EUROPÄISCHE
KOMMISSION

Brüssel, den 21.4.2021
COM(2021) 206 final

2021/0106 (COD)

Vorschlag für eine

VERORDNUNG DES EUROPÄISCHEN PARLAMENTS UND DES RATES

ZUR FESTLEGUNG HARMONISIERTER VORSCHRIFTEN FÜR KÜNSTLICHE INTELLIGENZ (GESETZ ÜBER KÜNSTLICHE INTELLIGENZ) UND ZUR ÄNDERUNG BESTIMMTER RECHTSAKTE DER UNION

{SEC(2021) 167 final} - {SWD(2021) 84 final} - {SWD(2021) 85 final}

BEGRÜNDUNG

1. KONTEXT DES VORSCHLAGS

1.1. Gründe und Ziele des Vorschlags

Diese Begründung ist dem Vorschlag für eine Verordnung beigefügt, mit der harmonisierte Vorschriften für künstliche Intelligenz festgelegt werden (Gesetz über künstliche Intelligenz). Künstliche Intelligenz (KI) bezeichnet eine Reihe von Technologien, die sich rasant entwickeln und einen vielfältigen Nutzen für Wirtschaft und Gesellschaft über das gesamte Spektrum industrieller und gesellschaftlicher Aktivitäten hinweg hervorbringen können. Der Einsatz künstlicher Intelligenz zur Verbesserung von Prognosen, zur Optimierung von Abläufen und der Ressourcenzuweisung sowie zur Personalisierung der Diensteerbringung kann für die Gesellschaft und die Umwelt von Nutzen sein und Unternehmen sowie der europäischen Wirtschaft Wettbewerbsvorteile verschaffen. Bedarf besteht insbesondere in Sektoren, von denen eine große Wirkung ausgeht, wie Klimaschutz, Umwelt und Gesundheit, öffentlicher Sektor, Finanzen, Mobilität, Inneres und Landwirtschaft. Dieselben Faktoren und Techniken, die für den sozioökonomischen Nutzen der KI sorgen, können aber auch neue Risiken oder Nachteile für den Einzelnen oder die Gesellschaft hervorbringen. Vor dem Hintergrund des rasanten technologischen Wandels und möglicher Herausforderungen ist die EU entschlossen, einen ausgewogenen Ansatz zu erreichen. Es liegt im Interesse der Union, die technische Führungsrolle der EU auszubauen und dafür zu sorgen, dass die Europäerinnen und Europäer von den im Einklang mit den Werten, Grundrechten und Prinzipien der Union entwickelten und funktionierenden neuen Technologien profitieren können.

Dieser Vorschlag geht auf das politische Engagement von Präsidentin von der Leyen zurück, die in ihren politischen Leitlinien für die Kommission (2019-2024) – „Eine Union, die mehr erreichen will“[1] – ankündigte, dass die Kommission einen Legislativvorschlag für ein koordiniertes europäisches Konzept für die menschlichen und ethischen Aspekte der KI vorlegen wird. Im Nachgang zu dieser Ankündigung veröffentlichte die Kommission am 19. Februar 2020 ihr Weißbuch zur KI – Ein europäisches Konzept für Exzellenz und Vertrauen[2]. In dem Weißbuch legt sie die politischen Optionen dar, wie die Nutzung von KI gefördert und gleichzeitig die mit bestimmten Anwendungen dieser Technologie verbundenen Risiken eingedämmt werden können. Dieser Vorschlag zielt darauf ab, einen Rechtsrahmen für eine vertrauenswürdige KI zu schaffen, damit das zweite Ziel für den Aufbau eines Ökosystems für Vertrauen umgesetzt werden kann. Der Vorschlag beruht auf den Werten und Grundrechten der EU und will erreichen, dass Privatpersonen und andere Nutzer KI-gestützten Lösungen vertrauen und gleichzeitig Unternehmen Anreize erhalten, diese zu entwickeln. KI sollte ein Instrument sein, das als positive Kraft für die Gesellschaft im Dienst der Menschen steht und das letztlich zu einem größeren Wohlbefinden der Menschen beiträgt. Vorschriften für KI, die auf dem Unionsmarkt verfügbar ist oder anderweitig Menschen in der Union beeinflusst, sollten daher auf den Menschen ausgerichtet sein, damit Menschen darauf vertrauen können, dass die Technik sicher angewandt wird und den Gesetzen, auch den Grundrechten, genügt. Nach Veröffentlichung des Weißbuchs leitete die Kommission eine breit angelegte Konsultation der Interessenträger ein, die reges Interesse zeigten und sich in großer Zahl beteiligten und die weitestgehend regulatorische Maßnahmen zur Bewältigung

[1] https://ec.europa.eu/commission/sites/beta-political/files/political-guidelines-next-commission_de.pdf

[2] Weißbuch zur künstlichen Intelligenz – Ein europäisches Konzept für Exzellenz und Vertrauen, COM(2020) 65 final, 2020.

der Herausforderungen und Bedenken, die der zunehmende Einsatz von KI mit sich bringt, befürworteten.

Der Vorschlag ist zudem eine Reaktion auf die vom Europäischen Parlament und dem Europäischen Rat ausdrücklich und wiederholt erhobenen Forderungen nach legislativen Maßnahmen zur Gewährleistung eines reibungslos funktionierenden Binnenmarkts für Systeme der künstlichen Intelligenz (KI-Systeme), mit denen sowohl der Nutzen als auch die Risiken der KI auf Unionsebene angemessen geregelt werden. Er unterstützt das vom Europäischen Rat[3] formulierte Ziel der Union, bei der Entwicklung einer sicheren, vertrauenswürdigen und ethisch vertretbaren künstlichen Intelligenz weltweit eine Führungsrolle einzunehmen, und sorgt für den vom Europäischen Parlament[4] ausdrücklich geforderten Schutz von Ethikgrundsätzen.

2017 forderte der Europäische Rat „ein Bewusstsein für die Dringlichkeit der Auseinandersetzung mit neuen Trends“, auch für „Themen wie künstliche Intelligenz....“, „wobei zugleich ein hohes Niveau in Bezug auf Datenschutz, digitale Rechte und ethische Standards gewahrt werden muss“[5]. In seinen Schlussfolgerungen von 2019 zu dem koordinierten Plan für künstliche Intelligenz „Made in Europe“[6] betont der Rat ferner, wie wichtig es ist, die uneingeschränkte Achtung der Rechte der europäischen Bürgerinnen und Bürger zu gewährleisten, und ruft dazu auf, die maßgeblichen geltenden Rechtsvorschriften zu überprüfen, um sicherzustellen, dass sie im Hinblick auf die neuen Chancen und Herausforderungen, die sich durch künstliche Intelligenz ergeben, zweckdienlich sind. Der Europäische Rat forderte zudem eine klare Festlegung von KI-Anwendungen, die als hochriskant eingestuft werden sollten[7].

In seinen jüngsten Schlussfolgerungen vom 21. Oktober 2020 forderte der Rat zudem, dass Probleme wie Undurchsichtigkeit, Komplexität, der sogenannte „Bias“, ein gewisses Maß an Unberechenbarkeit und teilweise autonomes Verhalten einiger KI-Systeme angegangen werden müssen, um deren Vereinbarkeit mit den Grundrechten sicherzustellen und die Durchsetzung der Rechtsvorschriften zu erleichtern[8].

Auch das Europäische Parlament hat sich intensiv mit dem Thema der KI befasst. Im Oktober 2020 nahm es eine Reihe von Entschließungen zur KI an, u. a. zur Ethik[9], zivilrechtlichen Haftung[10] und zum Urheberrecht[11]. 2021 folgten weitere Entschließungen zur KI im

---

3 Europäischer Rat, Außerordentliche Tagung des Europäischen Rates (1. und 2. Oktober 2020) – Schlussfolgerungen, EUCO 13/20, 2020, S. 6.

4 Entschließung des Europäischen Parlaments vom 20. Oktober 2020 mit Empfehlungen an die Kommission zu dem Rahmen für die ethischen Aspekte von künstlicher Intelligenz, Robotik und damit zusammenhängenden Technologien, 2020/2012 (INL).

5 Europäischer Rat, Tagung des Europäischen Rates (19. Oktober 2017) – Schlussfolgerung, EUCO 14/17, 2017, S. 7.

6 Rat der Europäischen Union, Künstliche Intelligenz b) Schlussfolgerungen zu dem koordinierten Plan für künstliche Intelligenz – Annahme, 6177/19, 2019.

7 Europäischer Rat, Außerordentliche Tagung des Europäischen Rates (1. und 2. Oktober 2020) – Schlussfolgerungen, EUCO 13/20, 2020.

8 Rat der Europäischen Union, Schlussfolgerungen des Vorsitzes – Die Charta der Grundrechte im Zusammenhang mit künstlicher Intelligenz und dem digitalen Wandel, 11481/20, 2020.

9 Entschließung des Europäischen Parlaments vom 20. Oktober 2020 mit Empfehlungen an die Kommission zu dem Rahmen für die ethischen Aspekte von künstlicher Intelligenz, Robotik und damit zusammenhängenden Technologien, 2020/2012 (INL).

10 Entschließung des Europäischen Parlaments vom 20. Oktober 2020 mit Empfehlungen an die Kommission für eine Regelung der zivilrechtlichen Haftung beim Einsatz künstlicher Intelligenz, 2020/2014(INL).

Strafrecht[12] sowie in der Bildung, der Kultur und im audiovisuellen Bereich[13]. In seiner Entschließung zu dem Rahmen für die ethischen Aspekte von künstlicher Intelligenz, Robotik und damit zusammenhängenden Technologien empfiehlt das Europäische Parlament der Kommission insbesondere legislative Maßnahmen vorzuschlagen, um so die Chancen und den Nutzen künstlicher Intelligenz auszuschöpfen, aber auch dafür zu sorgen, dass Ethik-Grundsätze geschützt werden. Die Entschließung enthält den Legislativvorschlag für eine Verordnung über Ethik-Grundsätze für die Entwicklung, den Einsatz und die Nutzung von künstlicher Intelligenz, Robotik und damit zusammenhängenden Technologien im Wortlaut. Dieser Vorschlag berücksichtigt die vorstehende Entschließung des Europäischen Parlaments unter uneingeschränkter Wahrung der Grundsätze der Verhältnismäßigkeit, Subsidiarität und besseren Rechtsetzung und steht damit in Einklang mit den von Präsidentin von der Leyen in ihren politischen Leitlinien gemachten politischen Zusagen hinsichtlich der Behandlung der vom Europäischen Parlament angenommenen Entschließungen nach Artikel 225 AEUV.

Vor diesem politischen Hintergrund legt die Kommission ihren Vorschlag für einen Rechtsrahmen zur Künstlichen Intelligenz vor, mit dem konkret die folgenden **Ziele** angestrebt werden:

- Es muss gewährleistet sein, dass die auf dem Unionsmarkt in Verkehr gebrachten und verwendeten KI-Systeme sicher sind und die bestehenden Grundrechte und die Werte der Union wahren.
- Zur Förderung von Investitionen in KI und innovativen KI muss Rechtssicherheit gewährleistet sein.
- Governance und die wirksame Durchsetzung des geltenden Rechts zur Wahrung der Grundrechte sowie die Sicherheitsanforderungen an KI-Systeme müssen gestärkt werden.
- Die Entwicklung eines Binnenmarkts für rechtskonforme, sichere und vertrauenswürdige KI-Anwendungen muss erleichtert werden und es gilt, eine Marktfragmentierung zu verhindern.

Mit Blick auf diese Ziele enthält dieser Vorschlag einen ausgewogenen horizontalen Regulierungsansatz für KI, der die Verhältnismäßigkeit wahrt und auf die Mindestanforderungen beschränkt ist, die zur Bewältigung der in Verbindung mit KI auftretenden Risiken und Probleme notwendig ist, ohne die technologische Entwicklung übermäßig einzuschränken oder zu behindern oder anderweitig die Kosten für das Inverkehrbringen von KI-Lösungen unverhältnismäßig in die Höhe zu treiben. Der Vorschlag zielt auf einen robusten und flexiblen Rechtsrahmen ab. Einerseits ist der Vorschlag in seinen grundlegenden Regulierungsentscheidungen umfassend und zukunftsorientiert. Dies gilt auch für die von den KI-Systemen zu erfüllenden und auf Grundsätzen beruhenden Anforderungen. Andererseits wird ein Regulierungssystem geschaffen, das die Verhältnismäßigkeit wahrt und auf genau definierte Risiken ausgerichtet ist. Dieser Regulierungsansatz schafft keine unnötigen Handelsbeschränkungen und der Gesetzgeber schreitet nur in solchen konkreten

---

[11] Entschließung des Europäischen Parlaments vom 20. Oktober 2020 zu den Rechten des geistigen Eigentums bei der Entwicklung von KI-Technologien, 2020/2015(INI).

[12] Europäisches Parlament – Berichtsentwurf über künstliche Intelligenz im Strafrecht und ihre Verwendung durch die Polizei und Justizbehörden in Strafsachen, 2020/2016(INI).

[13] Europäisches Parlament – Entwurf eines Berichts über künstliche Intelligenz in der Bildung, der Kultur und dem audiovisuellen Bereich, 2020/2017(INI). So hat die Kommission den Aktionsplan für digitale Bildung 2021-2027 angenommen: „Neuaufstellung des Bildungswesens für das digitale Zeitalter“. Der Aktionsplan sieht die Entwicklung von Ethik-Leitlinien für die Nutzung von KI und Daten im Bildungswesen vor – Mitteilung der Kommission, COM(2020) 624 final.

Situationen ein, in denen ein berechtigter Anlass für Bedenken besteht oder in denen vernünftigerweise davon ausgegangen werden kann, dass solche Bedenken in naher Zukunft auftreten werden. Gleichzeitig enthält der Rechtsrahmen Mechanismen, mit denen er flexibel und dynamisch an die technologische Entwicklung und neue bedenkliche Situationen angepasst werden kann.

Der Vorschlag enthält harmonisierte Vorschriften für die Entwicklung, das Inverkehrbringen und die Verwendung von KI-Systemen in der Union, die im Verhältnis zu den Risiken stehen. Die vorgeschlagene Begriffsbestimmung für KI ist zukunftstauglich. Während einige besonders schädliche KI-Praktiken, die gegen die Werte der Union verstoßen, verboten sind, werden für die Zwecke der Strafverfolgung für bestimmte Anwendungen biometrischer Fernidentifizierungssysteme konkrete Beschränkungen und Sicherheitsmaßnahmen vorgeschlagen. Der Vorschlag enthält eine solide Risiko-Methodik zur Einstufung von Hochrisiko-KI-Systemen, d. h. solchen Systemen, die erhebliche Risiken für die Gesundheit und Sicherheit oder die Grundrechte von Personen bergen. Solche KI-Systeme müssen horizontalen Auflagen für vertrauenswürdige KI genügen und Konformitätsbewertungsverfahren unterzogen werden, bevor sie in der Union in Verkehr gebracht werden dürfen. Damit die Sicherheit und die Einhaltung bestehender Rechtsvorschriften zum Schutz der Grundrechte über den gesamten Lebenszyklus von KI-Systemen hinweg gewahrt bleiben, werden Anbietern und Nutzern dieser Systeme berechenbare, verhältnismäßige und klare Pflichten auferlegt. Für einige KI-Systeme werden nur minimale Transparenzpflichten vorgeschlagen, insbesondere für den Einsatz von Chatbots oder „Deepfakes“.

Die vorgeschlagenen Vorschriften werden von den Mitgliedstaaten mittels einer Leitungsstruktur durchgesetzt, die auf bereits vorhandenen Strukturen aufbaut, sowie mittels eines Kooperationsmechanismus auf Unionsebene, auf der ein Europäischer Ausschuss für künstliche Intelligenz eingesetzt wird. Zusätzliche Maßnahmen werden zur Unterstützung von Innovation, vor allem in Form von KI-Reallaboren, sowie zur Verringerung des Verwaltungsaufwands und zur Förderung von kleinen und mittleren Unternehmen (KMU) und Startups vorgeschlagen.

1.2. Kohärenz mit den bestehenden Vorschriften in diesem Politikbereich

Die horizontale Ausrichtung des Vorschlags erfordert die uneingeschränkte Kohärenz mit dem bestehenden Unionsrecht, das auf Sektoren Anwendung findet, in denen Hoch-Risiko-KI-Systeme bereits jetzt oder wahrscheinlich in naher Zukunft eingesetzt werden.

Auch mit der EU-Grundrechtecharta und dem geltenden Sekundärrecht der Union zum Daten- und Verbraucherschutz, zur Nichtdiskriminierung und zur Gleichstellung der Geschlechter ist die Kohärenz gewährleistet. Die Datenschutz-Grundverordnung (Verordnung (EU) 2016/679) und die Strafverfolgungsrichtlinie (Richtlinie (EU) 2016/680) bleiben von dem Vorschlag unberührt und werden durch harmonisierte Vorschriften für Entwurf, Entwicklung und Verwendung bestimmter Hochrisiko-KI-Systeme sowie durch Beschränkungen für bestimmte Anwendungen biometrischer Fernidentifizierungssysteme ergänzt. Darüber hinaus ergänzt der Vorschlag geltendes Unionsrecht zur Nichtdiskriminierung, indem konkrete Anforderungen zur Minimierung des Risikos der Diskriminierung durch Algorithmen, vor allem in Bezug auf Entwurf und Qualität von für die Entwicklung von KI-Systemen verwendeten Datensätzen, aufgenommen wurden, und Tests, Risikomanagement, Dokumentation und menschliche Aufsicht über die gesamte Lebensdauer von KI-Systemen hinweg verbindlich vorgeschrieben werden. Der Vorschlag lässt die Anwendung des Wettbewerbsrechts der Union unberührt.

Im Hinblick auf Hochrisiko-KI-Systeme, bei denen es sich um Sicherheitskomponenten von Produkten handelt, wird dieser Vorschlag zur Wahrung der Kohärenz, zur Vermeidung von

Überschneidungen und zur Verringerung des Verwaltungsaufwands in die bereits vorhandenen sektorspezifischen Sicherheitsvorschriften eingebunden. So werden die in diesem Vorschlag enthaltenen Anforderungen an KI-Systeme im Falle von Hochrisiko-KI-Systemen, die mit unter den Neuen Rechtsrahmen (New Legislative Framework, NLF) fallenden Produkten (z. B. Maschinen, medizinische Geräte, Spielzeug) in Verbindung stehen, im Rahmen der bestehenden Konformitätsbewertungsverfahren nach dem einschlägigen NLF-Recht geprüft. Für das Zusammenspiel der Anforderung gilt, dass die von den jeweiligen KI-Systemen abhängigen Sicherheitsrisiken den Anforderungen dieses Vorschlags unterliegen, während mit dem NLF-Recht die Sicherheit des Endprodukts insgesamt gewährleistet werden soll, weshalb diese Vorschriften konkrete Anforderungen an die sichere Integration von KI-Systemen in das Endprodukt enthalten können. Dieser Ansatz lässt sich auch gut daran erkennen, dass der Vorschlag für eine Maschinenverordnung am selben Tag wie dieser Vorschlag angenommen werden soll. Für Hochrisiko-KI-Systeme in Verbindung mit Produkten, die unter die einschlägigen Vorschriften des Alten Konzepts fallen (z. B. Luftfahrt, Fahrzeuge) würde dieser Vorschlag nicht unmittelbar gelten. Allerdings müssen die in diesem Vorschlag festgelegten und vorab zu erfüllenden wesentlichen Anforderungen an Hochrisiko-KI-Systeme bei der Annahme einschlägiger Durchführungsrechtsakte oder delegierter Rechtsakte in diesen Rechtsakten berücksichtigt werden.

Bei KI-Systemen, die von regulierten Kreditinstituten bereitgestellt oder verwendet werden, sollten die für die Aufsicht über die Rechtsvorschriften der Union im Bereich der Finanzdienstleistungen zuständigen Behörden auch als die zuständigen Behörden für die Aufsicht über die Anforderungen dieses Vorschlags benannt werden, um eine kohärente Durchsetzung der sich aus diesem Vorschlag ergebenden Pflichten und der Rechtsvorschriften der Union im Bereich der Finanzdienstleistungen zu gewährleisten, in denen die KI-Systeme zu einem gewissen Grad implizit in Verbindung mit dem internen Unternehmensführungssystem der Kreditinstitute reguliert sind. Im Sinne einer noch größeren Kohärenz werden die in diesem Vorschlag vorgesehenen Konformitätsbewertungen und einige verfahrenstechnische Pflichten der Anbieter in die Verfahren eingebunden, die nach der Richtlinie 2013/36/EU über den Zugang zur Tätigkeit von Kreditinstituten und die Beaufsichtigung von Kreditinstituten und Wertpapierfirmen[14] einzuhalten sind.

Zudem steht der Vorschlag in Einklang mit dem geltenden EU-Dienstleistungsrecht, unter das auch die in der E-Commerce-Richtlinie 2000/31/EG[15] regulierten Vermittlungsdienste und der jüngste Kommissionsvorschlag für das Gesetz über digitale Dienste[16] fallen.

Der Vorschlag gilt nicht für die KI-Systeme, die als Komponenten von IT-Großsystemen in dem von der Agentur der Europäischen Union für das Betriebsmanagement von IT-Großsystemen (eu-LISA) verwalteten Raum der Freiheit, der Sicherheit und des Rechts vor Ablauf eines Jahres ab dem Zeitpunkt der Anwendung dieser Verordnung in Verkehr gebracht oder in Betrieb genommen wurden, sofern der Ersatz oder die Änderung der entsprechenden

---

[14] Richtlinie 2013/36/EU des Europäischen Parlaments und des Rates vom 26. Juni 2013 über den Zugang zur Tätigkeit von Kreditinstituten und die Beaufsichtigung von Kreditinstituten und Wertpapierfirmen, zur Änderung der Richtlinie 2002/87/EG und zur Aufhebung der Richtlinien 2006/48/EG und 2006/49/EG (ABl. L 176 vom 27.6.2013, S. 338).

[15] Richtlinie 2000/31/EG des Europäischen Parlaments und des Rates vom 8. Juni 2000 über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt („Richtlinie über den elektronischen Geschäftsverkehr“) (ABl. L 178 vom 17.7.2000, S. 1).

[16] Siehe Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über einen Binnenmarkt für digitale Dienste (Gesetz über digitale Dienste) und zur Änderung der Richtlinie 2000/31/EG, COM(2020) 825 final.

Rechtsakte die Konzeption oder die Zweckbestimmung der betreffenden KI-Systeme erheblich ändert.

1.3. Kohärenz mit der Politik der Union in anderen Bereichen

Der Vorschlag ist Teil eines umfassenderen Pakets von Maßnahmen, mit denen die im Weißbuch zur KI untersuchten Probleme, die sich bei der Entwicklung und der Verwendung von KI stellen, angegangen werden sollen. Daher werden Kohärenz und Komplementarität mit anderen laufenden oder geplanten Initiativen der Kommission, die sich ebenfalls mit diesen Problemen befassen, gewährleistet. Hierunter fallen die Überarbeitung der sektorspezifischen Produktvorschriften (z. B. die Maschinenrichtlinie, die Richtlinie über die allgemeine Produktsicherheit) sowie Initiativen, die sich mit Haftungsfragen im Zusammenhang mit den neuen Technologien, auch KI-Systemen, befassen. Die Initiativen werden auf diesem Vorschlag aufbauen und ihn ergänzen und so für Rechtsklarheit sorgen und die Entwicklung eines Ökosystems für Vertrauen in die KI in Europa fördern.

Der Vorschlag steht zudem in Einklang mit der von der Kommission insgesamt verfolgten Digitalstrategie, indem er dazu beiträgt, eine Technologie zu fördern, die den Menschen zugutekommt – eines der drei Hauptziele, die in der Mitteilung zur „Gestaltung der digitalen Zukunft Europas“ genannt werden[17]. Es wird ein kohärenter, wirksamer und angemessener Rahmen geschaffen, mit dem sichergestellt wird, dass KI so entwickelt wird, dass die Rechte der Menschen geachtet werden und sie ihr Vertrauen verdient – damit ist Europa für das digitale Zeitalter gewappnet und die nächsten zehn Jahre werden zur **digitalen Dekade**[18].

Darüber hinaus ist die Förderung der auf KI beruhenden Innovation eng mit dem **Daten-Governance-Gesetz**[19], der **Richtlinie über offene Daten**[20] und anderen Initiativen im Rahmen der **EU-Strategie für Daten**[21] verknüpft, mit denen vertrauenswürdige Mechanismen und Dienste für die Weiterverwendung, das Teilen und die Zusammenführung von Daten festgelegt werden, die für die Entwicklung hochwertiger datengesteuerter KI-Modelle entscheidend sind.

Mit dem Vorschlag wird zudem die Position der Union bei der Formulierung weltweiter Normen und Standards sowie der Förderung vertrauenswürdiger KI, die mit den Werten und Interessen der Union in Einklang stehen, erheblich gestärkt. Er bietet der Union eine solide Grundlage für ihre weiteren Gespräche zur Fragen der KI mit ihren externen Partnern, auch Drittländern, und in internationalen Gremien.

2. RECHTSGRUNDLAGE, SUBSIDIARITÄT UND VERHÄLTNISMÄßIGKEIT

2.1. Rechtsgrundlage

Rechtsgrundlage für den Vorschlag ist zunächst Artikel 114 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV), der die Annahme von Maßnahmen für die Errichtung und das Funktionieren des Binnenmarkts vorsieht.

---

17 Mitteilung der Kommission „Gestaltung der digitalen Zukunft Europas“, COM(2020) 67.

18 Digitaler Kompass 2030:der europäische Weg in die digitale Dekade.

19 Vorschlag für eine Verordnung über europäische Daten-Governance (Data-Governance-Gesetz), COM(2020) 767.

20 Richtlinie (EU) 2019/1024 des Europäischen Parlaments und des Rates vom 20. Juni 2019 über offene Daten und die Weiterverwendung von Informationen des öffentlichen Sektors (PE/28/2019/REV/1, ABl. L 172 vom 26.6.2019, S. 56).

