Herausragende Masterarbeiten

Autor*in

Luke Niklas Schmidt

Studiengang

Wirtschaftsrecht für die Unternehmenspraxis, LL.M.

Masterarbeitstitel

Die KI-Verordnung - konkreter Handlungsbedarf

RPTU

Distance and Independent Studies Center
DISC

Inhaltsverzeichnis

Teil 1: Einleitung 1

A. Einführung 1

B. Zielsetzung, Aufbau und Methodik 2

Teil 2: Hauptteil 3

A. Zweck, Ansatz und Steuerungselemente der KI-VO 3

B. Anwendungsbereich 5

I. Sachlicher Anwendungsbereich 5

II. Räumlich-persönlicher Anwendungsbereich 8

III. Zeitlicher Anwendungsbereich 10

IV. Zwischenergebnis 11

C. Klassifizierung 12

I. Verbotene Praktiken 12

II. Hochrisiko-KI-Systeme 14

III. KI-Systeme mit begrenztem Risiko 16

IV. KI-Systeme mit minimalem Risiko 17

V. GPAI-Modelle 18

VI. Zwischenergebnis 20

D. Universeller Handlungsbedarf 20

I. Mapping und Sicherstellung von KI-Compliance 20

II. KI-Kompetenz 21

III. Einführung organisatorischer Strukturmaßnahmen 28

IV. Zwischenergebnis 30

E. Risikospezifischer Handlungsbedarf 31

I. Handlungsbedarf für Anbieter und Betreiber von verbotenen KI-Systemen und KI-Systemen mit minimalem Risiko 31

II. Handlungsbedarf für Anbieter und Betreiber von Hochrisiko-KI-Systemen 32

1. Übersicht über den Handlungsbedarf für Anbieter und Betreiber 32

2. Umsetzung des Risikomanagementsystems nach Art. 9 KI-VO 37

III. Handlungsbedarf für Betreiber von KI-Systemen mit begrenztem Risiko: Die Deepfake-Kennzeichnungspflicht 49

IV. Zwischenergebnis 54

Teil 3: Fazit 54

Literaturverzeichnis 56

Erklärung über selbstständige Bearbeitung ……keine Seitenangabe

Teil 1: Einleitung

A. Einführung

„The rise of AI could be the worst or the best thing that has happened for humanity.“[1]

Diese Worte äußerte Stephen Hawking 2017 auf der Technologiekonferenz „Web Summit“. Bereits Jahre vor der breitflächigen Verfügbarkeit von KI-Anwendungen wies er auf den ambivalenten Charakter Künstlicher Intelligenz (KI) hin, die sowohl gravierende Risiken als auch enorme Chancen für Wirtschaft und Gesellschaft birgt: Gefahren wie mangelhafte Transparenz bei der Entscheidungsfindung oder autonomes Arbeiten von KI, das zu menschlichem Kontrollverlust führen kann, stehen Potenziale zu Effizienzsteigerungen oder zur Innovationsentwicklung gegenüber. Insofern kommt der Regulierung von KI eine eminente Bedeutung zu, um potenzielle Gefahren einzudämmen, ohne die Innovationskraft zu bremsen.

Dieser Thematik begegnete die Europäische Union (EU) mit dem Erlass der Verordnung (EU) 2024/1689 des europäischen Parlaments und des Rates vom 13.06.2024 zur Festlegung harmonisierter Vorschriften für KI[2] (auch KI-VO bzw. AI Act genannt). Sie verfolgt das Ziel, die Einführung menschenzentrierter und vertrauenswürdiger KI und deren Innovationspotenzial im EU-Binnenmarkt zu fördern und dabei den EU-Werten gerecht zu werden, insbesondere einen hohen Schutz von Gesundheit, Sicherheit und Grundrechte, einschließlich Rechtsstaatlichkeit, Demokratie und Umweltschutz, zu gewährleisten (Art. 1 Abs. 1 KI-VO, ErwG 1, 2). Insoweit strebt die EU mit der KI-VO weltweit eine Führungsrolle bei der Einführung und Entwicklung sicherer und vertrauenswürdiger KI an (ErwG 2, 8 S. 4).

KI dient inzwischen für viele Unternehmen als probates Werkzeug, insbesondere in Kundenkontakt, Marketing sowie Forschung und Entwicklung; eine im Sommer 2025 durchgeführte Befragung von 604 Unternehmen in Deutschland ab 20 Beschäftigten[3] ergab, dass etwa jedes dritte Unternehmen KI nutzt und knapp die Hälfte den Einsatz von KI plant bzw. prüft.[4] Als wesentlichstes Hindernis für die Nutzung von KI wurde u.a. die Verunsicherung durch rechtliche Hürden und Unklarheiten (53 %) angegeben. 70 % der Befragten, die erwarten, von den Regelungen der KI-VO betroffen zu sein, gehen davon aus, ein oder mehrere

[1] Stephen William Hawking (* 08.01.1942 in Oxford, England; † 14.03.2018 in Cambridge, England), theoretischer Physiker und Astrophysiker, in einer Videoansprache auf dem Web Summit 2017 in Lissabon, Portugal am 06.11.2017, zitiert nach: https://www.forbes.com/sites/johnkoetsier/2017/11/06/stephen-hawking-issues-stern-warning-on-ai-could-be-worst-thing-for-humanity/.
[2] ABl. EU 2024, Nr. L 2024/1689.
[3] Aus Gründen der besseren Lesbarkeit verwendet diese Arbeit das generische Maskulinum. Sämtliche Personenbezeichnungen beziehen sich wertungsfrei auf alle Geschlechter gleichermaßen.
[4] *Bitkom*, Durchbruch bei Künstlicher Intelligenz, o.S.

Hochrisiko-KI-Systeme (folgend: HKIS) – und damit solche, die den strengsten Anforderungen unterliegen – zu betreiben. Diese Kombination aus strengen Vorgaben und Verunsicherung erhöht das Risiko von Verstößen und Sanktionen. Angesichts des sukzessiven Geltungsbeginns der Vorschriften der KI-VO besteht daher ein erheblicher Handlungsbedarf für von der VO betroffene Unternehmen, die einschlägigen Pflichten zu kennen und umzusetzen.

B. Zielsetzung, Aufbau und Methodik

Ziel der Ausführung ist die Analyse des aus der KI-VO resultierenden Handlungsbedarfs für die Unternehmenspraxis. Dazu sollen auszugsweise zentrale betriebliche Handlungsnotwendigkeiten erörtert und zusätzlich untersucht werden, wie sich eine Umsetzung in der Praxis gestalten könnte, wobei treffende Beispiele an geeigneten Stellen zu einem fundierten Verständnis beitragen. Angesichts der Vielzahl potenziell von der KI-VO betroffener Unternehmen kommt der Examinierung des Handlungsbedarfs nicht nur ein akademisches Interesse, sondern auch eine praktische Relevanz zu. Aufgrund des restriktiven Umfangs der Ausarbeitung wird der Untersuchungsgegenstand eingegrenzt: Es soll nur der betriebliche Handlungsbedarf für Anbieter und Betreiber von KI-Systemen analysiert werden, andere Akteure sowie Behörden und Mitgliedstaaten werden explizit ausgeklammert.

Zunächst werden basale Aspekte der VO dargelegt, bevor ihr Anwendungsbereich zur Bestimmung, wann Unternehmen von der KI-VO erfasst sind, untersucht wird. Es folgt eine Darstellung und Einteilung der KI-Systeme in Gefahrenklassen, die maßgeblich für die konkreten Pflichten ist, ergänzt durch Praxisbeispiele zur Verdeutlichung, welcher Kategorie die in den Unternehmen eingesetzten KI-Systeme unterliegen. Nach der insofern erfolgten Untersuchung des ersten Teils der allgemeinen Handlungsnotwendigkeiten, werden der weitergehende universelle und risikospezifische Handlungsbedarf analysiert. Es sollen selektierte, wesentliche Pflichten verschiedener Risikokategorien erörtert und praktische Umsetzungsmöglichkeiten aufgezeigt werden. Die Arbeit schließt mit einer resümierenden Darstellung der Ergebnisse und praktischen Handlungsempfehlungen.

Die methodische Vorgehensweise stützt sich auf eine fundierte Literaturrecherche. Dabei werden verschiedene Gattungen wie juristische Fachartikel, Kommentare, Monografien und Sammelbände ausgewertet und analysiert sowie relevante KI-VO-Vorschriften mittels juristischer Auslegungsmethoden interpretiert. Ferner werden die Erwägungsgründe sowie EU-Leitlinien und Praxisleitfäden berücksichtigt. Aufgrund der Aktualität der Thematik und teils noch nicht geltender Vorschriften ist die Auswertung einschlägiger Rechtsprechung begrenzt. Zwischenergebnisse dienen der Kohärenz der Arbeit durch Darstellung der Quintessenz der Kapitel.

Teil 2: Hauptteil

A. Zweck, Ansatz und Steuerungselemente der KI-VO

Die KI-VO gilt als weltweit erstes Regelwerk für KI[5] und ist gem. Art. 113 KI-VO am 01.08.2024 in Kraft getreten, nachdem sie am 12.07.2024 im Amtsblatt der EU veröffentlicht wurde. Sie zielt auf die Schaffung eines einheitlichen Rechtsrahmens insbesondere für die Entwicklung, das Inverkehrbringen, die Inbetriebnahme und die Verwendung von KI-Systemen in der Union ab, der in Einklang mit den EU-Werten steht (vgl. ErwG 1). Die VO ist von sozial-ethischen Wertvorstellungen geprägt und dient entsprechend ihrer menschenzentrierten Ausrichtung (Art. 1 Abs. 1 KI-VO) primär dem Schutz der in der EU ansässigen bzw. niedergelassenen KI-Betroffenen und ist insofern als Schutzregime konzipiert.[6] Als EU-Verordnung ist ihr die Eigenschaft immanent, dass sie gem. Art. 288 UAbs. 2 AEUV allgemeine Geltung entfaltet, in all ihren Teilen verbindlich ist und unmittelbar einheitlich in jedem EU-Mitgliedstaat gilt, sodass es keines Umsetzungsaktes in nationales Recht bedarf. Die VO folgt einem risikobasierten Ansatz, wonach Art und Inhalt der Vorschriften auf die von KI-Systemen ausgehende jeweilige Risikointensität und den Risikoumfang angepasst sind (ErwG 26). Dabei differenziert die KI-VO im Rahmen eines pyramidalen Aufbaus zwischen vier Risikoklassen: unannehmbares, hohes, begrenztes und minimales Risiko.[7] Anhand dieser Klassifizierung werden verschieden strenge Anforderungen an die KI-Systeme gestellt, wobei die Härte der Vorschriften in direktem Verhältnis zum potenziellen Risiko für die Gesellschaft steht;[8] je höher das Risiko, desto strenger die Anforderungen. Der Ansatz intendiert, potenziell nachteilige Auswirkungen technologischer Entwicklungen und ihre Innovationschancen in ein ausgewogenes Verhältnis zu setzen.[9]

Zur inhaltlichen Ausgestaltung der VO kann die Europäische Kommission (folgend: Kommission), delegierte Rechtsakte, Normungsaufträge zur Erstellung harmonisierter Normen bzw. Durchführungsrechtsakte und Leitlinien erlassen. Zusätzlich wird es Praxisleitfäden und Verhaltenskodizes geben. Delegierte Rechtsakte, die gem. Art. 290 Abs. 1 UAbs 1 AEUV allgemeine Geltung entfalten und in den EU-Mitgliedstaaten verbindlich sind, ermöglichen eine Reaktion auf technische Entwicklungen und Anpassung des Regelungsrahmens (ErwG 173).[10] Innerhalb von fünf Jahren ab dem 01.08.2024 (Art. 97 Abs. 2 S. 1 KI-VO) können sie u.a. erlassen werden, um die Risikoeinstufung gewisser KI-Systeme als HKIS zu modifizieren

[5] *Kommission*, Künstliche Intelligenz – Fragen und Antworten, o.S.
[6] *Krönke*, NVwZ 2024, 529, 530.
[7] *Kommission*, AI Act, o.S.
[8] *Dubovitskaya*, AG 2024, 877, 877, Rn. 2; *von Welser*, GRUR-Prax 2024, 485, 485, Rn. 6.
[9] *Roth-Isigkeit*, KIR 2024, 15, 16.
[10] *Brandt-Steinke*, in: BeckOK KI-Recht Art. 97 Rn. 3.

(Art. 6 Abs. 6, 7 KI-VO) und Anhang III der VO – eine Liste mit konkreten Anwendungsfällen von HKIS – dynamisch anzupassen, sodass die Liste um neue HKIS erweitert oder bestehende gestrichen werden (Art. 7 Abs. 1, 3 KI-VO), um ein angemessenes Schutzniveau zu gewährleisten und gleichzeitig Überregulierung zu vermeiden. Ferner können etwa das Konformitätsbewertungsverfahren gem. Art. 43 Abs. 5 KI-VO geändert oder die Schwellenwerte für KI-Modelle mit allgemeinem Verwendungszweck (General Purpose AI Models, folgend: GPAI-Modelle) gem. Art. 51 Abs. 3 KI-VO aktualisiert werden. Daher sollten Unternehmen regelmäßig prüfen, ob delegierte Rechtsakte erlassen wurden, da diese zu einer Änderung der Klassifizierung ihrer KI-Systeme führen und neue Pflichten begründen können.

Die VO knüpft an das dem Produktsicherheitsrecht entstammende Regulierungskonzept des New Legislative Framework (NLF) an.[11] Es zeichnet sich dadurch aus, dass die VO nur die wesentlichsten Vorgaben regelt und die Kommission zur Konkretisierung der abstrakt gehaltenen Vorschriften Normungsaufträge nach Art. 40 Abs. 2 KI-VO an die Normungsorganisationen CEN und CENELEC erteilt, die praxisrelevante technische Umsetzungslösungen unter Beteiligung von Industrieakteuren und Interessenträgern in Form von harmonisierten Normen ausarbeiten.[12] Die Befolgung harmonisierter Normen nach Veröffentlichung im EU-Amtsblatt ist nicht obligatorisch, begründet jedoch gem. Art. 40 Abs. 1 KI-VO eine Konformitätsvermutung[13] bezüglich der Einhaltung der Vorgaben an HKIS und GPAI-Modelle und erweist sich angesichts des mit alternativen Eigenlösungen verbundenen Mehraufwands und der Rechtsunsicherheit regelmäßig als praktikablerer Weg zur Compliance (vgl. ErwG 121). Besonders für kleine und mittlere Unternehmen ist deren Einhaltung sinnvoll, da es für sie häufig aufgrund fehlenden rechtlichen Wissens und finanzieller Mittel schwierig ist, eigenständige Lösungen zu entwickeln.[14] Zum Stand der Ausarbeitung existieren Normungsentwürfe, eine Veröffentlichung steht jedoch noch aus. Sofern keine geeigneten harmonisierten Normen bestehen, kann die Kommission gem. Art. 41 Abs. 1 KI-VO mittels Durchführungsrechtsakte gemeinsame Spezifikationen als temporäre Überbrückungslösung festlegen, bis taugliche harmonisierte Normen vorliegen, deren Einhaltung ebenfalls eine Konformitätsvermutung begründet (Art. 41 Abs. 3 KI-VO).[15]

Die Kommission erarbeitet Leitlinien als Orientierungshilfe für die praktische Umsetzung der VO, etwa zu den in Art. 5 KI-VO genannten verbotenen Praktiken (Art.

[11] *Gerdemann*, NJW 2024, 2209, 2209, Rn. 1.
[12] ErwG 121; *Gerdemann*, MMR 2024, 614, 615; *Kilian*, in: BeckOK KI-Recht Art. 40 Rn. 2; *von Welser*, GRUR-Prax 2024, 485, 487, Rn. 27.
[13] *Gerdemann*, MMR 2024, 614, 616; *Kilian*, in: BeckOK KI-Recht Art. 40 Rn. 2.
[14] *Kilian*, in: BeckOK KI-Recht Art. 40 Rn. 5.
[15] *Gerdemann*, MMR 2024, 614, 616.

96 Abs. 1 lit. b KI-VO) oder den in Art. 50 KI-VO normierten Transparenzpflichten (lit. d), um die Verständlichkeit bestimmter Vorschriften zu fördern und sie zu konkretisieren (Art. 96 Abs. 1 KI-VO).[16] Partiell ist diese Befugnis auch außerhalb von Art. 96 KI-VO normiert (z.B. Art. 63 Abs. 1 KI-VO). Obwohl Leitlinien keine verbindliche Wirkung entfalten,[17] kommt ihnen als Auslegungshilfe für die teils unscharfen Vorschriften zentrale Bedeutung für eine möglichst einheitliche Umsetzung zu.[18] Ferner unterstützen Praxisleitfäden (Art. 56 KI-VO) bei der Einhaltung und Umsetzung der Vorgaben für GPAI-Modelle, indem sie z.B. bei der Ermittlung systemischer Risiken und deren Ursachen oder bei der Einhaltung der Transparenzvorgaben des Art. 50 KI-VO bezüglich Kennzeichnung künstlicher Inhalte Orientierung bieten.[19] Auch wenn das Büro für Künstliche Intelligenz (folgend: KI-Büro) Anbieter von GPAI-Modellen „ersuchen" kann, Leitfäden zu befolgen (Art. 56 Abs. 7 S. 1 KI-VO), sind sie bei philologischer Auslegung des Worts „ersuchen" nicht bindend.[20] Zwar begründet ihre Befolgung de jure keine Konformitätsvermutung, erleichtert jedoch die Darlegung der Pflichteneinhaltung (vgl. etwa Art. 53 Abs. 4 KI-VO).[21]

Ferner ermöglichen Verhaltenskodizes (Art. 95 KI-VO), freiwillige Selbstverpflichtungen zur Anwendung gewisser Anforderungen einzugehen, wodurch Unternehmen den Vertrauensaufbau fördern können.[22] Solche Kodizes können einzelne oder alle Anforderungen für HKIS auf nicht hochriskante KI-Systeme erstrecken oder spezifische Anforderungen für alle KI-Systeme vorsehen (Art. 95 Abs. 1, 2 KI-VO). Die Kodizes werden in inklusiver Weise von nicht-staatlichen Akteuren wie KI-Anbietern, KI-Betreibern und Stakeholdern, ggf. auch branchenspezifisch oder regional, entwickelt (Art. 95 Abs. 3 KI-VO, vgl. auch ErwG 165).[23]

B. Anwendungsbereich

Zur Ermittlung des konkreten Handlungsbedarfs haben Unternehmen in einem ersten Schritt zu prüfen, ob der Anwendungsbereich der KI-VO für sie eröffnet ist. Ein Handlungsbedarf ergibt sich nur für die Unternehmen, für die der Anwendungsbereich in räumlich-persönlicher, sachlicher und zeitlicher Hinsicht eröffnet ist.

I. Sachlicher Anwendungsbereich

Der sachliche Anwendungsbereich erfasst vor allem KI-Systeme, daneben GPAI-Modelle, als Regelungsgegenstände und knüpft an deren Inverkehrbringen (Art. 3

[16] *Brandt-Steinke*, in: BeckOK KI-Recht Art. 96 Rn. 1; *Hartmann*, in: KI-VO 2026 Art. 96 Rn. 1.
[17] Vgl. z.B. *Kommission*, KI-System-Leitlinien, S. 2, Rn. 7; *Kommission*, Verbotene-Praktiken-Leitlinien, S. 2, Rn. 5; vgl. auch EuGH, Urteil v. 14. Juni 2011 – C-360/09 –, juris (Rn. 23).
[18] *Brandt-Steinke*, in: BeckOK KI-Recht Art. 96 Rn. 12.
[19] *Schneider*, in: BeckOK KI-Recht Art. 56 Rn. 4.
[20] *Schneider*, in: BeckOK KI-Recht Art. 56 Rn. 21.
[21] Vgl. *Kilian*, in: BeckOK KI-Recht Art. 40 Rn. 4.
[22] *Gorzala*, in: BeckOK KI-Recht Art. 95 Rn. 1, 2.
[23] *Gorzala*, in: BeckOK KI-Recht Art. 95 Rn. 25; *Schneider*, in: BeckOK KI-Recht Art. 56 Rn. 7.

Nr. 9 KI-VO), Inbetriebnehmen (Art. 3 Nr. 11 KI-VO) und Verwenden als maßgebliche Handlungen an.[24] Durch den horizontalen Regulierungsansatz der VO sind sämtliche KI-Systeme und GPAI-Modelle sektor- bzw. branchenunabhängig zumindest indirekt von den KI-VO-Regelungen betroffen.[25] Die in Art. 3 Nr. 1 KI-VO normierte Definition des KI-Systems orientiert sich an dem technologieneutralen Begriffsverständnis der OECD, da ein technikbasierter Ansatz Gefahr liefe, im Zuge der dynamischen Entwicklung zu veralten (vgl. Seite 1-2, Rn. 6 S. 2, 3 der KI-System-Leitlinien (folgend: KISL)).[26] Demnach handelt es sich bei einem KI-System um ein „maschinengestütztes System, das für einen in unterschiedlichem Grad autonomen Betrieb ausgelegt ist, nach seiner Betriebsaufnahme anpassungsfähig sein kann und aus den erhaltenen Eingaben für explizite oder implizite Ziele ableitet, wie Ausgaben wie Vorhersagen, Inhalte, Empfehlungen oder Entscheidungen erstellt werden, die physische oder virtuelle Umgebungen beeinflussen können“. Somit werden KI-Systeme anhand besonderer Leistungen definiert.[27] ErwG 12 und die KI-System-Leitlinien konkretisieren die Definition und unterstützen Unternehmen bei der Einordnung, ob es sich bei ihren Systemen um KI-Systeme handelt, die den Vorgaben der VO unterliegen (vgl. Seite 1, Rn. 3 S. 2 KISL).

KI-Systeme unterscheiden sich vor allem durch die Modellinferenz[28], also die Fähigkeit, Modelle oder Algorithmen aus Eingaben oder Daten abzuleiten, die die bloße Datenverarbeitung übersteigt, von konventionellen, nicht der KI-VO unterfallenden Softwaresystemen bzw. -anwendungen, deren automatisch ausgeführte Operationen allein auf menschlich vorgegebene Regeln zurückzuführen sind (ErwG 12). Das eigenständige Ableiten wird nach ErwG 12 durch Techniken wie maschinelles Lernen oder logik- und wissensgestützte Konzepte ermöglicht, wobei erstere sich dadurch auszeichnen, dass das System aus Daten lernt, wie bestimmte Ziele realisiert werden können, während bei letzterem auf Basis kodierter Informationen oder symbolischer Darstellungen der zugrunde liegenden Aufgabe abgeleitet wird. Ansätze des maschinellen Lernens umfassen gem. den Seiten 7-8, Rn. 32-38 KISL Möglichkeiten, wie ein System aus Daten lernt, etwa durch überwachtes (Lernen anhand von gekennzeichneten Daten, z.B. KI-gestützte E-Mail-Spam-Erkennungssysteme), unüberwachtes (Lernen anhand von Mustern, z.B. KI-Systeme, die Pharmaunternehmen für Arzneimittelentdeckungen nutzen), selbstüberwachtes (Lernen anhand von aus ungekennzeichneten Daten erstellten eigenen Kennzeichnungen, z.B. Sprachmodelle, die lernen, das folgende Element

[24] *Voigt*, in: BeckOK KI-Recht Art. 2 Rn. 16.
[25] *Dubovitskaya*, AG 2024, 877, 877, Rn. 2; *Weltersbach/Aslan*, BKR 2025, 49, 57.
[26] *Vasel*, EuZW 2024, 829, 830; *Wendehorst et al.*, MMR 2024, 605, 606.
[27] *Vasel*, EuZW 2024, 829, 830.
[28] *Krönke*, NVwZ 2024, 529, 529.

in einem Satz zu prognostizieren) oder bestärkendes Lernen (Lernen anhand von Erfahrungen durch systematisches Ausprobieren, sogenanntes „Trial and Error“, z.B. KI-gestützte Roboterarme, die Objekte greifen können) oder Deep Learning (KI-Systeme, die auf Grundlage großer Trainingsdatenmengen automatisch Merkmale aus Rohdaten lernen und z.B. Vorhersagen mit hoher Präzision treffen oder Muster erkennen). Bei logik- und wissensgestützten Konzepten lernen KI-Systeme nach Seite 8, Rn. 39 KISL aus kodiertem Wissen (Regeln und Fakten) und ziehen Schlussfolgerungen mittels logischer Ableitungen (z.B. klassische Sprachverarbeitungsmodelle). Die Fähigkeit zum eigenständigen Ableiten bildet die Grundlage autonomer Lern-, Schlussfolgerungs- und Modellierungsprozesse (ErwG 12) und ist konstitutiv für die Qualifikation als KI-System (Seite 6, Rn. 26 S. 4 KISL).

Die der Definition des KI-Systems immanente essenzielle Fähigkeit zur Autonomie korrespondiert mit der durch das Ableiten resultierenden Fähigkeit, eigene Schlussfolgerungen zu treffen, wobei kein explizites Mindestmaß an Autonomie gefordert wird (Seite 3, Rn. 15 KISL).[29] Vielmehr liegt Autonomie angelehnt an ErwG 12 bei allen Systemen vor, die bis zu einem gewissen Grad unabhängig von menschlichem Zutun mit ihrer Umgebung interagieren (Seite 4, Rn. 20 KISL). Charakteristisch für KI-Systeme ist nach Seite 13, Rn. 59 KISL überdies ihre Fähigkeit, auf Basis komplexer Datenmuster und -beziehungen differenzierte Ausgaben zu erzeugen, wodurch sie vielschichtiger argumentieren können und sich von Nicht-KI-Systemen abheben. Anpassungs- oder Lernfähigkeit nach Betriebsaufnahme ist nicht nötig, sodass es sich bei der Fähigkeit zum automatischen Lernen um ein fakultatives Element handelt (Seiten 4-5, Rn. 23 KISL).

Zur praktischen Bestimmung, ob der sachliche Anwendungsbereich für das jeweilige Unternehmen eröffnet ist und damit konkreter Handlungsbedarf durch Einhaltung der Vorgaben der VO besteht, erscheint eine exemplarische praxisnahe Darbietung hilfreich. Keine Anwendung findet die VO neben den bereits dargelegten Systemen, die ausschließlich starre, menschlich vorab festgelegte Regeln befolgen, auf allgemeine Softwareanwendungen wie einfache Excel-Summenfunktionen oder Taschenrechner, wohingegen intelligente Smart-Home-Geräte, digitale Assistenten oder Programme zum automatisierten Fahren von der KI-VO erfasst sind.[30] Ebenso erfasst sind Chatbots, die auf einem festen Large Language Model (folgend: LLM) basieren oder medizinische Bilderkennungssysteme, die etwa Hautaufnahmen analysieren und Ärzte bei der Diagnose und Bewertung von Krankheitszuständen unterstützen.[31] Ferner sind Systeme für einfache

[29] *Chibanguza/Steege*, NJW 2024, 1769, 1770, Rn. 7.
[30] *Hilgendorf/Härtlein*, KI-VO 2025a Art. 2 Rn. 8.
[31] *Wendehorst et al.*, MMR 2024, 605, 612, 613.

Datenverarbeitung wie Datenbankverwaltungssysteme oder Systeme zur Visualisierung wie Software zur Verkaufsberichtsvisualisierung zur Feststellung von Absatztrends aufgrund fehlender Lern-, Schlussfolgerungs- oder Modellierungsprozesse gem. Seiten 10-11, Rn. 46 und 47 KISL nicht vom Anwendungsbereich der VO umfasst. Ebenso keine Anwendung findet sie auf klassische Heuristik gestützte Systeme, die auf regelgestützten Ansätzen oder Mustererkennung basieren und vordefinierte Regeln oder Algorithmen zur Ableitung nutzen (etwa Schachprogramme mit heuristischen Evaluierungsfunktionen), da diesen Systemen die Fähigkeit zur Anpassung und Verallgemeinerung fehlt (Seite 11, Rn. 48 KISL). Auch einfache Vorhersagesysteme wie Finanzprognosesysteme zur Vorhersage künftiger Aktienkurse oder statische Schätzsysteme fallen nicht in den Anwendungsbereich, da sie nicht ausreichend leistungsfähig sind (Seiten 11-12, Rn. 49-51 KISL).

