Bundesministerium
Inneres

Sicherheitsakademie

SIAK-Journal – Zeitschrift für Polizeiwissenschaft und polizeiliche Praxis

Wendehorst, Christiane

Die neue KI-Verordnung der EU. Konsequenzen im Zuständigkeitsbereich des Bundesministeriums für Inneres

SIAK-Journal − Zeitschrift für Polizeiwissenschaft und polizeiliche Praxis (4/2024), 30-42.

doi: 10.7396/2024_4_C

Um auf diesen Artikel als Quelle zu verweisen, verwenden Sie bitte folgende Angaben:

Wendehorst, Christiane (2024). Die neue KI-Verordnung der EU. Konsequenzen im Zuständigkeitsbereich des Bundesministeriums für Inneres, SIAK-Journal − Zeitschrift für Polizeiwissenschaft und polizeiliche Praxis (4), 30-42, Online: https://dx.doi.org/10.7396/2024_4_C.

Online publiziert: 3/2025

Die neue KI-Verordnung der EU

Konsequenzen im Zuständigkeitsbereich des Bundesministeriums für Inneres

CHRISTIANE WENDEHORST,
Universitätsprofessorin für Zivilrecht und stv. Vorständin des Instituts für Innovation und Digitalisierung im Recht an der Universität Wien.

Die neue EU-Verordnung über künstliche Intelligenz (KI) soll sicherstellen, dass die Bürger ebenso wie Behörden und Unternehmen in diese Zukunftstechnologie Vertrauen haben dürfen. Sie bringt eine Reihe neuer Pflichten mit sich für Akteure, die KI-Systeme entwickeln und anbieten oder sonst in die Vertriebskette eingebunden sind, aber auch für Betreiber von KI-Systemen. Behörden, die sich fortgeschrittener IT-Lösungen für die Erfüllung ihrer Aufgaben bedienen, müssen daher künftig prüfen, ob diese IT-Lösungen als KI-Systeme zu qualifizieren sind und, wenn ja, ob sie zu den teilweise verbotenen oder den Hochrisiko-KI-Systemen zählen und ob besondere Transparenzpflichten gelten. Behörden im Zuständigkeitsbereich des Bundesministeriums für Inneres (BMI) sind, wenn sie KI-Systeme für sensible Aufgaben nutzen – etwa in den Bereichen Polizei und Sicherheit, Asyl und Migration oder Schutz Kritischer Infrastruktur – sehr häufig von den besonderen Anforderungen erfasst. Da die ersten Bestimmungen schon ab 2. Februar 2025 anwendbar sein werden, sind Behörden gut beraten, sich frühzeitig auf die neuen Anforderungen einzustellen.

1. EINFÜHRUNG

Mit Ablauf des 1. August 2024 ist die lange erwartete Verordnung über künstliche Intelligenz (KI-VO) der EU in Kraft getreten.[1] Damit wurde einstweilen ein Schlussstrich unter ein Gesetzgebungsverfahren gesetzt, das etwas mehr als drei Jahre gedauert hat, aber schon seit etwa 2018 vorbereitet worden war.[2] Erste Vorschriften – genauer gesagt die Kapitel I und II – werden schon ab 2. Februar 2025 anwendbar sein, der Rest wird gestaffelt bis spätestens August 2027 anwendbar werden.[3] Ziel der Verordnung ist es ausweislich ihres einleitenden Artikels, das Funktionieren des Binnenmarktes zu verbessern und die Einführung einer menschenzentrierten und vertrauenswürdigen KI zu fördern. Es soll ein hohes Schutzniveau in Bezug auf Gesundheit, Sicherheit und Grundrechte gewährleistet werden, das insbesondere auch Demokratie, Rechtsstaatlichkeit und Umweltschutz in den Blick nimmt.[4] Die KI-Verordnung strebt an, den Balanceakt zwischen einem Schutz vor allfälligen schädlichen Auswirkungen von KI-Systemen und der Förderung von Innovation in der EU zu schaffen. Sie hat auch massive Auswirkungen auf den Zuständigkeitsbereich des BMI.

2. DIE KI-VO ALS RISIKOBASIERTES PRODUKTSICHERHEITSRECHT

Während die KI-VO im Vorfeld eine ähnliche Aufmerksamkeit auf sich gezogen

hat wie die Datenschutzgrundverordnung (DSGVO) und mit dieser (sowie im Bereich der Strafverfolgung dem auf der Richtlinie 2016/680 beruhenden 3. Hauptstück des Datenschutzgesetztes (DSG)) funktionell eng verzahnt ist, unterscheidet sie sich von der DSGVO ganz wesentlich im Regulierungsmodell. Prägend ist dabei der Charakter als Produktsicherheitsrecht und – damit eng verknüpft – der risikobasierte Ansatz.

2.1 Allgemeine Merkmale von Produktsicherheitsrecht

Die neue KI-VO stellt sich strukturell als klassisches Produktsicherheitsrecht dar, wie es für eine breite Palette von Produkten – von Maschinen über Medizinprodukte bis hin zu Kinderspielzeug – seit Jahrzehnten existiert und sowohl in produktspezifischen Rechtsakten[5] als auch, als Auffangregelung, in der Allgemeinen Produktsicherheits-VO niedergelegt ist.

Zu den Merkmalen klassischen Produktsicherheitsrechts[6] gehört die Formulierung wesentlicher Anforderungen an die Sicherheit, die jedes erfasste Produkt erfüllen muss und für deren Einhaltung primär der Hersteller verantwortlich ist. Die Konformität eines Produkts mit den wesentlichen Anforderungen (ausgewiesen durch das CE-Kennzeichen) wird entweder vom Hersteller selbst bewertet oder aber von Dritten, meist sogenannten notifizierten Stellen, die ihrerseits von sogenannten notifizierenden Behörden überwacht werden. Vom Produktsicherheitsrecht und der damit eng verzahnten Marktüberwachungs-VO[7] werden aber auch andere Akteure in der Vertriebskette in die Pflicht genommen, etwa Händler und – bei Herstellern in Drittstaaten – Bevollmächtigte in der Union sowie Importeure. Überwacht wird die Einhaltung des gesamten Systems von Marktüberwachungsbehörden.

