derrufen, einen Protektor oder die Begünstigten austauschen, so kann der Begründer weiterhin als wirtschaftlicher Eigentümer des Trust-Vermögens angesehen werden. Die Voraussetzungen für das Einfrieren dieser Vermögenswerte wären somit gegeben. Ob eine Person im Namen oder auf Anweisung einer anderen Person handelt, ist ebenfalls im Einzelfall zu prüfen. Indizien sind eine faktische und funktionale Kontrolle über die handelnde Person und Anzeichen für ein koordiniertes Vorgehen.

Der Autor:

Mag. Pitor Daniel Kocab, LL.M., ist Rechtsanwalt bei Schönherr Rechtsanwälte in Wien und ist unter anderem auf das Sanktionsrecht spezialisiert.

lesen.lexisnexis.at/autor/Daniel Kocab/Pitor

Foto: Yannik Zurflüh

Alina Alavi Kia/Stephanie Maier-Herbeck

Ein Jahr KI-VO – Risikoklassifizierung als Herausforderung in der Praxis

» RdW 2025/454

Künstliche Intelligenz hat das Potenzial, erhebliche gesellschaftliche und wirtschaftliche Vorteile zu schaffen, birgt jedoch auch gewisse Risiken.[1] Als besondere Ausprägung des umfangreichen Produktsicherheitsrechts der Europäischen Union[2] etabliert die am 1. 8. 2024 in Kraft getretene KI-Verordnung[3] („KI-VO" bzw „AI Act") Rahmenbedingungen für den EU-weiten Einsatz von KI. Ziel ist es, einerseits einen sicheren und vertrauenswürdigen KI-Einsatz und andererseits ein hohes Schutzniveau für die Gesundheit, Sicherheit und Grundrechte der Bevölkerung zu gewährleisten.[4] Bei Nichteinhaltung dieser Vorschriften drohen erhebliche Geldbußen.

1. Einleitung

Der Anwendungsbeginn der Regelungen in der KI-VO erfolgt gestaffelt:

Seit 2. 2. 2025 sind die Bestimmungen zur KI-Kompetenz sowie zu verbotenen KI-Systemen anwendbar.[5] Auf einer zweiten und dritten Stufe finden die besonders strengen Vorschriften für sogenannte „Hochrisiko-KI-Systeme" Anwendung. Hierbei ist zu differenzieren: Die Vorschriften für Hochrisikosysteme, die als besonders kritisch eingestuft sind – dh solche gem Anhang III KI-VO – sowie fast alle übrigen Vorschriften der KI-VO greifen ab 2. 8. 2026.[6] Ab 2. 8. 2027 sind sodann die Vorschriften für jene Hochrisiko-KI-Systeme anwendbar, die unter Anhang I fallen.[7]

Der Großteil der Vorschriften der KI-VO gilt damit spätestens ab dem 2. 8. 2026 und lässt somit nicht mehr lange auf sich warten; vieles ist aber im Detail noch offen. Es ist also für Anbieter und Betreiber als Hauptadressaten der KI-VO unumgänglich, sich mit der KI-VO auseinanderzusetzen. Insb für Unternehmen, die KI-Systeme anbieten oder betreiben, die in den Hochrisiko-Bereich fallen könnten, ist es unabdingbar, sich frühzeitig mit der Einstufung, ob es sich bei dem KI-System um ein Hochrisiko-KI-System handelt (Risikoklassifizierung), auseinanderzusetzen. Denn der Großteil der Pflichten nach der KI-VO betrifft Hochrisiko-KI-Systeme.[8] Diese Risikoklassifizierung ist in der Praxis jedoch deutlich komplexer, als es auf den ersten Blick erscheinen mag. Der gegenständliche Beitrag dient dazu, einen Überblick über die KI-VO, die nun seit einem Jahr in Geltung ist, zu geben und sodann eine mögliche Hilfestellung für die in der Praxis so relevante Risikoklassifizierung zu bieten.

Bevor jedoch näher auf die Anforderungen und Herausforderungen der Risikoklassifizierung eingegangen wird, erfolgt ein kurzer Überblick zur Systematik und zum Regelungsinhalt der KI-VO.

1 Die Autorinnen danken Frau Mag. *Christina Kampner* und Herrn Dr. *Felix Krysa* für die Unterstützung.

2 *Borges*, Der Begriff des KI-Systems – Tatbestandsmerkmale und Auslegungsansätze, CR 2023, 706 (706 Rz 2).

3 Verordnung (EU) 2024/1689 des Europäischen Parlaments und des Rates vom 13. Juni 2024 zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz.

4 ErwGr 1 KI-VO.

5 Art 113 UAbs 3 lit a KI-VO.

6 Art 113 UAbs 2 KI-VO.

7 Art 113 UAbs 3 lit c KI-VO.

8 Vgl den umfassenden Pflichtenkatalog in Art 6 ff KI-VO.

2. Überblick über den Regelungsinhalt der KI-VO

2.1. Sachlicher Anwendungsbereich

Ungeachtet gesetzlich vorgesehener Ausnahmen[9] ist für die Anwendung der KI-VO maßgebend, dass es sich um den Einsatz eines KI-Systems iSd KI-VO handelt. Art 3 Z 1 der KI-VO definiert ein „KI-System" wie folgt: *„Ein maschinengestütztes System, das für einen in unterschiedlichem Grade autonomen Betrieb ausgelegt ist und das nach seiner Betriebsaufnahme anpassungsfähig sein kann und das aus den erhaltenen Eingaben für explizite oder implizite Ziele ableitet, wie Ausgaben wie etwa Vorhersagen, Inhalte, Empfehlungen oder Entscheidungen erstellt werden, die physische oder virtuelle Umgebungen beeinflussen können."*