Überdies normiert Art. 2 KI-VO Ausnahmen, die den sachlichen Anwendungsbereich konkretisieren. Demnach sind KI-Systeme für ausschließlich Verteidigungs- oder militärische Zwecke sowie Zwecke der nationalen Sicherheit (Art. 2 Abs. 3 KI-VO), ebenso vom sachlichen Anwendungsbereich ausgeklammert wie KI-Systeme und KI-Modelle, die dem alleinigen Zweck der Forschung und Entwicklung dienen (Art. 2 Abs. 6 KI-VO) und Forschungs-, Test- und Entwicklungstätigkeiten zu KI-Systemen oder KI-Modellen vor deren Inverkehrbringen oder Inbetriebnahme (Art. 2 Abs. 8 KI-VO). Auch unterfallen frei und quelloffenen lizenzierte KI-Systeme nicht der VO, sofern sie keine verbotenen, hochriskanten oder den Transparenzpflichten des Art. 50 KI-VO unterliegenden KI-Systeme sind (Art. 2 Abs. 12 KI-VO). Die Ausnahmen in Abs. 6, 8 und 12 sollen die Innovationsfähigkeit in der EU fördern. Eine besondere Regelung gilt gem. Art. 2 Abs. 2 S. 1 KI-VO für produktbezogene HKIS, die in Zusammenhang mit Produkten stehen, die unter die in Anhang I Abschnitt B gelisteten Harmonisierungsrechtsvorschriften fallen und vornehmlich dem „alten Rechtsrahmen“ angehören.[32] Auf diese Systeme ist die KI-VO nicht direkt anwendbar.[33] Die Regelungen der KI-VO werden über die Art. 102-109 KI-VO in die einschlägigen Rechtsakte überführt, sodass die materiellen Regelungen der VO auch für diese HKIS mittelbar gelten (vgl. ErwG 49).[34] Aus Anhang I Abschnitt B geht hervor, dass dies u.a. für die zivile Luftfahrt und den Kraftfahrzeugbau relevant ist.

II. Räumlich-persönlicher Anwendungsbereich

Die KI-VO adressiert in persönlicher Hinsicht Akteure und betroffene Personen. Zu den Akteuren zählen nach Art. 3 Nr. 8 KI-VO vor allem Anbieter und Betreiber, auf

[32] *Wendehorst*, in: KI-VO 2026 Art. 2 Rn. 33.
[33] *Voigt*, in: BeckOK KI-Recht Art. 2 Rn. 34.
[34] *Hilgendorf/Härtlein*, KI-VO 2025a Art. 2 Rn. 10; *Voigt*, in: BeckOK KI-Recht Art. 2 Rn. 35.

die sich die Regelungen der VO primär beziehen.[35] Anbieter sind nach Art. 3 Nr. 3 KI-VO natürliche oder juristische Personen, Behörden, Einrichtungen oder sonstige Stellen, die ein KI-System oder ein GPAI-Modell entwickeln oder entwickeln lassen und unter eigenem Namen oder ihrer Handelsmarke in Verkehr bringen oder das KI-System unter eigenem Namen oder ihrer Handelsmarke in Betrieb nehmen, unabhängig von einer möglichen Entgeltlichkeit. Anbieter können also auch Unternehmen sein, die eine Fremdentwicklung beauftragen und diese eigenständig betreiben.[36] Betreiber sind natürliche oder juristische Personen, Behörden, Einrichtungen oder sonstige Stellen, die ein KI-System in eigener Verantwortung verwenden, außer, das KI-System wird im Rahmen einer persönlichen und nicht beruflichen Tätigkeit verwendet (Art. 3 Nr. 4 KI-VO). Für die Unternehmenspraxis hat das Merkmal der „eigenen Verantwortung" die Folge, dass nicht der Angestellte, sondern der Unternehmer als Weisungsbefugter zum Betreiber wird, wenn er den betrieblichen Einsatz anweist.[37] Ferner könnten Unternehmen unbewusst durch unbekannte mitarbeiterseitige Nutzung von „Schatten-KI" zur Einhaltung der Betreiberpflichten verpflichtet werden, wenn Mitarbeiter über eigene oder Unternehmensgeräte KI-Systeme wie Chatbots, etwa zum Verfassen von Mails, nutzen; um dies zu vermeiden, sollten eigene KI-Systeme etabliert werden.[38]

Die Rollen setzen an verschiedenen Tätigkeiten an. Der Anbieterbegriff knüpft am Entwickeln und Inverkehrbringen an, der Betreiberbegriff an der Verwendung;[39] ferner bezieht sich letzterer nur auf KI-Systeme, nicht auch GPAI-Modelle. Exemplarisch ist der Entwickler von Auswertungsprogrammen für Lebensläufe Anbieter und das dieses Programm nutzende Unternehmen Betreiber.[40] Keine Anwendung findet die VO gem. Art. 2 Abs. 10 KI-VO (Haushaltsausnahme) auf natürliche Personen, die KI-Systeme zu ausschließlich persönlichen und nicht beruflichen Tätigkeiten nutzen (z.B. ausschließlich private Nutzung von ChatGPT)[41]. Eine weitere Ausnahme ist in Art. 2 Abs. 4 KI-VO unter den dort genannten Voraussetzungen für Behörden in Drittländern und internationale Organisationen vorgesehen.

Durch Art. 2 Abs. 1 lit. a-c KI-VO wird neben der persönlichen auch die räumliche Komponente geregelt, d.h. welche Akteure örtlich gesehen unter die VO fallen. Erfasst sind Anbieter, die in der EU KI-Systeme in Verkehr bringen oder in Betrieb nehmen oder GPAI-Modelle in Verkehr bringen, unabhängig davon, ob sie in der

[35] *Krönke*, NVwZ 2024, 529, 530; *von Welser*, GRUR-Prax 2024, 485, 486, Rn. 10; *Wendt/Wendt*, Das neue Recht der KI, § 3 Rn. 49.
[36] *Chibanguza/Steege*, NJW 2024, 1769, 1770, Rn. 12.
[37] *Borges*, CR 2024a, 497, 505, Rn. 87; *Hilgendorf/Härtlein*, KI-VO 2025a Art. 2 Rn. 4.
[38] *Braegelmann*, KIR 2024, 39, 39, 40.
[39] *von Welser*, GRUR-Prax 2024, 485, 486, Rn. 10.
[40] *Kommission*, Künstliche Intelligenz – Fragen und Antworten, o.S.
[41] *Chibanguza/Steege*, NJW 2024, 1769, 1770, Rn. 13.

EU oder einem Drittland niedergelassen sind (lit. a), Betreiber von KI-Systemen, die ihren Sitz in der Union haben oder sich dort befinden (lit. b) und Anbieter und Betreiber von KI-Systemen, die ihren Sitz in einem Drittland haben oder sich dort befinden, wenn die vom KI-System erzeugte Ausgabe in der EU verwendet wird (lit. c). Demnach verankert die VO Marktort- (lit. a) und Niederlassungsprinzip (lit. b).[42] Mit lit. c kommt ihr eine über die Grenzen der EU weiterreichende extraterritoriale Wirkung zu, um Umgehungen der VO durch außerhalb der EU stehende Akteure wie OpenAI zu vermeiden und einen effektiven Grundrechtsschutz zu gewährleisten (vgl. ErwG 21, 22).[43] In der Literatur wird gefordert, lit. c aus Praktikabilitätsgründen in Einklang mit ErwG 22 S. 4 teleologisch zu reduzieren, sodass die KI-VO nur bei einer beabsichtigten Verwendung des Outputs in der EU Anwendung finden sollte.[44] In der Praxis nutzen in Deutschland ansässige Unternehmen häufig KI-Systeme von außerhalb der EU ansässigen Unternehmen, etwa von taiwanesischen Unternehmen entwickelte KI-Bewertungsprogramme für Lebensläufe.[45] Hier wäre das deutsche Unternehmen Betreiber i.S.d. Art. 2 Abs. 1 lit. b KI-VO, weil sein Sitz in der EU situiert ist und es das System entsprechend Art. 3 Nr. 4 KI-VO in eigener Verantwortung verwendet.[46] Sofern auch der sachliche und zeitliche Anwendungsbereich eröffnet sind, unterliegt es den Betreiberpflichten.

III. Zeitlicher Anwendungsbereich

Art. 113 KI-VO sieht eine gestaffelte Anwendbarkeit der VO vor, um betroffenen Akteuren ausreichend Zeit einzuräumen, sich auf die Rechtslage vorzubereiten.[47] Nach Art. 113 KI-VO gilt die KI-VO grundsätzlich ab 02.08.2026. Die Vorschriften zu den verbotenen Praktiken und zur KI-Kompetenz sind seit 02.02.2025 anwendbar (Art. 113 lit. a KI-VO), da die Akteure frühzeitig einen sachkundigen Umgang mit KI lernen sollen, die Vorgaben zu GPAI-Modellen seit 02.08.2025 (Art. 113 lit. b KI-VO). Ferner gelten seit 02.08.2025 die Vorgaben zu notifizierenden Behörden und Stellen, zur Governance, zur Wahrung der Vertraulichkeit und die Sanktionsvorschriften, mit Ausnahme der Geldbußen für Anbieter von GPAI-Modellen. Zur Durchführung der VO hatte jeder Mitgliedstaat bis 02.08.2025 nationale Sanktionsvorschriften zu erlassen (Art. 99 Abs. 1 KI-VO) und gem. Art. 70 Abs. 1 S. 1 KI-VO im Rahmen der Governance-Vorschriften eine notifizierende Behörde und eine

[42] *Krönke*, NVwZ 2024, 529, 530; *Voigt*, in: BeckOK KI-Recht Art. 2 Rn. 17; *Wendt/Wendt*, Das neue Recht der KI, § 3 Rn. 53.
[43] *Buchalik/Gehrmann*, CR 2024, 145, 147, Rn. 13; *Krönke*, NVwZ 2024, 529, 530; *Wendehorst*, in: KI-VO 2026 Art. 2 Rn. 25; *Wendt/Wendt*, Das neue Recht der KI, § 3 Rn. 55.
[44] U.a. *Krönke*, NVwZ 2024, 529, 530; *Schopper/Raschner*, KIR 2025, 91, 98, 99; *Voigt*, in: BeckOK KI-Recht Art. 2 Rn. 27.
[45] *Schopper/Raschner*, KIR 2025, 91, 95.
[46] *Schopper/Raschner*, KIR 2025, 91, 95.
[47] *Hilgendorf/Härtlein*, KI-VO 2025a Vor Art. 6 ff. Rn. 9; *Teichmann*, ZD 2025, 495, 496; *von Welser*, GRUR-Prax 2024, 485, 486, Rn. 12.

Marktüberwachungsbehörde als zuständige nationale Behörden einzurichten oder zu benennen. Deutschland konnte die Frist nicht wahren, jedoch existiert nunmehr ein Referentenentwurf für ein Durchführungsgesetz zur KI-VO, in dessen Art. 1 das KI-Marktüberwachungs- und Innovationsförderungsgesetz (KI-MIG) verortet ist. § 2 Abs. 1 respektive § 3 Abs. 1 KI-MIG sieht die Bundesnetzagentur als zuständige Marktüberwachungs- und notifizierende Behörde vor, soweit diese Aufgabe keiner anderen Behörde zugewiesen ist. Im Übrigen sollen grundsätzlich nach § 15 Abs. 1 KI-MIG die Vorschriften des Ordnungswidrigkeitengesetzes für Verstöße nach Art. 99 Abs. 3-5 KI-VO entsprechend gelten. Die Vorgaben an die in Anhang III aufgeführten anwendungsbezogenen HKIS gelten wie auch die Transparenzpflichten nach Art. 50 KI-VO ab 02.08.2026, die Pflichten für unter Anhang I fallende produktbezogene HKIS ab 02.08.2027 (Art. 113 lit. c KI-VO).[48] Bereits bestehende KI-Systeme und GPAI-Modelle genießen begrenzten Bestandsschutz (Art. 111 KI-VO), sodass eine verbindliche Einhaltung der Vorgaben für diese erst später gilt. Die KI-VO vermag den ganzen Lebenszyklus von KI zu regulieren, was daran deutlich wird, dass sie nicht nur Anforderungen an die Entwicklung stellt, sondern auch Pflichten nach Inverkehrbringen vorsieht, etwa eine Überwachungspflicht.[49]

IV. Zwischenergebnis

Für Unternehmen besteht zunächst der Handlungsbedarf, zu ermitteln, ob die KI-VO anwendbar ist. Bei Prüfung des sachlichen Anwendungsbereichs ist zu untersuchen, ob ihre Systeme bzw. Anwendungen als KI-System bzw. GPAI-Modell zu qualifizieren sind, wobei die KI-System-Leitlinien unterstützen. KI-Systeme zeichnen sich besonders durch ihre Fähigkeit zu eigenständigen Schlussfolgerungen (Ableitungen) und Autonomie aus. Das System muss sich selbst Regeln geben können und nicht nur nach menschlichen Handlungsanweisungen verfahren; regelbasierte Software bzw. Programme sind keine KI-Systeme und daher nicht vom Anwendungsbereich erfasst.[50] Auch ist zu bestimmen, welche Akteurrolle das Unternehmen ausfüllt, da hieran unterschiedliche Pflichten anknüpfen. Trotz gestaffelter Geltung empfiehlt es sich, proaktiv zu handeln und frühzeitig durch Aufbau personeller und organisatorischer Strukturen sowie Erstellung von Konzepten zur Umsetzung künftiger Pflichten Compliance mit der VO herzustellen und vorab noch nicht verbindliche Vorgaben weitestmöglich einzuhalten (vgl. Kapitel D., Abschnitt I. und III.), damit Compliance-Practices erprobt werden können und KI-

[48] Mit dem „Digital-Omnibus“ hat die Kommission am 19.11.2025 jedoch vorgeschlagen, die Fristen für Anhang I- und Anhang III-HKIS nach hinten zu verschieben (vgl. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52025PC0836).
[49] *Chibanguza/Steege*, NJW 2024, 1769, 1770, Rn. 9.
[50] *Roth-Isigkeit*, KIR 2024, 15, 16.

Anwendungen nicht ab Geltung der Vorgaben in die Illegalität abdriften.[51] Angesichts der bei Verstößen drohenden Sanktionen ist Unternehmen bei Zweifeln über ihre Betroffenheit von der KI-VO die Konsultation externen Rechtsrats anzuraten.

C. Klassifizierung

Nach Feststellung der Anwendbarkeit der VO haben Unternehmen in einem weiteren Schritt zu prüfen, welcher Risikoklasse ihre Systeme unterfallen. Unterschieden wird zwischen KI-Systemen mit unannehmbarem Risiko, hochriskanten KI-Systemen, KI-Systemen mit begrenztem Risiko und KI-Systemen mit minimalem Risiko. Ergänzend stehen GPAI-Modelle. Jedes KI-System ist vor dessen Inverkehrbringen in eine Kategorie einzuteilen, wobei die Klassifizierung grundsätzlich durch die Anbieter anhand des Verordnungstextes und einschlägiger Leitlinien erfolgt und maßgeblich für die konkret einzuhaltenden Pflichten ist.[52]

I. Verbotene Praktiken

Art. 5 KI-VO regelt einen abschließenden Katalog verbotener KI-Praktiken, die wegen ihres unannehmbar hohen Risikos für die EU-Werte, vor allem die Grundrechte, mit dem Ziel einer menschenzentrierten und vertrauenswürdigen KI unvereinbar sind, weshalb die Nutzung von KI-Systemen in den dort aufgeführten grundrechtssensiblen Bereichen untersagt ist (vgl. ErwG 28, Seite 2, Rn. 8 Verbotene-Praktiken-Leitlinien (folgend: VPL)).[53] Zur Auslegung der in der Literatur[54] wegen vieler unbestimmter Rechtsbegriffe kritisierten Verbote dienen die Leitlinien zu verbotenen KI-Praktiken, die Beispiele bieten und den Rechtsanwendern so bei Ermittlung, ob ihre KI-Praktiken als verboten gelten, unterstützen (vgl. Seite 1, Rn. 4 und Seite 160, Rn. 432 VPL) und der Rechtssicherheit Rechnung tragen.[55] Dadurch, dass Art. 5 KI-VO an konkrete Tätigkeiten und nicht an KI-Systeme anknüpft, liegt ein tätigkeitsbezogener Ansatz zugrunde.[56] Verboten werden das Inverkehrbringen, die Inbetriebnahme und die Verwendung gewisser KI-Systeme zu manipulativen, ausbeuterischen oder sozialen Kontroll- oder Überwachungspraktiken (Seite 2, Rn. 8 VPL). Die acht normierten Praktiken können in die Kategorien „Manipulation“, Kategorisierung“ und Überwachung“ gegliedert werden.[57]

Unter die Kategorie der Manipulation fallen KI-Praktiken, die auf unterschwellige Beeinflussung, vorsätzliche Manipulation oder Täuschung (lit. a) oder das

[51] Vgl. sinngemäß *Gerdemann*, NJW 2024, 2209, 2210, Rn. 2.
[52] Vgl. *Lauber-Rönsberg et al.*, KIR 2025, 399,405; *Ossmann-Magiera/Dehmel*, KIR 2024, 134,135.
[53] *Hilgendorf/Härtlein*, KI-VO 2025a Vor. Art. 5 Rn. 1; *Raue*, in: BeckOK KI-Recht Art. 5 Rn. 1; *Wendehorst*, in: KI-VO 2026 Art. 5 Rn. 1.
[54] Vgl. etwa *Krönke*, NVwZ 2024, 529, 531; *Möller-Klapperich*, NJ 2024, 337, 340; *Schwartmann et al.*, EuDIR 2025, 74, 83, Rn. 67.
[55] Vgl. *Schwartmann et al.*, EuDIR 2025, 74, 74, 83, Rn. 2, 66.
[56] *Wendehorst*, in: KI-VO 2026 Art. 5 Rn. 2.
[57] *Hilgendorf/Härtlein*, KI-VO 2025a Vor. Art. 5 Rn. 2.

Ausnutzen gruppenspezifischer Vulnerabilitäten bzw. Schutzbedürftigkeit (lit. b) gerichtet sind und darauf abzielen, das menschliche Verhalten derart zu beeinflussen, dass ihnen oder Dritten erheblicher Schaden physischer, psychischer oder finanzieller Natur (vgl. ErwG 29 S. 2) zugefügt werden kann. Die Verbote dienen dem Schutz der individuellen Entscheidungsautonomie (vgl. ErwG 29 S. 1, Seite 21, Rn. 59 VPL). Nach lit. a verboten ist z.B. die Manipulation der Gehirnaktivitäten in einem durch Hirnaktivitäten steuerbaren Computerspiel mittels KI-gestützten Neuro-Technologien, die das Gehirn heimlich zum Offenlegen sensibler Daten wie Bankinformationen trainieren (Seiten 24-25, Rn. 66 VPL). Nach lit. b verboten wäre etwa ein KI-gestütztes Spielzeug zur Interaktion mit Kindern, das sie durch gezielte Anreize zu gefährlichem Verhalten verleitet (Seite 41, Rn. 105 VPL).

Bei der Kategorisierung werden Menschen anhand gewisser Faktoren Gruppen zugeordnet.[58] Untersagt ist KI-gestütztes „Social Scoring", d.h. eine Bewertung natürlicher Personen basierend auf ihrem sozialen Verhalten, ihren Eigenschaften oder Persönlichkeitsmerkmalen, wenn dies zu einer ungerechtfertigten bzw. unverhältnismäßigen Benachteiligung oder Schlechterstellung führt oder entgegen dem Zweck der initialen Datenerfassung geschieht (lit. c).[59] Ferner ist die merkmalbasierte Risikobewertung zur Vorhersage, ob eine Person eine Straftat begehen wird, aufgrund der Unschuldsvermutung (vgl. ErwG 42 S. 1) verboten, außer das KI-System dient lediglich der Unterstützung einer auf objektiven Tatsachen beruhenden menschlichen Bewertung (lit. d). Verboten wäre also ein KI-System zur Terrorismusbekämpfung und Vorhersage der Begehung von Straftaten, das sich nur auf Alter und Staatsangehörigkeit stützt (Seite 82, Rn. 202 VPL). Zudem ist die biometrische Kategorisierung natürlicher Personen bezüglich diskriminierungsanfälliger Merkmale wie Religion oder Sexualität verboten, sofern es keine rechtmäßig erworbenen biometrische Datensätze sind (lit. g). Somit ist etwa ein KI-System verboten, das die politische Orientierung von Nutzern sozialer Medien mittels ihrer biometrischen Daten (Art. 3 Nr. 34 KI-VO) der hochgeladenen Fotos analysiert, um gezielt politische Nachrichten zu senden (Seite 110, Rn. 280 VPL).

Der Bereich der Überwachung betrifft KI-Systeme zur Emotionserkennung an Arbeitsplätzen und in Bildungseinrichtungen. Sie sind nur erlaubt, wenn medizinisch oder sicherheitstechnisch nötig (lit. f), etwa eine Emotionserkennung zur Unterstützung autistischer Arbeitnehmer (Seite 105, Rn. 263 VPL). Zudem ist die Datenbankerstellung oder -erweiterung zur Gesichtserkennung durch Scaping, d.h. ungezieltes Auslesen von Gesichtsbildern aus Überwachungsaufnahmen und dem

[58] *Hilgendorf/Härtlein*, KI-VO 2025a Vor. Art. 5 Rn. 3.
[59] *Chibanguza/Steege*, NJW 2024, 1769, 1771, Rn. 23.

Internet, verboten (lit. e), da es das Gefühl der Massenüberwachung verstärkt (ErwG 43). So ist das ungezielte Auslesen sozialer Medien zur Sammlung von Gesichtsbildern und deren Verknüpfung mit verfügbaren Informationen, damit das System Gesichtsmerkmale transformieren und so ermitteln kann, ob ein Gesicht auf einem hochgeladenen Bild mit einem Gesicht aus der Datenbank übereinstimmt (Seite 94, Rn. 232 VPL), verboten. Generell untersagt sind auch biometrische Echtzeit-Fernidentifizierungssysteme zu Strafverfolgungszwecken in öffentlich zugänglichen Räumen (lit. h). Die in lit. h genannten Ausnahmen gelten nicht unmittelbar; vielmehr können die EU-Staaten nach Art. 5 Abs. 5 KI-VO und unter Beachtung der Abs. 2-7 nationale Rechtsgrundlagen schaffen, um biometrische Echtzeit-Fernidentifizierungen in den dort vorgesehenen Fällen zu gestatten.[60]

Angesichts empfindlicher Geldbußen von bis zu 35 Millionen Euro oder bis zu 7 % des weltweiten Gesamtjahresumsatzes des vorigen Geschäftsjahres, je nach dem, welcher Betrag höher ausfällt (Art. 99 Abs. 3 KI-VO), sollten Unternehmen stets darauf achten und überprüfen, keine verbotenen Praktiken vorzunehmen.

II. Hochrisiko-KI-Systeme

Die KI-VO unterscheidet zwischen produktbezogenen und anwendungs- bzw. einsatzfeldbezogenen HKIS.[61] Die Klassifizierung als HKIS hängt maßgeblich von der Zweckbestimmung bzw. dem Einsatzgebiet ab (vgl. ErwG 52).[62] Nach Art. 6 Abs. 1 KI-VO sind KI-Systeme dann HKIS, wenn sie selbst ein Produkt oder ein Sicherheitsbauteil eines Produkts einer in Anhang I aufgeführten das Produktsicherheitsrecht betreffenden Harmonisierungsrechtsvorschrift sind und zusätzlich einer unabhängigen Konformitätsbewertung durch Dritte unterworfen sind. Diese Systeme sind insbesondere für den Schutz von Leib und Leben essenziell.[63] Dabei sind Produkte (und deren Sicherheitsbauteile) betroffen, denen – selbst ohne Nutzung von KI-Systemen – erhöhte Risiken zugeschrieben werden und daher einer Konformitätsbewertung durch Dritte anstatt einer Selbstzertifizierung unterzogen werden müssen, weshalb sie bei Nutzung von KI als Sicherheitskomponente den strengen Anforderungen für HKIS unterliegen.[64] Exemplarisch genannt seien gem. Anhang I und ErwG 50 u.a. Maschinen, Spielzeug und Medizinprodukte, wobei als Beispiel für ein produktbezogenes HKIS eine KI-Anwendung für die roboterassistierte Chirurgie angeführt werden kann.[65] Art. 6 Abs. 2 i.V.m. Anhang III KI-VO zielt auf den Anwendungskontext ab, knüpft an KI-spezifische Gefahren an und erfasst

[60] *Roth-Isigkeit*, KIR 2024, 15, 17; *Schwartmann et al.*, EuDIR 2025, 74, 80, Rn. 43.
[61] *Gerdemann*, NJW 2024, 2209, 2209, Rn. 2; *von Welser*, GRUR-Prax 2024, 485, 486, Rn. 21, 24.
[62] *Ebers/Streitbörger*, RDi 2024, 393, 394, Rn. 7; *Möller-Klapperich*, NJ 2024, 337, 340.
[63] *Gerdemann*, NJW 2024, 2209, 2209, Rn. 2; *Weltersbach/Aslan*, BKR 2025, 49, 52.
[64] *Ruschemeier*, in: KI-VO 2026 Art. 6 Rn. 28.
[65] *Kommission*, Künstliche Intelligenz – Exzellenz und Vertrauen, o.S.

einsatzfeldbezogene KI-Systeme, die aufgrund ihrer Zweckbestimmung ein erhebliches Risiko für Gesundheit, Sicherheit oder Grundrechte verkörpern und daher als hochriskant einzustufen sind (vgl. ErwG 52).[66] Aus dem Umkehrschluss zu Art. 6 Abs. 4 KI-VO und unter Zugrundelegung des Art. 3 Nr. 12 KI-VO ergibt sich, dass dem Anbieter vor Inverkehrbringen die Festlegung des Verwendungszwecks und -kontextes und somit auch die Risikoklassifizierung obliegt.[67] Anhang III listet acht Hochrisikobereiche auf: Biometrie, kritische Infrastruktur, allgemeine und berufliche Bildung (z.B. KI-Systeme zur Prüfungsbewertung), Beschäftigung, Personalmanagement und Zugang zur Selbstständigkeit (z.B. Software zur Bewertung von Jobbewerbern), Zugänglichkeit und Inanspruchnahme grundlegender privater und öffentlicher Dienste und Leistungen (z.B. KI-Systeme zur Kreditwürdigkeitsbewertung), Strafverfolgung (z.B. KI-Systeme zur Überprüfung der Echtheit von Beweismitteln), Migration, Asyl und Grenzkontrolle (z.B. KI-Systeme zur automatisierten Prüfung von Visumsanträgen) sowie Rechtspflege und demokratische Prozesse (z.B. KI-Lösungen zur Suche nach Gerichtsurteilen).[68] Ein KI-System, das in besagten Bereichen angewendet wird, gilt somit grundsätzlich als hochriskant.[69]

KI-Systeme dieser Bereiche gelten dann nicht als hochriskant, wenn sie nach Art. 6 Abs. 3 UAbs. 1 KI-VO kein erhebliches Risiko für Gesundheit, Sicherheit oder Grundrechte darstellen, was u.a. der Fall ist, wenn sie nicht das Ergebnis der Entscheidungsfindung wesentlich beeinflussen, da sie nur Hilfstätigkeiten erfüllen. Das liegt etwa vor, wenn das System dazu bestimmt ist, eng gefasste Verfahrensaufgaben vorzunehmen (Art. 6 Abs. 3 UAbs. 2 lit. a KI-VO) und den Menschen nur bei einer eigenen Entscheidung als Werkzeug unterstützt[70] – z.B. bei einer Kategorisierung von Dokumenten oder einer Erkennung von Duplikaten gem. ErwG 53 – oder wenn das KI-System zur Ergebnisverbesserung einer zuvor abgeschlossenen menschlichen Tätigkeit bestimmt ist (lit. b). Nach der Rückausnahme des Art. 6 Abs. 3 UAbs. 3 KI-VO liegt jedoch ungeachtet der nur unterstützenden Funktion stets ein HKIS vor, wenn das System ein Profiling natürlicher Personen vornimmt. Dies wäre der Fall, wenn ein KI-System Jobbewerbungen vorsortiert und automatisch auswertet, sodass der beste Bewerber vorne erscheint, weil die Auswertung personenbezogener Daten zur Prognose der Arbeitsleistung Profiling darstellt.[71]

Halten Anbieter ein dem Anhang III unterfallendes KI-System nach Abs. 3 nicht für hochriskant, haben sie ihre Einschätzung gem. Abs. 4 vor Inverkehrbringen bzw.

