KI-Verordnung und Risikomanagement für Hochrisiko-Systeme

Dr. Thomas Kahler

Hochschule Darmstadt So/Se 2025

Was ist KI?

Definition Künstliche Intelligenz (Art. 3 Nr. 1 KI-VO)

„KI-System“ 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;

Definition Künstliche Intelligenz (Art. 3 Nr. 1 KI-VO)

- ...ein maschinengestütztes System,
- das für einen in unterschiedlichem Grade autonomen Betrieb ausgelegt ist
- und das nach seiner Betriebsaufnahme anpassungsfähig sein kann und

Definition Künstliche Intelligenz (Art. 3 Nr. 1 KI-VO)

- 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;

Definition Künstliche Intelligenz (Erwwg. 12)

Der Begriff „KI-System“ in dieser Verordnung sollte klar definiert und eng mit der Tätigkeit internationaler Organisationen abgestimmt werden, die sich mit KI befassen, um Rechtssicherheit, mehr internationale Konvergenz und hohe Akzeptanz sicherzustellen und gleichzeitig Flexibilität zu bieten, um den raschen technologischen Entwicklungen in diesem Bereich Rechnung zu tragen. Darüber hinaus sollte die Begriffsbestimmung auf den wesentlichen Merkmalen der KI beruhen, die sie von einfacheren herkömmlichen Softwaresystemen und Programmierungsansätzen abgrenzen, und sollte sich nicht auf Systeme beziehen, die auf ausschließlich von natürlichen Personen definierten Regeln für das automatische Ausführen von Operationen beruhen. Ein wesentliches Merkmal von KI-Systemen ist ihre Fähigkeit, abzuleiten. Diese Fähigkeit bezieht sich auf den Prozess der Erzeugung von Ausgaben, wie Vorhersagen, Inhalte, Empfehlungen oder Entscheidungen, die physische und digitale Umgebungen beeinflussen können, sowie auf die Fähigkeit von KI-Systemen, Modelle oder Algorithmen oder beides aus Eingaben oder Daten abzuleiten. Zu den Techniken, die während der Gestaltung eines KI-Systems das Ableiten ermöglichen, gehören Ansätze für maschinelles Lernen, wobei aus Daten gelernt wird, wie bestimmte Ziele erreicht werden können, sowie logik- und wissensgestützte Konzepte, wobei aus kodierten Informationen oder symbolischen Darstellungen der zu lösenden Aufgabe abgeleitet wird.

Definition Künstliche Intelligenz (Erwwg. 12)

Die Fähigkeit eines KI-Systems, abzuleiten,

geht über die einfache Datenverarbeitung hinaus, indem Lern-, Schlussfolgerungs- und Modellierungsprozesse ermöglicht werden. Die Bezeichnung „maschinenbasiert“ bezieht sich auf die Tatsache, dass KI-Systeme von Maschinen betrieben werden. Durch die Bezugnahme auf explizite oder implizite Ziele wird betont, dass KI-Systeme gemäß explizit festgelegten Zielen oder gemäß impliziten Zielen arbeiten können. Die Ziele des KI-Systems können sich — unter bestimmten Umständen — von der Zweckbestimmung des KI-Systems unterscheiden. Für die Zwecke dieser Verordnung sollten Umgebungen als Kontexte verstanden werden, in denen KI-Systeme betrieben werden, während die von einem KI-System erzeugten Ausgaben verschiedene Funktionen von KI-Systemen widerspiegeln, darunter Vorhersagen, Inhalte, Empfehlungen oder Entscheidungen. KI-Systeme sind mit verschiedenen Graden der Autonomie ausgestattet, was bedeutet, dass sie bis zu einem gewissen Grad unabhängig von menschlichem Zutun agieren und in der Lage sind, ohne menschliches Eingreifen zu arbeiten. Die Anpassungsfähigkeit, die ein KI-System nach Inbetriebnahme aufweisen könnte, bezieht sich auf seine Lernfähigkeit, durch sie es sich während seiner Verwendung verändern kann. KI-Systeme können eigenständig oder als Bestandteil eines Produkts verwendet werden, unabhängig davon, ob das System physisch in das Produkt integriert (eingebettet) ist oder der Funktion des Produkts dient, ohne darin integriert zu sein (nicht eingebettet).

Definition Künstliche Intelligenz (Erwwg. 12)

Welche Rolle spielen die Erwägungsgründe bei der Auslegung der KI-VO?

Was ist das Verhältnis zwischen Erwägungsgründe und KI-VO?

Zielsetzung der KI-Verordnung I

Zweck dieser Verordnung ist es,

*das Funktionieren des Binnenmarkts zu verbessern und

*die Einführung einer auf den Menschen ausgerichteten und vertrauenswürdigen künstlichen Intelligenz (KI) zu fördern, sowie

*die Innovation zu unterstützen.

Zielsetzung der KI-Verordnung II

Hohes Schutzniveau in Bezug auf

*Gesundheit, Sicherheit und

*die in der Charta verankerten Grundrechte, einschließlich

*Demokratie, Rechtsstaatlichkeit und Umweltschutz

zu gewährleisten und

vor schädlichen Auswirkungen zu schützen

Die Entstehung der KI-Verordnung

April 2021:	Vorschlag der Kommission
Dezember 2023:	Verabschiedung EU-Parlament und Rat
01. August 2024:	Inkrafttreten

Gestufte Geltung

1. Stufe:	02.Februar 2025 KI-Kompetenz Verbotene Praktiken
2. Stufe:	02. August 2025
Volle Geltung	02. August 2026
Geltung?	02. August 2027

KI - Verordnung statt Richtlinie

- EU-Verordnung
- Gilt unmittelbar, EU-weit
- Ohne Umsetzungsakt
- Z.B. DSGVO (DS-Richtlinie 95/46)

KI - Verordnung statt Richtlinie

- EU-Richtlinie
- Bedarf Umsetzung durch nationales Gesetz
- Z.B. DS-Richtlinie 95/46: Umsetzung BDSG

Anwendungsbereich

Herkömmliche Systematik:

- Sachlicher Anwendungsbereich
- Räumlicher Anwendungsbereich
- Persönlicher Anwendungsbereich

Anwendungsbereich

Marktortprinzip (Art. 2 Abs. 1 lit. a KI-VO)

Anbieter (vgl. Art. 3 Nr. 3 KI-VO)

* die in der EU KI-Systeme in Verkehr bringen oder in Betrieb nehmen oder
* KI-Modelle mit allgemeinem Verwendungszweck in EU in Verkehr bringen,
* unabhängig davon, ob diese Anbieter in Union oder in Drittland niedergelassen sind

Anwendungsbereich

Betreiber

von KI-Systemen (vgl. Art. 3 Nr. 4 KI-VO)

*die Sitz oder Aufenthalt in der EU haben

(Art. 2 Abs. 1 lit. b KI-VO)