Zentrales Merkmal des Produktsicherheitsrechts des sogenannten „neuen Rechtsrahmens“[8] ist es ferner, dass nicht alle Einzelheiten auf gesetzlicher Ebene selbst festgelegt sind, sondern auch in untergesetzlichen Rechtsvorschriften (entweder delegierten Rechtsakten oder Durchführungsrechtsakten) oder in sogenannten „harmonisierten Normen“, dh von privaten Akteuren formulierten Standards, die auf der Grundlage eines Auftrags der Europäischen Kommission entwickelt und von dieser später angenommen und im Amtsblatt veröffentlicht wurden.

Schließlich gehört auch der sogenannte „risikobasierte Ansatz“ zu den Grundmerkmalen des Produktsicherheitsrechts, dh die Anforderungen an die Produktsicherheit sowie die konkrete Ausgestaltung des Konformitätsbewertungsverfahrens hängen ganz wesentlich von dem abstrakten Risiko ab, das ein Produkt darstellt. Nicht unüblich ist es, explizit Kataloge von „Hochrisiko-Produkten“ zu spezifizieren (zB bei Maschinen[9]) oder aber von Vornherein alle erfassten Produkte in Risikoklassen einzuordnen (zB bei Medizinprodukten[10]).

2.2 Besonderheiten der KI-VO im Vergleich zu anderem Produktsicherheitsrecht

Auch die neue KI-VO folgt diesem, nunmehr seit Jahrzehnten bekannten und bewährten, Ansatz. Dabei haben die Eigenheiten von KI bzw der politische Prozess allerdings einige Adaptierungen erforderlich gemacht.

2.2.1 Erweiterung des Risikobegriffs auf Grundrechtsrisiken

Zunächst einmal sind die Gefahren, die von KI-Systemen ausgehen, teilweise anders strukturiert als die Gefahren durch Maschinen, Medizinprodukte oder Kinderspielzeug.[11] Während es bei derartigen

traditionellen Produkten ganz zentral um die Gesundheit und körperliche Unversehrtheit von Menschen geht, geht es bei KI-Systemen mindestens auch – wenn nicht sogar in erster Linie – um Risiken wie Diskriminierung, Totalüberwachung oder Manipulation von Menschen, oder gar um Risiken für die ganze Gesellschaft, wie etwa für Demokratie oder Rechtsstaatlichkeit. Die KI-VO hat daher einen stark erweiterten Risikobegriff gewählt, der neben klassischen Sicherheitsrisiken eben auch diese KI-spezifischen Risiken erfasst und sie einheitlich als Risiken für die Grundrechte (Grundrechtsrisiken) qualifiziert. Dies ist in dieser Form im Produktsicherheitsrecht bislang einzigartig. Damit geht auch einher, dass manche Vorgaben an KI-Systeme und deren Nutzung (zB absolute Verbote mancher KI-Anwendungen oder bestimmte Transparenzanforderungen) keine Entsprechung im übrigen Produktsicherheitsrecht haben.

2.2.2 Regulierung auch der Betreiber

Sodann nimmt die KI-VO nicht nur die klassischen Akteure in die Pflicht, also die Hersteller (von der KI-VO „Anbieter" genannt) und weitere Akteure in der Vertriebskette, sondern auch die Betreiber von KI-Systemen, sofern diese das KI-System nicht nur in einer privaten und nicht beruflichen Funktion nutzen. Auch dies ist in dieser Form im Produktsicherheitsrecht einzigartig, weil bislang die Nutzer nur als geschützter, aber nicht als verpflichteter Personenkreis in Erscheinung getreten sind. Damit müssen auch alle (professionellen) Nutzer von KI – einschließlich aller öffentlichen Stellen – künftig aufmerksam mitverfolgen, ob und welche Pflichten sich für sie gegebenenfalls aus der KI-VO ergeben. Die wichtigsten dieser Pflichten sind in Art 4 und 5, in Art 26 und 27, in Art 50 sowie in Art 86 KI-VO niedergelegt.

2.2.3 Mitdenken von Innovationsförderung

Keine Entsprechung im übrigen Produktsicherheitsrecht findet auch Kapitel VI mit diversen Maßnahmen zur Innovationsförderung, insbesondere zu sogenannten „KI-Reallaboren" (besser bekannt unter dem Begriff „regulatory sandboxes") und Tests von KI-Systemen unter realen Bedingungen.

2.2.4 Verhältnis zu Individualrechten

Schließlich hat sich im Laufe der Verhandlungen ein dem Produktsicherheitsrecht eigentlich fremdes Element eingeschlichen, nämlich – wenn auch sehr begrenzt – Individualrechte, wie etwa ein Recht auf Beschwerde bei einer Marktüberwachungsbehörde oder unter bestimmten Umständen ein Recht auf Erläuterung der Entscheidungsfindung im Einzelfall.[12]

Dazu, auch Anspruchsgrundlagen für eine Haftung auf Schadenersatz aufzunehmen, ist es allerdings nicht mehr gekommen. Stattdessen soll die Haftung auf Schadenersatz einerseits aus dem allgemeinen Produkthaftungsrecht folgen, das durch eine neue und an die Herausforderungen der Digitalisierung angepasste Produkthaftungs-RL[13] harmonisiert werden wird, und andererseits aus dem nationalen Recht der Verschuldenshaftung, das möglicherweise noch durch eine eigene KI-Haftungs-RL[14] modifiziert werden könnte.

2.3 Der risikobasierte Ansatz der KI-VO

Das wohl bekannteste Merkmal der neuen KI-VO ist ihr risikobasierter Ansatz, der – wie bereits erläutert – eigentlich ein ganz typischer Bestandteil moderner Produktsicherheitsgesetzgebung ist. Im Kern geht es um eine Abstufung der Regulierungsintensität (Strenge der Sicherheitsanforderungen, Verfahren der Konformitätsbewertung usw) nach der Höhe der abstrakten

Risiken, die durch ein KI-System und seine Anwendung geschaffen werden.