Als Hilfestellung zur Ermittlung, ob eine Software als KI-System iSd KI-VO einzuordnen ist, hat die Europäische Kommission im Februar 2025 „Leitlinien zur Definition eines Systems der künstlichen Intelligenz"[10] veröffentlicht. Es handelt sich dabei um unverbindliche Leitlinien, die als Hilfestellung dienen sollen und im Laufe der Zeit bei Bedarf aktualisiert werden. In diesen Leitlinien wird klargestellt, dass die Definition eines KI-Systems darauf abzielt, ein breites Spektrum von KI-Systemen zu umfassen, aber gleichzeitig die Komplexität und Vielfalt von KI-Systemen widerspiegeln soll.

2.2. Wesentliche Regelungspunkte und Akteure

Basierend auf dem Lebenszyklus einer KI definiert die KI-VO primär Pflichten für unterschiedliche Akteure. Diese Pflichten nach der KI-VO treffen Anbieter, Betreiber, Bevollmächtigte, Einführer oder Händler. Aufgrund der Vielzahl der sie treffenden Pflichten sind Anbieter[11] und Betreiber[12] die Hauptadressaten der KI-VO.

Der Begriff des „Anbieters" iSd KI-VO deckt sich mit jenem des „Herstellers" in anderen Rechtsvorschriften, etwa im Bereich des Produktsicherheitsrechts.[13] Unter „Betreiber" versteht die KI-VO eine juristische Person, die ein KI-System in eigener Verantwortung verwendet, also auf eigene Rechnung und auf eigenes Risiko.[14]

Die KI-VO verfolgt einen risikobasierten Ansatz, der zu einer gesetzlich festgelegten Risikoklassifizierung führt. Danach wird zwischen verbotenen KI-Systemen,[15] Hochrisiko-KI-Systemen,[16] Systemen mit begrenztem Risiko[17] und solchen mit minimalem Risiko unterschieden. Daneben gibt es noch zusätzliche Regelungen für KI-Modelle mit allgemeinem Verwendungszweck („GPAI-Modelle"),[18] die jedoch im Rahmen dieses Beitrags nicht näher beleuchtet werden.

Siehe Abbildung auf Seite 596

Die Einordnung in eine dieser Risikoklassen ist die Grundvoraussetzung, um in der Praxis identifizieren zu können, welche konkreten Pflichten die Entwicklung, Bereitstellung oder Verwendung eines KI-Systems mit sich bringt.

KI-Systeme, die ein inakzeptables Risiko aufweisen, dürfen nicht eingesetzt werden. So sind zum Schutz wesentlicher Werte der EU insb folgende Praktiken verboten (Art 5 Abs 1 KI-VO):

- Unterschwellige Manipulation (Art 5 Abs 1 lit a);
- Ausnutzung einer Schwäche oder Schutzbedürftigkeit (Art 5 Abs 1 lit b);
- Bewertung oder Klassifizierung auf der Grundlage von sozialem Verhalten, sogenanntes *„Social Scoring"* (Art 5 Abs 1 lit c);
- Emotionserkennungssysteme (Art 5 Abs 1 lit f).

Die Europäische Kommission hat im Februar 2025 unverbindliche „Leitlinien zu verbotenen Praktiken der künstlichen Intelligenz"[19] mit dem Zweck veröffentlicht, die in Art 5 KI-VO lediglich abstrakt umschriebene Aufzählung verbotener Praktiken zu konkretisieren. Mit rechtlichen Erläuterungen und Beispielen sollen diese bei der Prüfung helfen, welche Praktiken aufgrund ihrer potenziellen Risiken für die europäischen Werte und Grundrechte als inakzeptabel gelten.

Die Zuordnung zur nächsten Risikostufe – jene der Hochrisiko-KI-Systeme – wird nachfolgend im Detail in Abschnitt 3. erläutert.

Einfache KI-Systeme, von denen keine besonderen Risiken ausgehen, werden als KI-Systeme mit minimalem Risiko bezeichnet. Sie dürfen grds ohne Erfüllung besonderer Maßnahmen eingesetzt werden. Anbieter und Betreiber können sich jedoch freiwillig Verhaltenskodizes unterwerfen.

2.3. Pflichten

Die Pflichten nach der KI-VO knüpfen an die Einordnung in eine Risikoklasse an und treffen vorrangig Anbieter und Betreiber von Hochrisiko-KI-Systemen. Die Pflichten sind im Einzelnen sehr umfangreich und erfordern eine entsprechende Auseinandersetzung und Vorbereitung. Kurz gesagt: Die Einhaltung der Pflichten lässt sich nicht von heute auf morgen umsetzen.[20]

2.4. Sanktionen

Die KI-VO verpflichtet die Mitgliedstaaten, „Vorschriften für Sanktionen und andere Durchsetzungsmaßnahmen" zu erlassen. Zudem sieht die KI-VO folgende Geldbußen vor, bei deren Verhängung ua die Art, Schwere und Dauer des jeweiligen Verstoßes,