---

[66] *Ruschemeier*, in: KI-VO 2026 Art. 6 Rn. 2, 32, 85.
[67] *Ossmann-Magiera/Dehmel*, KIR 2024, 134, 135; *Ruschemeier*, in: KI-VO 2026 Art. 6 Rn. 86, 99; *Spiegel/Höving*, KIR 2025, 231, 232.
[68] *Kommission*, AI Act, o.S.; *Kommission*, Künstliche Intelligenz – Fragen und Antworten, o.S.
[69] *Braun Binder/Egli*, MMR 2024, 626, 627.
[70] *Hilgendorf/Härtlein*, KI-VO 2025a Art. 6 Rn. 17.
[71] *Hilgendorf/Härtlein*, KI-VO 2025a Art. 6 Rn. 24.

Inbetriebnahme zu dokumentieren und sich und das System gem. Art. 49 Abs. 2 KI-VO in der EU-Datenbank nach Art. 71 KI-VO zu registrieren. Für die Unternehmenspraxis wichtig ist, dass der Anbieter bei einer Fehleinschätzung bzgl. der Risikoeinstufung von Anfang an allen Pflichten für HKIS unterliegt.[72] Aus dem Umkehrschluss zu Art. 80 Abs. 2, 4 KI-VO ergibt sich, dass irrtümliche Fehleinschätzungen keine Geldbuße nach sich ziehen;[73] sie kommen nur bei vorsätzlicher Fehleinschätzung mit dem Ziel der Umgehung der Vorschriften für HKIS in Betracht (Art. 80 Abs. 7 KI-VO). Insofern ist Anbietern von HKIS wegen ihres Haftungsrisikos[74] Vorsicht bei der Einschätzung zu raten. Zur Unterstützung der rechtssicheren Einordnung sind bis 02.02.2026 Leitlinien mit Praxisbeispielen vorgesehen (Art. 6 Abs. 5 KI-VO). Um dem Bedürfnis nach Technologieoffenheit und der damit einhergehenden dynamischen Entwicklung von KI gerecht zu werden (ErwG 52 S. 2, Art. 6 Abs. 8 KI-VO), kann die Kommission per delegiertem Rechtsakt die Bedingungen in Art. 6 Abs. 3 UAbs. 2 KI-VO ändern (Art. 6 Abs. 6-8 KI-VO) und den Katalog des Anhangs III anpassen (Art. 7 KI-VO). Daher ist es für Rechtsanwender unerlässlich, den Rechtsstand auf Aktualität zu überprüfen und ggf. nötige Änderungen zu veranlassen, um stets im Einklang mit dem geltenden Recht zu stehen.[75]

Ein Pflichtenverstoß wird mit Geldbußen in Höhe von bis zu 15 Millionen Euro oder bis zu 3 % des weltweiten Gesamtjahresumsatzes des vorigen Geschäftsjahres, je nach dem, welcher Betrag höher ist, geahndet (Art. 99 Abs. 4 KI-VO).

III. KI-Systeme mit begrenztem Risiko

KI-Systeme mit begrenztem Risiko unterliegen den Transparenzpflichten des Art. 50 KI-VO, sofern sie nicht etwa der Strafverfolgung dienen. Umfasst sind Situationen, in denen Nutzern bewusst sein muss, dass sie mit KI interagieren.[76] Informations- und Kennzeichnungspflichten bestehen für Anbieter von KI-Systemen, die für die direkte Interaktion mit Menschen bestimmt sind (Abs. 1) oder synthetische Audio-, Bild-, Video- oder Textinhalte erzeugen (Abs. 2), ferner für Betreiber von Emotionserkennungssystemen und Systemen zur biometrischen Kategorisierung, soweit sie nicht nach Art. 5 KI-VO verboten sind (Abs. 3) sowie Betreiber eines KI-Systems, das Bild-, Ton- oder Videoinhalte erzeugt oder manipuliert, die ein Deepfake darstellen oder zu veröffentlichende Texte über Angelegenheiten von öffentlichem Interesse erzeugt oder manipuliert (Abs. 4). Beispiele für solche KI-Systeme sind Chatbots im Kundenservice auf Unternehmenswebseiten oder

[72] *Hilgendorf/Härtlein*, KI-VO 2025a Art. 6 Rn. 16.
[73] Ähnlich: *Hilgendorf/Härtlein*, KI-VO 2025a Art. 80 Rn. 3.
[74] *Chibanguza/Steege*, NJW 2024, 1769, 1772, Rn. 31.
[75] Vgl. *Klawonn*, in: BeckOK KI-Recht Art. 6 Rn. 21.
[76] *Chibanguza/Steege*, NJW 2024, 1769, 1773, Rn. 42.

Social Bots, die Inhalte in sozialen Medien erzeugen oder kommentieren (Abs. 1) sowie generative KI-Systeme, die basierend auf Trainings- und Inputdaten neue Inhalte erzeugen können (Abs. 2, 4) wie ChatGPT, Dall-E, Midjourney oder Suno AI – nicht aber Systeme zur Grammatikkontrolle mit Verbesserungsfunktion wie DeepL Write – und Systeme, die Mimik, Gestik oder Sprechverhalten auswerten, nach ErwG 18 S. 3 aber keine Systeme zur Ermüdungserkennung bei Berufskraftfahrern oder -piloten zur Unfallprävention (Abs. 3).[77] Art. 50 KI-VO bezweckt also den Schutz der Rechte und Interessen Dritter vor Täuschungs-, Manipulations- und Verwechslungsrisiken durch KI-Systeme mit menschenähnlichen Fähigkeiten, indem Betroffene informiert werden, dass sie mit einer KI interagieren; dazu adressiert Abs. 1 die Risiken eines Identitätsbetrugs oder einer Täuschung (ErwG 132 S. 1), während es Abs. 2 und 4 durch die Kennzeichnung KI-generierter oder -manipulierter Inhalte ermöglichen, diese von menschlichen Inhalten zum Schutz vor Desinformation durch Deepfakes (Art. 3 Nr. 60 KI-VO) abzugrenzen.[78] Die Transparenzpflicht des Abs. 3 dient der Information über die Verarbeitung biometrischer Daten, da etwa mittels eines „Facial Action Coding Systems", das mimischen Regungen Emotionen zuordnet, Erkenntnisse über Menschen gewonnen werden, die nur ungern offengelegt werden.[79] Praxisrelevant ist, dass ein den Pflichten des Art. 50 KI-VO unterfallendes KI-System zeitgleich ein HKIS i.S.v. Art. 6 KI-VO sein kann (z.B. ein Emotionserkennungssystem gem. Art. 6 Abs. 2 i.V.m. Anhang III Nr. 1 lit. c KI-VO); dann sind nach Art. 50 Abs. 6 KI-VO und ErwG 132 S. 1, 2 die Transparenzpflichten des Art. 50 KI-VO und die Vorgaben für HKIS nach Kapitel III einzuhalten.[80] Als Hilfe zur rechtssicheren Einhaltung der Transparenzvorgaben sind Leitlinien und Praxisleitfäden vorgesehen, deren Befolgung empfohlen wird (Art. 50 Abs. 7, 96 Abs. 1 UAbs. 1 lit. d KI-VO). Für die Gestaltung der Sanktionshöhe bei Zuwiderhandlungen gegen die Transparenzvorschriften (Art. 99 Abs. 4 lit. g KI-VO) wird auf die Ausführungen zu den HKIS verwiesen.

IV. KI-Systeme mit minimalem Risiko

KI-Systeme mit minimalem oder keinem Risiko bilden die unterste Stufe der Risikopyramide. Sie unterliegen angesichts ihrer maximal sehr geringen Auswirkungen auf Rechte Dritter keinen expliziten Vorgaben; es ist nur die Förderung der KI-Kompetenz zu beachten. Jedoch ist eine freiwillige Befolgung von Verhaltenskodizes (Art. 95 KI-VO) möglich, die etwa Vorgaben für HKIS enthalten können (vgl.

[77] *Kumkar/Griesel*, KIR 2024, 117, 125; *Lauber-Rönsberg*, in: BeckOK KI-Recht Art. 50 Rn. 14, 26; *Hilgendorf/Härtlein*, KI-VO 2025a Art. 50 Rn. 2.
[78] *Spiegel/Höving*, KIR 2025, 231, 234; *Teichmann*, ZD 2025, 495, 496; *Roth-Isigkeit*, KIR 2024, 15, 18; *Lauber-Rönsberg*, in: BeckOK KI-Recht Art. 50 Rn. 6, 7, 11, 62.
[79] *Lauber-Rönsberg*, in: BeckOK KI-Recht Art. 50 Rn. 6, 42; *Martini*, in: KI-VO 2026 Art. 50 Rn. 95.
[80] *Spiegel/Höving*, KIR 2025, 231, 235; *Lauber-Rönsberg*, in: BeckOK KI-Recht Art. 50 Rn. 2, 77; *Martini*, in: KI-VO 2026 Art. 50 Rn. 1, 21.

ErwG 165).[81] Eine Einhaltung durch nicht verpflichtete Unternehmen unterstützt diese bei der Setzung höherer Standards und kann ihnen nicht nur bei der Stärkung der Wettbewerbsfähigkeit assistieren, sondern auch Best Practices sowie das Vertrauen der Gesellschaft in KI fördern.[82] Beispiele sind KI-gestützte Spamfilter, KI-basierte Videospiele und gewisse KI-gestützte Empfehlungssysteme.[83]

V. GPAI-Modelle

GPAI-Modellen (Art. 51ff. KI-VO) wurde ein eigenes, neben dem risikobasierten Ansatz stehendes, Regulierungsregime zuteil; die Vorgaben sind zusätzlich zu denen der jeweiligen Risikostufe einzuhalten.[84] GPAI-Modelle zeichnen sich dadurch aus, dass sie eine „erhebliche allgemeine Verwendbarkeit" aufweisen, d.h. keinen festen Bestimmungszweck haben, dazu befähigt sind, „ein breites Spektrum unterschiedlicher Aufgaben kompetent zu erfüllen" und „in eine Vielzahl nachgelagerter Systeme oder Anwendungen integriert werden" können (Art. 3 Nr. 63 KI-VO). Ihr Einsatz umfasst vielfältige Anwendungsfelder und sie werden regelmäßig mit großen Datenmengen trainiert (Seite 3, Rn. 4 GPAI-Modell-Leitlinien, ErwG 97). Davon abzugrenzen sind KI-Systeme mit allgemeinem Verwendungszweck, die auf GPAI-Modellen beruhen und vielen Zwecken dienen können (Art. 3 Nr. 66 KI-VO). KI-Modelle sind essenzielle Komponenten von KI-Systemen und regelmäßig in diese integriert, sodass sie als Basis für verschiedenste Systeme dienen und deren aufgabenerfüllenden Teil, etwa Anwendungssoftware, darstellen;[85] durch weitere Elemente, z.B. eine Nutzerschnittstelle, können sie selbst zu einem KI-System werden (ErwG 97 S. 6-8). Die Vorgaben für GPAI-Modelle sind nach Integrierung des KI-Modells in ein KI-System weiter zu beachten (ErwG 97 S. 9). Zu GPAI-Modellen zählen große generative KI-Modelle, die Text-, Audio-, Bild- oder Videoinhalte erzeugen können (ErwG 99, 105 S. 1). So sind vor allem LLM's wie GPT-4, Gemini, Llama 3.1, Luminous oder die bildgenerierende KI Midjourney GPAI-Modelle.[86] Unternehmen können Sprachmodelle als Betreiber adaptieren und als Basis für eigene Wissensmanagement- und Chat-KI-Systeme nutzen.[87]

Zur Bestimmung, ob ein GPAI-Modell vorliegt, wird auf „training compute", die Rechenleistung, die zum Training eines Modells benötigt wird, abgestellt (Seite 5, Rn. 15 GPAI-Modell-Leitlinien (folgend: GPAI-ML)). Demnach liegt ein GPAI-Modell

[81] *Chibanguza/Steege*, NJW 2024, 1769, 1774, Rn. 46; *Spiegel/Höving*, KIR 2025, 231, 235.
[82] *Chibanguza/Steege*, NJW 2024, 1769, 1774, Rn. 46; *Gorzala*, in: BeckOK KI-Recht Art. 95 Rn. 2.
[83] *Wendt/Wendt*, Das neue Recht der KI, § 5 Rn. 45; *von Welser*, GRUR-Prax 2024, 485, 487, Rn. 33; *Weltersbach/Aslan*, BKR 2025, 49, 53.
[84] *Chibanguza/Steege*, NJW 2024, 1769, 1774, Rn. 47.
[85] *Hofmann-Coombe*, § 7, in: *Hilgendorf/Roth-Isigkeit*, Die neue Verordnung der EU, Rn. 17; *Möller-Klapperich*, NJ 2024, 337, 341.
[86] *Bernsteiner/Schmitt*, in: KI-VO 2026 Art. 51 Rn. 13; *von Welser*, GRUR-Prax 2024, 485, 487, Rn. 34.
[87] *Klos/Taylan*, CCZ 2024, 205, 207, 209.

vor, wenn besagte Rechenleistung eine kumulierte Menge von 10^{23} Gleitkommaoperationen (Art. 3 Nr. 67 KI-VO), gemessen in FLOP (floating point operations), überschreitet und Sprache, Bilder oder Videos aus Text generieren kann (Seite 6, Rn. 17 GPAI-ML).[88] Ein Modell, das zwar ein training compute von 10^{23} FLOP übersteigt und aus Sprache Text erzeugt, ist mangels Fähigkeit zur Erfüllung eines breiten Aufgabenspektrums aber kein GPAI-Modell, wenn es nur einen eng begrenzten Aufgabenbereich (z.B. nur Sprache transkribieren oder Bildauflösungen verbessern) bewältigen kann (Seiten 7 und 8, Rn. 20 GPAI-ML). Bei der Klassifizierung helfen die Beispiele auf den Seiten 7 und 8, Rn. 20, 21 GPAI-ML.

GPAI-Modelle werden danach unterschieden, ob von ihnen systemische Risiken ausgehen, also Risiken, die aufgrund ihrer Reichweite oder wegen vorhersehbarer negativer Folgen für wesentliche Schutzgüter erhebliche Auswirkungen auf den Unionsmarkt haben (Art. 3 Nr. 65 KI-VO), oder nicht. Eine Einstufung als GPAI-Modell mit systemischem Risiko erfolgt entweder, wenn es über Fähigkeiten mit hohem Wirkungsgrad (vgl. Art. 3 Nr. 64 KI-VO) verfügt, was bei einem Trainingsaufwand von mehr als 10^{25} FLOP vermutet wird oder wenn die Kommission anhand der Kriterien in Anhang XIII entscheidet, dass ein GPAI-Modell entsprechende Fähigkeiten oder Wirkkraft besitzt (Art. 51 Abs. 1, 2 KI-VO). Beispiele für systemische Risiken sind in ErwG 110 und im Safety-and-Security-Kapitel des GPAI-Modell-Praxisleitfadens aufgeführt (Seite 35ff.). Das Bestehen eines systemischen Risikos ist anbieterseitig unter Zugrundelegung einschlägiger Argumente widerlegbar (Art. 52 Abs. 2 KI-VO, Seiten 12 und 13, Rn. 34, 35 GPAI-ML).

Anbieter von GPAI-Modellen ohne systemisches Risiko unterliegen Dokumentations- und Transparenzpflichten, der Pflicht zur Erstellung einer Strategie zur Einhaltung des Urheberrechts sowie zur Veröffentlichung einer Trainingsdatenzusammenfassung (Art. 53 Abs. 1 KI-VO). Ergänzend können Transparenzpflichten nach Art. 50 KI-VO einschlägig sein.[89] Für frei und quelloffen lizenzierte GPAI-Modelle ohne systemisches Risiko gelten geringere Pflichten (Art. 53 Abs. 2 KI-VO). Anbieter von GPAI-Modellen mit systemischem Risiko treffen hingegen extensivere Pflichten über den ganzen Modelllebenszyklus (Seite 9, Rn. 24 GPAI-ML), darunter Anmelde-, Bewertungs-, Risikominderungs-, Dokumentations- und Cybersicherheitsvorgaben (Art. 52 Abs. 1, 55 Abs. 1 KI-VO). Daher müssen Unternehmen nicht nur prüfen, ob sie GPAI-Modelle anbieten, sondern auch, ob von diesen systemische Risiken ausgehen. Es empfiehlt sich die Konsultation der GPAI-ML für den Pflichtenumfang und der GPAI-Modell-Praxisleitfäden für die Umsetzung

[88] *Wendt/Wendt*, Das neue Recht der KI, § 11 Rn. 5.
[89] Vgl. *Becker/Feuerstack*, KIR 2024, 62, 67.

konkreter Compliance-Maßnahmen, um den Aufwand zu begrenzen (vgl. Seite 4, Rn. 10 GPAI-ML, ErwG 117 S. 1, 2). Letztere sollten bis zur Veröffentlichung harmonisierter Normen eingehalten werden, um Compliance mit den Pflichten nachzuweisen (Art. 53 Abs. 4, 55 Abs. 2 KI-VO). Aufgrund möglicher Schwellenwertanpassungen durch die Kommission (Art. 51 Abs. 3 KI-VO, Seite 6, Rn. 16 GPAI-ML, ErwG 111 S. 8) ist eine fortlaufende Überwachung der Rechtslage geboten.

VI. Zwischenergebnis

Der zweite Schritt für Unternehmen besteht darin, herauszufinden, welcher Risikokategorie ihre Anwendungen angehören. Leitlinien und Praxisleitfäden unterstützen durch Auslegung unbestimmter Rechtsbegriffe und Darstellung praxisorientierter Beispiele und Umsetzungsmaßnahmen. Da die Kommission die Klassifizierungsvoraussetzungen an den technischen Fortschritt anpassen kann, sodass KI-Systeme künftig der nächsthöheren oder -niedrigeren Kategorie angehören könnten, wodurch Unternehmen andere Vorgaben als bisher zu erfüllen hätten, ist eine stetige Beobachtung der Rechtslage geboten. Dazu gehören auch Leitlinien und Praxisleitfäden. Um der Gefahr eines Kategoriewechsels vorzubeugen, sollten Unternehmen erwägen, vorab freiwillig die Vorgaben höherer Kategorien umzusetzen; so bestünde auch bei Kategoriewechseln weiter Compliance mit der KI-VO.[90]

D. Universeller Handlungsbedarf

Nachdem Unternehmen eine Bestandsaufnahme unternommen haben, ob und inwieweit sie von der VO betroffen sind und damit die ersten Schritte des Handlungsbedarfs getätigt haben, gilt es nun, die Pflichten der VO einzuhalten.[91] Dieses Kapitel behandelt den weiteren universellen Handlungsbedarf, der alle Anbieter und Betreiber von KI-Systemen jeglicher Risikokategorien betrifft, namentlich das Mapping, die Vermittlung von KI-Kompetenz und die Einführung organisatorischer Strukturmaßnahmen. Die Umsetzung wird mittels Praxisbeispielen verdeutlicht.

I. Mapping und Sicherstellung von KI-Compliance

Zur Herstellung von Compliance mit der KI-VO sind im Rahmen einer extensiven Bestandsaufnahme sämtliche KI-Systeme zu identifizieren und sodann in einem zentralen KI-Verzeichnis unter Zuordnung der Rolle des Unternehmens (etwa Anbieter oder Betreiber), der Risikokategorie (etwa Hochrisiko oder begrenztes Risiko), der Nutzer sowie des Einsatzbereichs und der Funktionalitäten zu erfassen.[92] Als Hilfestellung bei der Einordnung dienen die detaillierten Ausführungen

[90] *Weltersbach/Aslan*, BKR 2025, 49, 53.
[91] *Klos/Taylan*, CCZ 2024, 205, 210.
[92] *Klos/Taylan*, CCZ 2024, 205, 210; *Knappertsbusch/Rappenglück*, CR 2025, 281, 283, Rn. 26; *Weltersbach/Aslan*, BKR 2025, 49, 54.

samt Praxisbeispielen in den Kapiteln B und C. Danach ist abhängig von Rolle, Risikoklasse und Einsatzbereich zu examinieren, welche Pflichten gem. der VO einzuhalten sind, bevor konkrete Umsetzungs- bzw. Risikominderungsmaßnahmen erarbeitet werden.[93] Auch diese Informationen sollten in das Verzeichnis aufgenommen werden. Eine derartige Dokumentation ermöglicht den Verantwortlichen und den Regulierungsbehörden einen umfassenden Überblick und gewährleistet Transparenz.[94] Insofern Unternehmen bereits ähnliche Verzeichnisse bzw. eine Configuration Management Database (CMDB), die Informationen aus verschiedenen Datenbeständen zentral vereint, etabliert haben, kann es zweckmäßig sein, auf diesen zur Suche nach KI-Systemen aufzubauen.[95] Einzuhalten sind je nach Risikoklassifizierung, Rolle und Einsatzbereich vor allem die Vorschriften zu den verbotenen Praktiken (Art. 5 KI-VO), HKIS (v.a. Art. 6-27 KI-VO), KI-Systemen mit begrenztem Risiko (Art. 50 KI-VO) oder GPAI-Modellen (Art. 50-55 KI-VO). Ergänzend sind einschlägige unions- und nationalrechtliche Vorschriften, insbesondere datenschutz-, wettbewerbs-, marken- und urheberrechtliche Regelungen zu beachten, etwa die eventuelle Pflicht zur Durchführung einer Datenschutz-Folgenabschätzung nach Art. 35 DSGVO oder das durch Art. 22 Abs. 1 DSGVO begründete Recht Betroffener auf Entscheidungen mit menschlicher Beteiligung.[96] Überdies kommt vor allem den §§ 44b, 60d UrhG praktische Relevanz zu, wenn Unternehmen urheberrechtlich geschützte Inhalte für ihre KI-Systeme zu Trainingszwecken verwenden oder sonstige mittels KI generierte Inhalte nutzen.[97]

Vorausschauend agierende Unternehmen sollten zudem geplante künftige KI-Einsätze reflektieren und davon ausgehend deren Auswirkungen auf Prozesse und Entscheidungsstrukturen evaluieren.[98] So ließen sich frühzeitig adäquate Maßnahmen planen. Künftig geplante KI-Systeme könnten nach dem angeführten Schema in ein separates Verzeichnis aufgenommen werden. Um eine wirksame Compliance zu ermöglichen, ist neben der Etablierung organisatorischer Strukturen zur Festlegung konkreter Zuständigkeiten, Kontrollmechanismen und Prozesse zunächst die Vermittlung von KI-Kompetenz essenziell.

II. KI-Kompetenz

KI-Kompetenz bezeichnet die Fähigkeiten, Kenntnisse und das Verständnis, die es Anbietern, Betreibern und Betroffenen ermöglichen, KI-Systeme sachkundig einzusetzen und sich der Chancen, Risiken und möglichen Schäden durch KI

[93] *Klos/Taylan*, CCZ 2024, 205, 210, 211; *Weltersbach/Aslan*, BKR 2025, 49, 54.
[94] *Klos/Taylan*, CCZ 2024, 205, 211.
[95] *Klos/Taylan*, CCZ 2024, 205, 211.
[96] *Klos/Taylan*, CCZ 2024, 205, 210; *Rappenglück/Vonthien*, RDi 2025, 398, 403, Rn. 52, 53, 54.
[97] *Rappenglück/Vonthien*, RDi 2025, 398, 403, Rn. 54.
[98] *Rappenglück/Vonthien*, RDi 2025, 398, 403, Rn. 53; *Weltersbach/Aslan*, BKR 2025, 49, 54.

bewusst zu werden (Art. 3 Nr. 56 KI-VO). Anbieter und Betreiber müssen adäquate Maßnahmen treffen, um ein ausreichendes Maß an KI-Kompetenz bei den mit KI-Systemen befassten Personen sicherzustellen. Dabei sind technische Kenntnisse, Erfahrung, Ausbildung, Schulung und der Einsatzkontext sowie die Personen, bei denen die KI-Systeme eingesetzt werden sollen, zu berücksichtigen (Art. 4 KI-VO).

Zwar erfasst Art. 4 KI-VO seinem Wortlaut nach nur Anbieter und Betreiber von KI-Systemen, nicht auch von GPAI-Modellen. Das Telos der Vorschrift liegt jedoch darin, einen maximalen Nutzen aus KI unter Wahrung der Grundrechte, Gesundheit und Sicherheit zu ermöglichen, indem alle relevanten Akteure der KI-Wertschöpfungskette die nötigen Kenntnisse erlangen, um fundierte Entscheidungen zu treffen und die Einhaltung der Vorgaben der VO sicherzustellen (ErwG 20 S. 1, 3). Die Grundgedanken der VO stützen sich also auf die Minimierung möglicher von KI ausgehender Risiken und die Förderung von Chancen durch ihren Einsatz.[99] Auch von GPAI-Modellen können Gefahren für besagte Schutzgüter ausgehen, wenn nicht ausreichend kompetentes Personal mit Kenntnissen über die Funktionsweise oder die Auswirkungen von GPAI-Modellen bzw. deren Ausgaben eingesetzt wird. Zudem findet sich die normative Verortung des Art. 4 KI-VO im ersten Kapitel („allgemeine Bestimmungen"), was indiziert, dass alle in der VO aufgeführte KI-Systeme und -Modelle von der Vorschrift erfasst sein sollten. So führen telelogische und systematische Auslegung zum selben Ergebnis. Insoweit erscheint deren Ergebnis gegenüber der philologischen Auslegung vorzugswürdig. Daher sollten auch Anbieter von GPAI-Modellen der Pflicht des Art. 4 KI-VO unterliegen.[100] Selbst bei Verneinung einer Rechtspflicht erschiene die freiwillige Vermittlung von KI-Kompetenz sinnvoll, um die Potenziale von KI zu nutzen, die Risiken zu kennen und Kunden- und Geschäftspartnervertrauen zu fördern.

Aufgrund der risikoneutralen Ausgestaltung des Art. 4 KI-VO kommt der KI-Kompetenz eine tragende Rolle zu. Sie gilt als Grundpflicht für sämtliche Anbieter und Betreiber jeglicher beruflich genutzter KI-Systeme und trägt dazu bei, dass diese die Vorgaben der KI-VO einhalten können.[101] Sobald KI in Arbeitsprozesse eingebettet ist, selbst wenn nur Chatbots oder Übersetzungssoftware genutzt werden, ist KI-Kompetenz sicherzustellen.[102] Insofern haben Unternehmen Maßnahmen zur Förderung der KI-Kompetenz anzubieten, da die bloße Bitte zur Lektüre der Gebrauchs- bzw. Trainingsanweisung eines KI-Systems an das Personal allein

[99] *BNetzA*, Hinweispapier Art. 4, S. 2.
[100] Zum selben Ergebnis kommt *Kaufmann*, in: BeckOK KI-Recht Art. 4 Rn. 16.
[101] Vgl. *Wendehorst*, in: KI-VO 2026 Art. 4 Rn. 1, 4.
[102] *Knappertsbusch/Rappenglück*, CR 2025, 281, 283, Rn. 15.

regelmäßig unzureichend ist.[103] Dennoch kann sie für Betreiber erste Anhaltspunkte zur Herstellung von KI-Kompetenz in Bezug auf das KI-System bieten.

Die Pflicht zur Sicherstellung von KI-Kompetenz geht über das eigene mit KI-Systemen befasste Personal hinaus und umfasst auch „andere Personen, die in ihrem Auftrag mit dem Betrieb und der Nutzung von KI-Systemen befasst sind" (Art. 4 KI-VO). Somit betrifft die Pflicht zur Herstellung von KI-Kompetenz nicht nur eigene weisungsgebundene Arbeitnehmer, sondern je nach Risiko auch Kunden, Auftragnehmer oder Dienstleister, etwa selbstständige Leistungserbringer oder Leiharbeitnehmer, die mit KI-Systemen arbeiten.[104] Daher ist der Auftraggeber auch für deren KI-Kompetenz verantwortlich. Bei praxisgerechter Auslegung des Art. 4 KI-VO sollte sich die Reichweite der Pflicht an den Einflussmöglichkeiten der Unternehmen auf die weiterzubildenden Personen orientieren.[105] Diese dürften in der Praxis bei „anderen Personen", die nicht ihrem arbeitsrechtlichen Weisungsrecht unterliegen, regelmäßig begrenzt sein, weshalb es zweckdienlich sein kann, künftige Vertragsverhältnisse nur noch mit solchen Externen, die in Verrichtung ihrer Arbeit mit KI-Systemen befasst sind, einzugehen, die eine KI-Kompetenz etwa durch Zertifikate oder eigene Schulungskonzepte nachweisen.[106] Es sollte vertraglich fixiert werden, dass Externe, sofern nötig, vor Systemzugriff an essenziellen Schulungen des Auftraggebers teilnehmen müssen.