21 Mitteilung der Kommission „Eine europäische Datenstrategie“, COM(2020) 66 final.

Dieser Vorschlag bildet ein Kernelement der EU-Strategie für den digitalen Binnenmarkt. Hauptziel dieses Vorschlags ist, durch die Festlegung harmonisierter Vorschriften, insbesondere in Bezug auf die Entwicklung, das Inverkehrbringen und den Einsatz von Produkten und Diensten, die KI-Techniken anwenden, oder von eigenständigen KI-Systemen, für ein reibungsloses Funktionieren des Binnenmarkts zu sorgen. Einige Mitgliedstaaten ziehen bereits nationale Vorschriften in Erwägung, damit sichergestellt ist, dass KI sicher ist und unter Einhaltung der Grundrechte entwickelt und verwendet wird. Daraus dürften sich vor allem die beiden folgende Probleme ergeben: i) eine Fragmentierung des Binnenmarkts in wesentlichen Fragen, insbesondere mit Blick auf die Anforderungen an KI-Produkte und -Dienste, deren Vermarktung und Verwendung sowie auf die Haftung und die Aufsicht durch öffentliche Behörden, und ii) die erheblich geringere Rechtssicherheit sowohl für Anbieter als auch Nutzer von KI-Systemen im Hinblick darauf, wie bestehende und neue Vorschriften auf solche Systeme in der Union angewandt werden. Angesichts des großen Umfangs des grenzüberschreitenden Waren- und Dienstleistungsverkehrs lassen sich diese beiden Probleme am besten durch unionsweit harmonisierte Rechtsvorschriften lösen.

So werden in dem Vorschlag die gemeinsamen Anforderungen an Konzeption und Entwicklung bestimmter KI-Systeme festgelegt, die zwingend eingehalten werden müssen, bevor diese Systeme in Verkehr gebracht werden dürfen, und die weiter durch harmonisierte technische Normen konkretisiert werden. Der Vorschlag befasst sich auch mit der Situation nach dem Inverkehrbringen von KI-Systemen, indem eine abgestimmte Vorgehensweise für nachträgliche Kontrollen vorgesehen wird.

Da dieser Vorschlag konkrete Vorschriften zum Schutz von Privatpersonen im Hinblick auf die Verarbeitung personenbezogener Daten enthält, mit denen vor allem die Verwendung von KI-Systemen zur biometrischen Fernidentifizierung in Echtzeit in öffentlich zugänglichen Räumen für die Zwecke der Strafverfolgung eingeschränkt wird, sollte sich diese Verordnung in Bezug auf diese konkreten Vorschriften auch auf Artikel 16 AEUV stützen.

2.2. Subsidiarität (bei nicht ausschließlicher Zuständigkeit)

Es liegt in der Natur der KI, die häufig auf großen und vielfältigen Datensätzen beruht und die in alle im Binnenmarkt in Verkehr gebrachte Produkte oder Dienste eingebettet sein kann, dass die Ziele dieses Vorschlags von den Mitgliedstaaten nicht allein effizient erreicht werden können. Zudem wird der reibungslose unionsweite Waren- und Dienstleistungsverkehr im Zusammenhang mit KI-Systemen durch das Entstehen eines Flickenteppichs potenziell abweichender nationaler Vorschriften behindert, die zudem die Sicherheit und den Schutz der Grundrechte sowie die Einhaltung der Werte der Union länderübergreifend nur unzureichend gewährleisten können. Einzelstaatliche Konzepte zur Lösung der Probleme werden nur zu mehr Rechtsunsicherheit und zu Hemmnissen sowie zu einer langsameren Markteinführung von KI führen.

Die Ziele dieses Vorschlags können besser auf Unionsebene erreicht werden, denn nur so lässt sich eine weitere Fragmentierung des Binnenmarkts verhindern, die dazu führen würde, dass potenziell widersprüchliche nationale Bestimmungen den freien Waren- und Dienstleistungsverkehr von Produkten, in die KI eingebettet ist, unmöglich machen. Ein solider europäischer Rechtsrahmen für eine vertrauenswürdige KI wird auch für gleiche Wettbewerbsbedingungen sorgen und alle Menschen schützen, gleichzeitig jedoch die Wettbewerbsfähigkeit Europas und die Industriebasis im KI-Bereich stärken. Nur durch gemeinsames Handeln auf Unionsebene kann die Union ihre Souveränität im digitalen Bereich schützen und ihre Instrumente und Regelungsbefugnisse zur Gestaltung globaler Regeln und Standards einsetzen.

2.3. Verhältnismäßigkeit

Der Vorschlag baut auf dem bestehenden Rechtsrahmen auf, ist verhältnismäßig und zur Erreichung seiner Ziele notwendig, da mit ihm ein risikobasierter Ansatz verfolgt wird und regulatorische Belastungen nur dann entstehen, wenn davon auszugehen ist, dass ein KI-System hohe Risiken für die Grundrechte und die Sicherheit darstellt. Für andere, KI-Systeme, die kein hohes Risiko darstellen, werden nur sehr wenige Transparenzpflichten auferlegt, etwa dahingehend, dass bei der Interaktion mit Menschen der Einsatz von KI-Systemen angezeigt werden muss. Im Falle von Hochrisiko-KI-Systemen sind die Anforderungen an hohe Datenqualität, Dokumentation und Rückverfolgbarkeit, Transparenz, menschliche Aufsicht, Präzision und Robustheit unerlässlich, um die Risiken für die Grundrechte und die Sicherheit abzumildern, die mit diesen KI verbunden sind und die nicht durch andere bestehende Rechtsvorschriften abgedeckt werden. Anbieter und Nutzer werden bei der Einhaltung der in dem Vorschlag festgelegten Anforderungen durch harmonisierte Standards, Orientierungshilfen und Instrumente zur Einhaltung der Vorschriften unterstützt, die auch ihre Kosten gering halten. Die den Akteuren entstehenden Kosten stehen im Verhältnis zu den erreichten Zielen, dem wirtschaftlichen Nutzen sowie dem guten Ruf, die die Akteure von der vorgeschlagenen Regelung erwarten können.

2.4. Wahl des Instruments

Die Wahl einer Verordnung als Rechtsinstrument ist durch die Notwendigkeit einer einheitlichen Anwendung der neuen Vorschriften gerechtfertigt, beispielsweise im Hinblick auf die Begriffsbestimmung für KI, das Verbot bestimmter schädlicher Praktiken, die durch KI ermöglicht werden, und die Einstufung bestimmter KI-Systeme. Die unmittelbare Anwendbarkeit einer Verordnung nach Artikel 288 AEUV verringert die Rechtsfragmentierung und erleichtert die Entwicklung eines Binnenmarkts für rechtmäßige, sichere und vertrauenswürdige KI-Systeme. Hierzu wird insbesondere ein Bündel harmonisierter zentraler Anforderungen an als hochriskant eingestufte KI-Systeme eingeführt. Darüber hinaus werden Pflichten für Anbieter und Nutzer dieser Systeme festgelegt, um den Schutz der Grundrechte und die Rechtssicherheit sowohl für Akteure als auch Nutzer zu verbessern.

Darüber hinaus sind die Bestimmungen der Verordnung nicht übermäßig präskriptiv und lassen den Mitgliedstaaten auf verschiedenen Ebenen Raum für Maßnahmen in Bezug auf Elemente, die den Zielen der Initiative nicht zuwiderlaufen, insbesondere im Hinblick auf die interne Organisation des Marktüberwachungssystems und die Einführung innovationsfördernder Maßnahmen.

3. ERGEBNISSE DER EX-POST-BEWERTUNG, DER KONSULTATION DER INTERESSENTRÄGER UND DER FOLGENABSCHÄTZUNG

3.1. Konsultation der Interessenträger

Dieser Vorschlag ist das Ergebnis einer umfangreichen Konsultation aller wichtigen Interessenträger, bei der die allgemeinen Grundsätze und Mindeststandards für die Konsultation von Interessenträgern durch die Kommission angewandt wurden.

Gleichzeitig mit der Veröffentlichung des Weißbuchs zur Künstlichen Intelligenz am 19. Februar 2020 wurde eine öffentliche Online-Konsultation gestartet, die bis zum 14. Juni 2020 lief. Ziel der Konsultation war die Einholung von Ansichten und Stellungnahmen zum Weißbuch. Sie richtete sich an alle Interessenträger des öffentlichen und privaten Sektors, auch an Regierungen, lokale Behörden, gewerbliche und nichtgewerbliche Organisationen, Sozialpartner, Sachverständige und Hochschulen sowie an Bürgerinnen und Bürger. Nach

Auswertung der eingegangenen Antworten veröffentlichte die Kommission auf ihrer Website[22] eine Zusammenfassung der Ergebnisse sowie die einzelnen Antworten.

Insgesamt gingen 1215 Beiträge ein, davon 352 von Unternehmen oder Unternehmensorganisationen/-verbänden, 406 von Einzelpersonen (92 % Personen aus der EU), 152 von Hochschul-/Forschungsinstituten und 73 von öffentlichen Stellen. 160 Antworten gingen von Vertretern der Zivilgesellschaft ein (darunter 9 Verbraucherorganisationen, 129 NRO und 22 Gewerkschaften), 72 Antworten von „Sonstigen“. Unter den 352 Unternehmens- und Industrievertretern waren 222 Vertreter von Unternehmen, bei denen es sich zu 41,5 % um Vertreter von Kleinstunternehmen sowie kleinen und mittleren Unternehmen handelte. Bei den übrigen handelte es sich um Unternehmensverbände. Insgesamt kamen 84 % der Antworten der Unternehmens- und Industrievertreter aus der EU-27. Je nach Frage nutzten 81 bis 598 Teilnehmer die Möglichkeit, Kommentare frei zu formulieren. Über 450 Positionspapiere wurden mittels der EU-Survey-Website eingereicht, entweder als Anlage zu den Antworten auf den Fragebogen (über 400) oder als eigenständige Beiträge (über 50).

Insgesamt besteht unter den Interessenträgern Einvernehmen über den Handlungsbedarf. Eine große Mehrheit der Interessenträger stimmt der Auffassung zu, dass Regelungslücken bestehen oder neue Vorschriften benötigt werden. Allerdings weisen mehrere Interessenträger die Kommission darauf hin, dass Überschneidungen, widersprüchliche Auflagen oder eine Überregulierung vermieden werden sollten. Viele Kommentare unterstrichen die Bedeutung der Technologieneutralität und eines die Verhältnismäßigkeit wahrenden Rechtsrahmens.

Die Interessenträger forderten mehrheitlich eine enge, klare und genaue Begriffsbestimmung künstlicher Intelligenz. Neben einer Klärung des Begriffs der KI unterstrichen sie auch die Notwendigkeit, die Begriffe „Risiko“, „hohes Risiko“, „niedriges Risiko“, „biometrische Fernidentifizierung“ und „Schaden“ zu definieren.

Die meisten Teilnehmer befürworten ausdrücklich den risikobasierten Ansatz. Ein Ansatz, der sich auf die Risiken stützt, wurde im Vergleich zu einer undifferenzierten Regulierung aller KI-Systeme als die bessere Option betrachtet. Die Festlegung der Art der Risiken und Gefahren sollte von den jeweiligen Sektoren und vom Einzelfall abhängig gemacht werden Bei der Bewertung der Risiken sollte auch deren rechtliche und sicherheitsrelevante Auswirkung berücksichtigt werden.

Reallabore könnten zur Förderung von KI sehr nützlich sein und werden von einigen Interessenträgern, vor allem Unternehmensverbänden, begrüßt.

Über die Hälfte der Teilnehmer, die zu den Durchsetzungsmodellen Stellung genommen haben, insbesondere Unternehmensverbände, begrüßen im Falle von Hochrisiko-KI-Systemen eine Kombination aus einer Vorab-Selbstbewertung des Risikos und einer Ex-post-Durchsetzung.

3.2. Einholung und Nutzung von Expertenwissen

Der Vorschlag beruht auf in einem Zeitraum von zwei Jahren durchgeführten Analysen und der engen Einbeziehung von Interessenträgern, auch von Hochschulen, Unternehmen, Sozialpartnern, Nichtregierungsorganisationen, Mitgliedstaaten, Bürgerinnen und Bürgern. 2018 begannen die vorbereitenden Arbeiten mit der Einsetzung einer **hochrangigen Expertengruppe für KI**, die sich aus 52 renommierten Sachverständigen zusammensetzte, die ein breites Spektrum abdeckten und deren Aufgabe es war, die Kommission bei der

[22] Alle Ergebnisse der Konsultation finden Sie hier.

Umsetzung der Strategie für Künstliche Intelligenz zu beraten. Im April 2019 unterstützte die Kommission[23] die zentralen Anforderungen, die die hochrangige Expertengruppe in ihre Ethik-Leitlinien für vertrauenswürdige KI[24] aufgenommen hatte und die überarbeitet worden waren, um die über 500 Beiträge von Interessenträgern zu berücksichtigen. Die zentralen Anforderungen sind Ausdruck eines breit gefassten und gemeinsamen Ansatzes, der angesichts der Fülle der von vielen privaten und öffentlichen Organisationen in Europa und weltweit entwickelten Ethik-Codes und Ethik-Grundsätzen darauf hinausläuft, dass Entwicklung und Verwendung von KI von bestimmten wesentlichen werteorientierten Grundsätzen geleitet sein sollten. Für die praktische Umsetzung dieser Anforderungen im Rahmen eines Pilotverfahrens mit über 350 Organisationen wurde eine Bewertungsliste für vertrauenswürdige künstliche Intelligenz (*Assessment List for Trustworthy Artificial Intelligence*, ALTAI)[25] erstellt.

Zudem wurde eine **KI-Allianz**[26] ins Leben gerufen, die etwa 4000 Interessenträgern die Möglichkeit gibt, über eine Plattform technologische und gesellschaftliche Aspekte der KI zu diskutieren und jährlich in einer KI-Versammlung zusammen zu kommen.

Dieser inklusive Ansatz wurde mit dem **Weißbuch** zur KI weiterentwickelt, auf das Kommentare, darunter über 450 Positionspapiere, von über 1250 Interessenträgern eingingen. Daraufhin veröffentlichte die Kommission eine erste Folgenabschätzung, auf die wiederum über 130 Kommentare eingingen[27]. Zudem wurden **weitere Workshops und Veranstaltungen für Interessenträger** organisiert, deren Ergebnisse die Analysen der Folgenabschätzung und die in diesem Vorschlag getroffene Wahl der politischen Optionen unterstützen[28]. Darüber hinaus flossen die Ergebnisse einer in Auftrag gegebenen **externen Studie** mit in die Folgenabschätzung ein.

3.3. Folgenabschätzung

Entsprechend ihrer Strategie für eine bessere Rechtsetzung führte die Kommission eine Folgenabschätzung für diesen Vorschlag durch, die vom Ausschuss für Regulierungskontrolle der Kommission geprüft wurde. Am 16. Dezember 2020 fand eine Sitzung mit dem Ausschuss für Regulierungskontrolle statt, der eine ablehnende Stellungnahme abgab. Nachdem die Folgenabschätzung unter Berücksichtigung der Kommentare gründlich überarbeitet und erneut vorgelegt wurde, gab der Ausschuss für Regulierungskontrolle am 21. März 2021 eine befürwortende Stellungnahme ab. Die Stellungnahmen des Ausschusses für Regulierungskontrolle, die Empfehlungen und eine Erläuterung dazu, inwiefern diese Berücksichtigung gefunden haben, sind Anhang 1 der Folgenabschätzung zu entnehmen.

Die Kommission prüfte verschiedene politische Optionen daraufhin, inwieweit sich mit ihnen das übergeordnete Ziel des Vorschlags erreichen lässt, nämlich durch Schaffung der Voraussetzungen für die Entwicklung und Verwendung vertrauenswürdiger KI in der Union, **das reibungslose Funktionieren des Binnenmarkts zu gewährleisten**.

---

23 Europäische Kommission, Schaffung von Vertrauen in eine auf den Menschen ausgerichtete künstliche Intelligenz, COM(2019) 168.

24 HLEG, *Ethics Guidelines for Trustworthy AI*, 2019.

25 HLEG, *Assessment List for Trustworthy Artificial Intelligence (ALTAI) for self-assessment*, 2020.

26 Die KI-Allianz, ein Forum unterschiedlichster Interessenträger, wurde 2018 gegründet: https://ec.europa.eu/digital-single-market/en/european-ai-alliance.

27 Europäische Kommission, *Inception Impact Assessment For a Proposal for a legal act of the European Parliament and the Council laying down requirements for Artificial Intelligence*.

28 Einzelheiten aller durchgeführten Konsultationen sind Anhang 2 der Folgenabschätzung zu entnehmen.

Hierzu wurden vier politische Optionen geprüft, die regulatorische Maßnahmen in unterschiedlichem Ausmaß vorsehen:

- **Option 1**: EU-Rechtsetzungsinstrument zur Einrichtung eines Systems zur freiwilligen Kennzeichnung;
- **Option 2**: ein sektorspezifischer „Ad-hoc"-Ansatz;
- **Option 3**: ein horizontales EU-Rechtsetzungsinstrument gestützt auf Verhältnismäßigkeit und einen risikobasierten Ansatz;
- **Option 3+**: ein horizontales EU-Rechtsetzungsinstrument gestützt auf Verhältnismäßigkeit und einen risikobasierten Ansatz, ergänzt durch einen Verhaltenskodex für KI-Systeme, die kein hohes Risiko darstellen;
- **Option 4**: ein horizontales EU-Rechtsetzungsinstrument, mit dem obligatorische Anforderungen an alle KI-Systeme, unabhängig von dem mit diesen verbundenen Risiko, festgelegt werden.

Nach bewährter Methodik der Kommission wurde jede politische Option im Hinblick auf ihre wirtschaftlichen und gesellschaftlichen Auswirkungen mit besonderem Augenmerk auf die Auswirkungen auf die Grundrechte geprüft. Bevorzugt wird die Option 3+, d. h. ein Rechtsrahmen ausschließlich für Hochrisiko-KI-Systeme und die Möglichkeit für alle Anbieter von KI-Systemen, die kein hohes Risiko darstellen, sich an einen Verhaltenskodex zu halten. Die für Hochrisiko-KI-Systeme geltenden Anforderungen werden sich auf Daten, Dokumentation und Rückverfolgbarkeit, Bereitstellung von Informationen und Transparenz, menschliche Aufsicht sowie Robustheit und Genauigkeit beziehen. Unternehmen können freiwillig Verhaltenskodizes für andere KI-Systeme einführen.

Die bevorzugte Option wurde als geeignet erachtet, die Ziele dieses Vorschlags in effizientester Weise zu erreichen. Indem KI-Entwickler und KI-Nutzer verpflichtet werden, ein begrenztes, aber wirkungsvolles Bündel von Maßnahmen zu ergreifen, werden mit der bevorzugten Option, bei der gezielte Anforderungen nur für solche Systeme gelten, bei denen ein hohes Risiko besteht, dass Grundrechte verletzt werden und die Sicherheit von Menschen gefährdet wird, das Risiko solcher Verstöße eingedämmt und zudem eine effiziente Aufsicht und Durchsetzung unterstützt. Die dadurch bei dieser Option minimierten Rechtsbefolgungskosten führen dazu, dass die Einführung nicht aufgrund höherer Preise und Rechtsbefolgungskosten unnötigerweise hinausgezögert wird. Um etwaige Nachteile für KMU zu vermeiden, umfasst diese Option mehrere Bestimmungen, mit denen KMU nicht nur bei der Rechtsbefolgung und Kostenreduzierung, sondern auch bei der Einrichtung von Reallaboren unterstützt werden, sowie die Pflicht, bei der Festsetzung der Gebühren für die Konformitätsbewertung die Interessen von KMU zu berücksichtigen.

Mit der bevorzugten Option lässt sich das Vertrauen der Menschen in KI erhöhen, Unternehmen haben Rechtssicherheit und die Mitgliedstaaten sehen sich nicht mehr veranlasst, einseitig Maßnahmen zu ergreifen, die zu einer Fragmentierung des Binnenmarkts führen würden. Die mit dem größeren Vertrauen steigende Nachfrage und das infolge der Rechtssicherheit größere Angebot sowie der ungehinderte grenzüberschreitende Warenverkehr von KI-Systemen dürften zu einem florierenden Binnenmarkt für KI führen. Die Europäische Union wird die Entwicklung eines schnell wachsenden KI-Ökosystems innovativer Dienste und Produkte, in die KI-Technologie eingebettet ist, oder eigenständiger KI-Systeme weiter vorantreiben, um so die digitale Autonomie zu vergrößern.

Unternehmen oder öffentliche Stellen, die KI-Anwendungen entwickeln oder verwenden, die ein hohes Risiko für die Sicherheit oder Grundrechte von Bürgerinnen und Bürgern darstellen,

sind verpflichtet, bestimmte Anforderungen und Verpflichtungen einzuhalten. Für die Einhaltung dieser Anforderungen entstehen bis 2025 für die Lieferung eines durchschnittlichen Hochrisiko-KI-Systems im Wert von etwa 170 000 EUR Kosten von etwa 6000 EUR bis 7000 EUR. Abhängig von der jeweiligen Anwendung fallen für KI-Nutzer gegebenenfalls zudem die jährlichen Kosten für die Zeit an, die für die menschliche Aufsicht aufgewandt werden muss. Diese wurden mit etwa 5000 EUR bis 8000 EUR pro Jahr veranschlagt. Für Lieferanten von Hochrisiko-KI könnten zudem Überprüfungskosten in Höhe von 3000 EUR bis 7500 EUR anfallen. Unternehmen oder öffentliche Stellen, die nicht als hochriskant eingestufte KI-Anwendungen entwickeln oder nutzen, hätten nur eine minimale Informationspflicht. Sie könnten sich jedoch entscheiden, mit anderen gemeinsam einen Verhaltenskodex über die Einhaltung geeigneter Anforderungen festzulegen und dafür zu sorgen, dass ihre KI-Systeme vertrauenswürdig sind. In diesem Fall würden sich die Kosten höchstens auf dem Niveau für Hochrisiko-KI-Systeme bewegen, wahrscheinlich jedoch darunter.

Welche Auswirkungen die politischen Optionen auf die verschiedenen Kategorien von Interessenträgern haben (Wirtschaftsakteure/Unternehmen, Konformitätsbewertungsstellen, Normungsgremien und sonstige öffentliche Gremien, Privatpersonen/Bürgerinnen und Bürger, Forschung), wird im Einzelnen in Anhang 3 der Folgenabschätzung in der Anlage zu diesem Vorschlag erläutert.

3.4. Effizienz der Rechtsetzung und Vereinfachung

Dieser Vorschlag enthält die Pflichten für Anbieter und Nutzer von Hochrisiko-KI-Systemen. Anbieter, die solche Systeme entwickeln und in der Union in Verkehr bringen, erhalten Rechtssicherheit und die Gewissheit, dass bei der grenzüberschreitenden Bereitstellung von Diensten und Produkten im Zusammenhang mit KI keine Hindernisse auftauchen. Kunden werden größeres Vertrauen in die von Unternehmen eingesetzte KI haben. Nationale öffentliche Verwaltungen werden vom gestiegenen Vertrauen der Öffentlichkeit in die Verwendung von KI und den gestärkten Durchsetzungsmechanismen profitieren (durch die Einführung eines europäischen Koordinierungsmechanismus, die Bereitstellung angemessener Kapazitäten und die Erleichterung von Audits der KI-Systeme durch neue Anforderungen an die Dokumentation, Rückverfolgbarkeit und Transparenz). Darüber hinaus zielt der Rechtsrahmen auf innovationsspezifische Maßnahmen, beispielsweise Reallabore und konkrete Maßnahmen ab, mit denen Kleinnutzer und Kleinanbieter von Hochrisiko-KI-Systemen darin unterstützt werden, die neuen Vorschriften einzuhalten.

Der Vorschlag zielt zudem speziell auf die Stärkung der europäischen Wettbewerbsfähigkeit und Industriebasis im Bereich der KI ab. Die Kohärenz mit bestehenden sektorspezifischen Unionsvorschriften für KI-Systeme (z. B. für Produkte und Dienste) ist gewährleistet, was zu größerer Klarheit führt und die Durchsetzung der neuen Vorschriften erleichtert.

3.5. Grundrechte

Durch ihre besonderen Merkmale (z. B. Undurchsichtigkeit, Komplexität, Datenabhängigkeit, autonomes Verhalten) kann die Verwendung von KI dazu führen, dass einige der in der EU-Grundrechtecharta (im Folgenden die „Charta“) verankerten Grundrechte verletzt werden. Der Vorschlag zielt darauf ab, diese Grundrechte in hohem Maße zu schützen und durch einen klar festgelegten risikobasierten Ansatz verschiedene Ursachen für Risiken anzugehen. Alle an der Wertschöpfungskette Beteiligten unterliegen einer Reihe von Anforderungen an vertrauenswürdige KI und verhältnismäßigen Pflichten, damit die durch die Charta geschützten Rechte noch stärker geschützt werden: die Würde des Menschen (Artikel 1), die Achtung des Privatlebens und der Schutz personenbezogener Daten (Artikel 7 und 8), die Nichtdiskriminierung (Artikel 21) und die Gleichheit von Frauen und Männern (Artikel 23).