2.3.1 Die Stufen der „Risikopyramide“

Dabei kennt die KI-VO eine „Risikopyramide“[15] mit grundsätzlich sechs Stufen. Gleichsam die Spitze der Pyramide bilden die verbotenen KI-Anwendungen gemäß Kapitel II, deren Risiken so bedenklich erschienen, dass sie ganz untersagt werden mussten. Es folgen besonders geregelte Risikostufen erlaubter KI-Anwendungen: die Hochrisiko-KI-Systeme gemäß Kapitel III, die KI-Systeme mit besonderen Transparenzanforderungen gemäß Kapitel IV (etwa Deepfakes, biometrische Kategorisierung oder Emotionserkennung), die ein systemisches Risiko bildenden KI-Modelle mit allgemeinem Verwendungszweck (etwa sehr große Sprachmodelle wie GPT4) und die übrigen KI-Modelle mit allgemeinem Verwendungszweck (Kapitel V). Wichtig zu betonen ist, dass sich diese Risikostufen nicht wechselseitig ausschließen, dh ein KI-System kann beispielsweise ein Hochrisiko-KI-System sein und zugleich besonderen Transparenzanforderungen unterliegen. Gleichsam den breiten Sockel der Pyramide bilden diejenigen – zahlenmäßig allermeisten – KI-Systeme, die keiner besonders geregelten Risikostufe angehören. Für sie gibt es so gut wie keine bindenden Vorgaben in der KI-VO.

2.3.2 Hochrisiko-KI-Anwendungen

Die wichtigste Risikostufe, der die mit Abstand meisten Regelungen der KI-VO gewidmet sind, stellen die Hochrisiko-KI-Systeme dar. Für sie gelten besondere Anforderungen, die gerade dafür sorgen sollen, dass KI-Systeme in Europa vertrauenswürdig sind. Diese Anforderungen reichen von der Einrichtung eines Risikomanagement-Systems über Daten und Daten-Governance, technische Dokumentation und Aufzeichnungspflichten, Informations- und Instruktionspflichten, menschliche Aufsicht und Überwachung bis hin zu Treffsicherheit, Robustheit und Cybersicherheit. Dabei gibt es grundsätzlich zwei Möglichkeiten, wie ein KI-System als ein Hochrisiko-KI-System klassifiziert werden kann.

Die eine Möglichkeit (Art 6 Abs 1) hängt eng zusammen mit der oben dargestellten Struktur des Produktsicherheitsrechts. Wenn ein (anderes) reguliertes Produkt, das ein KI-System ist oder ein KI-System als Sicherheitsbauteil verwendet, unter (anderem) Produktsicherheitsrecht einer Konformitätsbewertung durch Dritte unterliegt, ist das betreffende KI-System automatisch auch ein Hochrisiko-KI-System im Sinne der KI-VO. Dies betrifft also beispielsweise KI-Systeme, die Medizinprodukte sind oder die – im Bereich der Robotik – in Maschinen integriert sind. Die besonderen Anforderungen der KI-VO an Hochrisiko-KI-Systeme werden in diesen Fällen grundsätzlich im Rahmen des Konformitätsbewertungsverfahrens mitgeprüft, das nach (anderem) Produktsicherheitsrecht ohnehin vorgesehen ist. Für die betreffenden Regelungen gilt eine besonders lange Übergangsfrist, und sie sind erst mit 2. August 2027 anwendbar.[16]

Unabhängig davon ist ein KI-System gemäß Art 6 Abs 2 als Hochrisiko-KI-System einzuordnen, wenn es in Anhang III der KI-VO aufgezählt ist. Anhang III kennt zunächst acht Bereiche bzw Anwendungsgruppen, die vom europäischen Gesetzgeber vorgegeben sind und innerhalb derer gewisse KI-Systeme bzw KI-Anwendungen als Hochrisiko-Anwendungen ausgewiesen werden können. Bei Erlass der KI-VO wurden den einzelnen Bereichen jeweils ein bis fünf konkret beschriebene Anwendungen zugeordnet. Ein Beispiel für eine Anwendung im Bereich „Rechts-

pflege und demokratische Prozesse“ wäre: „KI-Systeme, die bestimmungsgemäß von einer oder im Namen einer Justizbehörde verwendet werden sollen, um eine Justizbehörde bei der Ermittlung und Auslegung von Sachverhalten und Rechtsvorschriften und bei der Anwendung des Rechts auf konkrete Sachverhalte zu unterstützen, oder die auf ähnliche Weise für die alternative Streitbeilegung genutzt werden sollen.“ Anders als die acht Bereiche selbst können die konkret erfassten Anwendungen von der Kommission im Wege delegierter Rechtsakte geändert werden, dh es können unter bestimmten Bedingungen neue KI-Anwendungen hinzugefügt oder bestehende gestrichen werden.[17]

Die Tatsache alleine, dass eine Anwendung in Anhang III einzuordnen ist, heißt allerdings noch nicht zwingend, dass das betreffende KI-System auch ein Hochrisiko-KI-System ist. Ausnahmsweise gilt nämlich nach Art 6 Abs 3 ein in Anhang III genanntes KI-System nicht als hochriskant, wenn es kein erhebliches Risiko der Beeinträchtigung in Bezug auf die Gesundheit, Sicherheit oder Grundrechte natürlicher Personen birgt, insbesondere indem es nicht das Ergebnis der Entscheidungsfindung wesentlich beeinflusst. In Bezug auf die oben als Beispiel genannte Anwendung für Justizbehörden könnte dies etwa KI-Systeme für die allgemeine Recherche in einer Rechtsdatenbank betreffen, weil es sich dabei um eine bloß vorbereitende Aufgabe handelt, die relativ weit vom Treffen der eigentlichen rechtlichen Entscheidung entfernt ist.

Grundsätzlich muss jeder Anbieter selbst beurteilen, ob das von ihm angebotene KI-System ein Hochrisiko-KI-System darstellt. Ein Anbieter, der zur Auffassung gelangt, dass sein in Anhang III aufgeführtes KI-System konkret nicht hochriskant ist, muss seine Bewertung dokumentieren und das KI-System entsprechend registrieren. Die Kommission wird bis spätestens Februar 2026 Leitlinien zur praktischen Umsetzung bereitstellen.[18]

3. BEDEUTUNG FÜR DEN ZUSTÄNDIGKEITSBEREICH DES BMI

Der Zuständigkeitsbereich des österreichischen BMI und seiner nachgeordneten Behörden ist von der neuen KI-VO in fast allen Aspekten potenziell massiv betroffen. Dabei gilt für Behörden, die fortgeschrittene IT-Lösungen anwenden wollen, folgende grobe Checkliste:

(1) Liegt die konkrete IT-Lösung im Anwendungsbereich der KI-VO, dh liegt die geplante Tätigkeit im Anwendungsbereich der KI-VO und liegt ein KI-System vor?

