Unterabteilung Europa
Fachbereich Europa

Deutscher Bundestag

Infobrief

Zu rechtlichen Vorgaben der Verordnung über Künstliche Intelligenz für den Einsatz von KI in Behörden der EU-Mitgliedstaaten

Dr. Kristina Müller, Regina Wigand, LL.M. (LSE)

© 2025 Deutscher Bundestag

EU 6 - 3010 - 032/25

Zu rechtlichen Vorgaben der Verordnung über Künstliche Intelligenz für den Einsatz von KI in Behörden der EU-Mitgliedstaaten

Verfasser/in:	RRn Dr. Kristina Müller; Regina Wigand, LL.M. (LSE)
Aktenzeichen:	EU 6 - 3010 - 032/25
Abschluss der Arbeit:	7. Juli 2025
Fachbereich:	EU 6: Fachbereich Europa

Der Fachbereich Europa der Unterabteilung Europa unterstützt die Mitglieder des Deutschen Bundestagesbei ihrer mandatsbezogenen Tätigkeit. Die Arbeiten geben nicht die Auffassung des Deutschen Bundestages, eines seiner Organe oder der Bundestagsverwaltung wieder. Vielmehr liegen sie in der fachlichen Verantwortung der Verfasserinnen und Verfasser sowie der Fachbereichsleitung.

Inhaltsverzeichnis

1. Einleitung 5

2. Fragen im Zusammenhang mit der Anbieter- und Betreibereigenschaft 8
2.1. Entwickeln lassen und Einkaufen von KI-Systemen 8
2.1.1. KI-Systeme 9
2.1.2. Entwickeln lassen oder einkaufen – Abgrenzung zwischen Anbieter- und Betreiberrolle 9
2.2. Entwickeln (lassen) von KI-Modellen mit allgemeinem Verwendungszweck 11
2.2.1. KI-Modelle mit allgemeinem Verwendungszweck 11
2.2.2. Anbietereigenschaft hinsichtlich GPAI-Modellen: Inverkehrbringen 14
2.2.3. Anbietereigenschaft hinsichtlich GPAI-Modellen: Fine-Tuning 15
2.2.3.1. Verfeinern von GPAI-Modellen 16
2.2.3.2. Verfeinern von GPAI-Modellen mit systemischem Risiko 17
2.2.4. Vorgaben im Zusammenhang mit Trainingsdaten 18
2.2.4.1. Urheberrechtstrategie gemäß Art. 53 Abs. 1 Buchst. c KI-VO 18
2.2.4.2. Exkurs: Haftungsrisiken bezüglich fehler- oder mangelhafter Trainingsdaten 20

3. Registrierungspflichten für Hochrisiko-KI-Systeme 21
3.1. Hochrisiko-Anwendungen 21
3.2. Registrierung in der EU-Datenbank 24
3.3. Registrierung in einer nationalen Datenbank 25

4. Dokumentations- und Auskunftspflichten, Kompetenzen der Überwachungsbehörden nach der KI-VO 25
4.1. Anbieter von Hochrisiko-KI-Systemen 25
4.1.1. Pflichten hinsichtlich der Einstufung als nicht hochriskant 25
4.1.2. Pflichten hinsichtlich der KI-VO-Konformität von HRKS 26
4.2. Betreiber von Hochrisiko-KI-Systemen 28
4.3. Anbieter von GPAI-Modellen 28
4.3.1. Pflichten für Anbieter von GPAI-Modellen aus Art. 53 Abs. 1 KI-VO 29
4.3.2. Pflichten für Anbieter von GPAI-Modellen mit systemischem Risiko aus Art. 55 Abs. 1 KI-VO 31
4.3.3. Sonstiges zur Pflichterfüllung und Auskunftspflichten 31
4.4. Darüber hinaus: Umfassende Dokumentation der Risikoeinstufung? 32

5. Transparenzpflichten hinsichtlich des Outputs bzw. der Interaktion von KI-Anwendungen mit dem Menschen 33
5.1. Kennzeichnungspflichten für Anbieter von KI-Systemen, die für die direkte Interaktion mit natürlichen Personen bestimmt sind (Abs. 1) 34

5.2. Kennzeichnungspflichten für Anbieter von KI-Systemen, die synthetische Audio-, Bild-, Video- oder Textinhalte erzeugen oder manipulieren (Abs. 2) 35
5.3. Kennzeichnungspflichten für Betreiber von KI-Systemen zur Emotionserkennung oder biometrischen Kategorisierung (Abs. 3) 36
5.4. Kennzeichnungspflichten von Betreibern für Deepfakes (Abs. 4 UAbs. 1) 36
5.5. Kennzeichnungspflichten von Betreibern hinsichtlich künstlich erzeugter oder manipulierter Texte zur Information über Angelegenheiten öffentlichen Interesses (Abs. 4 UAbs. 2) 37
5.6. Form der Kennzeichnung und Konkretisierung durch Praxisleitfäden (Abs. 5, 8) 38
5.7. Verhältnis zu sonstigen Kennzeichnungs- bzw. Transparenzpflichten (Abs. 6) 39

6. Kompetenzbildung gemäß Art. 4 KI-VO 40
6.1. Pflicht zur Herstellung ausreichender KI-Kompetenz 40
6.2. Differenzierung nach Anwender, Kontext und Betroffenen 41
6.3. Zur Frage konkreter Lerninhalte und Lernformate 44
6.3.1. Mindestanforderungen laut den FAQ der Kommission zu Art. 4 KI-VO 44
6.3.2. Einzelaspekte in den FAQ der Kommission zu Art. 4 KI-VO 45
6.4. Best Practices? 46
6.4.1. Living Repository of AI Literacy Practices 46
6.4.2. KI-Strategie der Kommission 47
6.4.3. Ansätze im Schrifttum 48
6.5. Dokumentation von Kompetenzbildungsmaßnahmen? 49

7. Compliance-Management: KI-Beauftragter und KI-Governance 50
7.1. KI-Beauftragter 50
7.2. KI-Governance 51

8. Beispiel: Einsatz generativer KI-Systeme mit allgemeinem Verwendungszweck 55
8.1. Verbotene Praktiken: Untersagung 55
8.2. Hochrisiko-Nutzung? 57
8.2.1. Ausschluss der Nutzung im Hochrisiko-Bereich 57
8.2.2. Nutzung im Hochrisiko-Bereich 57
8.3. Kennzeichnung und Kompetenzbildung 58
8.4. Sonstige Aspekte 58

1. Einleitung

Die rasante Entwicklung und Verbreitung Künstlicher Intelligenz (KI) macht vor der öffentlichen Verwaltung nicht Halt: KI bietet weitreichende Möglichkeiten, **Prozesse zu optimieren, zu modernisieren und zu beschleunigen**. Gleichzeitig entstehen neue Herausforderungen, insbesondere im Hinblick auf einen verantwortungsvollen und rechtskonformen Einsatz von KI.

Dieser Infobrief behandelt rechtliche Aspekte, die für **Behörden der EU-Mitgliedstaaten** gemäß der **Verordnung über Künstliche Intelligenz (KI-VO)**[1] der EU bei der Einführung und Nutzung von KI-Anwendungen relevant sein können.

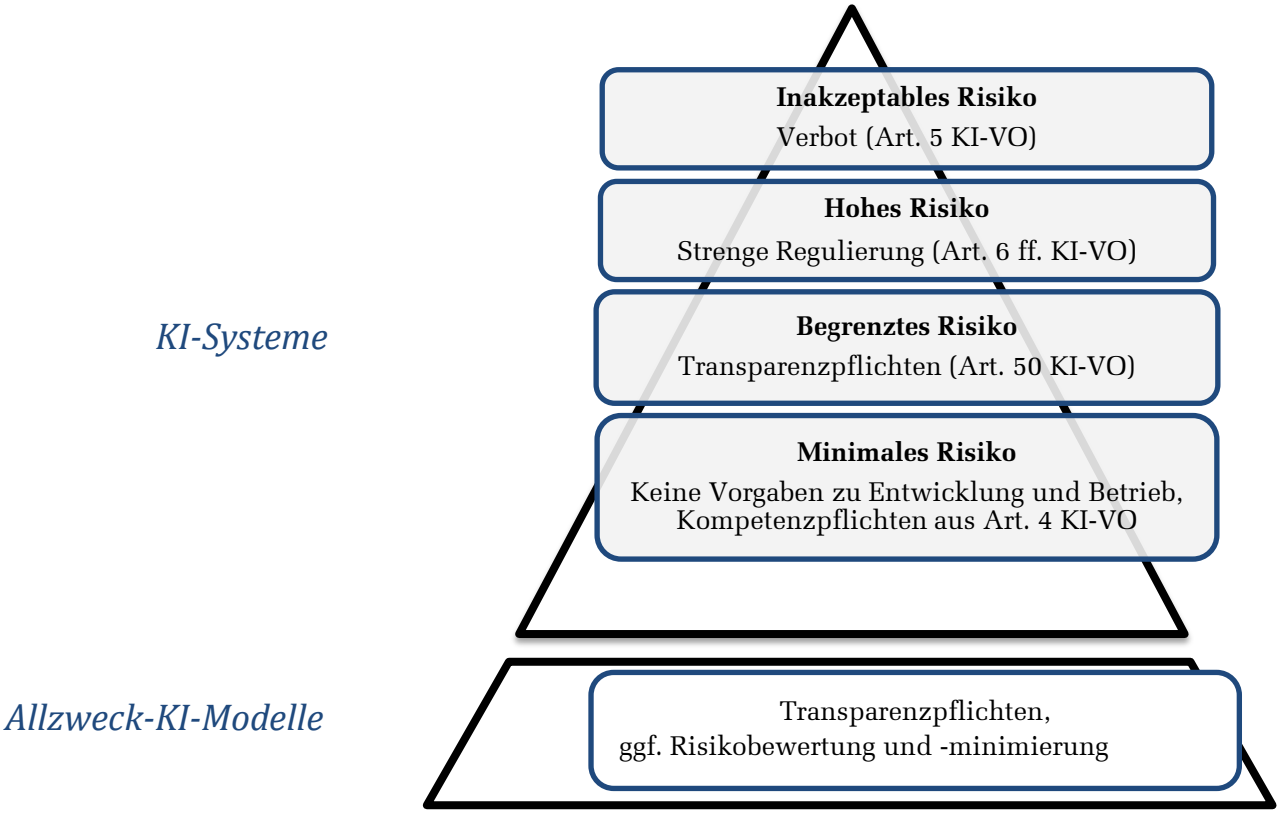
Behandelt werden Fragestellungen im Zusammenhang mit der **Anbieter- oder Betreibereigenschaft** von Behörden (Ziff. 2.), **Registrierungspflichten** für KI-Systeme (Ziff. 3.) sowie sonstigen **Dokumentations- und Transparenzpflichten** (Ziff. 4., 5.). Der Infobrief geht auf die Pflichten zur **Kompetenzbildung** im KI-Bereich (Ziff. 6.) und auf die Frage ein, ob Organisationsstrukturen für ein **Compliance-Management** geschaffen werden sollten (Ziff. 7). Abschließend werden Maßnahmen dargestellt, die Behörden bei der Einführung eines **generativen Allzweck-KI-Systems** wie **ChatGPT, Claude oder Gemini** beachten sollten (Ziff. 8.).

Die KI-VO schafft einen Rechtsrahmen, der den Schutz der Grundrechte und die Sicherheit von KI-Anwendungen gewährleisten und gleichzeitig Innovation fördern soll. Mit Blick auf **KI-Systeme** verfolgt die KI-VO einen **risikobasierten Ansatz**, der Anwendungen in vier Risikokategorien einteilt, an die unterschiedlich strenge Rechtsfolgen geknüpft sind, vgl. Erwägungsgrund (ErwG) 26 KI-VO. Weitere Regelungen beziehen sich auf bestimmte **KI-Modelle**.[2]

---

1 Verordnung (EU) 2024/1689 des Europäischen Parlaments und des Rates vom 13. Juni 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, ABl. L 2024/1689, 12. Juli 2024.

2 S. näher Ziff. 2.1.1., 2.2.1. zur Differenzierung zwischen KI-Systemen i. S. v. Art. 3 Nr. 1 KI-VO und Allzweck-KI-Modellen i. S. v. Art. 3 Nr. 63 KI-VO.



Systematik: Risikobasierter Ansatz nach der KI-VO[3]

Der KI-VO liegt ein **horizontaler Regelungsansatz** zugrunde, weshalb sich ihre sektorübergreifenden Regelungen grundsätzlich gleichermaßen auf private und **staatliche Akteure** beziehen.[4] Behörden können insbesondere als Anbieter i. S. v. Art. 3 Nr. 3 KI-VO und Betreiber i. S. v. Art. 3 Nr. 4 KI-VO von KI-Anwendungen verpflichtet sein.[5] Für die Behörden der Mitgliedstaaten bedeutet dies, dass bei der Implementierung und Nutzung von KI-Technologien die Vorgaben der KI-VO zu durchdringen und zu beachten sind.

3 Transparenzpflichten nach Art. 50 KI-VO und Pflichten bezüglich Hochrisiko-KI-Systemen können nebeneinander bestehen.

4 *Guckelberger*, Hochrisiko-KI-Systeme in der Verwaltung, DÖV 2025, S. 45 (46).

5 S. Ziff. 2.

Die Darstellung beschränkt sich auf die **KI-VO in der am 1. August 2024 in Kraft getretenen Fassung**, unabhängig vom Geltungsbeginn einzelner Bestimmungen gemäß Art. 111, 113 KI-VO.[6] Sonstige Rechtsbereiche wie die Vorgaben der Datenschutzgrundverordnung (DSGVO)[7], das Urheber- und Vergaberecht, Haftungsregelungen sowie das nationale Verwaltungs- und Verfassungsrecht[8] werden nicht im Einzelnen analysiert.

Es wird darauf hingewiesen, dass die in der KI-VO vorgesehene **Konkretisierung** durch Normen europäischer Normungsorganisationen, Durchführungsrechtsakte der Europäischen Kommission (Kommission), Praxisleitfäden und Leitlinien sowie nationale Rechtsakte[9] **nicht abgeschlossen** ist. Dies gilt auch für die Erschließung der KI-VO durch das rechtswissenschaftliche Schrifttum. Schließlich liegt, soweit ersichtlich, noch keine Rechtsprechung der Unionsgerichte zur Auslegung und Anwendung der KI-VO vor. Eine **abschließende** Entscheidung über die **Interpretation der KI-VO** obliegt dem Europäischen Gerichtshof (EuGH).

---

6 Es sei darauf hingewiesen, dass eine Verschiebung des Geltungsbeginns einiger Verpflichtungen der KI-VO um diskutiert wird, s. etwa https://www.heise.de/news/KI-Verordnung-Teilweise-Verschiebung-nicht-mehr-ausgeschlossen-10436515.html. Vgl. zu potenziellen Vereinfachungen der Anforderungen an Unternehmen: *Gkristsi/Haeck*, EU Kommission opens door for 'targeted changes' to AI Act, Politico, 13. Mai 2025; *Kafsack*, EU-Kommission will KI-Gesetz vereinfachen, FAZ, 10. April 2025, S. 16; Kommission, Aktionsplan für den KI-Kontinent – Q&A. Vgl. zudem den Draghi-Report, Teil B, Abschnitt 1, Kapitel 3, S. 79, wonach die Komplexität und das Risiko von Unstimmigkeiten zwischen der KI-VO und der DSGVO die KI-Entwicklung durch europäische Akteure untergraben könne.

7 Grundsätzlich gilt, dass KI-Systeme oder Modelle, die personenbezogene Daten verarbeiten, auch in den Anwendungsbereich der DSGVO fallen. Vgl. dazu bspw. European Data Protection Board, Opinion 28/2024 on certain data protection aspects related to the processing of personal data in the context of AI models, 17. Dezember 2024; European Data Protection Board, Statement 3/2024 on data protection authorities' role in the Artificial Intelligence Act framework, 16. Juli 2024; Bitkom, Generative KI im Unternehmen, Leitfaden 2025, S. 25 ff.; *Wilmer*, in: Jandt/Steidle, Datenschutz im Internet, 2. Aufl. 2025, Rn. 660 ff.

8 Vgl. etwa *Pilniok*, Unionsrechtliche Regulierung des Einsatzes von KI-Systemen in der öffentlichen Verwaltung, DÖV 2024, S. 581 (591), wonach neben der KI-VO und anderen Unionsrechtsakten „erheblicher Raum" für das mitgliedstaatliche Verwaltungsrecht bleibe. Vgl. zudem *Hornung*, in: Schoch/Schneider, Verwaltungsrecht, 6. EL November 2024, § 35a VwVfG, Rn. 50 ff. zu bereits bestehenden spezifischen KI-Vorgaben auf Landesebene. Vgl. auch *Guckelberger*, Hochrisiko-KI-Systeme in der Verwaltung, DÖV 2025, S. 45 (S. 55 f.), zur Bedeutung des nationalen Verfassungsrechts und der behördlichen Bindung an nationale Grundrechte unter Verweis auf: BVerfG, Urteil vom 16. Februar 2023, 1 BvR 1547/19, 1 BvR 2634/20, Automatisierte Datenanalyse, Rn. 100; BVerfG, Urteil vom 1. Oktober 2024, 1 BvR 1160/19, Rn. 127. Es wäre indes zu klären, inwieweit nach dem Geltungsbeginn der KI-VO die Unionsgrundrechte maßgeblicher Rechtmäßigkeitsmaßstab für behördliches Handeln würden. Vgl. schließlich den Hinweis bei *Martini/Botta*, Der Staat und das Metaversum, MMR 2023, S. 887 (896), auf ein noch von der Vorgängerregierung vorgeschlagenes Beschäftigtendatenschutzgesetz, das den Einsatz von KI-Systemen adressieren sollte. Nationale Regelungen zum Arbeitnehmerschutz im Zusammenhang mit KI sind nach Art. 2 Nr. 11 KI-VO zulässig.

9 Öffentlich wurde bisher nur der mit der Neuwahl überholte Referentenentwurf der Vorgängerregierung vom Richtlinien 2014/90/EU, (EU) 2016/797 und (EU) 2020/1828 (Verordnung über künstliche Intelligenz), im Folgenden: Referentenentwurf, KI-VO-Durchführungsgesetz(EU) 2024/1689 des Europäischen Parlaments und des Rates vom 13. Juni 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), im Folgenden: Referentenentwurf, KI-VO-Durchführungsgesetz, Stand 4. Dezember 2024.

2. Fragen im Zusammenhang mit der Anbieter- und Betreibereigenschaft

Die KI-VO verpflichtet diverse Akteuere entlang der KI-Wertschöpfungskette, vgl. Art. 3 Nr. 8 i. V. m. Art. 2 KI-VO. Für mitgliedstaatliche Behörden dürften insbesondere Pflichten als **Anbieter i. S. v. Art. 3 Nr. 3 KI-VO** oder **Betreiber i. S. v. Art. 3 Nr. 4 KI-VO** in Betracht kommen.

Anbieter ist gemäß Art. 3 Nr. 3 KI-VO

- jede „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“.

Betreiber ist gemäß Art. 3 Nr. 4 KI-VO

- jede „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“.

Differenzierung zwischen Anbieter und Betreiber[10]

Bereits aus Art. 3 Nr. 3 und Art. 3 Nr. 4 KI-VO ergibt sich, dass **Anbieterpflichten** sowohl für „**KI-Systeme**“ i. S. v. Art. 3 Nr. 1 KI-VO als auch „**KI-Modelle mit allgemeinem Verwendungszweck**“ i. S. v. Art. 3 Nr. 63 KI-VO bestehen können. **Betreiberpflichten** sind dagegen **nur für KI-Systeme** vorgesehen, nicht für KI-Modelle.

Nachfolgend wird auf Verhaltensweisen eingegangen, die die Anbietereigenschaft hinsichtlich KI-Systemen und -Modellen sowie die Betreibereigenschaft von KI-Systemen auslösen können.

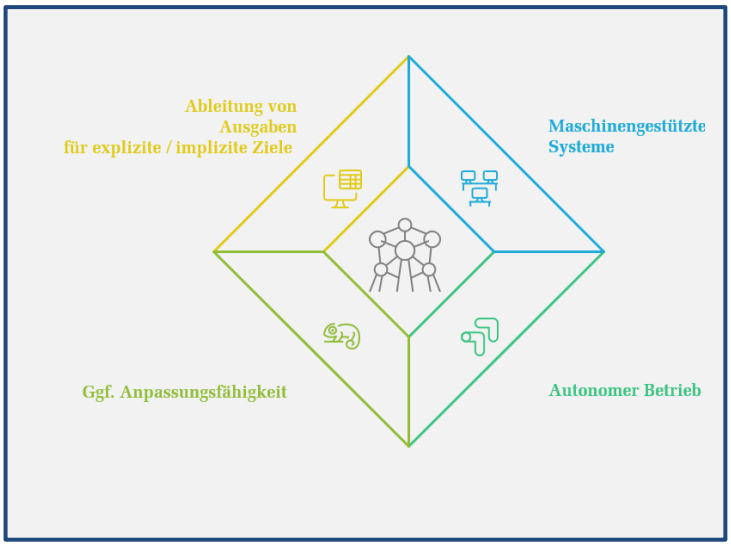
2.1. Entwickeln lassen und Einkaufen von KI-Systemen

In Betracht kommt, dass eine Behörde ein KI-System i. S. v. Art. 3 Nr. 1 KI-VO von einem Dritten für ihre Bedürfnisse entwickeln lässt oder ein einsatzbereites KI-System einkauft. Nachfolgend wird auf den Begriff des KI-Systems (Ziff. 2.1.1.) und auf die rechtliche Einstufung des „Entwickeln lassens“ oder Einkaufens eigegangen (Ziff. 2.1.2.).

10 Icons von NapkinAI.

2.1.1. KI-Systeme

Nach Art. 3 Nr. 1 KI-VO kennzeichnet sich ein KI-System dadurch aus, dass es sich um ein **maschinengestütztes System** handelt, das für einen in unterschiedlichem Grade **autonomen Betrieb** angelegt ist, nach seiner Betriebsaufnahme **anpassungsfähig sein kann** und das aus den erhaltenen Eingaben **Ausgaben** für explizite oder implizite Ziele **ableitet**, wie etwa Vorhersagen, Inhalte, Empfehlungen oder Entscheidungen, die physische oder virtuelle Umgebungen beeinflussen können.[11] Diese Merkmale dienen gemäß ErwG 12 Satz 2 KI-VO der Abgrenzung zu herkömmlichen Softwaresystemen und Programmierungsansätzen. Systeme, die auf ausschließlich von natürlichen Personen definierten Regeln für das automatische Ausführen von Operationen beruhen, sind nach ErwG 12 Satz 2 KI-VO keine KI-Systeme.



Merkmale von KI-Systemen[13]

Die **Kommission** hat (nicht rechtsverbindliche) **Leitlinien** zur Definition von KI-Systemen veröffentlicht, die die einzelnen Begriffsmerkmale der Definition näher erläutern.[12]

2.1.2. Entwickeln lassen oder einkaufen – Abgrenzung zwischen Anbieter- und Betreiberrolle

Aus Art. 3 Nr. 3 KI-VO folgt, dass – sofern die weiteren Voraussetzungen gegeben sind – ein Entwickeln lassen die **Anbietereigenschaft** hinsichtlich KI-Systemen begründen kann. In diesem Fall würden Behörden – **je nach Risikostufe** (s. Grafik in Ziff. 1) – die jeweiligen **Anbieterpflichten** der KI-VO treffen. Da ein beauftragter Entwickler voraussichtlich nicht selbst Anbieter wäre, müsste etwa über **entsprechende Verträge sichergestellt** werden, dass der Entwickler das KI-System so konzipiert, dass die Behörde ihren Pflichten aus der KI-VO (und weiteren Rechtsakten wie der DSGVO und dem Urheberrecht) genügen kann.

---

11 Die Definition ist an die überarbeitete Definition der OECD angeglichen, vgl. dazu: *Hense/Mustać*, AI Act kompakt, Compliance, management & use cases in corporate practice, 2025, S. 1 ff.; *van Eecke/Regenhardt* in: Pehlivan/Forgó/Valcke, The EU AI Act, 1. Aufl. 2025, S. 57 ff.

12 Kommission, Approval of the content of the draft Communication from the Commission - Commission Guidelines on the definition of an artificial intelligence system established by Regulation (EU) 2024/1689 (AI Act), KOM(2025) 924 endg., 6. Februar 2025.

13 Diese und weitere der folgenden Grafiken wurden mit NapkinAI erstellt.

Der Branchenverband Bitkom hat darauf hingewiesen, dass der Begriff „**Entwickeln lassen**“ einer weiteren **Konkretisierung** bedürfe. Es sei unklar, wie genau der potenziell zugrunde zu legende Auftragscharakter zu bestimmen sei, „etwa ob das KI-System […] speziell oder jedenfalls mit einem hohen Individualisierungsgrad gerade für den konkreten ‚Besteller‘ und den konkret anvisierten Einsatzbereich entwickelt werden muss.“ Offen sei auch, ob die Bereitstellung eines solchen Systems innerhalb eines Gesamtunternehmens oder Mutterkonzerns ebenfalls ein „Entwickeln lassen“ durch die empfangene Unternehmenseinheit darstelle.[14]

Jedenfalls dürfte der **bloße Kauf** eines KI-Systems zur Nutzung den **Anbieterbegriff nicht erfüllen**.[15] Bei Verwendung eines gekauften KI-Systems in eigener Verantwortung wäre die Behörde lediglich **Betreiber** i. S. v. Art. 3 Nr. 4 KI-VO. Die daran anknüpfenden Pflichten richten sich wiederum nach der Risikostufe des KI-Systems. In jedem Fall wäre auch hier darauf zu achten, dass nur solche KI-Systeme eingekauft werden, die gewährleisten, dass den entsprechenden **Pflichten aus der KI-VO entsprochen werden kann**. Sofern ein System zu Hochrisiko-Zwecken eingesetzt werden soll, ist darauf zu achten, dass das System anbieterseitig für diesen Zweck ausgewiesen ist, den Anforderungen an ein Hochrisiko-KI-System (**HRKS**) entspricht und dies vertraglich fixiert ist.[16] Hintergrund ist, dass andernfalls eine **zweckändernde Verwendung** i. S. v. Art. 25 KI-VO durch die Behörde in Betracht kommt, die die **Anbieterpflichten für HRKS aus Art. 16 KI-VO** auslösen kann.