9 Vgl Art 2 Abs 2 ff KI-VO.
10 Abrufbar unter: https://digital-strategy.ec.europa.eu/de/library/commission-publishes-guidelines-ai-system-definition-facilitate-first-ai-acts-rules-application (9. 8. 2025).
11 Vgl Art 6 ff KI-VO.
12 Vgl Art 26 KI-VO.
13 *Wendehorst* in *Martini/Wendehorst*, KI-VO (2024) Art 3 Rz 64.
14 Art 3 Z 4 KI-VO; *Wendehorst* in *Martini/Wendehorst*, KI-VO Art 3 Rz 84.
15 Art 5 KI-VO.
16 Art 6 KI-VO.
17 Art 50 KI-VO.
18 Art 51 ff KI-VO.
19 Abrufbar unter: https://digital-strategy.ec.europa.eu/de/library/commission-publishes-guidelines-prohibited-artificial-intelligence-ai-practices-defined-ai-act (9. 8. 2025).
20 Auf eine Auflistung der umfassenden Pflichten wird im Rahmen dieses Beitrags verzichtet.

das Verschulden und der verursachte Schaden zu berücksichtigen sind (Art 99 Abs 7 KI-VO):

- bis zu 35 Mio € oder 7 % des weltweiten Jahresumsatzes für Verstöße gegen die Vorschriften über verbotene Praktiken gem Art 5 (Art 99 Abs 3 KI-VO);
- bis zu 15 Mio € oder 3 % des weltweiten Jahresumsatzes für Verstöße gegen verschiedene Pflichten der Anbieter, deren Bevollmächtigte, Betreiber, Einführer oder Händler (Art 16, 22, 23, 24, 26, 31, 33 Abs 1, 3 und 4 sowie Art 34 und 50 (Art 99 Abs 4 KI-VO);
- bis zu 7,5 Mio € oder 1 % des weltweiten Jahresumsatzes im Falle der Bereitstellung falscher, unvollständiger oder irreführender Informationen an notifizierte Stellen oder zuständige nationale Behörden auf deren Auskunftsersuchen hin (Art 99 Abs 5 KI-VO).

Für Start-ups und KMU sollen die Sanktionen geringer ausfallen, weshalb lediglich der niedrigere Betrag verhängt wird.[21]

3. Risikoklassifizierung nach der KI-VO und die Folgen

3.1. Allgemein

Die Relevanz der Zuordnung eines KI-Systems zu einer der Risikokategorien der KI-VO folgt aus den mit dieser Einordnung korrespondierenden Pflichten, die die KI-VO den involvierten Akteuren – insb den Anbietern – auferlegt. Jede Risikokategorie geht mit unterschiedlichen rechtlichen Anforderungen einher, die in der Praxis erhebliche Auswirkungen haben können. Dies lässt sich exemplarisch an den weitreichenden Pflichten für Anbieter von Hochrisiko-KI-Systemen illustrieren: Bspw treffen den Anbieter eines Hochrisiko-KI-Systems bereits während der Trainingsphase umfassende Pflichten im Bereich der Datengovernance. Zudem ist während des gesamten Lebenszyklus des Hochrisiko-KI-Systems eine angemessene menschliche Aufsicht sicherzustellen.

So ist – auch vor dem Hintergrund der drohenden Sanktionen – verständlich, dass die Frage, ob ein KI-System als Hochrisiko-KI-System einzustufen ist, für Anbieter und Betreiber von KI-Systemen von höchstem Interesse ist. Auch in unserer Beratungspraxis hat sich im vergangenen Jahr gezeigt, dass diese Risikoklassifizierung eine hohe praktische Relevanz hat, die Akteure aufgrund der komplex beschriebenen Voraussetzungen in Art 6 KI-VO und den darin verwiesenen Anhängen I und III der KI-VO aber vor eine große (rechtliche) Herausforderung stellt.

In Art 6 KI-VO werden die Voraussetzungen für eine Einstufung als Hochrisiko-KI-Systeme festgelegt. Grob zusammengefasst wird unterschieden in:[22]

- Produktbezogene Hochrisiko-KI-Systeme (Art 6 Abs 1 KI-VO iVm Anhang I) und
- Hochrisiko-KI-Systeme nach Einsatzbereich (Art 6 Abs 2 KI-VO iVm Anhang III).

Die Komplexität für die Risikoklassifizierung in der Praxis ergibt sich daraus, dass Hochrisiko-KI-Systeme zwar grds in Art 6 KI-VO geregelt sind, dieser Artikel aber auf die Anhänge I und III

21 Vgl *Feiler/Forgó*, KI-VO (2024) Art 99 Rz 1 f.

22 *Feiler/Forgó*, KI-VO Art 6 Rz 52.

der Verordnung verweist. Zu berücksichtigen sind darüber hinaus aber auch die Ausnahmen von einer Einordnung als Hochrisiko-KI-System, die in Art 6 Abs 3 KI-VO enthalten sind und die umständlich (und bisweilen auch inhaltlich nicht eindeutig) formuliert sind. Zuletzt werden diese Ausnahmen wiederum durch eine Gegenausnahme in Art 6 Abs 3 UAbs 2 KI-VO eingeschränkt.

Die von der Kommission gem Art 6 Abs 5 KI-VO bis zum 2. 2. 2026 zu veröffentlichenden Leitlinien zur praktischen Umsetzung samt einer umfassenden Liste praktischer Beispiele für Anwendungsfälle für KI-Systeme, die hoch riskant sind, werden daher mit Spannung erwartet. Auf diese Leitlinien zu warten, stellt aber für viele Unternehmen keine Option dar, weil die Pflichten für Hochrisiko-KI-Systeme nach Anhang III KI-VO bereits mit August 2026 in Geltung treten und für viele der Hochrisiko-Pflichten eine Vorbereitungszeit von einem halben Jahr viel zu kurz erscheint. Kurzum: Anbieter und Betreiber müssen sich schon jetzt mit der Risikoklassifizierung ihrer KI-Systeme auseinandersetzen.