Anwendungsbereich

Sonstige Akteure (vgl. Art. 3 Nr. 8 KI-VO)

*Einführer,

*Händler,

*Produkthersteller,

*Bevollmächtigte von Anbietern mit Sitz Nicht-EU

(Art. 2 Abs. 1 lit. d bis lit. f KI-VO)

Anwendungsbereich

Betroffene Personen (Def. Art. 3 Nr. 50 KI-VO)

*im Sinne von Art. 4 Nr. 1 DSGVO

(Art. 2 Abs. 2 lit. g KI-VO)

Anwendungsbereich

Ergebnisprinzip (Art. 2 Abs. 1 lit. c) KI-VO)

Die KI-VO gilt auch, sofern

- das von KI-System hervorgebrachte Ergebnis
- in der EU verwendet wird

(„Anbieter und Betreiber von KI-Systemen, die ihren Sitz in einem Drittland haben oder sich in einem Drittland befinden, *wenn die vom KI-System hervorgebrachte Ausgabe in der Union verwendet wird...*“)

Anwendungsbereich

Zuständigkeit der EU (Art. 2 Abs. 3 KI-VO)

- Prinzip der begrenzten Einzelermächtigung
- Z.B. keine Anwendung für Verteidigung und nat. Sicherheit

Anwendungsbereich

Privilegierung Wissenschaft (Art. 2 Abs. 6)

KI-VO gilt nicht,

- wenn KI-Systeme oder KI-Modelle, einschließlich ihrer Ausgabe
- zum alleinigen Zweck der wissenschaftlichen Forschung u. Entwicklung
- entwickelt und in Betrieb genommen wird

Anwendungsbereich

<u>Forschungs-, Test- und Entwicklungstätigkeiten</u> (Art. 2 Abs. 8)

KI-VO gilt nicht für Forschungs-, Test- und Entwicklungstätigkeiten zu KI-Systemen oder KI-Modellen,

*__bevor__ diese in Verkehr gebracht oder in Betrieb genommen werden.

*Rückausnahme: Tests unter Realbedingungen fallen nicht unter diesen Ausschluss.

Anwendungsbereich

Haushaltsprivileg (Art. 2 Abs. 10)

KI-VO gilt nicht für die

*Pflichten v. Betreibern, die natürliche Personen sind und

*KI-Systeme im Rahmen einer ausschließlich persönlichen und nicht beruflichen Tätigkeit verwenden

Anwendungsbereich

Privileg für Open Source (Art. 2 Abs. 12)

KI-VO gilt nicht für KI-Systeme,

*die unter freien und quelloffenen Lizenzen bereitgestellt werden,
*es sei sie werden als

**Hochrisiko-KI-Systeme oder als
**KI-System, das unter Artikel 5 oder 50 fällt,

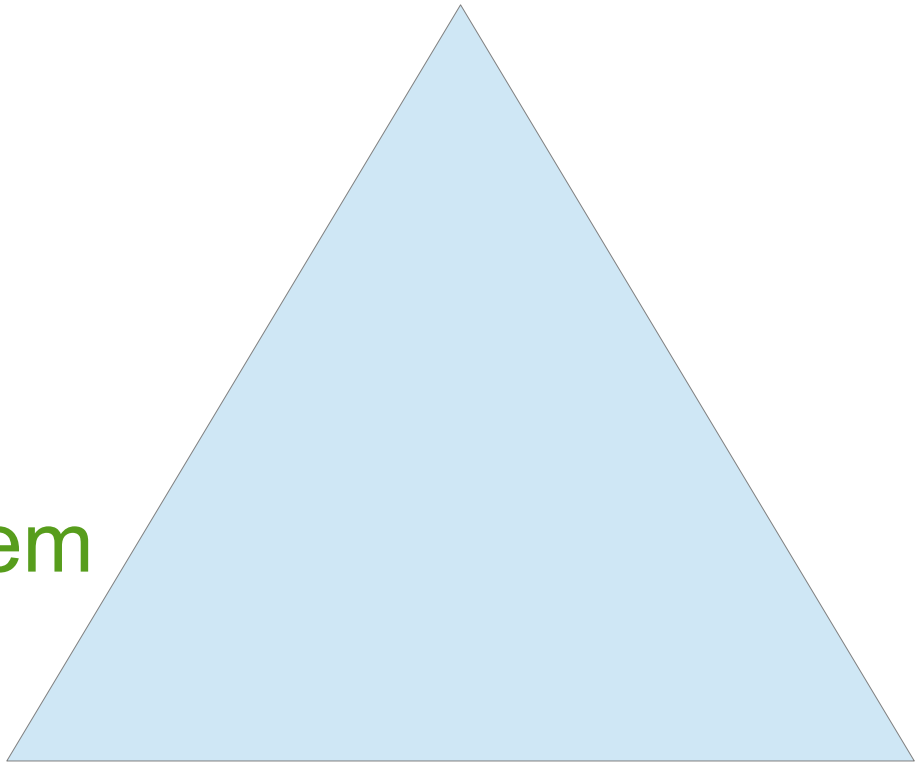
in Verkehr gebracht oder in Betrieb genommen.

Risikobezogener Ansatz

Verbotene Praktiken

Hochrisiko-KI-Systeme

KI-Systeme mit allgemeinem Anwendungszweck



Risikobezogener Ansatz

Definition Risiko (Art. 3 Nr.2)

Kombination aus der

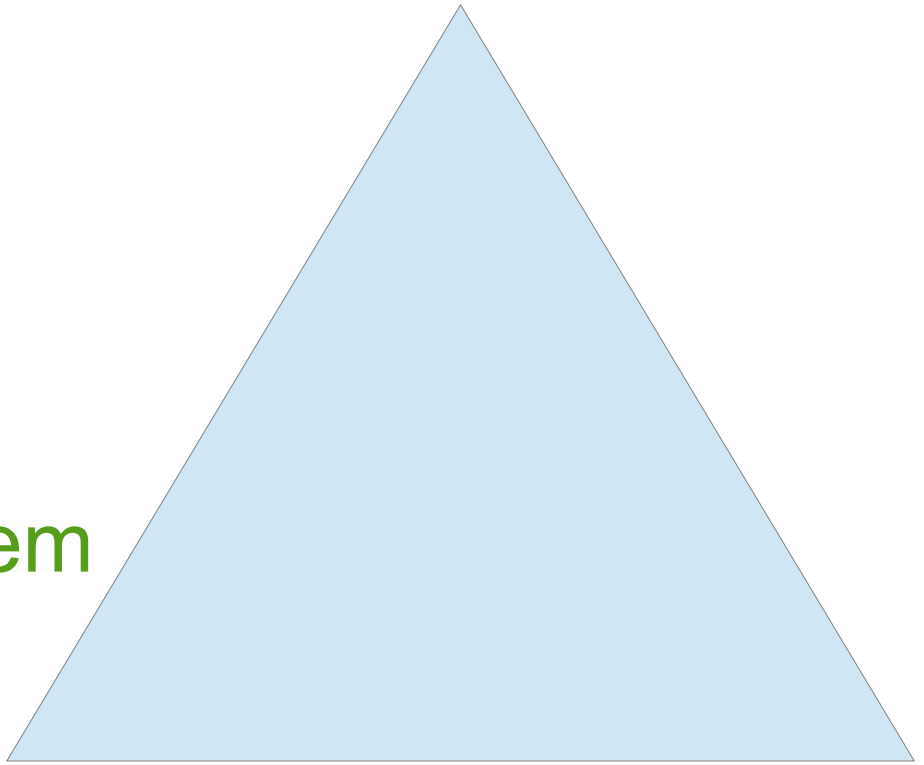
- Wahrscheinlichkeit des Auftretens eines Schadens und
- der Schwere dieses Schadens