Die Vermittlung von KI-Kompetenz baut auf den durch das Mapping gewonnenen Erkenntnissen zum internen KI-Einsatz auf: Die Determinierung der Funktionalitäten, Einsatzbereiche und Risikokategorien der Systeme sowie die Tätigkeiten und Rollen der Personen bilden das Fundament für eine kontextbezogene Ermittlung des individuell notwendigen Umfangs der KI-Kompetenz.[107] Zur Bestimmung des individuellen Maßes an KI-Kompetenz kann für jeden Mitarbeiter auf die Risikokategorie der KI-Systeme, mit denen er umgeht, deren Funktionalitäten, Zweck und Kontext und sein Vorwissen abgestellt werden, ferner auf seine Rolle sowie auf die Tiefe, mit der KI-Systeme genutzt, vertrieben oder entwickelt werden.[108] Darauf basierend lassen sich verschieden profunde modulare Schulungskonzepte erstellen, deren Art und Reichweite sich an besagten Faktoren orientieren, da nicht jeder Mitarbeiter den gleichen Kenntnisstand benötigt.[109] Aus Praktikabilitätsgründen

[103] *Kommission*, KI-Kompetenz – Fragen & Antworten, o.S.
[104] *Kommission*, KI-Kompetenz – Fragen & Antworten, o.S.; *Albrecht*, GWR 2025, 303, 303; *Möller-Klapperich*, NJ 2025, 193, 194.
[105] *Fleck*, KIR 2024, 99, 101; *Möller-Klapperich*, NJ 2025, 193, 197.
[106] Vgl. *Kaufmann*, in: BeckOK KI-Recht Art. 4 Rn. 24; *Möller-Klapperich*, NJ 2025, 193, 195.
[107] Vgl. *Rappenglück/Vonthien*, RDi 2025, 398, 402, Rn. 40.
[108] *BNetzA*, Hinweispapier Art. 4, S. 4; *Chibanguza/Steege*, NJW 2024, 1769, 1771, Rn. 18; *Knappertsbusch/Rappenglück*, CR 2025, 281, 283, Rn. 20.
[109] Vgl. *Fleck*, KIR 2024, 99, 101, 102.; *Rappenglück/Vonthien*, RDi 2025, 398, 402, Rn. 42.

kann die Kompetenzbemessung anstatt individuell personenbezogen auch anhand aller im selben Einsatzfeld tätigen Mitarbeiter erfolgen.[110]

Art. 4 KI-VO verlangt für alle Mitarbeiter mit KI-Bezug ein einheitliches technisches, ethisches und rechtliches Grundverständnis bezüglich KI-Systemen, das sich in technischem Basiswissen zur Funktionsweise von KI-Systemen erschöpft, wobei vorrangig Trainingsdaten, Fähigkeiten und potenzielle Fehlerquellen (z.B. Halluzinationen, Overfitting oder defizitäre Generalisierung), algorithmische Entscheidungsabläufe und systembedingte Verzerrungen (Bias), etwa aufgrund fehlerhafter Trainingsdaten, bedeutsam sind.[111] Aus ethischer Perspektive sind insbesondere Möglichkeiten zur Identifizierung manipulativer Systemeigenschaften, zur Integration von sozialen Standards in die Systemnutzung sowie zur Vermeidung diskriminierender Ergebnisse von Belang, während in rechtlicher Hinsicht Kenntnisse zu den wichtigsten gesetzlichen Vorgaben wie Verboten, Transparenzvorgaben und Haftungsrisiken eminent sind, wobei auch einschlägige Vorschriften aus anderen Rechtsgebieten wie dem Datenschutz- oder Urheberrecht zu berücksichtigen sind.[112] Datenschutzrechtlich sollten u.a. die Risiken thematisiert werden, die mit der Verarbeitung personenbezogener Daten durch ein KI-System unter Berücksichtigung der Datenschutzgrundsätze nach Art. 5 Abs. 1 DSGVO einhergehen.[113] Ferner ist das Personal hinsichtlich der Grenzen der Systeme und deren Ausgaben zu sensibilisieren – Ausgaben sind stets kritisch zu hinterfragen, anstatt blind auf deren Korrektheit zu vertrauen (Automation Bias).[114] Die Fähigkeit zur Risikoabschätzung und verständlichen Offenlegung der Konsequenzen des KI-Einsatzes für Betroffene ist aufzubauen (ErwG 20 S. 2).[115] Ziel ist also, dass Mitarbeiter Chancen und Risiken von KI kennen, wissen, wann ein KI-System vorliegt, welche Gefahren entstehen können und wie sie sicher mit KI-Systemen im Alltagsgeschäft umzugehen haben. Auch sollen sie befähigt werden, fachkundige Entscheidungen zu KI-Systemen zu treffen, die Konsequenzen KI-gestützter Entscheidungen zu verstehen, eine KI-Folgenabschätzung vorzunehmen sowie ihre Arbeitsabläufe, auch mit Blick auf sicheres Prompting, effizienter zu gestalten.[116]

Aufbauend auf einer solchen Basisschulung sollten vertiefte mehrstufige Schulungs- bzw. Fortbildungsprogramme mit individuellen Schwerpunkten auf gezielte

[110] Vgl. *Möller-Klapperich*, NJ 2025, 193, 197.
[111] *Kommission*, KI-Kompetenz – Fragen & Antworten, o.S.; *Knappertsbusch/Rappenglück*, CR 2025, 281, 283, 284, Rn. 19, 28; *Schippel*, KIR 2025, 119, 120.
[112] *Knappertsbusch/Rappenglück*, CR 2025, 281, 283, 284, Rn. 19, 27; *Rappenglück/Vonthien*, RDi 2025, 398, 402, Rn. 43.
[113] Vgl. *Rost/Wanser*, EuDIR 2025, 276, 279, Rn. 14.
[114] *Rappenglück/Vonthien*, RDi 2025, 398, 400, Rn. 19.
[115] *Knappertsbusch/Rappenglück*, CR 2025, 281, 282, Rn. 7.
[116] *Fleck*, KIR 2024, 99, 101; *Schippel*, KIR 2025, 119, 120, 123.

Personengruppen (z.B. Accounting, IT oder Personal) zugeschnitten werden – ausgehend von Bedürfnissen, Rolle und Verantwortung.[117] Während Betriebsmitarbeiter oder solche mit Kundenbezug nur so weit zu schulen sind, dass sie KI-Systeme im Tagesgeschäft effizient, sicher und verantwortungsvoll einsetzen, sich deren Auswirkungen bewusst sind und ein Verständnis für Ausgaben aufweisen, müssen IT-Sicherheitsexperten auch mit regulatorischen Anforderungen, technischen Kenntnissen wie den genutzten Algorithmen und Programmieransätzen, des Modelltrainings sowie Maßnahmen des Risikomanagements (folgend: RM) vertraut sein, die Strategien zur Risikominderung umfassen.[118] Der nötige Kompetenzumfang richtet sich ferner nach der Risikokategorie der Systeme; so benötigen etwa mit HKIS befasste Personen aufgrund der systemimmanenten Komplexität und des Risikopotenzials profundere Kenntnisse als bei anderen KI-Systemen.[119] Vor allem sind regelmäßige Schulungen der mit der menschlichen Aufsicht (Art. 14 KI-VO) betrauten Personen unerlässlich, um die Systeme adäquat überwachen zu können und potenzielle Risiken frühestmöglich zu erkennen und zu vermeiden oder mindern (vgl. ErwG 73),[120] wobei Art. 14 Abs. 4 KI-VO das Maß an KI-Kompetenz bei der menschlichen Aufsicht konkretisiert. Insofern bildet Art. 4 KI-VO den Grundstein für die Erfüllung der Pflichten aus Art. 16, 26 Abs. 2 KI-VO. Extensive KI-Kompetenzen, etwa in Bezug auf rechtliche Vorgaben, ethische Fallstricke, Kontrollmechanismen oder vertiefte technische Kenntnisse benötigen ferner z.B. Juristen, Entwickler, technische Mitarbeiter oder Entscheidungsträger.[121] Der Ansatz des mehrstufigen Schulungsmodells wird bereits in vielen Unternehmen angewandt, darunter Generali, IBM und EnBW; Generali differenziert sein Schulungskonzept etwa in Basiskurse für alle zur Vermittlung eines einheitlichen KI-Grundverständnisses, vertiefende Kurse für Mitarbeiter mit direktem KI-Bezug und fortgeschrittene Kurse für Mitarbeiter in der Entwicklung von KI-Systemen.[122]

Die Ausgestaltung der Schulungen ist den Unternehmen überlassen, es ist jedoch „nach besten Kräften sicherzustellen“ (Art. 4 KI-VO), dass eine „ausreichende“ KI-Kompetenz aufgebaut wird. Wann diese vorliegt, regelt die VO nicht. Legt man diesen Passus philologisch aus, erschließt sich, dass sich Unternehmen jedenfalls ernsthaft in zumutbarer Weise um eine angemessene Vermittlung von KI-Kompetenz bemühen müssen. Demnach impliziert besagte Passage, dass die verschieden profunde Vermittlung von KI-Kompetenz auch von den zur Verfügung

[117] *Albrecht*, GWR 2025, 303, 304; *Fleck*, KIR 2024, 99, 101; *Schippel*, KIR 2025, 119, 120, 123.
[118] *Schippel*, KIR 2025, 119, 122, 123.
[119] *Kaufmann*, in: BeckOK KI-Recht Art. 4 Rn. 40; *Schippel*, KIR 2025, 119, 121.
[120] *Schippel*, KIR 2025, 119, 121, 122.
[121] *Kommission*, KI-Kompetenz – Fragen & Antworten, o.S.
[122] *KI-Büro*, Living Repository, S. 10, 15, 24.

stehenden Ressourcen (finanziell und personell) abhängt, sodass an große, international agierende Unternehmen höhere Anforderungen zu stellen sind als an KMU.[123] Generell sind Schulungen möglichst nutzerfreundlich und anwendungsorientiert mit Fallbeispielen aus dem Arbeitsalltag zu konzipieren.[124] Dabei sollte ein interdisziplinärer Ansatz verfolgt werden, indem technische, rechtliche und ethische Aspekte vermittelt werden. Booking.com schult etwa seine Mitarbeiter der Rechtsabteilung beim Einsatz von KI zur Betrugserkennung in Zahlungssystemen, um Kreditkartenbetrug entgegenzuwirken.[125]

Zwar dürfen Schulungen unternehmensintern erfolgen, angesichts fundierterer Expertise kann es aber zweckmäßig sein, sie von spezialisierten externen Dienstleistern, qualifizierten Bildungseinrichtungen oder Lernplattformen durchführen zu lassen.[126] Maßgeblich ist allein, dass die Mitarbeiter im Anschluss als KI-kompetent gelten, mithin KI-Systeme kontextadäquat, verantwortungsvoll und rechtskonform einsetzen und Folgewirkungen berücksichtigen können,[127] sodass Fehlanwendungen, Sicherheitsrisiken und nicht intendierte Diskriminierungen erkannt und verhindert werden können.[128] Ob ein angemessenes KI-Kompetenzniveau besteht, lässt sich mittels interner Governance- und Compliance-Strukturen oder anhand etablierter Standards wie der ISO/IEC 42001:2023 für KI-Managementsysteme prüfen.[129] Ergänzend sind Abschlusstests nach Schulungen empfehlenswert; bei Nichtbestehen des Tests, sind weitere Schulungen erforderlich. Zur nachhaltigen Sicherstellung von KI-Kompetenz dient eine regelmäßige Überprüfung durch simulierte Testszenarien, um die Handlungssicherheit und den Wissensstand der Mitarbeiter zu evaluieren. Bei Defiziten sollten gezielte Nachschulungen erfolgen, um die ermittelten individuellen Kompetenzlücken zu schließen.

Außerdem können standardisierte Zertifizierungsprogramme anerkannter Institutionen zur Sicherung eines homogenen Kompetenzniveaus beitragen, was vor allem bei HKIS und in regulierten Branchen nötig erscheint, wo angesichts extensiver Pflichten und erhöhter Risiken einheitliche, vertiefte Kenntnisse der befassten Personen erforderlich sind.[130] Um KI-Kompetenz lebhaft zu vermitteln, eignen sich zudem praxisorientierte interaktive bzw. gruppenbasierte Formate wie Workshops, simulierte praxisnahe Entscheidungsszenarien, Planspiele oder projektbezogenes

[123] Vgl. *Fleck*, KIR 2024, 99, 101.
[124] *Fleck*, KIR 2024, 99, 101.
[125] *KI-Büro*, Living Repository, S. 12.
[126] *Fleck*, KIR 2024, 99, 102.
[127] *Knappertsbusch/Rappenglück*, CR 2025, 281, 283, Rn. 21.
[128] *Rappenglück/Vonthien*, RDi 2025, 398, 400, Rn. 19.
[129] *Knappertsbusch/Rappenglück*, CR 2025, 281, 283, Rn. 25.
[130] *Rappenglück/Vonthien*, RDi 2025, 398, 402, 403 Rn. 46; *Wendehorst*, in: KI-VO 2026 Art. 4 Rn. 39.

Lernen.[131] So kann die Problemlösungsfähigkeit im Umgang mit KI-Systemen im Austausch mit anderen trainiert werden, wodurch das (technische) Verständnis gefördert wird.[132] Sinnvoll ist hierbei eine bereichsübergreifende Zusammensetzung der Teilnehmer, um Perspektivwechsel und Wissensaustausch zu ermöglichen.[133] Interaktive Formate sollten zeitlich gesehen auf modulare Schulungen folgen, um das theoretisch erlangte Wissen anhand von Praxisbeispielen in simulierter Umgebung zu testen. Ein Beispiel für interaktive Lernformate bietet IBM mit der „watsonx Challenge", bei der Mitarbeiter freiwillig KI-Lösungen für ihren Arbeitsbereich auf Basis der unternehmenseigenen Plattform entwickeln und damit ihr KI-Wissen in der Praxis anwenden.[134] Die hohe Beteiligung von 60 %[135] zeigt, dass spielerische Formate zur Etablierung einer innovationsfreundlichen Unternehmenskultur beitragen und Mitarbeiter zum Aufbau einer profunderen KI-Kompetenz motivieren können. Ein weiteres Beispiel bietet das Energieunternehmen Verbund mit seiner „FrAIday" Initiative, bei der Mitarbeiter in freiwilligen monatlichen 50-minütigen Sessions in Form von Vorträgen, Fragerunden und einem Quiz neue KI-Funktionalitäten kennenlernen.[136] Außerdem empfehlen sich regelmäßige interne Austauschrunden, in denen Erfahrungen mit KI geteilt werden.

Überdies kann KI-Kompetenz mittels interner oder externer E-Learning-Plattformen vermittelt werden, die flexibles Lernen ermöglichen und bei konkretem Bedarf in einer Praxissituation unterstützen können. Als Inhalte bieten sich zu bearbeitende Aufgaben, Videovorträge oder Podcasts an, die synchron oder asynchron vorliegen und an die Mitarbeiterrolle und die Komplexität des entsprechenden KI-Systems anknüpfen.[137] Als Umsetzungsbeispiel dient die interne Lernplattform von IBM, die, je nach Aufgabengebiet und Einsatzkontext, unterschiedlich profunde Schulungsmodule anbietet und eine jährliche Mindestlernzeit von 40 Stunden vorsieht.[138] Weitere geeignete Maßnahmen sind Kooperationen mit Forschungseinrichtungen oder Universitäten und der Aufbau einer Feedback-Kultur.[139] In Zusammenarbeit mit besagten Institutionen hat Generali etwa interne KI-Akademien erschaffen, um talentierte Mitarbeiter für neue KI-bezogene Jobs auszubilden.[140]

Als Orientierung dient das vom KI-Büro herausgegebene „Living Repository of AI Literacy Practices", das Praxisbeispiele zur Vermittlung von KI-Kompetenz

[131] *Rappenglück/Vonthien*, RDi 2025, 398, 403 Rn. 46; *Schippel*, KIR 2025, 119, 122.
[132] *Wendehorst*, in: KI-VO 2026 Art. 4 Rn. 40.
[133] *Wendehorst*, in: KI-VO 2026 Art. 4 Rn. 41.
[134] *KI-Büro*, Living Repository, S. 24, 25.
[135] *KI-Büro*, Living Repository, S. 25.
[136] *KI-Büro*, Living Repository, S. 71, 72.
[137] Vgl. *KI-Büro*, Living Repository, S. 10.
[138] *KI-Büro*, Living Repository, S. 24.
[139] *KI-Büro*, Living Repository, S. 7, 9, 35, 70, 72.
[140] *KI-Büro*, Living Repository, S. 10.

illustriert und so Anregungen für eigene Konzepte bietet, ohne dabei die enthaltenen Beispiele auf eine Konformität mit Art. 4 KI-VO zu bewerten.[141] Anhand der Diversität der dort vertretenen Ansätze zeigt sich, dass die Vermittlung stets individuell unter Beachtung der bereits dargelegten Faktoren zu erfolgen hat. Ferner unterstützt das KI-Büro im Zuge des KI-Pakts bei der Vermittlung von KI-Kompetenz mittels Veranstaltungen und Webinaren zum Wissensaustausch; zusätzlich stellt die Lernplattform „KI-Campus" Onlinekurse, Videos, Podcasts und Tools bereit.[142] Für KMU und Startups bieten die European Digital Innovation Hubs (EDIHs) und die Mittelstand-Digital Zentren (MDZ) individuelle Unterstützung beim Aufbau von KI-Kompetenz, u.a. durch Workshops, Roadshows und Vorträge.[143]

Die VO sieht keine expliziten Sanktionen für Verstöße gegen Art. 4 KI-VO vor; die EU-Staaten normieren nach Art. 99 Abs. 1 KI-VO nationale Sanktionen.[144] Unzureichende KI-Kompetenz kann aber aufsichts-, zivil- oder ordnungsrechtliche Folgen sowie Reputations- und Vertrauensverluste nach sich ziehen.[145] Sie kann zudem hinsichtlich der nach Art. 26 Abs. 2 KI-VO gebotenen menschlichen Aufsicht bei HKIS mittelbar bußgeldrelevant (Art. 99 Abs. 4 lit. e KI-VO) und mittelbar bei der Bußgeldbemessung nach Art. 99 Abs. 7 KI-VO bei Verstößen gegen andere Vorgaben bedeutsam sein.[146] Zivilrechtlich kann mangelnde KI-Kompetenz wegen nicht erfolgter Schulungen und Mitarbeiterqualifizierungen haftungsbegründend sein, da dies als Verletzung von Verkehrspflichten nach § 823 Abs. 1 BGB oder Verstoß gegen Schutzgesetze nach § 823 Abs. 2 BGB gewertet werden kann, wenn etwa Risiken verkannt, diskriminierende Entscheidungen gefällt oder Rechtsgüter Dritter infolge einer Verletzung von Kontrollpflichten geschädigt werden.[147] Ab 02.08.2026 soll die Einhaltung des Art. 4 KI-VO kontrolliert werden, wobei das KI-Büro keine „strengen Anforderungen" an die Vorschrift stellt.[148]

III. Einführung organisatorischer Strukturmaßnahmen

Zur Sicherstellung von KI-Compliance und KI-Kompetenz sind organisatorische Maßnahmen zu ergreifen. Zu empfehlen ist die Implementierung einer verbindlichen KI-Richtlinie bzw. von Standards zur Sicherstellung eines unternehmenseinheitlichen Stands, alternativ können vorhandene Compliance-Richtlinien um einen KI-Abschnitt ergänzt werden.[149] Der Inhalt ist auf das jeweilige Unternehmen,

[141] *KI-Büro*, Living Repository, S. 1.
[142] *BNetzA*, Hinweispapier Art. 4, S. 6, 7.
[143] *BNetzA*, Hinweispapier Art. 4, S. 6, 7; *Kommission*, KI-Kompetenz – Fragen & Antworten, o.S.
[144] Bisher fehlt eine solche Sanktionsregelung noch, vgl. Art. 1 § 15 des Referentenentwurfs.
[145] *Rappenglück/Vonthien*, RDi 2025, 398, 401, Rn. 29, 35.
[146] *Knappertsbusch/Rappenglück*, CR 2025, 281, 282, 284 Rn. 7, 32.
[147] *Rappenglück/Vonthien*, RDi 2025, 398,401, Rn. 30,31; *Wendehorst*, in: KI-VO 2026 Art.4 Rn.15.
[148] *Kommission*, KI-Kompetenz – Fragen & Antworten, o.S.
[149] *Kaufmann*, in: BeckOK KI-Recht Art. 4 Rn. 37; *Klos/Taylan*, CCZ 2024, 205, 210; *Wendehorst*, in: KI-VO 2026 Art. 4 Rn. 33.

abhängig von Branche und Einsatzfeld der KI-Systeme, zuzuschneiden. Es sollten Verantwortlichkeiten, Kontrollinstanzen und allgemeine Vorgaben zum reflektierten Umgang mit KI-Systemen und Risiken determiniert, etwa Regelungen zur Auswahl, Beschaffung und Verwaltung, und die Einhaltung der Vorgaben der KI-VO und anderer einschlägiger Rechtsgebiete sichergestellt werden.[150] Auch sollte verankert werden, welche KI-Systeme zulässig sind, welche Prüf- und Genehmigungsprozesse neue KI-Systeme durchlaufen müssen und in welchen Zyklen Anwendungsbewertungen der KI-Systeme erfolgen.[151] Ferner können Best Practices und ethische Grundsätze den Mitarbeitern Anhaltspunkte zum Umgang mit KI-Systemen bieten.[152] Aus Transparenzgründen sollten detaillierte Dokumentations- und Nachweispflichten sowie Regelungen zur Überwachung der Systemanwendung fixiert werden.[153] So ist in haftungstechnischer Sicht die Aufbewahrung von Zertifikaten und Dokumentation von Art und Zeitpunkt jeder absolvierten Schulung in Bezug auf sämtliche Mitarbeiter sowie weiterer Maßnahmen zur Vermittlung von KI-Kompetenz und zur Herstellung von Compliance mit den KI-VO-Vorgaben essenziell, um fehlendes Verschulden infolge einer Verletzung des Art. 4 KI-VO in Bußgeldverfahren nachzuweisen.[154] Sinnvoll ist zudem die Festlegung regelmäßiger Schulungsintervalle (je nach Rolle und Einsatzfeld z.B. quartalsweise oder jährlich) und ergänzender Schulungspflichten bei Einführung neuer oder wesentlicher Änderung oder Kategoriewechsel bestehender KI-Systeme. Die Nutzung und Erweiterung eines Compliance Management Systems bietet sich an.[155]

Eine weitere fakultative Maßnahme ist die Benennung eines KI-Beauftragten. Es kann eine neue zentrale Stelle errichtet oder der Aufgabenbereich einer bestehenden erweitert werden;[156] so könnten etwa Datenschutz- oder IT-Sicherheitsbeauftragte zusätzlich als KI-Beauftragte fungieren, sofern kein Interessenkonflikt besteht. Alternativ kann ein interdisziplinäres KI-Gremium errichtet werden, dem Mitarbeiter aus den Bereichen Compliance, Recht, IT, Datenschutz, RM, Personal und den operativen Geschäftsbereichen angehören könnten.[157] Dieser Ansatz eignet sich vor allem für große Unternehmen, in denen KI dezentral verwendet wird und diverse Bereiche tangiert sind; er bietet den Vorteil der Aggregation spezifischer Expertise, wodurch ein holistischer Ansatz im Umgang mit KI verfolgt

[150] *Klos/Taylan*, CCZ 2024, 205, 210; *Rappenglück/Vonthien*, RDi 2025, 398, 404, Rn. 58, 59; *Weltersbach/Aslan*, BKR 2025, 49, 51.
[151] *Albrecht*, GWR 2025, 303, 304; *Rappenglück/Vonthien*, RDi 2025, 398, 404, Rn. 59.
[152] *Wendehorst*, in: KI-VO 2026 Art. 4 Rn. 33.
[153] *Albrecht*, GWR 2025, 303, 304; *Klos/Taylan*, CCZ 2024, 205, 211; *Rappenglück/Vonthien*, RDi 2025, 398, 404, Rn. 61.
[154] *BNetzA*, Hinweispapier Art. 4, S. 3, 5; *Kommission*, KI-Kompetenz – Fragen & Antworten, o.S.; *Albrecht*, GWR 2025, 303, 304; *Kaufmann*, in: BeckOK KI-Recht Art. 4 Rn. 50.
[155] *Klos/Taylan*, CCZ 2024, 205, 210.
[156] *Klos/Taylan*, CCZ 2024, 205, 210.
[157] *Klos/Taylan*, CCZ 2024, 205, 210; *Rappenglück/Vonthien*, RDi 2025, 398, 404, Rn. 65.

würde.[158] Zu den Aufgaben zählt sicherzustellen, dass rechtliche Vorgaben eingehalten und Risikobewertungen durchgeführt werden, um Risiken frühzeitig zu erkennen und Reduktionsmaßnahmen einzuleiten.[159] Hinzu tritt die Mitwirkung an der strategischen Ausrichtung der KI-Nutzung durch Etablierung einer KI-Strategie und Planung und Umsetzung von KI-Projekten; ferner übernähme sie die Koordination von KI-Kompetenz-Schulungen, das Monitoring der KI-Richtlinie, die Funktion des Ansprechpartners für KI-bezogene Fragen und die abteilungsübergreifende Abstimmung zwischen Geschäftsleitung, Compliance und IT, auch im Hinblick, ob die KI-Strategie mit den Unternehmenszielen harmonisiert.[160] Ergänzend obliegt ihr die Beobachtung und Umsetzung regulatorischer Entwicklungen, vor allem in Bezug auf Änderungen der VO oder veröffentlichte harmonisierte Normen und Leitlinien. Der Mehrwert der Stelle liegt somit in der rechtlichen Absicherung des KI-Einsatzes und der Etablierung überprüfbarer Strukturen zur Sicherung von KI-Kompetenz.[161] Alternativ können einzelne Mitarbeiter aller Abteilungen besonders trainiert werden, um ihrer Abteilung als Anlaufstelle bei KI-Fragen zu dienen und dort für einen verantwortungsvollen KI-Umgang zu sorgen.[162]

Aufgrund des dynamischen technologischen Fortschritts sind KI-Richtlinien, Schulungskonzepte und weitere Maßnahmen zur Vermittlung von KI-Kompetenz regelmäßig auf Aktualität und Effektivität zu evaluieren und an neue regulatorische, judikative und technologische Entwicklungen anzupassen.[163] In der Praxis etwa evaluiert Generali seine Maßnahmen jährlich und ergänzt sie bei Bedarf, während IBM seine Lernplattform ebenfalls ständig um neue Inhalte ergänzt.[164] Zur Bewertung der Effektivität der KI-Kompetenz-Maßnahmen bietet es sich an, qualitative und quantitative Kennzahlen zu messen, um Defizite systematisch zu identifizieren, Programme zu optimieren und den Fortschritt zu verfolgen. Erfasst werden können Teilnahmequoten, erfolgreiche Kursabschlüsse, die mitarbeiterbezogene auf der Lernplattform verbrachte Lernzeit, die auf Feedback basierende Zufriedenheit der Teilnehmer mit den Inhalten hinsichtlich bedarfsgerechter Anpassungen oder der individuell wahrgenommene Kompetenzzuwachs der Mitarbeiter.[165]

IV. Zwischenergebnis

Die Vermittlung von KI-Kompetenz gilt als zentrale, iterativ überprüfbare Pflicht für alle Anbieter und Betreiber von KI-Systemen. Sie kann durch eine obligatorische

[158] *Klos/Taylan*, CCZ 2024, 205, 210; *Rappenglück/Vonthien*, RDi 2025, 398, 404, Rn. 65.
[159] *Klos/Taylan*, CCZ 2024, 205, 210.
[160] *Kaufmann*, in: BeckOK KI-Recht Art. 4 Rn. 44; *Wendehorst*, in: KI-VO 2026 Art. 4 Rn. 42, 43.
[161] *Rappenglück/Vonthien*, RDi 2025, 398, 404, Rn. 64, 66.
[162] *KI-Büro*, Living Repository, S. 34, 35.
[163] *Rappenglück/Vonthien*, RDi 2025, 398, 402, Rn. 44; *Schippel*, KIR 2025, 119, 121.
[164] *KI-Büro*, Living Repository, S. 11, 25.
[165] *KI-Büro*, Living Repository, S. 11, 16, 25.