Im **Leitfaden des Bitkom „Generative KI im Unternehmen“** wird ergänzend darauf hingewiesen, dass auch rechtliche Aspekte hinsichtlich der DSGVO, der Cybersicherheit, Schutzrechten und des Arbeitsrechts bereits im Rahmen der Beschaffung berücksichtigt werden sollten, da sich die im eingekauften Produkt enthaltene **Rechtsmängel auch auf die Einsatzphase auswirken** würden.[17] Der Leitfaden enthält eine „Checkliste und Vorüberlegungen vor der Beschaffung von KI“ (IT Procurement).[18] Auch wenn er auf Unternehmen zugeschnitten ist, könnten gleichwohl u. a. folgende darin empfohlene Schritte hilfreich sein:

- Erstellung einer **generellen KI-Strategie** zur Dokumentation, in welcher Weise die Nutzung von KI-Anwendungen zur Erreichung der betrieblichen Ziele beitragen soll;
- **Festlegung der wesentlichen technischen, kommerziellen und rechtlichen Anforderungen**;
- Entscheidung, ob die Leistung als „**AI as a Service“** oder als **„on premise-Installation“** bezogen werden soll;
- Festlegung der wichtigsten **rechtlichen „Must-have“- oder „No-Go“-Konditionen** und des **Umfangs der Lizenzierung** bzw. der **Nutzungsrechte** an der KI sowie hinsichtlich der von

14 Bitkom, Umsetzungsleitfaden zur KI-Verordnung, 29. Oktober 2024, S. 38.

15 Vgl. *Guckelberger*, Hochrisiko-KI-Systeme in der Verwaltung, DÖV 2025, S. 45 (51).

16 *Schwartmann u. a.*, KI-VO, Leitfaden für die Praxis, 2024, S. 92.

17 Bitkom, Generative KI im Unternehmen, Leitfaden 2025, S. 22.

18 Bitkom, Generative KI im Unternehmen, Leitfaden 2025, S. 19 ff.

der KI verwendeten internen oder externen Daten („Input“) und den dadurch generierten Daten („Output“);

– Bewertung, ob die Implementation bzw. Integration der KI intern erfolgt oder ob dafür ein externer IT-Servicepartner nötig /sinnvoll ist;

– **Rechtliche Gesichtspunkte**: u. a. Berücksichtigung der Anbieter-AGB und Vertragsbedingungen.

2.2. Entwickeln (lassen) von KI-Modellen mit allgemeinem Verwendungszweck

In Betracht kommt auch, dass Behörden KI-Modelle selbst entwickeln oder entwickeln lassen. Nachfolgend wird darauf eingegangen, was unter den von der KI-VO regulierten KI-Modellen zu verstehen ist (Ziff. 2.2.1.), unter welchen Voraussetzungen von einem – die Anbietereigenschaft auslösenden – Inverkehrbringen von KI-Modellen auszugehen ist (Ziff. 2.2.2.) und inwieweit die Veränderung bestehender (Open-Source-)KI-Modelle Anbieterpflichten begründen kann (Ziff. 2.2.3.). Schließlich werden rechtliche Aspekte im Zusammenhang mit den für Entwicklung von KI-Modellen wichtigen Trainingsdaten genannt (Ziff. 2.2.4.).

2.2.1. KI-Modelle mit allgemeinem Verwendungszweck

Die KI-VO reguliert **KI-Modelle**[19] **mit allgemeinem Verwendungszweck** (engl. General Purpose Artificial Intelligence Models – **GPAI-Modelle**, Allzweck-KI-Modelle).

Die Regelungen in Art. 3 Nr. 63, Art. 51 ff. KI-VO wurden erst während des europäischen Gesetzgebungsverfahrens eingefügt. Der Vorschlag der Kommission aus 2021[20] sah einen rein risikobasierten Ansatz für KI-Systeme vor, der auf ihren konkreten Einsatzzweck abstellte und kaum anwendungsunabhängige Anforderungen vorgab.[21] Die neu eingefügten Regelungen waren eine Reaktion auf die Markteinführung von ChatGPT, eines **KI-Systems mit allgemeinem Verwendungszweck** i. S. v. Art. 3 Nr. 66 KI-VO (**GPAI-Systeme**),[22] das auf dem Large Language Model (**LLM**) GPT und damit auf einem **GPAI-Modell beruht**.[23]

---

19 Der Begriff „KI-Modell“ als solcher ist in der KI-VO nicht definiert.

20 Kommission, Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz (Gesetz über künstliche Intelligenz) und zur Änderung bestimmter Rechtsakte der Union, KOM(2021) 206 endg., 21. April 2021.

21 *Bomhard/Siglmüller*, AI Act – das Trilogergebnis, RDi 2024, S. 45 (49).

22 Dies sind KI-Systeme, die auf einem GPAI-Modell beruhen und die in der Lage sind, eine Vielzahl von Zwecken zu erfüllen.

23 Vgl. zum Ganzen: *Bomhard/Siglmüller*, AI Act – das Trilogergebnis, RDi 2024, S. 45 (49); *Bond/Abbady*, in: Pehlivan/Forgó/Valcke, The EU AI Act, 1. Aufl. 2025, S. 827 ff.; *Hacker/Berz*, Der AI Act der Europäischen Union – Überblick, Kritik und Ausblick, ZRP 2023, S. 226; *Martini/Wiesehöfer*, Auf dem Weg zur Regulierung von General-Purpose-AI – eine erste Bestandsaufnahme und Kritik der Regelungsentwürfe, NVwZ 2024, S. 137.

GPAI-Modelle werden in der Regel mit großen Datenmengen durch verschiedene Methoden, etwa überwachtes, unüberwachtes und bestärkendes Lernen, trainiert, vgl. ErwG 97 Satz 3 KI-VO. Nach ErwG 98 KI-VO sollten Modelle mit mindestens einer Milliarde Parametern, die mit einer großen Datenmenge unter umfassender Selbstüberwachung trainiert werden, als GPAI-Modelle gelten. In ErwG 99 KI-VO heißt es, dass **große generative KI-Modelle** ein typisches Beispiel für ein GPAI-Modell seien, da sie eine flexible Erzeugung von Inhalten ermöglichten, etwa in Form von Text-, Audio-, Bild- oder Videoinhalten, die leicht ein breites Spektrum unterschiedlicher Aufgaben umfassen könnten.

GPAI-Modell steht für General Purpose Artificial Intelligence Model (auch: Allzweck-KI-Modell).

- GPAI-Modelle sind für eine breite Palette von Aufgaben einsetzbar, statt auf ein bestimmtes, enges Anwendungsfeld spezialisiert zu sein. Solche Modelle sind in der Lage, verschiedene, nicht näher spezifizierte Aufgaben auszuführen (vgl. Art. 3 Nr. 63 KI-VO). Die Anbieterpflichten sind in Art. 53 KI-VO normiert.
- Erhöhte Anforderungen werden an KI-Modelle mit **systemischem Risiko** i. S. v. Art. 3 Nr. 65, Art. 51 KI-VO geknüpft, vgl. Art. 55 KI-VO.

Die FAQ der Kommission zu GPAI-Modellen stellen klar, dass auch Modelle mit nur einer Modalität (Text, Audio, Bilder oder Video) GPAI-Modelle sein können.[24] Zudem hat die Kommission mit der Ausarbeitung von Leitlinien zur Klärung des Umfangs der Verpflichtungen von Anbietern von GPAI-Modellen begonnen. Darüber hinaus hat sie ein Arbeitsdokument veröffentlicht,[25] das die Grundlage für eine öffentliche Konsultation zu Leitlinien der Kommission für Anbieter von GPAI-Modellen darstellt. Dieses **Arbeitsdokument GPAI-Modelle** hat zwar keine Bindungswirkung für die finalen Leitlinien. Es sei aber darauf hingewiesen, dass darin die Frage, ob ein GPAI-Modell vorliegt, in erster Linie anhand der verwendeten Gleitkommaoperationen pro Sekunde (**FLOPS**; Floating Point Operations Per Second) und der **Art bzw. Breite der Trainingsdaten** bestimmt wird.[26]

Die Pflichten für **Anbieter von GPAI-Modellen** richten sich nach Art. 52 ff. KI-VO. Art. 52 KI-VO betrifft das Verfahren zur Einstufung als GPAI-Modell. **Art. 53 KI-VO** regelt die **Pflichten für Anbieter von GPAI-Modellen**. **Art. 55 KI-VO** enthält zusätzliche Vorgaben für Anbieter von GPAI-Modellen mit **systemischem Risiko** i. S. v. Art. 51 KI-VO i. V. m. Art. 3 Nr. 64, 65 KI-VO (s. noch Ziff. 2.2.3.1.2., Ziff. 4.3.2.). Unter systemischem Risiko ist ein Risiko zu verstehen, das auf der hohen Wirkkraft des Modells beruht, für GPAI-Modelle spezifisch ist und erhebliche Auswirkungen auf den Unionsmarkt hat, die sich in großem Umfang über die gesamte Wertschöpfungskette hinweg verbreiten können. Solche erheblichen Auswirkungen können bspw. in negativen Auswirkungen auf die öffentliche Sicherheit, die Grundrechte oder die Gesellschaft bestehen. Nach

24 Kommission, General-Purpose AI Models in the AI Act – Questions & Answers.

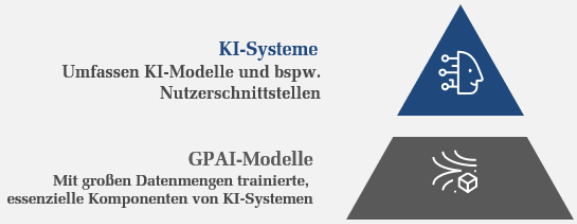
25 AI Office, Working Document, Targeted consultation in preparation of the Commission guidelines to clarify the scope of the obligations of providers of general-purpose AI models in the AI Act

26 Vgl. im Einzelnen: AI Office, Working Document, S. 3 f.: „Training compute is an imperfect proxy for generality and capabilities but currently the best metric for legal certainty“.

Art. 51 Abs. 1 Buchst. a, Abs. 2 KI-VO ist von einem GPAI-Modell mit systemischem Risiko auszugehen, wenn die kumulierte Menge der für sein Training verwendeten Berechnungen, gemessen in Gleitkommaoperationen, mehr als 10^{25} beträgt.

Dass die KI-VO **keine Pflichten für Betreiber von GPAI-Modellen** vorsieht, liegt daran, dass KI-Modelle stets in ein **KI-System integriert** werden müssen, um nutzbar zu sein, also „betrieben" werden zu können.[27] In ErwG 97 Sätze 7 bis 9 KI-VO heißt es:

> „Obwohl **KI-Modelle** wesentliche Komponenten von KI-Systemen sind, **stellen sie für sich genommen keine KI-Systeme** dar. Damit KI-Modelle zu KI-Systemen werden, ist die Hinzufügung weiterer Komponenten, zum Beispiel einer Nutzerschnittstelle, erforderlich. KI-Modelle sind in der Regel in KI-Systeme integriert und Teil davon."[28]



KI-Modell und KI-System

Ein **KI-System** ist die vollständige Anwendung, die in der Praxis einsatzfähig ist und ein oder mehrere KI-Modelle enthält. Beispiel: ChatGPT.

GPAI-Modelle sind eine wesentliche Komponente von KI-Systemen. Sie werden i. d. R. mit großen Datenmengen durch verschiedene Methoden (bspw. überwachtes, unüberwachtes und bestärkendes Lernen) trainiert. Damit KI-Modelle zu KI-Systemen werden, ist die Hinzufügung weiterer Komponenten, zum Beispiel einer Nutzerschnittstelle, erforderlich. Beispiel: GPT-4.

---

27 Bitkom, Umsetzungsleitfaden zur KI-Verordnung, 29. Oktober 2024, S. 33. Dies schließt nicht aus, dass neben Anbieterpflichten für KI-Modelle zusätzliche (Anbieter-) Pflichten hinsichtlich der KI-Systeme gelten, in die das GPAI-Modell integriert wird, vgl. Bitkom, Umsetzungsleitfaden zur KI-Verordnung, 29. Oktober 2024, S. 31 f.

28 Vgl. auch: Bitkom, Umsetzungsleitfaden zur KI-Verordnung, 29. Oktober 2024, S. 28: „Bei einem KI-System handelt es sich um die funktionsfähige und regelmäßig mit einer Benutzeroberfläche ausgestattete KI-Anwendung, während das KI-Modell das dahinterstehende (technische) Herzstück darstellt. […] Ein System wird also gerade dann zum KI-System, wenn ein KI-Modell in eine Applikations- oder Systemumgebung integriert wird. Während das KI-System – bildlich gesprochen – die KI ‚zum Anfassen und Nutzen' darstellt, ist das KI-Modell die dahinterstehende und für den Nutzer ‚unsichtbare' Funktionsweise, welche ohne Integration in ein System nicht nutzbar ist. KI-Modelle sind damit zwar wesentliche Komponenten von KI-Systemen, denen aber ohne das Hinzufügen weiterer Komponenten die ‚Systemeigenschaft' fehlt". Siehe zur Abgrenzung auch *Hecht*, Regulierung von GPAI-Modellen durch die KI-Verordnung, KIR 2025, S. 30 ff.

2.2.2. Anbietereigenschaft hinsichtlich GPAI-Modellen: Inverkehrbringen

Aus Art. 3 Nr. 3 KI-VO folgt, dass Behörden (nur) dann Anbieter von GPAI-Modellen sind, wenn sie das Modell nach dem Entwickeln bzw. Entwickeln lassen „**in Verkehr bringen**“.

Aus ErwG 97 KI-VO ergibt sich hierzu Folgendes:

> „Es sollte klar sein, dass die Pflichten für die Anbieter von KI-Modellen mit allgemeinem Verwendungszweck gelten sollten, sobald die KI-Modelle mit allgemeinem Verwendungszweck in Verkehr gebracht werden.“ (ErwG 97 Satz 10 KI-VO)
>
> „KI-Modelle mit allgemeinem Verwendungszweck können auf verschiedene Weise in Verkehr gebracht werden, unter anderem über Bibliotheken, Anwendungsprogrammierschnittstellen (API), durch direktes Herunterladen oder als physische Kopie.“ (ErwG 97 Satz 4 KI-VO)
>
> „Wenn der Anbieter eines KI-Modells mit allgemeinem Verwendungszweck ein eigenes Modell **in sein eigenes KI-System integriert**, das auf dem Markt bereitgestellt oder **in Betrieb genommen wird**, sollte jenes Modell als in Verkehr gebracht gelten und sollten daher die Pflichten aus dieser Verordnung für Modelle weiterhin zusätzlich zu den Pflichten für KI-Systeme gelten.“ (ErwG 97 Satz 11 KI-VO)
>
> „Die für Modelle festgelegten **Pflichten sollten in jedem Fall nicht gelten**, wenn ein eigenes Modell für **rein interne Verfahren** verwendet wird, die für die **Bereitstellung** eines Produkts oder einer **Dienstleistung an Dritte** nicht wesentlich sind, und die Rechte natürlicher Personen nicht beeinträchtigt werden.“ (ErwG 97 Satz 12 KI-VO)[29]

Sofern die Behörde also ein eigenes GPAI-Modell entwickelt, das sie – wovon auszugehen ist – nicht separat auf den Markt bringt, kann sie ausweislich ErwG 97 Satz 11 KI-VO Anbieter dieses Modells i. S. v. Art. 3 Nr. 3 KI-VO werden, wenn sie es in ein KI-System integriert und dieses in Betrieb nimmt.[30] Aus ErwG 97 Satz 12 KI-VO ergibt sich jedoch, dass die Anbieterpflichten dann nicht gelten sollten, wenn das jeweilige Modell für das vorgenannte „**rein interne Verfahren**“ verwendet wird.

---

29 Vgl. auch Kommission, General-Purpose AI Models in the AI Act – Questions & Answers, zu der Frage, was ein Anbieter eines GPAI-Modells ist.

30 Vgl. dazu: Bitkom, Umsetzungsleitfaden zur KI-Verordnung, 29. Oktober 2024, S. 31: „[…] die Einstufung als Anbieter [hängt] entscheidend davon ab, ob ein tatbestandliches Inverkehrbringen durch das Unternehmen vorliegt. Das Unternehmen integriert das weiter trainierte KI-Modell in spezifische KI-Systeme für die konkrete unternehmenseigene Anwendung zur Klassifizierung und zur Übersetzung von Texten […]. Das KI-Modell selbst wird vom Unternehmen nicht extern am Markt bereitgestellt, sodass insoweit kein Inverkehrbringen des (weiter trainierten) Modells als solches durch das Unternehmen vorliegt. Allerdings könnte das KI-Modell dennoch als in Verkehr gebracht gelten, weil es vom Unternehmen in ein eigenes KI-System integriert und dieses System durch bestimmungsgemäßen Eigengebrauch (Textklassifikation; Übersetzung) in Betrieb genommen wird (vgl. ErwG 97 Satz 8 KI-VO; genaue Bedeutung und Wirkungsweise dieser Feststellung im nicht-bindenden ErwG aber noch klarzustellen)“.

Hintergrund dürfte sein, dass die Anbieterpflichten aus Art. 52 ff. KI-VO geschaffen wurden, weil Anbieter von GPAI-Modellen entlang der KI-Wertschöpfungskette eine besondere Rolle und Verantwortung wahrnehmen, da die von ihnen bereitgestellten Modelle die Grundlage für eine Reihe nachgelagerter Systeme bilden können, vgl. ErwG 101 KI-VO.[31] Die Transparenz- und Dokumentationspflichten sind nicht zuletzt darauf gerichtet, Anbietern von KI-Systemen, die das GPAI-Modell integrieren wollen, Informationen zur Verfügung zu stellen. Wenn das GPAI-Modell aber nur intern verwendet wird und auch sonst **keine Berührungspunkte zu Dritten** bzw. **Rechten natürlicher Personen** bestehen, wären solche Pflichten unverhältnismäßig. Es ist allerdings weder aus den ErwG der KI-VO noch aus dem Arbeitsdokument GPAI-Modelle ersichtlich, welche konkreten Fallgestaltungen hiervon erfasst sein könnten.

2.2.3. Anbietereigenschaft hinsichtlich GPAI-Modellen: Fine-Tuning

Als Anwendungsfall könnte in Betracht kommen, dass eine Behörde ein GPAI-Modell nicht vollständig selbst entwickelt bzw. entwickeln lässt, sondern stattdessen Open-Source-KI-Modelle verfeinert („Fine-Tuning"). In diesem Fall ist fraglich, ob bzw. unter welchen Voraussetzungen eine solche Feinabstimmung dazu führt, dass von einem neuen Modell auszugehen ist. Anders als für HRKS (vgl. Art. 25, Art. 3 Nr. 23 KI-VO) enthält die KI-VO für GPAI keine Regelungen dazu, ab welchem Grad der **Modifikation von einem neuen GPAI-Modell** auszugehen ist. Die KI-VO legt damit auch nicht fest, unter welchen Voraussetzungen derjenige, der die Veränderung vornimmt, **selbst zum Anbieter** wird und damit den Pflichten aus Art. 52 ff. KI-VO unterliegt.

Die KI-VO setzt solche „Verfeinerungen" bzw. Änderungen, insbesondere von Open-Source-Modellen[32], voraus. In ErwG 97 Satz 4 KI-VO heißt es zu GPAI-Modellen:

> „**Diese Modelle können weiter geändert oder zu neuen Modellen verfeinert werden**."

ErwG 109 Satz 3 KI-VO lautet:

> „Im Falle einer **Änderung oder Feinabstimmung** eines Modells sollten die **Pflichten der Anbieter von KI-Modellen** mit allgemeinem Verwendungszweck **auf diese Änderung oder Feinabstimmung beschränkt sein**, indem beispielsweise die bereits vorhandene technische Dokumentation um Informationen über die Änderungen, einschließlich neuer Trainingsdatenquellen, ergänzt wird, um die in dieser Verordnung festgelegten Pflichten in der Wertschöpfungskette zu erfüllen."

---

31 *Woller/Terharen*, in: Zankl, KI-VO, 2025, Art. 53 KI-VO, Rn. 2.

32 Vgl. Art. 53 Abs. 2 Satz 1 KI-VO, der ausdrücklich auf die Open-Source-Bereitstellung von KI-Modellen zur Änderung durch Dritte Bezug nimmt.

Das **Arbeitsdokument GPAI-Modelle** adressiert ausdrücklich die Frage, ab welchem Modifikationsgrad durch einen **Dritten** („**downstream modifier**“)[33] die Anbietereigenschaft für GPAI-Modelle (s. Ziff. 2.2.3.1.1.) bzw. GPAI-Modelle mit systemischem Risiko (s. Ziff. 2.2.3.1.2.) ausgelöst wird.[34] Nach Einschätzung des Büros[35] bzw. dem Amts für Künstliche Intelligenz (**Amt für KI**)[36] führt nicht jede Veränderung eines GPAI-Modells dazu, dass von einem neuen Modell auszugehen ist. Dies sei vielmehr nur dann der Fall, wenn die Änderungen einen wesentlichen Einfluss auf die Gründe haben, die hinter den Verpflichtungen für Anbieter von GPAI-Modellen stehen.[37] Bei dem nachfolgend skizzierten Ansatz des Amts für KI handelt es sich lediglich um eine **vorläufige Annäherung**, die **keine Bindungswirkung für die endgültigen Leitlinien** hat.

2.2.3.1. Verfeinern von GPAI-Modellen

Das Arbeitsdokument sieht für GPAI-Modelle folgende Abgrenzung vor: Ein **downstream modifier** sollte dann als Anbieter gelten, wenn der **Umfang der für die Modifizierung** des Modells verwendeten **Rechenressourcen größer ist als ein Drittel des Schwellenwerts für Trainingsberechnungen für das ursprüngliche Modell** (d. h. derzeit etwa $3 \cdot 10^{21}$ FLOP).[38] Zusätzlich ist erforderlich, dass er das Modell in Verkehr bringt.

Ab dem vorgenannten Schwellenwert sei davon auszugehen, dass das geänderte Modell im Vergleich zum ursprünglichen Modell eine **wesentliche Änderung der Eigenschaften und des Verhaltens** aufweise. Diese Unterschiede könnten für das Amt für KI, die zuständigen nationalen Behörden und/oder nachgelagerte Anbieter relevant sein und rechtfertigten, dass der downstream modifier den Verpflichtungen gemäß Art. 53 Abs. 1 Buchst. a und b KI-VO unterliege. Zudem könne davon ausgegangen werden, dass **eine beträchtliche Menge an Daten** verwendet wurde, die für die Urheberrechtspolitik und die Zusammenfassung der Trainingsinhalte relevant sein könnten. Dies rechtfertige die Anwendbarkeit auch von Art. 53 Abs. 1 Buchst. c und d KI-VO.[39]

---

33 Diese Konstellation, in der ein Dritter das GPAI-Modell ändert, ist von Änderungen des GPAI-Modells durch den ursprünglichen Anbieter zu unterscheiden, siehe dazu: AI Office, Working Document, Targeted consultation in preparation of the Commission guidelines to clarify the scope of the obligations of providers of general-purpose AI models in the AI Act, S. 5 f.

34 Vgl. Kommission, General-Purpose AI Models in the AI Act – Questions & Answers.

35 Vgl. Art. 3 Nr. 47 KI-VO, in dem „Büro für Künstliche Intelligenz“ definiert wird als „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“.

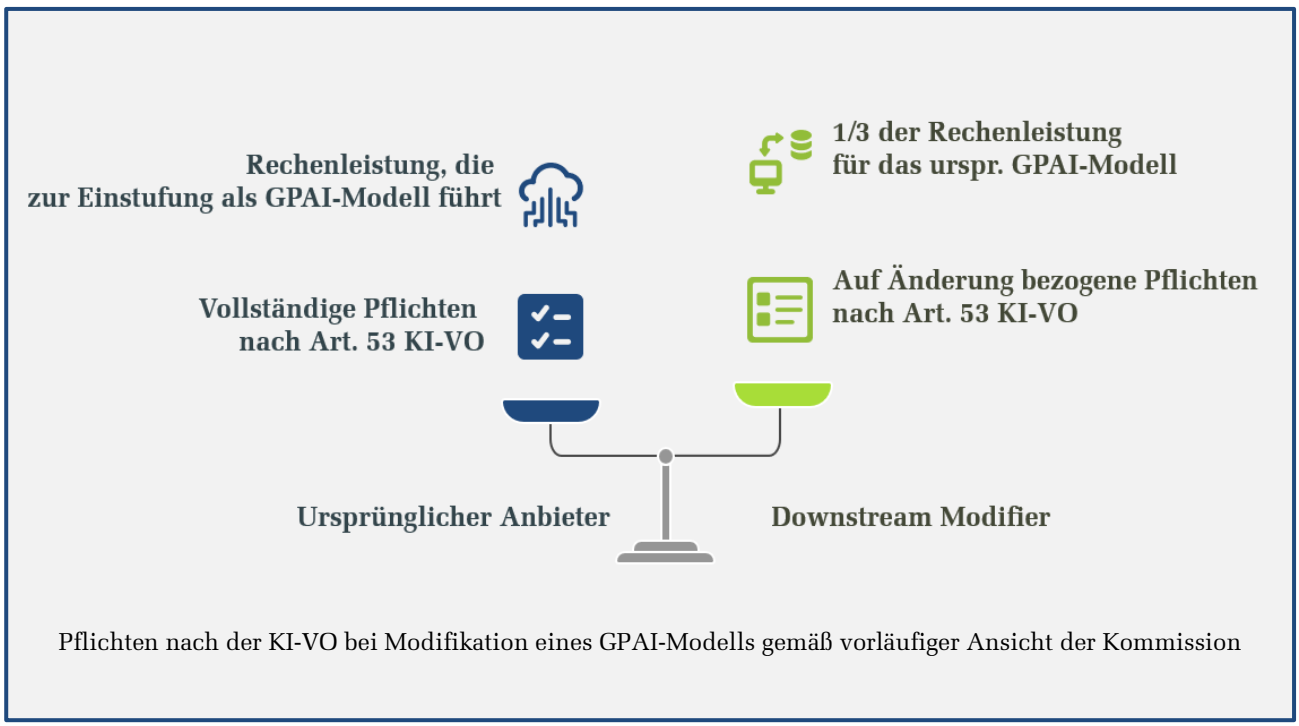
36 Vgl. Beschluss der Kommission vom 24. Januar 2024 zur Einrichtung des Europäischen Amts für Künstliche Intelligenz, ABl. C, C/2024/1459, 14. Februar 2024.