3.2. Anknüpfungspunkt: Zweckbestimmung des Anbieters

Die Risikoklassifizierung knüpft an den spezifischen Zweck an, der mit dem Einsatz des jeweiligen KI-Systems verfolgt wird. Für die Praxis maßgeblich ist daher, dass die Risikoklassifizierung stets einzelfallbezogen anhand des ganz spezifischen, geplanten Einsatzzwecks des KI-Systems zu erfolgen hat.

Diese sogenannte „Zweckbestimmung" ist definiert als *„die Verwendung, für die ein KI-System laut Anbieter bestimmt ist, einschließlich der besonderen Umstände und Bedingungen für die Verwendung, entsprechend den vom Anbieter bereitgestellten Informationen in den Betriebsanleitungen, im Werbe- oder Verkaufsmaterial und in diesbezüglichen Erklärungen sowie in der technischen Dokumentation"* (Art 3 Z 12 KI-VO). Es geht also schon aus der Definition der Zweckbestimmung hervor, dass stets der vom Anbieter festgelegte Zweck für die weitere Beurteilung maßgeblich ist.

Auch wenn Art 6 KI-VO seinem Wortlaut nach nicht ausdrücklich auf die Zweckbestimmung Bezug nimmt, ist diese Definition nach hA auf die Frage der Hochrisiko-Einstufung übertragbar.[23]

Für die Einordnung eines KI-Systems als Hochrisiko-KI-System iSd KI-VO ist primär die vom Anbieter definierte Zweckbestimmung maßgeblich.[24] Es kommt also darauf an, für welchen Einsatz der Anbieter das KI-System „zweckwidmet". Potenziell denkbare weitere Einsatzmöglichkeiten des Systems, die der Anbieter jedoch bei der Entwicklung nicht im Blick hatte, bleiben demgegenüber unbeachtlich. Der Anbieter hat es daher grds selbst in der Hand, durch eine gezielte Festlegung des Einsatzbereichs sein KI-System auf Anwendungsfelder zu beschränken, die nicht zu einer Hoch-Risiko-Klassifizierung führen.[25] Vor dem Hintergrund, dass die KI-VO in Teilen eine besondere Ausprägung des Produktsicherheitsrechts ist, erscheint dies auch sachgerecht, weil der Anbieter ja nicht alle zweckwidrigen Einsätze seines KI-Systems mitberücksichtigen kann. Eine ausdrückliche Negativabgrenzung möglicher Hochrisikobereiche ist nicht erforderlich. Ungeklärt bleibt allerdings, ob und in welchem Umfang der Anbieter offenkundige Hochrisikozwecke ohne sachliche Rechtfertigung ausschließen darf.[26]

3.2.1. Zweckänderung durch den Betreiber maßgeblich?

In bestimmten Konstellationen ist jedoch nicht die vom Anbieter vorgegebene Zweckbestimmung, sondern eine spätere Zweckänderung durch andere Akteure – insb durch den Betreiber – maßgeblich. Art 25 Abs 1 lit c KI-VO ordnet an, dass ein Betreiber als Anbieter gilt, wenn er die Zweckbestimmung eines ursprünglich nicht als Hochrisiko eingestuften KI-Systems so modifiziert, dass *„das betreffende KI-System zu einem Hochrisiko-KI-System [...] wird"*. Durch eine solche Zweckänderung wird der Betreiber daher rechtlich in die Rolle des Anbieters versetzt und unterliegt folglich denselben Pflichten. Die „Hochstufung" bezieht sich dabei nur auf das konkret geänderte System und wirkt nicht auf baugleiche Systeme derselben Art.[27]

3.3. Hochrisiko-Klassifizierung: Prüfschema grafisch dargestellt

Die nachstehende grafische Darstellung gibt einen Überblick über das Vorgehen zur Einordnung eines KI-Systems als Hochrisiko-KI-System nach Art 6 KI-VO.

Siehe Abbildung auf Seite 598

3.4. Hochrisiko-Klassifizierung: Prüfschritte

Art 6 KI-VO unterscheidet zwei Gruppen von Hochrisiko-KI-Systemen: einerseits jene, die aufgrund ihrer Zuordnung zu einer Produktgruppe *per se* ein Hochrisiko-KI-System sind (produktbezogene Hochrisiko-KI-Systeme gem Art 6 Abs 1 iVm Anhang I KI-VO), und andererseits jene KI-Systeme, die aufgrund des konkreten, geplanten Einsatzbereichs als Hochrisiko-KI-System einzuordnen sind (Hochrisiko-KI-Systeme aufgrund des Einsatzbereichs gem Art 6 Abs 2 iVm Anhang III KI-VO).