(2) Unterliegt der geplante Einsatz des KI-Systems möglicherweise einem vollständigen oder partiellen Verbot nach der KI-VO, insbesondere im Bereich biometrischer Technologien?

(3) Ist der geplante Einsatz als Anwendung eines Hochrisiko-KI-Systems zu qualifizieren, und welche allgemeinen oder besonderen Betreiberpflichten gelten?

(4) Unterliegt der geplante Einsatz besonderen Transparenzpflichten?

3.1 Anwendungsbereich der KI-VO

Dabei gilt es allerdings zunächst zu prüfen, ob eine Tätigkeit generell in den Anwendungsbereich der KI-VO fällt. Gemäß Art 2 Abs 3 gilt die KI-VO nämlich nur in den unter das Unionsrecht fallenden Bereichen und berührt keinesfalls die Zuständigkeiten der Mitgliedstaaten in Bezug auf die nationale Sicherheit.

3.1.1 Abgrenzung zu außerhalb des Unionsrechts fallenden Bereichen

Die Einschränkung auf unter das Unionsrecht fallende Bereiche schließt zunächst Bereiche aus, die eng mit der nationalen Souveränität der Mitgliedstaaten[19] verbunden sind. Zur ähnlich lautenden Be-

schränkung in Art 2 Abs 2 DSGVO liegt mittlerweile eine gefestigte Judikatur des Europäischen Gerichtshofs (EuGH) vor. Danach sind Ausnahmen vom Anwendungsbereich der DSGVO eng auszulegen.[20] Verneint wurde eine Ausnahme beispielsweise für den Bereich des Straßenverkehrs,[21] für die Durchführung von Wahlen[22] und sogar für einen vom Parlament eines Mitgliedstaats in Ausübung seines Kontrollrechts eingesetzten Untersuchungsausschuss, und zwar selbst für den Fall, dass dieser sich auf Tätigkeiten einer polizeilichen Staatsschutzbehörde bezieht.[23]

Für die Ausnahme bleibt letztlich nur die nationale Sicherheit einschließlich Tätigkeiten im Rahmen der Gemeinsamen Außen- und Sicherheitspolitik der Union[24] übrig. Der Bereich der nationalen Sicherheit umfasst Tätigkeiten der Inlands- und Auslandsgeheimdienste sowie Tätigkeiten zur Gewährleistung der Sicherheit des Staates.[25] Es geht im Kern um die Zuständigkeit der Mitgliedstaaten für die Abwehr äußerer Angriffe und innerer Attacken auf die staatliche Ordnung.[26] Letzteres umfasst insbesondere Verhütung und Repression von terroristischen Aktivitäten.[27] Nicht vom Begriff der nationalen Sicherheit erfasst ist jedenfalls der Bereich der Strafverfolgung, einschließlich der Bekämpfung auch schwerer Kriminalität, der eher unter den Begriff der „öffentlichen Sicherheit" zu fassen ist und vollständig in den Anwendungsbereich der KI-VO fällt.[28] Das Gleiche gilt für die Bereiche Migration, Asylwesen und Grenzkontrollmanagement.[29]

Der Tätigkeitsbereich des BMI (anders als derjenige des Bundesministeriums für Landesverteidigung) liegt damit ganz überwiegend im Anwendungsbereich der KI-VO, wobei sich beispielsweise im Bereich der Terrorbekämpfung oder der zivil-militärischen Zusammenarbeit aber auch gewisse Grauzonen ergeben.

3.1.2 Unsicherheitsfaktor: Begriff des KI-Systems

Noch nicht abschließend geklärt ist freilich, welche IT-Lösungen überhaupt die Definition eines „KI-Systems" erfüllen. Dieses ist in Art 3 Nr 1 definiert als „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". An dieser – an die überarbeitete Definition der Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD) von November 2023[30] angepassten – Begriffsbestimmung ist fast alles unklar.[31] In anderem Zusammenhang hat die Verfasserin gemeinsam mit KI-Experten einen „Drei-Faktor-Ansatz" entwickelt, der ansetzt an (1) der Rolle von Daten oder Erfahrungswissen beim Zustandekommen und Pflegen des Systems, (2) dem Maß an zielorientierter Optimierung oder Suche im Zeitpunkt der Anwendung und (3) dem Ermessensspielraum aufgrund der mangelnden formalen Bestimmtheit der Aufgabe im Einsatz.[32] Der Europäischen Kommission kommt bei der Verfassung von Leitlinien, wie der Begriff des KI-Systems auszufüllen ist, größtmögliche Freiheit zu. Diese Leitlinien werden bis Anfang 2025 erwartet, und erst aus ihnen wird sich letztlich ergeben, welche IT-Anwendungen von der KI-VO erfasst sind und welche nicht. Derzeit kann man davon ausgehen, dass solche Anwendungen erfasst sind, die auf Methoden maschinellen Lernens beruhen, ebenso wie logik- oder wissensgestützte Systeme.

3.2 Verbotene KI-Anwendungen

In Art 5 der KI-VO ist eine Reihe von

KI-Anwendungen bzw KI-Praktiken aufgrund ihrer unvertretbar hohen Risiken für die Grundrechte verboten worden. Dabei werden in Art 5 Abs 1 lit a bis g zunächst bestimmte KI-Praktiken als solche verboten („Per-se-Verbote"). Eine Sonderstellung nehmen die Regelungen in Art 5 Abs 1 lit h mit Abs 2 bis 7 ein, die sämtlich der biometrischen Echtzeit-Fernidentifizierungssysteme in öffentlich zugänglichen Räumen zu Strafverfolgungszwecken gewidmet sind und die eigentlich eher materielle und prozedurale Bedingungen für einen solchen Einsatz festschreiben. Die Verbote sind bereits ab 2. Februar 2025 anwendbar.

3.2.1 Per-se-Verbote

Per se verboten ist beispielsweise die KI-gestützte Bewertung oder Vorhersage des Risikos, dass eine natürliche Person eine Straftat begehen wird, soweit diese ausschließlich auf der Grundlage des Profiling einer natürlichen Person oder der Bewertung ihrer persönlichen Merkmale und Eigenschaften erfolgt.[33] Erlaubt ist allerdings die bloße Unterstützung einer von Menschen vorgenommenen Bewertung, ob eine Person an einer kriminellen Aktivität beteiligt war, wenn sich die Bewertung bereits auf objektive und überprüfbare Tatsachen stützt, die in unmittelbarem Zusammenhang mit einer kriminellen Aktivität stehen.