37 AI Office, Working Document, Targeted consultation in preparation of the Commission guidelines to clarify the scope of the obligations of providers of general-purpose AI models in the AI Act, S. 8.

38 Vgl. AI Office, Working Document, Targeted consultation in preparation of the Commission guidelines to clarify the scope of the obligations of providers of general-purpose AI models in the AI Act, S. 9.

39 Ebenda.

Im Einklang mit ErwG 109 KI-VO seien die genannten Anbieterpflichten auf die jeweilige Änderung beschränkt. Die Dokumentation nach Art. 53 Abs. 1 Buchst. a und b KI-VO müsse sich also nur auf die Modifikation beziehen und die Urheberrechtserklärung gemäß Art. 53 Abs. 1 Buchst. c KI-VO sowie die Zusammenfassung der Trainingsinhalte gemäß Art. 53 Abs. 1 Buchst. d KI-VO müsse nur die im Rahmen der Modifikation verwendeten Daten berücksichtigen.[40]



Pflichten nach der KI-VO bei Modifikation eines GPAI-Modells gemäß vorläufiger Ansicht der Kommission

2.2.3.2. Verfeinern von GPAI-Modellen mit systemischem Risiko

Im Zusammenhang mit dem Verfeinern von GPAI-Modellen mit systemischem Risiko sieht das Arbeitsdokument für GPAI-Modelle folgenden Ansatz vor:[41]

Ein downstream modifier sollte als Anbieter eines GPAI-Modells mit systemischem Risiko gelten, wenn eine der beiden folgenden Bedingungen erfüllt ist:

1. Das ursprüngliche Modell **ist ein GPAI-Modell** mit systemischem Risiko und der Umfang der für die Modifizierung des Modells verwendeten Rechenressourcen ist größer als ein Drittel des Schwellenwerts für Trainingsberechnungen für das ursprüngliche Modell gemäß Art. 51 Abs. 2 KI-VO;

40 Ebenda.

41 Ebenda, S. 9 f.

2. Das ursprüngliche Modell **ist kein GPAI-Modell** mit systemischem Risiko, der downstream modifier kennt den kumulativen Betrag der für das Training dieses ursprünglichen Modells verwendeten Rechenressourcen und zusammen mit dem Betrag der für die Modifizierung des Modells verwendeten Rechenressourcen ergibt sich eine Summe, die größer ist als der in Art. 51 Abs. 2 KI-VO festgelegte Schwellenwert für Trainingsberechnungen für das ursprüngliche Modell (d. h. derzeit 10^{25} FLOP).

Der Schwellenwert in Nr. 1 sei gewählt worden, weil bei der Änderung eines Modells unter Verwendung eines Drittels des Schwellenwerts für Trainingsberechnungen i. S. v. Art. 51 Abs. 2 KI-VO (d. h. derzeit 10^{25} FLOP) davon ausgegangen werden könne, dass das geänderte Modell im Vergleich zum ursprünglichen Modell ein erheblich verändertes Systemrisiko aufweise. Insbesondere kann nach Ansicht des Amts für KI nicht davon ausgegangen werden, dass der ursprüngliche Anbieter die Veränderung des Systemrisikos durch eine solche Modifikation in seiner Systemrisikobewertung und -minderung berücksichtigt habe.

Der Schwellenwert in Nr. 2 diene dazu, sicherzustellen, dass modifizierte GPAI-Modelle, die den Schwellenwert für Trainingsberechnungen i. S. v. Art. 51 Abs. 2 KI-VO erreichen, unter die Verpflichtungen für GPAI-Modelle mit systemischem Risiko fallen. Dies liege daran, dass in diesem Fall das ursprüngliche Modell keiner Systemrisikobewertung oder -minderung unterzogen wurde und der Schwellenwert erst durch die Veränderung erreicht werde.

Wenn downstream modifier unter die Bedingung 1 fallen, sollen ihre Pflichten nicht auf die Modifikation beschränkt sein. Das bedeutet, dass die in Art. 55 Abs. 1 KI-VO geforderte Bewertung und Minderung des Systemrisikos für das geänderte Modell erneut durchgeführt werden sollte, wobei alle verfügbaren Informationen über das ursprüngliche Modell zu berücksichtigen seien. Außerdem müsse der Anbieter die Kommission gemäß Art. 52 Abs. 1 KI-VO unterrichten.

2.2.4. Vorgaben im Zusammenhang mit Trainingsdaten

Ein wichtiger Aspekt beim Entwickeln bzw. Entwickeln lassen von GPAI-Modellen ist die Frage, mit welchen Daten die Modelle trainiert werden. Anders als dies nach Art. 10 KI-VO für Anbieter von Hochrisiko-KI-Systemen (**HRKS**) der Fall ist, sieht Art. 53 KI-VO für Anbieter von GPAI-Modellen keine umfangreichen qualitativen Anforderungen an die Trainingsdaten[42] vor.

2.2.4.1. Urheberrechtstrategie gemäß Art. 53 Abs. 1 Buchst. c KI-VO

Die Vorbereitung des KI-Trainings durch das Zusammenstellen von Trainingsinhalten und das eigentliche Trainieren des neuronalen Netzes werfen – neben **datenschutzrechtlichen Fragen**[43] –

42 Dies sind nach Art. 3 Nr. 29 KI-VO „Daten, die zum Trainieren eines KI-Systems verwendet werden, wobei dessen lernbare Parameter angepasst werden“.

43 Vgl. European Data Protection Board, Opinion 28/2024 certain data protection aspects related to the processing of personal data in the context of AI models, 17. Dezember 2024; Bitkom, Generative KI im Unternehmen, Leitfaden 2025, S. 25 ff. Vgl. zudem jüngst die Eilentscheidung des Oberlandesgerichts Köln, Beschluss vom 23. Mai 2025, 15 UKl. 2/25, dazu, dass dass Meta Nutzerdaten ohne Einwilligung zu KI-Trainingszwecken verwendet darf.

auch (bislang ungeklärte) Rechtsfragen im Zusammenhang mit **Schutzrechten** (insbesondere Urheberrechten) auf.[44]

Art. 53 Abs. 1 Buchst. c KI-VO bestimmt, dass die Anbieter von GPAI-Modellen eine Strategie zur Einhaltung des **EU-Urheberrechts** und damit zusammenhängender Rechte und insbesondere zur Ermittlung und Einhaltung eines gemäß Art. 4 Abs. 3 der Urheberechtsrichtlinie 2019/790[45] geltend gemachten Rechtsvorbehalts auf den Weg bringen (vgl. auch ErwG 105 f. KI-VO). Diese Vorgabe ist dann bedeutend, **wenn Trainingsinhalte nicht ausschließlich selbst erstellt** oder **umfassend einlizenziert** werden.[46] Denn in diesem Fall sind zwar Vervielfältigungen und Entnahmen urheberrechtlich geschützter, rechtmäßig zugänglicher Inhalte für Text- und Data-Mining gemäß Art. 4 Abs. 1 Urheberechtsrichtlinie 2019/790 unionsrechtlich zulässig. Dies gilt aber dann nicht, wenn der jeweilige Rechteinhaber der Trainingsdaten einen Rechtsvorbehalt i. S. v. Art. 4 Abs. 3 Urheberrechtsrichtlinie 2019/790 erklärt hat.[47] Da Art. 53 Abs. 1 Buchst. c KI-VO auf den Rechtsvorbehalt ausdrücklich Bezug nimmt, verletzen Anbieter von GPAI-Modellen sowohl das Urheberrecht als auch die KI-VO, wenn sie einem solchen Rechtsvorbehalt zuwiderhandeln.[48] In der Praxis wären diese Vorgaben dann relevant, wenn externe Trainingsinhalte genutzt werden sollten, ohne hierfür Nutzungsrechte zu erwerben.

Konkretisierungen dieser Anforderungen stehen noch aus. Am 11. März 2025 hat die Kommission den **dritten Entwurf des Verhaltenskodexes für GPAI** veröffentlicht.[49] Dieser auf Art. 56 KI-VO gestützte Kodex soll bis zur Erarbeitung harmonisierter Normen i. S. v. Art. 40 KI-VO dazu dienen, die Pflichten aus Art. 53, 55 KI-VO zu konkretisieren. Für Anbieter von GPAI-Modellen, die sich an den nicht rechtsverbindlichen Verhaltenskodex halten, gilt die Vermutung, dass sie die entsprechenden Anforderungen der KI-VO einhalten, vgl. Art. 53 Abs. 4, Art. 55 Abs. 2 KI-

---

44 Vgl. näher zur Relevanz der Urheberrechte an KI-Trainingsdaten auf Anbieter-, Betreiber- und Nutzerseite: Bitkom, Generative KI im Unternehmen, Leitfaden 2025, S. 41 ff.; *Dregelies*, KI-Training unter dem AI Act, GRUR 2024, S. 1484 ff. Siehe auch das Vorabentscheidungsverfahren zum EuGH in der Rs. C-250/25, Like Company/Google Ireland Limited.

45 Richtlinie (EU) 2019/790 des Europäischen Parlaments und des Rates vom 17. April 2019 über das Urheberrecht und die verwandten Schutzrechte im digitalen Binnenmarkt und zur Änderung der Richtlinien 96/9/EG und 2001/29/EG, ABl. L 130, 17. Mai 2019, S. 92 (berichtigte Fassung).

46 Vgl. Bitkom, Umsetzungsleitfaden zur KI-Verordnung, 29. Oktober 2024, S. 178 f.

47 Vgl. ausführlich: *Bernsteiner/Schmitt*, in: Martini/Wendehorst, Verordnung über künstliche Intelligenz, 2024, Art. 53 KI-VO, Rn. 32 ff.; *Woller/Terharen*, in: Zankl, KI-VO, 2025, Art. 53 KI-VO, Rn. 22 f.

48 Vgl. Bitkom, Umsetzungsleitfaden zur KI-Verordnung, 29. Oktober 2024, S. 179.

49 Abrufbar unter: https://digital-strategy.ec.europa.eu/de/library/third-draft-general-purpose-ai-code-practice-published-written-independent-experts. Nach Art. 56 Abs. 9 KI-VO mussten Praxisleitfäden bis zum 2. Mai 2025 vorliegen. Das Amt für KI hat offenbar angekündigt, dass der Verhaltenskodex jedenfalls bis zum Inkrafttreten der Art. 51 ff. KI-VO am 2. August 2025 vorliegen werde, vgl. *Gkristsi/Haeck*, EU Commission opens door for ‘targeted changes’ to AI Act, Politico, 13. Mai 2025.

VO. Der dritte Entwurf enthält auch einen **Abschnitt zu den (Selbst-)Verpflichtungen der Anbieter von GPAI-Modellen hinsichtlich des Urheberrechts**.[50]

2.2.4.2. Exkurs: Haftungsrisiken bezüglich fehler- oder mangelhafter Trainingsdaten

Der Vollständigkeit halber wird darauf hingewiesen, dass nicht auszuschließen ist, dass Fehler und Mängel in den Trainingsdaten eines GPAI-Modells zu fehlerhaften Ergebnissen der jeweiligen Anwendung (KI-System, bspw. Chatbot) führen können. Es kommen dann grundsätzlich vertragliche und außervertragliche Haftungsansprüche (Deliktsrecht und Produzentenhaftung) in Betracht.[51]

Auf EU-Ebene hat die Kommission beschlossen, den Vorschlag für die sog. **KI-Haftungsrichtlinie**[52] zur Harmonisierung verschuldensabhängiger Ansprüche vorerst **nicht weiter zu verfolgen**.[53]

Die neue **Produkthaftungsrichtlinie 2024/2853** (**ProduktthaftungsRL**)[54] vom 18. November 2024 umfasst KI-relevante Neuerungen. Die Richtlinie gilt für Produkte, die **nach dem 9. Dezember 2026 in Verkehr gebracht oder in Betrieb genommen werden**. Die Mitgliedstaaten müssen die Bestimmungen der neuen ProduktthaftungsRL bis zum **9. Dezember 2026** umsetzen. Sie modernisiert die bestehenden Vorschriften über die verschuldensunabhängige Gefährdungshaftung und Schadensersatzpflicht für **fehlerhafte Produkte**, um sie an die technologische Weiterentwicklung anzupassen. Zu diesen neuen Technologien zählt nach ErwG 3 ProduktthaftungRL auch **KI**. Die Richtlinie stellt klar, dass auch **Software** zu den erfassten Produkten zählt. Der Kreis der Haftenden wird erweitert, indem er bspw. auch Akteure einschließt, die das Produkt wesentlich verändern, vgl. Art. 8 Abs. 2 ProduktthaftungsRL. Zum **ersatzfähigen Schaden** zählen nunmehr auch der **Verlust oder die Beschädigung von Daten**, vgl. Art. 6 Abs. 1 Buchst. c ProduktthaftungsRL. Zudem sind bei der Beurteilung der **Fehlerhaftigkeit** eines Produkts auch die Auswirkungen der Fähigkeit, nach dem Inverkehrbringen oder der Inbetriebnahme **weiter zu lernen**, zu berücksichtigen, vgl. Art. 7 Abs. 2 Buchst. c ProduktthaftungRL. Darüber hinaus enthalten Art. 9, 10 ProduktthaftungRL Regelungen, die den Zugang zu Beweismitteln erleichtern und Beweiserleichterungen vorsehen, um den Schwierigkeiten potenzieller Kläger angesichts der technologischen Komplexität bspw. beim Einsatz von maschinellem Lernen Rechnung zu tragen.[55]

---

50 Abrufbar unter: https://digital-strategy.ec.europa.eu/en/library/third-draft-general-purpose-ai-code-practice-published-written-independent-experts.

51 Vgl. die Darstellung: Bitkom, Generative KI im Unternehmen, Leitfaden 2025, S. 53 ff.

52 Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates zur Anpassung der Vorschriften über außervertragliche zivilrechtliche Haftung an künstliche Intelligenz (Richtlinie über KI-Haftung), KOM(2022) 496 endg., 28. September 2022.

53 Vgl. Kommission, Arbeitsprogramm für 2025, KOM(2025) 45 endg., 11. Februar 2025, Anhang I.

54 Richtlinie (EU) 2024/2853 des Europäischen Parlaments und des Rates vom 23. Oktober 2024 über die Haftung für fehlerhafte Produkte und zur Aufhebung der Richtlinie 85/374/EWG des Rates, ABl. L, 2024/2853, 18. November 2024.

55 Vgl. dazu: Fachbereich Europa, Maßnahmen der EU zur Regulierung von KI, EU 6 - 3000 - 001/25, 27. Februar 2025, S. 20 ff.

3. Registrierungspflichten für Hochrisiko-KI-Systeme

Fraglich ist, inwieweit Behörden verpflichtet sind, die bei ihnen zum Einsatz kommenden KI-Systeme öffentlich zu machen.

Insofern gilt, dass Registrierungspflichten in **externen Datenbanken auf EU-Ebene** bzw. **auf nationaler Ebene** nur für Anbieter und bestimmte Betreiber von **Hochrisiko-KI-Systemen** (**HRKS**) i. S. v. **Art. 6 Abs. 2, Anhang III KI-VO** vorgesehen sind.

Diese Pflichten für HRKS gelten gemäß Art. 113 Abs. 2 KI-VO ab dem **2. August 2026**. Für HRKS, die vor dem 2. August 2026 in Verkehr gebracht oder in Betrieb genommen wurden, gelten die Bestimmungen gemäß Art. 111 Abs. 2 KI-VO – abgesehen von verbotenen Praktiken nach Art. 5 KI-VO – nur bei nachträglicher erheblicher Veränderung oder wenn die HRKS bestimmungsgemäß **von Behörden** verwendet werden sollen. Dann sind die Maßnahmen zur Einhaltung der KI-VO bis zum **2. August 2030** zu ergreifen.

3.1. Hochrisiko-Anwendungen

Entscheidend für die Frage, ob Registrierungspflichten in externen Datenbanken – und sonstige strenge Anforderungen der KI-VO – gelten, ist, ob es sich um ein **HRKS** i. S. v. Art. 6 KI-VO handelt. Aus den ErwG 46 Satz 5, 48 KI-VO ergibt sich, dass nur solche KI-Systeme als hochriskant eingestuft werden sollten, die erhebliche schädliche Auswirkungen auf die Gesundheit, die Sicherheit und insbesondere die Grundrechte von Personen in der EU haben.

Im Schrifttum wird darauf hingewiesen, dass die in Art. 6 Abs. 2 i. V. m. Anhang III KI-VO genannten Systeme „in hohem Maß **Bezüge zum staatlichen Bereich**“ aufwiesen.[56] Dies dürfte insbesondere im Gegensatz zu den in Art. 6 Abs. 1 KI-VO geregelten HRKS gelten, die einen stärkeren Bezug zu physischen Produkten und bereits geltenden Produktsicherheitsvorschriften aufweisen.[57]

Der Inhalt von Anhang III KI-VO lässt sich wie folgt zusammenfassen:

Nr. 1: KI-Systeme zur **biometrischen Fernidentifizierung, Emotionserkennung und biometrischen Kategorisierung** (z. B. KI-System zur rückwirkenden Identifizierung eines Ladendiebs);

Nr. 2: **KI-Sicherheitskomponenten in kritischen Infrastrukturen** (z. B. Verkehr), deren Ausfall das Leben und die Gesundheit der Bürger gefährden könnte;

Nr. 3: KI-Lösungen, die in **Bildungseinrichtungen** eingesetzt werden und die den Zugang zu Bildung und den Verlauf des Berufslebens einer Person bestimmen können (z. B. Bewertung von Prüfungen);

---

56 *Guckelberger*, Hochrisiko-KI-Systeme in der Verwaltung, DÖV 2025, S. 45 (47, Hervorhebungen hinzugefügt).

57 Nach Art. 6 Abs. 1 KI-VO sind KI-Systeme, die als Sicherheitsbauteil eines Produkts verwendet werden sollen oder selbst ein Produkt sind, das unter die in Anhang I KI-VO aufgeführten Harmonisierungsvorschriften der EU fällt, hochriskant, wenn diese Harmonisierungsvorschriften eine Konformitätsbewertung durch Dritte für das Inverkehrbringen oder die Inbetriebnahme vorsehen. Vgl. Fachbereich Europa, Maßnahmen der EU zur Regulierung von KI, EU 6 - 3000 - 001/25, 27. Februar 2025, S. 14.

Nr. 4: KI-Tools für die **Beschäftigung, das Management von Arbeitnehmern** und den Zugang zur Selbstständigkeit (z. B. Lebenslauf-Sortierungssoftware für die Einstellung);

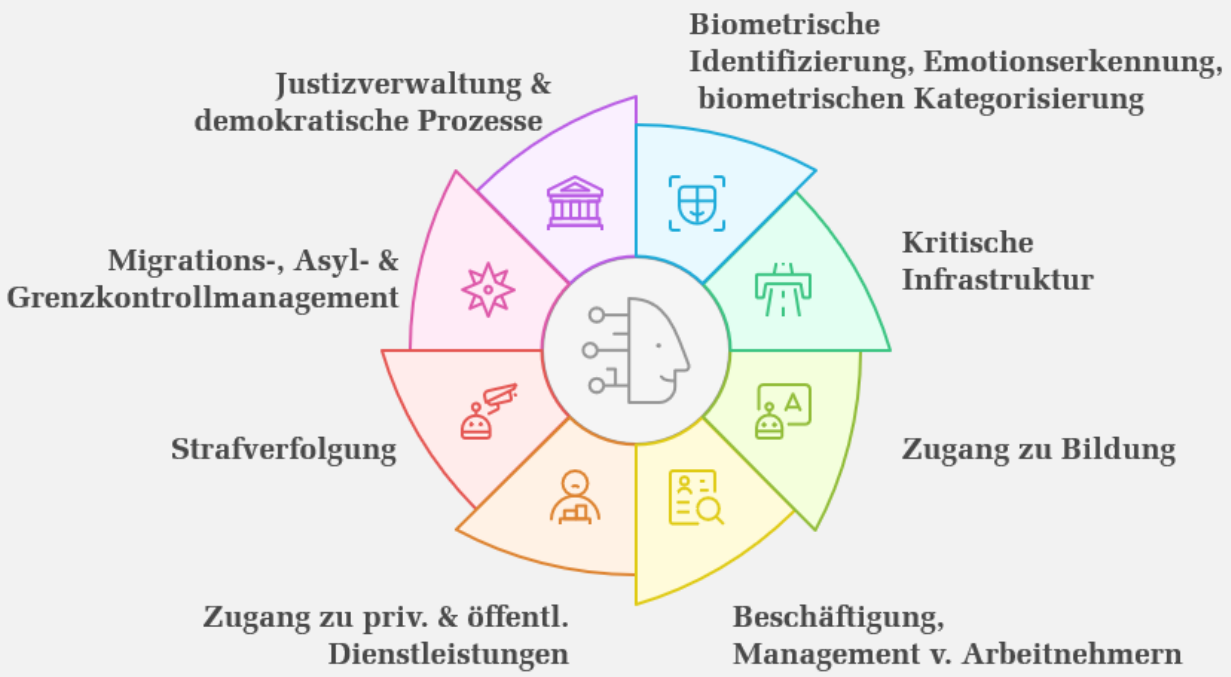
Nr. 5: Bestimmte KI-Anwendungsfälle, die genutzt werden, um Zugang zu wesentlichen privaten und **öffentlichen Dienstleistungen** zu gewähren (z. B. Kreditbewertung, die den Bürgern die Möglichkeit verwehrt, einen Kredit zu erhalten);

Nr. 6: KI-Anwendungsfälle in der **Strafverfolgung**, die in die Grundrechte der Menschen eingreifen können (z. B. Bewertung der Zuverlässigkeit von Beweismitteln);

Nr. 7: KI-Anwendungsfälle im **Migrations-, Asyl- und Grenzkontrollmanagement** (z. B. automatisierte Prüfung von Visumanträgen);

Nr. 8: KI-Lösungen für die **Justizverwaltung** und **demokratische Prozesse** (z. B. KI-Lösungen zur Vorbereitung von Gerichtsurteilen).[58]

Hochrisiko-KI-Anwendungen i. S. v. Art. 6 Abs. 2, Anhang III KI-VO



58 Kommission, KI-Gesetz.

Neben den offenkundig auf Behörden zugeschnittenen Anwendungsfällen (Zugang zu öffentlichen Dienstleistungen, Strafverfolgung, Migrations-, Asyl- und Grenzkontrollmanagement, Justizverwaltung) könnte der Einsatz von HRKS in Behörden auch im Bereich der **Beschäftigung und des Personalmanagements** i. S. v. Anhang III Nr. 4 KI-VO von Bedeutung sein. Dabei geht es um den Einsatz von KI-Systemen für die Einstellung oder Auswahl von Personen, insbesondere um gezielte Stellenanzeigen zu schalten, Bewerbungen zu sichten oder zu filtern und Bewerber zu bewerten (Buchst. a). Außerdem könnten KI-Systeme in Betracht kommen, die die Bedingungen von Arbeitsverhältnissen, Beförderungen und Kündigungen beeinflussen. Darüber hinaus könnte der Einsatz von KI-Systemen erwogen werden, die für die Zuweisung von Aufgaben aufgrund des individuellen Verhaltens, persönlicher Merkmale und Eigenschaften oder für die Beobachtung und Bewertung der Leistung und des Verhaltens von Personen in solchen Beschäftigungsverhältnissen verwendet werden sollen (Buchst. b).

In diesem Zusammenhang ist auf die **Ausnahmebestimmung** in **Art. 6 Abs. 3 UAbs. 1 KI-VO** hinzuweisen. Danach gilt ein in Anhang III genanntes KI-System **nicht als hochriskant**, „wenn es **kein erhebliches Risiko** der Beeinträchtigung in Bezug auf die Gesundheit, Sicherheit oder Grundrechte natürlicher Personen birgt, indem es unter anderem **nicht das Ergebnis der Entscheidungsfindung wesentlich beeinflusst**.“ Dafür muss das KI-System nach Art. 6 Abs. 3 UAbs. 2 KI-VO darauf angelegt sein,

- für eine eng gefasste Verfahrensaufgabe bestimmt zu sein,
- das Ergebnis einer zuvor abgeschlossenen menschlichen Tätigkeit zu verbessern,
- Entscheidungsmuster oder Abweichungen von früheren Entscheidungsmustern zu erkennen
- oder eine vorbereitende Aufgabe für eine Bewertung durchzuführen, die für die Zwecke der in Anhang III aufgeführten Anwendungsfälle relevant ist. Nach ErwG 53 Satz 13 KI-VO fallen hierunter „u. a. intelligente Lösungen für die **Bearbeitung von Dossiers**, wozu verschiedene Funktionen wie **Indexierung**, **Suche**, **Text- und Sprachverarbeitung** oder Verknüpfung von Daten mit anderen Datenquellen gehören, oder KI-Systeme, die für die **Übersetzung von Erstdokumenten** verwendet werden.“

Guckelberger verweist darauf, dass **KI-Systeme in der öffentlichen Verwaltung** oft nur unterstützend eingesetzt werden sollen, weshalb sich bereits jetzt schwierige Abgrenzungsprobleme abzeichneten.[59]

Darüber hinaus könnte für (Parlaments-)Verwaltungen Anhang III Nr. 8 Buchst. b Satz 1 KI-VO relevant sein. Danach gelten auch solche KI-Systeme als hochriskant, die **bestimmungsgemäß** verwendet werden sollen, um das **Ergebnis einer Wahl oder eines Referendums oder das Wahlverhalten natürlicher Personen bei der Ausübung ihres Wahlrechts bei einer Wahl oder einem Referendum zu beeinflussen**. Nicht dazu gehören gemäß Anhang III Nr. 8 Buchst. b Satz 2 KI-Systeme, deren Ausgaben natürliche Personen nicht direkt ausgesetzt sind. Dies betrifft bspw.