Mit dem Vorschlag soll verhindert werden, dass Menschen davor zurückschrecken, ihr Recht auf Meinungsfreiheit (Artikel 11) und auf Versammlungs- und Vereinigungsfreiheit (Artikel 12) auszuüben, und sichergestellt werden, dass das Recht auf einen wirksamen Rechtsbehelf und ein unparteiisches Gericht und die Unschuldsvermutung und Verteidigungsrechte (Artikel 47 und 48) sowie der allgemeine Grundsatz guter Verwaltung gewahrt werden. Zudem wird sich der Vorschlag in bestimmten Bereichen positiv auf einige gruppenspezifische Rechte auswirken, beispielsweise auf das Recht der Arbeitnehmer auf gerechte und angemessene Arbeitsbedingungen (Artikel 31), den Verbraucherschutz (Artikel 28), die Rechte des Kindes (Artikel 24) und die Integration von Menschen mit Behinderung (Artikel 26). Darüber hinaus geht es um das Recht auf ein hohes Umweltschutzniveau und die Verbesserung der Umweltqualität (Artikel 37), auch in Bezug auf die Gesundheit und Sicherheit von Menschen. Die Verpflichtung zu Vorabtests, Risikomanagement und menschlicher Aufsicht werden die Achtung auch anderer Grundrechte erleichtern, da sich so das Risiko, in kritischen Bereichen wie Bildung, Ausbildung, Beschäftigung, wichtige Dienste, Strafverfolgung und Justiz mithilfe der KI falsche oder verzerrte Entscheidungen zu treffen, verringern lässt. Sollten Grundrechte trotzdem noch verletzt werden, werden die betroffenen Personen die Möglichkeit haben, wirksame Rechtsmittel einzulegen, da für Transparenz und Rückverfolgbarkeit der KI-Systeme im Verbund mit starken Ex-post-Kontrollen gesorgt ist.

Mit dem Vorschlag werden der unternehmerischen Freiheit (Artikel 16) und der Freiheit der Kunst und der Wissenschaft (Artikel 13) einige Beschränkungen auferlegt, um Kohärenz mit der übergeordneten Begründung des öffentlichen Interesses herzustellen. Hierunter fallen beispielsweise Gesundheit, Sicherheit, Verbraucherschutz und der Schutz anderer Grundrechte („verantwortungsvolle Innovation“) bei der Entwicklung und Verwendung von Hochrisiko-KI-Technik. Diese Beschränkungen sind verhältnismäßig und auf das notwendige Minimum beschränkt, um schwerwiegende Sicherheitsrisiken und mögliche Verletzungen der Grundrechte zu verhindern und abzumildern.

Auch die Pflicht zu größerer Transparenz wird das Recht auf Schutz des geistigen Eigentums (Artikel 17 Absatz 2) nicht unverhältnismäßig beeinträchtigen, da sie auf die Mindestinformationen beschränkt ist, die eine Person benötigt, um ihr Recht auf einen wirksamen Rechtsbehelf auszuüben, sowie auf die Transparenz, die Aufsichts- und Durchsetzungsbehörden im Rahmen ihrer Aufgaben benötigen. Jede Offenlegung von Informationen erfolgt unter Einhaltung der einschlägigen Rechtsvorschriften, auch der Richtlinie (EU) 2016/943 über den Schutz vertraulichen Know-hows und vertraulicher Geschäftsinformationen (Geschäftsgeheimnisse) vor rechtswidrigem Erwerb sowie rechtswidriger Nutzung und Offenlegung. Benötigen öffentliche und notifizierte Stellen für die Prüfung der Einhaltung der wesentlichen Pflichten Zugang zu vertraulichen Informationen oder zu Quellcodes, sind sie zur Wahrung der Vertraulichkeit verpflichtet.

4. AUSWIRKUNGEN AUF DEN HAUSHALT

Die Mitgliedstaaten müssen die für die Durchführung der rechtlichen Anforderungen zuständigen Aufsichtsbehörden benennen. Deren Aufsichtsfunktion könnte sich auf bestehende Vereinbarungen stützen, beispielsweise in Bezug auf die Konformitätsbewertungsstellen oder die Marktüberwachung, was jedoch ausreichende technische Kenntnisse sowie personelle und finanzielle Ressourcen erforderlich macht. Abhängig von der in jedem Mitgliedstaat bereits vorhandenen Struktur kann sich dies auf 1 bis 25 Vollzeitäquivalente je Mitgliedstaat belaufen.

Ein detaillierter Überblick über die anfallenden Kosten ist dem Finanzbogen im Anhang zu diesem Vorschlag zu entnehmen.

5. WEITERE ANGABEN

5.1. Durchführungspläne sowie Überwachungs-, Bewertungs- und Berichterstattungsmodalitäten

Damit mit dem Vorschlag dessen konkrete Ziele auch wirksam erreicht werden können, kommt es auf einen robusten Beobachtungs- und Bewertungsmechanismus an. Der Kommission obliegt die Beobachtung der Auswirkungen der vorgeschlagenen Bestimmungen. Sie wird ein System aufbauen, das es ermöglicht, eigenständige Hochrisiko-KI-Anwendungen in einer öffentlichen, unionsweiten Datenbank zu registrieren. Anhand dieser Registrierung werden zuständige Behörden, Nutzer und sonstige Interessierte überprüfen können, ob ein betreffendes Hochrisiko-KI-System die in dem Vorschlag festgelegten Anforderungen erfüllt, und für solche KI-Systeme, die ein hohes Risiko für die Einhaltung der Grundrechte darstellen, kann eine verstärkte Aufsicht ausgeübt werden. KI-Anbieter werden verpflichtet sein, bei ihren Eingaben in diese Datenbank aussagekräftige Angaben zu ihren Systemen und zur für diese Systeme durchgeführten Konformitätsbewertung zu machen.

Zudem werden KI-Anbieter verpflichtet, die nationalen zuständigen Behörden zu informieren, sobald sie Kenntnis über schwerwiegende Vorfälle oder Fehlfunktionen erlangen, die eine Verletzung der Pflicht zur Wahrung der Grundrechte darstellen, sowie über jeden Rückruf oder jede Rücknahme von KI-Systemen vom Markt. Es ist dann Aufgabe der nationalen Behörden, den Vorfall oder die Fehlfunktion zu untersuchen, alle notwendigen Informationen zu sammeln und der Kommission zusammen mit den geeigneten Metadaten zu übermitteln. Die Kommission wird die Informationen zu den Vorfällen durch eine umfassende Analyse des KI-Markts insgesamt ergänzen.

Fünf Jahre nach dem Zeitpunkt, nach dem der vorgeschlagene KI-Rechtsrahmen anwendbar wird, wird die Kommission einen Bericht veröffentlichen, in dem sie den vorgeschlagenen KI-Rechtsrahmen bewertet und überprüft.

5.2. Ausführliche Erläuterung einzelner Bestimmungen des Vorschlags

5.2.1. ANWENDUNGSBEREICH UND BEGRIFFSBESTIMMUNGEN (TITEL I)

Titel I enthält den Gegenstand der Verordnung und den Anwendungsbereich der neuen Vorschriften für das Inverkehrbringen, die Inbetriebnahme und die Verwendung von KI-Systemen. Er enthält auch die Begriffsbestimmungen, die in diesem Rechtsinstrument durchweg verwendet werden. Ziel der in diesem Rechtsrahmen festgelegten Begriffsbestimmung für KI-Systeme ist es, so technologieneutral und zukunftstauglich wie möglich zu sein und den rasanten Entwicklungen in der KI-Technologie und auf dem KI-Markt Rechnung zu tragen. Damit die notwendige Rechtssicherheit gegeben ist, wird Titel I durch Anhang I ergänzt, in dem Konzepte und Techniken für die KI-Entwicklung detailliert aufgeführt sind und von der Kommission in dem Umfang angepasst werden, wie sich neue technologische Entwicklungen ergeben. Im Sinne gleicher Wettbewerbsbedingungen werden auch die wichtigsten Beteiligten über die gesamte KI-Wertschöpfungskette hinweg klar benannt, wie beispielsweise die Anbieter und Nutzer von KI-Systemen, bei denen es sich sowohl um öffentliche als auch um private Akteure handeln kann.

5.2.2. VERBOTENE PRAKTIKEN IM BEREICH DER KÜNSTLICHEN INTELLIGENZ (TITEL II)

Titel II enthält eine Liste verbotener KI-Praktiken. Die Verordnung verfolgt einen risikobasierten Ansatz, bei dem zwischen Anwendungen von KI unterschieden wird, die ein i) unannehmbares Risiko, ii) ein hohes Risiko und iii) ein geringes oder minimales Risiko darstellen. Die Aufstellung der verbotenen Praktiken in Titel II umfasst alle KI-Systeme, die als unannehmbar gelten, weil sie Werte der Union, beispielsweise Grundrechte, verletzen. Die Verbote gelten für Praktiken, die ein erhebliches Potenzial haben, Personen zu manipulieren, indem sie auf Techniken zur unterschwelligen Beeinflussung zurückgreifen, die von diesen Personen nicht bewusst wahrgenommen werden, oder die die Schwächen bestimmter schutzbedürftiger Gruppen wie Kinder oder Personen mit Behinderungen ausnutzen, um deren Verhalten massiv so zu beeinflussen, dass sie selbst oder eine andere Person psychisch oder physisch geschädigt werden könnten. Andere manipulative oder ausbeuterische Praktiken, die Erwachsene betreffen und möglicherweise durch KI-Systeme erleichtert werden, könnten unter die bestehenden Rechtsvorschriften für den Datenschutz, Verbraucherschutz und digitale Dienste fallen, auf deren Grundlage natürliche Personen Anspruch auf angemessene Informationen haben und es ihnen freisteht, Profiling- oder andere Praktiken, die Einfluss auf ihr Verhalten haben könnten, abzulehnen. Der Vorschlag sieht auch vor, die Bewertung des sozialen Verhaltens für allgemeine Zwecke mithilfe von KI durch öffentliche Behörden („Social Scoring“) zu verbieten. Schließlich soll der Einsatz von biometrischen Echtzeit-Fernidentifizierungssystemen in öffentlich zugänglichen Räumen für die Zwecke der Strafverfolgung bis auf wenige Ausnahmen verboten werden.

5.2.3. HOCHRISIKO-KI-SYSTEME (TITEL III)

Titel III enthält spezifische Vorschriften für KI-Systeme, die ein hohes Risiko für die Gesundheit und Sicherheit oder für die Grundrechte natürlicher Personen darstellen. Entsprechend dem risikobasierten Ansatz sind solche Hochrisiko-KI-Systeme auf dem europäischen Markt zugelassen, sofern sie bestimmten zwingend vorgeschriebenen Anforderungen genügen und vorab eine Konformitätsbewertung durchgeführt wird. Die Einstufung als Hochrisiko-KI-System beruht auf der Zweckbestimmung des KI-Systems entsprechend den bestehenden EU-Produktsicherheitsvorschriften. Damit hängt die Einstufung als Hochrisiko-KI-System nicht nur von der Funktion dieses Systems ab, sondern auch von seinem konkreten Zweck und seinen Anwendungsmodalitäten.

In Titel III Kapitel 1 sind die Einstufungsregeln angegeben und zwei Hauptkategorien für Hochrisiko-KI-Systeme festgelegt:

- KI-Systeme, die als Sicherheitskomponenten von Produkten, die einer Vorab-Konformitätsbewertung durch Dritte unterliegen, verwendet werden sollen;
- sonstige eigenständige KI-Systeme, die ausdrücklich in Anhang III genannt werden und sich vor allem auf die Grundrechte auswirken.

Die in Anhang III aufgeführte Liste der Hochrisiko-KI-Systeme enthält einige KI-Systeme, bei denen sich bereits gezeigt hat oder bei denen absehbar ist, dass die Risiken tatsächlich eintreten. Damit die Verordnung an neue Verwendungszwecke und Anwendungen von KI angepasst werden kann, hat die Kommission die Möglichkeit, die Liste der Hochrisiko-KI-Systeme, die in bestimmten festgelegten Bereichen verwendet werden, mithilfe einer Reihe von Kriterien und einer Methodik für die Risikoabschätzung auszuweiten.

In Kapitel 2 ist festgelegt, welche rechtlichen Anforderungen Hochrisiko-KI-Systeme in Bezug auf Daten, Daten-Governance, Dokumentation und das Führen von Aufzeichnungen, Transparenz und Bereitstellung von Informationen für die Nutzer, menschliche Aufsicht,

Robustheit, Genauigkeit und Sicherheit erfüllen müssen. Die vorgeschlagenen Mindestanforderungen, die sich aus den von über 350 Organisationen[29] erprobten Ethik-Leitlinien der HEG[30] ableiten, sind bereits gängige Praxis für viele gewissenhaften Akteure und das Ergebnis der Vorarbeiten der letzten zwei Jahre. Sie stimmen auch weitestgehend mit anderen internationalen Empfehlungen und Grundsätzen überein, wodurch sichergestellt wird, dass der vorgeschlagene KI-Rahmen mit den Vorgaben übereinstimmt, die von den internationalen Handelspartnern der EU festgelegt wurden. Es liegt im Ermessen des Anbieters des jeweiligen KI-Systems, mit welchen technischen Lösungen er die Einhaltung dieser Anforderungen konkret erreicht – sei es durch Normen oder sonstige technische Spezifikationen oder durch andere Entwicklungen entsprechend dem allgemeinen wissenschaftlich-technischen Know-how. Diese Flexibilität ist besonders wichtig, denn sie ermöglicht es den Anbietern von KI-Systemen, unter Berücksichtigung des Stands der Technik und des wissenschaftlich-technischen Fortschritts auf dem Gebiet selbst zu entscheiden, wie sie die für sie geltenden Anforderungen zu erfüllen beabsichtigen.

Kapitel 3 enthält eine Reihe klarer horizontaler Pflichten für Anbieter von Hochrisiko-KI-Systemen. Auch für Nutzer und andere Beteiligte entlang der KI-Wertschöpfungskette (z. B. Einführer, Händler, Bevollmächtigte) gelten verhältnismäßige Pflichten.

Kapitel 4 bildet den Rahmen für die Einbeziehung notifizierter Stellen als unabhängige Dritte in die Konformitätsbewertungsverfahren, während in Kapitel 5 die je nach Art des Hochrisiko-KI-Systems einzuhaltenden Konformitätsbewertungsverfahren im Einzelnen erläutert werden. Mit dem Konzept der Konformitätsbewertung sollen die Belastungen für die Wirtschaftsakteure und notifizierten Stellen, deren Kapazität mit der Zeit schrittweise hochgefahren werden muss, möglichst gering gehalten werden. KI-Systeme, die als Sicherheitskomponenten von Produkten eingesetzt werden sollen, die unter die einschlägigen Rechtsvorschriften des neuen Rechtsrahmens fallen (z. B. Maschinen, Spielzeug, medizinische Geräte), unterliegen denselben Ex-ante- und Ex-post-Mechanismen für die Rechtsbefolgung und Durchsetzung wie das Produkt, dessen Komponente sie sind. Der wesentliche Unterschied liegt darin, dass die Ex-ante- und Ex-post-Mechanismen nicht nur die Einhaltung der durch sektorspezifische Vorschriften vorgegebenen Anforderungen gewährleisten, sondern auch die Einhaltung der in dieser Verordnung festgelegten Anforderungen.

Für die eigenständigen Hochrisiko-KI-Systeme, auf die in Anhang III verwiesen wird, wird ein neues Rechtsbefolgungs- und Durchsetzungssystem festgelegt. Dies entspricht dem Muster des neuen Rechtsrahmens, bei dem die einschlägigen Rechtsvorschriften durch interne Kontrollprüfungen des Anbieters umgesetzt werden. Ausgenommen hiervon sind die biometrischen Fernidentifizierungssysteme, die einer Konformitätsbewertung durch Dritte unterliegen. Eine umfassende Ex-ante-Konformitätsbewertung mittels interner Prüfungen könnte in Kombination mit einer soliden Ex-post-Durchsetzung eine wirksame und sinnvolle Lösung für solche Systeme darstellen, zumal sich die Regulierung noch in der Anfangsphase befindet und in dem äußerst innovativen KI-Sektor Auditing-Erfahrungen erst jetzt gesammelt werden. Damit eigenständige Hochrisiko-KI-Systeme mittels interner Prüfungen bewertet werden können, muss die Einhaltung aller Anforderungen der Verordnung vorab vollständig, wirkungsvoll und sorgfältig dokumentiert werden, ferner gilt es, robuste Qualitäts- und Risikomanagementsysteme zu befolgen und eine Beobachtung nach dem Inverkehrbringen zu

[29] Sie wurden auch von der Kommission in ihrer Mitteilung aus dem Jahr 2019 zu einem auf den Menschen ausgerichteten Ansatz für KI gebilligt.

[30] Hochrangige Expertengruppe für künstliche Intelligenz, *Ethics Guidelines for Trustworthy AI* (Ethik-Leitlinien für eine vertrauenswürdige KI), 2019.

gewährleisten. Sobald ein Anbieter die jeweilige Konformitätsbewertung durchgeführt hat, sollte er diese eigenständigen Hochrisiko-KI-Systeme in eine von der Kommission verwaltete EU-Datenbank eintragen, um so die Transparenz gegenüber der Öffentlichkeit zu erhöhen und die Aufsicht sowie die Ex-post-Überwachung durch die zuständigen Behörden zu stärken. Aus Gründen der Kohärenz mit den bestehenden Produktsicherheitsvorschriften wird bei KI-Systemen, bei denen es sich um Sicherheitskomponenten von Produkten handelt, hingegen das System der Konformitätsbewertungsverfahren durch Dritte verfolgt, das sich bereits im Rahmen der einschlägigen sektorspezifischen Produktsicherheitsvorschriften bewährt hat. Bei wesentlichen Änderungen der KI-Systeme (vor allem bei Änderungen, die über die Festlegungen des Anbieters in seiner technischen Dokumentation sowie über das hinausgehen, was zum Zeitpunkt der Ex-ante-Konformitätsbewertung geprüft wurde), muss vorab eine erneute Konformitätsbewertung durchgeführt werden.

5.2.4. TRANSPARENZPFLICHTEN FÜR BESTIMMTE KI-SYSTEME (TITEL VI)

Titel IV befasst sich mit spezifischen Manipulationsrisiken bestimmter KI-Systeme. Transparenzpflichten gelten für Systeme, die i) mit Menschen interagieren, ii) zur Erkennung von Emotionen oder zur Assoziierung (gesellschaftlicher) Kategorien anhand biometrischer Daten eingesetzt werden oder iii) Inhalte erzeugen oder manipulieren („Deepfakes“). Interagieren Personen mit KI-Systemen oder werden deren Emotionen oder Merkmale durch automatisierte Mittel erkannt, müssen die Menschen hierüber informiert werden. Wird ein KI-System eingesetzt, um Bild-, Audio- oder Video-Inhalte zu erzeugen oder zu manipulieren, sodass sie von authentischen Inhalten kaum zu unterscheiden sind, sollte, abgesehen von legitimen Zwecken (wie Strafverfolgung, Meinungsfreiheit), die Pflicht zur Offenlegung der Tatsache vorgeschrieben werden, dass der Inhalt durch automatisierte Mittel erzeugt wurde. So können bewusste Entscheidungen getroffen oder bestimmte Situationen vermieden werden.

5.2.5. MAßNAHMEN ZUR INNOVATIONSFÖRDERUNG (TITEL V)

Titel V wurde im Hinblick auf das Ziel aufgenommen, einen innovationsfreundlichen, zukunftstauglichen und widerstandsfähigen Rechtsrahmen zu schaffen. Hierzu werden die nationalen zuständigen Behörden aufgefordert, Reallabore einzurichten und die grundlegenden Bedingungen für die Leitung, Aufsicht und Haftung festzulegen. KI-Reallabore bieten, auf der Grundlage eines mit den zuständigen Behörden vereinbarten Testplans, für eine begrenzte Zeit kontrollierte Testumgebungen für innovative Technologien. Titel V enthält zudem Maßnahmen zur Reduzierung des Verwaltungsaufwands für KMU und Start-ups.

5.2.6. LEITUNG UND DURCHFÜHRUNG (TITEL VI, VII UND VII)

Titel VI enthält Vorgaben für die Leitungsstrukturen auf Unionsebene und nationaler Ebene. Der Vorschlag sieht die Einrichtung eines Europäischen Ausschusses für künstliche Intelligenz (im Folgenden der „Ausschuss“) auf Unionsebene vor, der sich aus Vertretern der Mitgliedstaaten und der Kommission zusammensetzt. Der Ausschuss soll zu einer wirksamen Zusammenarbeit der nationalen Aufsichtsbehörden und der Kommission beitragen und so eine reibungslose, wirksame und harmonisierte Durchführung dieser Verordnung erleichtern und darüber hinaus die Kommission fachlich beraten. Ferner soll der Ausschuss bewährte Verfahrensweise aus den Mitgliedstaaten sammeln und weitergeben.

Auf nationaler Ebene werden die Mitgliedstaaten eine oder mehrere nationale zuständige Behörden (darunter die nationale Aufsichtsbehörde) benennen müssen, die die Anwendung und Durchführung der Verordnung überwachen. Der Europäische Datenschutzbeauftragte gilt

als zuständige Behörde für die Aufsicht über die Organe, Einrichtungen und sonstigen Stellen der Union, die in den Anwendungsbereich dieser Verordnung fallen.

Titel VII soll durch die Einrichtung einer unionsweiten Datenbank für eigenständige Hochrisiko-KI-Systeme, die sich vor allem auf die Grundrechte auswirken, der Kommission und den nationalen Behörden die Beobachtungsaufgaben erleichtern. Die Datenbank wird von der Kommission betrieben. Gespeist wird sie durch die Anbieter der KI-Systeme, die ihre Systeme registrieren müssen, bevor sie sie in Verkehr bringen oder anderweitig in Betrieb nehmen können.

Titel VIII enthält die Beobachtungs- und Meldepflichten für die Anbieter von KI-Systemen im Hinblick auf die Beobachtung nach dem Inverkehrbringen sowie die Meldung und Untersuchung von Vorfällen und Fehlfunktionen im KI-Zusammenhang. Auch die Marktüberwachungsbehörden werden den Markt kontrollieren und die Einhaltung der mit allen bereits in Verkehr gebrachten Hochrisiko-KI-Systemen verbundenen Pflichten und Anforderungen prüfen. Die Marktüberwachungsbehörden werden mit allen in der Verordnung (EU) 2019/1020 über die Marktüberwachung festgelegten Befugnissen ausgestattet. Die Ex-post-Durchsetzung soll sicherstellen, dass öffentliche Behörden über die Befugnisse und Ressourcen verfügen, damit sie, eingreifen können, sollten sich bei bereits in Verkehr gebrachten KI-Systemen unerwartete Risiken ergeben, die ein rasches Handeln erfordern. Darüber hinaus werden sie darauf achten, dass die Akteure ihren in der Verordnung festgelegten Pflichten nachkommen. Der Vorschlag sieht nicht die automatische Schaffung weiterer Gremien oder Behörden auf Ebene der Mitgliedstaaten vor. Die Mitgliedstaaten können sich daher auf bereits vorhandene sektorspezifische Behörden und deren Fachkenntnisse stützen, denen die Befugnisse zur Beobachtung und Durchsetzung der Bestimmungen dieser Verordnung übertragen werden.

All dies geschieht unbeschadet der in den Mitgliedstaaten bereits vorhandenen Systeme und Zuweisung von Befugnissen für die Ex-post-Durchsetzung der Pflichten in Bezug auf die Grundrechte. Sofern dies für die Wahrnehmung ihrer Aufgaben notwendig ist, werden die bestehenden Aufsichts- und Durchsetzungsbehörden auch befugt sein, Unterlagen, die auf der Grundlage dieser Verordnung aufbewahrt werden, anzufordern oder Zugang zu diesen Unterlagen zu erhalten, sowie gegebenenfalls Marktüberwachungsbehörden aufzufordern, das Hochrisiko-KI-System mit technischen Mitteln zu prüfen.

5.2.7. VERHALTENSKODIZES (TITEL IX)

Titel IX enthält die Grundlagen zur Schaffung von Verhaltenskodizes, die Anbietern von KI-Systemen, die kein hohes Risiko darstellen, Anreize geben sollen, die zwingend vorgeschriebenen Anforderungen an Hochrisiko-KI-Systeme (nach Titel III) freiwillig anzuwenden. Anbieter von KI-Systemen, die kein hohes Risiko darstellen, können selbst Verhaltenskodizes festlegen und umsetzen. Diese Kodizes können auch freiwillige Verpflichtungen beispielsweise im Hinblick auf die ökologische Nachhaltigkeit, den Zugang für Personen mit Behinderungen, die Beteiligung von Interessenträgern an Entwurf und Entwicklung von KI-Systemen sowie die Diversität des Entwicklungsteams enthalten.

5.2.8. SCHLUSSBESTIMMUNGEN (TITEL X, XI UND XII)

Titel X unterstreicht, dass alle Parteien verpflichtet sind, die Vertraulichkeit der Informationen und Daten zu wahren, und enthält Vorschriften für den Austausch von während der Durchführung der Verordnung erworbenen Informationen. Titel X enthält auch Maßnahmen, mit denen durch wirksame, verhältnismäßige und abschreckende Strafen bei Verstößen gegen die Bestimmungen eine effiziente Durchführung der Verordnung gewährleistet werden soll.

Titel XI enthält die Regeln für die Ausübung der Befugnisübertragung und der Durchführungsbefugnisse. Der Vorschlag sieht vor, dass der Kommission die Befugnis übertragen wird, zur Gewährleistung einer einheitlichen Anwendung der Verordnung gegebenenfalls Durchführungsrechtsakte oder zur Aktualisierung oder Ergänzung der Listen in den Anhängen I bis VII delegierte Rechtsakte zu erlassen.

Titel XII enthält die Pflicht der Kommission, regelmäßig zu bewerten, ob Anhang III aktualisiert werden muss, und regelmäßig Berichte über die Bewertung und Überprüfung der Verordnung vorzulegen. Der Titel enthält zudem die Schlussbestimmungen, einschließlich einer differenzierten Übergangsfrist mit Blick auf das Datum, ab dem die Verordnung Anwendung findet, um allen Parteien eine reibungslose Durchführung zu erleichtern.