Gleichfalls verboten ist die individuelle biometrische Kategorisierung natürlicher Personen, um ihre Rasse, ihre politischen Einstellungen, ihre Gewerkschaftszugehörigkeit, ihre religiösen oder weltanschaulichen Überzeugungen, ihr Sexualleben oder ihre sexuelle Ausrichtung zu erschließen oder abzuleiten. Erlaubt ist allerdings die Kennzeichnung oder Filterung rechtmäßig erworbener biometrischer Datensätze (zB Fotos) auf der Grundlage biometrischer Daten oder die Kategorisierung biometrischer Daten im Bereich der Strafverfolgung.[34]

Ein weiteres Beispiel für eine per-se-verbotene Anwendung wäre die Erstellung oder Erweiterung von Datenbanken zur Gesichtserkennung durch das ungezielte Auslesen von Gesichtsbildern aus dem Internet oder von Überwachungsaufnahmen.

3.2.2 Sonderfall: biometrische Echtzeit-Fernidentifikation zu Strafverfolgungszwecken

Wie bereits erwähnt, hat die Verwendung biometrischer Echtzeit-Fernidentifizierungssysteme in öffentlich zugänglichen Räumen zu Strafverfolgungszwecken eine Sonderregelung erfahren. Zunächst einmal ist eine solche Verwendung materiell nur zulässig, wenn sie für einen von drei erlaubten Zwecken unbedingt erforderlich ist. Dies ist (1) die gezielte Suche nach bestimmten Opfern von Entführung, Menschenhandel oder sexueller Ausbeutung sowie die Suche nach vermissten Personen, (2) das Abwenden einer konkreten, erheblichen und unmittelbaren Gefahr für das Leben oder die körperliche Unversehrtheit natürlicher Personen oder einer tatsächlichen und bestehenden oder tatsächlichen und vorhersehbaren Gefahr eines Terroranschlags, sowie (3) das Aufspüren oder Identifizieren einer Person, die der Begehung einer Straftat verdächtigt wird, zum Zwecke der Durchführung von strafrechtlichen Ermittlungen oder von Strafverfahren oder der Vollstreckung einer Strafe. Dabei muss die Straftat in Anhang II zur KI-VO aufgeführt und in Österreich im Höchstmaß mit einer freiheitsentziehenden Maßnahme von mindestens vier Jahren bedroht sein.

Auch wenn ein erlaubter Zweck vorliegt, muss eine strenge Verhältnismäßigkeitsprüfung erfolgen, ist die Maßnahme auf das geografisch und persönlich unbedingt erforderliche Maß zu beschränken und sind Schutzvorkehrungen gegen übermäßige Grundrechtseingriffe zu ergreifen. Insbesondere hat vor einem Einsatz – sofern

kein Notfall vorliegt – eine Grundrechtsfolgenabschätzung gemäß Art 27 KI-VO zu erfolgen und muss das verwendete KI-System in einer EU-Datenbank registriert worden sein. Ferner bedarf es jeweils einer vorherigen Genehmigung durch eine vom österreichischen Gesetzgeber festzulegende Stelle, die eine Justizbehörde oder eine unabhängige Verwaltungsbehörde sein muss. Zusätzlich hat eine Mitteilung über die Verwendung an die zuständige Marktüberwachungsbehörde und die nationale Datenschutzbehörde zu erfolgen. Diese Behörden haben der Kommission entsprechende Jahresberichte vorzulegen.

Wichtig ist, zu betonen, dass sich österreichische Behörden für die biometrische Echtzeit-Fernidentifizierung zu Strafverfolgungszwecken grundsätzlich nicht unmittelbar auf die KI-VO stützen können. Vielmehr stellen deren Regelungen nur den äußersten Rahmen des Zulässigen dar und ist Österreich angehalten, in seinem nationalen Recht die erforderlichen detaillierten Vorschriften für die Beantragung, Erteilung und Ausübung der Genehmigungen sowie für die entsprechende Beaufsichtigung und Berichterstattung festzulegen.[35] In diesen Vorschriften muss auch genau festgelegt werden, im Hinblick auf welche der nach der KI-VO erlaubten Ziele und welche der nach der KI-VO an sich potenziell erfassten Straftaten die zuständigen Behörden ermächtigt werden können, KI-Systeme zu verwenden. Die Mitgliedstaaten teilen der Kommission diese Vorschriften spätestens 30 Tage nach ihrem Erlass mit. Österreich könnte dabei auch strengere Rechtsvorschriften für die Verwendung biometrischer Fernidentifizierungssysteme erlassen, als von der KI-VO an sich erlaubt wäre.

3.3 Hochrisiko-KI-Anwendungen

Es gehört zu den wichtigsten Fragen, die sich Anbieter und Betreiber von KI-Systemen künftig zu stellen haben, ob das von ihnen angebotene oder betriebene KI-System als Hochrisiko-KI-System einzuordnen ist. Nahezu alle der in Anhang III genannten acht Bereiche von Hochrisiko-KI-Systemen betreffen in irgendeiner Weise den Zuständigkeitsbereich des BMI oder können auch das BMI und seine nachgeordneten Behörden betreffen. Diese acht Bereiche sind: 1. Biometrie; 2. Kritische Infrastruktur; 3. Allgemeine und berufliche Bildung; 4. Beschäftigung, Personalmanagement und Zugang zur Selbstständigkeit; 5. Zugänglichkeit und Inanspruchnahme grundlegender privater und grundlegender öffentlicher Dienste und Leistungen; 6. Strafverfolgung; 7. Migration, Asyl und Grenzkontrolle; 8. Rechtspflege und demokratische Prozesse. Dabei wird im Folgenden nur der Fall beleuchtet, dass Behörden als Betreiber von KI-Systemen auftreten. Sollten sich Behörden entschließen, selbst KI-Systeme zu entwickeln bzw entwickeln zu lassen oder aber die Zweckbestimmung eines KI-Systems wesentlich zu ändern oder einem KI-Modell mit allgemeinem Verwendungszweck eine konkrete Zweckbestimmung hohen Risikos zu geben, können sie nach Art 25 KI-VO zusätzlich den Anbieterpflichten unterliegen.