59 *Guckelberger*, Hochrisiko-KI-Systeme in der Verwaltung, DÖV 2025, S. 45 (48). In diesem Sinne auch: *Pilniok*, Unionsrechtliche Regulierung des Einsatzes von KI-Systemen in der öffentlichen Verwaltung, DÖV 2024, S. 581 (589).

Instrumente zur Organisation, Optimierung oder Strukturierung politischer Kampagnen in administrativer oder logistischer Hinsicht. Die **Nutzung von GPAI für rein organisatorische Zwecke ist demnach auch im Kontext von Wahlen unproblematisch**. Im Schrifttum wird darauf hingewiesen, dass auch solche KI-Systeme nicht erfasst seien, die als **Informationssysteme** eingesetzt werden und aufgrund technisch bedingter Verzerrungen die Meinungsbildung beeinflussen könnten, ohne dass sie mit einer entsprechenden Zwecksetzung in Betrieb genommen wurden. Dies könne bei GPAI-Systemen der Fall sein, wenn ihre Datenbasis politische Tendenzen enthalte oder entwickle.[60]

Weitere Klarheit zur Auslegung von Anhang III KI-VO könnten die bereits angekündigten Leitlinien der Kommission zu HRKS i. S. v. Art. 96 Abs. 1 Buchst. a KI-VO bringen.[61]

3.2. Registrierung in der EU-Datenbank

Eine Pflicht zur Registrierung in der EU-Datenbank i. S. v. Art. 71 KI-VO bestünde nach Art. 16 Buchst. i, Art. 49 Abs. 1 KI-VO dann, wenn die jeweilige Behörde i. S. v. Art. 3 Nr. 3 KI-VO **Anbieter** eines **HRKS** i. S. v. Art. 6 Abs. 2 i. V. m. **Anhang III Nr. 1, 3 bis 8 KI-VO** wäre.

Eine Registrierungspflicht besteht nach Art. 16 Buchst. i, Art. 49 Abs. 2 KI-VO auch für solche KI-Systeme, die zwar dem Anwendungsbereich von Anhang III KI-VO unterfallen, **vom Anbieter** jedoch gemäß Art. 6 Abs. 3 KI-VO **nicht als hochriskant** eingestuft wurden.

Aus Art. 26 Abs. 8, Art. 49 Abs. 3 und Art. 71 Abs. 3 KI-VO folgt, dass zudem **bestimmte Betreiber** i. S. v. Art. 3 Nr. 4 KI-VO registrierungspflichtig sind, wenn sie ein KI-System i. S. v. Art. 6 Abs. 2 i. V. m. **Anhang III Nr. 1, 3 bis 8 KI-VO** nutzen wollen. Der Kreis der registrierungspflichtigen Betreiber wird in den vorgenannten Bestimmungen in der deutschen Fassung nicht einheitlich angegeben. Während nach Art. 26 Abs. 8 KI-VO nur „Organe, Einrichtungen oder sonstige Stellen der Union“ registrierungspflichtig sein sollen, nennt Art. 49 Abs. 3 KI-VO „**Behörden** oder Organe, Einrichtungen oder sonstige Stellen der Union“. Art. 71 Abs. 3 KI-VO nennt allgemein „Behörden, Einrichtungen oder sonstige Stellen“. In der englischen Fassung wird in Art. 26 Abs. 8 und Art. 49 Abs. 3 KI-VO aber jeweils auf „public authorities, or Union institutions, bodies, offices or agencies“ rekurriert. Es dürften folglich auch **nationale Behörden** als Betreiber von HRKS i. S. v. Art. 6 Abs. 2 i. V. m. Anhang III Nr. 1, 3 bis 8 KI-VO registrierungspflichtig sein.[62]

Die aus Art. 49 Abs. 3 KI-VO folgende Pflicht besteht darin, sich in der Datenbank zu registrieren und das bereits vom Anbieter gelistete HRKS auszuwählen, dessen Verwendung geplant ist, vgl. ErwG 131 Satz 2 KI-VO. Stellt der jeweilige Betreiber beim Registrierungsversuch fest, dass

---

60 Vgl. *Schwartmann u. a.*, KI-VO, Leitfaden für die Praxis, 2024, S. 111.

61 Vgl. unten auf der Seite: https://digital-strategy.ec.europa.eu/en/news/commission-seeks-input-clarify-rules-general-purpose-ai-models.

62 Vgl. auch: *Kasper,* Die Verwaltung in der KI-Regulierung, DÖV 2025, S. 471 (475): Verpflichtung öffentlicher Betreiber von Hochrisiko-KI-Systemen sowohl auf nationaler Ebene als auch auf EU-Ebene.

das betreffende HRKS vom Anbieter noch nicht in der EU-Datenbank hinterlegt ist, hat er einstweilen von der Verwendung abzusehen und den Anbieter oder Händler zu informieren.

Die EU-Datenbank wird gemäß Art. 71 Abs. 1 Satz 1 KI-VO von der Kommission errichtet und in Zusammenarbeit mit den Mitgliedstaaten geführt. Die einzugebenden Informationen finden sich gemäß Art. 71 Abs. 2, 3 KI-VO in Anhang VIII KI-VO. Zweck der EU-Datenbank ist es, die **Arbeit der Kommission und der Mitgliedstaaten im KI-Bereich zu erleichtern** und die **Transparenz gegenüber der Öffentlichkeit** zu erhöhen, vgl. ErwG 131 Satz 1 KI-VO. Gemäß Art. 49 Abs. 4 KI-VO werden Daten zu HRKS in den Bereichen Strafverfolgung, Migration, Asyl und Grenzkontrollen allerdings in einem sicheren, nicht öffentlichen Teil der Datenbank registriert, auf den nur die Kommission und die zuständigen nationalen Behörden Zugriff haben.

3.3. Registrierung in einer nationalen Datenbank

Eine Ausnahme von der Registrierungspflicht in der EU-Datenbank besteht für die in Anhang III Nr. 2 KI-VO genannten HRKS im Bereich der kritischen Infrastruktur. Diese KI-Systeme werden gemäß Art. 49 Abs. 5 KI-VO auf **nationaler Ebene** registriert.

4. Dokumentations- und Auskunftspflichten, Kompetenzen der Überwachungsbehörden nach der KI-VO

Neben externen Registrierungspflichten sieht die KI-VO weitere Dokumentationspflichten sowie Auskunftspflichten gegenüber den zuständigen Behörden vor.

Spezifische Dokumentations- und Auskunftspflichten bestehen dann, wenn eine Behörde **Anbieter eines HRKS** (Ziff. 4.1.), **Betreiber eines HRKS** (Ziff. 4.2.) oder **Anbieter** eines **GPAI-Modells** (Ziff. 4.3.) ist. Ziff. 4.4. behandelt die Frage, ob darüber hinaus eine **allgemeine Dokumentation der Risikoeinstufung** von KI-Anwendungen erstellt werden sollte.

Hinsichtlich der **zuständigen Behörde** gilt, dass die **Kommission** nach Art. 88 Abs. 1 Satz 1 KI-VO ausschließlich zur Überwachung und Durchsetzung der Bestimmungen über **GPAI-Modelle** zuständig ist (vgl. ErwG 162 KI-VO). Art. 88 Abs. 1 Satz 2 KI-VO bestimmt, dass die Kommission dem Amt für KI die Durchführung dieser Aufgaben überträgt. Das Amt für KI ist nach Art. 75 Abs. 1 KI-VO zudem befugt, die Konformität eines KI-Systems der KI-VO zu überwachen und zu beaufsichtigen, wenn dieses KI-System auf einem GPAI-Modell beruht und Modell und System vom selben Anbieter entwickelt wurden (vgl. ErwG 161 Satz 2 KI-VO). Im Übrigen sind die **Mitgliedstaaten** für die Überwachung und Durchsetzung des AI Act bezüglich **KI-Systemen** zuständig (vgl. ErwG 161 Satz 3 KI-VO).

4.1. Anbieter von Hochrisiko-KI-Systemen

4.1.1. Pflichten hinsichtlich der Einstufung als nicht hochriskant

Sollte eine Behörde als Anbieter eines HRKS i. S. v. Art. 6 Abs. 2, Anhang III KI-VO der Auffassung sein, dass dieses i. S. v. Art. 6 Abs. 3 KI-VO nicht hochriskant ist, müsste sie ihre Bewertung

gemäß **Art. 6 Abs. 4 KI-VO dokumentieren** und die **Dokumentation auf Verlangen der zuständigen nationalen Behörde**[63] **vorlegen**, vgl. Art. 6 Abs. 4 Satz 2, Art. 80 KI-VO (s. auch Ziff. 3.2. zur Registrierungspflicht in der EU-Datenbank).[64]

4.1.2. Pflichten hinsichtlich der KI-VO-Konformität von HRKS

Nach **Art. 18 KI-VO** hat der Anbieter eines HRKS für einen Zeitraum von zehn Jahren ab dem Inverkehrbringen oder der Inbetriebnahme folgende Unterlagen für die zuständigen nationalen Behörden bereitzuhalten:

- die technische Dokumentation i. S. v. Art. 11 KI-VO und Anhang IV KI-VO;
- die Dokumentation zum Qualitätsmanagementsystem (QMS) i. S. v. Art. 17 KI-VO, welches die Einrichtung, Anwendung und Dokumentation eines Risikomanagementsystems gemäß Art. 9 KI-VO sowie das nach Art. 72 Abs. 1 KI-VO einzurichtende und zu dokumentierende System zur Beobachtung nach dem Inverkehrbringen umfasst;
- die Dokumentation über etwaige von notifizierten Stellen genehmigte Änderungen und gegebenenfalls die von den notifizierten Stellen ausgestellten Entscheidungen und sonstigen Dokumente.[65]
- die EU-Konformitätserklärung i. S. v. Art. 47 KI-VO und Anhang V KI-VO.

Nach Art. 19 KI-VO müssen Anbieter zudem die von ihren HRKS **automatisch erzeugten Protokolle** i. S. v. **Art. 12 Abs. 1 KI-VO** aufbewahren, soweit diese Protokolle ihrer Kontrolle unterliegen. Art. 21 Abs. 2 KI-VO bestimmt, dass die Anbieter einer zuständigen Behörde auf begründete Anfrage hin gegebenenfalls Zugang zu diesen Protokollen gewähren.

Fraglich ist, ob sich **darüber hinaus** Dokumentationspflichten ergeben. Nach Art. 16 Buchst. k KI-VO müssen Anbieter von HRKS auf begründete Anfrage einer zuständigen nationalen Behörde hin nachweisen, dass das HRKS die **Anforderungen aus Art. 8 bis Art. 15 KI-VO erfüllt**.[66] Art. 17 Abs. 1 Buchst. k KI-VO sieht außerdem vor, dass das Qualitätsmanagementsystem (QMS) „Sys-

---

63 Nach dem Referentenentwurf, KI-VO-Durchführungsgesetz, Stand 4. Dezember 2024 wäre dies die Bundesnetzagentur.

64 Vgl. *Anderl/Ciarnau*, in: Zankl, KI-VO, 2025, Art. 6 KI-VO, Rn. 44, dazu, dass diese Dokumentation entsprechend ihres Regelungszwecks aktuell zu halten sei.

65 QMS und technische Dokumentation sind für die externe und interne Konformitätsprüfung i. S. v. Art. 43 i. V. m. Anhang VI, VII KI-VO die wesentlichen Dokumente.

66 In inhaltlich-technischer Sicht gilt, dass die Kommission nach Art. 40 Abs. 2 KI-VO Normungsaufträge erteilt, die diese Anforderungen abdecken. Art. 6 Abs. 5 KI-VO sieht vor, dass die Kommission spätestens bis zum 2. Februar 2026 Leitlinien zur praktischen Umsetzung der Bestimmungen über die Klassifizierung von HRKS (Art. 6 KI-VO) zur Verfügung stellt. Hieraus könnte sich ggf. eine Klarstellung der Anbieterpflichten in diesem Zusammenhang ergeben. Vgl. die Ankündigung zu einer Konsultation in diesem Bereich: https://digital-strategy.ec.europa.eu/en/news/commission-seeks-input-clarify-rules-general-purpose-ai-models (am Seitenende).

teme und Verfahren für die Aufzeichnung **sämtlicher einschlägigen Dokumentation und Informationen**“ umfasst. Nach Art. 21 Abs. 1 KI-VO übermitteln Anbieter von HRKS einer zuständigen nationalen Behörde auf deren begründete Anfrage hin „**sämtliche Informationen und Dokumentation**, die erforderlich sind, um die **Konformität des HRKS** mit Art. 8 bis 15 KI-VO nachzuweisen.“ Im Schrifttum wird darauf hingewiesen, dass der Umfang der Auskunftspflicht aus Art. 21 Abs. 1 KI-VO **inhaltlich nicht** begrenzt sei. Sie könne potenziell alle Unterlagen und Informationen umfassen, die zur Beweisführung notwendig seien. Dies gehe über die Dokumentation i. S. v. Art. 18 KI-VO hinaus und umfasse etwa Pläne und informelle Protokolle.[67]

Mit der Auskunftsplicht korrespondieren **Befugnisse der nationalen**[68] **Marktüberwachungsbehörden**. Diese richten sich gemäß Art. 74 Abs. 1 KI-VO zunächst nach der Marktüberwachungsverordnung 2019/1020 (**MÜ-VO**)[69]. Nach Art. 74 Abs. 1 i. V. m. Art. 14 Abs. 4 Buchst. a MÜ-VO zählt dazu u. a. die Befugnis, von allen nach der KI-VO Verpflichteten die **Vorlage von relevanten Dokumenten**, **technischen Spezifikationen**, **Daten** oder **Informationen über die Konformität** und **technische Aspekte** des KI-Systems zu verlangen.[70] Darüber hinaus enthält Art. 74 Abs. 12, 13 KI-VO spezielle Befugnisse hinsichtlich HRKS. Nach Art. 74 Abs. 12 KI-VO gewähren die Anbieter den Marktüberwachungsbehörden – sofern dies relevant und erforderlich ist – uneingeschränkten Zugang zur **Dokumentation** sowie zu den für die Entwicklung von HRKS **verwendeten Trainings-, Validierungs- und Testdatensätzen**. Nach Art. 74 Abs. 13 KI-VO können die Marktüberwachungsbehörden „als letztes Mittel“ Zugang zum **Quellcode** des HRKS erhalten, wenn dies zur Bewertung der Einhaltung von Art. 8 bis 15 KI-VO erforderlich ist.[71]

Bei **HRKS** i. S. v. **Anhang III KI-VO** sind außerdem die in **Art. 77 KI-VO** normierten Befugnisse der von den Mitgliedstaaten zu benennenden nationalen Behörden oder öffentlichen Stellen für die Einhaltung des EU-Rechts zum Schutz der Grundrechte zu beachten.[72] Diese sind nach Art. 77 Abs. 1 KI-VO befugt, sämtliche auf Grundlage der KI-VO erstellte oder geführte Dokumentationen anzufordern und einzusehen, sofern dies zur wirksamen Aufgabenwahrnehmung im

---

67 *Anderl/Ciarnau*, in: Zankl, KI-VO, 2025, Art. 21 KI-VO, Rn. 6.

68 Abweichend von der grundsätzlichen Zuständigkeit nationaler Marktüberwachungsbehörden für die Überwachung von KI-Systemen bestimmt Art. 75 Abs. 1 KI-VO die Zuständigkeit des europäischen Amts für KI, wenn das KI-System auf einem GPAI-Modell beruht und Modell und System vom selben Anbieter entwickelt werden. Art. 75 Abs. 2 KI-VO sieht vor, dass die nationalen Marktüberwachungsbehörden mit dem Amt für KI zusammenarbeiten und das KI-Gremium sowie andere Marktüberwachungsbehörden unterrichten, wenn sie hinreichenden Grund zur Annahme haben, dass KI-Systeme mit allgemeinem Verwendungszweck, die von Betreibern direkt für mindestens einen Zweck, der gemäß der KI-VO als hochriskant eingestuft ist, verwendet werden können, nicht mit den in der KI-VO festgelegten Anforderungen konform sind. Vgl. zu dieser Bestimmung *Schmidl/Rohner*, in: Zankl, KI-VO, 2025, Art. 75 KI-VO, Rn. 11 ff.

69 Verordnung (EU) 2019/1020 des Europäischen Parlaments und des Rates vom 20. Juni 2019 über Marktüberwachung und die Konformität von Produkten sowie zur Änderung der Richtlinie 2004/42/EG und der Verordnungen (EG) Nr. 765/2008 und (EU) Nr. 305/2011, ABl. L 169 vom 25. Juni 2019, S. 1 (konsolidierte Fassung v. 23. Mai 2024).

70 Vgl. Art. 74 Abs. 5 KI-VO zur Möglichkeit des Fernzugriffs in bestimmten Fällen.

71 Siehe dazu: *Kasper,* Die Verwaltung in der KI-Regulierung, DÖV 2025, S. 471 (476 f.).

72 Vgl. Bundesministerium für Wirtschaft und Energie, Liste nach Art. 77 Abs. 2 KI-Verordnung v. 19. Dezember 2024.

Rahmen ihrer Befugnisse notwendig ist. Sollte die Dokumentation i. S. v. Art. 77 Abs. 1 KI-VO nicht ausreichen, können diese Behörden bei den Marktüberwachungsbehörden einen Antrag auf Durchführung eines technischen Tests des HRKS stellen, vgl. Art. 77 Abs. 3 KI-VO.

Art. 78 Abs. 2 Satz 1 KI-VO bestimmt für alle an der Anwendung der KI-VO beteiligten Behörden, dass diese nur Daten anfragen, die für die Bewertung des von KI-Systemen ausgehenden Risikos und für die Ausübung ihrer Befugnisse in Übereinstimmung mit der MÜ-VO „unbedingt erforderlich“ sind.[73]

4.2. Betreiber von Hochrisiko-KI-Systemen

Für Betreiber von HRKS bestimmt Art. 26 Abs. 6 UAbs. 1 KI-VO, dass sie die von ihrem HRKS **automatisch erzeugten Protokolle**, soweit diese ihrer Kontrolle unterliegen, für einen der Zweckbestimmung des HRKS angemessenen Zeitraum aufbewahren. Dieser umfasst mindestens sechs Monate, sofern im geltenden Unionsrecht oder nationalen Recht nichts anderes bestimmt ist.

Soweit darüber hinaus eine Pflicht zur Erstellung einer **Datenschutzfolgeabschätzung** (Art. 26 Abs. 9 KI-VO) oder – für Einrichtungen des öffentlichen Rechts – einer **Grundrechte-Folgenabschätzung** (Art. 27 KI-VO) besteht, sind diese von den nationalen Behörden nicht nur intern aufzubewahren. Es muss vielmehr eine Zusammenfassung der jeweiligen Ergebnisse in der EU-Datenbank registriert werden, vgl. Art. 26 Abs. 8, Art. 49 Abs. 3, Anhang VIII Abschnitt C Nr. 4, 5, KI-VO.

Darüber hinaus normiert die KI-VO keine ausdrücklichen Dokumentationspflichten für Betreiber von HRKS. Art. 26 Abs. 12 KI-VO bestimmt allgemein, dass sie mit den zuständigen Behörden bei allen Maßnahmen zusammenarbeiten, die im Zusammenhang mit dem HRKS zur Umsetzung der KI-VO ergriffen werden.

Was behördliche Überwachungsbefugnisse, insbesondere Informationsverlangen, angeht, gelten die Art. 74 Abs. 1 KI-VO i. V. m. Art. 14 MÜ-VO, Art. 77 und Art. 78 KI-VO.

4.3. Anbieter von GPAI-Modellen

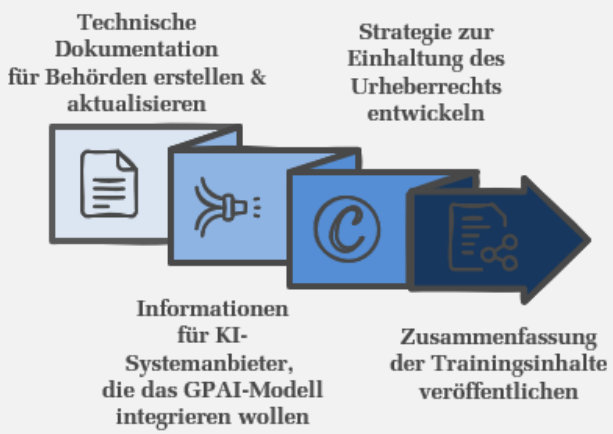
Die Pflichten für Anbieter von GPAI-Modellen aus Art. 52 ff. KI-VO gelten gemäß Art. 113 Abs. 3 Buchst. b KI-VO grundsätzlich ab dem **2. August 2025**. Eine Ausnahme besteht für GPAI-Modelle, die zu diesem Zeitpunkt in der EU bereits in Verkehr gebracht worden sind. Bei ihnen ist die Konformität mit der KI-VO gemäß Art. 111 Abs. 3 KI-VO bis zum 2. August 2027 sicherzustellen.

---

73 Vgl. *Schmidl/Rohner*, in: Zankl, KI-VO, 2025, Art. 78 KI-VO, Rn. 9, dazu, dass die Befugnisse der zuständigen Behörden angesichts der Formulierung „unbedingt erforderlich“ restriktiv auszulegen seien.

4.3.1. Pflichten für Anbieter von GPAI-Modellen aus Art. 53 Abs. 1 KI-VO

Vorbehaltlich des **Ausnahmetatbestands bei einer Open-Source-Bereitstellung**[74] gemäß Art. 53 Abs. 2 KI-VO[75] normiert Art. 53 Abs. 1 Buchst. a bis d KI-VO verschiedene Dokumentations- und Transparenzpflichten.



Pflichten f. Anbieter von GPAI-Modellen aus Art. 53 Abs. 1 KI-VO

Nach Art. 53 Abs. 1 Buchst. a KI-VO haben Anbieter von GPAI-Modellen eine **technische Dokumentation des Modells zu** erstellen und zu aktualisieren, die mindestens die in Anhang XI KI-VO aufgeführten Informationen enthält, damit sie dem Amt für KI und den zuständigen nationalen Behörden auf Anfrage zur Verfügung gestellt werden kann.

Hinsichtlich der Transparenz der **Trainingsdaten bzw. -verfahren** (s. Ziff. 2.2.4.) hat die technische Dokumentation nach Anhang XI KI-VO – „soweit es anhand der Größe und des Risikoprofils des betreffenden Modells angemessen ist“[76] – u. a. folgenden Inhalt:

- die Entwurfsspezifikationen des Modells und des **Trainingsverfahrens** einschließlich Trainingsmethoden und -techniken (Anhang XI Nr. 2 Abschnitt 1 Buchst. b KI-VO);[77]

- gegebenenfalls Informationen über die für das Trainieren, Testen und Validieren **verwendeten Daten**, einschließlich der **Art und Herkunft der Daten** und der Aufbereitungsmethoden (zum Beispiel Bereinigung, Filterung usw.), der **Zahl der Datenpunkte**, ihres Umfangs und ihrer Hauptmerkmale; gegebenenfalls die Art und Weise, wie die Daten erlangt und ausge-

74 Die Ausnahme bezieht sich auf Art. 53 Abs. 1 Buchst. a und b KI-VO.

75 Siehe dazu etwa: *Bond/Abbady*, in: Pehlivan/Forgó/Valcke, The EU AI Act, 1. Aufl. 2025, S. 855.

76 Vgl. zur Relativierung der Pflichten anhand der Größe des Modells sowie des Anbieters: ErwG 109 Satz 1 KI-VO; *Bernsteiner/Schmitt*, in: Martini/Wendehorst, Verordnung über künstliche Intelligenz, 2024, Art. 53 KI-VO, Rn. 13.

77 Dies schließt nach Ansicht in der Literatur die Angabe der Methode des maschinellen Lernens (überwachtes/unüberwachtes Lernen etc.) und das verwendete Trainingsmodell ein (Generative-Adversarial-Netze/Diffusiuonsmodelle etc.), vgl. *Bernsteiner/Schmitt*, in: Martini/Wendehorst, Verordnung über künstliche Intelligenz, 2024, Art. 53 KI-VO, Rn. 20 m. w. N. aus dem Schrifttum.

wählt wurden, sowie alle anderen Maßnahmen zur Feststellung, ob Datenquellen ungeeignet sind, und Methoden zur Erkennung ermittelbarer Verzerrungen (Anhang XI Abschnitt Nr. 2 Buchst. c KI-VO);[78]

– die für das Trainieren des Modells verwendeten Rechenressourcen (zum Beispiel Anzahl der Gleitkommaoperationen), die Trainingszeit und andere **relevante Einzelheiten im Zusammenhang mit dem Trainieren** (Anhang XI Abschnitt 1 Nr. 2 Buchst. d KI-VO).[79]

Darüber hinaus sind nach **Art. 53 Abs. 1 Buchst. b KI-VO nachgelagerten Anbietern i. S. v. Art. 3 Nr. 68 KI-VO**[80] Informationen und die Dokumentationen u. a. gemäß Anhang XII KI-VO zur Verfügung zu stellen.[81] Dazu zählen nach Anhang XII Nr. 2 Buchst. c KI-VO „**gegebenenfalls Informationen über die für das Trainieren**, Testen und Validieren **verwendeten Daten**, einschließlich der Art und Herkunft der Daten und der Aufbereitungsmethoden".[82]

Nach Art. 53 Abs. 1 Buchst. d KI-VO erstellen und veröffentlichen die Anbieter von GPAI-Modellen zudem eine **hinreichend detaillierte Zusammenfassung** der für das **Training** des GPAI-Modells **verwendeten Inhalte** nach einer vom Amt für KI bereitgestellten Vorlage[83] (**Trainingsdatenzusammenfassung**).[84] Diese Bestimmung steht im Zusammenhang mit der nach Art. 53 Abs. 1 Buchst. c KI-VO zu entwickelnden **Urheberrechtsstrategie** (s. dazu oben Ziff. 2.2.4.1.). Nach ErwG 107 KI-VO dient die Zusammenfassung dazu, die Transparenz der beim Training von

---

78 Vgl. im Einzelnen dazu: *Bernsteiner/Schmitt*, in: Martini/Wendehorst, Verordnung über künstliche Intelligenz, 2024, Art. 53 KI-VO, Rn. 20 m. w. N. aus dem Schrifttum.