2021/0106 (COD)

Vorschlag für eine

VERORDNUNG DES EUROPÄISCHEN PARLAMENTS UND DES RATES

ZUR FESTLEGUNG HARMONISIERTER VORSCHRIFTEN FÜR KÜNSTLICHE INTELLIGENZ (GESETZ ÜBER KÜNSTLICHE INTELLIGENZ) UND ZUR ÄNDERUNG BESTIMMTER RECHTSAKTE DER UNION

DAS EUROPÄISCHE PARLAMENT UND DER RAT DER EUROPÄISCHEN UNION -

gestützt auf den Vertrag über die Arbeitsweise der Europäischen Union, insbesondere auf die Artikel 16 und 114,

auf Vorschlag der Europäischen Kommission,

nach Zuleitung des Entwurfs des Gesetzgebungsakts an die nationalen Parlamente,

nach Stellungnahme des Europäischen Wirtschafts- und Sozialausschusses[31],

nach Stellungnahme des Ausschusses der Regionen[32],

gemäß dem ordentlichen Gesetzgebungsverfahren,

in Erwägung nachstehender Gründe:

(1) Zweck dieser Verordnung ist es, das Funktionieren des Binnenmarkts zu verbessern, indem ein einheitlicher Rechtsrahmen insbesondere für die Entwicklung, Vermarktung und Verwendung künstlicher Intelligenz im Einklang mit den Werten der Union festgelegt wird. Diese Verordnung beruht auf einer Reihe von zwingenden Gründen des Allgemeininteresses, wie einem hohen Schutz der Gesundheit, der Sicherheit und der Grundrechte, und gewährleistet den grenzüberschreitenden freien Verkehr KI-gestützter Waren und Dienstleistungen, wodurch verhindert wird, dass die Mitgliedstaaten die Entwicklung, Vermarktung und Verwendung von KI-Systemen beschränken, sofern dies nicht ausdrücklich durch diese Verordnung erlaubt wird.

(2) Systeme der künstlichen Intelligenz (KI-Systeme) können problemlos in verschiedenen Bereichen der Wirtschaft und Gesellschaft, auch grenzüberschreitend, eingesetzt werden und in der gesamten Union verkehren. Einige Mitgliedstaaten haben bereits die Verabschiedung nationaler Vorschriften in Erwägung gezogen, damit künstliche Intelligenz sicher ist und unter Einhaltung der Grundrechte entwickelt und verwendet wird. Unterschiedliche nationale Vorschriften können zu einer Fragmentierung des Binnenmarkts führen und würden die Rechtssicherheit für Akteure, die KI-Systeme entwickeln oder verwenden, beeinträchtigen. Daher sollte in der gesamten Union ein einheitlich hohes Schutzniveau sichergestellt werden, wobei Unterschiede, die den freien Verkehr von KI-Systemen und damit zusammenhängenden Produkten und Dienstleistungen im Binnenmarkt behindern, vermieden werden sollten, indem den Akteuren einheitliche Verpflichtungen auferlegt werden und der gleiche Schutz der zwingenden Gründe des Allgemeininteresses und

[31] ABl. C […] vom […], S. […].
[32] ABl. C […] vom […], S. […].

der Rechte von Personen im gesamten Binnenmarkt auf der Grundlage des Artikels 114 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV) gewährleistet wird. Soweit diese Verordnung konkrete Vorschriften zum Schutz von Privatpersonen im Hinblick auf die Verarbeitung personenbezogener Daten enthält, mit denen vor allem die Verwendung von KI-Systemen zur biometrischen Echtzeit-Fernidentifizierung in öffentlich zugänglichen Räumen zu Strafverfolgungszwecken eingeschränkt wird, sollte sich diese Verordnung in Bezug auf diese konkreten Vorschriften auch auf Artikel 16 AEUV stützen. Angesichts dieser konkreten Vorschriften und des Rückgriffs auf Artikel 16 AEUV ist es angezeigt, den Europäischen Datenschutzausschuss zu konsultieren.

(3) Künstliche Intelligenz bezeichnet eine Reihe von Technologien, die sich rasant entwickeln und zu vielfältigem Nutzen für Wirtschaft und Gesellschaft über das gesamte Spektrum industrieller und gesellschaftlicher Aktivitäten hinweg beitragen können. Durch die Verbesserung der Vorhersage, Optimierung der Abläufe, Ressourcenzuweisung und Personalisierung digitaler Lösungen, die Einzelpersonen und Organisationen zur Verfügung stehen, kann die Verwendung künstlicher Intelligenz den Unternehmen wesentliche Wettbewerbsvorteile verschaffen und zu guten Ergebnissen für Gesellschaft und Umwelt führen, beispielsweise in den Bereichen Gesundheitsversorgung, Landwirtschaft, allgemeine und berufliche Bildung, Infrastrukturmanagement, Energie, Verkehr und Logistik, öffentliche Dienstleistungen, Sicherheit, Justiz, Ressourcen- und Energieeffizienz sowie Klimaschutz und Anpassung an den Klimawandel.

(4) Gleichzeitig kann künstliche Intelligenz je nach den Umständen ihrer konkreten Anwendung und Nutzung Risiken mit sich bringen und öffentliche Interessen und Rechte schädigen, die durch das Unionsrecht geschützt sind. Ein solcher Schaden kann materieller oder immaterieller Art sein.

(5) Daher ist ein Rechtsrahmen der Union mit harmonisierten Vorschriften für künstliche Intelligenz erforderlich, um die Entwicklung, Verwendung und Verbreitung künstlicher Intelligenz im Binnenmarkt zu fördern und gleichzeitig einen hohen Schutz öffentlicher Interessen wie Gesundheit und Sicherheit und den Schutz der durch das Unionsrecht anerkannten und geschützten Grundrechte zu gewährleisten. Zur Umsetzung dieses Ziels sollten Vorschriften für das Inverkehrbringen und die Inbetriebnahme bestimmter KI-Systeme festgelegt werden, um das reibungslose Funktionieren des Binnenmarkts zu gewährleisten, sodass diesen Systemen der Grundsatz des freien Waren- und Dienstleistungsverkehrs zugutekommen kann. Durch die Festlegung dieser Vorschriften unterstützt die Verordnung das vom Europäischen Rat[33] formulierte Ziel der Union, bei der Entwicklung einer sicheren, vertrauenswürdigen und ethisch vertretbaren künstlichen Intelligenz weltweit eine Führungsrolle einzunehmen, und sorgt für den vom Europäischen Parlament[34] ausdrücklich geforderten Schutz von Ethikgrundsätzen.

(6) Der Begriff „KI-System“ sollte klar definiert werden, um Rechtssicherheit zu gewährleisten und gleichzeitig genügend Flexibilität zu bieten, um künftigen technologischen Entwicklungen Rechnung zu tragen. Die Begriffsbestimmung sollte

[33] Europäischer Rat, Außerordentliche Tagung des Europäischen Rates (1. und 2. Oktober 2020) – Schlussfolgerungen, EUCO 13/20, 2020, S. 6.

[34] Entschließung des Europäischen Parlaments vom 20. Oktober 2020 mit Empfehlungen an die Kommission zu dem Rahmen für die ethischen Aspekte von künstlicher Intelligenz, Robotik und damit zusammenhängenden Technologien, 2020/2012 (INL).

auf den wesentlichen funktionalen Merkmalen der Software beruhen, insbesondere darauf, dass sie im Hinblick auf eine Reihe von Zielen, die vom Menschen festgelegt werden, Ergebnisse wie Inhalte, Vorhersagen, Empfehlungen oder Entscheidungen hervorbringen kann, die das Umfeld beeinflussen, mit dem sie interagieren, sei es physisch oder digital. KI-Systeme können so konzipiert sein, dass sie mit verschiedenen Graden der Autonomie arbeiten und eigenständig oder als Bestandteil eines Produkts verwendet werden können, unabhängig davon, ob das System physisch in das Produkt integriert ist (eingebettet) oder der Funktion des Produkts dient, ohne darin integriert zu sein (nicht eingebettet). Die Bestimmung des Begriffs „KI-System" sollte durch eine Liste spezifischer Techniken und Konzepte für seine Entwicklung ergänzt werden, die im Lichte der Marktentwicklungen und der technischen Entwicklungen auf dem neuesten Stand gehalten werden sollte, indem die Kommission delegierte Rechtsakte zur Änderung dieser Liste erlässt.

(7) Der in dieser Verordnung verwendete Begriff „biometrische Daten" steht im Einklang mit dem Begriff „biometrische Daten" im Sinne von Artikel 4 Nummer 14 der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates[35], Artikel 3 Nummer 18 der Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates[36] und Artikel 3 Nummer 13 der Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates[37] und sollte im Einklang damit ausgelegt werden.

(8) Der in dieser Verordnung verwendete Begriff „biometrisches Fernidentifizierungssystem" sollte funktional definiert werden als KI-System, das dem Zweck dient, natürliche Personen aus der Ferne durch Abgleich der biometrischen Daten einer Person mit den in einer Referenzdatenbank gespeicherten biometrischen Daten zu identifizieren, ohne dass der Nutzer des KI-Systems vorher weiß, ob die Person anwesend sein wird und identifiziert werden kann, und unabhängig davon, welche Technik, Verfahren oder Arten biometrischer Daten dazu verwendet werden. Angesichts ihrer unterschiedlichen Merkmale und Einsatzformen sowie der unterschiedlichen Risiken, die mit ihnen verbunden sind, sollte zwischen biometrischen Echtzeit-Fernidentifizierungssystemen und Systemen zur nachträglichen biometrischen Fernidentifizierung unterschieden werden. Bei „Echtzeit-Systemen" erfolgen die Erfassung der biometrischen Daten, der Abgleich und die Identifizierung unverzüglich, zeitnah oder auf jeden Fall ohne erhebliche Verzögerung. In diesem Zusammenhang sollte es keinen Spielraum für eine Umgehung der Bestimmungen dieser Verordnung über die „Echtzeit-Nutzung" der betreffenden KI-Systeme geben, indem kleinere Verzögerungen vorgesehen werden.

---

35 Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (ABl. L 119 vom 4.5.2016, S. 1).

36 Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates vom 23. Oktober 2018 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen und sonstigen Stellen der Union, zum freien Datenverkehr und zur Aufhebung der Verordnung (EG) Nr. 45/2001 und des Beschlusses Nr. 1247/2002/EG (ABl. L 295 vom 21.11.2018, S. 39).

37 Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates (Richtlinie zum Datenschutz bei der Strafverfolgung) (ABl. L 119 vom 4.5.2016, S. 89).

„Echtzeit-Systeme“ umfassen die Verwendung von „Live-Material“ oder „Near-live-Material“ wie Videoaufnahmen, die von einer Kamera oder einem anderen Gerät mit ähnlicher Funktion erzeugt werden. Bei Systemen zur nachträglichen Identifizierung hingegen wurden die biometrischen Daten schon zuvor erfasst und der Abgleich und die Identifizierung erfolgen erst mit erheblicher Verzögerung. Dabei handelt es sich um Material wie Bild- oder Videoaufnahmen, die von Video-Überwachungssystemen oder privaten Geräten vor der Anwendung des KI-Systems auf die betroffenen natürlichen Personen erzeugt wurden.

(9) Für die Zwecke dieser Verordnung sollte der Begriff „öffentlich zugänglicher Raum“ so verstanden werden, dass er sich auf einen der Öffentlichkeit zugänglichen physischen Ort bezieht, unabhängig davon, ob sich der betreffende Ort in privatem oder öffentlichem Eigentum befindet. Daher erfasst der Begriff keine privaten Orte, wie Privathäuser, private Clubs, Büros, Lager und Fabriken, die normalerweise für Dritte, einschließlich Strafverfolgungsbehörden, nicht frei zugänglich sind, es sei denn, diese wurden ausdrücklich eingeladen oder ihr Zugang ausdrücklich erlaubt. Auch Online-Räume werden nicht erfasst, da es sich nicht um physische Räume handelt. Die bloße Tatsache, dass bestimmte Bedingungen für den Zugang zu einem bestimmten Raum gelten können, wie Eintrittskarten oder Altersbeschränkungen, bedeutet jedoch nicht, dass der Raum im Sinne dieser Verordnung nicht öffentlich zugänglich ist. Folglich sind neben öffentlichen Räumen wie Straßen, relevanten Teilen von Regierungsgebäuden und den meisten Verkehrsinfrastrukturen auch Bereiche wie Kinos, Theater, Geschäfte und Einkaufszentren in der Regel öffentlich zugänglich. Ob ein bestimmter Raum öffentlich zugänglich ist, sollte jedoch von Fall zu Fall unter Berücksichtigung der Besonderheiten der jeweiligen individuellen Situation entschieden werden.

(10) Um gleiche Wettbewerbsbedingungen und einen wirksamen Schutz der Rechte und Freiheiten natürlicher Personen in der gesamten Union zu gewährleisten, sollten die in dieser Verordnung festgelegten Vorschriften in nichtdiskriminierender Weise für Anbieter von KI-Systemen – unabhängig davon, ob sie in der Union oder in einem Drittland niedergelassen sind – und für Nutzer von KI-Systemen, die in der Union ansässig oder niedergelassen sind, gelten.

(11) Angesichts ihres digitalen Charakters sollten bestimmte KI-Systeme in den Anwendungsbereich dieser Verordnung fallen, selbst wenn sie in der Union weder in Verkehr gebracht noch in Betrieb genommen oder verwendet werden. Dies ist beispielsweise der Fall, wenn ein in der Union ansässiger oder niedergelassener Akteur bestimmte Dienstleistungen an einen außerhalb der Union ansässigen oder niedergelassenen Akteur im Zusammenhang mit einer Tätigkeit vergibt, die von einem KI-System ausgeübt werden soll, das als hochriskant einzustufen wäre und sich auf in der Union ansässige natürliche Personen auswirken würde. Unter diesen Umständen könnte das von dem Akteur außerhalb der Union betriebene KI-System Daten verarbeiten, die rechtmäßig in der Union erhoben und aus der Union übertragen wurden, und sodann dem vertraglichen Akteur in der Union die aus dieser Verarbeitung resultierenden Ergebnisse dieses KI-Systems liefern, ohne dass dieses KI-System dabei in der Union in Verkehr gebracht, in Betrieb genommen oder verwendet wird. Um die Umgehung dieser Verordnung zu verhindern und einen wirksamen Schutz in der Union ansässiger natürlicher Personen zu gewährleisten, sollte diese Verordnung auch für Anbieter und Nutzer von KI-Systemen gelten, die in einem Drittland ansässig oder niedergelassen sind, soweit die von diesen Systemen erzeugten Ergebnisse in der Union verwendet werden. Um jedoch bestehenden

Vereinbarungen und besonderen Erfordernissen für die Zusammenarbeit mit ausländischen Partnern, mit denen Informationen und Beweismittel ausgetauscht werden, Rechnung zu tragen, sollte diese Verordnung nicht für Behörden eines Drittlands und internationale Organisationen gelten, wenn sie im Rahmen internationaler Übereinkünfte tätig werden, die auf nationaler oder europäischer Ebene für die Zusammenarbeit mit der Union oder ihren Mitgliedstaaten im Bereich der Strafverfolgung und der justiziellen Zusammenarbeit geschlossen wurden. Solche Übereinkünfte wurden bilateral zwischen Mitgliedstaaten und Drittstaaten oder zwischen der Europäischen Union, Europol und anderen EU-Agenturen einerseits und Drittstaaten und internationalen Organisationen andererseits geschlossen.

(12) Diese Verordnung sollte auch für Organe, Einrichtungen und sonstige Stellen der Union gelten, wenn sie als Anbieter oder Nutzer eines KI-Systems auftreten. KI-Systeme, die ausschließlich für militärische Zwecke entwickelt oder verwendet werden, sollten vom Anwendungsbereich dieser Verordnung ausgenommen werden, wenn diese Verwendung in den ausschließlichen Zuständigkeitsbereich der Gemeinsamen Außen- und Sicherheitspolitik fällt, der in Titel V des Vertrags über die Europäische Union (EUV) geregelt ist. Diese Verordnung sollte die Bestimmungen über die Verantwortlichkeit der Vermittler in der Richtlinie 2000/31/EG des Europäischen Parlaments und des Rates [in der durch das Gesetz über digitale Dienste geänderten Fassung] unberührt lassen.

(13) Um einen einheitlichen und hohen Schutz öffentlicher Interessen im Hinblick auf die Gesundheit und Sicherheit sowie die Grundrechte zu gewährleisten, werden für alle Hochrisiko-KI-Systeme gemeinsame Normen vorgeschlagen. Diese Normen sollten mit der Charta der Grundrechte der Europäischen Union (im Folgenden die „Charta“) im Einklang stehen, nichtdiskriminierend sein und mit den internationalen Handelsverpflichtungen der Union vereinbar sein.

(14) Um ein verhältnismäßiges und wirksames verbindliches Regelwerk für KI-Systeme einzuführen, sollte ein klar definierter risikobasierter Ansatz verfolgt werden. Bei diesem Ansatz sollten Art und Inhalt solcher Vorschriften auf die Intensität und den Umfang der Risiken zugeschnitten werden, die von KI-Systemen ausgehen können. Es ist daher notwendig, bestimmte Praktiken im Bereich der künstlichen Intelligenz zu verbieten und Anforderungen an Hochrisiko-KI-Systeme und Verpflichtungen für die betreffenden Akteure sowie Transparenzpflichten für bestimmte KI-Systeme festzulegen.

(15) Abgesehen von den zahlreichen nutzbringenden Verwendungsmöglichkeiten künstlicher Intelligenz kann diese Technik auch missbraucht werden und neue und wirkungsvolle Instrumente für manipulative, ausbeuterische und soziale Kontrollpraktiken bieten. Solche Praktiken sind besonders schädlich und sollten verboten werden, weil sie im Widerspruch zu den Werten der Union stehen, nämlich der Achtung der Menschenwürde, Freiheit, Gleichheit, Demokratie und Rechtsstaatlichkeit sowie der Grundrechte in der Union, einschließlich des Rechts auf Nichtdiskriminierung, Datenschutz und Privatsphäre sowie der Rechte des Kindes.

(16) Das Inverkehrbringen, die Inbetriebnahme oder die Verwendung bestimmter KI-Systeme, die dazu bestimmt sind, menschliches Verhalten nachteilig zu beeinflussen, und die zu physischen oder psychischen Schäden führen dürften, sollte verboten werden. Solche KI-Systeme setzen auf eine vom Einzelnen nicht zu erkennende unterschwellige Beeinflussung oder sollen die Schutzbedürftigkeit von Kindern und anderen aufgrund ihres Alters oder ihrer körperlichen oder geistigen Behinderung

beeinträchtigten Personen ausnutzen. Dies geschieht mit der Absicht, das Verhalten einer Person wesentlich zu beeinflussen, und zwar in einer Weise, die dieser oder einer anderen Person Schaden zufügt oder zufügen kann. Diese Absicht kann nicht vermutet werden, wenn die nachteilige Beeinflussung des menschlichen Verhaltens auf Faktoren zurückzuführen ist, die nicht Teil des KI-Systems sind und außerhalb der Kontrolle des Anbieters oder Nutzers liegen. Forschung zu legitimen Zwecken im Zusammenhang mit solchen KI-Systemen sollte durch das Verbot nicht unterdrückt werden, wenn diese Forschung nicht auf eine Verwendung des KI-Systems in Beziehungen zwischen Mensch und Maschine hinausläuft, durch die natürliche Personen geschädigt werden, und wenn diese Forschung im Einklang mit anerkannten ethischen Standards für die wissenschaftliche Forschung durchgeführt wird.

(17) KI-Systeme, die von Behörden oder in deren Auftrag das soziale Verhalten natürlicher Personen für allgemeine Zwecke bewerten, können zu diskriminierenden Ergebnissen und zur Ausgrenzung bestimmter Gruppen führen. Sie können die Menschenwürde und das Recht auf Nichtdiskriminierung sowie die Werte der Gleichheit und Gerechtigkeit verletzen. Solche KI-Systeme bewerten oder klassifizieren die Vertrauenswürdigkeit natürlicher Personen auf der Grundlage ihres sozialen Verhaltens in verschiedenen Zusammenhängen oder aufgrund bekannter oder vorhergesagter persönlicher Eigenschaften oder Persönlichkeitsmerkmale. Die aus solchen KI-Systemen erzielte soziale Bewertung kann zu einer Schlechterstellung oder Benachteiligung bestimmter natürlicher Personen oder ganzer Gruppen natürlicher Personen in sozialen Zusammenhängen, die in keinem Zusammenhang zu den Umständen stehen, unter denen die Daten ursprünglich erzeugt oder erfasst wurden, oder zu einer Schlechterstellung in einer Weise führen, die im Hinblick auf ihr soziales Verhalten oder dessen Tragweite ungerechtfertigt oder unverhältnismäßig ist. Solche KI-Systeme sollten daher verboten werden.

(18) Die Verwendung von KI-Systemen zur biometrischen Echtzeit-Fernidentifizierung natürlicher Personen in öffentlich zugänglichen Räumen zu Strafverfolgungszwecken gilt als besonders in die Rechte und Freiheiten der betroffenen Personen eingreifend, da sie die Privatsphäre eines großen Teils der Bevölkerung beeinträchtigt, ein Gefühl der ständigen Überwachung weckt und indirekt von der Ausübung der Versammlungsfreiheit und anderer Grundrechte abhalten kann. Darüber hinaus bergen die Unmittelbarkeit der Auswirkungen und die begrenzten Möglichkeiten weiterer Kontrollen oder Korrekturen im Zusammenhang mit der Verwendung solcher in Echtzeit betriebener Systeme erhöhte Risiken für die Rechte und Freiheiten der Personen, die von Strafverfolgungsmaßnahmen betroffen sind.

(19) Die Verwendung solcher Systeme zu Strafverfolgungszwecken sollte daher untersagt werden, außer in drei erschöpfend aufgeführten und eng abgegrenzten Fällen, in denen die Verwendung unbedingt erforderlich ist, um einem erheblichen öffentlichen Interesse zu dienen, dessen Bedeutung die Risiken überwiegt. Zu diesen Fällen gehört die Suche nach potenziellen Opfern von Straftaten, einschließlich vermisster Kinder, bestimmte Gefahren für das Leben oder die körperliche Unversehrtheit natürlicher Personen oder die Gefahr eines Terroranschlags sowie das Erkennen, Aufspüren, Identifizieren oder Verfolgen von Tätern oder Verdächtigen von Straftaten im Sinne des Rahmenbeschlusses 2002/584/JI des Rates[38], sofern diese Straftaten in dem betreffenden Mitgliedstaat nach dessen Recht mit einer Freiheitsstrafe oder einer

[38] Rahmenbeschluss 2002/584/JI des Rates vom 13. Juni 2002 über den Europäischen Haftbefehl und die Übergabeverfahren zwischen den Mitgliedstaaten (ABl. L 190 vom 18.7.2002, S. 1).

freiheitsentziehenden Maßregel der Sicherung im Höchstmaß von mindestens drei Jahren bedroht sind. Eine solche Schwelle für eine Freiheitsstrafe oder eine freiheitsentziehende Maßregel der Sicherung nach nationalem Recht trägt dazu bei sicherzustellen, dass die Straftat schwerwiegend genug ist, um den Einsatz biometrischer Echtzeit-Fernidentifizierungssysteme zu rechtfertigen. Darüber hinaus sind einige der 32 im Rahmenbeschluss 2002/584/JI des Rates aufgeführten Straftaten in der Praxis eher relevant als andere, da der Rückgriff auf die biometrische Echtzeit-Fernidentifizierung für die konkrete Erkennung, Aufspürung, Identifizierung oder Verfolgung eines Täters oder Verdächtigen einer der verschiedenen aufgeführten Straftaten voraussichtlich in äußerst unterschiedlichem Maße erforderlich und verhältnismäßig sein wird und da dabei die wahrscheinlichen Unterschiede in Schwere, Wahrscheinlichkeit und Ausmaß des Schadens oder möglicher negativer Folgen zu berücksichtigen sind.

(20) Um sicherzustellen, dass diese Systeme verantwortungsvoll und verhältnismäßig genutzt werden, ist es auch wichtig, festzulegen, dass in jedem dieser drei erschöpfend aufgeführten und eng abgegrenzten Fälle bestimmte Elemente berücksichtigt werden sollten, insbesondere in Bezug auf die Art des dem Antrag zugrunde liegenden Falls und die Auswirkungen der Verwendung auf die Rechte und Freiheiten aller betroffenen Personen sowie auf die für die Verwendung geltenden Schutzvorkehrungen und Bedingungen. Darüber hinaus sollte die Verwendung biometrischer Echtzeit-Fernidentifizierungssysteme in öffentlich zugänglichen Räumen für die Zwecke der Strafverfolgung angemessenen zeitlichen und räumlichen Beschränkungen unterliegen, wobei insbesondere den Beweisen oder Hinweisen in Bezug auf die Bedrohungen, die Opfer oder den Täter Rechnung zu tragen ist. Die Personenreferenzdatenbank sollte für jeden Anwendungsfall in jeder der drei oben genannten Situationen geeignet sein.

(21) Jede Verwendung biometrischer Echtzeit-Fernidentifizierungssysteme in öffentlich zugänglichen Räumen zu Strafverfolgungszwecken sollte einer ausdrücklichen spezifischen Genehmigung durch eine Justizbehörde oder eine unabhängige Verwaltungsbehörde eines Mitgliedstaats unterliegen. Eine solche Genehmigung sollte grundsätzlich vor der Verwendung eingeholt werden, außer in hinreichend begründeten dringenden Fällen, d. h. in Situationen, in denen es wegen der Notwendigkeit der Verwendung der betreffenden Systeme tatsächlich und objektiv unmöglich ist, vor dem Beginn der Verwendung eine Genehmigung einzuholen. In solchen dringenden Fällen sollte die Verwendung auf das absolut notwendige Mindestmaß beschränkt werden und angemessenen Schutzvorkehrungen und Bedingungen unterliegen, die im nationalen Recht festgelegt sind und im Zusammenhang mit jedem einzelnen dringenden Anwendungsfall von der Strafverfolgungsbehörde selbst präzisiert werden. Darüber hinaus sollte die Strafverfolgungsbehörde in solchen Situationen versuchen, so bald wie möglich eine Genehmigung einzuholen, wobei sie begründen sollte, warum sie diese nicht früher beantragen konnte.