Risikobezogener Ansatz

Verbotene Praktiken

Hochrisiko-KI-Systeme

KI-Systeme mit allgemeinem Anwendungszweck



Verbotene Praktiken im KI-Bereich

- Techniken der unterschwelligen Beeinflussung oder manipulative Techniken
- Ausnutzen der Vunerabilität oder Schutzbedürftigkeit nat. Personen (-gruppen)
- Bewertung oder Einstufung zur Benachteiligung nat. Personen oder Personengruppen
- Risikobewertung eine Straftat zu begehen auf Basis des Profiling
- Verwendung von Datenbanken zur Gesichtserkennung durch das ungezielte Auslesen von Gesichtsbildern aus dem Internet oder von Überwachungsaufnahmen
- Ableitung von Emotionen am Arbeitsplatz und in Bildungseinrichtungen
- Biometrische Kategorisierung
- Biometrischer Echtzeit-Fernidentifizierungssysteme in öffentlich zugänglichen Räumen zu Strafverfolgungszwecken

Verbotene Praktiken im KI-Bereich

Artikel 5 Verbotene Praktiken im KI-Bereich

(1) Folgende Praktiken im KI-Bereich sind verboten:

a) das Inverkehrbringen, die Inbetriebnahme oder die Verwendung eines KI-Systems, das Techniken der unterschwelligen

Beeinflussung außerhalb des Bewusstseins einer Person oder absichtlich manipulative oder täuschende Techniken mit

dem Ziel oder der Wirkung einsetzt, das Verhalten einer Person oder einer Gruppe von Personen wesentlich zu

verändern, indem ihre Fähigkeit, eine fundierte Entscheidung zu treffen, deutlich beeinträchtigt wird, wodurch sie

veranlasst wird, eine Entscheidung zu treffen, die sie andernfalls nicht getroffen hätte, und zwar in einer Weise, die dieser Person, einer anderen Person oder einer Gruppe von Personen erheblichen Schaden zufügt oder mit hinreichender Wahrscheinlichkeit zufügen wird.

Verbotene Praktiken im KI-Bereich

Artikel 5 Verbotene Praktiken im KI-Bereich

(1) Folgende Praktiken im KI-Bereich sind verboten:

b) das Inverkehrbringen, die Inbetriebnahme oder die Verwendung eines KI-Systems, das eine Vulnerabilität oder

Schutzbedürftigkeit einer natürlichen Person oder einer bestimmten Gruppe von Personen

aufgrund ihres Alters, einer Behinderung oder einer bestimmten sozialen oder wirtschaftlichen Situation

mit dem Ziel oder der Wirkung ausnutzt,

das Verhalten dieser Person oder einer dieser Gruppe angehörenden Person in einer Weise wesentlich zu verändern, die

dieser Person oder einer anderen Person erheblichen Schaden zufügt oder mit hinreichender Wahrscheinlichkeit zufügen wird;

Verbotene Praktiken im KI-Bereich

Artikel 5 Verbotene Praktiken im KI-Bereich

(1) Folgende Praktiken im KI-Bereich sind verboten:

c) das Inverkehrbringen, die Inbetriebnahme oder die Verwendung von KI-Systemen zur Bewertung oder Einstufung von natürlichen Personen oder Gruppen von Personen über einen bestimmten Zeitraum
auf der Grundlage ihres sozialen Verhaltens oder bekannter, abgeleiteter oder vorhergesagter persönlicher Eigenschaften oder Persönlichkeitsmerkmale,
wobei die soziale Bewertung zu einem oder beiden der folgenden Ergebnisse führt:

i) Schlechterstellung oder Benachteiligung bestimmter natürlicher Personen oder Gruppen von Personen in sozialen Zusammenhängen, die in keinem Zusammenhang zu den Umständen stehen, unter denen die Daten ursprünglich erzeugt oder erhoben wurden;

ii) Schlechterstellung oder Benachteiligung bestimmter natürlicher Personen oder Gruppen von Personen in einer Weise,

die im Hinblick auf ihr soziales Verhalten oder dessen Tragweite ungerechtfertigt oder unverhältnismäßig ist;

Verbotene Praktiken im KI-Bereich

Artikel 5 Verbotene Praktiken im KI-Bereich

(1) Folgende Praktiken im KI-Bereich sind verboten:

d) das Inverkehrbringen, die Inbetriebnahme für diesen spezifischen Zweck oder die Verwendung eines KI-Systems zur Durchführung von Risikobewertungen in Bezug auf natürliche Personen,

um das Risiko, dass eine natürliche Person eine Straftat begeht,

ausschließlich auf der Grundlage des Profiling einer natürlichen Person oder der Bewertung ihrer persönlichen Merkmale und Eigenschaften zu bewerten oder vorherzusagen;

dieses Verbot gilt nicht für KI-Systeme, die dazu verwendet werden, die durch Menschen durchgeführte Bewertung der Beteiligung einer Person an einer kriminellen Aktivität, die sich bereits auf objektive und überprüfbare Tatsachen stützt, die in unmittelbarem Zusammenhang mit einer kriminellen Aktivität stehen, zu unterstützen;

Verbotene Praktiken im KI-Bereich

Artikel 5 Verbotene Praktiken im KI-Bereich

(1) Folgende Praktiken im KI-Bereich sind verboten:

e) das Inverkehrbringen, die Inbetriebnahme für diesen spezifischen Zweck oder die Verwendung von KI-Systemen,

Die Datenbanken zur Gesichtserkennung durch

das ungezielte Auslesen von Gesichtsbildern

aus dem Internet oder

von Überwachungsaufnahmen erstellen oder erweitern;

Verbotene Praktiken im KI-Bereich

Artikel 5 Verbotene Praktiken im KI-Bereich

(1) Folgende Praktiken im KI-Bereich sind verboten:

f) das Inverkehrbringen, die Inbetriebnahme für diesen spezifischen Zweck oder die Verwendung von KI-Systemen zur