3.4.1. Produktbezogene Hochrisiko-KI-Systeme

Der erste Prüfschritt betrifft also die Frage, ob es sich beim konkreten KI-System um ein produktbezogenes Hochrisiko-KI-Sys-

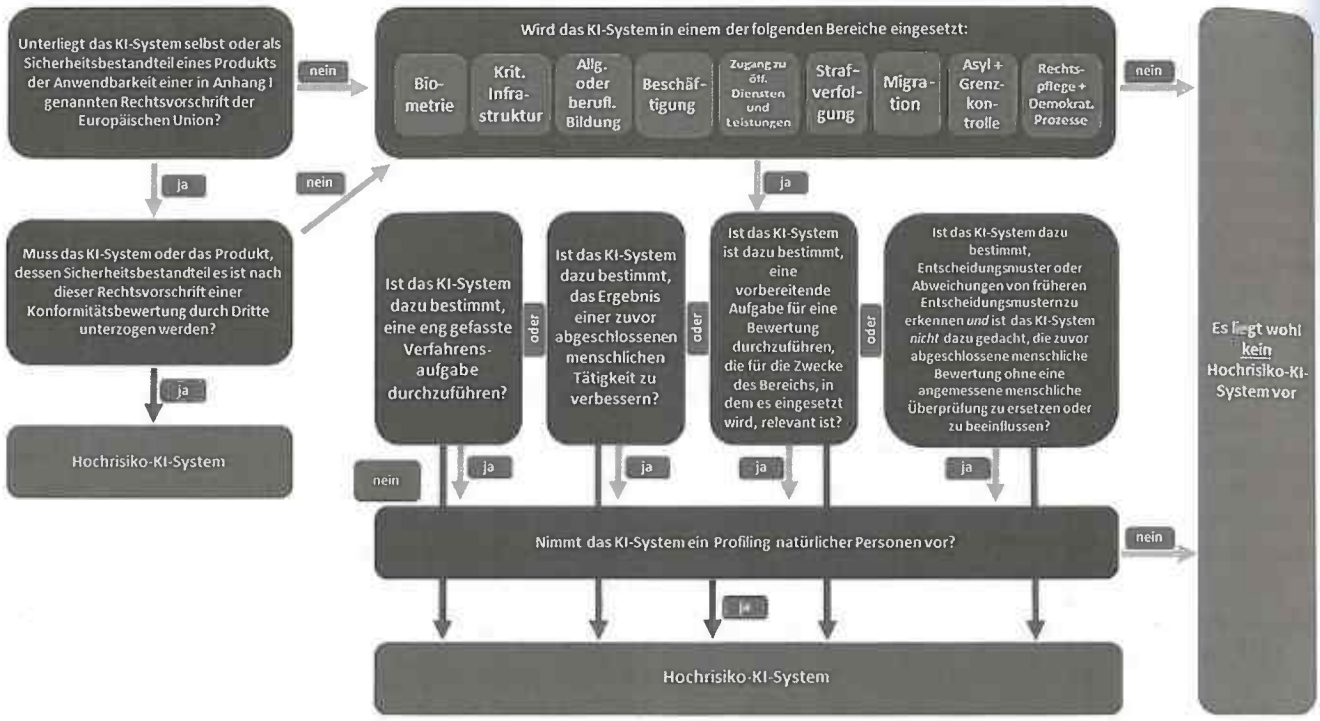
23 So *Ebers/Streitbörger*, Die Regulierung von Hochrisiko-KI-Systemen in der KI-Verordnung, in RDi-Sonderausgabe „Künstliche Intelligenz" (2024) 393 Rz 7.

24 Vgl *Ebers/Streitbörger* in RDi-Sonderausgabe „Künstliche Intelligenz" 393 Rz 7.

25 *Borges*, Die europäische KI-Verordnung (AI Act) Teil 2 – Risikomanagement für Hochrisiko-KI-Systeme, CR 2024, 565 (569 Rz 35, 38–42); *Ebers/Streitbörger* in RDi-Sonderausgabe „Künstliche Intelligenz" 393 Rz 11.

26 *Ebers/Streitbörger* in RDi-Sonderausgabe „Künstliche Intelligenz" 393 Rz 11.

27 *Borges*, CR 2024, 565 (569 Rz 46).



tem handelt. Das ist dann der Fall, wenn das KI-System ein Produkt oder eine Sicherheitskomponente von einem Produkt ist, das in den Anwendungsbereich einer der in Anhang I aufgelisteten EU-Produktregulierungen fällt. Umfasst sind bspw Maschinen, Aufzüge, Spielzeug, persönliche Schutzausrüstungen und Medizinprodukte.

Voraussetzung für die Einstufung als Hochrisiko-KI nach Art 6 Abs 1 iVm Anhang I KI-VO ist zudem, dass die jeweilige Produktregulierung eine Konformitätsbewertung vorsieht.

Ist das der Fall, handelt es sich bei dem KI-System um ein Hochrisiko-KI-System. Anwendungsausnahmen gibt es bei diesen produktbezogenen Hochrisiko-KI-Systemen nicht, sodass die Prüfung bereits hier endet.

3.4.2. *Hochrisiko-KI-Systeme aufgrund des Einsatzbereichs*

Losgelöst vom Produktsicherheitsrecht legt Art 6 Abs 2 KI-VO fest, dass KI-Systeme, die in einen Einsatzbereich des Anhangs III KI-VO fallen, Hochrisiko-KI-Systeme sind. Bei den in Anhang III KI-VO genannten Einsatzbereichen handelt es sich insb um solche, bei denen anzunehmen ist, dass ein KI-System ein hohes Risiko für die Gesundheit und Sicherheit oder die Grundrechte von Personen mit sich bringen kann.

In Anhang III werden acht Einsatzbereiche aufgelistet, die sogenannten „kritischen Einsatzbereiche". Erfasst sind bspw Personalmanagement, Strafverfolgung, Asyl und Rechtspflege. In diesen Einsatzbereichen sind wiederum konkrete Funktionalitäten definiert. ZB nennt Anhang III KI-VO im Einsatzbereich „Personalmanagement" KI-Systeme, die bestimmungsgemäß für das Recruiting verwendet werden sollen. In den Bereichen „Strafverfolgung" und „Asyl" wird der Einsatz von KI-basierten Lügendetektoren genannt. In der Rechtspflege soll zB die KI-basierte Unterstützung bei der Auslegung von Sachverhalten durch Justizbehörden in den Hochrisiko-Bereich fallen.