(22) Darüber hinaus sollte innerhalb des durch diese Verordnung vorgegebenen erschöpfenden Rahmens festgelegt werden, dass eine solche Verwendung im Hoheitsgebiet eines Mitgliedstaats im Einklang mit dieser Verordnung nur möglich sein sollte, sofern der betreffende Mitgliedstaat in seinen detaillierten nationalen Rechtsvorschriften ausdrücklich vorgesehen hat, dass eine solche Verwendung genehmigt werden kann. Folglich steht es den Mitgliedstaaten im Rahmen dieser Verordnung frei, eine solche Möglichkeit generell oder nur in Bezug auf einige der in

dieser Verordnung genannten Ziele, für die eine genehmigte Verwendung gerechtfertigt sein kann, vorzusehen.

(23) Die Verwendung von KI-Systemen zur biometrischen Echtzeit-Fernidentifizierung natürlicher Personen in öffentlich zugänglichen Räumen zu Strafverfolgungszwecken erfordert zwangsläufig die Verarbeitung biometrischer Daten. Die Vorschriften dieser Verordnung, die vorbehaltlich bestimmter Ausnahmen eine solche Verwendung auf der Grundlage von Artikel 16 AEUV verbieten, sollten als *Lex specialis* in Bezug auf die in Artikel 10 der Richtlinie (EU) 2016/680 enthaltenen Vorschriften über die Verarbeitung biometrischer Daten gelten und somit die Verwendung und Verarbeitung der betreffenden biometrischen Daten umfassend regeln. Eine solche Verwendung und Verarbeitung sollte daher nur möglich sein, soweit sie mit dem in dieser Verordnung festgelegten Rahmen vereinbar ist, ohne dass es den zuständigen Behörden bei ihren Tätigkeiten zu Strafverfolgungszwecken Raum lässt, außerhalb dieses Rahmens solche Systeme zu verwenden und die damit verbundenen Daten aus den in Artikel 10 der Richtlinie (EU) 2016/680 aufgeführten Gründen zu verarbeiten. In diesem Zusammenhang soll diese Verordnung nicht als Rechtsgrundlage für die Verarbeitung personenbezogener Daten gemäß Artikel 8 der Richtlinie (EU) 2016/680 dienen. Die Verwendung biometrischer Echtzeit-Fernidentifizierungssysteme in öffentlich zugänglichen Räumen zu anderen Zwecken als der Strafverfolgung, auch durch zuständige Behörden, sollte jedoch nicht unter den in dieser Verordnung festgelegten spezifischen Rahmen für diese Verwendung zu Strafverfolgungszwecken fallen. Eine solche Verwendung zu anderen Zwecken als der Strafverfolgung sollte daher nicht der Genehmigungspflicht gemäß dieser Verordnung und der zu ihrer Durchführung anwendbaren detaillierten nationalen Rechtsvorschriften unterliegen.

(24) Jede Verarbeitung biometrischer Daten und anderer personenbezogener Daten im Zusammenhang mit der Verwendung von KI-Systemen für die biometrische Identifizierung, ausgenommen im Zusammenhang mit der Verwendung biometrischer Echtzeit-Fernidentifizierungssysteme in öffentlich zugänglichen Räumen zu Strafverfolgungszwecken im Sinne dieser Verordnung, einschließlich der Fälle, in denen diese Systeme von den zuständigen Behörden in öffentlich zugänglichen Räumen zu anderen Zwecken als der Strafverfolgung genutzt werden, sollte weiterhin allen Anforderungen genügen, die sich gegebenenfalls aus Artikel 9 Absatz 1 der Verordnung (EU) 2016/679, Artikel 10 Absatz 1 der Verordnung (EU) 2018/1725 und Artikel 10 der Richtlinie (EU) 2016/680 ergeben.

(25) Nach Artikel 6a des dem EUV und dem AEUV beigefügten Protokolls Nr. 21 über die Position des Vereinigten Königreichs und Irlands hinsichtlich des Raums der Freiheit, der Sicherheit und des Rechts sind die auf der Grundlage des Artikels 16 AEUV festgelegten Vorschriften in Artikel 5 Absatz 1 Buchstabe d und Artikel 5 Absätze 2 und 3 dieser Verordnung in Bezug auf die Verarbeitung personenbezogener Daten durch die Mitgliedstaaten im Rahmen der Ausübung von Tätigkeiten, die in den Anwendungsbereich des Dritten Teils Titel V Kapitel 4 und 5 AEUV fallen, für Irland nicht bindend, wenn Irland nicht durch die Vorschriften gebunden ist, die die Formen der justiziellen Zusammenarbeit in Strafsachen oder der polizeilichen Zusammenarbeit regeln, in deren Rahmen die auf der Grundlage des Artikels 16 AEUV festgelegten Vorschriften eingehalten werden müssen.

(26) Nach den Artikeln 2 und 2a des dem EUV und dem AEUV beigefügten Protokolls Nr. 22 über die Position Dänemarks ist Dänemark durch die auf der Grundlage des Artikels 16 AEUV festgelegten Vorschriften in Artikel 5 Absatz 1 Buchstabe d und Artikel 5 Absätze 2 und 3 dieser Verordnung in Bezug auf die Verarbeitung

personenbezogener Daten durch die Mitgliedstaaten im Rahmen der Ausübung von Tätigkeiten, die in den Anwendungsbereich des Dritten Teils Titel V Kapitel 4 und 5 AEUV fallen, weder gebunden noch zu ihrer Anwendung verpflichtet.

(27) Hochrisiko-KI-Systeme sollten nur dann auf dem Unionsmarkt in Verkehr gebracht oder in Betrieb genommen werden, wenn sie bestimmte verbindliche Anforderungen erfüllen. Mit diesen Anforderungen sollte sichergestellt werden, dass Hochrisiko-KI-Systeme, die in der Union verfügbar sind oder deren Ergebnisse anderweitig in der Union verwendet werden, keine unannehmbaren Risiken für wichtige öffentliche Interessen der Union bergen, wie sie im Unionsrecht anerkannt und geschützt sind. Als hochriskant sollten nur solche KI-Systeme eingestuft werden, die erhebliche schädliche Auswirkungen auf die Gesundheit, die Sicherheit und die Grundrechte von Personen in der Union haben; etwaige mögliche Beschränkungen des internationalen Handels, die sich daraus ergeben, sollten so gering wie möglich bleiben.

(28) KI-Systeme könnten negative Auswirkungen auf die Gesundheit und Sicherheit von Personen haben, insbesondere wenn solche Systeme als Komponenten von Produkten zum Einsatz kommen. Im Einklang mit den Zielen der Harmonisierungsrechtsvorschriften der Union, die den freien Verkehr von Produkten im Binnenmarkt erleichtern und gewährleisten sollen, dass nur sichere und anderweitig konforme Produkte auf den Markt gelangen, ist es wichtig, dass die Sicherheitsrisiken, die ein Produkt als Ganzes aufgrund seiner digitalen Komponenten, einschließlich KI-Systeme, mit sich bringen kann, angemessen vermieden und gemindert werden. So sollten beispielsweise zunehmend autonome Roboter – sei es in der Fertigung oder in der persönlichen Assistenz und Pflege – in der Lage sein, sicher zu arbeiten und ihre Funktionen in komplexen Umgebungen zu erfüllen. Desgleichen sollten die immer ausgefeilteren Diagnosesysteme und Systeme zur Unterstützung menschlicher Entscheidungen im Gesundheitssektor, in dem die Risiken für Leib und Leben besonders hoch sind, zuverlässig und genau sein. Das Ausmaß der negativen Auswirkungen des KI-Systems auf die durch die Charta geschützten Grundrechte ist bei der Einstufung eines KI-Systems als hochriskant von besonderer Bedeutung. Zu diesen Rechten gehören die Würde des Menschen, die Achtung des Privat- und Familienlebens, der Schutz personenbezogener Daten, die Freiheit der Meinungsäußerung und die Informationsfreiheit, die Versammlungs- und Vereinigungsfreiheit, die Nichtdiskriminierung, der Verbraucherschutz, die Arbeitnehmerrechte, die Rechte von Menschen mit Behinderungen, das Recht auf einen wirksamen Rechtsbehelf und ein unparteiisches Gericht, die Unschuldsvermutung und das Verteidigungsrecht sowie das Recht auf eine gute Verwaltung. Es muss betont werden, dass Kinder – zusätzlich zu diesen Rechten – über spezifische Rechte verfügen, wie sie in Artikel 24 der EU-Charta und im Übereinkommen der Vereinten Nationen über die Rechte des Kindes (UNCRC) (im Hinblick auf das digitale Umfeld weiter ausgeführt in der Allgemeinen Bemerkung Nr. 25 des UNCRC) verankert sind; in beiden wird die Berücksichtigung der Schutzbedürftigkeit der Kinder gefordert und ihr Anspruch auf den Schutz und die Fürsorge festgelegt, die für ihr Wohlergehen notwendig sind. Darüber hinaus sollte dem Grundrecht auf ein hohes Umweltschutzniveau, das in der Charta verankert ist und mit der Unionspolitik umgesetzt wird, bei der Bewertung der Schwere des Schadens, den ein KI-System u. a. in Bezug auf die Gesundheit und Sicherheit von Menschen verursachen kann, ebenfalls Rechnung getragen werden.

(29) In Bezug auf Hochrisiko-KI-Systeme, bei denen es sich um Sicherheitskomponenten von Produkten oder Systemen oder selbst um Produkte oder Systeme handelt, die in

den Anwendungsbereich der Verordnung (EG) Nr. 300/2008 des Europäischen Parlaments und des Rates[39], der Verordnung (EU) Nr. 167/2013 des Europäischen Parlaments und des Rates[40], der Verordnung (EU) Nr. 168/2013 des Europäischen Parlaments und des Rates[41], der Richtlinie 2014/90/EU des Europäischen Parlaments und des Rates[42], der Richtlinie (EU) 2016/797 des Europäischen Parlaments und des Rates[43], der Verordnung (EU) 2018/858 des Europäischen Parlaments und des Rates[44], der Verordnung (EU) 2018/1139 des Europäischen Parlaments und des Rates[45] und der Verordnung (EU) 2019/2144 des Europäischen Parlaments und des Rates[46] fallen, ist es angezeigt, diese Rechtsakte zu ändern, damit die Kommission – aufbauend auf den technischen und regulatorischen Besonderheiten des jeweiligen Sektors und ohne Beeinträchtigung bestehender Governance-, Konformitätsbewertungs- und Durchsetzungsmechanismen sowie der darin eingerichteten Behörden – beim Erlass von etwaigen künftigen delegierten Rechtsakten oder Durchführungsrechtsakten auf der Grundlage der genannten Rechtsakte die in der vorliegenden Verordnung festgelegten verbindlichen Anforderungen an Hochrisiko-KI-Systeme berücksichtigt.

(30) In Bezug auf KI-Systeme, bei denen es sich um Sicherheitskomponenten von Produkten oder selbst um Produkte handelt, die unter bestimmte

---

39 Verordnung (EG) Nr. 300/2008 des Europäischen Parlaments und des Rates vom 11. März 2008 über gemeinsame Vorschriften für die Sicherheit in der Zivilluftfahrt und zur Aufhebung der Verordnung (EG) Nr. 2320/2002 (ABl. L 97 vom 9.4.2008, S. 72).

40 Verordnung (EU) Nr. 167/2013 des Europäischen Parlaments und des Rates vom 5. Februar 2013 über die Genehmigung und Marktüberwachung von land- und forstwirtschaftlichen Fahrzeugen (ABl. L 60 vom 2.3.2013, S. 1).

41 Verordnung (EU) Nr. 168/2013 des Europäischen Parlaments und des Rates vom 15. Januar 2013 über die Genehmigung und Marktüberwachung von zwei- oder dreirädrigen und vierrädrigen Fahrzeugen (ABl. L 60 vom 2.3.2013, S. 52).

42 Richtlinie 2014/90/EU des Europäischen Parlaments und des Rates vom 23. Juli 2014 über Schiffsausrüstung und zur Aufhebung der Richtlinie 96/98/EG des Rates (ABl. L 257 vom 28.8.2014, S. 146).

43 Richtlinie (EU) 2016/797 des Europäischen Parlaments und des Rates vom 11. Mai 2016 über die Interoperabilität des Eisenbahnsystems in der Europäischen Union (ABl. L 138 vom 26.5.2016, S. 44).

44 Verordnung (EU) 2018/858 des Europäischen Parlaments und des Rates vom 30. Mai 2018 über die Genehmigung und die Marktüberwachung von Kraftfahrzeugen und Kraftfahrzeuganhängern sowie von Systemen, Bauteilen und selbstständigen technischen Einheiten für diese Fahrzeuge, zur Änderung der Verordnungen (EG) Nr. 715/2007 und (EG) Nr. 595/2009 und zur Aufhebung der Richtlinie 2007/46/EG (ABl. L 151 vom 14.6.2018, S. 1).

45 Verordnung (EU) 2018/1139 des Europäischen Parlaments und des Rates vom 4. Juli 2018 zur Festlegung gemeinsamer Vorschriften für die Zivilluftfahrt und zur Errichtung einer Agentur der Europäischen Union für Flugsicherheit sowie zur Änderung der Verordnungen (EG) Nr. 2111/2005, (EG) Nr. 1008/2008, (EU) Nr. 996/2010, (EU) Nr. 376/2014 und der Richtlinien 2014/30/EU und 2014/53/EU des Europäischen Parlaments und des Rates, und zur Aufhebung der Verordnungen (EG) Nr. 552/2004 und (EG) Nr. 216/2008 des Europäischen Parlaments und des Rates und der Verordnung (EWG) Nr. 3922/91 des Rates (ABl. L 212 vom 22.8.2018, S. 1).

46 Verordnung (EU) 2019/2144 des Europäischen Parlaments und des Rates vom 27. November 2019 über die Typgenehmigung von Kraftfahrzeugen und Kraftfahrzeuganhängern sowie von Systemen, Bauteilen und selbstständigen technischen Einheiten für diese Fahrzeuge im Hinblick auf ihre allgemeine Sicherheit und den Schutz der Fahrzeuginsassen und von ungeschützten Verkehrsteilnehmern, zur Änderung der Verordnung (EU) 2018/858 des Europäischen Parlaments und des Rates und zur Aufhebung der Verordnungen (EG) Nr. 78/2009, (EG) Nr. 79/2009 und (EG) Nr. 661/2009 des Europäischen Parlaments und des Rates sowie der Verordnungen (EG) Nr. 631/2009, (EU) Nr. 406/2010, (EU) Nr. 672/2010, (EU) Nr. 1003/2010, (EU) Nr. 1005/2010, (EU) Nr. 1008/2010, (EU) Nr. 1009/2010, (EU) Nr. 19/2011, (EU) Nr. 109/2011, (EU) Nr. 458/2011, (EU) Nr. 65/2012, (EU) Nr. 130/2012, (EU) Nr. 347/2012, (EU) Nr. 351/2012, (EU) Nr. 1230/2012 und (EU) 2015/166 der Kommission (ABl. L 325 vom 16.12.2019, S. 1).

Harmonisierungsrechtsvorschriften der Union fallen, ist es angezeigt, sie im Rahmen dieser Verordnung als hochriskant einzustufen, wenn das betreffende Produkt gemäß den einschlägigen Harmonisierungsrechtsvorschriften der Union dem Konformitätsbewertungsverfahren durch eine als unabhängige Dritte auftretende Konformitätsbewertungsstelle unterzogen wird. Dabei handelt es sich insbesondere um Produkte wie Maschinen, Spielzeuge, Aufzüge, Geräte und Schutzsysteme zur bestimmungsgemäßen Verwendung in explosionsgefährdeten Bereichen, Funkanlagen, Druckgeräte, Sportbootausrüstung, Seilbahnen, Geräte zur Verbrennung gasförmiger Brennstoffe, Medizinprodukte und In-vitro-Diagnostika.

(31) Die Einstufung eines KI-Systems als hochriskant gemäß dieser Verordnung sollte nicht zwangsläufig bedeuten, dass von dem Produkt, dessen Sicherheitskomponente das KI-System ist, oder dem KI-System als Produkt selbst nach den Kriterien der einschlägigen Harmonisierungsrechtsvorschriften der Union für das betreffende Produkt ein hohes Risiko ausgeht. Dies betrifft insbesondere die Verordnung (EU) 2017/745 des Europäischen Parlaments und des Rates[47] und die Verordnung (EU) 2017/746 des Europäischen Parlaments und des Rates[48], in denen für Produkte, die ein mittleres und hohes Risiko bergen, eine Konformitätsbewertung durch Dritte vorgesehen ist.

(32) Bei eigenständigen KI-Systemen, d. h. Hochrisiko-KI-Systemen, bei denen es sich um andere Systeme als Sicherheitskomponenten von Produkten handelt oder die selbst Produkte sind, ist es angezeigt, sie als hochriskant einzustufen, wenn sie aufgrund ihrer Zweckbestimmung ein hohes Risiko bergen, die Gesundheit und Sicherheit oder die Grundrechte von Personen zu schädigen, wobei sowohl die Schwere des möglichen Schadens als auch die Wahrscheinlichkeit seines Auftretens zu berücksichtigen sind, und sofern sie in einer Reihe von Bereichen verwendet werden, die in der Verordnung ausdrücklich festgelegt sind. Die Bestimmung dieser Systeme erfolgt nach derselben Methode und denselben Kriterien, die auch für künftige Änderungen der Liste der Hochrisiko-KI-Systeme vorgesehen sind.

(33) Technische Ungenauigkeiten von KI-Systemen, die für die biometrische Fernidentifizierung natürlicher Personen bestimmt sind, können zu verzerrten Ergebnissen führen und eine diskriminierende Wirkung haben. Dies ist von besonderer Bedeutung, wenn es um das Alter, die ethnische Herkunft, das Geschlecht oder Behinderungen geht. Daher sollten biometrische Echtzeit-Fernidentifizierungssysteme und Systeme zur nachträglichen biometrischen Fernidentifizierung als hochriskant eingestuft werden. Angesichts der mit ihnen verbundenen Risiken sollten für beide Arten von biometrischen Fernidentifizierungssystemen besondere Anforderungen im Hinblick auf die Protokollierungsfunktionen und die menschliche Aufsicht gelten.

(34) Was die Verwaltung und den Betrieb kritischer Infrastrukturen anbelangt, so sollten KI-Systeme, die als Sicherheitskomponenten für das Management und den Betrieb des Straßenverkehrs sowie für die Wasser-, Gas-, Wärme- und Stromversorgung verwendet werden sollen, als hochriskant eingestuft werden, da ihr Ausfall oder ihre

---

[47] Verordnung (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 117 vom 5.5.2017, S. 1).

[48] Verordnung (EU) 2017/746 des Europäischen Parlaments und des Rates vom 5. April 2017 über In-vitro-Diagnostika und zur Aufhebung der Richtlinie 98/79/EG und des Beschlusses 2010/227/EU der Kommission (ABl. L 117 vom 5.5.2017, S. 176).

Störung in großem Umfang das Leben und die Gesundheit von Menschen gefährden und zu erheblichen Störungen bei der normalen Durchführung sozialer und wirtschaftlicher Tätigkeiten führen kann.

(35) KI-Systeme, die in der allgemeinen oder beruflichen Bildung eingesetzt werden, insbesondere um den Zugang von Personen zu Bildungs- und Berufsbildungseinrichtungen oder ihrer Zuordnung dazu zu bestimmen oder um Personen im Rahmen von Prüfungen als Teil ihrer Ausbildung oder als Voraussetzung dafür zu bewerten, sollten als hochriskant angesehen werden, da sie über den Verlauf der Bildung und des Berufslebens einer Person entscheiden und daher ihre Fähigkeit beeinträchtigen können, ihren Lebensunterhalt zu sichern. Bei unsachgemäßer Konzeption und Verwendung können solche Systeme das Recht auf allgemeine und berufliche Bildung sowie das Recht auf Nichtdiskriminierung verletzen und historische Diskriminierungsmuster fortschreiben.

(36) KI-Systeme, die in den Bereichen Beschäftigung, Personalmanagement und Zugang zur Selbstständigkeit eingesetzt werden, insbesondere für die Einstellung und Auswahl von Personen, für Entscheidungen über Beförderung und Kündigung sowie für die Zuweisung, Überwachung oder Bewertung von Personen in Arbeitsvertragsverhältnissen, sollten ebenfalls als hochriskant eingestuft werden, da diese Systeme die künftigen Karriereaussichten und die Lebensgrundlagen dieser Personen spürbar beeinflussen können. Einschlägige Arbeitsvertragsverhältnisse sollten Beschäftigte und Personen erfassen, die Dienstleistungen über Plattformen erbringen, auf die im Arbeitsprogramm der Kommission für 2021 Bezug genommen wird. Solche Personen sollten grundsätzlich nicht als Nutzer im Sinne dieser Verordnung gelten. Solche Systeme können während des gesamten Einstellungsverfahrens und bei der Bewertung, Beförderung oder Nichtbeförderung von Personen in Arbeitsvertragsverhältnissen historische Diskriminierungsmuster fortschreiben, beispielsweise gegenüber Frauen, bestimmten Altersgruppen und Menschen mit Behinderungen oder Personen mit einer bestimmten rassischen oder ethnischen Herkunft oder sexuellen Ausrichtung. KI-Systeme zur Überwachung der Leistung und des Verhaltens dieser Personen können sich auch auf ihre Rechte auf Datenschutz und Privatsphäre auswirken.

(37) Ein weiterer Bereich, in dem der Einsatz von KI-Systemen besondere Aufmerksamkeit verdient, ist der Zugang zu und die Nutzung von bestimmten grundlegenden privaten und öffentlichen Diensten und Leistungen, die erforderlich sind, damit die Menschen uneingeschränkt an der Gesellschaft teilhaben oder ihren Lebensstandard verbessern können. Insbesondere KI-Systeme, die zur Kreditpunktebewertung oder zur Bewertung der Kreditwürdigkeit natürlicher Personen verwendet werden, sollten als Hochrisiko-KI-Systeme eingestuft werden, da sie den Zugang dieser Personen zu Finanzmitteln oder wesentlichen Dienstleistungen wie Wohnraum, Elektrizität und Telekommunikationsdienstleistungen bestimmen. KI-Systeme, die zu diesem Zweck eingesetzt werden, können zur Diskriminierung von Personen oder Gruppen führen und historische Diskriminierungsmuster, beispielsweise aufgrund der rassischen oder ethnischen Herkunft, einer Behinderung, des Alters oder der sexuellen Ausrichtung, fortschreiben oder neue Formen von Diskriminierung mit sich bringen. Angesichts des sehr begrenzten Auswirkungen und der auf dem Markt verfügbaren Alternativen ist es angezeigt, KI-Systeme zur Kreditwürdigkeitsprüfung und Kreditpunktebewertung auszunehmen, wenn sie von kleinen Anbietern für den Eigenbedarf in Betrieb genommen werden. Natürliche Personen, die staatliche Unterstützungsleistungen und -dienste von Behörden beantragen oder erhalten, sind in der Regel von diesen

Leistungen und Diensten abhängig und befinden sich gegenüber den zuständigen Behörden in einer prekären Lage. Wenn KI-Systeme eingesetzt werden, um zu bestimmen, ob solche Leistungen und Dienste von den Behörden verweigert, gekürzt, widerrufen oder zurückgefordert werden sollten, können sie erhebliche Auswirkungen auf die Existenzgrundlage der Menschen haben und ihre Grundrechte wie das Recht auf sozialen Schutz, Nichtdiskriminierung, Menschenwürde oder einen wirksamen Rechtsbehelf verletzen. Solche Systeme sollten daher als hochriskant eingestuft werden. Dennoch sollte diese Verordnung die Entwicklung und Anwendung innovativer Ansätze in der öffentlichen Verwaltung nicht behindern, die von einer breiteren Verwendung konformer und sicherer KI-Systeme profitieren würde, sofern diese Systeme kein hohes Risiko für juristische und natürliche Personen bergen. Schließlich sollten KI-Systeme, die bei der Entsendung oder der Priorisierung der Entsendung von Rettungsdiensten eingesetzt werden, ebenfalls als hochriskant eingestuft werden, da sie in für das Leben und die Gesundheit von Personen und für ihr Eigentum sehr kritischen Situationen Entscheidungen treffen.