Basisschulung aller Mitarbeiter zur Schaffung eines einheitlichen KI-Grundverständnisses und darauf aufbauenden, rollen- und aufgabenspezifischen Vertiefungsschulungen, sichergestellt werden, zusätzlich durch interaktive praxisorientierte Workshops, Simulationsszenarien und eine E-Learning-Plattform. Eine Vielfalt unterschiedlicher Lernformate kann das Mitarbeiterengagement erhöhen. Zur nachhaltigen Sicherung der Einhaltung der KI-VO-Vorgaben und KI-Kompetenz sollten flankierende organisatorische Maßnahmen wie die Etablierung verbindlicher KI-Richtlinien, die Ernennung eines KI-Beauftragten und die regelmäßige Weiterentwicklung und Aktualisierung der Maßnahmen erfolgen. Die konkrete Reichweite der KI-Kompetenz ist umstritten. Um Verstöße gegen Art. 4 KI-VO zu vermeiden und Unternehmensstrukturen und Mitarbeiter zukunftssicher aufzustellen, empfiehlt es sich, einen eher weiteren KI-Kompetenz-Begriff zu verfolgen und Mitarbeitern eher zu tiefe als zu oberflächliche Kenntnisse zu vermitteln, was zugleich vertrauensbildend gegenüber Kunden und Partnern wirken kann. Bis zu einer Konkretisierung (etwa durch die Rechtsprechung) können sich Unternehmen zum Aufbau von Strukturen zur Sicherung von KI-Compliance und zur Vermittlung von KI-Kompetenz an den Good Practices des Living Repository orientieren.

E. Risikospezifischer Handlungsbedarf

Im Anschluss an die risikoneutrale Pflicht zur Herstellung von KI-Kompetenz wird nun der risikospezifische Handlungsbedarf ausgehend von der vorgenommenen Risikoklassifizierung der Anwendungen anhand selektierter Pflichten erläutert und deren praktische Umsetzung illustriert. Der Fokus liegt auf HKIS und KI-Systemen mit begrenztem Risiko, GPAI-Modelle bleiben außer Betracht.

I. Handlungsbedarf für Anbieter und Betreiber von verbotenen KI-Systemen und KI-Systemen mit minimalem Risiko

Der Handlungsbedarf in Bezug auf nach Art. 5 KI-VO verbotene KI-Systeme beschränkt sich darauf, deren Inverkehrbringen, Inbetriebnahme oder Verwendung umgehend zu unterlassen, da diese Praktiken untersagt und bußgeldbewährt sind (Art. 99 Abs. 3 KI-VO). Insofern ist das KI-System derart zu verändern, dass kein Verbotstatbestand mehr erfüllt ist oder es muss gelöscht bzw. vernichtet werden. Bei an Dritte lizenzierten Systemen können im Zuge des Löschens bzw. Vernichtens vertragliche Konflikte entstehen, die sich aber über die Grundsätze der Unmöglichkeit oder (Teil-)Nichtigkeit von Rechtsnormen zuwiderlaufender Rechtsgeschäfte lösen lassen (§§ 275 Abs. 1, 326 Abs. 1 BGB bzw. §§ 134, 139 BGB).[166]

[166] *Kress/Mienert*, Umgang mit verbotenen KI-Systemen, in: *Baum et al.*, Umsetzungsleitfaden zur KI-VO, S. 84.

Für KI-Systeme mit minimalem Risiko besteht kein obligatorischer Handlungsbedarf. Eine freiwillige Einhaltung von Verhaltenskodizes nach Art. 95 KI-VO ist möglich und kann Wettbewerbsfähigkeit, Reputation und Kundenvertrauen stärken.

II. Handlungsbedarf für Anbieter und Betreiber von Hochrisiko-KI-Systemen

Zunächst wird eine Übersicht samt Umsetzungshinweisen zu den Anforderungen und Pflichten der Anbieter und Betreiber von HKIS illustriert. Es folgen detaillierte Ausführungen zur praktischen Umsetzung des für HKIS besonders relevanten RM.

1. Übersicht über den Handlungsbedarf für Anbieter und Betreiber

Anbieter von HKIS haben gem. Art. 16 lit. a KI-VO vor Markteinführung die Einhaltung der Art. 8-15 KI-VO sicherzustellen. Die Regelungen verlangen im Rahmen eines Compliance-by-Design-Ansatzes teils eine spezifische Systemkonzeption, um Compliance-Verstöße zu minimieren.[167] Nach Art. 8 Abs. 1 S. 1 KI-VO ist bei Erfüllung der Art. 8-15 KI-VO der Systemzweckbestimmung Rechnung zu tragen, sodass je nach System disparate Risikominderungsmaßnahmen statthaft sind, und der „allgemein anerkannte Stand der Technik" zu beachten: das, was je nach Branche als adäquat angesehen wird.[168] Art. 8 Abs. 2 KI-VO erlaubt Anbietern von Systemen nach Art. 6 i.V.m. Anhang I Abschnitt A KI-VO die Integration der Vorgaben der Art. 9-15 KI-VO in existente Verfahren des Produktsicherheitsrechts.

Der Handlungsbedarf besteht zunächst in der Etablierung eines zweckbezogenen, den gesamten Lebenszyklus des HKIS umfassenden und regelmäßig zu aktualisierenden RM (Art. 9 KI-VO), um potenzielle Risiken identifizieren und beurteilen sowie adäquate Maßnahmen ergreifen zu können. Ferner sind die Vorgaben der Daten-Governance einzuhalten. Werden datenbasierte Trainingsverfahren angewandt, ist eine ausreichende Trainings-, Validierungs- und Testdatenqualität hinsichtlich Genauigkeit, Relevanz, Repräsentativität und Vollständigkeit zu gewährleisten. Die Datensätze müssen typische kontextsensitive, geografische und funktionale Gegebenheiten abbilden und sind auf drohende Diskriminierungen, Sicherheits- oder Gesundheitsrisiken infolge von Verzerrungen zu prüfen (Art. 10 KI-VO); diese sind durch geeignete Maßnahmen zu minimieren.[169] Ziel ist die Erzeugung qualitativ hochwertiger, fehlerfreier und fairer Ergebnisse. Dabei sind zugleich die Pflichten der DSGVO einzuhalten (vgl. Art. 2 Abs. 7 KI-VO, ErwG 27 S. 4, 7), vor allem bezüglich der rechtmäßigen Trainingsdatenerhebung.[170] Nach einem Urteil des OLG Köln kann die Nutzung „öffentlicher" personenbezogener Daten aus

[167] *Wendt/Wendt*, Das neue Recht der KI, § 7 Rn. 5.
[168] *Spindler/Gerdemann*, § 5, in: *Hilgendorf/Roth-Isigkeit*, Die neue Verordnung der EU, Rn. 2.
[169] *Becker/Feuerstack*, KIR 2024, 62, 66; *Teichmann*, ZD 2025, 495, 497; *Wendt/Wendt*, Das neue Recht der KI, § 6 Rn. 16, 18.
[170] OLG Köln, Urteil v. 23. Mai 2025 – 15 UKl 2/25 –, juris (Rn. 46); *Teichmann*, ZD 2025, 495, 500.

sozialen Netzwerken zulässig sein, wenn aufgrund der Datenmenge keine Identifizierung Einzelner möglich ist.[171] Zur Stärkung der Rechtssicherheit erscheint eine Konkretisierung der unbestimmten Rechtsbegriffe der Relevanz und Repräsentativität (Art. 10 Abs. 3 S. 1 KI-VO) geboten. Zudem sind die Vorgaben an die technische Dokumentation (Art. 11 KI-VO) als Compliance-Nachweis und zur Prüfung durch die nationalen Behörden und notifizierten Stellen einzuhalten. Sie ist vor Inverkehrbringen oder Inbetriebnahme zu erstellen, permanent zu aktualisieren und hat sich inhaltlich an Anhang IV zu orientieren, wonach etwa die Zweckbestimmung oder Informationen über die Überwachung, Kontrolle und Funktionsweise des Systems umfasst sind. KMU und Startups profitieren von Erleichterungen.

Überdies sind den Lebenszyklus umfassende Aufzeichnungspflichten zu befolgen (Art. 12 KI-VO). Um Risiken nach Art. 79 Abs. 1 KI-VO zu erkennen und die Systemüberwachung gem. Art. 72 KI-VO zu erleichtern, werden gewisse Ereignisse über Protokolle („Logs“) automatisch aufgezeichnet; so sind das Funktionieren des Systems bzw. dessen Entscheidungen lückenlos rückverfolgbar.[172] Es sind etwa relevante Protokolle wie Abfrageereignisse oder Entscheidungspfade zu speichern, um bei Vorfällen Ursachenforschung betreiben und Entscheidungen nachvollziehen zu können.[173] Zudem sind Systeme so transparent zu gestalten, dass Betreiber ihre Ausgaben angemessen interpretieren und das System korrekt und sicher verwenden können (Art. 13 KI-VO), wobei Betriebsanleitungen unterstützen, die etwa über Fähigkeiten, Leistungsgrenzen und Software-Updates des KI-Systems oder Maßnahmen zur menschlichen Aufsicht informieren (Art. 13 Abs. 3 lit. b, d, e KI-VO). Eine wirksame menschliche Aufsicht ist während des gesamten Lebenszyklus insofern sicherzustellen, als dass es der betreiberseitig mit dieser Aufgabe betrauten Person möglich sein muss, Systemfehlfunktionen zu erkennen und zu beheben, Ausgaben korrekt zu interpretieren und ihnen nicht übermäßig zu vertrauen – Systeme erzeugen nur Empfehlungen, auf denen basierend Menschen als letztentscheidungsbefugte Instanz eine Wahl fällen – und den Betrieb etwa mittels einer Stopptaste zu beenden (Art. 14 KI-VO). Die Aufsichtsperson muss das System verstehen und beeinflussen können („Human-in-the-Loop“), eine tiefgehende Erklärbarkeit i.S.v. „Explainable AI“ (xAI) ist nicht nötig.[174] Zuletzt müssen die Systeme kontinuierlich ein angemessenes Maß an Genauigkeit, Robustheit und Cybersicherheit gewährleisten (Art. 15 KI-VO). Dies erfordert Resilienz sowohl gegenüber Fehlern aufgrund interner wie externer Faktoren und dass sie Störungssicherheitspläne und Fail-Safe-Vorkehrungen zur Schadensminimierung

[171] OLG Köln, Urteil v. 23. Mai 2025 – 15 UKl 2/25 –, juris (Rn. 49, 91, 96, 98, 99, 115, 116, 118).
[172] *Becker/Feuerstack*, KIR 2024, 62, 66; *Weltersbach/Aslan*, BKR 2025, 49, 55.
[173] *Teichmann*, ZD 2025, 495, 497.
[174] *Dienes*, MMR 2024, 456, 461; *Teichmann*, ZD 2025, 495, 497.

enthalten, um Ausfälle abfedern zu können (technische Redundanz),[175] als auch gegen Versuche Dritter, Ausgaben durch Ausnutzen von Systemschwächen zu verändern (Art. 15 Abs. 4, 5 KI-VO). Daher sind Maßnahmen zu treffen, die unautorisierten Zugriff und Manipulation verhindern, damit das System beständig funktionieren kann. Es muss durch präventive Maßnahmen zur Angriffserkennung, -beseitigung und -vermeidung auf Cyberangriffe wie „Adversarial Attacks" vorbereitet sein – dabei handelt es sich um Datenvergiftung (Trainingsdatensatzmanipulation) im Rahmen des Lernvorgangs, Modellvergiftung (Manipulation vortrainierter Komponenten) oder Eingaben mit dem Zweck, das Modell zu täuschen, was etwa mittels marginal modifizierter Bilder zur Überlistung eines Erkennungssystems erfolgen kann (feindliche Beispiele oder Modellumgehung).[176] Bei der Umsetzung kann die ISO/IEC TR 24028 helfen. Zur Bestimmung des Genauigkeits- und Robustheitsmaßes sollen Benchmarks und Messmethoden entwickelt werden (Art. 15 Abs. 2 KI-VO). Bei nach Inverkehrbringen oder Inbetriebnahme iterativ weiterlernenden HKIS sind „Rückkopplungsschleifen", d.h. eine Beeinflussung früherer verzerrter Ausgaben auf künftige Vorgänge, möglichst zu verhindern und angemessene Risikominderungsmaßnahmen zu konzipieren (Art. 15 Abs. 4 UAbs. 3 KI-VO). Nach Veröffentlichung harmonisierter Normen sollten Anbieter ihre HKIS an diesen ausrichten, um die Konformitätsvermutung des Systems nach Art. 40 Abs. 1 KI-VO mit den Vorgaben der Art. 8-15 KI-VO auszulösen.[177]

Ferner sind Anbieter nach Art. 16 lit. b-l KI-VO verpflichtet, ihren eingetragenen Handelsnamen bzw. ihre -marke und Kontaktanschrift anzugeben, ein Qualitätsmanagement (folgend: QM) nach Art. 17 KI-VO einzurichten und die Dokumentation nach Art. 18 KI-VO sowie grundsätzlich die in ihren HKIS automatisch erzeugten Protokolle gem. Art. 19 i.V.m. Art. 12 Abs. 1 KI-VO aufzubewahren. Zu den QM-Mindestanforderungen zählen nach Art. 17 Abs. 1 KI-VO die Implementierung eines Compliance-Konzepts bezüglich Änderungen an dem KI-System, Untersuchungs-, Test- und Validierungsverfahren vor, während und nach Systementwicklung sowie die Etablierung eines Risikomanagementsystems (folgend: RMS (Art. 9 KI-VO)). Harmonisierte Normen mit Querschnittsfunktion für QM und RM sollen künftig Aufschluss über eine praktische Umsetzung des QM geben.[178] Zudem ist sicherzustellen, dass das HKIS vor Inverkehrbringen oder Inbetriebnahme einem Konformitätsbewertungsverfahren nach Art. 43 KI-VO unterzogen wird, das die Einhaltung der Art. 8-15 KI-VO bestätigt. Während für die meisten in Anhang III genannten HKIS eine interne Kontrolle ausreicht (Art. 43 Abs. 2, Anhang VI KI-

[175] *Teichmann*, ZD 2025, 495, 498.
[176] *Teichmann*, ZD 2025, 495, 498; *Wendt/Wendt*, Das neue Recht der KI, § 6 Rn. 59, 60.
[177] Vgl. *Ebers/Streitbörger*, RDi 2024, 393, 397, Rn. 31.
[178] *Wendt/Wendt*, Das neue Recht der KI, § 7 Rn. 9.

VO), nimmt das Verfahren für biometrische HKIS grundsätzlich eine externe notifizierte Stelle vor (Art. 43 Abs. 1 KI-VO).[179] Bei Anhang I-HKIS sind die Vorgaben aus Abschnitt 2 von Kapitel III in das jeweils einschlägige Verfahren einzubeziehen (Art. 43 Abs. 3 S. 2 KI-VO). Nach Abschluss des Verfahrens ist eine EU-Konformitätserklärung auszufüllen und zehn Jahre aufzubewahren (Art. 47 KI-VO), eine CE-Kennzeichnung anzubringen (Art. 48 KI-VO) und die Registrierungspflichten nach Art. 49 Abs. 1 KI-VO für Anhang III-Systeme in der EU-Datenbank (Art. 71 KI-VO) zu befolgen. Nach Inverkehrbringen haben Anbieter ein System zur Beobachtung des HKIS einzurichten und zu dokumentieren (Art. 72 KI-VO) sowie Korrekturmaßnahmen zu ergreifen; bleiben letztere erfolglos, ist das System zu deaktivieren. Betreiber und Händler sind zu informieren, wenn sie eine Nichtkonformität des Systems mit der VO befürchten (Art. 20 KI-VO). Gravierende Vorfälle sind den nationalen Marktüberwachungsbehörden zu melden (Art. 73 Abs. 1 KI-VO). Ferner besteht eine Mitwirkungs- und Nachweispflicht gegenüber Behörden sowie das Erfordernis, dass die Systeme Barrierefreiheitsanforderungen erfüllen.

Die Betreiberpflichten sind in Art. 26 KI-VO geregelt. Nach Art. 26 Abs. 1, 3, 5 KI-VO haben Betreiber von HKIS adäquate technische und organisatorische Maßnahmen zu treffen, um eine Nutzung ausschließlich gem. Betriebsanleitung und in Einklang mit der KI-VO und sonstigem Unions- und nationalem Recht sicherzustellen. Hierzu zählen auch die kontinuierliche Überwachung des Systems anhand der Betriebsanleitung inklusive einer eventuell nach Art. 72 KI-VO relevanten Information des Anbieters, wenn das Systemverhalten von den Anleitungsvorgaben differiert[180] und eine Einstellung der Nutzung, sollte eine anleitungskonforme Systemverwendung befürchten lassen, dass das System ein Risiko nach Art. 79 Abs. 1 KI-VO birgt; dann sind Anbieter oder Händler und die Marktüberwachungsbehörde unverzüglich zu informieren. Bei schwerwiegenden Vorfällen (Art. 3 Nr. 49 KI-VO), ist zunächst der Anbieter zu informieren, anschließend der Händler und die Marktüberwachungsbehörde (Art. 26 Abs. 5 S. 3 KI-VO). Zudem haben Betreiber die menschliche Aufsicht geeigneten Personen mit entsprechend profunder KI-Kompetenz zu übertragen und diese angemessen zu unterstützen (Art. 26 Abs. 2 KI-VO). Ferner ist zu gewährleisten, dass die Eingabedaten der Zweckbestimmung des Systems entsprechen und repräsentativ genug sind (Art. 26 Abs. 4 KI-VO), um Ergebnisse zu vermeiden, für die das System nicht ausgelegt ist, weshalb für diese keine RM-Maßnahmen bestehen und dass vorhandene, automatisch erzeugte Protokolle mindestens sechs Monate aufbewahrt werden (Art. 26 Abs. 6 KI-VO).[181]

[179] *Gerdemann*, NJW 2024, 2209, 2214, Rn. 21.
[180] *Dubovitskaya*, AG 2024, 877, 883, Rn. 29.
[181] *Linardatos*, ZIP 2024, 2497, 2502.

Vor Inbetriebnahme oder Verwendung eines HKIS am Arbeitsplatz hat der Arbeitgeber als Betreiber die Arbeitnehmervertreter und betroffenen Arbeitnehmer zu informieren (Art. 26 Abs. 7 KI-VO). Betriebsverfassungsrechtlich relevant ist ein Beschluss des ArbG Hamburg, wonach der Einsatz bestimmter KI-Systeme (hier: ChatGPT) kein Mitbestimmungsrecht des Betriebsrats (§ 87 Abs. 1 Nr. 6 BetrVG) auslöst, sofern die Nutzung browserbasiert über private Accounts erfolgt, eine Betriebsvereinbarung zur Browsernutzung besteht und der Arbeitgeber keinen Zugriff auf die aufgezeichneten Daten hat.[182] Geringe Änderungen dieses Falls, etwa ein arbeitgeberseitiger Zugriff auf eingegebene Daten oder eine Programmierung des Systems auf Unternehmensrechnern, können aber ein Mitbestimmungsrecht begründen.[183] Auch wenn der Entscheidung keine Bindungswirkung zukommt, könnte sie Auswirkungen auf künftige Entscheidungen haben und soll Arbeitgeber dafür sensibilisieren, dass die Nutzung von (Hochrisiko-)KI-Systemen eine vorherige Mitbestimmung des Betriebsrats voraussetzen kann und häufig auch wird.

Zudem müssen Betreiber von Anhang III-HKIS Betroffene über die Verwendung des HKIS informieren, wenn es die Person betreffende Entscheidungen fällt oder bei solchen unterstützt (Art. 26 Abs. 11 KI-VO); unter den Voraussetzungen des Art. 86 KI-VO ist ihr die Entscheidung zu erläutern. Überdies haben Betreiber aller HKIS die Pflicht zur Kooperation mit den zuständigen Behörden (Art. 26 Abs. 12 KI-VO) sowie zur Durchführung einer Datenschutz-Folgenabschätzung (Art. 26 Abs. 9 KI-VO). Weitere Pflichten gelten für Betreiber von HKIS zur nachträglichen biometrischen Fernidentifizierung im Zusammenhang mit Straftaten (Art. 26 Abs. 10 KI-VO), ferner in Gestalt von Registrierungspflichten gem. Art. 49 KI-VO etwa für EU-Einrichtungen (Art. 26 Abs. 8 KI-VO) sowie in Form einer Grundrechte-Folgenabschätzung für Betreiber anwendungsbezogener HKIS außerhalb des Bereichs der kritischen Infrastruktur, die öffentliche Dienste erbringen (Art. 27 KI-VO). Letztere müssen etwa Betreiber von HKIS für die Risikobewertung und Preisbildung von Lebens- und Krankenversicherungen vornehmen (Anhang III Nr. 5 lit. c).[184] Betreiber sollten vertraglich regeln, dass Anbieter ihnen die technische Dokumentation aufgrund ihrer Konformitätsnachweisfunktion vollständig überlassen, um Kosten durch die Erstellung zu vermeiden und klären, welches Maß an Transparenz auf welche Weise zur intendierten Verwendung erreicht wird.[185]

Unter den Voraussetzungen des Art. 25 KI-VO kann der Betreiber in die Pflichten des Anbieters einrücken. Dies gilt dann nur für das einzelne HKIS.[186] Das ist der

[182] ArbG Hamburg, Beschluss v. 16. Januar 2024 – 24 BVGa 1/24 –, juris (Rn. 39, 42, 43).
[183] *Kössel*, DB 2024, 1069, 1073.
[184] *Ebers/Streitbörger*, RDi 2024, 393, 399, Rn. 43.
[185] *Dubovitskaya*, AG 2024, 877, 881, 882, Rn. 23, 24.
[186] *Borges*, CR 2024b, 565, 573, Rn. 88.

Fall, wenn er den Eindruck vermittelt, Anbieter zu sein (lit. a), eine wesentliche Veränderung des HKIS vornimmt (lit. b) oder die Zweckbestimmung so ändert, dass das System fortan als HKIS einzustufen ist (lit. c). Als Folge werden die Betreiber als Quasi-Anbieter den weiten Anbieterpflichten des Art. 16 KI-VO unterworfen, was zu Umsetzungsschwierigkeiten sowie zusätzlichen Kosten und Aufwand führen kann. Praxisrelevant ist vor allem die Zweckbestimmungsänderung nach lit. c: Nutzt ein Unternehmen etwa ChatGPT zur Bewertung von Bewerbungen nach Scores, ändert es die Zweckbestimmung eines (nicht hochriskanten) GPAI-Modells, sodass ein HKIS entsteht (Anhang III Nr. 4 lit. a KI-VO), wodurch die Pflichten des Art. 16 KI-VO einzuhalten sind.[187] So wäre ein vollständiges Konformitätsbewertungsverfahren durchzuführen und für die Einhaltung der Art. 8-15 KI-VO zu sorgen, wobei der Erstanbieter mit dem Quasi-Anbieter zur Erfüllung seiner Anbieterpflichten kooperieren muss, sofern er nicht eindeutig bestimmt hat, dass sein KI-System nicht in ein HKIS umgewandelt werden darf (Art. 25 Abs. 2 S. 2, 3 KI-VO). Bloßes Prompting kann dabei nicht als Zweckbestimmungsänderung qualifiziert werden.[188] Auch wenn Art. 25 KI-VO eher restriktiv ausgelegt werden sollte,[189] ist HKIS-Betreibern dringend eine ausschließliche Nutzung gem. der Gebrauchsanleitung und unter Beachtung der KI-VO und dem nationalen Recht anzuraten. Sie sollten ständig kontrollieren, dass das HKIS mitarbeiterseitig nicht entgegen der Zweckbestimmung verwendet wird und eigene Änderungen mit den Gründen, warum sie nicht „wesentlich“ sind, dokumentieren.[190]

Eine zentrale Pflicht für HKIS-Anbieter betrifft das RM (Art. 9 KI-VO), das aufgrund seiner besonderen Bedeutung tiefer beleuchtet wird. Seine Relevanz folgt aus Art. 8 Abs. 1 S. 2 KI-VO, wonach das RMS maßgeblich zur Einhaltung der Art. 8-15 KI-VO beiträgt und aus seiner Funktion als Instrument zur Verwirklichung des in Art. 1 Abs. 1 KI-VO geforderten Schutzniveaus für wesentliche Rechtsgüter.

2. Umsetzung des Risikomanagementsystems nach Art. 9 KI-VO

Anbieter von HKIS haben zwecks Bewältigung und Minimierung KI-bezogener Risiken ein RMS einzurichten, zu nutzen, zu dokumentieren und über den gesamten Systemlebenszyklus aufrechtzuerhalten (Art. 9 Abs. 1-3 KI-VO). Risiko bezeichnet dabei die Kombination aus Eintrittswahrscheinlichkeit und Schwere eines Schadens (Art. 3 Abs. 2 KI-VO). Ziel des RMS ist die Etablierung eines fortlaufenden, iterativen Prozesses zur systematischen Identifizierung, Bewertung und Reduzierung von Gesundheits-, Sicherheits- und Grundrechtsrisiken (vgl. ErwG 65 S. 1, 2,

[187] *Ebers/Streitbörger*, RDi 2024, 393, 399, Rn. 46.
[188] *Linardatos*, ZIP 2024, 2497, 2502.
[189] Vgl. *Dubovitskaya*, AG 2024, 877, 880, Rn. 16; *Linardatos*, ZIP 2024, 2497, 2502, 2506.
[190] *Borges*, CR 2024b, 565, 575, Rn. 105; *Wybitul*, BB 2024, 2179, 2181.