79 *Bernsteiner/Schmitt*, in: Martini/Wendehorst, Verordnung über künstliche Intelligenz, 2024, Art. 53 KI-VO, Rn. 20, wonach aus dieser Beschreibung die Funktionsweise und Leistungsfähigkeit des Modells hervorgehen müsse.

80 Dies sind Anbieter eines KI-Systems, einschließlich eines KI-Systems mit allgemeinem Verwendungszweck, das ein KI-Modell integriert, unabhängig davon, ob das KI-Modell von ihnen selbst bereitgestellt und vertikal integriert wird oder von einer anderen Einrichtung auf der Grundlage vertraglicher Beziehungen bereitgestellt wird.

81 Vgl. *Bernsteiner/Schmitt*, in: Martini/Wendehorst, Verordnung über künstliche Intelligenz, 2024, Art. 53 KI-VO, Rn. 23, 28, dazu, dass und inwieweit Art. 53 Abs. 1 Buchst. b Ziff. i KI-VO zusätzlich eine Verständnisverschaffungspflicht normiere und dass Art. 53 Abs. 1 Buchst. b i. V. m. Anhang XII KI-VO ggf. als Schutzgesetz i. S. v. § 823 BGB angesehen werden könne.

82 *Bernsteiner/Schmitt*, in: Martini/Wendehorst, Verordnung über künstliche Intelligenz, 2024, Art. 53 KI-VO, Rn. 20, weisen darauf hin, dass es sich hierbei um eine „verkürzte" Darstellung der Transparenzangaben nach Art. 53 Abs. 1 Buchst. a, Anhang XI Nr. 2 Buchst. c KI-VO handele.

83 Die Annahme der Vorlage ist für das zweite Quartal 2025 geplant, vgl. https://digital-strategy.ec.europa.eu/de/policies/ai-code-practice.

84 Vgl. *Bernsteiner/Schmitt*, in: Martini/Wendehorst, Verordnung über künstliche Intelligenz, 2024, Art. 53 KI-VO, Rn. 20, 47, dazu, dass sich hier Überschneidungen mit Art. 53 Abs. 1 Buchst. a, Anhang IX Nr. 2 Buchst. c KI-VO und Art. 53 Abs. 1 Buchst. b, Anhang XII Nr. 2 Buchst. c KI-VO ergäben. Es sei aber nur für die Pflicht aus Art. 53 Abs. 1 Buchst. d KI-VO eine Mustervorlage der Kommission vorgesehen. Zudem sei davon auszugehen, dass die Informationen für nachgelagerte Anbieter aus Art. 53 Abs. 1 Buchst. b KI-VO detaillierter sein müssten als die in erster Linie für Schutzrechteinhaber relevante Trainingsdatenzusammenfassung aus Art. 53 Abs. 1 Buchst. d KI-VO.

GPAI-Modellen verwendeten Daten, einschließlich **urheberrechtlich geschützter Texte und Daten**, zu erhöhen. Der Umfang dieser Zusammenfassung solle unter gebührender Berücksichtigung von Geschäftsgeheimnissen allgemein weitreichend und nicht technisch detailliert sein, um Parteien mit berechtigtem Interesse, einschließlich Urheberrechtsinhabern, die Ausübung und Durchsetzung ihrer Rechte nach dem Unionsrecht zu erleichtern. Daher sollten ausweislich des ErwG 107 KI-VO beispielsweise die wichtigsten Datenerhebungen oder Datensätze aufgeführt werden, die beim Training des Modells verwendet wurden (etwa große private oder öffentliche Datenbanken oder Datenarchive), und eine beschreibende Erläuterung anderer verwendeter Datenquellen bereitgestellt werden.

4.3.2. Pflichten für Anbieter von GPAI-Modellen mit systemischem Risiko aus Art. 55 Abs. 1 KI-VO

Anbieter von GPAI-Modellen, welche ein **systemisches Risiko** bergen, müssen nach Art. 55 Abs. 1 Buchst. a KI-VO eine Modellbewertung mit standardisierten Protokollen und Instrumenten durchführen, die dem Stand der Technik entsprechen. Hierzu gehören auch die **Durchführung und Dokumentation von Angriffstests beim Modell**, um systemische Risiken zu ermitteln und zu mindern. Nach Art. 55 Abs. 1 Buchst. c KI-VO müssen sie einschlägige Informationen über **schwerwiegende Vorfälle und mögliche Abhilfemaßnahmen erfassen und dokumentieren** und das Amt für KI sowie gegebenenfalls die zuständigen nationalen Behörden unverzüglich darüber unterrichten.

4.3.3. Sonstiges zur Pflichterfüllung und Auskunftspflichten

Nach Art. 53 Abs. 4, Art. 55 Abs. 2 KI-VO können sich Anbieter von GPAI-Modellen bis zur Veröffentlichung einer harmonisierten Norm (vgl. Art. 40 KI-VO) auf Praxisleitfäden i. S. v. Art. 56 KI-VO stützen, um die Einhaltung des Art. 53 Abs. 1 und Art. 55 Abs. 1 KI-VO nachzuweisen. Der dritte Entwurf des **Verhaltenskodex für GPAI** (s. oben Ziff. 2.2.4.1.)[85] enthält dazu u. a. einen Abschnitt zu den **Transparenzanforderungen** aus Art. 53 Abs. 1 Buchst. a und b KI-VO, einschließlich einer **Mustervorlage**[86] zur Einhaltung dieser Vorgaben enthalten.

Die Kommission kann nach Art. 91 KI-VO den Anbieter des betreffenden KI-Modells mit allgemeinem Verwendungszweck auffordern, die gemäß den Art. 53, 55 KI-VO erstellte **Dokumentation** oder „**alle zusätzlichen Informationen vorzulegen, die erforderlich sind, um die Einhaltung dieser Verordnung durch den Anbieter zu beurteilen**“.

---

85 Vgl. https://digital-strategy.ec.europa.eu/de/library/third-draft-general-purpose-ai-code-practice-published-written-independent-experts; https://code-of-practice.ai/?section=summary. Siehe zum Zweck und Anwendungsbereich: Kommission, General-Purpose AI Models in the AI Act – Questions & Answers.

86 Abrufbar unter: https://digital-strategy.ec.europa.eu/en/library/third-draft-general-purpose-ai-code-practice-published-written-independent-experts.

4.4. Darüber hinaus: Umfassende Dokumentation der Risikoeinstufung?

Die KI-VO verpflichtet mitgliedstaatliche Behörden (und Unternehmen) nicht ausdrücklich dazu, sämtliche zum Einsatz kommende KI-Systeme nebst Risikoeinstufung in einem internen Register o. ä. nachzuhalten.[87]

Es stellt sich daher die Frage, ob es **gleichwohl sinnvoll** sein könnte, eine solche umfassende Dokumentation bzw. ein internes Register zu erstellen. Insofern dürfte zu berücksichtigen sein, dass Auskunftspflichten der Anbieter bzw. die **Informationsrechte** der zuständigen Behörden – jedenfalls teilweise – über die ausdrücklich normierten Dokumentationspflichten hinausgehen. Dies soll die **Behörden in die Lage versetzen**, die **Einhaltung der Anforderungen der KI-VO zu überprüfen**.

Insofern gilt, dass auch eine **fehlerhafte Nichteinstufung** einer KI-Anwendung bspw. als verbotene Praktik i. S. v. Art. 5 KI-VO (s. unten Ziff. 8.1.), als HRKS i. S. v. Art. 6 KI-VO oder als KI-System mit Transparenzrisiko i. S. v. 50 KI-VO (s. Ziff. 5.) dazu führen kann, dass die entsprechenden **Bestimmungen der KI-VO verletzt** werden. Vor diesem Hintergrund scheint es empfehlenswert, eine entsprechende Dokumentation vorzuhalten, um einen Überblick über eingesetzte KI-Anwendungen und deren Risikoeinstufung zu behalten, auf dieser Grundlage Verwendungshinweise für die Mitarbeitenden zu formulieren und die Einhaltung der KI-VO gegenüber den zuständigen Behörden ggf. nachweisen zu können.

Darüber hinaus verpflichtet **Art. 4 KI-VO** die Anbieter und Betreiber von KI-Systemen zur Vermittlung von KI-Kompetenzen an ihre Mitarbeitenden (s. Ziff. 6.). Der Umfang dieser Pflicht hängt auch von der Risikostufe (Hochrisiko, Transparenzrisiko, geringes Risiko) ab. Um **angemessene Kompetenzbildungsmaßnahmen** auf den Weg bringen zu können, ist ein Überblick über die relevanten KI-Systeme und deren **Risikostufe** erforderlich (s. Ziff. 6.2.).

Neben den Überwachungsbefugnissen der zuständigen Behörden ist zu bedenken, dass die KI-VO für Verstöße gegen Anbieter- und Betreiberpflichten **Sanktionen** vorsieht, vgl. Art. 99, 101 KI-VO. Die KI-VO stellt es zwar in das Regulierungsermessen der Mitgliedstaaten, in welchem **Umfang gegen Behörden und öffentliche Stellen**, die in dem betreffenden Mitgliedstaat niedergelassen sind, **Geldbußen** verhängt werden können, vgl. Art. 99 Abs. 8 KI-VO.[88] Im Schrifttum wird aber betont, dass es bereits dem Wortlaut, erst recht aber dem Telos von Art. 99 Abs. 8 KI-VO wider-

87 Eine freiwillige „Transparenzdatenbank“ über bestimmte KI-Systeme in der Bundesverwaltung führt das Bundesministerium des Innern und für Heimat: https://maki.beki.bund.de/a/bmi-makimo-app. Vgl. zum Ziel der Transparenz hinsichtlich der behördlichen Nutzung von KI auch: Leitlinien für den Einsatz Künstlicher Intelligenz in der Bundesverwaltung, Bundesministerium des Innern, 27. März 2025, S. 22.

88 Der Referentenentwurf der Vorgängerregierung für das Durchführungsgesetz zur KI-VO enthielt hierzu keine ausdrückliche Regelung, sondern verwies allgemein auf die Geltung des Ordnungswidrigkeitengesetzes. Vgl. Referentenentwurf, KI-VO-Durchführungsgesetz, Stand 4. Dezember 2024.

spreche, innerstaatlich keine oder eine auf null reduzierte Geldbuße für die öffentliche Hand vorzusehen.[89] Sofern die Bußgeldtatbestände für Behörden anwendbar sein sollten, gilt, dass sie voraussichtlich von einer vorsätzlichen oder **fahrlässigen Begehung** abhängen würden.[90] Auch mit Blick auf eine etwaige Exkulpation scheint eine Dokumentation der Risikoeinstufung verwendeter KI-Anwendungen daher sinnvoll.

Schließlich sieht auch die **eigene KI-Strategie der Kommission** („Künstliche Intelligenz in der Europäischen Kommission" (AI@EC)) die **Klassifizierung und Bewertung** bereits verwendeter oder zukünftiger KI-Systeme auf der Grundlage eines risikobasierten Ansatzes und unter Einhaltung der operativen Leitlinien der Kommission vor.[91] Zu den insofern anvisierten operativen Maßnahmen zählen die Erstellung und Pflege eines **aktuellen Registers der KI-Systeme**, die in der Kommission in Gebrauch sind, und deren Bewertung anhand der kommissionsweiten Leitlinien und rechtlichen Anforderungen.[92]

5. Transparenzpflichten hinsichtlich des Outputs bzw. der Interaktion von KI-Anwendungen mit dem Menschen

Neben den auf die KI-Systeme und ihre grundsätzliche Funktionsweise bezogenen Registrierungs- bzw. Dokumentationspflichten (s. oben Ziff. 3. und 4.) sieht **Art. 50 KI-VO Transparenz- bzw. Kennzeichnungspflichten** gegenüber Betroffenen vor.

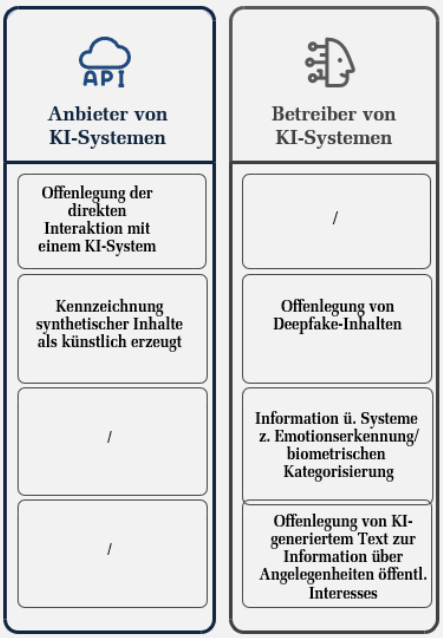
---

89 *Kasper,* Die Verwaltung in der KI-Regulierung, DÖV 2025, S. 471 (472). Vgl. *Meyberg*, in: BeckOK OWiG, Graf, 46. Edition, Stand: 1. April 2025, § 30 OWiG, Rn. 24, dazu, dass auch juristische Personen des öffentlichen Rechts Adressat einer Verbandsgeldbuße sein können.

90 Art. 99 KI-VO stellt nicht explizit auf ein vorsätzliches oder fahrlässiges Verhalten als Voraussetzung für die Sanktionsverhängung ab, sondern nennt dieses nur bezüglich der Strafzumessung. Im Schrifttum wird aber vertreten, dass die Verhängung von Geldbußen – da es sich um Strafrecht i. w. S. handele – Vorsatz oder Fahrlässigkeit voraussetze, vgl. *Anderl/Ciarnau*, in: Zankl, KI-VO, 2025, Art. 99 KI-VO, Rn. 16. Für diese Auslegung dürfte das Urteil des EuGH vom 5. Dezember 2023, Rs. C-683/21, Nacionalinis visuomenės sveikatos centras prie Sveikatos apsaugos ministerijos, Rn. 60 ff., zum ähnlich formulierten Art. 83 DSGVO sprechen. Danach kommt ein Bußgeld nur bei schuldhaftem Verhalten in Frage.

91 Kommission, Künstliche Intelligenz in der Europäischen Kommission (AI@EC) – Eine strategische Zielvorstellung für die Förderung der Entwicklung und Verwendung rechtskonformer, sicherer und vertrauenswürdiger Systeme der künstlichen Intelligenz in der Europäischen Kommission, KOM(2024) 380 endg., 24. Januar 2024, S. 5.

92 Kommission, Künstliche Intelligenz in der Europäischen Kommission (AI@EC) – Eine strategische Zielvorstellung für die Förderung der Entwicklung und Verwendung rechtskonformer, sicherer und vertrauenswürdiger Systeme der künstlichen Intelligenz in der Europäischen Kommission, KOM(2024) 380 endg., 24. Januar 2024, S. 5.



Transparenzpflichten nach Art. 50 KI-VO

Es geht darum, kenntlich zu machen, dass bestimmte Outputs KI-generiert sind bzw. dass Menschen gerade mit einem KI-System interagieren.

Art. 50 KI-VO sieht Regelungen für **Anbieter** (Abs. 1 und 2) und **Betreiber** (Abs. 3 und 4) bestimmter KI-Systeme vor. Es geht um KI-Systeme mit **Transparenzrisiko**, also um Systeme, die mit einem besonderen Manipulationsrisiko verbunden sind.[93] Hintergrund der Regelung ist, dass bestimmte **KI-Systeme**, die mit **natürlichen Personen interagieren** oder **Inhalte erzeugen** sollen, unabhängig von ihrer Einstufung als hochriskant ein **besonderes Risiko in Bezug auf Identitätsbetrug oder Täuschung** bergen können (ErwG 132 Satz 1 KI-VO).[94]

Die ab dem **2. August 2026** geltenden spezifischen Kennzeichnungspflichten werden nachfolgend aufgegliedert nach Anbieter- bzw. Betreibereigenschaft und Art des KI-Systems dargestellt. Punktuelle Ausnahmen gelten jeweils für die „Aufdeckung, Verhütung, Ermittlung oder Verfolgung von Straftaten“ (Abs. 1 Satz 2; Abs. 2 Satz 3; Abs. 3 Satz 2; Abs. 4 UAbs. 1 Satz 2; Abs. 4 UAbs. 1 Satz 2; ErwG 132 Satz 2 KI-VO).

5.1. Kennzeichnungspflichten für Anbieter von KI-Systemen, die für die direkte Interaktion mit natürlichen Personen bestimmt sind (Abs. 1)

Nach Art. 50 Abs. 1 Satz 1 KI-VO müssen **Anbieter** von KI-Systemen, die für die direkte Interaktion mit natürlichen Personen bestimmt sind (z. B. **Chatbots**, KI-basierte Assistenzsysteme, Pflegeroboter)[95], sicherstellen, dass die betreffenden Personen darüber **informiert werden, dass sie mit einem KI-System interagieren**.

Dies gilt nicht, wenn die Interkation mit einem KI-System aufgrund der Umstände und des Kontexts der Nutzung **offensichtlich** ist. Zur Beurteilung der Offensichtlichkeit ist entsprechend dem europäischen Verbraucherleitbild auf eine natürliche Person abzustellen, die angemessen informiert, aufmerksam und umsichtig ist (vgl. Art. 50 Abs. 1 Satz 1 2. Hs., ErwG 132 Satz 3 KI-VO).[96]

---

93 *Kumkar/Griesel*, Transparenzpflichten für Deepfakes und synthetische Medieninhalte in der KI-VO, KIR 2024, S. 117 (119).

94 Vgl. näher: *Martini*, in: Martini/Wendehorst, Verordnung über künstliche Intelligenz, 2024, Art. 50 KI-VO, Rn. 2 ff.

95 Vgl. *Martini*, in: Martini/Wendehorst, Verordnung über künstliche Intelligenz, 2024, Art. 50 KI-VO, Rn. 46, 48; *Leissler/Stahleder*, in: Zankl, KI-VO, 2025, Art. 50 KI-VO, Rn. 3.

96 *Merkle*, Transparenz nach der KI-Verordnung – von der Blackbox zum Open-Book?, RDi 2024, S. 414 (418).

Nach ErwG 132 Satz 4 KI-VO sollten die Merkmale von natürlichen Personen berücksichtigt werden, die aufgrund ihres Alters oder einer Behinderung **schutzbedürftigen Gruppen** angehören, soweit das KI-System auch mit diesen Gruppen interagieren soll.

Im Schrifttum wird die Ansicht vertreten, dass Offensichtlichkeit bei einem mit Menschen agierenden Roboter, **nicht** aber bei **Chatbots** gegeben sei. Bei diesen sei daher über die KI-Eigenschaft zu informieren.[97]

5.2. Kennzeichnungspflichten für Anbieter von KI-Systemen, die synthetische Audio-, Bild-, Video- oder Textinhalte erzeugen oder manipulieren (Abs. 2)

Nach Art. 50 Abs. 2 Satz 1 KI-VO müssen **Anbieter** von KI-Systemen – einschließlich solcher mit allgemeinem Verwendungszweck –, die **synthetische Audio-, Bild-, Video- oder Textinhalte erzeugen**, sicherstellen, dass diese Inhalte in einem **maschinenlesbaren Format gekennzeichnet** sind und als **künstlich erzeugt oder manipuliert erkennbar** sind. Die Norm wird als Reaktion auf die Entwicklung im Bereich **generativer KI** wie **ChatGPT** eingestuft[98] (vgl. auch ErwG 133 Sätze 1 bis 3 KI-VO).

Zur **technischen Umsetzung** dieser Pflicht heißt es in Art. 50 Abs. 2 Satz 2 KI-VO, dass die technischen Lösungen – soweit technisch möglich – „wirksam, interoperabel, belastbar und zuverlässig“ sein müssen, wobei die Besonderheiten und Beschränkungen der verschiedenen Arten von Inhalten, die Umsetzungskosten und der allgemein anerkannte Stand der Technik zu berücksichtigen sind. Als mögliche Techniken nennt ErwG 133 Satz 4 KI-VO Wasserzeichen, Metadatenidentifizierungen, kryptografische Methoden zum Nachweis der Herkunft und Authentizität des Inhalts, Protokollierungsmethoden, Fingerabdrücke oder andere Techniken, oder je nach Sachlage eine Kombination solcher Techniken.[99]

Nach Art. 50 Abs. 2 Satz 3 1. und 2. Alternative KI-VO gilt die Pflicht nicht, soweit die KI-Systeme eine **unterstützende Funktion für die Standardbearbeitung** ausführen oder die vom Betreiber bereitgestellten Eingabedaten bzw. deren **Semantik nicht wesentlich verändern** (vgl. auch ErwG 133 Satz 7 KI-VO). Nach Einschätzung im Schrifttum geht es um Fälle, in denen das KI-System die **authentischen Inhalte nur marginal verändert** (bspw. Filter in Foto-Apps oder **Rechtschreib- und Grammatikprüfungen**, **Filter- und Sortierfunktionen**).[100]

---

97 *Martini*, in: Martini/Wendehorst, Verordnung über künstliche Intelligenz, 2024, Art. 50 KI-VO, Rn. 51 f.

98 *Martini*, in: Martini/Wendehorst, Verordnung über künstliche Intelligenz, 2024, Art. 50 KI-VO, Rn. 57.

99 Vgl. näher: *Martini*, in: Martini/Wendehorst, Verordnung über künstliche Intelligenz, 2024, Art. 50 KI-VO, Rn. 65 ff.

100 *Martini,* in: Martini/Wendehorst, Verordnung über künstliche Intelligenz, 2024, Art. 50 KI-VO, Rn. 68; *Leissler/Stahleder*, in: Zankl, KI-VO, 2025, Art. 50 KI-VO, Rn. 11.

5.3. Kennzeichnungspflichten für Betreiber von KI-Systemen zur Emotionserkennung oder biometrischen Kategorisierung (Abs. 3)

Art. 50 Abs. 3 Satz 1 KI-VO schreibt vor, dass **Betreiber** von KI-Systemen zur **Emotionserkennung** oder zur **biometrischen Kategorisierung** die betroffenen natürlichen Personen über den Betrieb des Systems informieren müssen. Ein Emotionserkennungssystem ist nach Art. 3 Nr. 39 KI-VO „ein KI-System, das dem Zweck dient, Emotionen oder Absichten natürlicher Personen auf der Grundlage ihrer biometrischen Daten festzustellen oder daraus abzuleiten." Ein System zur biometrischen Kategorisierung ist nach Art. 3 Nr. 40 KI-VO „ein KI-System, das dem Zweck dient, natürliche Personen auf der Grundlage ihrer biometrischen Daten bestimmten Kategorien zuzuordnen, sofern es sich um eine Nebenfunktion eines anderen kommerziellen Dienstes handelt und aus objektiven technischen Gründen unbedingt erforderlich ist." Nach ErwG 132 Satz 6 KI-VO können solche spezifischen Kategorien Aspekte wie etwa **Geschlecht, Alter, Haarfarbe, Augenfarbe, Tätowierungen, persönliche Merkmale, ethnische Herkunft sowie persönliche Vorlieben und Interessen** betreffen.

Hintergrund der Bestimmung ist, dass es sich bei den biometrischen Daten typischerweise um besonders schutzbedürftige Kategorien personenbezogener Daten i. S. v. Art. 9 DSGVO handelt, weshalb dem Einzelnen die Entscheidungsfreiheit zu gewährleisten ist, sich solchen Systemen auszusetzen.[101]

5.4. Kennzeichnungspflichten von Betreibern für Deepfakes (Abs. 4 UAbs. 1)

Art. 50 Abs. 4 UAbs. 1 KI-VO regelt die Kennzeichnung sog. **Deepfakes**: Nach Art. 50 Abs. 4 UAbs. 1 Satz 1 KI-VO müssen Betreiber eines KI-Systems, das **Bild-, Ton- oder Videoinhalte erzeugt oder manipuliert,** die ein Deepfake sind, offenlegen, dass die Inhalte künstlich erzeugt oder manipuliert wurden. Was unter einem **Deepfake** zu verstehen ist, ist in **Art. 3 Nr. 60 KI-VO** definiert Danach handelt es sich bei einem Deepfake um einen durch KI erzeugten oder manipulierten Bild-, Ton- oder Videoinhalt, der wirklichen Personen, Gegenständen, Orten, Einrichtungen oder Ereignissen ähnelt und einer Person fälschlicherweise als echt oder wahrheitsgemäß erscheinen würde.[102]

Ein **Deepfake** gemäß Art. 3 Nr. 60 KI-VO ist ein

- durch KI erzeugter oder manipulierter Bild-, Ton- oder Videoinhalt,
- der wirklichen Personen, Gegenständen, Orten, Einrichtungen oder Ereignissen ähnelt
- und einer Person fälschlicherweise als echt oder wahrheitsgemäß erscheinen würde.