(38) Maßnahmen von Strafverfolgungsbehörden im Zusammenhang mit bestimmten Verwendungen von KI-Systemen sind durch ein erhebliches Machtungleichgewicht gekennzeichnet und können zur Überwachung, Festnahme oder zum Entzug der Freiheit einer natürlichen Person sowie zu anderen nachteiligen Auswirkungen auf die in der Charta verankerten Grundrechte führen. Insbesondere wenn das KI-System nicht mit hochwertigen Daten trainiert wird, die Anforderungen an seine Genauigkeit oder Robustheit nicht erfüllt werden oder das System nicht ordnungsgemäß konzipiert und getestet wird, bevor es in Verkehr gebracht oder in anderer Weise in Betrieb genommen wird, kann es Personen in diskriminierender oder anderweitig falscher oder ungerechter Weise ausgrenzen. Darüber hinaus könnte die Ausübung wichtiger verfahrensrechtlicher Grundrechte wie des Rechts auf einen wirksamen Rechtsbehelf und ein unparteiisches Gericht sowie die Unschuldsvermutung und Verteidigungsrechte behindert werden, insbesondere wenn solche KI-Systeme nicht hinreichend transparent, erklärbar und dokumentiert sind. Daher ist es angezeigt, eine Reihe von KI-Systemen, die im Rahmen der Strafverfolgung eingesetzt werden sollen und bei denen Genauigkeit, Zuverlässigkeit und Transparenz besonders wichtig sind, als hochriskant einzustufen, um nachteilige Auswirkungen zu vermeiden, das Vertrauen der Öffentlichkeit zu erhalten und die Rechenschaftspflicht und einen wirksamen Rechtsschutz zu gewährleisten. Angesichts der Art der betreffenden Tätigkeiten und der damit verbundenen Risiken sollten diese Hochrisiko-KI-Systeme insbesondere KI-Systeme umfassen, die von Strafverfolgungsbehörden für individuelle Risikobewertungen, als Lügendetektoren und ähnliche Instrumente oder zur Ermittlung des emotionalen Zustands natürlicher Personen, zur Aufdeckung von „Deepfakes“, zur Bewertung der Zuverlässigkeit von Beweismitteln in Strafverfahren, zur Vorhersage des Auftretens oder erneuten Auftretens einer tatsächlichen oder potenziellen Straftat auf der Grundlage des Profils natürlicher Personen oder zur Bewertung von Persönlichkeitsmerkmalen und Eigenschaften oder vergangenen kriminellen Verhaltens von natürlichen Personen oder Gruppen, zur Erstellung eines Profils während der Aufdeckung, Untersuchung oder strafrechtlichen Verfolgung einer Straftat sowie zur Kriminalanalyse in Bezug auf natürliche Personen eingesetzt werden. KI-Systeme, die speziell für Verwaltungsverfahren in Steuer- und Zollbehörden bestimmt sind, sollten nicht als Hochrisiko-KI-Systeme gelten, die von Strafverfolgungsbehörden zum Zwecke der Verhütung, Aufdeckung, Untersuchung und strafrechtlichen Verfolgung von Straftaten eingesetzt werden.

(39) KI-Systeme, die in den Bereichen Migration, Asyl und Grenzkontrolle eingesetzt werden, betreffen Menschen, die sich häufig in einer besonders prekären Lage befinden und vom Ergebnis der Maßnahmen der zuständigen Behörden abhängig sind. Die Genauigkeit, der nichtdiskriminierende Charakter und die Transparenz der KI-Systeme, die in solchen Zusammenhängen eingesetzt werden, sind daher besonders wichtig, um die Achtung der Grundrechte der betroffenen Personen, insbesondere ihrer Rechte auf Freizügigkeit, Nichtdiskriminierung, den Schutz des Privatlebens und personenbezogener Daten, den internationalen Schutz und die gute Verwaltung, zu gewährleisten. Daher ist es angezeigt, KI-Systeme als hochriskant einzustufen, die von den zuständigen mit Aufgaben in den Bereichen Migration, Asyl und Grenzkontrolle betrauten Behörden für Folgendes eingesetzt werden: als Lügendetektoren und ähnliche Instrumente oder zur Ermittlung des emotionalen Zustand einer natürlichen Person; zur Bewertung bestimmter Risiken, die von natürlichen Personen ausgehen, die in das Hoheitsgebiet eines Mitgliedstaats einreisen oder ein Visum oder Asyl beantragen; zur Überprüfung der Echtheit der einschlägigen Dokumente natürlicher Personen; zur Unterstützung der zuständigen Behörden bei der Prüfung von Asyl- und Visumanträgen sowie Aufenthaltstiteln und damit verbundenen Beschwerden im Hinblick darauf, die Berechtigung der den Antrag stellenden natürlichen Personen festzustellen. KI-Systeme im Bereich Migration, Asyl und Grenzkontrolle, die unter diese Verordnung fallen, sollten den einschlägigen Verfahrensvorschriften der Richtlinie 2013/32/EU des Europäischen Parlaments und des Rates[49], der Verordnung (EG) Nr. 810/2009 des Europäischen Parlaments und des Rates[50] und anderen einschlägigen Rechtsvorschriften entsprechen.

(40) Bestimmte KI-Systeme, die für die Rechtspflege und demokratische Prozesse bestimmt sind, sollten angesichts ihrer möglichen erheblichen Auswirkungen auf die Demokratie, die Rechtsstaatlichkeit, die individuellen Freiheiten sowie das Recht auf einen wirksamen Rechtsbehelf und ein unparteiisches Gericht als hochriskant eingestuft werden. Um insbesondere den Risiken möglicher Verzerrungen, Fehler und Undurchsichtigkeiten zu begegnen, sollten KI-Systeme, die Justizbehörden dabei helfen sollen, Sachverhalte und Rechtsvorschriften zu ermitteln und auszulegen und das Recht auf konkrete Sachverhalte anzuwenden, als hochriskant eingestuft werden. Diese Einstufung sollte sich jedoch nicht auf KI-Systeme erstrecken, die für rein begleitende Verwaltungstätigkeiten bestimmt sind, die die tatsächliche Rechtspflege in Einzelfällen nicht beeinträchtigen, wie die Anonymisierung oder Pseudonymisierung gerichtlicher Urteile, Dokumente oder Daten, die Kommunikation zwischen dem Personal, Verwaltungsaufgaben oder die Zuweisung von Ressourcen.

(41) Die Tatsache, dass ein KI-System gemäß dieser Verordnung als hochriskant eingestuft wird, sollte nicht dahingehend ausgelegt werden, dass die Verwendung des Systems nach anderen Rechtsakten der Union oder nach nationalen Rechtsvorschriften, die mit dem Unionsrecht vereinbar sind, zwangsläufig rechtmäßig ist, beispielsweise in Bezug auf den Schutz personenbezogener Daten, die Verwendung von Lügendetektoren und ähnlichen Instrumenten oder anderen Systemen zur Ermittlung des emotionalen Zustand einer natürlichen Person. Eine solche Verwendung sollte weiterhin

[49] Richtlinie 2013/32/EU des Europäischen Parlaments und des Rates vom 26. Juni 2013 zu gemeinsamen Verfahren für die Zuerkennung und Aberkennung des internationalen Schutzes (ABl. L 180 vom 29.6.2013, S. 60).

[50] Verordnung (EG) Nr. 810/2009 des Europäischen Parlaments und des Rates vom 13. Juli 2009 über einen Visakodex der Gemeinschaft (Visakodex) (ABl. L 243 vom 15.9.2009, S. 1).

ausschließlich im Einklang mit den geltenden Anforderungen erfolgen, die sich aus der Charta, dem anwendbaren Sekundärrecht der Union und nationalen Recht ergeben. Diese Verordnung sollte nicht so verstanden werden, dass sie eine Rechtsgrundlage für die Verarbeitung personenbezogener Daten bildet, auch nicht für besondere Kategorien personenbezogener Daten.

(42) Zur Minderung der Risiken für Nutzer und betroffene Personen, die von auf dem Unionsmarkt in Verkehr gebrachten oder anderweitig in Betrieb genommenen Hochrisiko-KI-Systemen ausgehen, sollten bestimmte verbindliche Anforderungen gelten, wobei der Zweckbestimmung des Systems und dem vom Anbieter einzurichtenden Risikomanagementsystem Rechnung zu tragen ist.

(43) Die Anforderungen sollten für Hochrisiko-KI-Systeme im Hinblick auf die Qualität der verwendeten Datensätze, die technische Dokumentation und die Aufzeichnungspflichten, die Transparenz und die Bereitstellung von Informationen für die Nutzer, die menschliche Aufsicht sowie die Robustheit, Genauigkeit und Cybersicherheit gelten. Diese Anforderungen sind erforderlich, um die Risiken für die Gesundheit, die Sicherheit und die Grundrechte entsprechend der Zweckbestimmung des Systems wirksam zu mindern, und es stehen keine anderen weniger handelsbeschränkenden Maßnahmen zur Verfügung, sodass ungerechtfertigte Handelsbeschränkungen vermieden werden.

(44) Eine hohe Datenqualität ist für die Leistung vieler KI-Systeme von wesentlicher Bedeutung, insbesondere wenn Techniken eingesetzt werden, bei denen Modelle mit Daten trainiert werden, um sicherzustellen, dass das Hochrisiko-KI-System bestimmungsgemäß und sicher funktioniert und nicht zur Ursache für Diskriminierung wird, die nach dem Unionsrecht verboten ist. Für hochwertige Trainings-, Validierungs- und Testdatensätze müssen geeignete Daten-Governance- und Datenverwaltungsverfahren umgesetzt werden. Die Trainings-, Validierungs- und Testdatensätze sollten im Hinblick auf die Zweckbestimmung des Systems hinreichend relevant, repräsentativ, fehlerfrei und vollständig sein. Ferner sollten sie die geeigneten statistischen Merkmale haben, auch bezüglich der Personen oder Personengruppen, auf die das Hochrisiko-KI-System bestimmungsgemäß angewandt werden soll. Insbesondere sollten die Trainings-, Validierungs- und Testdatensätze, soweit dies angesichts der Zweckbestimmung erforderlich ist, den Eigenschaften, Merkmalen oder Elementen entsprechen, die für die besonderen geografischen, verhaltensbezogenen oder funktionalen Rahmenbedingungen oder den Zusammenhängen, in denen das KI-System bestimmungsgemäß verwendet werden soll, typisch sind. Um das Recht anderer auf Schutz vor Diskriminierung, die sich aus Verzerrungen in KI-Systemen ergeben könnte, zu wahren, sollten die Anbieter angesichts des erheblichen öffentlichen Interesses auch besondere Kategorien personenbezogener Daten verarbeiten dürfen, um Verzerrungen in Hochrisiko-KI-Systemen zu beobachten, zu erkennen und zu korrigieren.

(45) Für die Entwicklung von Hochrisiko-KI-Systemen sollten bestimmte Akteure wie Anbieter, notifizierte Stellen und andere einschlägige Stellen wie Zentren für digitale Innovation, Erprobungs- und Versuchseinrichtungen und Forscher in der Lage sein, in ihren jeweiligen Tätigkeitsbereichen, die mit dieser Verordnung in Zusammenhang stehen, auf hochwertige Datensätze zuzugreifen und diese zu nutzen. Die von der Kommission eingerichteten gemeinsamen europäischen Datenräume und die Erleichterung des Datenaustauschs im öffentlichen Interesse zwischen Unternehmen und mit Behörden werden entscheidend dazu beitragen, einen vertrauensvollen, rechenschaftspflichtigen und diskriminierungsfreien Zugang zu hochwertigen Daten

für das Training, die Validierung und das Testen von KI-Systemen zu gewährleisten. Im Gesundheitsbereich beispielsweise wird der europäische Raum für Gesundheitsdaten den diskriminierungsfreien Zugang zu Gesundheitsdaten und das Training von KI-Algorithmen mithilfe dieser Datensätze erleichtern, und zwar unter Wahrung der Privatsphäre, auf sichere, zeitnahe, transparente und vertrauenswürdige Weise und unter angemessener institutioneller Leitung. Die einschlägigen zuständigen Behörden, einschließlich sektoraler Behörden, die den Zugang zu Daten bereitstellen oder unterstützen, können auch die Bereitstellung hochwertiger Daten für das Training, die Validierung und das Testen von KI-Systemen unterstützen.

(46) Informationen darüber, wie Hochrisiko-KI-Systeme entwickelt wurden und wie sie während ihres gesamten Lebenszyklus funktionieren, sind unerlässlich, um die Einhaltung der Anforderungen dieser Verordnung überprüfen zu können. Dies erfordert die Führung von Aufzeichnungen und die Verfügbarkeit einer technischen Dokumentation, die alle erforderlichen Informationen enthält, um die Einhaltung der einschlägigen Anforderungen durch das KI-System zu beurteilen. Diese Informationen sollten die allgemeinen Merkmale, Fähigkeiten und Grenzen des Systems, die verwendeten Algorithmen, Daten, Trainings-, Test- und Validierungsverfahren sowie die Dokumentation des einschlägigen Risikomanagementsystems umfassen. Die technische Dokumentation sollte stets auf dem neuesten Stand gehalten werden.

(47) Um der Undurchsichtigkeit entgegenzuwirken, die bestimmte KI-Systeme für natürliche Personen unverständlich oder zu komplex erscheinen lässt, sollte für Hochrisiko-KI-Systeme ein gewisses Maß an Transparenz vorgeschrieben werden. Die Nutzer sollten in der Lage sein, die Ergebnisse des Systems zu interpretieren und es angemessen zu verwenden. Hochrisiko-KI-Systemen sollte daher die einschlägige Dokumentation und Gebrauchsanweisungen beigefügt sein und diese sollten präzise und eindeutige Informationen enthalten, gegebenenfalls auch in Bezug auf mögliche Risiken in Bezug auf die Grundrechte und Diskriminierung.

(48) Hochrisiko-KI-Systeme sollten so konzipiert und entwickelt werden, dass natürliche Personen ihre Funktionsweise überwachen können. Zu diesem Zweck sollte der Anbieter des Systems vor dem Inverkehrbringen oder der Inbetriebnahme geeignete Maßnahmen zur Gewährleistung der menschlichen Aufsicht festlegen. Insbesondere sollten solche Maßnahmen gegebenenfalls gewährleisten, dass das System integrierten Betriebseinschränkungen unterliegt, über die sich das System selbst nicht hinwegsetzen kann, dass es auf den menschlichen Bediener reagiert und dass die natürlichen Personen, denen die menschliche Aufsicht übertragen wurde, über die erforderliche Kompetenz, Ausbildung und Befugnis verfügen, um diese Aufgabe wahrzunehmen.

(49) Hochrisiko-KI-Systeme sollten während ihres gesamten Lebenszyklus beständig funktionieren und ein angemessenes Maß an Genauigkeit, Robustheit und Cybersicherheit entsprechend dem allgemein anerkannten Stand der Technik aufweisen. Der Genauigkeitsgrad und die Genauigkeitskennzahlen sollte den Nutzern mitgeteilt werden.

(50) Die technische Robustheit ist eine wesentliche Voraussetzung für Hochrisiko-KI-Systeme. Sie sollten widerstandfähig gegenüber Risiken im Zusammenhang mit den Grenzen des Systems (z. B. Fehler, Störungen, Unstimmigkeiten, unerwartete Situationen) sowie gegenüber böswilligen Eingriffen sein, die die Sicherheit des KI-Systems gefährden und zu schädlichen oder anderweitig unerwünschtem Verhalten führen können. Ein fehlender Schutz vor diesen Risiken könnte die Sicherheit

beeinträchtigen oder sich negativ auf die Grundrechte auswirken, wenn das KI-System beispielsweise falsche Entscheidungen trifft oder falsche oder verzerrte Ergebnisse hervorbringt.

(51) Die Cybersicherheit spielt eine entscheidende Rolle, wenn es darum geht sicherzustellen, dass KI-Systeme widerstandsfähig gegenüber Versuchen böswilliger Dritter sind, unter Ausnutzung der Schwachstellen der Systeme deren Verwendung, Verhalten, Leistung oder Sicherheitsmerkmale zu verändern. Cyberangriffe auf KI-Systeme können KI-spezifische Ressourcen wie Trainingsdatensätze (z. B. Datenvergiftung) oder trainierte Modelle (z. B. feindliche Angriffe) nutzen oder Schwachstellen in den digitalen Ressourcen des KI-Systems oder der zugrunde liegenden IKT-Infrastruktur ausnutzen. Um ein den Risiken angemessenes Cybersicherheitsniveau zu gewährleisten, sollten die Anbieter von Hochrisiko-KI-Systemen daher geeignete Maßnahmen ergreifen, wobei gegebenenfalls auch die zugrunde liegende IKT-Infrastruktur zu berücksichtigen ist.

(52) Als Teil der Harmonisierungsrechtsvorschriften der Union sollten Vorschriften für das Inverkehrbringen, die Inbetriebnahme und die Verwendung von Hochrisiko-KI-Systemen im Einklang mit der Verordnung (EG) Nr. 765/2008 des Europäischen Parlaments und des Rates[51] über die Vorschriften für die Akkreditierung und Überwachung von Produkten, dem Beschluss Nr. 768/2008/EG des Europäischen Parlaments und des Rates[52] über einen gemeinsamen Rechtsrahmen für die Vermarktung von Produkten und der Verordnung (EU) 2019/1020 des Europäischen Parlaments und des Rates[53] über Marktüberwachung und die Konformität von Produkten („neuer Rechtsrahmen für die Vermarktung von Produkten“) festgelegt werden.

(53) Es ist angemessen, dass eine bestimmte als Anbieter definierte natürliche oder juristische Person die Verantwortung für das Inverkehrbringen oder die Inbetriebnahme eines Hochrisiko-KI-Systems übernimmt, unabhängig davon, ob es sich bei dieser natürlichen oder juristischen Person um die Person handelt, die das System konzipiert oder entwickelt hat.

(54) Der Anbieter sollte ein solides Qualitätsmanagementsystem einrichten, die Durchführung des vorgeschriebenen Konformitätsbewertungsverfahrens sicherstellen, die einschlägige Dokumentation erstellen und ein robustes System zur Beobachtung nach dem Inverkehrbringen einrichten. Behörden, die Hochrisiko-KI-Systeme für den Eigengebrauch in Betrieb nehmen, können unter Berücksichtigung der Besonderheiten des Bereichs sowie der Zuständigkeiten und der Organisation der betreffenden Behörde die Vorschriften für das Qualitätsmanagementsystem als Teil des auf nationaler oder regionaler Ebene eingesetzten Qualitätsmanagementsystems annehmen und umsetzen.

---

51 Verordnung (EG) Nr. 765/2008 des Europäischen Parlaments und des Rates vom 9. Juli 2008 über die Vorschriften für die Akkreditierung und Marktüberwachung im Zusammenhang mit der Vermarktung von Produkten und zur Aufhebung der Verordnung (EWG) Nr. 339/93 des Rates (ABl. L 218 vom 13.8.2008, S. 30).

52 Beschluss Nr. 768/2008/EG des Europäischen Parlaments und des Rates vom 9. Juli 2008 über einen gemeinsamen Rechtsrahmen für die Vermarktung von Produkten und Aufhebung des Beschlusses 93/465/EWG des Rates (ABl. L 218 vom 13.8.2008, S. 82).

53 Verordnung (EU) 2019/1020 des Europäischen Parlaments und des Rates vom 20. Juni 2019 über Marktüberwachung und die Konformität von Produkten sowie zur Änderung der Richtlinie 2004/42/EG und der Verordnungen (EG) Nr. 765/2008 und (EU) Nr. 305/2011 (ABl. L 169 vom 25.6.2019, S. 1).

(55) Wird ein Hochrisiko-KI-System, bei dem es sich um eine Sicherheitskomponente eines Produkts handelt, das unter einschlägige sektorale Rechtsvorschriften des neuen Rechtsrahmen fällt, nicht unabhängig von dem Produkt in Verkehr gebracht oder in Betrieb genommen, so sollte der Hersteller des Endprodukts im Sinne der einschlägigen Rechtsvorschriften des neuen Rechtsrahmens die in dieser Verordnung festgelegten Anbieterpflichten erfüllen und insbesondere sicherstellen, dass das in das Endprodukt eingebettete KI-System den Anforderungen dieser Verordnung entspricht.

(56) Um die Durchsetzung dieser Verordnung zu ermöglichen und gleiche Wettbewerbsbedingungen für die Akteure zu schaffen, muss unter Berücksichtigung der verschiedenen Formen der Bereitstellung digitaler Produkte sichergestellt sein, dass unter allen Umständen eine in der Union ansässige oder niedergelassene Person den Behörden alle erforderlichen Informationen über die Konformität eines KI-Systems zur Verfügung stellen kann. Daher benennen Anbieter, die außerhalb der Union niedergelassen sind, vor der Bereitstellung ihrer KI-Systeme in der Union schriftlich einen in der Union niedergelassenen Bevollmächtigten für den Fall, dass kein Einführer ermittelt werden kann.

(57) Im Einklang mit den Grundsätzen des neuen Rechtsrahmens sollten besondere Verpflichtungen für einschlägige Wirtschaftsakteure, wie Einführer und Händler, festgelegt werden, um die Rechtssicherheit zu gewährleisten und die Einhaltung der Rechtsvorschriften durch die betreffenden Wirtschaftsakteure zu erleichtern.

(58) Angesichts des Charakters von KI-Systemen und der Risiken für die Sicherheit und die Grundrechte, die mit ihrer Verwendung verbunden sein können, ist es angebracht, besondere Zuständigkeiten für die Nutzer festzulegen, auch im Hinblick darauf, dass eine angemessene Überwachung der Leistung eines KI-Systems unter realen Bedingungen sichergestellt werden muss. Die Nutzer sollten insbesondere Hochrisiko-KI-Systeme gemäß der Gebrauchsanweisung verwenden, und es sollten bestimmte andere Pflichten in Bezug auf die Überwachung der Funktionsweise der KI-Systeme und gegebenenfalls auch Aufzeichnungspflichten festgelegt werden.

(59) Es ist angemessen, davon auszugehen, dass der Nutzer des KI-Systems eine natürliche oder juristische Person oder eine Behörde, Einrichtung oder sonstige Stelle ist, die für den Betrieb eines KI-Systems verantwortlich ist, es sei denn, das KI-System wird im Rahmen einer persönlichen nicht beruflichen Tätigkeit verwendet.

(60) Angesichts der Komplexität der Wertschöpfungskette im Bereich der künstlichen Intelligenz sollten einschlägige Dritte, insbesondere diejenigen, die am Verkauf und der Bereitstellung von Software, Software-Tools und Komponenten, vortrainierten Modellen und Daten beteiligt sind, oder Netzdienstbetreiber gegebenenfalls mit Anbietern und Nutzern, denen die Einhaltung der Verpflichtungen aus dieser Verordnung ermöglicht werden soll, und mit den gemäß dieser Verordnung eingerichteten zuständigen Behörden zusammenarbeiten.

(61) Die Normung sollte eine Schlüsselrolle dabei spielen, den Anbietern technische Lösungen zur Verfügung zu stellen, um die Einhaltung dieser Verordnung zu gewährleisten. Die Einhaltung harmonisierter Normen gemäß der Verordnung (EU) Nr. 1025/2012 des Europäischen Parlaments und des Rates[54] sollte den Anbietern den

[54] Verordnung (EU) Nr. 1025/2012 des Europäischen Parlaments und des Rates vom 25. Oktober 2012 zur europäischen Normung, zur Änderung der Richtlinien 89/686/EWG und 93/15/EWG des Rates sowie der Richtlinien 94/9/EG, 94/25/EG, 95/16/EG, 97/23/EG, 98/34/EG, 2004/22/EG, 2007/23/EG, 2009/23/EG und 2009/105/EG des Europäischen Parlaments und des Rates und zur Aufhebung des

Nachweis der Konformität mit den Anforderungen dieser Verordnung ermöglichen. Die Kommission könnte jedoch gemeinsame technische Spezifikationen in Bereichen annehmen, in denen es keine harmonisierten Normen gibt oder diese unzureichend sind.

(62) Um ein hohes Maß an Vertrauenswürdigkeit von Hochrisiko-KI-Systemen zu gewährleisten, sollten diese Systeme einer Konformitätsbewertung unterzogen werden, bevor sie in Verkehr gebracht oder in Betrieb genommen werden.

(63) Damit für die Betreiber möglichst wenig Aufwand entsteht und etwaige Doppelarbeit vermieden wird, sollte bei Hochrisiko-KI-Systemen im Zusammenhang mit Produkten, die nach dem neuen Rechtsrahmen unter bestehende Harmonisierungsrechtsvorschriften der Union fallen, im Rahmen der bereits in diesen Rechtsvorschriften vorgesehenen Konformitätsbewertung bewertet werden, ob diese KI-Systeme den Anforderungen dieser Verordnung genügen. Die Anwendbarkeit der Anforderungen dieser Verordnung sollte daher die besondere Logik, die Methodik oder die allgemeine Struktur der Konformitätsbewertung gemäß den einschlägigen spezifischen Rechtsvorschriften des neuen Rechtsrahmens unberührt lassen. Dieser Ansatz spiegelt sich voll und ganz in der Wechselwirkung zwischen dieser Verordnung und der [Maschinenverordnung] wider. Bei den Anforderungen in dieser Verordnung geht es um die Sicherheitsrisiken, die von KI-Systemen ausgehen, die Sicherheitsfunktionen in Maschinen steuern, wogegen bestimmte spezifische Anforderungen der [Maschinenverordnung] gewährleisten werden, dass ein KI-System auf sichere Weise in die gesamte Maschine integriert wird, damit die Sicherheit der Maschine insgesamt nicht beeinträchtigt wird. In der [Maschinenverordnung] wird der Begriff „KI-System“ genauso wie in dieser Verordnung definiert.

(64) Angesichts der umfassenderen Erfahrung professioneller dem Inverkehrbringen vorgeschalteter Zertifizierer im Bereich der Produktsicherheit und der unterschiedlichen Art der damit verbundenen Risiken empfiehlt es sich, zumindest während der anfänglichen Anwendung dieser Verordnung für Hochrisiko-KI-Systeme, die nicht mit Produkten in Verbindung stehen, den Anwendungsbereich der Konformitätsbewertung durch Dritte einzuschränken. Daher sollte die Konformitätsbewertung solcher Systeme in der Regel vom Anbieter in eigener Verantwortung durchgeführt werden, mit Ausnahme von KI-Systemen, die zur biometrischen Fernidentifizierung von Personen verwendet werden sollen, bei denen die Beteiligung einer notifizierten Stelle an der Konformitätsbewertung vorgesehen werden sollte, soweit diese Systeme nicht ganz verboten sind.

(65) Damit KI-Systeme, die zur biometrischen Fernidentifizierung von Personen verwendet werden sollen, einer Konformitätsbewertung durch Dritte unterzogen werden können, sollten die notifizierten Stellen gemäß dieser Verordnung von den zuständigen nationalen Behörden benannt werden, sofern sie eine Reihe von Anforderungen erfüllen, insbesondere in Bezug auf Unabhängigkeit, Kompetenz und Nichtvorliegen von Interessenkonflikten.