4).[191] Art. 9 KI-VO kommt eine Auffang- bzw. Klammerfunktion zu: Anders als die sonstigen HKIS-Anforderungen (Art. 10-15 KI-VO) enthält er keine gesonderten Teilanforderungen, um gewisse Risiken zu minimieren, sondern verpflichtet zur umfassenden Würdigung sowohl der dort gezielt erfassten Risiken, etwa Daten-Bias-Risiken und deren diskriminierende Wirkung (Art. 10 KI-VO), als auch sonstiger, dort nicht explizit adressierter Risiken für die genannten Rechtsgüter.[192]

Der erste Schritt zur Umsetzung des Art. 9 KI-VO ist die Schaffung organisatorischer, personeller und technischer Voraussetzungen, damit das RMS im Einklang mit Art. 9 Abs. 2-9 KI-VO betrieben werden kann.[193] Hierzu sind interne Richtlinien zur Festlegung von Zuständigkeiten, Verfahren und Verhaltensvorgaben für die Systemanwendung zu etablieren, fachlich geeignete Mitarbeiter einzusetzen und diesen technische Ressourcen wie Zugriffsrechte und Mittel zur Umsetzung von Risikotests bereitzustellen.[194] Die Kernfunktion des RMS sollte wegen ihrer Nähe zur Systementwicklung der F&E-Abteilung übertragen werden, die durch die Compliance-Abteilung – die auch das QM-System überwacht – hinsichtlich der Funktionsfähigkeit des Systems überwacht wird; angesichts der dem QM-System immanenten Compliance-Funktion zur Überwachung des RMS (Art. 17 Abs. 1 S. 1, 2 lit. g KI-VO) sollte aufgrund technischer Zusammenhänge von Art. 9 und 17 KI-VO eine enge Zusammenarbeit der beiden Abteilungen initiiert werden.[195]

Der zweite Umsetzungs- und erste Prozessschritt ist die Identifizierung und Beurteilung der vom KI-System ausgehenden Risiken (Art. 9 Abs. 2 S. 2 lit. a-c KI-VO, Ermittlungsphase). Die für RMS generell relevante ISO/IEC Guide 51:2014 definiert die Risikoidentifizierung als systematische Nutzung verfügbarer Informationen zur Identifikation potenzieller Schadensquellen (Nr. 3.10, 3.2). Dabei sind vor allem die intendierte Verwendung und der Nutzungskontext des HKIS zu beachten.[196] Mangels spezieller VO-Vorgaben sind allgemeine RM-Prinzipien heranzuziehen, die auf KI-bezogene Risiken ausgerichtet sind, etwa eine KI-spezifische Risikotaxonomie zur Risikokategorisierung, Incident Databases (risikobehaftete Vorfälle dokumentierende Datenbanken) und Szenarioanalysen; letztere sollen zur Abschätzung künftiger Entwicklungen im Rahmen von adäquaten Risikotests nach Art. 9 Abs. 6-8 KI-VO vollzogen werden.[197] Ferner eignen sich Unternehmens-, Umwelt-, System-, Prozess- und Dokumentenanalysen, Kreativitätstechniken

[191] *Gerdemann*, in: BeckOK KI-Recht Art. 9 Rn. 1.
[192] *Gerdemann*, in: BeckOK KI-Recht Art. 9 Rn. 5; *Schuett*, EJRR 2024, 367, 370.
[193] *Gerdemann*, in: BeckOK KI-Recht Art. 9 Rn. 16.
[194] *Gerdemann*, in: BeckOK KI-Recht Art. 9 Rn. 16.
[195] *Gerdemann*, in: BeckOK KI-Recht Art. 9 Rn. 10, 16.
[196] *Ossmann-Magiera/Dehmel*, KIR 2024, 134, 137.
[197] *Gerdemann*, in: BeckOK KI-Recht Art. 9 Rn. 35; *Schuett*, EJRR 2024, 367, 375.

sowie Früherkennungssysteme.[198] Für die gesamte Ermittlungsphase kann auch die IEC 31010:2019 herangezogen werden.[199] Es sind nur Gesundheits-, Sicherheits- und Grundrechtsrisiken zu identifizieren (Art. 9 Abs. 2 S. 2 lit. a KI-VO) und die ermittelten Risiken sollten in einem Risikoinventar aufgeführt werden (vgl. Kapitel D., Abschnitt I.). Ein HKIS zur Steuerung eines Chirurgieroboters erfordert etwa ein besonders auf Gesundheits- und Sicherheitsrisiken ausgerichtetes RMS.[200] Zu identifizieren sind zunächst bekannte und vernünftigerweise vorhersehbare Risiken bei bestimmungsgemäßem Gebrauch des HKIS (Art. 9 Abs. 2 S. 2 lit. a KI-VO). Als bekannt gelten eingetretene und mediale Beachtung gefundene Risiken sowie in etablierten Incident Databases ersichtliche Risiken, mithin ist das allgemeine Branchenwissen, aufbauend auf dem in Art. 8 Abs. 1 S. 1 KI-VO genannten allgemeinen Technikstand, entscheidend.[201] Ferner sind unbekannte, aber „vernünftigerweise" vorhersehbare Risken zu berücksichtigen, solche, die ein verständiger Durchschnittsanbieter erkennen würde, wenn er die im Verkehr erforderliche Sorgfalt anwendet, etwa weil sie sehr wahrscheinlich eintreten werden, wobei spezielle Kenntnisse maßstabsverschärfend wirken können.[202] Nur theoretisch mögliche oder grob unwahrscheinliche Risiken müssen nicht um jeden Preis identifiziert werden; es wird eine individuell verhältnismäßige Reichweite und Ressourceneinsatz bezüglich der Risikoidentifizierung gefordert, um exzessiven Aufwand zu vermeiden.[203] Anknüpfend ist umgekehrt je mehr Aufwand in die Vorhersehung eines Risikos zu investieren, desto gravierender die potenziellen Auswirkungen sind.[204] Nach systematischer und teleologischer Auslegung der Vorschrift unter Beachtung des lit. b sind auch solche Risiken zu berücksichtigen, die aufgrund einer vernünftigerweise vorhersehbaren Fehlanwendung auftreten können, da ohne vorherige Identifizierung keine Beurteilung möglich ist (vgl. lit. b).[205]

Als nächstes sind die identifizierten Risiken im Rahmen einer Abschätzung und Bewertung inhaltlich zu beurteilen. Nach Nr. 3.9 und 3.10 des ISO/IEC Guide 51:2014 ist die Risikoabschätzung die Einschätzung der Schadenseintrittswahrscheinlichkeit und der Schadensschwere. Dazu eignen sich Einflussdiagramme oder Bayes'sche Netze, die KI-bezogene Risiken u.a. unter Würdigung von wahrscheinlichen Prompts und Selbstlerneffekten berücksichtigen.[206] Die Risikobewertung dient der Evaluierung, ob die identifizierten und abgeschätzten Risiken isoliert

[198] *Braun Binder/Egli*, in: KI-VO 2026 Art. 9 Rn. 24.
[199] *Ossmann-Magiera/Dehmel*, KIR 2024, 134, 137.
[200] *Spindler/Gerdemann*, § 5, in: *Hilgendorf/Roth-Isigkeit*, Die neue Verordnung der EU, Rn. 11.
[201] *Gerdemann*, in: BeckOK KI-Recht Art. 9 Rn. 38; *Schuett*, EJRR 2024, 367, 376.
[202] *Braun Binder/Egli*, in: KI-VO 2026 Art. 9 Rn. 23; *Ossmann-Magiera/Dehmel*, KIR 2024, 134,136.
[203] *Gerdemann*, in: BeckOK KI-Recht Art. 9 Rn. 40; *König*, in: KI-VO 2025b, Art. 9 Rn. 18.
[204] *Schuett*, EJRR 2024, 367, 376.
[205] *Gerdemann*, in: BeckOK KI-Recht Art. 9 Rn. 41; *König*, in: KI-VO 2025b, Art. 9 Rn. 19.
[206] *Gerdemann*, in: BeckOK KI-Recht Art. 9 Rn. 43; *Schuett*, EJRR 2024, 367, 376.

betrachtet und gemeinsam vertretbar sind, d.h. eine gewisse Akzeptanzschwelle nicht überschreiten.[207] Art. 9 Abs. 2 S. 2 lit. b KI-VO verpflichtet zur Abschätzung und Bewertung von Risiken, die bei einer zweckbestimmten Systemverwendung, und durch eine vernünftigerweise vorhersehbare Fehlanwendung auftreten können. Unter letzterer versteht Art. 3 Nr. 13 KI-VO eine zweckfremde Systemverwendung, die sich aus vernünftigerweise absehbarem menschlichem Verhalten oder einer ebenso absehbaren Interaktion mit anderen Systemen ergeben kann. Erfasst sind neben unintendierten auch böswillige Fehlanwendungen – letztere lägen etwa vor, wenn absehbar ist, dass Betreiber ein HKIS zu verbotenen Zwecken nutzen werden, indem sie Systemfähigkeiten vorsätzlich manipulativ zur gezielten Verhaltensänderung ausnutzen, um die menschliche Entscheidungsfähigkeit zu beeinträchtigen.[208] Mit verhältnismäßigem Mitteleinsatz sollten Anbieter demnach mögliche Betreiber und Fehlanwendungen ermitteln.[209] Zur Bestimmung, wann eine vernünftigerweise vorhersehbare Fehlanwendung vorliegt, ist erneut auf die Sicht des verständigen Durchschnittsanbieters abzustellen, sodass gänzlich abwegige Fehlanwendungen aus Rechtssicherheitsgründen nicht erfasst sind.[210]

Nach Inverkehrbringen des Systems ist anhand der Daten des Monitoring-Systems (Art. 72 KI-VO) über den gesamten Lebenszyklus kontinuierlich zu prüfen, ob bisher nicht identifizierte Risiken bekannt geworden und auf Basis der Datenlage nun vernünftigerweise neue Risiken vorhersehbar sind.[211] So können auch Risiken, die aus nicht bestimmungsgemäßen Verwendungen oder unvorhersehbarem Miss- bzw. Fehlgebrauch in der Praxis entspringen, berücksichtigt werden; eine über Art. 72 KI-VO hinausgehende Informationsbeschaffung ist nicht nötig.[212] Entgegen dem Wortlaut des Art. 9 Abs. 2 S. 2 lit. c KI-VO sind neben der Risikobewertung auch eine -identifizierung und -abschätzung der aus dem Monitoring-System gewonnen Daten als vorgelagerte Prozessschritte nötig, sodass lit. c eine weitere Erkenntnisquelle zur Risikoidentifizierung und -beurteilung darstellt.[213]

Mangels näherer Vorgaben der VO zur Ausgestaltung der Ermittlungsphase wird ergänzend ein praxisnaher Ansatz zur Durchführung des ersten Prozessschritts in Bezug auf Grundrechtsrisiken skizziert. Das Modell des „Human Rights Impact Assessment“ besteht aus zwei Phasen: Zuerst sind Einsatzkontext und Hauptmerkmale des HKIS zu ermitteln, die Art der gesammelten Daten, potenziell betroffene Personengruppen und Grundrechte und relevante Gerichte mit ihren wichtigsten

[207] Vgl. Nr. 3.12 des ISO/IEC Guide 51:2014; vgl. auch *Schuett*, EJRR 2024, 367, 380.
[208] *Gerdemann*, in: BeckOK KI-Recht Art. 9 Rn. 46; *Hinderks*, ZUM 2022, 110, 118.
[209] *Gerdemann*, in: BeckOK KI-Recht Art. 9 Rn. 46*; Schuett*, EJRR 2024, 367, 377.
[210] *Gerdemann*, in: BeckOK KI-Recht Art. 9 Rn. 46*; Schuett*, EJRR 2024, 367, 377.
[211] *Gerdemann*, in: BeckOK KI-Recht Art. 9 Rn. 33, 48; *Schuett*, EJRR 2024, 367, 377.
[212] *König*, in: KI-VO 2025b, Art. 9 Rn. 23; *Schuett*, EJRR 2024, 367, 377.
[213] *Gerdemann*, in: BeckOK KI-Recht Art. 9 Rn. 49.

Entscheidungen.[214] Danach werden Daten anhand der HKIS-Merkmale gesammelt, damit auf Basis der Ergebnisse der ersten Phase Grundrechtsrisiken ermittelt werden können, bevor sie abgeschätzt und basierend auf dem Maßstab der Rechtsprechung als niedrig, mittel, hoch oder sehr hoch bewertet werden.[215]

Zur Aufwandsbegrenzung muss das RMS nur Risiken adressieren, die durch Systementwicklung oder -konzeption oder Bereitstellung technischer Informationen angemessen gemindert oder behoben werden können (Art. 9 Abs. 3 KI-VO); unmöglich oder nur unverhältnismäßig schwierig beheb- oder reduzierbare Risiken müssen nicht einbezogen werden.[216] Ob eine Risikominderung nur unverhältnismäßig möglich ist, kann erst nach Risikoidentifizierung und -bewertung bei Bestimmung der RM-Maßnahmen entschieden werden und stellt die Ausnahme dar, da die Bereitstellung der Informationen nach Art. 13 KI-VO regelmäßig risikomindernd wirkt.[217] Im Lichte des von der VO verfolgten hohen Schutzniveaus für wesentliche Rechtsgüter ist anzunehmen, dass ein HKIS gem. Art. 5 UAbs. 1 KI-VO analog nur in Verkehr gebracht und in Betrieb genommen werden darf, wenn es zwar Risiken aufweist, die nur mit unverhältnismäßigem Aufwand reduzierbar sind, das Gesamtrestrisiko aber vertretbar ist.[218] Aus Transparenzgründen sollte dokumentiert werden, welche Risiken aus welchen Gründen keinen Eingang in das RMS gefunden haben und warum der Aufwand als „unverhältnismäßig" deklariert wurde.

Nach Risikoidentifizierung und -beurteilung sind in einem zweiten Prozessschritt (Maßnahmenphase) geeignete und gezielte RM-Maßnahmen zu treffen (Art. 9 Abs. 2 S. 2 lit. d KI-VO). Geeignet sind Maßnahmen, die Risiken gänzlich bewältigen oder auf ein vertretbares Maß minimieren, sodass nur ein vertretbares Restrisiko i.S.d. Abs. 5 UAbs. 1 persistiert; eine völlige Risikobewältigung ist nicht obligatorisch.[219] Während nicht vertretbare Risiken mittels der Maßnahmen in Abs. 5 UAbs. 2 bis zur Vertretbarkeitsschwelle zu mindern sind, bedürfen die bereits bei der Risikobewertung als vertretbar eingestuften Risiken keiner weiteren Reduzierung; bei letzteren ist die Entscheidung zu dokumentieren und der Prozess beendet.[220] Die beiden Schritte sind so lange durchzuführen, bis alle Risiken als vertretbar beurteilt werden können, d.h. erweisen sich ergriffene Maßnahmen als unzureichend, um die Restrisiken auf ein vertretbares Maß zu minimieren, sind weitere

[214] *Mantelero*, Beyond Data, S. 52, 53.
[215] *Mantelero*, Beyond Data, S. 54, 55.
[216] *Gerdemann*, in: BeckOK KI-Recht Art. 9 Rn. 22; *König*, in: KI-VO 2025b, Art. 9 Rn. 27.
[217] *Gerdemann*, in: BeckOK KI-Recht Art. 9 Rn. 23.
[218] *Gerdemann*, in: BeckOK KI-Recht Art. 9 Rn. 24; vgl *Schuett*, EJRR 2024, 367, 377.
[219] *Gerdemann*, in: BeckOK KI-Recht Art. 9 Rn. 55; *Kaeber/Roth-Isigkeit*, LTZ 2025, 3, 4; *Ossmann-Magiera/Dehmel*, KIR 2024, 134, 137.
[220] *Braun Binder/Egli*, in: KI-VO 2026 Art. 9 Rn. 21; *Gerdemann*, in: BeckOK KI-Recht Art. 9 Rn. 44, 61; *Ossmann-Magiera/Dehmel*, KIR 2024, 134, 137; *Schuett*, EJRR 2024, 367, 377.

Maßnahmen zu treffen.[221] Besonders zu mindern sind Risiken für Minderjährige und andere schutzbedürftige Gruppen (Abs. 9), u.a. hinsichtlich einer leichteren Beeinflussbarkeit und Gesundheitsgefährdung wegen potenziell gesteigerter Anfälligkeit.[222] Es sind „gezielte" Maßnahmen zu treffen, d.h. solche, die passgenau auf die einzelnen Risiken zugeschnitten sind, damit sie bewältigt oder gemindert werden können, was in Einzelfällen nur durch Reduktion der Wirkmächtigkeit und entsprechender Drosselung der Funktionsstärke des Systems zu erreichen ist.[223]

Bei der Gestaltung der RM-Maßnahmen muss jedes relevante Restrisiko und das Gesamtrestrisiko des HKIS als vertretbar beurteilt werden (Art. 9 Abs. 5 UAbs. 1 KI-VO). Das Gesamtrisiko ist jenes, das nach Umsetzung der Maßnahmen fortbesteht.[224] Somit ist neben der gezielten Beurteilung der Einzelrisiken separat zu prüfen, ob die isoliert betrachtet vertretbaren Einzelrisiken in ihrer Kumulation, etwa wegen Wechselwirkungen, eine noch vertretbare Gesamtrisikoexposition aufweisen.[225] Auch wenn die VO nicht regelt, wann ein Risiko als „vertretbar" gilt, ist bei Beurteilung der Vertretbarkeit der Schwere eines wahrscheinlich entstehenden Schadens, seiner Eintrittswahrscheinlichkeit und dem Rang des betroffenen Rechtsguts hohes Gewicht beizumessen.[226] Zusätzlich können die in Nr. 6.2.1 des ISO/IEC Guide 51:2014 dargelegten Faktoren einbezogen werden, namentlich aktuelle gesellschaftliche Wertvorstellungen, die Suche nach einer optimalen Balance zwischen absoluter Sicherheit und Erreichbarkeit, Leistungsanforderungen an ein System und die Eignung zur Zweckerreichung und Kosteneffektivität. So kann bei der Frage der Vertretbarkeit beachtet werden, ob die Nützlichkeit des Systems so hoch ist, dass es gerechtfertigt ist, gewisse Risiken einzugehen und ob die Kosten für einzelne Risikomaßnahmen verhältnismäßig sind.[227] Insofern ist darauf abzustellen, wie das Restrisiko in Relation zum Nutzen des HKIS steht, wobei ein hoher Nutzen erhöhte Restrisiken rechtfertigen kann.[228] Sinnvoll erscheinen Risiko-Nutzen- und Kosten-Nutzen-Analysen zur Abwägung, ob die Kosten zur Umsetzung einer RM-Maßnahme die tatsächliche Risikoreduzierung rechtfertigen und inwieweit die RM-Maßnahme den Gesamtnutzen des HKIS beeinträchtigt.[229] Abhängig vom Rang des bedrohten Rechtsguts kann die Vertretbarkeitsschwelle auch bei unwahrscheinlichen Schadenseintritten niedriger anzusetzen

[221] *Braun Binder/Egli*, in: KI-VO 2026 Art. 9 Rn. 21; *Ossmann-Magiera/Dehmel*, KIR 2024, 134, 138; *Schuett*, EJRR 2024, 367, 377.
[222] *Gerdemann*, in: BeckOK KI-Recht Art. 9 Rn. 26, 27.
[223] *Gerdemann*, in: BeckOK KI-Recht Art. 9 Rn. 56.
[224] *König*, in: KI-VO 2025b, Art. 9 Rn. 33.
[225] *Gerdemann*, in: BeckOK KI-Recht Art. 9 Rn. 66, 67; *Schuett*, EJRR 2024, 367, 380.
[226] *Gerdemann*, in: BeckOK KI-Recht Art. 9 Rn. 63.
[227] *Gerdemann*, in: BeckOK KI-Recht Art. 9 Rn. 64.
[228] *König*, in: KI-VO 2025b, Art. 9 Rn. 34, 48; *Schuett*, EJRR 2024, 367, 379.
[229] *Fraser/Bello y Villarino*, EJRR 2024, 431, 439.

sein – etwa bei schweren Gefahren für die Gesundheit oder das Leben.[230] Generell gilt: Je höher die Schadenseintrittswahrscheinlichkeit und je gravierender Art und Umfang des potenziellen Schadens sind, desto eher gilt ein Risiko als nicht vertretbar.[231] Die Auslegungsbedürftigkeit des unbestimmten Rechtsbegriffs „vertretbar" birgt bis zur Konkretisierung der Vertretbarkeitsschwelle durch die Rechtsprechung die Gefahr, dass Anbieter Rest- und Gesamtrestrisiken nur selten als „unvertretbar" beurteilen werden, um sich intensivere RM-Maßnahmen zu sparen.

Bei Ergreifung der RM-Maßnahmen müssen Anbieter beachten, dass diese mit den von Art. 10-15 KI-VO geforderten Risikominderungsmaßnahmen harmonieren (Art. 9 Abs. 4 KI-VO) und dort nicht (hinreichend) erfasste Risiken über gezielte RM-Maßnahmen mindern, sodass übrige Lücken über die Maßnahmen nach Art. 9 KI-VO geschlossen werden; all solche Maßnahmen der Art. 9-15 KI-VO sollen kohärent sein.[232] Insofern soll im Rahmen einer Auswirkungsanalyse unter Beachtung der aus einer kombinierten Anwendung der Art. 8-15 KI-VO resultierenden Aus- und Wechselwirkungen die Effektivität des RM erhöht werden.[233] Bereits über Art. 10-15 KI-VO angemessen adressierte Risiken erfordern regelmäßig keine weiteren RM-Maßnahmen i.S.d. Art. 9 Abs. 5 UAbs. 2 KI-VO.[234] Ferner sind die Betreiberkenntnisse und Kenntnisse anderer in Verbindung zu dem System stehenden Personen sowie der voraussichtliche Betriebskontext des Systems zu beachten (Art. 9 Abs. 5 UAbs. 3 KI-VO). Somit ist die Betreibersicht maßgeblich, da sich die meisten Risiken erst im Betrieb zeigen und der Betreiber auf die Risikominderung einwirken kann.[235] Es ist die potenzielle Interaktion des KI-Systems mit seinem technischen Umfeld einzubeziehen und abzusehen, wie etwa mögliche Defekte an produktbezogenen HKIS die Systemfunktionsfähigkeit beeinträchtigen können.[236] So muss ein Anbieter von Sportbooten (Anhang I, Abschnitt A Nr. 3 KI-VO) mit KI-gestützter Geschwindigkeitsregulierung Maßnahmen für den Ausfall des Geschwindigkeitsmessers ergreifen, die verhindern, dass das Boot so lange beschleunigt, bis der Hinweis einer gewissen Geschwindigkeit erfolgen würde.[237]

Abs. 5 UAbs. 2 normiert drei an die Drei-Stufen-Methode des ISO/IEC Guide 51:2014 (vgl. Nr. 6.3.4, 6.3.5) angelehnte Maßnahmentypen, die im Stufenverhältnis stehen und dem Prinzip „Konstruktion vor Instruktion" folgen.[238] Die Einhaltung

[230] *Gerdemann*, in: BeckOK KI-Recht Art. 9 Rn. 63.
[231] *Gerdemann*, in: BeckOK KI-Recht Art. 9 Rn. 63.
[232] *Gerdemann*, in: BeckOK KI-Recht Art. 9 Rn. 57.
[233] *König*, in: KI-VO 2025b, Art. 9 Rn. 28, 29.
[234] *Gerdemann*, in: BeckOK KI-Recht Art. 9 Rn. 57.
[235] *König*, in: KI-VO 2025b, Art. 9 Rn. 39.
[236] *Gerdemann*, in: BeckOK KI-Recht Art. 9 Rn. 72.
[237] *Gerdemann*, in: BeckOK KI-Recht Art. 9 Rn. 72.
[238] *Gerdemann*, in: BeckOK KI-Recht Art. 9 Rn. 75; *Schuett*, EJRR 2024, 367, 380.

dieser Reihenfolge ist anzuraten, da sonst ergebnisunabhängig eine Verletzung der RM-Pflichten droht.[239] Dabei sind die „am besten geeigneten Maßnahmen“ zu treffen (Abs. 5 UAbs. 2) und nachvollziehbar zu dokumentieren; dazu kann sachverständiger Rat herangezogen werden.[240] Primär sind nach lit. a, soweit technisch möglich, Maßnahmen auf Konzeptions- und Entwicklungsebene zu ergreifen, sodass Anbieter potenzielle Risiken frühestmöglich bedenken sollten und insofern im Rahmen der funktionalen Systemausrichtung bis zur Vertretbarkeitsschwelle mindern können,[241] da systemintegrierte Maßnahmen Risiken effektiver minimieren als nachträgliche, weil sie der Risikoentstehung entgegenwirken (vgl. Nr. 6.3.5 des ISO/IEC Guide 51:2014). Werden Risiken in der Konzeptions- oder Entwicklungsphase übersehen und erst später identifiziert, ist eine erneute Auslegung der jeweiligen Phase nötig, um in dieser reduzierbare Risiken zu behandeln, weshalb eine phasenübergreifende Beteiligung des RMS und der Verantwortlichen sowie eine Dokumentation bei der KI-Entwicklung ratsam ist.[242] Der Maßnahmenergreifung auf Konstruktions- oder Entwicklungsebene ist jedoch nur Vorrang einzuräumen, soweit es technisch sinnvoll und vom Aufwand her verhältnismäßig ist, sodass nur bei einer nicht realisierbaren Risikominderung auf ein vertretbares Maß auf anderen Ebenen eine Rückkehr zur Konzeptions- oder Entwicklungsphase nötig ist.[243] Eine konstruktionsbezogene Maßnahme kann etwa in der Systemanpassung eines in ein HKIS integrierten LLM (z.B. ein Übersetzungssystem) bestehen, um toxische oder diskriminierende Ausgaben zu verhindern.[244]

Ist eine Risikobewältigung oder -minderung auf der ersten Ebene nicht (ausreichend) möglich, sind Minderungs- und Kontrollmaßnahmen zu ergreifen (lit. b). So sollen verbleibende Risiken gemindert bzw. die Funktionsweise der Systeme in Bezug auf Fehlfunktionen kontrolliert werden, um Risiken nachträglich zu minimieren, wobei auch Maßnahmen zum besseren Schutz gefährdeter Rechtsgüter bei Risikoeintritt möglich und die Maßnahmen regelmäßig auf ihre Effektivität zu prüfen und ggf. Alternativmaßnahmen zu treffen sind.[245] Anknüpfend an voriges Beispiel wären auf dieser Ebene – wenn die Anpassungen zur Vermeidung toxischer Sprache nicht genügten – Sicherheitsfilter oder sonstige Ansätze zur Inhaltserkennung, wie automatische Detektionsprogramme oder menschliche Aufsichtsmaßnahmen, denkbar, um risikorelevante Outputs erkennen und sperren zu können.[246]

[239] *Gerdemann*, in: BeckOK KI-Recht Art. 9 Rn. 75.
[240] *Ossmann-Magiera/Dehmel*, KIR 2024, 134, 138.
[241] *Gerdemann*, in: BeckOK KI-Recht Art. 9 Rn. 74, 76.
[242] *Gerdemann*, in: BeckOK KI-Recht Art. 9 Rn. 76.
[243] *Gerdemann*, in: BeckOK KI-Recht Art. 9 Rn. 77.
[244] *Schuett*, EJRR 2024, 367, 380.
[245] *Gerdemann*, in: BeckOK KI-Recht Art. 9 Rn. 74, 80, 81; *König*, in: KI-VO 2025b, Art. 9 Rn. 37.
[246] *Gerdemann*, in: BeckOK KI-Recht Art. 9 Rn. 79; *Schuett*, EJRR 2024, 367, 380.

Führen Maßnahmen der ersten beiden Ebenen nicht zu einer Behebung oder Reduzierung der relevanten Risiken bis zur Vertretbarkeitsschwelle, sind auf der letzten Ebene risikospezifische Betreiberinformationen i.S.d. Art. 13 KI-VO vorzuhalten, wobei die Betriebsanleitung u.a. Informationen zu Restrisiken und ergriffenen Minderungs- und Kontrollmaßnahmen enthält; ergänzend sind Schulungen für die Betreiber zu veranlassen (lit. c).[247] So sollen Betreiber Kenntnis über die bestehenden Restrisiken erlangen und ggf. eigene Konzepte erstellen, wie ein angemessener Umgang mit diesen und deren Minimierung auf ein vertretbares Maß erreicht werden kann.[248] Angesichts der komplexen Funktionszusammenhänge von KI-Systemen ist es diffizil, verständliche Hinweise zum risikominimierenden Umgang in der Betriebsanleitung darzulegen; gleiches gilt für anlassbezogene Risikomitteilungen (Art. 72 KI-VO), denen keine Maßnahmen der ersten beiden Ebenen vorausgehen.[249] Zur effektiven Minimierung eventuell entstehender Risiken sollte für dynamische HKIS daher ein fixer Kommunikationsweg mit dem Betreiber festgelegt werden.[250] Schulungen sind nur insoweit nötig, als sie Betreiber zu einem risikominimierenden Systemumgang befähigen und erfordern anbieterseitig keine eigenständige Durchführung, sondern nur einen Hinweis bezüglich der Notwendigkeit sowie eine ressourcentechnische Unterstützung.[251] Bei dem Beispiel der Übersetzungssoftware wären bei trotz den vorrangig ergriffenen Maßnahmen verbleibenden unvertretbaren Restrisiken Informationen zu den toxischen Sprachergebnissen, den ergriffenen Maßnahmen in Form von Sicherheitsfiltern, Detektionsprogrammen und menschlichen Aufsichtsmaßnahmen und Hinweise zum risikominimierenden Umgang bis zur Vertretbarkeitsschwelle bereitzustellen.

