernidentifizierungssysteme in öffentlichen Räumen zu Strafverfolgungszwecken** (Art. 5 Abs. 1 lit. h) KI-VO)

- Ein Echtzeit-System wird eingesetzt, um Personen mit ausstehenden Haftbefehlen bei einem Festival zu identifizieren.
- Ein KI-System, das in einem Park zur Identifizierung von Personen eingesetzt wird, die eine Bedrohung darstellen könnten.
- Ein KI-System der Polizei zur Identifizierung von Ladendieben und zum Abgleich ihrer Gesichtsbilder mit Kriminalitätsdatenbanken.

WESENTLICHE VERÄNDERUNG

Der Begriff „wesentliche Veränderung“ wird in Art. 3 Nr. 23 KI-Verordnung (KI-VO) wie folgt definiert:

„eine Veränderung eines KI-Systems nach dessen Inverkehrbringen oder Inbetriebnahme, die in der vom Anbieter durchgeführten ursprünglichen Konformitätsbewertung nicht vorgesehen oder geplant war und durch die die Konformität des KI-Systems mit den Anforderungen in Kapitel III Abschnitt 2 beeinträchtigt wird oder die zu einer Änderung der Zweckbestimmung führt, für die das KI-System bewertet wurde“

Es geht folglich um die gravierende Änderung eines KI-Systems nach seinem Inverkehrbringen oder seiner Inbetriebnahme, die in der ursprünglichen Konformitätsbewertung des Anbieters nicht vorgesehen oder geplant war. Sofern dadurch entweder die Konformität mit den Anforderungen des Kapitels III Abschnitt 2 (Anforderungen an Hochrisiko-KI-Systeme, Art. 8 ff. KI-VO) beeinträchtigt wird oder es zu einer Änderung der Zweckbestimmung kommt, wird die Änderung als „wesentlich“ eingestuft. Maßgeblich ist also, ob durch die Änderung die ursprünglich geprüfte Risikolage oder Zweckbestimmung so verändert wird, dass die damalige Konformitätsbewertung nicht mehr trägt.

Hinweis:
In der Praxis kann dies also beispielsweise das Nachrüsten neuer Funktionen (z. B. zusätzliche biometrische Erkennungsmerkmale), das Finetuning eines Hochrisiko-KI-Systems in Bezug auf neue, kritische Datensätze oder eine Zweckausweitung von einem rein unterstützenden System hin zu einem System mit automatisierter Entscheidungskompetenz betreffen. Erfolgt eine solche wesentliche Veränderung, kann der verändernde Akteur selbst zum Anbieter im Sinne der KI-VO mit entsprechender Pflicht zur (erneuten) Konformitätsbewertung, CE-Kennzeichnung, technischer Dokumentation und laufendem Risikomanagement werden (Art. 25 KI-VO).

Der Begriff der wesentlichen Änderung nach Art. 3 Nr. 23 KI-VO ist der Dreh- und Angelpunkt für die Aufrechterhaltung der Konformität eines KI-Systems. Er markiert die Grenze, ab der ein bestehendes System rechtlich als „neu“ eingestuft wird und eine erneute Konformitätsbewertung erforderlich macht. Entscheidend ist hierbei der Aspekt der Vorhersehbarkeit:

- **Geplante Iterationen:** Wenn ein Anbieter bereits im Rahmen seines Qualitätsmanagementsystems dokumentiert hat, wie sich das KI-Modell durch lernende Algorithmen weiterentwickeln wird, stellt diese geplante Anpassung in der Regel keine wesentliche Änderung dar.
- **Ungeplante Modifikationen:** Ein Wechsel der Hardware-Plattform, die Integration neuer Funktionalitäten oder der Einsatz in einem sicherheitskritischen Umfeld, das ursprünglich nicht vorgesehen war, lösen hingegen regelmäßig die Pflicht zur Neuzertifizierung aus.

Besonders problematisch ist diese Thematik bei agentischen Systemen, die autonom Werkzeuge auswählen und nutzen. Da der Anbieter nicht komplett überschauen kann, welche externen Schnittstellen oder Tools ein KI-Agent aufrufen wird, ist eine „Planung" im Sinne der KI-VO strukturell kaum möglich.

ZWECKBESTIMMUNG

Der Begriff „Zweckbestimmung" wird in Art. 3 Nr. 12 KI-Verordnung (KI-VO) folgendermaßen definiert:

„die Verwendung, für die ein KI-System laut Anbieter bestimmt ist, einschließlich der besonderen Umstände und Bedingungen für die Verwendung, entsprechend den vom Anbieter bereitgestellten Informationen in den Betriebsanleitungen, im Werbe- oder Verkaufsmaterial und in diesbezüglichen Erklärungen sowie in der technischen Dokumentation"

Der Gesetzgeber stellt hier also auf die vom Anbieter definierte Verwendung eines KI-Systems ab. Es geht darum, wofür das jeweilige KI-System ursprünglich konzipiert wurde, was auch besondere Einsatzumstände und Bedingungen umfasst.