(66) Im Einklang mit dem allgemein anerkannten Begriff der wesentlichen Änderung von Produkten, für die Harmonisierungsrechtsvorschriften der Union gelten, ist es angebracht, dass ein KI-System einer neuen Konformitätsbewertung unterzogen wird, wenn eine Änderung eintritt, die die Einhaltung dieser Verordnung durch das System

---

Beschlusses 87/95/EWG des Rates und des Beschlusses Nr. 1673/2006/EG des Europäischen Parlaments und des Rates (ABl. L 316 vom 14.11.2012, S. 12).

beeinträchtigen könnte, oder wenn sich die Zweckbestimmung des Systems ändert. Darüber hinaus müssen in Bezug auf KI-Systeme, die nach dem Inverkehrbringen oder der Inbetriebnahme weiterhin dazulernen (d. h. sie passen automatisch an, wie die Funktionen ausgeführt werden), Vorschriften festgelegt werden, nach denen Änderungen des Algorithmus und seiner Leistung, die vom Anbieter vorab festgelegt und zum Zeitpunkt der Konformitätsbewertung bewertet wurden, keine wesentliche Änderung darstellen sollten.

(67) Hochrisiko-KI-Systeme sollten grundsätzlich mit der CE-Kennzeichnung versehen sein, aus der ihre Konformität mit dieser Verordnung hervorgeht, sodass sie frei im Binnenmarkt verkehren können. Die Mitgliedstaaten sollten keine ungerechtfertigten Hindernisse für das Inverkehrbringen oder die Inbetriebnahme von Hochrisiko-KI-Systemen schaffen, die die in dieser Verordnung festgelegten Anforderungen erfüllen und mit der CE-Kennzeichnung versehen sind.

(68) Unter bestimmten Bedingungen kann die rasche Verfügbarkeit innovativer Technik für die Gesundheit und Sicherheit von Menschen und für die Gesellschaft insgesamt von entscheidender Bedeutung sein. Es ist daher angebracht, dass die Mitgliedstaaten aus außergewöhnlichen Gründen der öffentlichen Sicherheit, des Schutzes des Lebens und der Gesundheit natürlicher Personen und des Schutzes des gewerblichen und kommerziellen Eigentums das Inverkehrbringen oder die Inbetriebnahme von KI-Systemen, die keiner Konformitätsbewertung unterzogen wurden, genehmigen könnten.

(69) Um die Arbeit der Kommission und der Mitgliedstaaten im Bereich der künstlichen Intelligenz zu erleichtern und die Transparenz gegenüber der Öffentlichkeit zu erhöhen, sollten Anbieter von Hochrisiko-KI-Systemen, die nicht mit Produkten in Verbindung stehen, die unter die einschlägigen Harmonisierungsrechtsvorschriften der Union fallen, dazu verpflichtet werden, ihr Hochrisiko-KI-System in einer von der Kommission einzurichtenden und zu verwaltenden EU-Datenbank zu registrieren. Die Kommission sollte im Einklang mit der Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates[55] als für die Datenbank verantwortliche Stelle gelten. Um die volle Funktionsfähigkeit der Datenbank zu gewährleisten, sollte das Verfahren für die Einrichtung der Datenbank auch die Ausarbeitung von funktionalen Spezifikationen durch die Kommission und einen unabhängigen Prüfbericht umfassen.

(70) Bestimmte KI-Systeme, die mit natürlichen Personen interagieren oder Inhalte erzeugen sollen, können unabhängig davon, ob sie als hochriskant eingestuft werden, ein besonderes Risiko in Bezug auf Identitätsbetrug oder Täuschung bergen. Unter bestimmten Umständen sollte die Verwendung solcher Systeme daher – unbeschadet der Anforderungen an und Verpflichtungen für Hochrisiko-KI-Systeme – besonderen Transparenzpflichten unterliegen. Insbesondere sollte natürlichen Personen mitgeteilt werden, dass sie es mit einem KI-System zu tun haben, es sei denn, dies ist aufgrund der Umstände und des Kontexts der Nutzung offensichtlich. Darüber hinaus sollten natürliche Personen informiert werden, wenn sie einem Emotionserkennungssystem oder einem System zur biometrischen Kategorisierung ausgesetzt sind. Diese Informationen und Mitteilungen sollten für Menschen mit Behinderungen in

[55] Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (ABl. L 119 vom 4.5.2016, S. 1).

entsprechend barrierefrei zugänglicher Form bereitgestellt werden. Darüber hinaus sollten Nutzer, die ein KI-System zum Erzeugen oder Manipulieren von Bild-, Ton- oder Videoinhalten verwenden, die wirklichen Personen, Orten oder Ereignissen merklich ähneln und einer Person fälschlicherweise echt erscheinen würden, offenlegen, dass die Inhalte künstlich erzeugt oder manipuliert wurden, indem sie die Ergebnisse künstlicher Intelligenz entsprechend kennzeichnen und auf ihren künstlichen Ursprung hinweisen.

(71) Künstliche Intelligenz bezeichnet eine Reihe sich rasch entwickelnder Technologien, die neuartige Formen der Regulierungsaufsicht und einen sicheren Raum für die Erprobung erfordern, wobei gleichzeitig eine verantwortungsvolle Innovation und die Integration geeigneter Schutzvorkehrungen und Risikominderungsmaßnahmen gewährleistet werden müssen. Um einen innovationsfreundlichen, zukunftssicheren und gegenüber Störungen widerstandsfähigen Rechtsrahmen sicherzustellen, sollten die zuständigen nationalen Behörden eines oder mehrerer Mitgliedstaaten angehalten werden, Reallabore für künstliche Intelligenz einzurichten, um die Entwicklung und Erprobung innovativer KI-Systeme vor deren Inverkehrbringen oder anderweitiger Inbetriebnahme unter strenger Regulierungsaufsicht zu erleichtern.

(72) Die Ziele der Reallabore sollten darin bestehen, Innovationen im Bereich KI zu fördern, indem eine kontrollierte Versuchs- und Erprobungsumgebung für die Entwicklungsphase und die dem Inverkehrbringen vorgelagerte Phase geschaffen wird, um sicherzustellen, dass die innovativen KI-Systeme mit dieser Verordnung und anderen einschlägigen Rechtsvorschriften der Union und der Mitgliedstaaten in Einklang stehen. Darüber hinaus sollen sie die Rechtssicherheit für Innovatoren sowie die Aufsicht und das Verständnis der zuständigen Behörden in Bezug auf die Möglichkeiten, neu auftretenden Risiken und der Auswirkungen der KI-Nutzung verbessern und den Marktzugang beschleunigen, unter anderem indem Hindernisse für kleine und mittlere Unternehmen (KMU) und Start-up-Unternehmen abgebaut werden. Im Interesse einer unionsweit einheitlichen Umsetzung und der Erzielung von Größenvorteilen sollten gemeinsame Vorschriften für die Umsetzung von Reallaboren und ein Rahmen für die Zusammenarbeit zwischen den an der Beaufsichtigung der Reallabore beteiligten Behörden festgelegt werden. Die vorliegende Verordnung sollte im Einklang mit Artikel 6 Absatz 4 der Verordnung (EU) 2016/679 und Artikel 6 der Verordnung (EU) 2018/1725 sowie unbeschadet des Artikels 4 Absatz 2 der Richtlinie (EU) 2016/680 die Rechtsgrundlage für die Verwendung personenbezogener Daten, die für andere Zwecke erhoben werden, zur Entwicklung bestimmter KI-Systeme im öffentlichen Interesse innerhalb der KI-Reallabore bilden. Die am Reallabor Beteiligten sollten angemessene Schutzvorkehrungen treffen und mit den zuständigen Behörden zusammenarbeiten, unter anderem indem sie deren Anweisungen befolgen und zügig und nach Treu und Glauben handeln, um etwaige hohe Risiken für die Sicherheit und die Grundrechte, die bei der Entwicklung und Erprobung im Reallabor auftreten können, zu mindern. Das Verhalten der am Reallabor Beteiligten sollte berücksichtigt werden, wenn die zuständigen Behörden entscheiden, ob sie eine Geldbuße gemäß Artikel 83 Absatz 2 der Verordnung (EU) 2016/679 und Artikel 57 der Richtlinie (EU) 2016/680 verhängen.

(73) Um Innovationen zu fördern und zu schützen, ist es wichtig, die Interessen kleiner Anbieter und Nutzer von KI-Systemen besonders zu berücksichtigen. Zu diesem Zweck sollten die Mitgliedstaaten Initiativen ergreifen, die sich an diese Akteure richten, darunter auch Sensibilisierungs- und Informationsmaßnahmen. Darüber hinaus sind die besonderen Interessen und Bedürfnisse kleinerer Anbieter bei der

Festlegung der Gebühren für die Konformitätsbewertung durch die notifizierten Stellen zu berücksichtigen. Übersetzungen im Zusammenhang mit der verpflichtenden Dokumentation und Kommunikation mit Behörden können für Anbieter und andere Akteure, insbesondere den kleineren unter ihnen, erhebliche Kosten verursachen. Die Mitgliedstaaten sollten möglichst dafür sorgen, dass eine der Sprachen, die sie für die einschlägige Dokumentation der Anbieter und für die Kommunikation mit den Akteuren bestimmen und akzeptieren, eine Sprache ist, die von der größtmöglichen Zahl grenzüberschreitender Nutzer weitgehend verstanden wird.

(74) Um die Risiken bei der Durchführung, die sich aus mangelndem Wissen und fehlenden Fachkenntnissen auf dem Markt ergeben, zu minimieren und den Anbietern und notifizierten Stellen die Einhaltung ihrer Verpflichtungen aus dieser Verordnung zu erleichtern, sollten die KI-Abruf-Plattform, die europäischen Zentren für digitale Innovation und die Erprobungs- und Versuchseinrichtungen, die von der Kommission und den Mitgliedstaaten auf nationaler oder EU-Ebene eingerichtet wurden/werden, möglichst zur Durchführung dieser Verordnung beitragen. Sie können Anbieter und notifizierte Stellen im Rahmen ihres jeweiligen Auftrags und ihrer jeweiligen Kompetenzbereiche insbesondere technisch und wissenschaftlich unterstützen.

(75) Es ist angezeigt, dass die Kommission den Stellen, Gruppen oder Laboratorien, die gemäß den einschlägigen Harmonisierungsrechtsvorschriften der Union eingerichtet oder akkreditiert sind und Aufgaben im Zusammenhang mit der Konformitätsbewertung von Produkten oder Geräten wahrnehmen, die unter diese Harmonisierungsrechtsvorschriften der Union fallen, soweit wie möglich den Zugang zu Erprobungs- und Versuchseinrichtungen erleichtert. Dies gilt insbesondere für Expertengremien, Fachlaboratorien und Referenzlaboratorien im Bereich Medizinprodukte gemäß der Verordnung (EU) 2017/745 und der Verordnung (EU) 2017/746.

(76) Um eine reibungslose, wirksame und harmonisierte Umsetzung dieser Verordnung zu erleichtern, sollte ein Europäischer Ausschuss für künstliche Intelligenz eingerichtet werden. Der Ausschuss sollte für eine Reihe von Beratungsaufgaben zuständig sein und Stellungnahmen, Empfehlungen, Ratschlägen oder Leitlinien zu Fragen im Zusammenhang mit der Umsetzung dieser Verordnung abgeben, darunter zu technischen Spezifikationen oder bestehenden Normen in Bezug auf die in dieser Verordnung festgelegten Anforderungen; außerdem sollte er die Kommission in spezifischen Fragen im Zusammenhang mit künstlicher Intelligenz beraten und unterstützen.

(77) Den Mitgliedstaaten kommt bei der Anwendung und Durchsetzung dieser Verordnung eine Schlüsselrolle zu. Dazu sollte jeder Mitgliedstaat eine oder mehrere zuständige nationale Behörden benennen, die die Anwendung und Umsetzung dieser Verordnung beaufsichtigen. Um die Effizienz der Organisation aufseiten der Mitgliedstaaten zu steigern und eine offizielle Kontaktstelle gegenüber der Öffentlichkeit und anderen Ansprechpartnern auf Ebene der Mitgliedstaaten und der Union einzurichten, sollte in jedem Mitgliedstaat eine nationale Behörde als nationale Aufsichtsbehörde benannt werden.

(78) Damit Anbieter von Hochrisiko-KI-Systemen die Erfahrungen mit der Verwendung von Hochrisiko-KI-Systemen bei der Verbesserung ihrer Systeme und im Konzeptions- und Entwicklungsprozess berücksichtigen oder rechtzeitig etwaige Korrekturmaßnahmen ergreifen können, sollten alle Anbieter über ein System zur Beobachtung nach dem Inverkehrbringen verfügen. Dieses System ist auch wichtig,

damit den möglichen Risiken, die von KI-Systemen ausgehen, die nach dem Inverkehrbringen oder der Inbetriebnahme dazulernen, wirksamer und zeitnah begegnet werden kann. In diesem Zusammenhang sollten die Anbieter auch verpflichtet sein, ein System einzurichten, um den zuständigen Behörden schwerwiegende Vorfälle oder Verstöße gegen nationales Recht und Unionsrecht zum Schutz der Grundrechte zu melden, die sich aus der Verwendung ihrer KI-Systeme ergeben.

(79) Zur Gewährleistung einer angemessenen und wirksamen Durchsetzung der Anforderungen und Verpflichtungen gemäß dieser Verordnung, bei der es sich eine Harmonisierungsrechtsvorschrift der Union handelt, sollte das mit der Verordnung (EU) 2019/1020 eingeführte System der Marktüberwachung und der Konformität von Produkten in vollem Umfang gelten. Sofern dies für die Erfüllung ihres Auftrags erforderlich ist, sollten auch nationale Behörden oder Stellen, die die Anwendung des Unionsrechts zum Schutz der Grundrechte überwachen, einschließlich Gleichstellungsstellen, Zugang zu der gesamten im Rahmen dieser Verordnung erstellten Dokumentation haben.

(80) Die Rechtsvorschriften der Union über Finanzdienstleistungen enthalten Vorschriften und Anforderungen für die interne Unternehmensführung und das Risikomanagement, die für regulierte Finanzinstitute bei der Erbringung solcher Dienstleistungen gelten, auch wenn sie KI-Systeme verwenden. Um eine kohärente Anwendung und Durchsetzung der Verpflichtungen aus dieser Verordnung sowie der einschlägigen Vorschriften und Anforderungen der Rechtsvorschriften der Union für Finanzdienstleistungen zu gewährleisten, sollten die für die Beaufsichtigung und Durchsetzung der Rechtsvorschriften im Bereich der Finanzdienstleistungen zuständigen Behörden, gegebenenfalls einschließlich der Europäischen Zentralbank, auch als zuständige Behörden für die Überwachung der Durchführung dieser Verordnung, einschließlich der Marktüberwachungstätigkeiten, in Bezug auf von regulierten und beaufsichtigten Finanzinstituten bereitgestellte oder verwendete KI-Systeme benannt werden. Um die Kohärenz zwischen dieser Verordnung und den Vorschriften für Kreditinstitute, die unter die Richtlinie 2013/36/EU des Europäischen Parlaments und des Rates[56] fallen, weiter zu verbessern, ist es ferner angezeigt, das Konformitätsbewertungsverfahren und einige verfahrenstechnische Anbieterpflichten in Bezug auf das Risikomanagement, die Beobachtung nach dem Inverkehrbringen und die Dokumentation in die bestehenden Verpflichtungen und Verfahren gemäß der Richtlinie 2013/36/EU aufzunehmen. Zur Vermeidung von Überschneidungen sollten auch begrenzte Ausnahmen in Bezug auf das Qualitätsmanagementsystem der Anbieter und die Beobachtungspflichten der Nutzer von Hochrisiko-KI-Systemen in Betracht gezogen werden, soweit diese Kreditinstitute betreffen, die unter die Richtlinie 2013/36/EU fallen.

(81) Die Entwicklung anderer KI-Systeme als Hochrisiko-KI-Systeme im Einklang mit den Anforderungen dieser Verordnung kann zu einer stärkeren Verbreitung vertrauenswürdiger künstlicher Intelligenz in der Union führen. Anbieter von KI-Systemen, die kein hohes Risiko bergen, sollten angehalten werden, Verhaltenskodizes zu erstellen, um eine freiwillige Anwendung der für Hochrisiko-KI-Systeme

[56] Richtlinie 2013/36/EU des Europäischen Parlaments und des Rates vom 26. Juni 2013 über den Zugang zur Tätigkeit von Kreditinstituten und die Beaufsichtigung von Kreditinstituten und Wertpapierfirmen, zur Änderung der Richtlinie 2002/87/EG und zur Aufhebung der Richtlinien 2006/48/EG und 2006/49/EG (ABl. L 176 vom 27.6.2013, S. 338).

verbindlichen Anforderungen zu fördern. Darüber hinaus sollten die Anbieter auch ermutigt werden, freiwillig zusätzliche Anforderungen anzuwenden, z. B. in Bezug auf die ökologische Nachhaltigkeit, die barrierefreie Zugänglichkeit für Menschen mit Behinderungen, die Beteiligung der Interessenträger an der Konzeption und Entwicklung von KI-Systemen und die Vielfalt der Entwicklungsteams. Die Kommission kann Initiativen, auch sektoraler Art, ergreifen, um den Abbau technischer Hindernisse zu erleichtern, die den grenzüberschreitenden Datenaustausch im Zusammenhang mit der KI-Entwicklung behindern, unter anderem in Bezug auf die Infrastruktur für den Datenzugang und die semantische und technische Interoperabilität verschiedener Arten von Daten.

(82) Es ist wichtig, dass KI-Systeme im Zusammenhang mit Produkten, die gemäß dieser Verordnung kein hohes Risiko bergen und daher nicht die in dieser Verordnung festgelegten Anforderungen erfüllen müssen, dennoch sicher sind, wenn sie in Verkehr gebracht oder in Betrieb genommen werden. Um zu diesem Ziel beizutragen, würde die Richtlinie 2001/95/EG des Europäischen Parlaments und des Rates[57] als Sicherheitsnetz dienen.

(83) Zur Gewährleistung einer vertrauensvollen und konstruktiven Zusammenarbeit der zuständigen Behörden auf Ebene der Union und der Mitgliedstaaten, sollten alle an der Anwendung dieser Verordnung beteiligten Parteien die Vertraulichkeit der im Rahmen der Durchführung ihrer Tätigkeiten erlangten Informationen und Daten wahren.

(84) Die Mitgliedstaaten sollten alle erforderlichen Maßnahmen ergreifen, um sicherzustellen, dass die Bestimmungen dieser Verordnung eingehalten werden, und dazu u. a. wirksame, verhältnismäßige und abschreckende Sanktionen für Verstöße festlegen. Bei bestimmten Verstößen sollten die Mitgliedstaaten die in dieser Verordnung festgelegten Spielräume und Kriterien berücksichtigen. Der Europäische Datenschutzbeauftragte sollte befugt sein, gegen Organe, Einrichtungen und sonstige Stellen der Union, die in den Anwendungsbereich dieser Verordnung fallen, Geldbußen zu verhängen.

(85) Damit der Rechtsrahmen erforderlichenfalls angepasst werden kann, sollte der Kommission die Befugnis übertragen werden, gemäß Artikel 290 AEUV Rechtsakte zur Änderung der in Anhang I genannten Techniken und Konzepte für die Einstufung von KI-Systemen, der in Anhang II aufgeführten Harmonisierungsrechtsvorschriften der Union, der in Anhang III aufgeführten Hochrisiko-KI-Systeme, der Bestimmungen über die technische Dokumentation in Anhang IV, des Inhalts der EU-Konformitätserklärung in Anhang V, der Bestimmungen über die Konformitätsbewertungsverfahren in den Anhängen VI und VII und der Bestimmungen zur Festlegung der Hochrisiko-KI-Systeme zu erlassen, für die das Konformitätsbewertungsverfahren auf der Grundlage der Bewertung des Qualitätsmanagementsystems und der technischen Dokumentation gelten sollte. Es ist von besonderer Bedeutung, dass die Kommission im Zuge ihrer Vorbereitungsarbeit angemessene Konsultationen, auch auf der Ebene von Sachverständigen, durchführt, die mit den Grundsätzen in Einklang stehen, die in der Interinstitutionellen Vereinbarung vom 13. April 2016 über bessere Rechtsetzung[58] niedergelegt wurden. Um insbesondere für eine gleichberechtigte Beteiligung an der Vorbereitung

[57] Richtlinie 2001/95/EG des Europäischen Parlaments und des Rates vom 3. Dezember 2001 über die allgemeine Produktsicherheit (ABl. L 11 vom 15.1.2002, S. 4).

[58] ABl. L 123 vom 12.5.2016, S. 1.

delegierter Rechtsakte zu sorgen, erhalten das Europäische Parlament und der Rat alle Dokumente zur gleichen Zeit wie die Sachverständigen der Mitgliedstaaten, und ihre Sachverständigen haben systematisch Zugang zu den Sitzungen der Sachverständigengruppen der Kommission, die mit der Vorbereitung der delegierten Rechtsakte befasst sind.

(86) Zur Gewährleistung einheitlicher Bedingungen für die Durchführung dieser Verordnung sollten der Kommission Durchführungsbefugnisse übertragen werden. Diese Befugnisse sollten im Einklang mit der Verordnung (EU) Nr. 182/2011 des Europäischen Parlaments und des Rates[59] ausgeübt werden.

(87) Da das Ziel dieser Verordnung von den Mitgliedstaaten nicht ausreichend verwirklicht werden kann, sondern vielmehr wegen des Umfangs oder der Wirkung der Maßnahme auf Unionsebene besser zu verwirklichen ist, kann die Union im Einklang mit dem in Artikel 5 EUV verankerten Subsidiaritätsprinzip tätig werden. Entsprechend dem in demselben Artikel genannten Grundsatz der Verhältnismäßigkeit geht diese Verordnung nicht über das für die Verwirklichung dieses Ziels erforderliche Maß hinaus.

(88) Diese Verordnung sollte ab dem … [*Amt für Veröffentlichungen – bitte das in Artikel 85 festgelegte Datum einfügen*] gelten. Die Infrastruktur für die Leitung und das Konformitätsbewertungssystem sollte jedoch schon vorher einsatzbereit sein, weshalb die Bestimmungen über notifizierte Stellen und die Leitungsstruktur ab dem... [*Amt für Veröffentlichungen – bitte Datum einfügen – drei Monate nach Inkrafttreten dieser Verordnung*] gelten sollten. Darüber hinaus sollten die Mitgliedstaaten Vorschriften über Sanktionen, einschließlich Geldbußen, festlegen und der Kommission mitteilen sowie dafür sorgen, dass diese bis zum Geltungsbeginn dieser Verordnung ordnungsgemäß und wirksam umgesetzt werden. Daher sollten die Bestimmungen über Sanktionen ab dem [*Amt für Veröffentlichungen – bitte Datum einfügen – zwölf Monate nach Inkrafttreten dieser Verordnung*] gelten.

(89) Der Europäische Datenschutzbeauftragte und der Europäische Datenschutzausschuss wurden gemäß Artikel 42 Absatz 2 der Verordnung (EU) 2018/1725 angehört und haben am [...] eine Stellungnahme abgegeben —

HABEN FOLGENDE VERORDNUNG ERLASSEN:

TITEL I

ALLGEMEINE BESTIMMUNGEN

Artikel 1
Gegenstand

In dieser Verordnung wird Folgendes festgelegt:

a) harmonisierte Vorschriften für das Inverkehrbringen, die Inbetriebnahme und die Verwendung von Systemen der künstlichen Intelligenz (im Folgenden „KI-Systeme“) in der Union;

[59] Verordnung (EU) Nr. 182/2011 des Europäischen Parlaments und des Rates vom 16. Februar 2011 zur Festlegung der allgemeinen Regeln und Grundsätze, nach denen die Mitgliedstaaten die Wahrnehmung der Durchführungsbefugnisse durch die Kommission kontrollieren (ABl. L 55 vom 28.2.2011, S. 13).

b) Verbote bestimmter Praktiken im Bereich der künstlichen Intelligenz;

c) besondere Anforderungen an Hochrisiko-KI-Systeme und Verpflichtungen für Betreiber solcher Systeme;

d) harmonisierte Transparenzvorschriften für KI-Systeme, die mit natürlichen Personen interagieren sollen, für KI-Systeme zur Emotionserkennung und zur biometrischen Kategorisierung sowie für KI-Systeme, die zum Erzeugen oder Manipulieren von Bild-, Ton- oder Videoinhalten verwendet werden;

e) Vorschriften für die Marktbeobachtung und Marktüberwachung.

Artikel 2
Anwendungsbereich

(1) Diese Verordnung gilt für:

a) Anbieter, die KI-Systeme in der Union in Verkehr bringen oder in Betrieb nehmen, unabhängig davon, ob diese Anbieter in der Union oder in einem Drittland niedergelassen sind;

b) Nutzer von KI-Systemen, die sich in der Union befinden;

c) Anbieter und Nutzer von KI-Systemen, die in einem Drittland niedergelassen oder ansässig sind, wenn das vom System hervorgebrachte Ergebnis in der Union verwendet wird.

(2) Für Hochrisiko-KI-Systeme, die Sicherheitskomponenten von Produkten oder Systemen oder selbst Produkte oder Systeme sind, die in den Anwendungsbereich der folgenden Rechtsakte fallen, gilt nur Artikel 84 dieser Verordnung:

a) Verordnung (EG) Nr. 300/2008,

b) Verordnung (EU) Nr. 167/2013,

c) Verordnung (EU) Nr. 168/2013,

d) Richtlinie 2014/90/EU,

e) Richtlinie (EU) 2016/797,

f) Verordnung (EU) 2018/858,

g) Verordnung (EU) 2018/1139,

h) Verordnung (EU) 2019/2144.

(3) Diese Verordnung gilt nicht für KI-Systeme, die ausschließlich für militärische Zwecke entwickelt oder verwendet werden.

(4) Diese Verordnung gilt weder für Behörden in Drittländern noch für internationale Organisationen, die gemäß Absatz 1 in den Anwendungsbereich dieser Verordnung fallen, soweit diese Behörden oder Organisationen KI-Systeme im Rahmen internationaler Übereinkünfte im Bereich der Strafverfolgung und justiziellen Zusammenarbeit mit der Union oder mit einem oder mehreren Mitgliedstaaten verwenden.