Eine zentrale Anforderung an RMS ist es, das System zu testen, um die am besten geeigneten Maßnahmen zu ermitteln. Die Tests können selbst durchgeführt werden, angesichts des Vorhandenseins extensiver und qualitätsgeprüfter Testdatensätze und einer profunderen Expertise kann ein Outsourcing der Testverfahren an professionelle Anbieter jedoch sinnvoll sein; dabei muss der Anbieter des KI-Systems stets kontrollieren, dass die Testungen ordnungsgemäß vollzogen werden.[252] Unbeschadet den Vorgaben der KI-VO kann dem Systemanbieter nämlich im Falle von mangelnden oder unterbliebenen Tests eine zivilrechtliche Haftung drohen.[253]

Das Verhalten von KI-Systemen kann aufgrund ihres Komplexitätsgrades und ihrer Wandlungsfähigkeit unvorhersehbar sein, weshalb eine ex ante Prognose zur

[247] *Braun Binder/Egli*, in: KI-VO 2026 Art. 9 Rn. 39; *Gerdemann*, in: BeckOK KI-Recht Art. 9 Rn. 82.
[248] *Gerdemann*, in: BeckOK KI-Recht Art. 9 Rn. 62, 74, 83.
[249] *Gerdemann*, in: BeckOK KI-Recht Art. 9 Rn. 84, 85.
[250] *Gerdemann*, in: BeckOK KI-Recht Art. 9 Rn. 85.
[251] *Gerdemann*, in: BeckOK KI-Recht Art. 9 Rn. 86.
[252] *Gerdemann*, in: BeckOK KI-Recht Art. 9 Rn. 90; *Schuett*, EJRR 2024, 367, 382.
[253] *Braun Binder/Egli*, in: KI-VO 2026 Art. 9 Rn. 43.

Funktionsweise kompliziert ist; daher kommt verbindlichen Testungen hohe Relevanz zu.[254] Vor allem bei großen Datensätzen verarbeitenden Systemen, denen selbstlernende Elemente inhärent sind, sind selbst für Entwickler nicht immer alle internen Prozesse voll nachvollziehbar (Black-Box-Effekte).[255] Deshalb sind Testungen – d.h. eine Reihe von Aktivitäten zwecks Identifizierung und Bewertung der Systemeigenschaften (vgl. Nr. 3.131 des ISO/IEC/IEEE 29119-1:2022) – durchzuführen. So soll geprüft werden, ob das System tendenziell dem programmierten Verhalten folgt.[256] Auch wenn sie primär der Ermittlung der am besten geeigneten Maßnahmen dienen, indem potenzielle Maßnahmen hinsichtlich ihrer Effektivität etwa mittels eines sequenziellen Trial-and-Error-Verfahrens geprüft und evidenzbasiert gerankt werden, können durch Testungen auch bisher unbeachtete Risiken identifiziert und dann beurteilt werden, sodass sie für beide Prozessschritte bedeutsam sind.[257] Bei dem Beispiel des KI-Systems, das toxische Sprachoutputs erzielt, kommen viele Maßnahmen zur Risikoreduzierung in Frage, durch die Testverfahren soll aber das Risiko besser verstanden und so die effektivste Maßnahme ermittelt werden.[258] Ferner soll durch Testungen sichergestellt werden, dass HKIS permanent im Einklang mit ihrer Zweckbestimmung funktionieren (Art. 9 Abs. 6 KI-VO), wodurch dem Umstand Rechnung getragen wird, dass das Systemverhalten in der realen Anwendungsumgebung häufig von seinem initialen Verhalten in der Trainingsumgebung abweicht; dieses Phänomen nennt man „Distributional Shift" oder allgemeiner „Dataset Shift".[259] Zur Eindämmung dieser Problematik, die typisch für KI-Systeme ist, die Techniken des maschinellen Lernens nutzen, soll in Tests examiniert werden, unter welchen erwartungsgemäßen Realbedingungen es in seiner beabsichtigten Anwendungsumgebung wahrscheinlich eine schlechte Leistung erzielt („Out-of-Distribution-Detection"), um bestmögliche Maßnahmen treffen zu können.[260] Zuletzt dienen Testungen der Prüfung, ob das HKIS alle Vorgaben der Art. 8-15 KI-VO erfüllt und die dort speziell adressierten Risiken bewältigt bzw. gemindert wurden, wobei vor allem die Vorschriften der Daten-Governance (Art. 10 KI-VO) und der einhergehenden Diskriminierungsprävention sowie zur Genauigkeit, Robustheit und Cybersicherheit (Art. 15 KI-VO) zu akzentuieren sind, deren Einhaltung oft erst im Zuge von KI-Tests konstatiert werden kann.[261]

[254] *Gerdemann*, in: BeckOK KI-Recht Art. 9 Rn. 88, 91; *König*, in: KI-VO 2025b, Art. 9 Rn. 41.
[255] *Gerdemann*, in: BeckOK KI-Recht Art. 9 Rn. 88.
[256] *König*, in: KI-VO 2025b, Art. 9 Rn. 41.
[257] *Braun Binder/Egli*, in: KI-VO 2026 Art. 9 Rn. 42; *Gerdemann*, in: BeckOK KI-Recht Art. 9 Rn. 92.
[258] Vgl. *Schuett*, EJRR 2024, 367, 381.
[259] *Schuett*, EJRR 2024, 367, 381.
[260] *Gerdemann*, in: BeckOK KI-Recht Art. 9 Rn. 89; *Schuett*, EJRR 2024, 367, 381.
[261] *Gerdemann*, in: BeckOK KI-Recht Art. 9 Rn. 94.

Die Testverfahren sind mittels vorab festgelegter, für die Zweckbestimmung geeigneter, Metriken und Wahrscheinlichkeitsschwellenwerte durchzuführen (Art. 9 Abs. 8 S. 2 KI-VO). Referenzwerte nennt die VO nicht, diese sind somit angesichts der unterschiedlichen Funktionstypen und Einsatzbereiche von HKIS bis zur Veröffentlichung harmonisierter Normen unter Orientierung an den dem allgemeinen Technikstand entsprechenden Standards der jeweiligen Branche individuell zu bestimmen, da die Beurteilung der Geeignetheit kontextspezifisch erfolgen muss.[262] Metriken umfassen allgemeine und risikospezifische Bewertungskriterien sowie Leistungs- und Funktionsindikatoren, die dahingehend beurteilt werden, ob sie gewisse Benchmarks anhand von probabilistischen Skalenwerten erreichen.[263] Wahrscheinlichkeitsschwellenwerte dienen dabei als Beurteilungsmaßstab in Bezug auf eine probabilistische Skala, indem sie Grenzwerte vordefinieren.[264] Nach Art. 9 Abs. 7, 60 Abs. 1 KI-VO können Testverfahren unter den Voraussetzungen des Art. 60 Abs. 4 KI-VO Tests unter Realbedingungen einschließen, ohne dass sich Anbieter an einem KI-Reallabor gem. Art. 57 KI-VO beteiligen müssen, um die Entwicklung anwendungsbezogener HKIS zu beschleunigen (ErwG 141 S. 1). Eine Nutzung dieser Möglichkeit ist anzuraten, da solche Tests eine effektive Überprüfung auf Dataset Shifts und die Einhaltung der Art. 8-15 KI-VO ermöglichen.[265]

Die Testverfahren haben zwingend vor Inverkehrbringen oder Inbetriebnahme zu erfolgen (Abs. 8 S. 1). Erforderlich ist grundsätzlich nur ein einmaliges Testen, ein geeigneter Testzeitpunkt ist dabei im Anschluss an die Trainingsphase zu sehen, dann kann die Systemfunktionalität mit praxisnahen Eingaben getestet werden.[266] Nach Inverkehrbringen oder Inbetriebnahme sind weitere Tests nötig, wenn durch die Systembeobachtung (Art. 72 KI-VO) unvorhergesehene Risiken ermittelt werden; in dem Fall können bei der Selektion bzw. Adaption adäquater Maßnahmen weitere KI-Tests notwendig werden, um etwa geeignete Software Patches vorzunehmen.[267] Die Tests sollen garantieren, dass das HKIS weiterhin im Einklang mit den Vorgaben der KI-VO und gem. seiner Zweckbestimmung agiert.[268]

Ist das HKIS in Verkehr gebracht bzw. in Betrieb genommen worden, haben Anbieter aufgrund der Pflicht zur regelmäßigen systematischen Überprüfung und Aktualisierung des RMS (Art. 9 Abs. 2 S. 1 KI-VO) vor allem die Risikoidentifizierung und -beurteilung sowie die RM-Maßnahmen iterativ und anlassbezogen (z.B. bei Bekanntwerden neuer Risiken oder größeren Systemänderungen) vorzunehmen

[262] *Gerdemann*, in: BeckOK KI-Recht Art. 9 Rn. 98; *Schuett*, EJRR 2024, 367, 382.
[263] *Gerdemann*, in: BeckOK KI-Recht Art. 9 Rn. 98; *Schuett*, EJRR 2024, 367, 382.
[264] *Schuett*, EJRR 2024, 367, 382.
[265] *Gerdemann*, in: BeckOK KI-Recht Art. 9 Rn. 99; *König*, in: KI-VO 2025b, Art. 9 Rn. 45.
[266] *Gerdemann*, in: BeckOK KI-Recht Art. 9 Rn. 95, 96, 97.
[267] *Gerdemann*, in: BeckOK KI-Recht Art. 9 Rn. 96.
[268] *König*, in: KI-VO 2025b, Art. 9 Rn. 47.

und ggf. nachzusteuern.[269] Zudem ist die Effektivität des RM selbst regelmäßig zu überprüfen, dabei ist zu klären, ob die Vorgaben des Art. 9 KI-VO noch adäquat erfüllt werden, etwa die Fähigkeit zur Identifizierung, Bewertung und Bewältigung von Risiken; bei Bedarf sind Anpassungen vorzunehmen.[270] Die Pflicht zur ständigen Durchführung, Überwachung und Aktualisierung besteht über die gesamte Systemlebensdauer, mithin solange, wie von ihm Gesundheits-, Sicherheits- oder Grundrechtsrisiken ausgehen – insofern ist das RMS solange aufrechtzuerhalten, wie die Beobachtungspflicht (Art. 72 KI-VO) andauert, d.h. bis das KI-System aufgrund universeller Stilllegung von niemandem mehr verwendet wird oder wegen einer wesentlichen Änderung nicht mehr in seiner initialen Gestalt besteht.[271]

Ferner ist die in Art. 9 Abs. 1 KI-VO normierte Dokumentationspflicht zu erfüllen. Zwar konkretisiert die VO die zu dokumentierenden Elemente nicht, das Telos der Aufzeichnung ist jedoch in der Ermöglichung einer nachträglichen Überprüfung der Systemfunktionsweise durch interne Stellen und Aufsichtsbehörden (vgl. etwa Art. 9 Abs. 2 S. 1, Art. 77 KI-VO) zu deduzieren, weshalb eine nachhaltige analoge oder digitale Speicherung funktionserheblicher Informationen wie der Ablauf des RMS, bei seiner Anwendung aufgetretene risikorelevante Ereignisse und getroffene RM-Maßnahmen die Dokumentationspflicht erfüllen sollten.[272]

Die Komponenten des KI-RM können in bestehende dem Unionsrecht unterliegende sektorspezifische RMS integriert werden, um Doppelarbeit und Extrakosten zu vermeiden und Synergieeffekte durch ein einheitliches RMS mit produkt- und KI-bezogenen Risiken zu erzielen (Art. 9 Abs. 10 KI-VO).[273] Aufgrund unterschiedlicher unionsrechtlicher Anforderungen an die RMS ist bei einer Integration darauf zu achten, die Vorgaben aller betroffenen Rechtsakte zu erfüllen; eine undifferenzierte Konsolidierung von Prozessschritten ist zu vermeiden.[274] Die Zweckmäßigkeit einer Prozessintegration hängt von der Ausgestaltung des sektorspezifischen RMS und davon ab, inwiefern eine Kongruenz zwischen den für das KI-RMS relevanten Risiken mit den Gegenständen von sektorspezifischen RMS besteht.[275]

Die künftigen harmonisierten Normen werden für die praktische Umsetzung des RMS zentral sein, bis zu deren Veröffentlichung besteht Rechtsunsicherheit. Insofern ist Anbietern neben Rückgriffen auf die ISO/IEC Guide 51:2014 und die ISO/IEC 42001:2023 (unter Anpassung an die VO-Vorgaben) zu empfehlen, sich

[269] *Gerdemann*, in: BeckOK KI-Recht Art. 9 Rn. 19, 81; *Schuett*, EJRR 2024, 367, 377; *Teichmann*, ZD 2025, 495, 497.
[270] *Gerdemann*, in: BeckOK KI-Recht Art. 9 Rn. 19.
[271] *Gerdemann*, in: BeckOK KI-Recht Art. 9 Rn. 20, 21.
[272] *Gerdemann*, in: BeckOK KI-Recht Art. 9 Rn. 18; *Schuett*, EJRR 2024, 367, 374.
[273] *Spindler/Gerdemann*, § 5, in: *Hilgendorf/Roth-Isigkeit*, Die neue Verordnung der EU, Rn. 4.
[274] *Gerdemann*, in: BeckOK KI-Recht Art. 9 Rn. 28, 29.
[275] *Braun Binder/Egli*, in: KI-VO 2026 Art. 9 Rn. 49; *Gerdemann*, in: BeckOK KI-Recht Art. 9 Rn. 31.

an internationalen freiwilligen KI-Normungen wie der ISO/IEC 23894:2023 – die u.a. eine strukturierte Risikoidentifizierung unter Beachtung von Verzerrungen und Transparenz und eine Dokumentation der getroffenen RM-Maßnahmen fordert – sowie dem AI Risk Management Framework des NIST zu orientieren, da zu erwarten ist, dass die harmonisierten Normen Parallelen zu anerkannten internationalen Normungen aufweisen werden, vor allem in Bezug auf Prozessschritte und Benchmarks.[276] Auch wenn hierdurch keine Konformitätsvermutung begründet wird, kann bei gleichzeitiger Beachtung des Normungsprozesses der Anpassungsaufwand nach deren Veröffentlichung gesenkt werden.[277] Zudem sollten sich Anbieter bis zur Veröffentlichung hinsichtlich Konzeptions- und Entwicklungs- sowie Minderungs- und Kontrollmaßnahmen an brancheninternen, dem aktuellen Technikstand entsprechenden Lösungen ähnlicher HKIS orientieren, die zur Minimierung der spezifischen Risiken taugen.[278] Gleiches gilt für die im Rahmen von Testungen festzulegenden Metriken und Wahrscheinlichkeitsschwellenwerte.

III. Handlungsbedarf für Betreiber von KI-Systemen mit begrenztem Risiko: Die Deepfake-Kennzeichnungspflicht

Nachdem die Transparenzanforderungen an bestimmte KI-Systeme in Kapitel C., Abschnitt III. dargelegt wurden, soll nun die Umsetzung der Vorgaben des Art. 50 Abs. 4 UAbs. 1 KI-VO zur Offenlegung von Deepfakes beleuchtet werden. Die Norm leistet einen wesentlichen Beitrag zur Erreichung der in Art. 1 Abs. 1 KI-VO normierten Ziele: Durch Kennzeichnungspflichten wird einer vertrauenswürdigen KI und dem angestrebten hohen Schutz für Grundrechte, aber auch bezüglich der Demokratie und Rechtsstaatlichkeit Rechnung getragen, indem manipulative und intransparente Beeinflussungen und Desinformation vermieden werden sollen.

Nach Art. 50 Abs. 4 UAbs. 1 KI-VO müssen Betreiber von KI-Systemen, die Bild-, Ton- oder Videoinhalte erzeugen oder manipulieren, die Deepfakes sind, offenlegen, dass die Inhalte künstlich erzeugt oder manipuliert wurden, wenn die Verwendung nicht Strafverfolgungszwecken dient. Abs. 4 UAbs. 1 und Abs. 2 ergänzen sich, wie auch in dem im Dezember 2025 veröffentlichten ersten Praxisleitfadenentwurf zu den Transparenzpflichten des Art. 50 KI-VO deutlich wird:[279] Während Abs. 2 eine anbieterseitige (technische) Kennzeichnungspflicht für synthetisch erzeugte Inhalte vorsieht, normiert Abs. 4 UAbs. 1 eine betreiberseitige Offenlegungspflicht speziell für Deepfakes. Dabei fordert Abs. 2 eine maschinenlesbare

[276] *Gerdemann*, in: BeckOK KI-Recht Art. 9 Rn. 9, 102; *Schuett*, EJRR 2024, 367, 371; *Söbbing*, RDi 2025, 337, 344, 345 Rn. 62, 74.
[277] *Gerdemann*, in: BeckOK KI-Recht Art. 9 Rn. 102; *Schuett*, EJRR 2024, 367, 371.
[278] *Gerdemann*, in: BeckOK KI-Recht Art. 9 Rn. 78, 81.
[279] *Bontcheva et al.*, First Draft Code of Practice on Transparency, S. 21, 22.

Kennzeichnung, während Abs. 4 UAbs. 1 für Deepfakes eine menschenlesbare verlangt, sodass Deepfakes im Ergebnis im Zusammenspiel von Abs. 2 und Abs. 4 UAbs. 1 sowohl maschinen- als auch menschenlesbar sein müssen.

Betreiber eines KI-Systems i.S.d. Abs. 4 UAbs. 1 müssen zuerst festzustellen, ob ihr System Bild-, Ton- oder Videoinhalte erzeugt oder manipuliert. Während Bildinhalte Inhalte sind, die optisch wahrnehmbar sind, wie Fotografien oder grafische Darstellungen, basieren Toninhalte auf einer akustischen Wahrnehmung und umfassen etwa Podcasts, Musikstücke oder Radiobeiträge.[280] Bei Videoinhalten handelt es sich um bewegte Bilder, die vertont sein können, z.B. Clips, Kurz- oder Kinofilme.[281] Die genannten Medieninhalte werden erzeugt, wenn sie komplett künstlich erstellt, d.h. grundlegend neu kreiert werden; etwa, wenn ein Video ohne Vorlage generiert wird, das Politiker als Astronauten im Weltall darstellt.[282] Sie werden manipuliert, wenn durch das System bestehende, authentische Medieninhalte nachträglich wissentlich verfremdet werden, indem etwa zwei Gesichter auf einem echten Bild durch FaceSwap „getauscht" oder Videoinhalte modifiziert werden, was sich z.B. in einer gefälschten Videoaufnahme eines Prominenten widerspiegelt, der in dem modifizierten Video Aussagen tätigt, die so tatsächlich nie fielen.[283]

Als nächstes ist zu prüfen, ob die erzeugten oder manipulierten Medieninhalte Deepfakes sind. Deepfakes sind durch KI erzeugte oder manipulierte Bild-, Ton- oder Videoinhalte, die wirklichen Personen, Gegenständen, Orten, Einrichtungen oder Ereignissen ähneln und einer Person fälschlicherweise als echt oder wahrheitsgemäß erscheinen würden (Art. 3 Nr. 60 KI-VO). Somit ist ein Vergleich zwischen der vom System generierten und der echten Darstellung anzustellen, wobei eine relevante Abweichung konstatiert werden muss, um ein Deepfake zu sein.[284] „Echt oder wahrheitsgemäß" ist das, was tatsächlich existiert.[285] Allerdings sind nicht alle gefälschten Inhalten Deepfakes; existiert keine hinreichende Ähnlichkeit zur Wirklichkeit und ist es für den Betrachter evident, dass der Inhalt nicht echt ist, besteht keine Offenlegungspflicht, was vor allem bei erkennbar fiktionalen Inhalten wie Monstern oder einem Bild der explodierenden Erde der Fall ist.[286]

Der künstliche Inhalt muss keine konkrete, existierende Person abbilden oder dieser ähneln, etwa einem bestimmten Musiker – nach dem Regelungszweck, der im Schutz vor Desinformation und Manipulation liegt, ist bereits von einem Deepfake

[280] *Kumkar/Griesel*, KIR 2024, 117, 119.
[281] *Kumkar/Griesel*, KIR 2024, 117, 119.
[282] *Martini*, in: KI-VO 2026 Art. 50 Rn. 126; *Schwarz*, MMR 2025, 786, 788.
[283] *Martini*, in: KI-VO 2026 Art. 50 Rn. 126; *Schwarz*, MMR 2025, 786, 788.
[284] *Borges*, CR 2024c, 633, 637, Rn. 38.
[285] *Borges*, CR 2024c, 633, 638, Rn. 42.
[286] *Becker*, CR 2024, 353, 361, Rn. 70; *Borges*, CR 2024c, 633, 638, Rn. 45; *Lauber-Rönsberg*, in: BeckOK KI-Recht Art. 50 Rn. 62.

auszugehen, wenn abgebildete Personen, Orte, Gegenstände oder Ereignisse fiktiv sind, ihrer Art nach aber real existieren könnten.[287] Ein Deepfake liegt also auch vor, wenn ein KI-Avatar so gestaltet ist, dass der Betrachter ihn für eine echte Person halten könnte, was etwa bei täuschend echten, nicht existenten, Models in der Werbung der Fall ist; ferner bei echt wirkenden, erfundenen Naturkatastrophen oder Attentaten.[288] Kein Deepfake liegt vor, wenn KI-Bildbearbeitungstools nur zur Qualitätsverbesserung bestehender Fotos genutzt werden, da kein Irrtum über die Echtheit des Abbilds entsteht.[289] Auch sind z.B. Audioinhalte in Form von Podcasts, in denen sich nicht real existierende Personen unterhalten, Deepfakes.[290] Bei Prüfung, ob ein Deepfake vorliegt, gilt ein niedriger Maßstab: Entscheidend ist, ob ein durchschnittlich versierter, objektiver Rezipient bei flüchtiger Betrachtung von einem authentischen Inhalt ausgehen darf – auch wenn eine Person im Hintergrund ein drittes Bein hat, kann ein Deepfake vorliegen, wenn sich dies nicht evident aufdrängt.[291] Somit besteht die Offenlegungspflicht nur, wenn der Inhalt geeignet ist, den versierten, objektiven Betrachter über seine Authentizität zu täuschen.[292] Ist der Betreiber selbst nicht Ersteller oder Verwender des Inhalts – so bei ChatGPT, wobei der Betreiber Nutzern als Dienstleistung die Verwendung seines Systems ermöglicht und diese über Prompts selbst Inhalte erstellen – muss er abschätzen, ob der Inhalt als Deepfake zu qualifizieren ist und ihn ggf. kennzeichnen, wobei eine manuelle Betrachtung aller Inhalte kaum umsetzbar ist, weshalb ihm automatisierte Prüfungen in Form automatischer Filterungen zu raten sind.[293]

Die VO regelt nicht, wie die Offenlegung von Deepfakes genau erfolgt. Art. 50 Abs. 5 KI-VO normiert nur, dass diese in klarer und eindeutiger Weise unter Beachtung der Barrierefreiheitsvorgaben spätestens zu dem Zeitpunkt erfolgen muss, zu dem die Person den Inhalten erstmals ausgesetzt ist. ErwG 134 S. 1 ergänzt, dass sie mittels Kennzeichnung der Ausgaben erfolgt. Somit besteht je nach Art und Einsatz des Mediums ein Handlungsspielraum bezüglich Gestalt, Platzierung und Größe der Kennzeichnung, ohne dass eine Namensnennung des Betreibers nötig wäre, wobei bei der Ausgestaltung des Hinweises im Rahmen einer Einzelfallbetrachtung der konkrete Inhalt und der Adressatenkreis einzubeziehen sind; im Zweifel ist eine Ausrichtung am europäischen Verbraucherleitbild zu empfehlen.[294]

---

[287] *Borges*, CR 2024c, 633, 638, Rn. 47; *Lauber-Rönsberg*, in: BeckOK KI-Recht Art. 50 Rn. 62.
[288] *Becker*, CR 2024, 353, 361, Rn. 70; *Kumkar/Griesel*, KIR 2024, 117, 120; *Martini*, in: KI-VO 2026 Art. 50 Rn. 127.
[289] *Lauber-Rönsberg*, in: BeckOK KI-Recht Art. 50 Rn. 64.
[290] *Bischoff et al.*, Schritt 5.2.4, in: *Baum et al.*, Umsetzungsleitfaden zur KI-VO, S. 172.
[291] *Kumkar/Griesel*, KIR 2024, 117, 120; *Lauber-Rönsberg*, in: BeckOK KI-Recht Art. 50 Rn. 63; *Martini*, in: KI-VO 2026 Art. 50 Rn. 128.
[292] *Martini*, in: KI-VO 2026 Art. 50 Rn. 128.
[293] *Borges*, CR 2024c, 633, 639, 640, Rn. 59, 64, 65, 66.
[294] *Kumkar/Griesel*, KIR 2024, 117, 121, 122; *Lauber-Rönsberg*, in: BeckOK KI-Recht Art. 50 Rn. 69; *Martini*, in: KI-VO 2026 Art. 50 Rn. 157; *Merkle*, in: KI-VO 2025b, Art. 50 Rn. 144, 146.

Auch ist bei der Offenlegung danach zu differenzieren, ob der Inhalt vollständig künstlich erzeugt oder nur manipuliert wurde.[295] Aus dem Umkehrschluss zu Abs. 4 UAbs. 1 S. 3 folgt, dass alle Inhalte, die Deepfakes darstellen und nicht die Ausnahme erfüllen, eine unmittelbare optische oder akustische Nähe der Offenlegung zu ihm erfordern, sonst wäre die Privilegierung redundant.[296] So genügt eine ausschließliche „versteckte" Kennzeichnung in Begleitinformationen wie Video-, Bildunterschriften, Beschreibungstexten oder Show Notes (Podcasts) nicht.[297] Es ist eine mit dem Inhalt untrennbare Platzierung und Gestaltung nötig, die bei flüchtiger Inhaltsbetrachtung allgemein verständlich und leicht ersichtlich ist und auch bei Weiterverbreitung, etwa mittels Screenshots oder Reposts bei Social Media, erhalten bleibt.[298] Die Offenlegung zum Zeitpunkt der ersten Aussetzung erfordert bei Videoinhalten einen visuellen und bei Toninhalten einen akustischen Hinweis zu Beginn, da nicht alle Rezipienten den Inhalt vollständig konsumieren, aber dennoch eine Fehlvorstellung über die Authentizität entstehen kann.[299]

Eine mögliche Kennzeichnung für Bild- und Videoinhalte besteht in der Implementierung eines sichtbaren Wasserzeichens in das Deepfake, das klar und eindeutig den künstlichen Ursprung offenbart, alternativ oder zusätzlich kann ein textlicher Hinweis oder Banner im Inhalt erfolgen, der generell auf der Sprache der Nutzung des KI-Systems ist.[300] Während sich ein Hinweis durch den Begriff „Deepfake" für einen jüngeren oder technisch versierten Adressatenkreis anbietet, genügt diese Kennzeichnung nicht, wenn sich der Inhalt an ältere Menschen richtet, da sie häufig nichts aus dem Begriff schließen können.[301] Damit wäre für Ältere unklar, dass es sich nicht um einen authentischen Inhalt handelt, für sie eignet sich eher eine Kurzinformation (z.B. „Dieser Inhalt ist nicht echt. Er wurde per KI erzeugt/manipuliert."). Weitere Optionen sind das Einbetten von „cr"-Buttons („Content Credentials"), die bei Interaktion Informationen zur Herkunft des Inhalts offenlegen, die Anbringung eines „Made with AI"-Labels oder die Fortentwicklung bestehender Kennzeichen.[302] Der erste Entwurf des besagten Praxisleitfadens verfolgt einen ähnlichen Ansatz: Die Unterzeichner sollen ein (von der EU bereitgestelltes, einheitliches) KI-Symbol implementieren, das bei Interaktion offenlegt, was konkret KI-erzeugt oder -manipuliert wurde und haben das Symbol bei Deepfake-Bildern

[295] *Merkle*, in: KI-VO 2025b, Art. 50 Rn. 145.
[296] *Feltes*, JIPITEC 2025, 222, 232, Rn. 57; *Kumkar/Griesel*, KIR 2024, 117, 122.
[297] *Kumkar/Griesel*, KIR 2024, 117, 122; *Martini*, in: KI-VO 2026 Art. 50 Rn. 155.
[298] *Kraetzig*, CR 2024, 207, 211, Rn. 18; *Martini*, in: KI-VO 2026 Art. 50 Rn. 155, 156.
[299] *Kumkar/Griesel*, KIR 2024, 117, 122; *Lauber-Rönsberg*, in: BeckOK KI-Recht Art. 50 Rn. 74; *Merkle*, in: KI-VO 2025b, Art. 50 Rn. 152, 168.
[300] *Becker*, CR 2024, 353, 361, Rn. 73; *Martini*, in: KI-VO 2026 Art. 50 Rn. 156; *Merkle*, in: KI-VO 2025b, Art. 50 Rn. 148, 149.
[301] Vgl. *Merkle*, in: KI-VO 2025b, Art. 50 Rn. 149.
[302] *Kumkar/Griesel*, KIR 2024, 117, 121; *Merkle*, in: KI-VO 2025b, Art. 50 Rn. 150.

an einer festen, für Rezipienten klar sichtbaren Stelle anzubringen.[303] Bei Echtzeitvideos soll das KI-Symbol in nicht zu aufdringlicher und störender Weise grundsätzlich für die gesamte Videodauer (etwa Live-Übertragung) angezeigt werden und zu Beginn soll ein Hinweis auf das Vorliegen eines Deepfakes erfolgen, während bei aufgezeichneten Videos (etwa auf Plattformen) ein visueller textlicher Hinweis oder die Einblendung des KI-Symbols zu Videobeginn genügen soll; zusätzlich kann freiwillig oder alternativ das KI-Symbol wie bei Echtzeitvideos an einer festen, gut sichtbaren Stelle permanent während des Videos angezeigt und ggf. ergänzend am Ende des Videos ein Hinweis eingeblendet werden.[304] Für Deepfake-Toninhalte kommt vor allem eine klar und eindeutig auf den künstlichen Ursprung hinweisende Ansage in Betracht, die nach Art. 50 Abs. 5 KI-VO am Anfang des Inhalts ertönen muss.[305] Der Hinweis darf im Vergleich zum restlichen Inhalt nicht so leise sein, dass er nicht klar vernommen werden kann. Der erste Leitfadenentwurf differenziert zwischen Toninhalten unter 30 Sekunden (z.B. Werbespots) und längeren (z.B. Podcasts). Erstere werden durch einen kurzen akustischen Hinweis in einfacher Sprache zu Inhaltsbeginn gekennzeichnet, letztere erfordern zusätzliche Hinweise in regelmäßigen Intervallen und am Ende.[306] So werden auch später Einschaltende über die Deepfakeeigenschaft informiert.