Immer dann, wenn ein KI-System in einer in Anhang III KI-VO beschriebenen Funktionalität eingesetzt werden soll, geht die KI-VO davon aus, dass ein Risiko von diesem System ausgeht und klassifiziert das KI-System als Hochrisiko-KI-System.

3.4.3. *Ausnahmen gemäß Art 6 Abs 3 KI-VO*

Fällt hiernach das KI-System in einen Einsatzbereich des Anhangs III KI-VO, kann einer Einordnung als Hochrisiko-KI-System jedoch Art 6 Abs 3 KI-VO entgegenstehen. Art 6 Abs 3 KI-VO bezieht sich ausschließlich auf KI-Systeme, die nach Art 6 Abs 2 iVm Anhang III KI-VO als Hochrisiko-KI-Systeme einzuordnen wären, nicht auf die produktbezogenen Hochrisiko-KI-Systeme gem Art 6 Abs 1 iVm Anhang I KI-VO.

Bemerkenswert ist, dass die Ausgestaltung dieser vier Ausnahmen in der Literatur[28] durchwegs kritisch gesehen wird. Insoweit wird insb die Frage aufgeworfen, ob es einen großen Anwendungsbereich für diese – sehr spezifischen – Ausnahmen geben wird. Unklar ist insb auch die Abgrenzung der einzelnen Ausnahmen zueinander.

28 Vgl *Wendehorst* in *Martini/Wendehorst*, KI-VO Art 6 Rz 93 f; *Schwartmann/Köhler* in *Schwartmann/Keber/Zenner*, KI-VO Leitfaden für die Praxis (2024) Kapitel 1 Rz 129 ff.

Folgende Ausnahmen sieht Art 6 Abs 3 KI-VO vor:

a) Die erste Ausnahme betrifft KI-Systeme, die dazu bestimmt sind, eine eng gefasste Verfahrensaufgabe durchzuführen (Art 6 Abs 3 lit a KI-VO). Von dieser Ausnahme sollen KI-Systeme erfasst sein, die etwa unstrukturierte Daten in strukturierte Daten umwandeln, die eingehende Dokumente in Kategorien einordnen oder die zur Erkennung von Duplikaten eingesetzt werden. Diese Aufgaben sind so eng gefasst und begrenzt, dass sie nur beschränkte Risiken darstellen[29] und somit nicht als hoch riskant gelten sollen.
b) Die zweite Ausnahme umfasst solche KI-Systeme, die das Ergebnis einer zuvor abgeschlossenen menschlichen Tätigkeit verbessern sollen (Art 6 Abs 3 lit b KI-VO). Beispiel hierfür sind KI-Systeme, deren Ziel es ist, von Menschen verfasste Dokumente sprachlich zu verbessern, etwa den professionellen Ton, den wissenschaftlichen Sprachstil, oder den Text sonst einem bestimmten Stil anzupassen.[30]
c) Nach der dritten Ausnahme ist ein KI-System dann nicht hoch riskant, wenn es lediglich dazu dient, Entscheidungsmuster oder Abweichungen von früheren Entscheidungsmustern zu erkennen (Art 6 Abs 3 lit c KI-VO). Hier wird in den Erwägungsgründen ausgeführt, dass deswegen kein hohes Risiko bestehe, weil das KI-System nur auf eine zuvor abgeschlossene menschliche Entscheidung folge, die das KI-System ohne angemessene menschliche Überprüfung nicht ersetze oder beeinflusse. Als Beispiel nennen die Erwägungsgründe KI-Systeme, die in Bezug auf ein bestimmtes Benotungsmuster eines Lehrers dazu verwendet werden können, um nachträglich zu prüfen, ob der Lehrer möglicherweise von dem Benotungsmuster abgewichen ist, um so auf mögliche Unstimmigkeiten oder Unregelmäßigkeiten aufmerksam zu machen.[31]
d) Die vierte Ausnahme umfasst KI-Systeme, die für die Zwecke der in einem in Anhang III KI-VI genannten Einsatzbereiche lediglich eine vorbereitende Aufgabe für eine Bewertung durchführen. Sie zielt im Wesentlichen darauf ab, ganz einfache Vorbereitungstätigkeiten auszuführen, zB Dokumentenübersetzungen, Text- und Sprachverarbeitung.[32] Was darunter genau zu verstehen ist, wird in der Literatur[33] diskutiert und ist derzeit noch offen.