Ableitung von Emotionen einer natürlichen Person am Arbeitsplatz und

in Bildungseinrichtungen,

es sei denn, die Verwendung des KI-Systems soll aus medizinischen Gründen oder Sicherheitsgründen eingeführt oder auf den Markt gebracht werden;

Verbotene Praktiken im KI-Bereich

Artikel 5 Verbotene Praktiken im KI-Bereich

(1) Folgende Praktiken im KI-Bereich sind verboten:

g) das Inverkehrbringen, die Inbetriebnahme für diesen spezifischen Zweck oder die Verwendung von Systemen zur

biometrischen Kategorisierung, mit denen natürliche Personen individuell auf der Grundlage ihrer biometrischen Daten kategorisiert werden, um

ihre Rasse, ihre politischen Einstellungen, ihre Gewerkschaftszugehörigkeit, ihre religiösen oder weltanschaulichen Überzeugungen, ihr Sexualleben oder ihre sexuelle Ausrichtung zu erschließen oder abzuleiten;

dieses Verbot gilt nicht für die Kennzeichnung oder Filterung rechtmäßig erworbener biometrischer Datensätze, wie z. B. Bilder auf der Grundlage biometrischer Daten oder die Kategorisierung biometrischer Daten im Bereich der Strafverfolgung;

Verbotene Praktiken im KI-Bereich

Artikel 5 Verbotene Praktiken im KI-Bereich
(1) Folgende Praktiken im KI-Bereich sind verboten:
h) die Verwendung **biometrischer Echtzeit-Fernidentifizierungssysteme in öffentlich zugänglichen Räumen zu Strafverfolgungszwecken**,
außer wenn und insoweit dies im Hinblick auf eines der folgenden Ziele unbedingt erforderlich ist:
i) gezielte Suche nach bestimmten Opfern von Entführung, Menschenhandel oder sexueller Ausbeutung sowie die Suche nach vermissten Personen;
ii) Abwenden einer konkreten, erheblichen und unmittelbaren Gefahr für das Leben oder die körperliche Unversehrtheit natürlicher Personen oder einer tatsächlichen und bestehenden oder tatsächlichen und vorhersehbaren Gefahr eines Terroranschlags;
iii) Aufspüren oder Identifizieren einer Person, die der Begehung einer Straftat verdächtigt wird, zum Zwecke der Durchführung von strafrechtlichen Ermittlungen oder von Strafverfahren oder der Vollstreckung einer Strafe für die in Anhang II aufgeführten Straftaten, die in dem betreffenden Mitgliedstaat nach dessen Recht mit einer Freiheitsstrafe oder einer freiheitsentziehenden Maßregel der Sicherung im Höchstmaß von mindestens vier Jahren bedroht ist.
Unterabsatz 1 Buchstabe h gilt unbeschadet des Artikels 9 der Verordnung (EU) 2016/679 für die Verarbeitung biometrischer Daten zu anderen Zwecken als der Strafverfolgung.

Verbotene Praktiken im KI-Bereich

Artikel 5 Verbotene Praktiken im KI-Bereich

(2) Die Verwendung biometrischer Echtzeit-Fernidentifizierungssysteme in öffentlich zugänglichen Räumen zu Strafverfolgungszwecken im Hinblick auf die in Absatz 1 Unterabsatz 1 Buchstabe h genannten Ziele darf für die in

jenem Buchstaben genannten Zwecke
nur zur Bestätigung der Identität der speziell betroffenen Person erfolgen,
wobei folgende Elemente berücksichtigt werden:

a) die Art der Situation, die der möglichen Verwendung zugrunde liegt, insbesondere die Schwere, die Wahrscheinlichkeit und das Ausmaß des Schadens, der entstehen würde, wenn das System nicht eingesetzt würde;

b) die Folgen der Verwendung des Systems für die Rechte und Freiheiten aller betroffenen Personen, insbesondere die Schwere, die Wahrscheinlichkeit und das Ausmaß solcher Folgen.

Verbotene Praktiken im KI-Bereich

Artikel 5 Verbotene Praktiken im KI-Bereich

(2) ...

Darüber hinaus sind bei der Verwendung biometrischer Echtzeit-Fernidentifizierungssysteme in öffentlich zugänglichen Räumen zu Strafverfolgungszwecken im Hinblick auf die in Absatz 1 Unterabsatz 1 Buchstabe h des vorliegenden Artikels genannten Ziele notwendige und verhältnismäßige Schutzvorkehrungen und Bedingungen für die Verwendung im Einklang mit nationalem Recht über die Ermächtigung ihrer Verwendung einzuhalten, insbesondere in Bezug auf die zeitlichen, geografischen und personenbezogenen Beschränkungen. Die Verwendung biometrischer Echtzeit-Fernidentifizierungssysteme in öffentlich zugänglichen Räumen ist nur dann zu gestatten, wenn die Strafverfolgungsbehörde eine

Folgenabschätzung im Hinblick auf die Grundrechte gemäß Artikel 27 abgeschlossen und das System gemäß Artikel 49 in der EU-Datenbank registriert hat. In hinreichend begründeten dringenden Fällen kann jedoch mit der Verwendung solcher Systeme zunächst ohne Registrierung in der EU-Datenbank begonnen werden, sofern diese Registrierung unverzüglich erfolgt.

Verbotene Praktiken im KI-Bereich

Genehmigungsvorbehalt und Eilfälle biometrischen Echtzeit-Fernidentifizierungssystems

(3) Für die Zwecke des Absatz 1 Unterabsatz 1 Buchstabe h und des Absatzes 2 ist für jede Verwendung eines **biometrischen Echtzeit-Fernidentifizierungssystems in öffentlich zugänglichen Räumen zu Strafverfolgungszwecken**
eine vorherige Genehmigung erforderlich, die
von einer Justizbehörde oder einer unabhängigen Verwaltungsbehörde des Mitgliedstaats, in dem die Verwendung erfolgen soll, auf begründeten Antrag und gemäß den in Absatz 5 genannten detaillierten nationalen Rechtsvorschriften erteilt wird, wobei deren Entscheidung bindend ist.

In hinreichend begründeten **dringenden Fällen** kann jedoch mit der Verwendung eines solchen Systems zunächst ohne Genehmigung begonnen werden, sofern eine solche Genehmigung unverzüglich, spätestens jedoch innerhalb von 24 Stunden beantragt wird. Wird eine solche Genehmigung abgelehnt, so wird die Verwendung mit sofortiger Wirkung eingestellt und werden alle Daten sowie die Ergebnisse und Ausgaben dieser Verwendung unverzüglich verworfen und gelöscht.