Betreiber sollten prüfen, ob der Inhalt Teil eines offensichtlich künstlerischen, kreativen, satirischen, fiktionalen oder analogen Werks oder Programms ist, da für diese Inhalte geringere Transparenzpflichten gelten, weil die Kennzeichnung Darstellung oder Genuss des Werks nicht beeinträchtigen darf (Abs. 4 UAbs. 1 S. 3). Wann Offensichtlichkeit vorliegt, ist einzelfallabhängig zu bestimmen, die Rechtsprechung könnte dies konkretisieren.[307] Der erste Leitfadenentwurf führt erneut eine Kennzeichnung per KI-Symbol auf, das bei Videos nur zu Beginn nicht störend in einer Ecke platziert werden soll, bei Bildern soll es an angemessener Stelle abgebildet und kann auch in den Hintergrund integriert werden, sofern es ersichtlich bleibt und bei Toninhalten soll ein unaufdringlicher akustischer Hinweis zu Beginn ertönen, der auch in EU-einheitlichen Signalen erfolgen kann.[308]

Auch wenn der erste Leitfadenentwurf unverbindlich ist und seine Befolgung keinen Nachweis der Einhaltung des Art. 50 KI-VO darstellt,[309] ist Betreibern eine Orientierung an seinen Maßnahmen und Verfolgung des weiteren Entwicklungsprozesses zu empfehlen. So sollte ein eigenes KI-Symbol entwickelt werden, das

[303] *Bontcheva et al.*, First Draft Code of Practice on Transparency, S. 24, 28.
[304] *Bontcheva et al.*, First Draft Code of Practice on Transparency, S. 27, 28.
[305] *Merkle*, in: KI-VO 2025b, Art. 50 Rn. 152.
[306] *Bontcheva et al.*, First Draft Code of Practice on Transparency, S. 28.
[307] *Bischoff et al.*, Schritt 5.2.4, in: *Baum et al.*, Umsetzungsleitfaden zur KI-VO, S. 175.
[308] *Bontcheva et al.*, First Draft Code of Practice on Transparency, S. 29.
[309] *Bontcheva et al.*, First Draft Code of Practice on Transparency, S. 21.

für alle visuellen Deepfake-Inhalte verwendet wird und barrierefrei auszugestalten ist, etwa durch genügend Kontrast und eine Mindestgröße, wobei sich eine Orientierung an der ETSI EN 301 549 empfiehlt; zur Abgrenzung kann auch eins für KI-erzeugte und eins für KI-manipulierte Inhalte erstellt werden.[310] Die Kennzeichnungspraktiken sollten transparent dokumentiert und mit Beispielen erläutert werden, Mitarbeiter sollten geschult werden, wann, wie und wo eine Kennzeichnung, auch in Abgrenzung zu den privilegierten Zwecken, erfolgt.[311]

IV. Zwischenergebnis

Der risikospezifische Handlungsbedarf variiert je nach Risikokategorie. Während KI-Systeme mit minimalem Risiko keinen Pflichten unterliegen, sind verbotene KI-Systeme unverzüglich aus dem Verkehr zu ziehen oder so zu modifizieren, dass der Verbotstatbestand entfällt. Für KI-Systeme mit begrenztem Risiko gelten Transparenzpflichten, wobei sich bei Deepfakes für Betreiber die Etablierung eines KI-Symbols und eine Orientierung am ersten Leitfadenentwurf anbietet. Die extensivsten Pflichten treffen Anbieter und Betreiber von HKIS. Für die Umsetzung des RMS sind KI-spezifische Vorgaben zu beachten, die auch für Unternehmen mit bereits bestehenden RMS neu sind. Bis zur Veröffentlichung harmonisierter Normen empfiehlt sich eine Orientierung an etablierten Standards. Nach deren Veröffentlichung ist ihre Einhaltung aufgrund der Konformitätsvermutung zu raten.

Teil 3: Fazit

Die Ausführungen zeigen auf, dass der Handlungsbedarf je nach Risikokategorie unterschiedlich hoch ist. Selbst Unternehmen, die keine bewussten Anbieter oder Betreiber von KI-Systemen sind, können über die unbekannte mitarbeiterseitige Nutzung von „Schatten-KI“ zur Einhaltung der Betreiberpflichten der KI-VO verpflichtet werden. Insofern gilt es, klare Regeln im Umgang mit KI festzulegen und im besten Fall unternehmenseigene KI-Systeme bereitzustellen.

Unternehmen sollten in einem ersten Schritt prüfen, ob und in welcher Rolle sie von dem Anwendungsbereich der KI-VO erfasst sind sowie im Rahmen einer systematischen Bestandsaufnahme ermitteln, welche ihrer Systeme als KI-Systeme zu deklarieren sind und diese samt Rolle, Nutzer und Einsatzbereich in ein KI-Verzeichnis aufnehmen. In einem zweiten Schritt ist zu examinieren, welcher Klassifizierung die von ihnen genutzten bzw. in Verkehr gebrachten KI-Systeme unterliegen, die Risikokategorie sollte im KI-Verzeichnis ergänzt werden. Auch wenn die Klassifizierung dem Anbieter obliegt, sollten Betreiber diese kritisch betrachten und

[310] *Bontcheva et al.*, First Draft Code of Practice on Transparency, S. 26.
[311] *Bontcheva et al.*, First Draft Code of Practice on Transparency, S. 25.

zusätzlich eine eigene Einschätzung vornehmen und dokumentieren, um potenzielle Nachteile zu vermeiden.[312] Als nächstes sind effektive KI-Governance-Strukturen aufzubauen. Empfehlenswert ist dazu die Implementierung einer unternehmenseigenen, verbindlichen KI-Richtlinie mit klaren Verantwortlichkeiten, Kontrollinstanzen und Regeln zum Umgang mit KI-Systemen sowie die Benennung eines KI-Beauftragten, der als Ansprechpartner für KI-bezogene Fragen fungiert, die Einhaltung der KI-Richtlinie kontrolliert und die KI-Strategieentwicklung aktiv gestaltet. Zudem ist eine angemessene KI-Kompetenz der Mitarbeiter sicherzustellen, wozu sich je nach Einsatzbereich und Einstufung des KI-Systems neben interaktiven Workshops verschieden profunde synchrone und asynchrone modulare Schulungen anbieten, die auf einer Grundlagenschulung zur Ermöglichung eines einheitlichen KI-Basiswissens aufbauen. In einem letzten Schritt sind die sich speziell aus der Risikoklassifizierung ergebenden Pflichten umzusetzen: KI-Systeme mit minimalem Risiko unterliegen keinem zwingenden Handlungsbedarf, verbotene KI-Systeme sind umgehend aus dem Verkehr zu entfernen oder so anzupassen, dass der Verbotstatbestand entfällt. Betreiber von KI-Systemen mit begrenztem Risiko, etwa solchen, die Deepfake-Bilder erzeugen können, haben die Inhalte im Hinblick auf die Deepfakeeigenschaft zu prüfen und ggf. entsprechend zu kennzeichnen, z.B. mittels klar sichtbarem KI-Symbol an fester Stelle. Den extensivsten Pflichten unterliegen Anbieter und Betreiber von HKIS; insbesondere die Pflicht zur Umsetzung eines RMS ist aus Anbietersicht zentral, das zur Verwirklichung der Ziele der KI-VO in Form eines hohen Schutzes wesentlicher Rechtsgüter und zur Einhaltung der Vorgaben der Art. 8-15 KI-VO eminent ist. Zu sektorspezifischen RMS verpflichtete Unternehmen sollten prüfen, ob Komponenten des KI-RMS in dieses integriert werden können. Angesichts jederzeit möglicher Änderungen der Klassifizierungsvoraussetzungen ist eine freiwillige, präventive Erfüllung von Vorgaben höherer Kategorien zu erwägen, sofern dies wirtschaftlich vertretbar ist.

Zusammenfassend besteht aufgrund ausstehender Leitlinien, Praxisleitfäden, harmonisierter Normen und richtungsweisender Rechtsprechung weiter Rechtsunsicherheit für Unternehmen. Daher sollten sie die Entwicklungen verfolgen und sich an veröffentlichten Leitlinien und Praxisleitfäden orientieren. Sobald harmonisierte Normen veröffentlicht werden, sollte diesen wegen ihrer Konformitätsvermutung gefolgt werden, da sie eine kostengünstige Möglichkeit zur Einhaltung der Vorschriften bieten. Im Endeffekt besteht ein Erfordernis zur stetigen Beobachtung, ob neue harmonisierte Normen, delegierte Rechtsakte, Leitlinien oder Praxisleitfaden veröffentlicht wurden, die betriebliche Handlungsnotwendigkeiten auslösen.

[312] *Chibanguza/Steege*, NJW 2024, 1769, 1772, Rn. 31.

Literaturverzeichnis

Albrecht, Rolf, KI-Kompetenz im Unternehmen im Jahr 2025 – Umsetzung des Art. 4 KI-VO in der betrieblichen Praxis, GWR 2025, S. 303 – 305.

Baum, Sandra/Beer, Frank/Behrendt, Eric/Bischoff, Susan/Böken, Arnd/Breuer, Jan/Dalerci, Camilla/Danos, Vasilios et al., Umsetzungsleitfaden zur KI-Verordnung: Compliance in der Praxis – Schritt für Schritt, Version 2.0, Stand: 13.01.2026, Berlin 2026, abrufbar unter: https://www.bitkom.org/sites/main/files/2024-10/241028-bitkom-umsetzungsleitfaden-ki.pdf (zitiert als: *Bearbeiter*, Titel der Bearbeitung, in: *Baum et al.*, Umsetzungsleitfaden zur KI-VO).

Becker, Daniel/Feuerstack, Daniel, Die EU-KI-Verordnung: Überblick und Bewertung der finalen Fassung der KI-VO, KIR 2024, S. 62 – 69.

Becker, Maximilian, Generative KI und Deepfakes in der KI-VO: Für eine Positivkennzeichnung authentischer Inhalte, CR 2024, S. 353 – 366.

BeckOK KI-Recht, *Schefzig, Jens (Hrsg.)/Kilian, Robert (Hrsg.)*, 4. Edition, Stand: 01.11.2025, München 2025 (zitiert als: *Bearbeiter*, in: BeckOK KI-Recht).

Bitkom, Durchbruch bei Künstlicher Intelligenz, Presseinformation vom 15.09.2025, https://www.bitkom.org/Presse/Presseinformation/Durchbruch-Kuenstliche-Intelligenz#:~:text=Inzwischen%20nutzt%20etwa%20jedes%20dritte,im%20Vorjahr%20mit%2037%20Prozent, zuletzt abgerufen am 27.01.2026 (zitiert als: *Bitkom*, Durchbruch bei Künstlicher Intelligenz).

Bomhard, David (Hrsg.)/Pieper, Fritz-Ulli (Hrsg.)/Wende, Susanne (Hrsg.), KI-VO: Verordnung über künstliche Intelligenz, Frankfurt am Main 2025 (zitiert als: *Bearbeiter*, in: KI-VO 2025b).

Bontcheva, Kalina/Pedreschi, Dino/Riess, Christian/Bechmann, Anja/De Gregorio, Giovanni/Botan, Madalina, First Draft Code of Practice on Transparency of AI-Generated Content, https://ec.europa.eu/newsroom/dae/redirection/document/123074, zuletzt abgerufen am 27.01.2026 (zitiert als: *Bontcheva et al.*, First Draft Code of Practice on Transparency).

Borges, Georg, Die europäische KI-Verordnung (AI Act) – Teil 1 Überblick, Anwendungsbereich und erste Einschätzung, CR 2024, S. 497 – 507 (zitiert als: *Borges*, CR 2024a, 497).

Borges, Georg, Die europäische KI-Verordnung (AI Act) Teil 2 – Risikomanagement für Hochrisiko-KI-Systeme, CR 2024, S. 565 – 576 (zitiert als: *Borges*, CR 2024b, 565).

Borges, Georg, Die europäische KI-Verordnung (AI Act) Teil 3 – Transparenzpflichten, Durchsetzung, Gesamtbewertung, CR 2024, S. 633 – 648 (zitiert als: *Borges*, CR 2024c, 633).

Braegelmann, Tom, KI-VO und Compliance – aktuelle Brennpunkte: Schatten-KI und Co.: Rechtstreue Einhaltung geltender Gesetze und Minimierung des Haftungsrisikos, KIR 2024, S. 39 – 42.

Braun Binder, Nadja/Egli, Catherine, Umgang mit Hochrisiko-KI-Systemen in der KI-VO: Strenge Anforderungen der Art. 8 – 15 KI-VO, MMR 2024, S. 626 – 630.

Buchalik, Barbara/Gehrmann, Mareike Christine, Von Nullen und Einsen zu Paragraphen: Der AI Act, ein Rechtscode für Künstliche Intelligenz: Der horizontale und risikobasierte Ansatz für Produktsicherheitsaspekte von KI-Systemen und Allzweck-KI, CR 2024, S. 145 – 153.

Bundesnetzagentur, KI-Kompetenzen nach Artikel 4 KI-Verordnung, Hinweispapier vom Juni 2025, https://www.bundesnetzagentur.de/DE/Fachthemen/Digitales/KI/_functions/Hinweispapier.pdf?__blob=publicationFile&v=2, zuletzt abgerufen am 27.01.2026 (zitiert als: *BNetzA*, Hinweispapier Art. 4).

Büro für Künstliche Intelligenz, Living Repository of AI Literacy Practices, https://ec.europa.eu/newsroom/dae/redirection/document/112203, zuletzt abgerufen am 27.01.2026 (zitiert als: *KI-Büro*, Living Repository).

Chibanguza, Kuuya /Steege, Hans, Die KI-Verordnung – Überblick über den neuen Rechtsrahmen, NJW 2024, S. 1769 – 1775.

Dienes, Jennifer, Anforderungen an die menschliche Aufsicht über Künstliche Intelligenz: Verständnis als Kernelement des Art. 14 KI-VO, MMR 2024, S. 456 – 462.

Dubovitskaya, Elena, KI-Compliance aus Betreibersicht, AG 2024, S. 877 – 891.

Ebers, Martin/Streitbörger, Chiara, Die Regulierung von Hochrisiko-KI-Systemen in der KI-Verordnung, RDi 2024, S. 393 – 400.

Europäische Kommission, AI Act, https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai, zuletzt abgerufen am 27.01.2026 (zitiert als: *Kommission*, AI Act).

Europäische Kommission, Guidelines on the scope of the obligations for general-purpose AI models established by Regulation (EU) 2024/1689 (AI Act), Annex to the Communication to the Commission vom 18.07.2025, https://ec.europa.eu/newsroom/dae/redirection/document/118340, zuletzt abgerufen am 27.01.2026 (zitiert als: *Kommission*, GPAI-Modell-Leitlinien).

Europäische Kommission, KI-Kompetenz – Fragen & Antworten, https://digital-strategy.ec.europa.eu/de/faqs/ai-literacy-questions-answers, zuletzt abgerufen am 27.01.2026 (zitiert als: *Kommission*, KI-Kompetenz – Fragen & Antworten).

Europäische Kommission, Künstliche Intelligenz – Exzellenz und Vertrauen, https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/excellence-and-trust-artificial-intelligence_de, zuletzt abgerufen am 27.01.2026 (zitiert als: *Kommission*, Künstliche Intelligenz – Exzellenz und Vertrauen).

Europäische Kommission, Künstliche Intelligenz – Fragen und Antworten*, https://ec.europa.eu/commission/presscorner/detail/de/qanda_21_1683, zuletzt abgerufen am 27.01.2026 (zitiert als: *Kommission*, Künstliche Intelligenz – Fragen und Antworten).

Europäische Kommission, Leitlinien der Kommission zur Definition eines Systems der künstlichen Intelligenz gemäß der Verordnung (EU) 2024/1689 (KI-Verordnung), Mitteilung der Kommission vom 29.07.2025, https://ec.europa.eu/newsroom/dae/redirection/document/118628, zuletzt abgerufen am 27.01.2026 (zitiert als: *Kommission*, KI-System-Leitlinien).

Europäische Kommission, Leitlinien der Kommission zu verbotenen Praktiken der künstlichen Intelligenz gemäß der Verordnung (EU) 2024/1689 (KI-Verordnung), Mitteilung der Kommission vom 29.07.2025, https://ec.europa.eu/newsroom/dae/redirection/document/118661, zuletzt abgerufen am 27.01.2026 (zitiert als: *Kommission*, Verbotene-Praktiken-Leitlinien).

Feltes, Nicolaj, Article 50 AI Act: Do the Transparency Provisions Improve Upon the Commission's Draft?, JIPITEC 2025, S. 222 – 237.

Fleck, Tilmann, AI literacy als Rechtsbegriff: Anforderungen an die KI-Kompetenz nach Art. 4 KI-VO, KIR 2024, S. 99 – 103.

Fraser, Henry/Bello y Villarino, José-Miguel, Acceptable Risks in Europe's Proposed AI Act: Reasonableness and Other Principles for Deciding How Much Risk Management Is Enough, EJRR 2024, S. 431 – 446.

Gerdemann, Simon, Harmonisierte Normen und ihre Bedeutung für die Zukunft der KI: Auswirkungen und praktische Anwendung, MMR 2024, S. 614 – 621.

Gerdemann, Simon, Konformitätsbewertung als Kernpflicht der KI-Verordnung, NJW 2024, S. 2209 – 2215.

Hilgendorf, Eric/Härtlein, Johannes, KI-VO: Verordnung über künstliche Intelligenz, Baden-Baden 2025 (zitiert als: *Hilgendorf/Härtlein*, KI-VO 2025a).

Hilgendorf, Eric (Hrsg.)/Roth-Isigkeit, David (Hrsg.), Die neue Verordnung der EU zur Künstlichen Intelligenz: Rechtsfragen und Compliance, 2. Aufl., München 2025 (zitiert als: *Bearbeiter*, Titel der Bearbeitung, in: *Hilgendorf/Roth-Isigkeit*, Die neue Verordnung der EU).

Hinderks, Tobias, Die Kennzeichnungspflicht von Deepfakes, ZUM 2022, S. 110 – 119.

ISO/IEC, Guide 51:2014: Safety aspects – Guidelines for their inclusion in standards, 3. Edition, abrufbar unter: https://www.bsigroup.com/contentassets/fb7f1499fa6f43c6b9084be8c2378bc9/iso_iec_guide_51_2014e---safety-aspects----guidelines-for-their-inclusion-in-standards.pdf, zuletzt abgerufen am 27.01.2026.

ISO/IEC/IEEE, 29119-1:2022: Software and systems engineering – Software testing – Part 1: General concepts, 2. Edition, abrufbar unter: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9698145, zuletzt abgerufen am 27.01.2026.

Kaeber, David/Roth-Isigkeit, David, Risikoermittlung für Hochrisiko-KI-Systeme nach der KI-VO, LTZ 2025, S. 3 – 10.

Klos, Christian/Taylan, Ramazan, Von der Theorie zur Praxis: Die EU-KI-Verordnung effektiv umsetzen, CCZ 2024, S. 205 – 211.

Knappertsbusch, Inka/Rappenglück, David, KI-Kompetenz und verbotene KI-Praktiken als Compliance-Pflichten für Arbeitgeber: Anforderungen an die strategische Neuausrichtung der innerbetrieblichen Governance, CR 2025, S. 281 – 289.

Kössel, Andreas, KI und Arbeitsrecht – Individual- und kollektivarbeitsrechtliche Aspekte und Lösungen zum KI-Einsatz, DB 2024, S. 1069 – 1073.

Kraetzig, Viktoria, Deliktsschutz gegen KI-Abbilder – Teil 1: Täuschende Deepfakes, CR 2024, S. 207 – 212.

Krönke, Christoph, Das europäische KI-Gesetz: Eine Verordnung mit Licht und Schatten, NVwZ 2024, S. 529 – 534.

Kumkar, Lea Katharina/Griesel, Moritz, Transparenzpflichten für Deepfakes und synthetische Medieninhalte in der KI-VO: Analyse und Bewertung der Pflichten gem. Art. 50 Abs. 2 und Abs. 4 KI-VO, KIR 2024, S. 117 – 126.

Lauber-Rönsberg, Anne/Meinel, Philip/Laux, Johann/Ruschemeier, Hannah, Hochrisiko oder Ausnahme? Zur Auslegung von Art. 6 Abs. 3 KI-VO, KIR 2025, S. 399 – 407.

Linardatos, Dimitrios, Hochrisiko-KI-Systeme und Verantwortungsverschiebung in der Wertschöpfungskette, ZIP 2024, S. 2497 – 2506.

Mantelero, Alessandro, Beyond Data: Human Rights, Ethical and Social Impact Assessment in AI, Den Haag 2022, abrufbar unter: https://link.springer.com/content/pdf/10.1007/978-94-6265-531-7.pdf, zuletzt abgerufen am 27.01.2026.

Martini, Mario (Hrsg.)/Wendehorst, Christiane (Hrsg.), KI-VO: Verordnung über künstliche Intelligenz, 2. Aufl., München 2026 (zitiert als: *Bearbeiter*, in: KI-VO 2026).

Möller-Klapperich, Julia, Die neue KI-Verordnung der EU, NJ 2024, S. 337 – 342.

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

Ossmann-Magiera, Lea Ludmilla/Dehmel, Susanne, Das Risikomanagementsystem nach den neuen Regeln für Künstliche Intelligenz: Was bedeutet Art. 9 KI-VO für die Praxis?, KIR 2024, S. 134 – 140.

Rappenglück, David/Vonthien, Maximilian, Art. 4 KI-VO operativ umsetzen – Ein Drei-Säulen-Ansatz für KI-Kompetenz, KI-Governance und KI-Compliance im Unternehmen, RDi 2025, S. 398 – 405.

Rost, Maria Christina/Wanser, Carola, Künstliche Intelligenz und Datenschutz: Die Notwendigkeit von KI-Kompetenz zur Absicherung der Datenschutzgrundsätze, EuDIR 2025, S. 276 – 280.

Roth-Isigkeit, David, Der neue Rechtsrahmen für Künstliche Intelligenz in der Europäischen Union: Regelungsgegenstand, Lücken und Problemstellungen der neuen KI-Regulierung, KIR 2024, S. 15 – 20.

Samwald, Matthias/Ziosi, Marta/Zacherl, Alexander/Bengio, Yoshua/Privitera, Daniel/Rajkumar, Nitarshan/Schaake, Marietje/Reuel, Anka/Anderljung, Markus, Code of Practice for General-Purpose AI Models: Safety and Security Chapter, https://ec.europa.eu/newsroom/dae/redirection/document/118119, zuletzt abgerufen am 27.01.2026.

Schippel, Robert, Trainingsvorgaben: Wie kann man KI-Kompetenz nach Art. 4 KI-VO vermitteln? Strategievorschlag zur effektiven Vermittlung von KI-Kompetenz, KIR 2025, S. 119 – 124.

Schopper, Alexander/Raschner, Patrick, Der internationale Anwendungsbereich der KI-VO in Drittstaatskonstellationen: Grundfragen zur extraterritorialen Wirkung, KIR 2025, S. 91 – 100.

Schuett, Jonas, Risk Management in the Artificial Intelligence Act, EJRR 2024, S. 367 – 385.

Schwartmann, Rolf/Zenner, Kai/Köhler, Moritz, Handreichung zu den verbotenen Praktiken gemäß der KI-VO unter Berücksichtigung der Leitlinien der Kommission, EuDIR 2025, S. 74 – 84.

Schwarz, Sibylle, Transparenzpflichten KI-generierter Textinhalte: Redaktionsausnahme: Art. 50 KI-VO, MMR 2025, S. 786 – 790.

Söbbing, Thomas, Die Anforderungen an das Qualitätsmanagement durch die KI-Verordnung, RDi 2025, S. 337 – 345.

Spiegel, Ulrich/Höving, Maximilian, Die Klassifizierung von KI-Systemen nach der KI-VO: Vorschlag zur matrixbasierten Risikoklassifizierung, KIR 2025, S. 231 – 239.

Teichmann, Fabian, Neuer Rechtsrahmen für vertrauenswürdige KI: Risikobasierte Regulierung, Transparenzpflichten und Schnittstellen zum Datenschutzrecht, ZD 2025, S. 495 – 501.

Vasel, Johann Justus, Sieben Sünden und Defizite europäischer KI-Regulierung, EuZW 2024, S. 829 – 835.

von Welser, Marcus, Die KI-Verordnung – ein Überblick über das weltweit erste Regelwerk für künstliche Intelligenz, GRUR-Prax 2024, S. 485 – 488.

Weltersbach, Max/Aslan, Gabriel, Praktische Umsetzung der KI-VO – Komponenten zur strategischen Ausrichtung: Ein Blick auf die regulierungsstrategische Umsetzung innerhalb der Institute, BKR 2025, S. 49 – 57.

Wendehorst, Christiane/Nessler, Bernhard/Aufreiter, Alexander/Aichinger, Gregor, Der Begriff des „KI-Systems" unter der neuen KI-VO: Vorschlag eines „Drei-Faktor-Ansatzes" zur Bewältigung technischer und juristischer Ungereimtheiten, MMR 2024, S. 605 – 613.

Wendt, Janine/Wendt, Domenik H., Das neue Recht der Künstlichen Intelligenz: KI-Verordnung, Leitlinien, Delegierte Rechtsakte, 2. Aufl., Baden-Baden 2025.

Wybitul, Tim, Welche Pflichten haben Betreiber von Hochrisiko-KI-Systemen nach der EU-KI-Verordnung?, BB 2024, S. 2179 – 2183.

Bitte beachten Sie, dass auch frühere eigene Texte entsprechend als Quelle kenntlich zu machen sind

Hiermit versichere ich, ***(Name),*** dass ich die Masterarbeit (bei einer Gruppenarbeit gemäß § 14 Absatz 8 StuPrO den entsprechend gekennzeichneten Teil der Arbeit) selbstständig verfasst und weder diese Arbeit noch Teile davon an anderer Stelle zu Prüfungszwecken eingereicht habe, sowie keine anderen als die angegebenen Quellen und Hilfsmittel benutzt habe.

Schwalbach, 19.01.2026, Luke Niklas Schmidt

Ort, Datum Unterschrift