Hintergrund der Regelung ist, dass sich Deepfakes durch den technischen Fortschritt in der jüngeren Vergangenheit stark verbreitet haben. Die synthetisch erstellten Fotos, Vi-

101 Vgl. *Martini*, in: Martini/Wendehorst, Verordnung über künstliche Intelligenz, 2024, Art. 50 KI-VO, Rn. 70 ff., auch zum sonstigen Regelungsrahmen der KI-VO bezüglich biometrischer Daten und zu den Anforderungen der DSGVO.

102 Vgl. näher: *Martini*, in: Martini/Wendehorst, Verordnung über künstliche Intelligenz, 2024, Art. 50 KI-VO, Rn. 99 ff. Vgl. auch: Fachbereich Europa, Transparenzpflichten bei der Nutzung KI-generierter bildlicher Darstellungen in Werbekampagnen, EU 6 - 3000 - 034/24, 2. September 2024.

deos und Audioaufnahmen sind so realistisch, dass sie sich nur mit Schwierigkeiten von authentischen Medieninhalten unterscheiden lassen.[103] Die daraus folgenden **Risiken** werden als erheblich eingestuft: Es drohten – gerade im politischen Kontext – Persönlichkeitsrechtsverletzungen, Reputationsschäden, fehlerhafte Attribution von Geschehnissen oder Charaktereigenschaften sowie Desinformationskampagnen.[104]

Gemäß Art. 50 Abs. 4 UAbs. 1 Satz 3 KI-VO besteht jedoch eine **eingeschränkte Transparenzpflicht** bei Inhalten, die Teil eines **offensichtlich künstlerischen, kreativen, satirischen, fiktionalen oder analogen Werks oder Programms** sind. In diesem Fall beschränken sich die Transparenzpflichten darauf, das Vorhandensein von Deepfakes in einer geeigneten Weise offenzulegen, die die Darstellung oder den Genuss des Werks nicht beeinträchtigt.

Als eine Umsetzungsoptionen wird im Schrifttum die Nutzung von sog. **Content Credentials** genannt, die über einen Button abgerufen werden können.[105] Dabei handelt es sich um digitale Informationen, die an ein digitales Medium (z. B. Bild, Video, Audio, Text) angehängt werden, um **Herkunft, Urheberschaft, Bearbeitungsschritte und Authentizität** nachvollziehbar zu machen. Sie basieren auf offenen Standards, die beispielsweise von der **Coalition for Content Provenance and Authenticity (C2PA),**[106] einem Zusammenschluss von Unternehmen wie Adobe, Microsoft, BBC und Intel, entwickelt wurden. Die Software fügt Metadaten zu einem Medium hinzu, die den Ursprung des Inhalts belegen (z. B. „von einer KI generiert“ und Zeitpunkt der Erstellung). Es verwendet digitale Signaturen, die nicht nachträglich manipuliert werden können, und bietet ein einheitliches Format, das von verschiedenen Plattformen gelesen und angezeigt werden kann.[107]

5.5. Kennzeichnungspflichten von Betreibern hinsichtlich künstlich erzeugter oder manipulierter Texte zur Information über Angelegenheiten öffentlichen Interesses (Abs. 4 UAbs. 2)

Transparenzpflichten unterliegen auch **Betreiber eines KI-Systems, das Text erzeugt oder manipuliert, der veröffentlicht wird**, **um die Öffentlichkeit über Angelegenheiten von öffentlichem Interesse** zu informieren, vgl. Art. 50 Abs. 4 UAbs. 2 Satz 1 KI-VO. Sie müssen offenlegen, dass der Text künstlich erzeugt oder manipuliert wurde. Die eigenständige Vorschrift für reine Textinhalte wurde im Trilog-Verfahren nachträglich ergänzt.[108]

---

103 *Kumkar/Griesel*, Transparenzpflichten für Deepfakes und synthetische Medieninhalte in der KI-VO, KIR 2024, S. 117.

104 *Martini*, in: Martini/Wendehorst, Verordnung über künstliche Intelligenz, 2024, Art. 50 KI-VO, Rn. 94 ff.; *Kumkar/Griesel*, Transparenzpflichten für Deepfakes und synthetische Medieninhalte in der KI-VO, KIR 2024, S. 117 (118).

105 *Merkle*, Transparenz nach der KI-Verordnung – von der Blackbox zum Open-Book?, RDi 2024, S. 414 (420).

106 Siehe Website der C2PA.

107 Vgl. darüber hinaus zu den Anforderungen an die Offenlegung: *Martini*, in: Martini/Wendehorst, Verordnung über künstliche Intelligenz, 2024, Art. 50 KI-VO, Rn. 104 ff.

108 *Kumkar/Griesel*, Transparenzpflichten für Deepfakes und synthetische Medieninhalte in der KI-VO, KIR 2024, S. 117 (119).

Wann ein Text eine „**Angelegenheit von öffentlichem Interesse**“ betrifft, wird in der KI-VO nicht näher konkretisiert. Ziel der Vorschrift ist es, „den öffentlichen Diskurs vor einer Erosion des Vertrauens in die Integrität meinungsbildungsrelevanter Inhalte zu schützen“.[109] Insofern dürften der Adressatenkreis und der Inhalt des Texts maßgeblich sein: Im Gegensatz zu Texten mit überschaubarem Adressatenkreis dürften Posts in sozialen Netzwerken in den Anwendungsbereich der Norm fallen. Das Inhaltskriterium dürfte insbesondere Themen mit Relevanz für die öffentliche Meinungsbildung bzw. den demokratischen Diskurs erfassen. Im Schrifttum geht man davon aus, dass hierunter „**jedenfalls politische, gesellschaftliche, wirtschaftliche und kulturelle Angelegenheiten** fallen, die **über ein kleines (Fach-)Publikum hinauswirken**“.[110] Eine wichtige Indizfunktion komme der Frage zu, ob und inwieweit die Angelegenheit im öffentlichen Diskurs Widerhall finde.[111] Andere Stimmen im Schrifttum gehen davon aus, dass der Begriff voraussichtlich weit ausgelegt werde, sodass bspw. die meisten Presseartikel der Transparenzpflicht unterfallen würden.

Nach ErwG 134 Satz 4 KI-VO gilt die Kennzeichnungspflicht jedoch dann nicht, wenn die durch KI erzeugten Inhalte einem Verfahren der **menschlichen Überprüfung** oder **redaktionellen Kontrolle** unterzogen wurden und eine **natürliche oder juristische Person** die **redaktionelle Verantwortung** für die Veröffentlichung der Inhalte trägt.[112]

Die **Umsetzung** der Offenlegung ist dem Betreiber überlassen. Denkbar wären etwa explizite Hinweise im Text oder in einer Fußnote (z.B. „Dieser Artikel wurde ganz oder teilweise mit Hilfe künstlicher Intelligenz erstellt“), die Verwendung von Symbolen oder Labels (z. B. „AI“ oder „AI-assisted“) oder Einträge in den Metadaten (kryptografische Wasserzeichen).[113] Letztere gelten bei Textinhalten weniger effektiv als bei Bilddateien, da diese bei Prozessen wie Formatierung, Kopieren und Einfügen nicht mitübertragen werden.[114]

5.6. Form der Kennzeichnung und Konkretisierung durch Praxisleitfäden (Abs. 5, 8)

Wie unter Ziff. 4.1.1. bis 4.1.5. deutlich wurde, befasst sich Art. 50 KI-VO mehr mit dem „Ob“ als mit dem „Wie“ der Kennzeichnung.[115] Die Modalitäten der Kennzeichnung sind weitgehend den Verpflichteten überlassen. Aus Art. 50 Abs. 5 KI-VO ergeben sich aber **Rahmenbedingungen**:

---

109 *Martini*, in: Martini/Wendehorst, Verordnung über künstliche Intelligenz, 2024, Art. 50 KI-VO, Rn. 113.

110 *Martini*, in: Martini/Wendehorst, Verordnung über künstliche Intelligenz, 2024, Art. 50 KI-VO, Rn. 113.

111 *Martini*, in: Martini/Wendehorst, Verordnung über künstliche Intelligenz, 2024, Art. 50 KI-VO, Rn. 113.

112 Vgl. auch: *Leissler/Stahleder*, in: Zankl, KI-VO, 2025, Art. 50 KI-VO, Rn. 19.

113 Im Internet finden sich diverse Leitfäden von Universitäten zur Verwendung von KI in wissenschaftlichen Publikationen. Vgl. etwa: https://lehren-und-lernen-mit-ki.uni-graz.at/de/ki-nutzung-kennzeichnen/; https://www.ulb.tu-darmstadt.de/forschen_publizieren/ki/index.de.jsp.

114 Vgl. *Molavi Vasse'i*, Watermarking von KI-generierten Inhalten als regulatorisches Instrument, RDi 2024, S. 406 (409).

115 *Merkle*, Transparenz nach der KI-Verordnung – von der Blackbox zum Open-Book?, RDi 2024, S. 414 (420).

Zu **Form und Zeitpunkt** der Kennzeichnung schreibt Art. 50 Abs. 5 Satz 1 KI-VO vor, dass die Informationen den betreffenden natürlichen Personen „**spätestens zum Zeitpunkt der ersten Interaktion oder Aussetzung in klarer und eindeutiger Weise bereitgestellt**“ werden müssen. Nach Art. 50 Abs. 5 Satz 2 KI-VO müssen die Informationen den „geltenden **Barrierefreiheitsanforderungen**“ entsprechen (vgl. auch ErwG 132 Satz 7 KI-VO).[116]

Angesichts der eher unbestimmten Vorgaben zur Umsetzung der Kennzeichnungspflichten besteht einerseits **Entscheidungsspielraum** aufseiten der Anbieter bzw. Betreiber hinsichtlich Art, Platzierung und Größe der Kennzeichnung.[117] Andererseits besteht auch **Rechtsunsicherheit und Konkretisierungsbedarf**. Insofern könnten die gemäß Art. 50 Abs. 7 KI-VO zu erarbeitenden Praxisleitfäden des Amts für KI oder die Leitlinien der Kommission nach Art. 96 Abs. 1 Buchst. d KI-VO für mehr Klarheit sorgen.[118]

5.7. Verhältnis zu sonstigen Kennzeichnungs- bzw. Transparenzpflichten (Abs. 6)

Die zuvor genannten Kennzeichnungs- und Transparenzpflichten (Art. 50 Abs. 1 bis 4 KI-VO) lassen die die Anforderungen und Pflichten bezüglich **HRKS** unberührt und berühren auch nicht andere Transparenzpflichten, die im Unionsrecht oder dem nationalen Recht für Betreiber von KI-Systemen festgelegt sind (Art. 50 Abs. 6 KI-VO).

Hinsichtlich der Regelungen für HRKS ist zum einen die **funktionale Transparenz** zu beachten, die Anbieter von HRKS gemäß **Art. 13 KI-VO** zu gewährleisten haben.[119] Nach Art. 13 Abs. 1 KI-VO sind HRKS so zu konzipieren und entwickeln, dass ihr Betrieb hinreichend transparent ist, damit die Betreiber die Ausgaben eines Systems angemessen interpretieren und verwenden können und damit die Anbieter und Betreiber die Pflichten aus der KI-VO erfüllen können.

Darüber hinaus ist für Betreiber von HRKS **Art. 26 Abs. 11 Satz 1 KI-VO** relevant. Danach haben Betreiber der in Anhang III KI-VO aufgeführten HRKS, die Entscheidungen bezüglich natürlicher Personen treffen oder bei solchen Entscheidungen Unterstützung leisten, die natürlichen Personen darüber zu informieren, dass sie der Verwendung des HRKS unterliegen (vgl. auch Art. 86 KI-VO).

---

116 Vgl. zu den Modalitäten: *Kumkar/Griesel*, Transparenzpflichten für Deepfakes und synthetische Medieninhalte in der KI-VO, KIR 2024, S 117 (122); *Martini*, in: Martini/Wendehorst, Verordnung über künstliche Intelligenz, 2024, Art. 50 KI-VO, Rn. 117 ff.

117 Vgl. *Kumkar/Griesel*, Transparenzpflichten für Deepfakes und synthetische Medieninhalte in der KI-VO, KIR 2024, S. 117 (121).

118 *Merkle*, Transparenz nach der KI-Verordnung – von der Blackbox zum Open-Book?, RDi 2024, S. 414 (417 f., 420).

119 Vgl. *Merkle*, Transparenz nach der KI-Verordnung – von der Blackbox zum Open-Book?, RDi 2024, S. 414 (417 f.).

6. Kompetenzbildung gemäß Art. 4 KI-VO

Art. 4 KI-VO normiert eine allgemeine Verpflichtung zur Kompetenzbildung. Danach müssen **Anbieter und Betreiber von KI-Systemen** „nach besten Kräften“ sicherstellen,

> „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“.[120]

Art. 4 KI-VO ist bereits am **2. Februar 2025** in Kraft getreten.

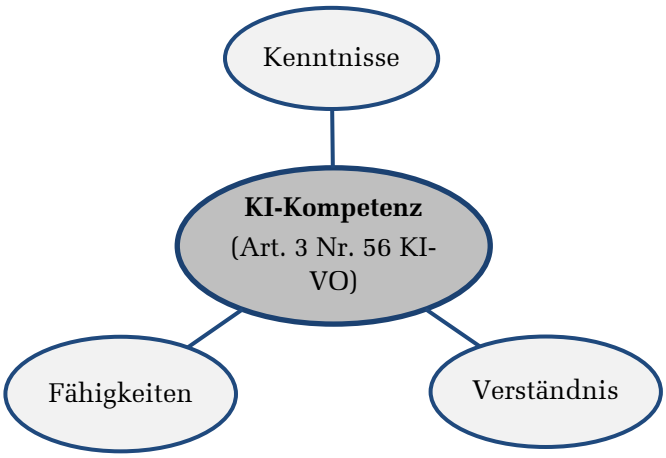
Der folgende Abschnitt geht näher auf den Umfang (Ziff. 6.1.) und die Kontextabhängigkeit (Ziff. 6.2.) der aus Art. 4 KI-VO folgenden Pflichten ein. Es wird beleuchtet, ob die KI-VO konkrete Lerninhalte oder -formate (Ziff. 6.3.) vorgibt und auf etwaige Best-Practice-Ansätze eingegangen (Ziff. 6.4.). Abschließend wird die Frage aufgeworfen, ob und in welcher Form die Kompetenzbildungsmaßnahmen dokumentiert werden sollten (Ziff. 6.5.).

6.1. Pflicht zur Herstellung ausreichender KI-Kompetenz

Die in Art. 4 KI-VO angesprochene **KI-Kompetenz** ist in Art. 3 Nr. 56 KI-VO legaldefiniert. Sie bezeichnet

> „die Fähigkeiten, die Kenntnisse und das Verständnis, die es Anbietern, Betreibern und Betroffenen […] ermöglichen, KI-Systeme sachkundig einzusetzen sowie sich der Chancen und Risiken von KI und möglicher Schäden, die sie verursachen kann, bewusst zu werden“.

Dimensionen der KI-Kompetenz nach Art. 3 Nr. 56 KI-VO



120 Vgl. zur Bedeutung der KI-Kompetenz für die technologische Entwicklung und Datenwirtschaft insgesamt – einschließlich des Einflusses auf Grund- und Menschenrechte – sowie zur Einordnung der KI-Kompetenz als gesamtgesellschaftliche Aufgabe: *Möller-Klapperich*, KI-Kompetenz, NJ 2025, S. 193 (193 f.).

Die Verpflichtung zum Aufbau von KI-Kompetenz gilt für **Anbieter und Betreiber** sowie für **alle KI-Systeme, unabhängig** von deren **Risikoeinstufung**.[121] Die Verpflichtung gilt zudem nicht nur für das **Personal**, sondern auch für **andere Personen**, die im Auftrag des Anbieters oder Betreibers mit dem Betrieb und der Nutzung von KI-Systemen befasst sind. Dies sind nach den **FAQ** der Kommission **zu Art. 4 KI-VO** Personen, bei denen es sich nicht um Arbeitnehmende handelt, sondern um Personen, die prinzipiell in den organisatorischen Zuständigkeitsbereich des Anbieters oder Betreibers fallen (bspw. **Auftragnehmer**, **Dienstleister** oder **Kunden**).[122]

Ziel der Verpflichtung ist es ausweislich ErwG 20 Satz 1 KI-VO, alle Anbieter, Betreiber und betroffene Personen mit den **notwendigen Konzepten** auszustatten, **um fundierte Entscheidungen über KI-Systeme zu treffen** und so den größtmöglichen Nutzen aus KI-Systemen zu ziehen. Gleichzeitig sollen Grundrechte, Gesundheit und Sicherheit gewahrt und eine demokratische Kontrolle ermöglicht werden.

Nach ErwG 20 Satz 2 KI-VO können **diese Konzepte** in Bezug auf den **jeweiligen Kontext unterschiedlich** sein und Folgendes umfassen:

- das Verstehen der korrekten Anwendung technischer Elemente in der **Entwicklungsphase** des KI-Systems;
- das Verstehen der bei der **Verwendung des KI-Systems** anzuwendenden Maßnahmen und der geeigneten Auslegung der Ausgaben des KI-Systems;
- im Falle betroffener Personen das nötige **Wissen, um zu verstehen**, wie sich mithilfe von KI getroffene Entscheidungen auf sie auswirken werden.

ErwG 20 Satz 3 KI-VO sieht vor, dass die KI-Kompetenz **allen einschlägigen Akteuren der KI-Wertschöpfungskette** die **Kenntnisse** vermitteln sollte, die **erforderlich** sind, um die **angemessene Einhaltung** und die **ordnungsgemäße Durchsetzung** der **KI-VO** sicherzustellen.[123]

6.2. Differenzierung nach Anwender, Kontext und Betroffenen

Es ergibt sich bereits aus Art. 4 i. V. m. ErwG 20 KI-VO, dass die Anforderungen an die KI-Kompetenz je nach der **Rolle und den Fähigkeiten des Anwenders**, dem **Kontext** des Einsatzes und

---

121 *Hense/Mustać*, AI Act kompakt, Compliance, management & use cases in corporate practice, 2025, S. 37; *Möller-Klapperich*, KI-Kompetenz, NJ 2025, S. 193 (194).

122 Kommission, AI Literacy – Questions & Answers.

123 Darüber hinaus heißt es in ErwG 20 Satz 4 KI-VO, dass die umfassende Umsetzung von KI-Kompetenzmaßnahmen und die Einführung geeigneter Folgemaßnahmen dazu beitragen könne, die Arbeitsbedingungen zu verbessern und die Konsolidierung und den Innovationspfad vertrauenswürdiger KI in der Union zu unterstützen. Letztlich soll damit die Gesamtheit der europäischen Bürgerinnen und Bürger dazu gebracht werden, sich kritisch und verantwortungsbewusst mit KI auseinanderzusetzen, indem Unternehmen und Behörden in die Pflicht genommen werden, vgl. *Hense/Mustać*, AI Act kompakt, Compliance, management & use cases in corporate practice, 2025, S. 38.

den **Betroffenen** variieren („einsatzgebiets- und personenrelative Formulierung“[124]). Die Formulierung, dass die Kompetenzbildungsmaßnahmen „**nach besten Kräften**“ zu ergreifen sind, wird im Schrifttum als „ressourcenabhängige Einschränkung der Schulungspflicht“ gedeutet.[125]

In den **Fragen und Antworten** (Frequently Asked Questions, FAQ) **der Kommission zu Art. 4 KI-VO** heißt es entsprechend, dass diese Norm darauf abziele, Schulungen und Hilfestellungen anzubieten, die dem **Wissensstand** und der **Art der Zielgruppen** sowie dem **Kontext** und dem **Zweck** der in der Organisation **verwendeten KI-Systeme** am besten entsprechen. Die verpflichteten Anbieter oder Betreiber sollten die **technischen Kenntnisse, Erfahrung und Ausbildung der Anwender**,[126] den **Kontext**, in dem die KI-Systeme eingesetzt werden sollen, und die **Personen, bei denen die KI-Systeme eingesetzt** werden sollen, berücksichtigen.[127]

Im Schrifttum hat bspw. *Schippel* folgende Zielgruppenanalyse vorgeschlagen:[128]

- **Betriebsmitarbeiter**: Mitarbeiter, die KI-Systeme im täglichen Betrieb nutzen, sollten geschult werden, um sie effektiv und sicher einsetzen zu können.

- **Datenanalysten**: Experten sollten große Datenmengen analysieren, Muster identifizieren, Erkenntnisse gewinnen und datenbasierte Entscheidungen zu unterstützen können.

- **Entscheidungsträger**: Führungskräfte und Manager, die strategische Entscheidungen im Zusammenhang mit KI-Systemen treffen, sollten ein Verständnis für die Risiken und Chancen von KI haben.

- **Entwickler von KI-Systemen:** Diese Mitarbeiter werden über fundierte technische Kenntnisse und Erfahrungen in der KI-Entwicklung verfügen.

- **IT-Sicherheitsexperten:** Fachleute, die für den Schutz von Informationssystemen und Daten vor Cyberangriffen und Sicherheitsrisiken verantwortlich sind, einschließlich der Sicherstellung der Integrität von KI-Anwendungen.

---

124 *Möller-Klapperich*, KI-Kompetenz, NJ 2025, S. 193 (195).

125 *Möller-Klapperich*, KI-Kompetenz, NJ 2025, S. 193 (197).

126 Vgl. Kommission, AI Literacy – Questions & Answers: Art. 4 KI-VO beinhalte zwar keine Pflicht, den KI-Wissensstand des Personals zu messen. Gleichwohl folge aus Art. 4 KI-VO die Pflicht von Anbietern und Betreibern von KI-Systemen, ein ausreichendes Maß an KI-Kompetenz zu gewährleisten, wobei das technische Wissen, die Erfahrung, die Aus- und Weiterbildung der Mitarbeitenden zu berücksichtigen seien.

127 Kommission, AI Literacy – Questions & Answers.

128 *Schippel*, Trainingsvorgaben: Wie kann man KI-Kompetenz nach Art. 4 KI-VO vermitteln?, KIR 2025, S. 119 (121).

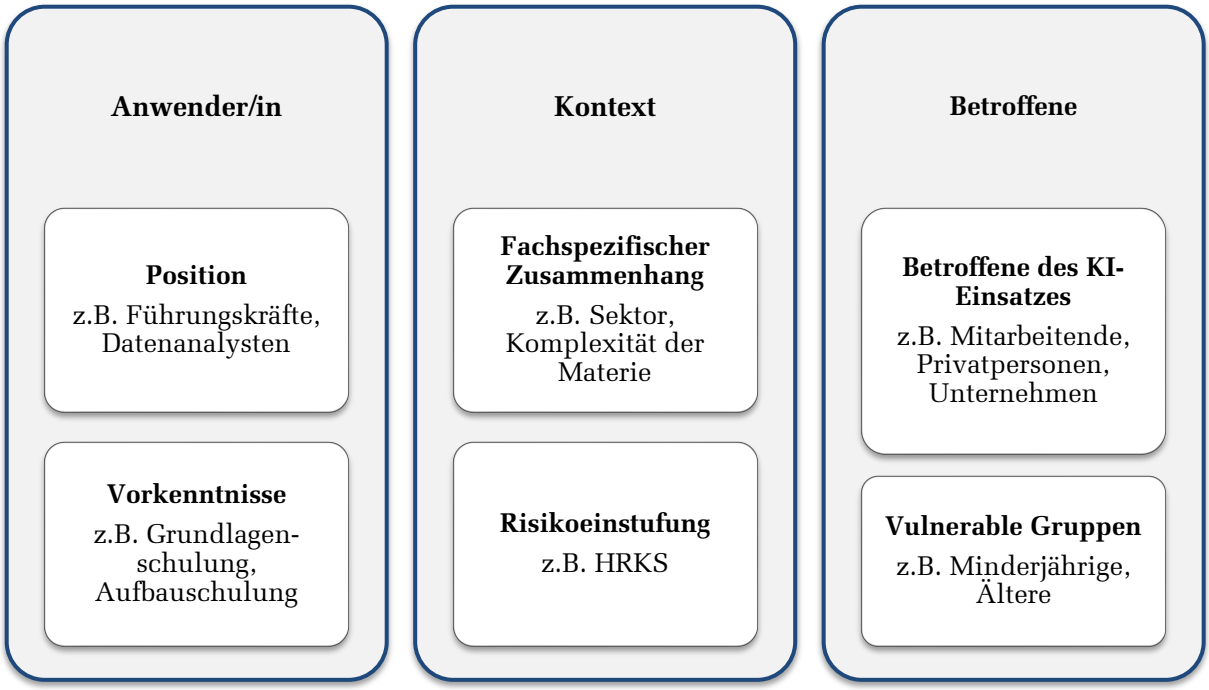
- **Mitarbeiter mit Kundenbezug:** Fachkräfte, die Kundenanfragen und -probleme bearbeiten, Unterstützung bieten und sicherstellen, dass die Kunden mit den Produkten oder Dienstleistungen des Unternehmens zufrieden sind, einschließlich der Nutzung von KI-gestützten Tools.

- **Produktmanager:** Verantwortliche, die die Entwicklung und Vermarktung von Produkten leiten.

- **Softwareentwickler:** Fachleute, die Softwareanwendungen entwerfen, entwickeln und implementieren.

Zum **Einsatzkontext** des KI-Systems gehört nach den **FAQ** der Kommission **zu Art. 4 KI-VO** auch eine **Risikobewertung**. Wenn beispielsweise die KI-Systeme der Organisation ein hohes Risiko darstellen, könnten gemäß Kapitel III der KI-VO zusätzliche Maßnahmen relevant sein, um sicherzustellen, dass die Mitarbeitenden wissen, wie sie mit den jeweiligen KI-Systemen umgehen müssen, und um Risiken zu vermeiden und/oder zu mindern.[129]

Faktoren, die es beim Zuschnitt der Kompetenzbildungsmaßnahmen zu berücksichtigen gilt



129 Kommission, AI Literacy – Questions & Answers.

6.3. Zur Frage konkreter Lerninhalte und Lernformate

Art. 4 KI-VO macht keine Vorgaben zu **konkreten Lerninhalten oder Lernformaten**.