3.3.1 Allgemeine Betreiberpflichten

Die Betreiber von Hochrisiko-KI-Systemen treffen eine ganze Reihe allgemeiner Pflichten nach der KI-VO. Dazu gehört das Treffen geeigneter technischer und organisatorischer Maßnahmen, um sicherzustellen, dass die Systeme entsprechend der Betriebsanleitung und nur durch Personal angewendet werden, das über die erforderliche Kompetenz, Ausbildung und Befugnis verfügt. Bei KI-Systemen, die noch im Betrieb weiterlernen (was bei Hochrisiko-KI-Systemen derzeit eher unüblich ist[36]), müssen sie auch dafür sorgen,

dass Eingabedaten angemessen und ausreichend repräsentativ sind. Betreiber von Hochrisiko-KI-Systemen müssen ferner die vom System automatisch erzeugten Protokolle für einen angemessenen Zeitraum von mindestens sechs Monaten aufbewahren, soweit diese Protokolle ihrer Kontrolle unterliegen.

Weitere allgemeine Pflichten können gegenüber Datenschutzbehörden und Arbeitnehmervertretern bestehen. Bei Entdeckung neuer Risiken oder schwerwiegenden Vorfällen müssen die Betreiber den Anbieter, weitere Glieder der Vertriebskette und die zuständigen Marktüberwachungsbehörden informieren. Strafverfolgungsbehörden dürfen (und müssen) dabei allerdings sensible operative Daten schützen.

3.3.2 Grundrechtsfolgenabschätzung

Ist der Betreiber eine Einrichtung des öffentlichen Rechts, eine private Einrichtung, die öffentliche Dienste erbringt, oder verwendet er das KI-System zur Prüfung der Kreditwürdigkeit natürlicher Personen oder zur Risikoeinschätzung bei Lebens- und Krankenversicherungen, muss er vor der Inbetriebnahme eines Hochrisiko-KI-Systems eine umfassende Grundrechtsfolgenabschätzung durchführen.[37] Diese tritt zu einer allfälligen Datenschutzfolgenabschätzung hinzu, kann sich mit dieser aber inhaltlich überschneiden.[38] Eine einmal durchgeführte Folgenabschätzung gilt dann auch für ähnliche Anwendungsfälle, doch muss bei wesentlichen Änderungen eine neue Folgenabschätzung erfolgen bzw ist die Folgenabschätzung zu aktualisieren. Die Ergebnisse sind der Marktüberwachungsbehörde mitzuteilen.

3.3.3 Informations- und Erläuterungspflichten

Wenn sie Entscheidungen treffen, die natürliche Personen betreffen, oder wenn sie bei solchen Entscheidungen Unterstützung leisten, haben Betreiber die natürlichen Personen über die Verwendung der Hochrisiko-KI-Systeme zu informieren. Im Bereich der Strafverfolgung bleibt es allerdings bei den bereits aus dem einschlägigen Datenschutzrecht (§§ 42 ff DSG) geltenden Informationspflichten.[39]

Die betroffenen Personen haben gemäß Art 86 KI-VO das Recht, vom Betreiber eine klare und aussagekräftige Erläuterung zur Rolle des KI-Systems im Entscheidungsprozess und zu den wichtigsten Elementen der getroffenen Entscheidung zu erhalten, wenn eine Entscheidung auf der Grundlage eines in Anhang III aufgeführten Hochrisiko-KI-Systems getroffen wurde, die rechtliche Auswirkungen für die betroffene Person hat oder sie in ähnlicher Weise erheblich beeinträchtigt. Überraschenderweise wurde an dieser Stelle kein ausdrücklicher Vorbehalt für den Bereich der Strafverfolgung gemacht, was möglicherweise ein Redaktionsversehen darstellt.

3.3.4 Nachträgliche biometrische Fernidentifizierung

Besondere Regelungen gelten auch hier für die biometrische Fernidentifizierung im Bereich der Strafverfolgung. Während die biometrische Fernidentifizierung in Echtzeit schon – eigentlich systemwidrig – im Kontext der verbotenen KI-Praktiken geregelt wurde, ist die nachträgliche biometrische Fernidentifizierung bei den Hochrisiko-KI-Systemen geregelt. Auch hier gilt die Pflicht, eine Genehmigung einzuholen, sofern das System nicht zur erstmaligen Identifizierung eines potenziellen Verdächtigen auf der Grundlage objektiver und nachprüfbarer Tatsachen, die in unmittelbarem Zusammenhang mit einer Straftat stehen, verwendet wird. Die Verwendung ist auf das für die Ermittlung einer bestimmten Straftat unbedingt erforderliche Maß zu beschränken.

In keinem Fall darf ein solches Hochrisiko-KI-System zur nachträglichen biometrischen Fernidentifizierung zu Strafverfolgungszwecken in nicht zielgerichteter Weise und ohne jeglichen Zusammenhang mit einer Straftat, einem Strafverfahren, einer tatsächlichen und bestehenden oder tatsächlichen und vorhersehbaren Gefahr einer Straftat oder der Suche nach einer bestimmten vermissten Person verwendet werden.

Es muss sichergestellt werden, dass die Strafverfolgungsbehörden keine ausschließlich auf der Grundlage der Ausgabe solcher Systeme zur nachträglichen biometrischen Fernidentifizierung beruhende Entscheidung, aus der sich eine nachteilige Rechtsfolge für eine Person ergibt, treffen.

Unabhängig vom Zweck oder Betreiber wird jede Verwendung solcher Hochrisiko-KI-Systeme in der einschlägigen Polizeiakte dokumentiert und der zuständigen Marktüberwachungsbehörde und der nationalen Datenschutzbehörde auf Anfrage zur Verfügung gestellt, ohne dabei sensible operative Daten offenzulegen. Die Betreiber legen den zuständigen Marktüberwachungsbehörden und den nationalen Datenschutzbehörden Jahresberichte über ihre Verwendung von Systemen zur nachträglichen biometrischen Fernidentifizierung vor. Auch hier können die Mitgliedstaaten strengere Rechtsvorschriften erlassen.