Sollte für das konkrete KI-System eine der oben genannten Ausnahmen greifen, ist schließlich noch die Einschränkung in Art 6 Abs 3 letzter Satz KI-VO zu beachten. Hiernach sollen die zuvor genannten Ausnahmen nicht gelten, wenn das KI-System ein *Profiling* natürlicher Personen vornimmt. Anders gesagt: Wenn ein KI-System ein *Profiling* einer natürlichen Person in einem in Anhang III KI-VO genannten Einsatzbereich durchführt, erübrigt sich die Prüfung der Ausnahmen nach Art 6 Abs 3 KI-VO; dieses KI-System ist stets als Hochrisiko-KI-System einzuordnen. Der Begriff des *Profiling* ist – so die Erwägungsgründe – iSv Art 4 Nr 4 DSGVO zu verstehen.[34]

Sollte ein Anbieter nach Prüfung der genannten Ausnahmen der Meinung sein, dass ein KI-System, das in einem in Anhang III KI-VO genannten Einsatzbereich eingesetzt werden soll, aufgrund der Anwendbarkeit der Ausnahmen nicht als hoch riskant einzuordnen ist (und das KI-System auch kein *Profiling* vornimmt), hat der Anbieter vor Inverkehrbringen oder Inbetriebnahme diese Bewertung zu dokumentieren (Art 6 Abs 4 KI-VO) und eine Registrierung in einer zu diesem Zweck zu erstellenden EU-Datenbank (siehe Art 71 KI-VO) vorzunehmen. Diese Datenbank existiert derzeit noch nicht; ebenso wenig sind Details zum Ablauf und den konkreten Anforderungen an die Registrierung bekannt.

3.5. Hochrisiko-Einstufung gilt für das gesamte KI-System

Wie eingangs erwähnt, richtet sich die Einstufung als Hochrisiko-KI-System iSd KI-VO grds nach der vom Anbieter vorgenommenen Zweckbestimmung. Offen ist jedoch, wie in jenen Fällen zu verfahren ist, in denen ein KI-System für verschiedene Anwendungsfelder konzipiert ist, von denen lediglich einige zu einer Einordnung des KI-Systems als Hochrisiko-KI-System führen würden. Wird ein solches System in einem anderen Kontext eingesetzt, der nach der KI-VO keine Hochrisikoeigenschaft begründet, stellt sich für Anbieter, aber insb auch für Betreiber die – relevante – Frage, ob das KI-System in allen Einsatzbereichen mit der Einstufung als Hochrisiko-KI-System „behaftet" ist und damit bei jeglichem Einsatz dieses KI-Systems den Anforderungen an Hochrisiko-KI-Systeme genügen muss.

Bei der KI-VO handelt es sich im Kern um Produktsicherheitsrecht.[35] Gegenstand der Regulierung ist das KI-System als (technisches) Produkt – unabhängig davon, in welchem Anwendungsbereich es konkret zum Einsatz gelangt. Diese beiden Argumente sprechen dafür, dass es auf den konkreten Einsatzbereich des KI-Systems nicht ankommen kann. Zudem kann eine Parallele zu den Medizinprodukten gezogen werden. Für diese hat der EuGH bereits judiziert, dass die konkrete Nutzung für die regulatorische Einordnung unbeachtlich sei.[36] Eine systembezogene Auslegung wird zudem durch den Wortlaut des Art 6 Abs 1 KI-VO gestützt, wonach die Einstufung als Hochrisiko-KI-System auf den Zeitraum vor dem erstmaligen Inverkehrbringen Bezug nimmt. Es scheint ferner nur schwer vorstellbar, dass ein Anbieter bei der Entwicklung eines vielseitig einsetzbaren KI-Systems die risikobezogenen Differenzierungen nach den einzelnen Einsatzgebieten unterscheidet und nur für diese den Anforderungen der KI-VO an ein Hochrisiko-KI-System genügt.

29 Siehe ErwGr 53 KI-VO.
30 Ibid.
31 Ibid.
32 Ibid.
33 Vgl *Wendehorst* in *Martini/Wendehorst*, KI-VO Art 6 Rz 93 f; *Schwartmann/Köhler* in *Schwartmann/Keber/Zenner*, KI-VO Leitfaden für die Praxis Kapitel 1 Rz 129 ff.
34 ErwGr 53 KI-VO.
35 Vgl *Roos/Weitz*, Hochrisiko-KI-Systeme im Kommissionsentwurf für eine KI-Verordnung, MMR 2021, 844 (846).
36 EuGH C-219/11, ECLI:EU:C:2012:742, Rn 30 f.

Für die rechtliche Einordnung eines KI-Systems als Hochrisiko-KI-System kommt es damit grds[37] nicht auf den konkreten Anwendungsfall des jeweiligen Systems an. Entscheidend ist vielmehr, ob das KI-System nach Maßgabe der vom Anbieter definierten Zweckbestimmung in einen Anwendungsbereich fällt, der zu einer Einordnung als Hochrisiko-KI-System führt.[38] Ist Letzteres bereits im Hinblick auf eine einzige vorgesehene Zweckbestimmung gegeben, so genügt dies, um das System insgesamt als Hochrisiko-KI-System zu qualifizieren – unabhängig davon, ob es im Einzelfall tatsächlich in einem solchen Bereich eingesetzt wird. Vereinfacht gesagt gilt allgemein: Wenn ein KI-System in einem Bereich als hoch riskant einzustufen ist, dann erstreckt sich diese Klassifizierung auf sämtliche Einsatzbereiche dieses KI-Systems. In solchen Konstellationen ist der Anbieter also unabhängig von dem konkreten Einsatzweck des KI-Systems verpflichtet, sämtliche regulatorischen Anforderungen zu erfüllen, die für Hochrisiko-KI-Systeme normiert sind. Abweichendes könnte jedoch uE möglicherweise im Hinblick auf die Betreiberpflichten gem Art 26 KI-VO zu erwägen sein. Wird ein KI-System ausschließlich in einem Kontext eingesetzt, der nach der KI-VO nicht zu einer Hochrisiko-Einstufung führen würde, verliert der Umstand, dass das System prinzipiell auch in Hochrisikobereichen einsetzbar wäre, für den Betreiber an rechtlicher Relevanz. In diesem konkreten Einsatzbereich kann sich die spezifische Gefahr, die zu einer Einordnung des KI-Systems als Hochrisiko-KI-System führt, aber gerade nicht verwirklichen. Die Systematik der KI-VO verdeutlicht zudem, dass die Risikoklassifizierung nicht an die technischen Fähigkeiten oder das Funktionsspektrum des Systems anknüpft, sondern allein an den vorgesehenen Einsatzkontext. Auch ist zu berücksichtigen, dass die KI-VO eine besondere Ausprägung des Produktsicherheitsrecht ist. Innerhalb dessen sind typischerweise jedoch gerade keine Verpflichtungen des Verwenders – wie sie Art 26 KI-VO normiert – vorgesehen.[39] Insofern stellt Art 26 KI-VO eine aus Sicht des klassischen Produktsicherheitsrechts atypische Regelung dar, die sich nicht ohne Weiteres auf dessen Dogmatik stützen lässt.