Verbotene Praktiken im KI-Bereich

Vorausssetzungen zur Erteilung einer Genehmigung für biometrischen Echtzeit-Fernidentifizierungssystems

(3) ...Die zuständige Justizbehörde oder eine unabhängige Verwaltungsbehörde, deren Entscheidung bindend ist, erteilt die Genehmigung nur dann,
wenn sie auf der Grundlage objektiver Nachweise oder eindeutiger Hinweise, die ihr vorgelegt werden,
davon überzeugt ist,
dass die Verwendung des betreffenden biometrischen Echtzeit-Fernidentifizierungssystems für das Erreichen eines der in Absatz 1 Unterabsatz 1 Buchstabe h genannten Ziele — wie im Antrag angegeben —
notwendig und verhältnismäßig ist und
insbesondere auf das in Bezug auf den Zeitraum sowie den geografischen und persönlichenAnwendungsbereich unbedingt erforderliche Maß beschränkt bleibt. Bei ihrer Entscheidung über den Antrag berücksichtigt diese Behörde die in Absatz 2 genannten Elemente. Eine Entscheidung, aus der sich eine nachteilige Rechtsfolge für eine Person ergibt, darf nicht ausschließlich auf der Grundlage der Ausgabe des biometrischen Echtzeit-Fernidentifizierungssystems getroffen werden.

Verbotene Praktiken im KI-Bereich

<u>Mitteilungspflicht für biometrischen Echtzeit-Fernidentifizierungssystems gegenüber Aufsichtsbehörde</u>

(4) Unbeschadet des Absatzes 3 wird jede Verwendung eines biometrischen Echtzeit-Fernidentifizierungssystems in öffentlich zugänglichen Räumen zu Strafverfolgungszwecken der zuständigen Marktüberwachungsbehörde und der nationalen Datenschutzbehörde gemäß den in Absatz 5 genannten nationalen Vorschriften mitgeteilt. Die Mitteilung muss mindestens die in Absatz 6 genannten Angaben enthalten und darf keine sensiblen operativen Daten enthalten.

Verbotene Praktiken im KI-Bereich

Öffnungsklausel für Mitgliedsstaaten für biometrischen Echtzeit-Fernidentifizierungssystems

(5) Ein Mitgliedstaat kann die Möglichkeit einer **vollständigen oder teilweisen Ermächtigung** zur Verwendung biometrischer Echtzeit-Fernidentifizierungssysteme in öffentlich zugänglichen Räumen zu Strafverfolgungszwecken innerhalb der in Absatz 1 Unterabsatz 1 Buchstabe h sowie Absätze 2 und 3 aufgeführten Grenzen und unter den dort genannten Bedingungen vorsehen.
Die betreffenden Mitgliedstaaten legen in ihrem nationalen Recht die erforderlichen **detaillierten Vorschriften** für die Beantragung, Erteilung und Ausübung der in Absatz 3 genannten Genehmigungen sowie für die entsprechende Beaufsichtigung und Berichterstattung fest. In diesen Vorschriften wird auch festgelegt, im Hinblick auf **welche** der in Absatz 1 Unterabsatz 1 Buchstabe h aufgeführten **Ziele** und **welche** der unter Buchstabe h Ziffer iii genannten **Straftaten** die zuständigen Behörden ermächtigt werden können, diese Systeme zu Strafverfolgungszwecken zu verwenden. Die Mitgliedstaaten **teilen der Kommission** diese Vorschriften spätestens 30 Tage nach ihrem Erlass **mit**.
Die **Mitgliedstaaten können** im Einklang mit dem Unionsrecht **strengere Rechtsvorschriften** für die Verwendung biometrischer Fernidentifizierungssysteme erlassen.

Verbotene Praktiken im KI-Bereich

Jahresbericht der nat. Marktüberwachungs- und DS-Aufsichtsbehörden für biometrischen Echtzeit-Fernidentifizierungssysteme

(6) Die nationalen **Marktüberwachungsbehörden und die nationalen Datenschutzbehörden** der Mitgliedstaaten, denen gemäß Absatz 4 die Verwendung biometrischer Echtzeit-Fernidentifizierungssysteme in öffentlich zugänglichen Räumen zu Strafverfolgungszwecken mitgeteilt wurden, legen der Kommission **Jahresberichte** über diese Verwendung vor. Zu diesem Zweck stellt die Kommission den Mitgliedstaaten und den nationalen Marktüberwachungs- und Datenschutzbehörden ein Muster zur Verfügung, das Angaben über die Anzahl der Entscheidungen der zuständigen Justizbehörden oder einer unabhängigen Verwaltungsbehörde, deren Entscheidung über Genehmigungsanträge gemäß Absatz 3 bindend ist, und deren Ergebnis enthält.

Verbotene Praktiken im KI-Bereich

Jahresbericht der EU-Kommission für biometrischen Echtzeit-Fernidentifizierungssysteme

(7) Die Kommission veröffentlicht Jahresberichte über die Verwendung biometrischer Echtzeit-Fernidentifizierungssysteme in öffentlich zugänglichen Räumen zu Strafverfolgungszwecken, die auf aggregierten Daten aus den Mitgliedstaaten auf der Grundlage der in Absatz 6 genannten Jahresberichte beruhen. Diese Jahresberichte dürfen keine sensiblen operativen Daten im Zusammenhang mit den damit verbundenen Strafverfolgungsmaßnahmen enthalten.

Verbotene Praktiken im KI-Bereich

Verhältnis zu anderen Rechtsvorschriften der EU

(8) Dieser Artikel berührt nicht die Verbote, die gelten, wenn KI-Praktiken gegen andere Rechtsvorschriften der Union verstoßen.

Hochrisiko-KI-Systeme: Überblick

Artikel 6

*KI als Produkt oder Produktbestandteil gem. Anhang I (nicht Teil der Veranstaltung)

*KI-Systeme gem. Anhang III

Hochrisiko-KI-Systeme: Anhang III

a) Biometrische Fernidentifizierungssysteme.

Ausnahme: Dazu gehören nicht KI-Systeme,
die bestimmungsgemäß für die biometrische Verifizierung, deren einziger Zweck darin besteht, zu bestätigen, dass eine bestimmte natürliche Person die Person ist, für die sie sich ausgibt, verwendet werden sollen;

Hochrisiko-KI-Systeme: Anhang III

b) KI-Systeme,
die bestimmungsgemäß für die biometrische Kategorisierung
nach sensiblen oder geschützten Attributen oder Merkmalen auf der Grundlage von Rückschlüssen auf diese Attribute oder Merkmale verwendet werden sollen;

Hochrisiko-KI-Systeme: Anhang III

c) KI-Systeme,

die bestimmungsgemäß zur Emotionserkennung verwendet werden sollen.

Hochrisiko-KI-Systeme: Anhang III

2. Kritische Infrastruktur:
KI-Systeme, die bestimmungsgemäß als Sicherheitsbauteile im Rahmen der Verwaltung und des Betriebs kritischer digitaler Infrastruktur, des Straßenverkehrs oder der Wasser-, Gas-, Wärme- oder Stromversorgung verwendet werden sollen.