3.4 KI-Anwendungen mit speziellem Transparenzbedarf

Für eine Reihe besonderer KI-Systeme gelten auch besondere Transparenzvorschriften. Für den Zuständigkeitsbereich des BMI sind diese in unterschiedlichem Maße relevant. Wichtig ist, zu betonen, dass bei all diesen besonderen Transparenzpflichten eine Ausnahme im Bereich der Strafverfolgung gilt, sofern die Systeme gesetzlich für diese Zwecke zugelassen sind, rechtskonform verwendet werden und geeignete Schutzvorkehrungen für die Rechte und Freiheiten Dritter bestehen.

KI-Systeme, die für die direkte Interaktion mit natürlichen Personen bestimmt sind (zB ChatBots) müssen so konzipiert und entwickelt werden, dass die betreffenden natürlichen Personen wissen, dass sie mit einem KI-System interagieren. Anbieter generativer KI-Systeme (zB ChatGPT) müssen sicherstellen, dass die Ausgaben in einem maschinenlesbaren Format als künstlich erzeugt oder manipuliert gekennzeichnet sind, soweit die Systeme nicht nur eine unterstützende Funktion für die Standardbearbeitung ausführen (zB Rechtschreibprüfung) oder die vom Betreiber bereitgestellten Eingabedaten oder deren Semantik nicht wesentlich verändern (zB Übersetzung). Bei Deepfakes muss offengelegt werden, dass die Inhalte künstlich erzeugt oder manipuliert wurden.

Betreiber eines KI-Systems, das Text erzeugt oder manipuliert, der veröffentlicht wird, um die Öffentlichkeit über Angelegenheiten von öffentlichem Interesse zu informieren (zB Pressemeldungen), müssen offenlegen, dass der Text künstlich erzeugt oder manipuliert wurde. Eine Ausnahme gilt aber, wenn Inhalte einem Verfahren der menschlichen Überprüfung oder redaktionellen Kontrolle unterzogen wurden und wenn eine natürliche oder juristische Person die redaktionelle Verantwortung für die Veröffentlichung der Inhalte trägt.

Bei Betrieb von Emotionserkennungssystemen oder Systemen zur biometrischen Kategorisierung müssen die betroffenen natürlichen Personen über den Betrieb des Systems informiert werden.

4. ZUSAMMENFASSUNG

Die neue KI-VO ist ein Prestigeprojekt des europäischen Gesetzgebers, das schwierige Verhandlungen erforderlich gemacht hat. Alle Beteiligten haben teils große

Zugeständnisse gemacht, um das Projekt rechtzeitig vor den Europawahlen 2024 abzuschließen. Dabei hat es sicherlich geholfen, dass die Entscheidung für ein Regulierungsmodell gefallen ist, das aus dem Produktsicherheitsrecht schon lange bekannt war. Dieses Regulierungsmodell ist vor allem ein risikobasiertes, dh je höher die Risiken für die Gesundheit und Sicherheit oder die Grundrechte einschließlich Demokratie und Rechtsstaatlichkeit, desto intensiver auch die Regulierung. Damit soll vermieden werden, dass Innovation in diesem besonders dynamischen Feld technologischer Entwicklung stärker behindert wird, als es zum Schutz wichtiger Rechtsgüter unbedingt erforderlich ist.

Der Zuständigkeitsbereich des BMI ist von der neuen KI-VO massiv betroffen. Sowohl auf Ebene der sogenannten verbotenen KI-Praktiken als auch auf Ebene der Hochrisiko-KI-Systeme und der KI-Systeme mit besonderem Transparenzbedarf dürften extrem viele Anwendungen potenziell erfasst sein. Man wird gut beraten sein, sich frühzeitig auf die neuen Vorgaben einzustellen, zumal die ersten Vorschriften – einschließlich zur Echtzeit-Fernidentifizierung in öffentlichen Räumen zu Strafverfolgungszwecken – bereits ab 2. Februar 2025 anwendbar sind. An vielen Stellen ist der österreichische Gesetzgeber auf den Plan gerufen, entsprechende nationalen Regelungen zu schaffen. Bemerkenswert erscheint der große Spielraum, welcher der Europäischen Kommission bei der näheren Ausgestaltung zugestanden wird – dies betrifft bereits die zentrale Frage, welche IT-Systeme überhaupt als KI-Systeme qualifiziert werden können. Generell ist anzumerken, dass mit der KI-VO erst ein Rahmen geschaffen wurde, der in den nächsten Jahren durch untergesetzliche Rechtsakte, Leitlinien, harmonisierte Normen, Verhaltenskodizes udgl schrittweise ausgefüllt wird. So gesehen gilt es, die weiteren Entwicklungen aufmerksam zu beobachten.

[1] *VO (EU) 2024/1689 des Europäischen Parlaments und des Rates vom 13. Juni 2024 zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz und zur Änderung der Verordnungen (EG) Nr 300/2008, (EU) Nr 167/2013, (EU) Nr 168/2013, (EU) 2018/858, (EU) 2018/1139 und (EU) 2019/2144 sowie der Richtlinien 2014/90/EU, (EU) 2016/797 und (EU) 2020/1828 (Verordnung über künstliche Intelligenz), ABl L 2024/1689, 1.*

[2] *Wendehorst in Martini/Wendehorst, KI-VO Kommentar (im Erscheinen) Art 1 Rz 22 ff.*

[3] *Art 113 KI-VO.*

[4] *Wendehorst in Martini/Wendehorst, KI-VO Kommentar Art 1 Rz 39 ff.*

[5] *Vgl Anhang I zur KI-VO.*

[6] *Umfangreiche Darstellung in Bekanntmachung der Kommission – Leitfaden für die Umsetzung der Produktvorschriften der EU 2022 („Blue Guide"), ABl C 2022/247, 6.*

[7] *VO (EU) 2019/1020 des Europäischen Parlaments und des Rates vom 20. Juni 2019 über Marktüberwachung und die Konformität von Produkten sowie zur Änderung der Richtlinie 2004/42/EG und der Verordnungen (EG) Nr 765/2008 und (EU) Nr 305/2011, ABl L 2019/169, 1.*

[8] *Blue Guide ABl C 2022/247, 9 ff.*

[9] *VO (EU) 2023/1230 des Europäischen Parlaments und des Rates vom 14. Juni 2023 über Maschinen und zur Aufhebung der Richtlinie*

2006/42/EG des Europäischen Parlaments und des Rates und der Richtlinie 73/361/EWG des Rates, ABl L 2023/165, 1.