Auf die Frage, ob das Amt für KI Leitlinien zu Art. 4 KI-VO ausarbeiten werde, heißt es in den FAQ der Kommission zu Art. 4 KI-VO, dass eine Orientierung bis auf Weiteres durch **Praxisbeispiele**, **Webinare** und **Klarstellungen in den FAQ** gewährleistet werde. Weitere Leitlinien zur Durchsetzung könnten von den **zuständigen nationalen Marktüberwachungsbehörden** bereitgestellt werden, sobald diese benannt seien. Das Amt für KI werde im Einklang mit Art. 66 Buchst. f und Art. 95 Abs. 2, 3 KI-VO eng mit dem Gremium für künstliche Intelligenz i. S. v. Art. 65 KI-VO zum Thema KI-Kompetenz zusammenarbeiten.

Die Kommission werde aber **Leitlinien** für die Anwendung der in Art. 8 bis 15 und Art. 25 KI-VO normierten Anforderungen an **HRKS** veröffentlichen, die bspw. hinsichtlich der menschlichen Aufsicht (Art. 14 KI-VO) und des Risikomanagements (Art. 9 KI-VO) auch Fragen der KI-Kompetenz beträfen.[130]

Weiter heißt es in den FAQ zu Art. 4 KI-VO, dass das Amt für KI **keine strikten Vorgaben** in Bezug auf Art. 4 KI-VO und dessen „ausreichendes Niveau an KI-Kompetenz“ machen werde. Im Gegenteil halte es ein gewisses Maß an Flexibilität für notwendig, wenn man das breite Themenfeld der KI-Kompetenz und die sich schnell entwickelnde KI-Kompetenz bedenke.

6.3.1. Mindestanforderungen laut den FAQ der Kommission zu Art. 4 KI-VO

Ungeachtet des vorstehenden flexiblen Ansatzes hat die Kommission Mindestanforderungen an die Erfüllung der Weiterbildungspflicht formuliert. Anbieter und Betreiber sollten nach Ansicht der Kommission **mindestens folgende Anforderungen** erfüllen:

- **Gewährleistung eines allgemeinen Verständnisses von KI** in ihrer Organisation: Was ist KI? Wie funktioniert sie? Welche KI wird in der Organisation eingesetzt? Was sind die Chancen und Gefahren?

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

- **Berücksichtigung des Risikos** der bereitgestellten oder betriebenen **KI-Systeme**: Was müssen Mitarbeitende wissen, wenn sie mit einem solchen KI-System zu tun haben? Was sind die Risiken, derer sie sich bewusst sein müssen, und müssen sie Minderungsmaßnahmen kennen?

- Konkreter Aufbau von **KI-Kompetenzmaßnahmen** auf Grundlage der vorhergehenden Analyse unter Berücksichtigung der folgenden Aspekte:

130 Kommission, AI Literacy – Questions & Answers.

- **die Unterschiede bei den technischen Kenntnissen**, der Erfahrung, der Aus- und Weiterbildung des Personals und anderer Personen (Wie viel wissen die Mitarbeitenden/die anderen Personen über KI und die verwendeten KI-Systeme? Was sollten sie sonst noch wissen?);

- **der Kontext**, in dem die KI-Systeme verwendet werden sollen, und der betroffenen Personen, bei denen die KI-Systeme verwendet werden sollen (In welchem Sektor und zu welchem Zweck/Dienst wird das KI-System verwendet?).

Die vorgenannten Erwägungen umfassen **rechtliche und ethische Aspekte**, weshalb nach den FAQ zu Art. 4 KI-VO die **Vermittlung eines Verständnisses der KI-VO** und von Grundsätzen von **Ethik** und **Governance** empfohlen werden.

6.3.2. Einzelaspekte in den FAQ der Kommission zu Art. 4 KI-VO

Die weiteren Antworten der Kommission in ihren FAQ zu Art. 4 KI-VO hinsichtlich der KI-Kompetenzbildung sind **Ausdruck des flexiblen Ansatzes** und der unter Ziff. 6.3.1. dargestellten Mindestanforderungen.[131]

Auf die Frage, ob eine **KI-Schulung** (AI training) nach Art. 4 KI-VO **verpflichtend** sei, heißt es, dass dies von der unter Ziff. 6.3.1. dargestellten **Analyse abhänge**. In vielen Fällen könne 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 sei darauf ausgelegt, Schulungen und Anleitungen anzubieten, die dem Wissensstand und der Art der Zielgruppen sowie dem Kontext und dem Zweck der in der Organisation verwendeten KI-Systeme am besten entsprechen. Dies stehe im Einklang mit anderen Bestimmungen der KI-VO. So verpflichte bspw. **Art. 26 Abs. 2 KI-VO** die **Betreiber von HRKS**, sicherzustellen, dass das Personal in der Praxis ausreichend geschult sei, um mit dem System umzugehen und die **menschliche Aufsicht** zu gewährleisten (Art. 14 KI-VO). Sich auf die Gebrauchsanweisung zu verlassen, reiche in diesem Fall nicht aus.

Auch auf die Frage nach dem **Schulungsformat** gebe es **keine einheitliche Antwort**. Das Amt für KI habe nicht die Absicht, strenge Anforderungen oder obligatorische Schulungen vorzuschreiben. In Anbetracht der Unterschiede zwischen den potenziell eingesetzten KI-Systemen und der Tatsache, dass der Kenntnis- und Erfahrungsstand sowie die Art der Ausbildung und Schulung der Mitarbeitenden variieren könnten, sei es angemessen, **verschiedene Schulungsniveaus** oder **Lernansätze** zu verwenden. Die Anforderungen an eine Schulung hingen vom konkreten Kontext ab. **Anregungen** könnten die im „**Living Repository zur KI-Kompetenz**“ gesammelten Praktiken liefern (s. Ziff. 6.4.1.).[132]

Auch auf die Frage, ob im Auftrag des Betreibers handelnde Dienstleister vertraglich verpflichtet sein sollten, ihre KI-Kompetenz nachzuweisen, heißt es, dass dies von der konkreten Art des KI-

131 Vgl. im Einzelnen: Kommission, AI Literacy – Questions & Answers.

132 Dieses ist hier abrufbar: https://digital-strategy.ec.europa.eu/en/library/living-repository-foster-learning-and-exchange-ai-literacy.

Systems und dem Risiko abhänge. Im Allgemeinen müssten Personen, die ebenso wie die Arbeitnehmer für einen Dienstleister oder Auftragnehmer arbeiteten, über die entsprechenden KI-Kenntnisse verfügen, um die betreffende Aufgabe zu erfüllen .

Zu der Frage, ob ein Unternehmen, dessen Mitarbeitende **ChatGPT** z. B. zum Schreiben von Werbetexten oder **zum Übersetzen von Texten** verwenden, die Anforderungen an die KI-Kompetenz einhalten müsse, heißt es in den FAQ zu Art. 4 KI-VO, dass die Mitarbeitenden **über die spezifischen Risiken**, z. B. bezüglich sog. „**KI-Halluzinationen**“, informiert werden sollten.

Bei Personen mit einem Abschluss oder Erfahrung im Bereich der KI-Entwicklung könne zwar grundsätzlich davon ausgegangen werden, dass sie die erforderliche KI-Kompetenz besitzen. Letztlich hänge dies aber vom jeweiligen KI-Tool und den spezifischen Qualifikationen der Personen ab. Zudem müsse die Geschwindigkeit der technologischen Entwicklungen berücksichtigt werden. Deshalb sollten Organisationen gleichwohl die unter Ziff. 6.3.1. dargestellte Analyse durchführen.[133]

6.4. Best Practices?

Bisher gibt es keine von der Kommission oder den deutschen Überwachungsbehörden ausdrücklich gebilligten Best Practices. Als Orientierung kommen das Living Repository of AI Literacy Practices (Ziff. 6.4.1.), die eigene KI-Strategie der Kommission (Ziff. 6.4.2.) und sonstige Ansätze im Schrifttum (Ziff. 6.4.3.) in Betracht.

6.4.1. Living Repository of AI Literacy Practices

Das sog. „**Living Repository of AI Literacy Practices**“ ist eine von der Kommission veröffentlichte (nicht vollständige) Sammlung von Kompetenzbildungsmaßnahmen, die von Mitgliedern des sog. KI-Pakts ergriffen werden.[134] Der KI-Pakt soll Interessenträger bei der Vorbereitung auf die Umsetzung der KI-VO unterstützen. Es geht u. a. darum, in vom **Amt für KI** organisierten **Webinaren**[135] – auch zur **KI-Kompetenz**[136] – bewährte Verfahren und interne Richtlinien auszutauschen.[137]

---

133 Zum Ganzen: Kommission, AI Literacy – Questions & Answers.

134 Dieses ist hier abrufbar: https://digital-strategy.ec.europa.eu/en/library/living-repository-foster-learning-and-exchange-ai-literacy.

135 Die Veranstaltungen sind hier abrufbar: https://digital-strategy.ec.europa.eu/en/policies/ai-pact-events.

136 Die Folien und das gestreamte Webinar zur Kompetenz können hier abgerufen werden: https://digital-strategy.ec.europa.eu/en/events/third-ai-pact-webinar-ai-literacy.

137 Vgl. zum Ganzen: Kommission, AI Pact.

Die im Repository zusammenstellten Ansätze sind nach den Hinweisen der Kommission allerdings nur als **Anregung** zu verstehen. Die Kommission betont, dass eine Übernahme der veröffentlichten Maßnahmen **keine Vermutung der Einhaltung von Art. 4 KI-VO begründe**. Die Veröffentlichung impliziere keinerlei Billigung oder Bewertung durch die Kommission.[138]

6.4.2. KI-Strategie der Kommission

Aufschluss darüber, was die Kommission selbst als Best Practices im Zusammenhang mit Art. 4 KI-VO erachtet, kann ihre eigene KI-Strategie geben.[139] Bestandteile dieser Strategie sind die „**Entwicklung einer Strategie für den Aufbau und die Erhaltung eines qualifizierten Personalbestands**“ und eine „**Bestandsaufnahme des möglichen Weiterbildungs-/Umschulungsbedarfs in verschiedenen Tätigkeitsbereichen**“. Dazu gehören u. a. die Ermittlung derzeit und künftig benötigter KI-Kompetenzen und das Erstellen eines besonderen Lernangebots, das eine praktische, leicht in Anspruch zu nehmende Beratung für das Personal auf allen Ebenen biete. Diese KI-Kompetenzen sollten auch bei künftigen Personaleinstellungen durchweg berücksichtigt werden. Darüber hinaus werde die Kommission besondere Qualifikationsprofile festlegen und dementsprechend Personal einstellen, das für die Entwicklung von KI-Tools innerhalb der Verwaltung benötigt werde.[140]

In den **FAQ zu Art. 4 KI-VO** werden auf dieser Grundlage bereits **umgesetzte Schritte** genannt:

- Einrichtung eines **internen KI-spezifischen Webportals** als **zentrale Anlaufstelle** für alle Mitarbeitenden für KI-bezogene Inhalte, d. h. KI-Leitlinien, KI-Schulungsressourcen, Veranstaltungen und Nachrichten.

- **Definition von KI-Lernpaketen** auf der Schulungsplattform der Kommission, die auf verschiedene **Zielgruppen zugeschnitten** sind, d. h. Generalist, Manager und Entwickler (Spezialist). Diese Pakete enthalten nach Angabe in den FAQ zu Art. 4 KI-VO eine kuratierte Liste relevanter Schulungen, die in „wesentlich“ (essential), „dringend empfohlen“ und „empfohlen“ eingestuft werden. Zusätzliche Schulungen und Aufzeichnungen von Webinaren seien auch auf der Plattform verfügbar.

- **Schulungen zu KI-Tools:** Es seien in einem spezifischen Abschnitt des KI-Portals die KI-Tools aufgeführt, die allen Mitarbeitern zur Verfügung stünden, einschließlich der relevanten Lernressourcen für jedes Tool. Es gebe regelmäßige Q&A-Sitzungen zur Verwendung von KI in der täglichen Arbeit.

---

138 Kommission, Living repository to foster learning and exchange on AI literacy, 4. Februar 2025; Kommission, AI talent, skills and literacy.

139 Kommission, Künstliche Intelligenz in der Europäischen Kommission (AI@EC) – Eine strategische Zielvorstellung für die Förderung der Entwicklung und Verwendung rechtskonformer, sicherer und vertrauenswürdiger Systeme der künstlichen Intelligenz in der Europäischen Kommission, KOM(2024) 380 endg., 24. Januar 2024.

140 Kommission, Künstliche Intelligenz in der Europäischen Kommission (AI@EC) – Eine strategische Zielvorstellung für die Förderung der Entwicklung und Verwendung rechtskonformer, sicherer und vertrauenswürdiger Systeme der künstlichen Intelligenz in der Europäischen Kommission, KOM(2024) 380 endg., 24. Januar 2024, S. 8.

– Es gebe eine **KI-Praxisgemeinschaft**, in der jede Person Fragen im Zusammenhang mit KI stellen und mit KI-Experten interagieren könne.[141]

6.4.3. Ansätze im Schrifttum

Nicht zuletzt angesichts der Auslegungs- und Konkretisierungsbedürftigkeit von Art. 4 KI-VO[142] gibt es diverse Beiträge im Schrifttum, die sich zu **Lerninhalten**, **Lernformaten** und der Frage positionieren, mit welchen **weiteren Maßnahmen** die Pflicht zur Herstellung ausreichender KI-Kompetenz erfüllt und dokumentiert werden kann.

Ohne Anspruch auf Vollständigkeit wird verwiesen auf:

– *Schippel*, Trainingsvorgaben: Wie kann man KI-Kompetenz nach Art. 4 KI VO vermitteln?, KIR 2025, S. 119 – 124;

– *Möller-Klapperich*, KI-Kompetenz, NJ 2025, S. 193 – 197;

– *Wendehorst,* in: Martini/Wendehorst, Verordnung über künstliche Intelligenz, 2024, Art. 4 KI-VO, Rn. 11 ff.;

– *Hense/Mustać*, AI Act kompakt, Compliance, management & use cases in corporate practice, 2025, S. 36 – 42.

In diesen Beiträgen wird bspw. darauf verwiesen, dass – sofern **externe Kurse gewählt** werden – auf die fachliche und pädagogische Qualität sowie auf den Zuschnitt auf die jeweiligen Bedürfnisse zu achten sei.[143] Neben den Schulungen wird empfohlen, weitere Maßnahmen zu ergreifen, etwa das Verfassen **interner Richtlinien und Standards** oder die **Benennung eines KI-Beauftragten** als Koordinator der Kompetenzbildung (s. Ziff. 7.1.).[144] In zeitlicher Hinsicht sei es wichtig, die Schulungen bereits vor dem Inverkehrbringen der KI-Systeme anzubieten und während des Betriebs der Systeme zu wiederholen sowie **stetig zu evaluieren** und zu optimieren.[145]

Diese Quellen können als **Orientierung** für die Ausarbeitung eines Konzepts zur Herstellung der KI-Kompetenz herangezogen werden. Es handelt sich aber **nicht** um von der Kommission bzw. nationalen Marktüberwachungsbehörden – und erst recht nicht von den Unionsgerichten – **anerkannte Best Practices**. Es bleibt abzuwarten, ob auf nationaler Ebene weitere Orientierung durch die zuständigen Marktüberwachungsbehörden gegeben wird.

---

141 Kommission, AI Literacy – Questions & Answers.

142 Vgl. *Möller-Klapperich*, KI-Kompetenz, NJ 2025, S. 193 (194).

143 Vgl. *Hense/Mustać*, AI Act kompakt, Compliance, management & use cases in corporate practice, 2025, S. 38.

144 *Wendehorst,* in: Martini/Wendehorst, Verordnung über künstliche Intelligenz, 2024, Art. 4 KI-VO, Rn. 12 ff.

145 *Schippel*, Trainingsvorgaben: Wie kann man KI-Kompetenz nach Art. 4 KI-VO vermitteln?, KIR 2025, S. 119 (120).

6.5. Dokumentation von Kompetenzbildungsmaßnahmen?

Die KI-VO schreibt eine Dokumentation ergriffener Kompetenzbildungsmaßnahmen **nicht ausdrücklich vor**. Zudem sind in den Art. 74 ff. KI-VO keine expliziten Befugnisse der zuständigen Behörden zur Durchsetzung von Art. 4 KI-VO vorgesehen und eine Missachtung von Art. 4 KI-VO gehört nicht zu den in Art. 99 Abs. 3 bis Abs. 5 KI-VO oder Art. 101 KI-VO ausdrücklich aufgelisteten bußgeldbewährten Verstößen.

Allerdings erstreckt sich die Beschwerdemöglichkeit zu den nationalen Überwachungsbehörden gemäß Art. 85 KI-VO auch auf Art. 4 KI-VO. Zudem sieht Art. 99 Abs. 1 KI-VO allgemein vor, dass die Mitgliedstaaten Sanktionen für Verstöße gegen die KI-VO normieren. Dies bezieht sich auch auf Art. 4 KI-VO.[146] Gleichwohl wird die Durchsetzbarkeit der Pflichten aus Art. 4 KI-VO angesichts der „weichen Formulierung" angezweifelt.[147] Soweit ersichtlich, war im Referentenentwurf der Vorgängerregierung für das Durchführungsgesetz zur KI-VO (Stand 4. Dezember 2024) kein entsprechender Bußgeldtatbestand enthalten.[148]

Das Amt für KI hat aber klargestellt, dass die **nationalen Marktüberwachungsbehörden** für die Überwachung der Pflichten aus Art. 4 KI-VO zuständig sind.[149] Diese könnten **auf der Grundlage nationaler Bestimmungen Sanktionen und andere Durchsetzungsmaßnahmen** wegen Verstößen gegen Art. 4 KI-VO verhängen. Diese nationalen Bestimmungen sollten **bis zum 2. August 2025** erlassen werden. Die Überwachungs- und Durchsetzungsvorschriften gelten nach Art. 113 Abs. 2 KI-VO zwar erst ab dem 2. August 2026. Dies hindert die zuständigen Behörden nach Ansicht des Amts für KI aber nicht daran, Maßnahmen mit Blick auf Verstöße zu ergreifen, die nach dem 2. August 2025 begangen wurden.[150] In Betracht kommt außerdem eine **privatrechtliche Durchsetzung**, sofern ein Schaden dadurch entsteht, dass die Verpflichtung aus Art. 4 KI-VO nicht eingehalten wurde.[151]

Vor diesem Hintergrund sollten die **ergriffenen Maßnahmen** im Rahmen von Art. 4 KI-VO **dokumentiert und aktuell gehalten werden**, um gegenüber den Aufsichtsbehörden die **Einhaltung von Art. 4 KI-VO nachweisen zu können**.

---

146 *Möller-Klapperich*, KI-Kompetenz, NJ 2025, S. 193 (195).

147 *Wendehorst*, in: Martini/Wendehorst, Verordnung über künstliche Intelligenz, 2024, Art. 4 KI-VO, Rn. 4.

148 Vgl. Referentenentwurf, KI-VO-Durchführungsgesetz, Stand 4. Dezember 2024.

149 Kommission, KI-Kompetenz – Fragen & Antworten, abrufbar unter: https://digital-strategy.ec.europa.eu/de/faqs/ai-literacy-questions-answers; Kommission, AI talent, skills and literacy. Vgl. zur Diskussion im deutschen Schrifttum, ob es sich lediglich um eine Norm mit Appellcharakter handele: *Möller-Klapperich*, KI-Kompetenz, NJ 2025, S. 193 (195); *Wendehorst*, in: Martini/Wendehorst, Verordnung über künstliche Intelligenz, 2024, Art. 4 KI-VO, Rn. 6.

150 Kommission, AI Literacy – Questions & Answers.

151 Vgl. Kommission, AI Literacy – Questions & Answers; *Möller-Klapperich*, KI-Kompetenz, NJ 2025, S. 193 (195).

Die Kommission hat in FAQ zu Art. 4 KI-VO klargestellt, dass zur Dokumentation der Einhaltung von Art. 4 KI-VO **kein Zertifikat** erforderlich sei. Organisationen könnten **interne Aufzeichnungen** über Schulungen und/oder andere Leitinitiativen führen.[152]

7. Compliance-Management: KI-Beauftragter und KI-Governance

Die KI-VO ist ein produktsicherheitsrechtlicher Rechtsakt, durch den nicht zuletzt die Grundrechte der Betroffenen geschützt werden sollen. Hierfür normiert die KI-VO anhand des risikobasierten Ansatzes **einzelne Anbieter- und Betreiberpflichten**.

Nicht ausdrücklich vorgeschrieben ist hingegen die Benennung eines KI-Beauftragten und/oder das Implementieren einer KI-Governance in der jeweiligen Organisation. Der folgende Abschnitt untersucht, unter welchen Umständen beides gleichwohl ratsam sein kann.

7.1. KI-Beauftragter

Die KI-VO enthält – anders als etwa Art. 37 DSGVO mit Blick auf den Datenschutz – **keine ausdrückliche Pflicht**, **einen Beauftragten für KI** oder sonstige Beauftragte bzw. Stellen zu benennen. Die KI-VO macht zudem – anders als der Digital Services Act[153] (Art. 41) und der Digital Markets Act[154] (Art. 28) – keine Vorgaben zur Einrichtung einer Compliance-Abteilung.

(Nur) für **Anbieter** von **HRKS** schreibt Art. 16 Buchst. c i. V. m. Art. 17 Abs. 1 Buchst. j KI-VO vor, dass sie als Bestandteil des **QMS** die **Handhabung der Kommunikation mit Externen,** namentlich mit den „zuständigen nationalen Behörden, anderen einschlägigen Behörden, auch Behörden, die den Zugang zu Daten gewähren oder erleichtern, notifizierten Stellen, anderen Akteuren, Kunden oder sonstigen interessierten Kreisen“ regeln müssen.[155] Nach Art. 17 Abs. 1 Buchst. m KI-VO muss das QMS außerdem einen **Rechenschaftsrahmen** beinhalten, der die Verantwortlichkeiten der Leitung und des sonstigen Personals in Bezug auf die Aspekte des QMS i. S. v. Art. 17 Abs. 1 KI-VO regelt. Es ist danach also festzulegen, wer **intern** für die **Einhaltung der einzelnen Inhalte des QMS verantwortlich** ist.[156] Die konkrete Ausgestaltung ist den Anbietern überlassen.

Betreiber von HRKS haben gemäß **Art. 26 Abs. 2 KI-VO** sicherzustellen, dass **natürliche Personen**, die über die **erforderliche Kompetenz, Ausbildung und Befugnis** verfügen, die **menschliche**

---

152 Kommission, AI Literacy – Questions & Answers.

153 Verordnung (EU) 2022/2065 des Europäischen Parlaments und des Rates vom 19. Oktober 2022 über einen Binnenmarkt für digitale Dienste und zur Änderung der Richtlinie 2000/31/EG (Gesetz über digitale Dienste), ABl. L 277, 27. Oktober 2022, S. 1 (berichtigte Fassung).

154 Verordnung (EU) 2022/1925 des Europäischen Parlaments und des Rates vom 14. September 2022 über bestreitbare und faire Märkte im digitalen Sektor und zur Änderung der Richtlinien (EU) 2019/1937 und (EU) 2020/1828 (Gesetz über digitale Märkte), ABl. L 265, 12. Oktober 2022, S. 1 (berichtigte Fassung).

155 Vgl. dazu: *Eisenberger*, in: Martini/Wendehorst, Verordnung über künstliche Intelligenz, 2024, Art. 17 KI-VO, Rn. 24.

156 *Eisenberger*, in: Martini/Wendehorst, Verordnung über künstliche Intelligenz, 2024, Art. 17 KI-VO, Rn. 27.

Aufsicht (vgl. Art. 14 KI-VO) über HRKS wahrnehmen und sie müssen den Personen die dafür erforderliche Unterstützung zukommen lassen (vgl. auch ErwG 73, 91 KI-VO).[157] ErwG 91 Satz 2 KI-VO bestimmt, dass die Betreiber insbesondere **geeignete** technische und **organisatorische Maßnahmen** treffen sollten, um sicherzustellen, dass sie HRKS gemäß den Betriebsanleitungen verwenden.

Aus Art. 16 f. und Art. 26 KI-VO ergeben sich damit für **HRKS** gewisse Anforderungen an die **personelle Organisation**. Für andere KI-Anwendungen ist dies nicht der Fall. Insbesondere hat die Kommission in den FAQ zu Art. 4 KI-VO auf die Frage, ob ein KI-Beauftragter erforderlich sei, geantwortet, dass **keine spezifische Governance-Struktur** vorgeschrieben sei, um den **KI-Kompetenzbildungsanforderungen** (s. Ziff. 6.) gerecht zu werden.[158]

Gleichwohl wird es im Schrifttum teils als **sinnvoll** angesehen, einen **KI-Beauftragten** zu benennen, der als **Koordinator der Kompetenzbildung** und **Ansprechperson** bei Fragen und Problemen fungieren könne.[159] Über die Schulung und Sensibilisierung von Mitarbeitenden hinaus werden als etwaige weitere Aufgaben eines KI-Beauftragten genannt:

- Dokumentation und Überwachung (notwendige Dokumentationen erstellen, z. B. Risikobewertungen oder technische Unterlagen);
- Sicherstellung der Compliance (Schnittstelle zwischen technischen Teams, der Unternehmensleitung und externen Prüfbehörden sein);
- Risikomanagement (Risiken im Zusammenhang mit dem Einsatz von KI frühzeitig erkennen und bewerten).[160]

7.2. KI-Governance

Die KI-VO schreibt den Akteuren **nicht ausdrücklich** vor, ein **umfassendes Konzept mit operativen und organisatorischen Maßnahmen (KI-Governance)** zur Gewährleistung der Einhaltung der KI-VO und sonstiger Gesetze zu entwickeln. Gleichwohl kann ein solches Konzept mit inhaltlichen und organisatorischen Komponenten zur Etablierung eines strukturierten Beschaffungsprozesses (s. Ziff. 2.1.2.), zum Nachweis der KI-VO-Konformität sämtlicher Anwendungen (s. Ziff. 4.4.) und der KI-Kompetenz sowie des fortlaufenden Monitorings des (kompetenten) Einsatzes von KI-Anwendungen (s. Ziff. 6.5.) **sinnvoll** sein. Eine entsprechende Governance-Strategie könnte – über die Einsetzung eines einzelnen KI-Beauftragten hinaus – ein **multidisziplinäres Team** umfassen, das eine **festgelegte AI (Compliance) Strategie implementieren**, Feedback einholen und Anwendungen monitoren könnte.