Hochrisiko-KI-Systeme: Anhang III

3. Allgemeine und berufliche Bildung

a) KI-Systeme, die bestimmungsgemäß zur Feststellung des Zugangs oder der Zulassung oder zur Zuweisung natürlicher Personen zu Einrichtungen aller Ebenen der allgemeinen und beruflichen Bildung verwendet werden sollen;

Hochrisiko-KI-Systeme: Anhang III

3. Allgemeine und berufliche Bildung

b) KI-Systeme, die bestimmungsgemäß für die Bewertung von Lernergebnissen verwendet werden sollen,

einschließlich des Falles, dass diese Ergebnisse dazu dienen, den Lernprozess natürlicher Personen in

Einrichtungen oder Programmen aller Ebenen der allgemeinen und beruflichen Bildung zu steuern;

Hochrisiko-KI-Systeme: Anhang III

3. Allgemeine und berufliche Bildung

c) KI-Systeme, die bestimmungsgemäß zum Zweck der Bewertung des angemessenen Bildungsniveaus, das eine

Person im Rahmen von oder innerhalb von Einrichtungen aller Ebenen der allgemeinen und beruflichen Bildung

erhalten wird oder zu denen sie Zugang erhalten wird, verwendet werden sollen

Hochrisiko-KI-Systeme: Anhang III

3. Allgemeine und berufliche Bildung

c) KI-Systeme, die bestimmungsgemäß zum Zweck der Bewertung des angemessenen Bildungsniveaus,
das eine Person im Rahmen von oder innerhalb von Einrichtungen aller Ebenen der allgemeinen und beruflichen Bildung erhalten wird oder zu denen sie Zugang erhalten wird, verwendet werden sollen.

Hochrisiko-KI-Systeme: Anhang III

3. Allgemeine und berufliche Bildung

d) KI-Systeme, die bestimmungsgemäß zur Überwachung und Erkennung von verbotenem Verhalten von Schülern bei Prüfungen im Rahmen von oder innerhalb von Einrichtungen aller Ebenen der allgemeinen und beruflichenBildung verwendet werden sollen.

Hochrisiko-KI-Systeme: Anhang III

4. Beschäftigung, Personalmanagement und Zugang zur Selbstständigkeit

a) KI-Systeme, die bestimmungsgemäß für die Einstellung oder Auswahl natürlicher Personen verwendet werden sollen,
insbesondere um gezielte Stellenanzeigen zu schalten, Bewerbungen zu sichten oder zu filtern und Bewerber zu bewerten;

Hochrisiko-KI-Systeme: Anhang III

4. Beschäftigung, Personalmanagement und Zugang zur Selbstständigkeit

b) KI-Systeme, die bestimmungsgemäß
für Entscheidungen, die die Bedingungen von Arbeitsverhältnissen, Beförderungen und Kündigungen von Arbeitsvertragsverhältnissen beeinflussen, für die Zuweisung von Aufgaben aufgrund des individuellen Verhaltens oder persönlicher Merkmale oder Eigenschaften oder für die Beobachtung und Bewertung der Leistung und des Verhaltens von Personen in solchen Beschäftigungsverhältnissen verwendet werden soll.

Hochrisiko-KI-Systeme: Anhang III

5. Zugänglichkeit und Inanspruchnahme grundlegender privater und grundlegender öffentlicher Dienste und Leistungen:

a) KI-Systeme, die bestimmungsgemäß von Behörden oder im Namen von Behörden verwendet werden sollen, um

zu beurteilen, ob natürliche Personen Anspruch auf grundlegende öffentliche Unterstützungsleistungen und -dienste,

einschließlich Gesundheitsdiensten, haben und

ob solche Leistungen und Dienste zu gewähren, einzuschränken, zu widerrufen oder zurückzufordern sind;

Hochrisiko-KI-Systeme: Anhang III

5. Zugänglichkeit und Inanspruchnahme grundlegender privater und grundlegender öffentlicher Dienste und Leistungen:

b) KI-Systeme, die bestimmungsgemäß für die Kreditwürdigkeitsprüfung und Bonitätsbewertung natürlicher

Personen verwendet werden sollen, mit Ausnahme von KI-Systemen, die zur Aufdeckung von Finanzbetrug

verwendet werden;

Hochrisiko-KI-Systeme: Anhang III

5. Zugänglichkeit und Inanspruchnahme grundlegender privater und grundlegender öffentlicher Dienste und Leistungen:

c) KI-Systeme, die bestimmungsgemäß für die Risikobewertung und Preisbildung in Bezug auf natürliche Personen

im Fall von Lebens- und Krankenversicherungen verwendet werden sollen;

Hochrisiko-KI-Systeme: Anhang III

5. Zugänglichkeit und Inanspruchnahme grundlegender privater und grundlegender öffentlicher Dienste und Leistungen:

d) KI-Systeme, die bestimmungsgemäß zur Bewertung und Klassifizierung von

Notrufen von natürlichen Personen

oder für die Entsendung oder Priorisierung des Einsatzes von Not- und Rettungsdiensten, einschließlich Polizei, Feuerwehr

und medizinischer Nothilfe, sowie für Systeme für die Triage von Patienten bei der Notfallversorgung

verwendet werden sollen.

Hochrisiko-KI-Systeme: Anhang III

6. Strafverfolgung, soweit ihr Einsatz nach einschlägigem Unionsrecht oder nationalem Recht zugelassen ist:

a) KI-Systeme, die bestimmungsgemäß von Strafverfolgungsbehörden oder in deren Namen oder von Organen, Einrichtungen und sonstigen Stellen der Union

zur Unterstützung von Strafverfolgungsbehörden oder in deren Namen
zur Bewertung des Risikos einer natürlichen Person, zum **Opfer von Straftaten** zu werden, verwendet werden sollen;

Hochrisiko-KI-Systeme: Anhang III

6. Strafverfolgung, soweit ihr Einsatz nach einschlägigem Unionsrecht oder nationalem Recht zugelassen ist:

b) KI-Systeme, die bestimmungsgemäß von Strafverfolgungsbehörden oder in deren Namen oder von Organen, Einrichtungen und sonstigen Stellen der Union zur Unterstützung von Strafverfolgungsbehörden

als Lügendetektoren oder ähnliche Instrumente verwendet werden sollen;

Hochrisiko-KI-Systeme: Anhang III

6. Strafverfolgung, soweit ihr Einsatz nach einschlägigem Unionsrecht oder nationalem Recht zugelassen ist:

c) KI-Systeme, die bestimmungsgemäß von Strafverfolgungsbehörden oder in deren Namen oder von Organen, Einrichtungen und sonstigen Stellen der Union zur Unterstützung von Strafverfolgungsbehörden zur Bewertung

der **Verlässlichkeit von Beweismitteln** im Zuge der Ermittlung oder Verfolgung von Straftaten verwendet werden sollen;