4. Fazit

Im ersten Jahr der KI-VO hat sich gezeigt, dass neben anderen Fragen insb die Risikoklassifizierung – also die Einordnung, ob ein KI-System nach der KI-VO als Hochrisiko-System gilt – für die Praxis eine Herausforderung darstellt, weil die Prüfung des Vorliegens eines Hochrisiko-KI-Systems iSd Art 6 Abs 2 iVm Anhang III KI-VO durchwegs komplex aufgebaut ist.

Die Risikoklassifizierung knüpft an die Zwecke des zu beurteilenden KI-Systems an. Relevant ist hier der vom Anbieter festgelegte Zweck. Unerheblich sind potenzielle, dh nicht konkret vom Anbieter geplante, Einsatzmöglichkeiten des KI-Systems. Ebenso unerheblich ist, wozu ein KI-System theoretisch in der Lage wäre.

Da der Anbieter die Einsatzbereiche und Zwecke des KI-Systems selbst bestimmt, hat er einen gewissen Gestaltungsspielraum. Wichtig ist dies aus folgendem Grund: Gelangt der Anbieter mit einem Einsatzbereich oder Zweck in den Hochrisiko-Bereich, ist das gesamte KI-System als Hochrisiko-KI-System einzuordnen.[40] Die Risikoklassifizierung gilt damit für das gesamte System und nicht für die konkreten Einsatzbereiche. Dies führt dazu, dass der Einsatz eines eigentlich „harmlosen" KI-Systems – bzw eines KI-Systems in einem „harmlosen" Einsatzbereich – mit Hochrisiko-Pflichten verbunden ist, wenn das KI-System seiner Zweckbestimmung nach auch in Hochrisiko-Einsatzbereichen eingesetzt werden soll. Das kann zB gelten, wenn ein KI-System zur automatisierten Filterung von Bewerbungen eingesetzt wird, dh in den Hochrisiko-Bereich fällt, aber dieselbe Filter-KI auch in anderen, Nicht-Hochrisiko-Einsatzbereichen (zB zur Dokumentenverwaltung) eingesetzt werden soll. In diesem Fall ist das KI-System insgesamt betrachtet, dh auch in einem „harmlosen" Einsatzbereich, ein Hochrisiko-KI-System. In diesem Zusammenhang gilt die Faustregel: „Einmal Hochrisiko, alles Hochrisiko".

Aufgrund der komplexen Regelungen für die Risikoklassifizierung werden mit großem Interesse die Leitlinien der Kommission zur praktischen Umsetzung samt einer umfassenden Liste praktischer Beispiele erwartet. Es bleibt zu hoffen, dass diese Leitlinien die Rechtsanwendung erleichtern werden, wenngleich diese nicht verbindliche Vorgaben, sondern lediglich Hilfestellungen bei der Risikoklassifizierung darstellen. Bis dahin sind Unternehmen angehalten, rechtzeitig Prozesse zu entwickeln und entsprechende Schulungen anzubieten, damit sie die ab 2. 8. 2026 in Kraft tretenden Pflichten für Hochrisiko-KI-Systeme einhalten können.

37 Eine Ausnahme besteht lediglich, soweit ein KI-System nachträglich und zweckentfremdet als Hochrisiko-KI-System eingesetzt wird; vgl weiterführend Abschnitt 2.1.

38 *Borges*, CR 2024, 565 (Rz 40 f).

39 *Eisenberger* in *Martini/Wendehorst*, KI-VO Art 26 Rz 2.

40 So unser Verständnis aus der Literatur, Entscheidungen gibt es dazu noch keine.

Die Autorin:

Mag. **Alina Alavi Kia** ist Rechtsanwältin bei CERHA HEMPEL und schwerpunktmäßig im Immaterialgüter-, Lauterkeits-, Medien- und Lebensmittelrecht tätig. Zudem beschäftigt sie sich mit Rechtsfragen im Bereich der künstlichen Intelligenz. Sie ist Autorin diverser Fachpublikationen, Vortragende bei Konferenzen und Lektorin an der FH Wien.

lesen.lexisnexis.at/autor/Alavi Kia/Alina

Foto: CERHA HEMPEL/Stefan Reichmann

Die Autorin:

MMag. **Stephanie Maier-Herbeck** ist Rechtsanwältin bei CERHA HEMPEL und schwerpunktmäßig im Bereich des Datenschutzrechts tätig. Sie beschäftigt sich aber auch mit Rechtsfragen die sich im Bereich des KI-Rechts stellen.

lesen.lexisnexis.at/autor/Maier-Herbeck/Stephanie

Foto: CERHA HEMPEL/Stefan Reichmann