10 *VO (EU) 2017/745 des Europäischen Parlaments und des Rates vom 5. April 2017 über Medizinprodukte, zur Änderung der Richtlinie 2001/83/EG, der Verordnung (EG) Nr 178/2002 und der Verordnung (EG) Nr 1223/2009 und zur Aufhebung der Richtlinien 90/385/EWG und 93/42/EWG des Rates, ABl L 2017/117, 1.*

11 *Unterscheidung zwischen „physischen" und „sozialen" Risiken entwickelt in Schneider/Wendehorst, Response to the Public Consultation on the White Paper (2020) 6f und später als Unterscheidung zwischen „Sicherheitsrisiken" und „Grundrechtsrisiken" im Vorschlag für eine KI-VO übernommen.*

12 *Wendehorst in Martini/Wendehorst, KI-VO Kommentar Art 1 Rz 61.*

13 *Unterzeichnete Fassung der Einigung zwischen Rat und Parlament am 23.10.2024, PE 7 2024 REV 1, 2022/0302(COD) für eine ausführlichere Behandlung der neuen Produkthaftungs-RL siehe Wendehorst in Martini/Wendehorst, KI-VO Kommentar Art 1 Rz 95ff.*

14 *Vorschlag für eine Richtlinie des europäischen Parlaments und des Rates zur Anpassung der Vorschriften über außervertragliche zivilrechtliche Haftung an künstliche Intelligenz (Richtlinie über KI-Haftung), COM(2022) 496 final; für eine ausführlichere Behandlung des Kommissionsvorschlages siehe Wendehorst in Martini/Wendehorst, KI-VO Kommentar Art 1 Rz 109ff.*

15 *Datenethikkommission der Bundesregierung, Gutachten (2019) 177.*

16 *Art 113 lit c KI-VO.*

17 *Ruschemeier in Martini/Wendehorst, KI-VO Kommentar Art 7 Rz 39ff.*

18 *Ruschemeier in Martini/Wendehorst, KI-VO Kommentar Art 6 Rz 33, 97; Hartmann in Martini/Wendehorst, KI-VO Kommentar Art 96 Rz 4.*

19 *EuGH C-311/18, Facebook Ireland/Schrems II, ECLI:EU:C:2020:559, Rn 81.*

20 *Grundlegend EuGH C439/19, Latvijas Republikas Saeima, ECLI:EU:C:2021:504, Rn 61ff; bestätigt etwa durch EuGH C34/21, Hauptpersonalrat der Lehrerinnen und Lehrer, ECLI:EU:C:2023:270, Rn 33; EuGH C306/21, Koalitsia „Demokratichna Bulgaria/Obedinenie", ECLI:EU:C:2022:813, Rn 35; EuGH C180/21, Inspektor v Inspektorata kam Visshia sadeben savet, ECLI:EU:C:2022:967, Rn 79; EuGH C33/22, Österreichische Datenschutzbehörde, ECLI:EU:C:2024:46, Rn 37.*

21 *EuGH C439/19, Latvijas Republikas Saeima, ECLI EU:C:2021:504, Rn 66.*

22 *EuGH C306/21, Koalitsia „Demokratichna Bulgaria/Obedinenie", ECLI:EU:C:2022:813, Rn 41.*

23 *EuGH, C33/22, Österreichische Datenschutzbehörde, ECLI:EU:C:2024:46, Rn 37ff.*

24 *EuGH C34/21, Hauptpersonalrat der Lehrerinnen und Lehrer, ECLI:EU:C:2023:270, Rn 34; EuGH C306/21, Koalitsia „Demokratichna Bulgaria/Obedinenie", ECLI:EU:C:2022:813, Rn 36.*

25 *Zerdick in Ehmann/Selmayr, Datenschutz-Grundverordnung: DS-GVO[3] (2024) Art. 2 Rz 8; Papakonstantinou/De Hert in SPHD/Papakonstantinou/De Hert, GDPR (2023) Art 2 Rz 73ff; Stender-Vorwachs/von Ungern-Sternberg/Wolff in Wolff/Brink/von Ungern-Sternberg, BeckOK Datenschutzrecht[48] DS-GVO Art. 23 Rz 26 (Stand 01.11.2021, beck-online.de).*

26 *Geiger/Kirchmair in Geiger/Khan/Kotzur/Kirchmair, EUV/AEUV Kommentar[7] (2023) EUV Art 4 Rz 4.*

27 *EuGH C-817/19, Ligue des droits humains, ECLI:EU:C:2022:491, Rn 170; EuGH 21.06.2022 – C-817/19EuZW 2022, 706 (712); EuGH C-140/20, Commissioner of An Garda Síochána, ECLI:EU:C:2022:258, Rn 61; EuGH C-623/17, Privacy International, ECLI:EU:C:2020:790, Rn 74; EuGH C-511/18, 512/18 und 520/18, La Quadrature du Net, ECLI:EU:C:2020:791, Rn 135.*

28 *EuGH C-140/20, Commissioner of the Garda Síochána, ECLI:EU:C:2022:258 Rn 59, 63.*

29 *Nr 6, 7 Annex III KI-VO.*

30 *OECD, Explanatory memorandum on the updated OECD definition of an AI system, 2024.*

31 *Wendehorst in Martini/Wendehorst, KI-VO Kommentar Art 3 Rz 50 ff.*

[32] *Wendehorst/Nessler/Aufreiter/Aichinger, Der Begriff des KI-Systems unter der neuen KI-VO – der Drei-Faktor-Ansatz, MMR 2024, 605.*

[33] *Wendehorst in Martini/Wendehorst, KI-VO Kommentar Art 5 Rz 82ff.*

[34] *Wendehorst in Martini/Wendehorst, KI-VO Kommentar Art 5 Rz 119ff.*

[35] *Wendehorst in Martini/Wendehorst, KI-VO Kommentar Art 5 Rz 181f.*

[36] *Wendehorst/Nessler/Aufreiter/Aichinger, MMR 2024, 605 (608f.).*

[37] *Art 27 KI-VO; siehe hierzu ausführlich Eisenberger in Martini/Wendehorst, KI-VO Kommentar Art 27 Rz 1ff.*

[38] *Eisenberger in Martini/Wendehorst, KI-VO Kommentar Art 27 Rz 57f.*

[39] *Eisenberger in Martini/Wendehorst, KI-VO Kommentar Art 26 Rz 39ff.*