Hochrisiko-KI-Systeme: Anhang III

6. Strafverfolgung, soweit ihr Einsatz nach einschlägigem Unionsrecht oder nationalem Recht zugelassen ist:

d) KI-Systeme, die bestimmungsgemäß von Strafverfolgungsbehörden oder in deren Namen oder von Organen, Einrichtungen und sonstigen Stellen der Union zur Unterstützung von Strafverfolgungsbehörden

zur Bewertung des Risikos, dass **eine natürliche Person eine Straftat begeht oder erneut begeht**, nicht nur auf der Grundlage der Erstellung von Profilen natürlicher Personen gemäß Artikel 3 Absatz 4 der Richtlinie (EU) 2016/680 oder zur

Bewertung persönlicher Merkmale und Eigenschaften oder vergangenen kriminellen Verhaltens von natürlichen Personen oder Gruppen verwendet werden sollen;

Hochrisiko-KI-Systeme: Anhang III

6. Strafverfolgung, soweit ihr Einsatz nach einschlägigem Unionsrecht oder nationalem Recht zugelassen ist:

e) KI-Systeme, die bestimmungsgemäß von Strafverfolgungsbehörden oder in deren Namen oder von Organen,Einrichtungen und sonstigen Stellen der Union zur Unterstützung von Strafverfolgungsbehörden

zur Erstellung von **Profilen** natürlicher Personen gemäß Artikel 3 Absatz 4 der Richtlinie (EU) 2016/680 im Zuge der **Aufdeckung, Ermittlung oder Verfolgung von Straftaten** verwendet werden sollen.

Hochrisiko-KI-Systeme: Anhang III

7. Migration, Asyl und Grenzkontrolle,
soweit ihr Einsatz nach einschlägigem Unionsrecht oder nationalem Recht zugelassen ist:

a) KI-Systeme, die bestimmungsgemäß von zuständigen Behörden oder in deren Namen oder Organen,

Einrichtungen und sonstigen Stellen der Union als **Lügendetektoren** verwendet werden sollen oder ähnliche Instrumente;

Hochrisiko-KI-Systeme: Anhang III

7. Migration, Asyl und Grenzkontrolle,
soweit ihr Einsatz nach einschlägigem Unionsrecht oder nationalem Recht zugelassen ist:

b) KI-Systeme, die bestimmungsgemäß von zuständigen Behörden oder in deren Namen oder von Organen, Einrichtungen und sonstigen Stellen der Union zur Bewertung eines Risikos verwendet werden sollen,

einschließlich eines **Sicherheitsrisikos**, eines **Risikos der irregulären Einwanderung oder eines Gesundheitsrisikos**,

das von einer natürlichen Person ausgeht, die in das Hoheitsgebiet eines Mitgliedstaats einzureisen beabsichtigt oder eingereist ist;

Hochrisiko-KI-Systeme: Anhang III

7. Migration, Asyl und Grenzkontrolle,
soweit ihr Einsatz nach einschlägigem Unionsrecht oder nationalem Recht zugelassen ist:

c) KI-Systeme, die bestimmungsgemäß von zuständigen Behörden oder in deren Namen oder von Organen, Einrichtungen und sonstigen Stellen der Union verwendet werden sollen, um zuständige Behörden bei der

Prüfung von **Asyl- und Visumanträgen sowie Aufenthaltstiteln** und damit **verbundenen Beschwerden** im Hinblick auf die **Feststellung der Berechtigung** der den Antrag stellenden natürlichen Personen, einschließlich damit zusammenhängender Bewertungen der Verlässlichkeit von Beweismitteln, zu unterstützen;

Hochrisiko-KI-Systeme: Anhang III

7. Migration, Asyl und Grenzkontrolle,
soweit ihr Einsatz nach einschlägigem Unionsrecht oder nationalem Recht zugelassen ist:

d) KI-Systeme, die bestimmungsgemäß von oder im Namen der zuständigen Behörden oder Organen, Einrichtungen und sonstigen Stellen der Union,
im Zusammenhang mit Migration, Asyl oder Grenzkontrolle zum Zwecke der **Aufdeckung, Anerkennung oder Identifizierung natürlicher Personen** verwendet werden sollen, mit Ausnahme der Überprüfung von Reisedokumenten.

Hochrisiko-KI-Systeme: Anhang III

8. Rechtspflege und demokratische Prozesse

a) 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;

Hochrisiko-KI-Systeme: Anhang III

8. Rechtspflege und demokratische Prozesse

b) KI-Systeme, die bestimmungsgemäß verwendet werden sollen, um das Ergebnis einer **Wahl oder eines Referendums** oder das **Wahlverhalten natürlicher Personen** bei der Ausübung ihres Wahlrechts bei einer Wahl oder einem Referendum zu beeinflussen.

Ausnahme: Dazu gehören nicht KI-Systeme, deren Ausgaben natürliche Personen nicht direkt ausgesetzt sind, wie Instrumente zur Organisation, Optimierung oder Strukturierung politischer Kampagnen in administrativer oder logistischer Hinsicht.

Hochrisiko-KI-Systeme: Ausnahmen

(3) Abweichend von Absatz 2 gilt ein in Anhang III genanntes KI-System nicht als hochriskant, wenn
es **kein erhebliches Risiko** der Beeinträchtigung in Bezug auf die Gesundheit, Sicherheit oder Grundrechte natürlicher Personen birgt, indem es unter anderem nicht das Ergebnis der Entscheidungsfindung wesentlich beeinflusst.
Unterabsatz 1 gilt, wenn eine der folgenden Bedingungen erfüllt ist:

a) das KI-System ist dazu bestimmt, eine eng gefasste Verfahrensaufgabe durchzuführen;

b) das KI-System ist dazu bestimmt, das Ergebnis einer zuvor abgeschlossenen menschlichen Tätigkeit zu verbessern

Hochrisiko-KI-Systeme: Ausnahmen

(3) Abweichend von Absatz 2 gilt ein in Anhang III genanntes KI-System nicht als hochriskant, wenn
es **kein erhebliches Risiko** der Beeinträchtigung in Bezug auf die Gesundheit, Sicherheit oder Grundrechte natürlicher Personen birgt, indem es unter anderem nicht das Ergebnis der Entscheidungsfindung wesentlich beeinflusst. Unterabsatz 1 gilt, wenn eine der folgenden Bedingungen erfüllt ist:

c) das KI-System ist dazu bestimmt, **Entscheidungsmuster** oder Abweichungen von früheren Entscheidungsmustern **zu erkennen,** und ist **nicht dazu gedacht**, die zuvor abgeschlossene **menschliche Bewertung** ohne eine angemessene menschliche Überprüfung zu ersetzen oder **zu beeinflussen**; oder
d) das KI-System ist dazu bestimmt, eine **vorbereitende Aufgabe** für eine Bewertung durchzuführen, die für die Zwecke derin Anhang III aufgeführten Anwendungsfälle relevant ist.