---

157 Vgl. dazu *Eisenberger*, in: Martini/Wendehorst, Verordnung über künstliche Intelligenz, 2024, Art. 17 KI-VO, Rn. 25.

158 Kommission, AI Literacy – Questions & Answers.

159 *Wendehorst*, in: Martini/Wendehorst, Verordnung über künstliche Intelligenz, 2024, Art. 4 KI-VO, Rn. 18.

160 Vgl. *Geyer*, Braucht ein Unternehmen einen KI Beauftragten (AI Officer)?, RDP Rechtsanwälte, 23. Januar 2025.

Aufschlussreich ist in diesem Zusammenhang die **KI-Strategie der Kommission**.[161] Diese formuliert eine strategische Zielvorstellung für die Förderung der Entwicklung und Verwendung rechtskonformer, sicherer und vertrauenswürdiger KI-Systeme in der Kommission. Die dort gelisteten Maßnahmen zur Beachtung des risikobasierten Ansatzes der KI-VO umfassen:

- Ausarbeitung interner **operativer Leitlinien**, die den Bediensteten – als Nutzer, Entwickler oder Auftraggeber von KI-Systemen – klare und pragmatische Anleitungen für die Inbetriebnahme solcher Systeme an die Hand geben;

- **Klassifizierung und Bewertung der KI-Systeme**, die in der Kommission **bereits verwendet** werden oder künftig **verwendet werden sollen**, auf der Grundlage eines risikobasierten Ansatzes und unter Einhaltung der operativen Leitlinien der Kommission;

- Vermeidung der Verwendung von KI-Systemen, die als mit europäischen Werten unvereinbar betrachtet werden oder von denen eine Bedrohung für die Gefahrenabwehr, die Sicherheit, die Gesundheit und die Grundrechte der Menschen ausgeht;

- **Schaffung geeigneter Organisations- und Leitungsstrukturen**, damit die Kommission ihren Verpflichtungen in Bezug auf die KI nachkommen kann.[162]

Zu den **organisatorischen** Maßnahmen, die die Kommission laut der Mitteilung ergreift, zählt die **interne KI-Governance** aus bestehenden internen Gremien, die folgende Aufgaben hat:

- Bewertung der KI-Aspekte bei neuen IT-Investitionen (über die bestehende kommissionsweite IT-Governance);

- Unterstützung und Überwachung der Einhaltung der operativen Leitlinien der Kommission;

- Unterstützung eines breit angelegten, von der Basis ausgehenden Netzes interessierter Kolleginnen und Kollegen in Fortführung des bestehenden AI@EC-Netzwerkes.[163]

---

161 Kommission, Künstliche Intelligenz in der Europäischen Kommission (AI@EC) – Eine strategische Zielvorstellung für die Förderung der Entwicklung und Verwendung rechtskonformer, sicherer und vertrauenswürdiger Systeme der künstlichen Intelligenz in der Europäischen Kommission, KOM(2024) 380 endg., 24. Januar 2024. Einen ähnlichen, allerdings nicht auf die KI-VO Bezug nehmenden Ansatz verfolgt der EuGH in seiner Artificial Intelligence Strategy. Darin geht es darum, Ziele und Anwendungsszenarien sowie Risiken und Risikominderungsmaßnahmen zu identifizieren, die Arbeitnehmenden mit den erforderlichen Kompetenzen auszustatten und über eine interne KI-Governance ein konstantes Monitoring eingesetzter KI zu gewährleisten.

162 Kommission, Künstliche Intelligenz in der Europäischen Kommission (AI@EC) – Eine strategische Zielvorstellung für die Förderung der Entwicklung und Verwendung rechtskonformer, sicherer und vertrauenswürdiger Systeme der künstlichen Intelligenz in der Europäischen Kommission, KOM(2024) 380 endg., 24. Januar 2024, S. 5.

163 Kommission, Künstliche Intelligenz in der Europäischen Kommission (AI@EC) – Eine strategische Zielvorstellung für die Förderung der Entwicklung und Verwendung rechtskonformer, sicherer und vertrauenswürdiger Systeme der künstlichen Intelligenz in der Europäischen Kommission, KOM(2024) 380 endg., 24. Januar 2024, S. 5 ff.

Zu den operativen Maßnahmen zählen:

- Erstellung und Pflege eines aktuellen **Registers der KI-Systeme**, die in der Kommission in Gebrauch sind, und deren **Bewertung anhand der kommissionsweiten Leitlinien und rechtlichen Anforderungen**.

- Erstellung und Pflege einer **Liste der bestehenden KI-Initiativen** und Unterbreitung von Vorschlägen für deren **Rangfolge**.

- **Ausarbeitung konkreter operativer Leitlinien**: thematische Leitlinien für das Personal im Hinblick auf die Auswahl, Beschaffung, Entwicklung, Erprobung und Einführung von KI-Lösungen (auf institutioneller und politischer Ebene) nach einem risikobasierten Ansatz, einschließlich allgemeiner und spezifischer Themen im Zusammenhang mit der KI-Cybersicherheit.

- Ausarbeitung von **Leitlinien** für die **Verwendung bestimmter KI-Systeme**: Vorschriften für den Einsatz spezifischer Instrumente wie der bereits aufgestellten internen Leitlinien für den Einsatz von auf **generativer künstlicher Intelligenz** beruhenden Online-Werkzeugen Dritter.

- Entwicklung einer Strategie für den **Aufbau und die Erhaltung eines qualifizierten Personalbestands** und **Bestandsaufnahme** des möglichen **Weiterbildungs-/Umschulungsbedarfs** in verschiedenen Tätigkeitsbereichen.

- Aufbau eines **Rahmens für das Änderungsmanagement und die Kommunikation zur Begleitung des Personals**: „Die Einführung von KI-Systemen führt zu einem tiefgreifenden Wandel der Arbeitsweise und der Kultur des öffentlichen Dienstes. Um diesen Übergang reibungslos, motivierend und wirksam zu unterstützen, werden gezielte Maßnahmen der gemeinsamen Gestaltung und der Kommunikation und Interaktion mit dem Personal geplant und durchgeführt. Dazu gehört auch die Sensibilisierung des Personals für KI und deren potenzielle Auswirkungen, die Weitergabe der Erfahrungen der Teams, die KI als erste eingeführt haben, der Einsatz von Vorreitern zur Verbreitung der Vorteile und bewährten Verfahren für einen wirksamen und verantwortungsvollen KI-Einsatz.“

- **Weiterführung und Verstärkung der Maßnahmen zur Unterstützung der Datenreife in der Kommission**, da Daten die Grundlage für einen korrekten und wirksamen KI-Einsatz bildeten. Entwicklung eines reibungslos funktionierenden Datenökosystems im Rahmen der internen Datenstrategie der Kommission (DataStrategy@EC), um die Datenbestände der Kommission miteinander zu verknüpfen und die Prozesse in der Kommission zu unterstützen. Dies werde entscheidend zu einer rascheren und einfacheren Einführung von KI-Systemen beitragen.

- **Ausarbeitung eines agilen und flexiblen Ansatzes für die Entwicklung und Verwendung von KI-Systemen** durch: i) die Nutzung spezifischer Infrastrukturen und Plattformen gemäß dem in der Digitalstrategie festgelegten Zwei-Säulen-Ansatz, ii) die optimale Nutzung des vorhandenen Fachwissens und anderer spezieller Ressourcen wie der Supercomputer im Europäischen Hochleistungsrechennetz (EuroHPC) und der Daten aus den neuen europäi-

schen Datenräumen, insbesondere den neuen europäischen Sprachdatenräumen, iii) die **Berücksichtigung eingegangener Verpflichtungen in Bezug auf die CO2- und Energiebilanz** und iv) die Gewährleistung der Sicherheit der Daten.

– Schaffung eines Rahmens für die **Weiterverwendung (und Mitgestaltung) quelloffener KI**, auch im Einklang mit der Strategie der Kommission für Open-Source-Software.

– Förderung des **Wissensaustauschs und Auslotung von Möglichkeiten der Zusammenarbeit mit den Organen, Einrichtungen und sonstigen Stellen der EU und mit den Mitgliedstaaten**. Dabei solle auf bestehende interinstitutionelle Kanäle und bestehende Kooperationsgremien der Mitgliedstaaten zurückgegriffen werden, z. B. das Netz der obersten IT-Beauftragten der Mitgliedstaaten, die Expertengruppe für Interoperabilität und die im Rahmen des Gesetzes für ein interoperables Europa vorgeschlagene GovTech- und Erprobungszusammenarbeit.[164]

Der Ansatz einer **KI-Governance** findet sich auch in der KI-Strategie des **EuGH**[165]. Die Governance-Struktur setzt sich aus vier Bausteinen zusammen:

– Ein Management Board, das dafür verantwortlich ist, dass angeschaffte oder entwickelte KI Grundrechte und ethische Prinzipien achtet.

– Ein Information Steering Committee, das die Ziele mit den verfügbaren Ressourcen in Einklang bringen soll, um dafür zu sorgen, dass sich die Investitionen optimal auszahlen;

– Ein AI+ Network, das die Bereiche ermitteln soll, in denen KI-Tools einen Nutzen für die laufenden Aktivitäten bringen werden. Das Netzwerk ist auch für die Prototypen und/oder Pilotprojekte zuständig, mit denen die geplanten Funktionen getestet und die Vorteile ihrer Umsetzung bewertet werden sollen.

– Architecture and data governance boards. Es handelt sich um schon bestehende Boards, die sich mit der IT-Infrastruktur und der Konsistenz und Kohärenz der Daten im gesamten EuGH befassen.[166]

Auch der Leitfaden von Bitkom zu generativer KI in Unternehmen empfiehlt die Implementierung einer KI-Governance. Dort heißt es, dass sich diese angesichts der **Komplexität** und Notwendigkeit **interdisziplinärer Prüfungen** empfehle. Diese Funktion könne sowohl rechtliche als auch technische Anforderungen an die Nutzung von KI-Systemen im Unternehmen bündeln, deren

164 Kommission, Künstliche Intelligenz in der Europäischen Kommission (AI@EC) – Eine strategische Zielvorstellung für die Förderung der Entwicklung und Verwendung rechtskonformer, sicherer und vertrauenswürdiger Systeme der künstlichen Intelligenz in der Europäischen Kommission, KOM(2024) 380 endg., 24. Januar 2024, S. 6 ff.

165 EuGH, Artificial Intelligence Strategy, S. 20 ff.

166 EuGH, Artificial Intelligence Strategy, S. 20 ff.

Einhaltung überwachen und darüber hinaus als Kompetenzstelle für interne und externe Ansprechpartner dienen.[167]

8. Beispiel: Einsatz generativer KI-Systeme mit allgemeinem Verwendungszweck

Ein denkbares Szenario für die Anwendung von KI in den Behörden der Mitgliedstaaten ist, dass sie ihren Mitarbeitern ein generatives KI-System mit allgemeinem Verwendungszweck wie bspw. ChatGPT, Claude oder Gemini zur Verfügung stellt.

Nachfolgend werden in diesem Zusammenhang geltende Anforderungen der KI-VO dargestellt. Diese beziehen sich auf die Untersagung verbotener KI-Praktiken (Art. 5 KI-VO, Ziff. 8.1.), den Umgang mit den besonderen Anforderungen an HRKS (Art. 8 ff. KI-VO, Ziff. 8.2.) sowie auf eventuelle Transparenzpflichten (Art. 50 KI-VO) und Kompetenzbildungsmaßnahmen (Art. 4 KI-VO, s. jeweils Ziff. 8.3.).

8.1. Verbotene Praktiken: Untersagung

Eine Behörde hat dafür Sorge zu tragen, dass es bei der Nutzung von GPAI-Systemen durch ihre Mitarbeitenden nicht zu den durch **Art. 5 KI-VO verbotenen Praktiken** kommt.

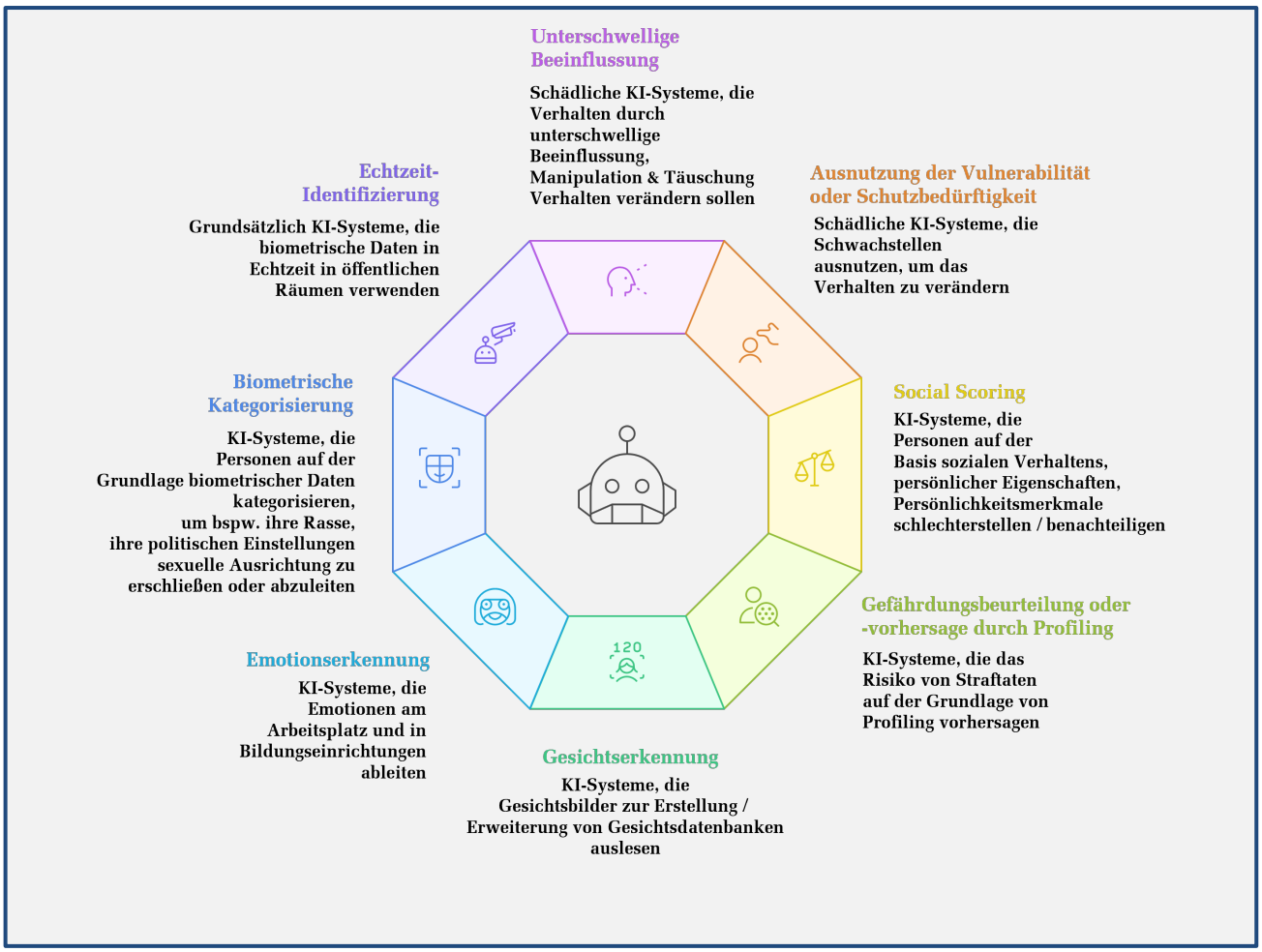
Die Vorschrift hat den Zweck, manipulative, ausbeuterische und soziale Kontrollpraktiken zu verhindern, die im Widerspruch zu den Werten der EU stehen (Achtung der Menschenwürde, Freiheit, Gleichheit, Demokratie und Rechtsstaatlichkeit sowie der in der Charta der Grundrechte der EU verankerten Grundrechte, einschließlich der Rechte auf Nichtdiskriminierung, Datenschutz und Privatsphäre sowie der Rechte des Kindes), vgl. ErwG 28 KI-VO. Sie gilt seit dem **2. Februar 2025**. Dass die Vorschriften über die Durchsetzung und Sanktionen erst später in Kraft treten (vgl. Art. 113 Abs. 2, Abs. 3 Buchst. b KI-VO), ändert nichts an der Rechtsverbindlichkeit und unmittelbaren Geltung von Art. 5 KI-VO. Dies führt dazu, dass Betroffene eine Verletzung von Art. 5 KI-VO vor nationalen Gerichten geltend machen können.[168]

---

167 Bitkom, Generative KI im Unternehmen, Leitfaden 2025, S. 23.

168 So: Kommission, Guidelines on prohibited artificial intelligence practices established by Regulation (EU) 2024/1689 (AI Act), Rn. 432.

Verbotene Praktiken gem. Art. 5 KI-VO



Die Kommission hat am 4. Februar 2025 **Leitlinien zu verbotenen Praktiken** i. S. v. Art. 5 KI-VO veröffentlicht. Sie sollen einen Überblick über KI-Praktiken geben, die aufgrund ihrer potenziellen Risiken für die europäischen Werte und Grundrechte als inakzeptabel erachtet werden.[169]

Zur **Anwendung der Verbote auf KI-Systeme mit allgemeinem Verwendungszweck** stellen die Leitlinien klar, dass die Verbote des Art. 5 KI-VO für jedes KI-System gelten, unabhängig davon, ob es „zweckbestimmt " oder „universell" anwendbar ist und ob es für die direkte Nutzung oder für die Integration in andere KI-Systeme gedacht ist. Dementsprechend solle jeder Akteur die Maßnahmen ergreifen, für die er aufgrund seiner Rolle und seiner Kontrolle über das System in der Wertschöpfungskette am besten geeignet ist, um eine verantwortungsvolle und sichere Bereitstellung und Nutzung von KI-Systemen zu gewährleisten. Von Betreibern werde daher erwartet,

169 Kommission, Guidelines on prohibited artificial intelligence practices established by Regulation (EU) 2024/1689 (AI Act).

dass sie ein KI-System **nicht in einer Weise nutzen, die nach Art. 5 KI-VO verboten ist,** und dass sie auch keine von den Systemanbietern eingeführten Sicherheitsvorkehrungen umgehen.[170]

Die Leitlinien der Kommission widmen sich – soweit ersichtlich – nicht der Frage, wie die Einhaltung von Art. 5 KI-VO in einer größeren Organisation sicherzustellen ist. Neben **zu dokumentierenden Schulungen** dürfte insofern die **Erstellung einer internen Nutzungsrichtlinie** in Betracht kommen, die nicht nur die einschlägigen rechtlichen Anforderungen berücksichtigt, sondern auf konkrete, für die jeweilige Behörde relevante Szenarien eingeht.[171]

8.2. Hochrisiko-Nutzung?

Grundsätzlich gilt, dass GPAI-Systeme als eigenständige HRKS eingesetzt werden oder Komponenten anderer HRKS sein können (vgl. ErwG 85 KI-VO). Hinsichtlich der Frage, welche **Verwendungen hochriskant** und ggf. für Behörden relevant sein könnten, wird auf Ziff. 3.1. verwiesen.

8.2.1. Ausschluss der Nutzung im Hochrisiko-Bereich

Soweit eine Behörde die Nutzung von GPAI-Systemen zu Hochrisikozwecken **ausschließt**, beschränkt sich der Pflichtenkreis auf die allgemeinen Regeln zur Kompetenzbildung und ggf. zur Kennzeichnung (s. Ziff. 8.3.).

Die Behörde muss aber – wie auch hinsichtlich Art. 5 KI-VO – **sicherstellen, dass die Verwendung von GPAI-Systemen durch die Mitarbeitenden den vorgegebenen Nutzungsrahmen** nicht verlässt.[172] Denkbar sind insofern **interne Leitlinien**, **Schulungen** oder **technische Vorkehrungen**, die etwa Warnhinweise anzeigen oder die Nutzung zu bestimmten Zwecken blockieren. So verfügt etwa ChatGPT, dessen Nutzungsrichtlinien die Verwendung für hochrisiko-bezogene Anwendungen verbieten, über inhaltliche Filter, die problematische, gefährliche oder schädliche Inhalte erkennen und blockieren können. Entsprechende **Belehrungen und Aufklärungen** sind hinreichend zu **dokumentieren**, um auf Fälle **nicht autorisierter hochriskanter Verwendungen** durch einzelne Mitarbeitende vorbereitet zu sein.[173]

8.2.2. Nutzung im Hochrisiko-Bereich

Sollte sich eine Behörde entschließen, die Nutzung von **ChatGPT** für **Hochrisiko-Zwecke** zuzulassen, wäre dies eine **Zweckänderung**.[174] Es läge dann ein Fall von Art. 25 Abs. 1 Buchst. c KI-VO vor, d. h. eine Änderung der Zweckbestimmung eines GPAI-Systems mit der Folge, dass dieses ein HRKS wird. Die Folge wäre, dass die Behörde die **umfangreichen Anbieterpflichten aus**

---

170 Kommission, Guidelines on prohibited artificial intelligence practices established by Regulation (EU) 2024/1689 (AI Act), C(2025) 884 final, 4 Februar 2025, Rn. 39 f.

171 Vgl. in diesem Sinne: Bitkom, Generative KI im Unternehmen, Leitfaden 2025, S. 25 ff.

172 *Schwartmann u. a.*, KI-VO, Leitfaden für die Praxis, 2024, S. 90 f.

173 *Schwartmann u. a.*, KI-VO, Leitfaden für die Praxis, 2024, S. 92.

174 ChatGPT ist ausweislich der offiziellen Nutzungsrichtlinien von OpenAI nicht für Hochrisiko-Zwecke zugelassen und an sich nicht als HRKS einzustufen.

Art. 16 KI-VO treffen würden. Dies dürfte einen erheblichen Kostenaufwand und Haftungsrisiken auslösen.[175] Sollte ein Einsatz von KI im Hochrisiko-Bereich gewünscht sein, könnten alternativ auch KI-Systeme mit entsprechender Zweckbestimmung beschafft werden. Dann würden die Behörde „nur“ die Betreiberpflichten aus Art. 26 f. KI-VO treffen.

8.3. Kennzeichnung und Kompetenzbildung

Für die Nutzung von GPAI-Systemen bestehen die allgemeinen Regeln zur **Kennzeichnung** nach Art. 50 KI-VO (s. Ziff. 5) und zur **Kompetenzbildung** nach Art. 4 KI-VO (s. Ziff. 6.).

Hinsichtlich der Kennzeichnungspflichten aus Art. 50 KI-VO dürften bei einer Bereitstellung eines GPAI-Systems wie ChatGPT, Claude, Gemini etc. zur Nutzung durch Mitarbeitende grundsätzlich nur etwaige Betreiberpflichten i. S. v. Art. 50 Abs. 4 KI-VO relevant sein. Im Bitkom-Leitfaden zur KI-VO wird indes erwogen, ob ein Akteur durch wesentliche Veränderungen an einem bestehenden KI-System – auch außerhalb des Anwendungsbereichs von Art. 25 KI-VO – zu dessen Anbieter werden könnte. Hierzu wird darauf verwiesen, dass Modifizierungen eines bestehenden KI-Systems durch dessen Betreiber oberhalb einer bestimmten Erheblichkeitsschwelle ein „Entwickeln“ darstellen könnten.[176] Sollte dies zutreffen, könnten bei wesentlichen Änderungen am bereitgestellten KI-System auch unterhalb der Hochrisiko-Schwelle Anbieterpflichten (aus Art. 50 Abs. 1, 2 KI-VO) gelten.

Hinsichtlich der KI-Kompetenz ergibt sich aus den FAQ der Kommission zu Art. 4 KI-VO, dass die Mitarbeitenden bei einem Einsatz von ChatGPT (und damit auch vergleichbaren Systemen) über die spezifischen Risiken, zum Beispiel KI-Halluzinationen, informiert werden sollten.

8.4. Sonstige Aspekte

Wie bereits mehrfach angedeutet, wirft die Verwendung von GPAI, insbesondere generativer KI, Rechtsfragen u. a. im Bereich des Datenschutzrechts[177] und des Urheberrechts auf, die nicht Gegenstand der vorliegenden Betrachtung sind.[178]

Das Generalsekretariat des Rates der EU hat ein Paper zu den **Gefahren und Risikominderungsmaßnahmen** im Zusammenhang mit dem Einsatz von ChatGPT in der öffentlichen Verwaltung mit dem Titel „ChatGPT in the Public Sector – overhyped or overlooked?“ veröffentlicht.[179]

Fachbereich Europa

---

175 Vgl. *Schwartmann u. a.*, KI-VO, Leitfaden für die Praxis, 2024, S. 90 f.

176 Bitkom, Umsetzungsleitfaden zur KI-Verordnung, 29. Oktober 2024, S. 40.

177 Siehe dazu: *Hardan*, Datenschutzkonforme Nutzung von KI-basierten Chatbots, ZD 2024, S. 663.

178 Vgl. Bitkom, Generative KI im Unternehmen, Leitfaden 2025, S. 24 ff.; *Schwartmann u. a.*, KI-VO, Leitfaden für die Praxis, 2024, S. 90.

179 Generalsekretariat des Rates der EU, ChatGPT in the Public Sector – overhyped or overlooked?, ART Research Paper, 24. April 2023.