Hinweis:
Beispielsweise kann die Zweckbestimmung eines KI-Chatbots das Ermöglichen von Kundensupport-Chat via Texteingabe sein. Der Anbieter muss diese Zweckbestimmung klar und deutlich, also in der Betriebsanleitung, im Werbematerial, in den technischen Unterlagen etc., dokumentieren.

Für die Regulierung ist die Zweckbestimmung wichtig, weil sowohl Risikobewertung als auch Zulassung darauf aufbauen. Ein Hochrisiko-KI-System ist nur dann gesetzlich ein solches, wenn es so verwendet wird, wie es spezifiziert wurde (Art. 6 KI-VO). Ändert sich der Zweck, muss das gesamte KI-System neu bewertet werden.

skillsforwork | manageforwork

Mitarbeitende wirksam schulen. Datenschutzdokumentation vereinfachen.

Weniger Aufwand und mehr Sicherheit – mit unseren Tools, die Datenschutzprozesse wirklich entlasten. Einfacher, digitaler und schneller.

Jetzt kostenfreie Demo sichern

www.skillsforwork.de
www.manageforwork.de

IT- & INFORMATIONS-SICHERHEIT UPDATE

Ihr digitaler Praxisratgeber für mehr Schutz Ihrer betrieblichen Informationen

Schnelles Filtern der News, die Sie brauchen

Aus Fehlern anderer lernen

Praxisnahe (Video-)Anleitungen

Audit-Prüflisten

Schulungsmaterial

Interpretation der Gesetze und Richtlinien

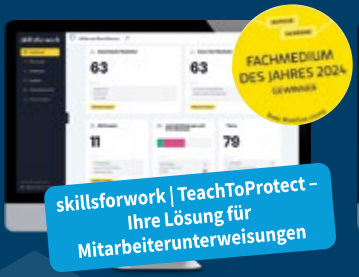
Darum sollten Sie nicht auf das IT- & Informationssicherheit-Update verzichten:

- Erhalten Sie alle 2 Wochen News, Praxistipps und Rechtsempfehlungen
- Sicherheitsmaßnahmen messbar machen, dank interaktiver Checklisten
- Arbeitshilfen im Onlinebereich sparen Zeit bei Schulungen, Richtlinien & Co.

Testen Sie das E-Magazin für mehr IT- und Informationssicherheit 1 Monat GRATIS

http://bit.ly/IT-Info-Update

Lernen Sie auch die Angebote von SafetyXperts kennen!



skillsforwork | TeachToProtect – Ihre Lösung für Mitarbeiterunterweisungen

safety@office, die Unterstützung speziell für Bürobetriebe

Ihr Arbeitsschutz-manager für die Gefähr-dungsbeurteilung

Testen Sie jetzt kostenlos weitere Lösungen, die Ihren Arbeitsalltag erleichtern: safetyxperts.de/shop


Geben Sie’s zu,
googeln hat
nicht geholfen ...
... aber in unserem Onlinebereich
finden Sie die Antwort!
privacyxperts.de
PRIVACYXPERTS

Impressum

PrivacyXperts – ein Unternehmensbereich des VNR Verlags für die Deutsche Wirtschaft AG,
Theodor-Heuss-Str. 2–4, 53095 Bonn
Handelsregister: HRB 8165
Registergericht: Amtsgericht Bonn vertreten durch den Vorstand: Richard Rentrop
Umsatzsteuer-Identifikationsnummer gemäß § 27a Umsatzsteuergesetz: DE 812639372
Telefon: 02 28 / 9 55 01 60
Fax: 02 28 / 3 69 64 80 (bei Rückfragen bitte Kundennummer angeben)
Vorstand: Richard Rentrop, Bonn
Internet: www.privacyxperts.de
E-Mail: kundendienst@privacyxperts.de
Herausgeber und redaktionell Verantwortlicher: Michael Jodda (Adresse siehe Verlag)
Autor: Michael Rohrlich, Würselen
Produktmanagement: Franziska Rohrbach, Bonn
Herstellungsleitung: Sebastian Gerber, Bonn
Satz & Layout: Deinzer Grafik, Gartow
Druck: DCM Druck Center Meckenheim GmbH, Werner-von-Siemens-Str. 13,
53340 Meckenheim
Titelbild: KI-generiert von HelgaArina – stock.adobe.com

Im Interesse der Lesbarkeit verzichten wir in unseren Publikationen auf geschlechtsbezogene Formulierungen. Selbstverständlich sind immer alle Geschlechterformen gemeint, auch wenn explizit nur eines der Geschlechter angesprochen wird.

ISBN: 978-3-8125-3992-0

30 x 13 mm **35 x 13 mm**

PRIVACYXPERTS

PX-EMF-Komp-26/26

www.privacyxperts.de