Hochrisiko-KI-Systeme: Keine Ausnahme für Profiling

Ungeachtet des Unterabsatzes 1 gilt ein in Anhang III aufgeführtes KI-System immer dann als hochriskant,

wenn es ein **Profiling natürlicher Personen** vornimmt.

Zum Beispiel: Schufa

Menschliche Aufsicht für Hochrisiko-KI-Systeme

- Beaufsichtigungsfähigkeit als design-Vorgabe

Hochrisiko-KI-Systeme werden so konzipiert und entwickelt, dass sie

* während der Dauer ihrer Verwendung

* — auch mit geeigneten Instrumenten einer Mensch-Maschine-Schnittstelle —

* von natürlichen Personen wirksam beaufsichtigt werden können.

Menschliche Aufsicht für Hochrisiko-KI-Systeme

- Ziel der Aufsicht

Die menschliche Aufsicht dient

*der Verhinderung oder Minimierung der Risiken für Gesundheit, Sicherheit oder Grundrechte,

*die entstehen können, wenn ein Hochrisiko-KI-System im Einklang mit seiner Zweckbestimmung oder im Rahmen einer vernünftigerweise vorhersehbaren Fehlanwendung verwendet wird,

**insbesondere wenn solche Risiken trotz der Einhaltung anderer Anforderungen dieses Abschnitts fortbestehen.

Menschliche Aufsicht für Hochrisiko-KI-Systeme

- Risikobasierte Aufsicht

Die Aufsichtsmaßnahmen müssen

*den Risiken, dem Grad der Autonomie und dem Kontext der Nutzung des Hochrisiko-KI-Systems angemessen sein und

*werden durch eine oder beide der folgenden Arten von Vorkehrungen gewährleistet:

a) Vorkehrungen, die vor dem Inverkehrbringen oder der Inbetriebnahme vom Anbieter bestimmt und, sofern technisch machbar, in das Hochrisiko-KI-System eingebaut werden;

b) Vorkehrungen, die vor dem Inverkehrbringen oder der Inbetriebnahme des Hochrisiko-KI-Systems vom Anbieter bestimmt werden und dazu geeignet sind, vom Betreiber umgesetzt zu werden.

Menschliche Aufsicht für Hochrisiko-KI-Systeme

- Beaufsichtigungsfähigkeit (1)

Für die Zwecke der Durchführung der Absätze 1, 2 und 3 wird das Hochrisiko-KI-System dem Betreiber so zur Verfügung gestellt, dass die natürlichen Personen, denen die menschliche Aufsicht übertragen wurde, angemessen und verhältnismäßig in der Lage sind,

a) die einschlägigen Fähigkeiten und Grenzen des Hochrisiko-KI-Systems angemessen zu verstehen und

seinen Betrieb ordnungsgemäß zu überwachen, einschließlich in Bezug auf das Erkennen und Beheben von Anomalien, Fehlfunktionen und unerwarteter Leistung;

b) sich einer möglichen Neigung zu einem automatischen oder übermäßigen Vertrauen in die von einem Hochrisiko-KI-System hervorgebrachte Ausgabe („Automatisierungsbias“) bewusst zu bleiben, insbesondere wenn Hochrisiko-KI-Systeme Informationen oder Empfehlungen ausgeben, auf deren Grundlage natürliche Personen Entscheidungen treffen;

Menschliche Aufsicht für Hochrisiko-KI-Systeme

- Beaufsichtigungsfähigkeit(2)

Für die Zwecke der Durchführung der Absätze 1, 2 und 3 wird das Hochrisiko-KI-System dem Betreiber so zur Verfügung gestellt, dass die natürlichen Personen, denen die menschliche Aufsicht übertragen wurde, angemessen und verhältnismäßig in der Lage sind,

c) die Ausgabe des Hochrisiko-KI-Systems richtig zu interpretieren, wobei beispielsweise die vorhandenen Interpretationsinstrumente und -methoden zu berücksichtigen sind;

d) in einer bestimmten Situation zu beschließen, das Hochrisiko-KI-System nicht zu verwenden oder die Ausgabe des Hochrisiko-KI-Systems außer Acht zu lassen, außer Kraft zu setzen oder rückgängig zu machen;

e) in den Betrieb des Hochrisiko-KI-Systems einzugreifen oder den Systembetrieb mit einer „Stopptaste“ oder einem ähnlichen Verfahren zu unterbrechen, was dem System ermöglicht, in einem sicheren Zustand zum Stillstand zu kommen.

Menschliche Aufsicht für Hochrisiko-KI-Systeme

- 4-Augen-Aufsicht für biometrische Fernidentifizierungssysteme

Bei den in Anhang III Nummer 1 Buchstabe a genannten Hochrisiko-KI-Systemen [biometrische Fernidentifizierungssysteme] müssen die in Absatz 3 des vorliegenden Artikels genannten Vorkehrungen so gestaltet sein, dass außerdem

*der Betreiber keine Maßnahmen oder Entscheidungen allein aufgrund des vom System hervorgebrachten Identifizierungsergebnisses trifft,

*solange diese Identifizierung nicht von mindestens zwei natürlichen Personen, die die notwendige Kompetenz, Ausbildung und Befugnis besitzen, getrennt überprüft und bestätigt wurde.

*Ausnahme: Die Anforderung einer getrennten Überprüfung durch mindestens zwei natürliche Personen gilt nicht für Hochrisiko-KI-Systeme,

**die für Zwecke in den Bereichen Strafverfolgung, Migration, Grenzkontrolle oder Asyl verwendet werden,

**wenn die Anwendung dieser Anforderung nach Unionsrecht oder nationalem Recht unverhältnismäßig wäre.

KI-Officer

- Aufgaben
  - Schulung
  - Führen des KI-Registers
  - Einordnen in Risikokategorien gem. KI-VO
  - Menschliche Aufsicht und Risikosteuerung der Hochrisiko-KI-Systeme (Art. 14 Abs. 4 KI-VO)
  - Überprüfung der Einhaltung der KI-VO: Audits

KI-Officer

- Rolle
    - Konflikthafte Rolle?
- Stellung
    - Direkte Berichtslinie an die Unternehmensführung
    - Alternativ: Stabsstelle

KI-Officer

- 2nd Line of Defence (LoD)
  - 3-Line-of-Defence-Modell
  - Abgrenzung zum „KI-Innovation Officer“

KI-Officer

- Kompetenz
  - Fachliche Kompetenz
    - Technik
    - Recht
    - Organisation
    - Kommunikation (u.a. Schulung)
  - Persönliche Kompetenz
    - Kommunikation (u.a. Schulung)

KI-Officer

- Vergleichbare Rollen
  - DSB
  - Compliance Officer
  - Informationssicherheitsbeauftragter (ISB)

KI-Officer

- Alternative Ausgestaltung
  - Option 1: Anlehnung an Compliance Beauftragten
    - Verantwortung für Aufbau und Umsetzung der Governance
  - Option 2: Anlehung an DSB
    - Ausschliesslich Beratungsmandat