(5) Die Anwendung der Bestimmungen über die Verantwortlichkeit der Vermittler in Kapitel II Abschnitt 4 der Richtlinie 2000/31/EG des Europäischen Parlaments und

des Rates[60] [*die durch die entsprechenden Bestimmungen des Gesetzes über digitale Dienste ersetzt werden sollen*] bleibt von dieser Verordnung unberührt.

Artikel 3
Begriffsbestimmungen

Für die Zwecke dieser Verordnung bezeichnet der Ausdruck

1. „System der künstlichen Intelligenz“ (KI-System) eine Software, die mit einer oder mehreren der in Anhang I aufgeführten Techniken und Konzepte entwickelt worden ist und im Hinblick auf eine Reihe von Zielen, die vom Menschen festgelegt werden, Ergebnisse wie Inhalte, Vorhersagen, Empfehlungen oder Entscheidungen hervorbringen kann, die das Umfeld beeinflussen, mit dem sie interagieren;
2. „Anbieter“ eine natürliche oder juristische Person, Behörde, Einrichtung oder sonstige Stelle, die ein KI-System entwickelt oder entwickeln lässt, um es unter ihrem eigenen Namen oder ihrer eigenen Marke – entgeltlich oder unentgeltlich – in Verkehr zu bringen oder in Betrieb zu nehmen;
3. „Kleinanbieter“ einen Anbieter, bei dem es sich um ein Kleinst- oder Kleinunternehmen im Sinne der Empfehlung 2003/361/EG der Kommission[61] handelt;
4. „Nutzer“ eine natürliche oder juristische Person, Behörde, Einrichtung oder sonstige Stelle, die ein KI-System in eigener Verantwortung verwendet, es sei denn, das KI-System wird im Rahmen einer persönlichen und nicht beruflichen Tätigkeit verwendet;
5. „Bevollmächtigter“ eine in der Union ansässige oder niedergelassene natürliche oder juristische Person, die vom Anbieter eines KI-Systems schriftlich dazu bevollmächtigt wurde, in seinem Namen die in dieser Verordnung festgelegten Pflichten zu erfüllen bzw. Verfahren durchzuführen;
6. „Einführer“ eine in der Union ansässige oder niedergelassene natürliche oder juristische Person, die ein KI-System, das den Namen oder die Marke einer außerhalb der Union ansässigen oder niedergelassenen natürlichen oder juristischen Person trägt, in der Union in Verkehr bringt oder in Betrieb nimmt;
7. „Händler“ eine natürliche oder juristische Person in der Lieferkette, die ein KI-System ohne Änderung seiner Merkmale auf dem Unionsmarkt bereitstellt, mit Ausnahme des Herstellers oder des Einführers;
8. „Akteur“ den Anbieter, den Nutzer, den Bevollmächtigten, den Einführer und den Händler;
9. „Inverkehrbringen“ die erstmalige Bereitstellung eines KI-Systems auf dem Unionsmarkt;

[60] Richtlinie 2000/31/EG des Europäischen Parlaments und des Rates vom 8. Juni 2000 über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt („Richtlinie über den elektronischen Geschäftsverkehr“) (ABl. L 178 vom 17.7.2000, S. 1).

[61] Empfehlung der Kommission vom 6. Mai 2003 betreffend die Definition der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen (ABl. L 124 vom 20.5.2003, S. 36).

10. „Bereitstellung auf dem Markt“ jede entgeltliche oder unentgeltliche Abgabe eines KI-Systems zum Vertrieb oder zur Verwendung auf dem Unionsmarkt im Rahmen einer Geschäftstätigkeit;

11. „Inbetriebnahme“ die Bereitstellung eines KI-Systems auf dem Unionsmarkt zum Erstgebrauch direkt an den Nutzer oder zum Eigengebrauch entsprechend seiner Zweckbestimmung;

12. „Zweckbestimmung“ die Verwendung, für die ein KI-System laut Anbieter bestimmt ist, einschließlich der besonderen Nutzungsumstände und Nutzungsbedingungen entsprechend den Angaben des Anbieters in der Gebrauchsanweisung, im Werbe- oder Verkaufsmaterial und in diesbezüglichen Erklärungen sowie in der technischen Dokumentation;

13. „vernünftigerweise vorhersehbare Fehlanwendung“ die Verwendung eines KI-Systems in einer Weise, die nicht seiner Zweckbestimmung entspricht, die sich aber aus einem vernünftigerweise vorhersehbaren menschlichen Verhalten oder einer vernünftigerweise vorhersehbaren Interaktion mit anderen Systemen ergeben kann;

14. „Sicherheitskomponente eines Produkts oder Systems“ einen Bestandteil eines Produkts oder Systems, der eine Sicherheitsfunktion für dieses Produkt oder System erfüllt oder dessen Ausfall oder Störung die Gesundheit und Sicherheit von Personen oder Sachen gefährdet;

15. „Gebrauchsanweisung“ die Informationen, die der Anbieter bereitstellt, um den Nutzer insbesondere über die Zweckbestimmung und die ordnungsgemäße Verwendung eines KI-Systems zu informieren, einschließlich der besonderen geografischen, verhaltensbezogenen oder funktionalen Rahmenbedingungen, unter denen ein Hochrisiko-KI-System bestimmungsgemäß verwendet werden soll;

16. „Rückruf eines KI-Systems“ jede Maßnahme, die auf die Rückgabe eines den Nutzern bereits zur Verfügung gestellten KI-Systems an den Anbieter abzielt;

17. „Rücknahme eines KI-Systems“ jede Maßnahme, mit der verhindert werden soll, das ein KI-System vertrieben, ausgestellt oder angeboten wird;

18. „Leistung eines KI-Systems“ die Fähigkeit eines KI-Systems, seine Zweckbestimmung zu erfüllen;

19. „notifizierende Behörde“ die nationale Behörde, die für die Einrichtung und Durchführung der erforderlichen Verfahren für die Bewertung, Benennung und Notifizierung von Konformitätsbewertungsstellen und für deren Überwachung zuständig ist;

20. „Konformitätsbewertung“ das Verfahren zur Überprüfung, ob die in Titel III Kapitel 2 dieser Verordnung festgelegten Anforderungen an ein KI-System erfüllt worden sind;

21. „Konformitätsbewertungsstelle“ eine Stelle, die Konformitätsbewertungstätigkeiten einschließlich Prüfungen, Zertifizierungen und Kontrollen durchführt und dabei als unabhängige Dritte auftritt;

22. „notifizierte Stelle“ eine Konformitätsbewertungsstelle, die gemäß dieser Verordnung und anderen einschlägigen Harmonisierungsvorschriften der Union benannt wurde;

23. „wesentliche Änderung“ eine Änderung des KI-Systems nach dessen Inverkehrbringen oder Inbetriebnahme, die sich auf die Konformität des KI-Systems

mit den Anforderungen in Titel III Kapitel 2 dieser Verordnung auswirkt oder zu einer Änderung der Zweckbestimmung führt, für die das KI-System geprüft wurde;

24. „CE-Konformitätskennzeichnung“ (CE-Kennzeichnung) eine Kennzeichnung, durch die ein Anbieter erklärt, dass ein KI-System die Anforderungen erfüllt, die in Titel III Kapitel 2 dieser Verordnung und in anderen einschlägigen Rechtsvorschriften der Union zur Harmonisierung der Bedingungen für die Vermarktung von Produkten („Harmonisierungsrechtsvorschriften der Union“), die die Anbringung dieser Kennzeichnung vorsehen, festgelegt sind;

25. „Beobachtung nach dem Inverkehrbringen“ alle Tätigkeiten, die Anbieter von KI-Systemen zur proaktiven Sammlung und Überprüfung von Erfahrungen mit der Nutzung der von ihnen in Verkehr gebrachten oder in Betrieb genommenen KI-Systeme durchführen, um festzustellen, ob unverzüglich nötige Korrektur- oder Präventivmaßnahmen zu ergreifen sind;

26. „Marktüberwachungsbehörde“ die nationale Behörde, die die Tätigkeiten durchführt und die Maßnahmen ergreift, die in der Verordnung (EU) 2019/1020 vorgesehen sind;

27. „harmonisierte Norm“ eine harmonisierte europäische Norm im Sinne des Artikels 2 Absatz 1 Buchstabe c der Verordnung (EU) Nr. 1025/2012;

28. „gemeinsame Spezifikationen“ ein Dokument, das keine Norm ist und das technische Lösungen enthält, deren Befolgung es ermöglicht, bestimmte Anforderungen und Verpflichtungen dieser Verordnung zu erfüllen;

29. „Trainingsdaten“ Daten, die zum Trainieren eines KI-Systems verwendet werden, wobei dessen lernbare Parameter und die Gewichte eines neuronalen Netzes angepasst werden;

30. „Validierungsdaten“ Daten, die zum Bewerten des trainierten KI-Systems und zum Abstimmen seiner nicht lernbaren Parameter und seines Lernprozesses verwendet werden, um unter anderem eine Überanpassung zu vermeiden; der Validierungsdatensatz kann ein separater Datensatz oder Teil des Trainingsdatensatzes mit fester oder variabler Aufteilung sein;

31. „Testdaten“ Daten, die für eine unabhängige Bewertung des trainierten und validierten KI-Systems verwendet werden, um die erwartete Leistung dieses Systems vor dessen Inverkehrbringen oder Inbetriebnahme zu bestätigen;

32. „Eingabedaten“ die in ein KI-System eingespeisten oder von diesem direkt erfassten Daten, auf deren Grundlage das System ein Ergebnis (Ausgabe) hervorbringt;

33. „biometrische Daten“ mit speziellen technischen Verfahren gewonnene personenbezogene Daten zu den physischen, physiologischen oder verhaltenstypischen Merkmalen einer natürlichen Person, die die eindeutige Identifizierung dieser natürlichen Person ermöglichen oder bestätigen, wie Gesichtsbilder oder daktyloskopische Daten;

34. „Emotionserkennungssystem“ ein KI-System, das dem Zweck dient, Emotionen oder Absichten natürlicher Personen auf der Grundlage ihrer biometrischen Daten festzustellen oder daraus abzuleiten;

35. „System zur biometrischen Kategorisierung“ ein KI-System, das dem Zweck dient, natürliche Personen auf der Grundlage ihrer biometrischen Daten bestimmten

Kategorien wie Geschlecht, Alter, Haarfarbe, Augenfarbe, Tätowierung, ethnische Herkunft oder sexuelle oder politische Ausrichtung zuzuordnen;

36. „biometrisches Fernidentifizierungssystem“ ein KI-System, das dem Zweck dient, natürliche Personen aus der Ferne durch Abgleich der biometrischen Daten einer Person mit den in einer Referenzdatenbank gespeicherten biometrischen Daten zu identifizieren, ohne dass der Nutzer des KI-Systems vorher weiß, ob die Person anwesend sein wird und identifiziert werden kann;

37. „biometrisches Echtzeit-Fernidentifizierungssystem“ ein biometrisches Fernidentifizierungssystem, bei dem die Erfassung biometrischer Daten, der Abgleich und die Identifizierung ohne erhebliche Verzögerung erfolgen; zur Vermeidung einer Umgehung der Vorschriften umfasst dies nicht nur die sofortige Identifizierung, sondern auch eine Identifizierung mit begrenzten kurzen Verzögerungen;

38. „System zur nachträglichen biometrischen Fernidentifizierung“ ein biometrisches Fernidentifizierungssystem, das kein biometrisches Echtzeit-Fernidentifizierungssystem ist;

39. „öffentlich zugänglicher Raum“ einen der Öffentlichkeit zugänglichen physischen Ort, unabhängig davon, ob dafür bestimmte Zugangsbedingungen gelten;

40. „Strafverfolgungsbehörde“:

    a) eine staatliche Stelle, die für die Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder die Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit, zuständig ist, oder

    b) eine andere Stelle oder Einrichtung, der durch das Recht der Mitgliedstaaten die Ausübung öffentlicher Gewalt und hoheitlicher Befugnisse zur Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder zur Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit, übertragen wurde;

41. „Strafverfolgung“ Tätigkeiten der Strafverfolgungsbehörden zur Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder zur Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit;

42. „nationale Aufsichtsbehörde“ die Behörde, der ein Mitgliedstaat die Verantwortung für die Durchführung und Anwendung dieser Verordnung, die Koordinierung der diesem Mitgliedstaat übertragenen Tätigkeiten, die Wahrnehmung der Funktion der zentralen Kontaktstelle für die Kommission und die Vertretung des Mitgliedstaats im Europäischen Ausschuss für künstliche Intelligenz überträgt;

43. „zuständige nationale Behörde“ die nationale Aufsichtsbehörde, die notifizierende Behörde und die Marktüberwachungsbehörde;

44. „schwerwiegender Vorfall“ ein Vorkommnis, das direkt oder indirekt eine der nachstehenden Folgen hat, hätte haben können oder haben könnte:

    a) den Tod oder die schwere gesundheitliche Schädigung einer Person, schwere Sach- oder Umweltschäden,

    b) eine schwere und unumkehrbare Störung der Verwaltung und des Betriebs kritischer Infrastrukturen.

Artikel 4
Änderungen des Anhangs I

Der Kommission wird die Befugnis übertragen, gemäß Artikel 73 delegierte Rechtsakte zur Änderung der Liste der Techniken und Konzepte in Anhang I zu erlassen, um diese Liste auf der Grundlage von Merkmalen, die den dort aufgeführten Techniken und Konzepten ähnlich sind, an Marktentwicklungen und technische Entwicklungen anzupassen.

TITEL II

VERBOTENE PRAKTIKEN IM BEREICH DER KÜNSTLICHEN INTELLIGENZ

Artikel 5

(1) Folgende Praktiken im Bereich der künstlichen Intelligenz sind verboten:

a) das Inverkehrbringen, die Inbetriebnahme oder die Verwendung eines KI-Systems, das Techniken der unterschwelligen Beeinflussung außerhalb des Bewusstseins einer Person einsetzt, um das Verhalten einer Person in einer Weise wesentlich zu beeinflussen, die dieser Person oder einer anderen Person einen physischen oder psychischen Schaden zufügt oder zufügen kann;

b) das Inverkehrbringen, die Inbetriebnahme oder die Verwendung eines KI-Systems, das eine Schwäche oder Schutzbedürftigkeit einer bestimmten Gruppe von Personen aufgrund ihres Alters oder ihrer körperlichen oder geistigen Behinderung ausnutzt, um das Verhalten einer dieser Gruppe angehörenden Person in einer Weise wesentlich zu beeinflussen, die dieser Person oder einer anderen Person einen physischen oder psychischen Schaden zufügt oder zufügen kann;

c) das Inverkehrbringen, die Inbetriebnahme oder die Verwendung von KI-Systemen durch Behörden oder in deren Auftrag zur Bewertung oder Klassifizierung der Vertrauenswürdigkeit natürlicher Personen über einen bestimmten Zeitraum auf der Grundlage ihres sozialen Verhaltens oder bekannter 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 ganzer Gruppen natürlicher Personen in sozialen Zusammenhängen, die in keinem Zusammenhang zu den Umständen stehen, unter denen die Daten ursprünglich erzeugt oder erfasst wurden;

ii) Schlechterstellung oder Benachteiligung bestimmter natürlicher Personen oder ganzer Gruppen natürlicher Personen, in einer Weise, die im Hinblick auf ihr soziales Verhalten oder dessen Tragweite ungerechtfertigt oder unverhältnismäßig ist;

d) 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 potenziellen Opfern von Straftaten oder nach vermissten Kindern;

ii) Abwenden einer konkreten, erheblichen und unmittelbaren Gefahr für das Leben oder die körperliche Unversehrtheit natürlicher Personen oder eines Terroranschlags;

iii) Erkennen, Aufspüren, Identifizieren oder Verfolgen eines Täters oder Verdächtigen einer Straftat im Sinne des Artikels 2 Absatz 2 des Rahmenbeschlusses 2002/584/JI des Rates[62], der in dem betreffenden Mitgliedstaat nach dessen Recht mit einer Freiheitsstrafe oder einer freiheitsentziehenden Maßregel der Sicherung im Höchstmaß von mindestens drei Jahren bedroht ist.

(2) Bei der Verwendung biometrischer Echtzeit-Fernidentifizierungssysteme in öffentlich zugänglichen Räumen zu Strafverfolgungszwecken im Hinblick auf die in Absatz 1 Buchstabe d genannten Ziele werden folgende Elemente berücksichtigt:

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.

Darüber hinaus sind bei der Verwendung biometrischer Echtzeit-Fernidentifizierungssysteme in öffentlich zugänglichen Räumen zu Strafverfolgungszwecken im Hinblick auf die in Absatz 1 Buchstabe d genannten Ziele notwendige und verhältnismäßige Schutzvorkehrungen und Bedingungen für die Verwendung einzuhalten, insbesondere in Bezug auf die zeitlichen, geografischen und personenbezogenen Beschränkungen.

(3) Im Hinblick auf Absatz 1 Buchstabe d und Absatz 2 ist für jede einzelne 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 im Einklang mit den in Absatz 4 genannten detaillierten Vorschriften des nationalen Rechts erteilt wird. In hinreichend begründeten dringenden Fällen kann jedoch mit der Verwendung des Systems zunächst ohne Genehmigung begonnen und die Genehmigung erst während oder nach der Nutzung beantragt werden.

Die zuständige Justiz- oder Verwaltungsbehörde 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 Buchstabe d genannten Ziele – wie im Antrag angegeben – notwendig und verhältnismäßig ist. Bei ihrer Entscheidung über den Antrag berücksichtigt die zuständige Justiz- oder Verwaltungsbehörde die in Absatz 2 genannten Elemente.

---

62 Rahmenbeschluss 2002/584/JI des Rates vom 13. Juni 2002 über den Europäischen Haftbefehl und die Übergabeverfahren zwischen den Mitgliedstaaten (ABl. L 190 vom 18.7.2002, S. 1).

(4) Ein Mitgliedstaat kann die Möglichkeit einer vollständigen oder teilweisen Genehmigung der Verwendung biometrischer Echtzeit-Identifizierungssysteme in öffentlich zugänglichen Räumen zu Strafverfolgungszwecken innerhalb der in Absatz 1 Buchstabe d, Absatz 2 und Absatz 3 aufgeführten Grenzen und unter den dort genannten Bedingungen vorsehen. Dieser Mitgliedstaat legt in seinem nationalen Recht die erforderlichen detaillierten Vorschriften für die Beantragung, Erteilung und Ausübung der in Absatz 3 genannten Genehmigungen sowie für die entsprechende Beaufsichtigung fest. In diesen Vorschriften wird auch festgelegt, im Hinblick auf welche der in Absatz 1 Buchstabe d genannten Ziele und welche der unter Ziffer iii genannten Straftaten die zuständigen Behörden ermächtigt werden können, diese Systeme zu Strafverfolgungszwecken zu verwenden.

TITEL III

HOCHRISIKO-KI-SYSTEME

KAPITEL 1

KLASSIFIZIERUNG VON KI-SYSTEMEN ALS HOCHRISIKO-SYSTEME

Artikel 6
Klassifizierungsvorschriften für Hochrisiko-KI-Systeme

(1) Ungeachtet dessen, ob ein KI-System unabhängig von den unter den Buchstaben a und b genannten Produkten in Verkehr gebracht oder in Betrieb genommen wird, gilt es als Hochrisiko-KI-System, wenn die beiden folgenden Bedingungen erfüllt sind:

a) das KI-System soll als Sicherheitskomponente eines unter die in Anhang II aufgeführten Harmonisierungsrechtsvorschriften der Union fallenden Produkts verwendet werden oder ist selbst ein solches Produkt;

b) das Produkt, dessen Sicherheitskomponente das KI-System ist, oder das KI-System selbst als Produkt muss einer Konformitätsbewertung durch Dritte im Hinblick auf das Inverkehrbringen oder die Inbetriebnahme dieses Produkts gemäß den in Anhang II aufgeführten Harmonisierungsrechtsvorschriften der Union unterzogen werden.

(2) Zusätzlich zu den in Absatz 1 genannten Hochrisiko-KI-Systemen gelten die in Anhang III genannten KI-Systeme ebenfalls als hochriskant.

Artikel 7
Änderungen des Anhangs III

(1) Der Kommission wird die Befugnis übertragen, gemäß Artikel 73 delegierte Rechtsakte zur Änderung der Liste in Anhang III zu erlassen, um Hochrisiko-KI-Systeme hinzuzufügen, die beide folgenden Bedingungen erfüllen:

a) die KI-Systeme sollen in einem der in Anhang III Nummern 1 bis 8 aufgeführten Bereiche eingesetzt werden;

b) die KI-Systeme bergen ein Risiko der Schädigung der Gesundheit oder der Beeinträchtigung der Sicherheit oder nachteiliger Auswirkungen auf die

Grundrechte, das im Hinblick auf die Schwere und die Wahrscheinlichkeit des Eintretens dem Risiko der Schädigung, Beeinträchtigung oder negativer Auswirkungen gleicht, das von den in Anhang III bereits aufgeführten Hochrisiko-KI-Systemen ausgeht, oder dieses übersteigt.

(2) Bei der Bewertung für die Zwecke des Absatzes 1, ob ein KI-System ein Risiko der Schädigung der Gesundheit oder der Beeinträchtigung der Sicherheit oder ein Risiko nachteiliger Auswirkungen auf die Grundrechte birgt, das dem Risiko der Schädigung oder Beeinträchtigung gleicht, das von den in Anhang III bereits aufgeführten Hochrisiko-KI-Systemen ausgeht, oder dieses übersteigt, berücksichtigt die Kommission folgende Kriterien:

a) die Zweckbestimmung des KI-Systems;

b) das Ausmaß, in dem ein KI-System verwendet wird oder voraussichtlich verwendet werden wird;

c) das Ausmaß, in dem durch die Verwendung eines KI-Systems schon die Gesundheit geschädigt, die Sicherheit beeinträchtigt oder negative Auswirkungen auf die Grundrechte verursacht worden sind oder nach Berichten oder dokumentierten Behauptungen, die den zuständigen nationalen Behörden übermittelt werden, Anlass zu erheblichen Bedenken hinsichtlich des Eintretens solcher Schäden, Beeinträchtigungen oder nachteiligen Auswirkungen besteht;

d) das potenzielle Ausmaß solcher Schäden, Beeinträchtigungen oder nachteiligen Auswirkungen, insbesondere hinsichtlich ihrer Intensität und ihrer Eignung, eine Vielzahl von Personen zu beeinträchtigen;

e) das Ausmaß, in dem potenziell geschädigte oder beeinträchtigte Personen von dem von einem KI-System hervorgebrachten Ergebnis abhängen, weil es insbesondere aus praktischen oder rechtlichen Gründen nach vernünftigem Ermessen unmöglich ist, sich diesem Ergebnis zu entziehen;

f) das Ausmaß, in dem potenziell geschädigte oder beeinträchtigte Personen gegenüber dem Nutzer eines KI-Systems schutzbedürftig sind, insbesondere aufgrund eines Ungleichgewichts in Bezug auf Machtposition, Wissen, wirtschaftliche oder soziale Umstände oder Alter;

g) das Ausmaß, in dem das mit einem KI-System hervorgebrachte Ergebnis leicht rückgängig zu machen ist, wobei Ergebnisse, die sich auf die Gesundheit oder Sicherheit von Personen auswirken, nicht als leicht rückgängig zu machen gelten;

h) das Ausmaß, in dem bestehende Rechtsvorschriften der Union Folgendes vorsehen:

i) wirksame Abhilfemaßnahmen in Bezug auf die Risiken, die von einem KI-System ausgehen, mit Ausnahme von Schadenersatzansprüchen,

ii) wirksame Maßnahmen zur Vermeidung oder wesentlichen Verringerung dieser Risiken.

KAPITEL 2

ANFORDERUNGEN AN HOCHRISIKO-KI-SYSTEME

Artikel 8
Einhaltung der Anforderungen

(1) Hochrisiko-KI-Systeme müssen die in diesem Kapitel festgelegten Anforderungen erfüllen.

(2) Bei der Gewährleistung der Einhaltung dieser Anforderungen wird der Zweckbestimmung des Hochrisiko-KI-Systems und dem in Artikel 9 genannten Risikomanagementsystem Rechnung getragen.

Artikel 9
Risikomanagementsystem

(1) Für Hochrisiko-KI-Systeme wird ein Risikomanagementsystem eingerichtet, angewandt, dokumentiert und aufrechterhalten.

(2) Das Risikomanagementsystem versteht sich als ein kontinuierlicher iterativer Prozess während des gesamten Lebenszyklus eines KI-Systems, der eine regelmäßige systematische Aktualisierung erfordert. Es umfasst folgende Schritte:

a) Ermittlung und Analyse der bekannten und vorhersehbaren Risiken, die von jedem Hochrisiko-KI-System ausgehen;

b) Abschätzung und Bewertung der Risiken, die entstehen können, wenn das Hochrisiko-KI-System entsprechend seiner Zweckbestimmung oder im Rahmen einer vernünftigerweise vorhersehbaren Fehlanwendung verwendet wird;

c) Bewertung anderer möglicherweise auftretender Risiken auf der Grundlage der Auswertung der Daten aus dem in Artikel 61 genannten System zur Beobachtung nach dem Inverkehrbringen;

d) Ergreifung geeigneter Risikomanagementmaßnahmen gemäß den Bestimmungen der folgenden Absätze.

(3) Bei den in Absatz 2 Buchstabe d genannten Risikomanagementmaßnahmen werden die Auswirkungen und möglichen Wechselwirkungen, die sich aus der kombinierten Anwendung der Anforderungen dieses Kapitels 2 ergeben, gebührend berücksichtigt. Diese Maßnahmen tragen dem allgemein anerkannten Stand der Technik Rechnung, wie er auch in einschlägigen harmonisierten Normen oder gemeinsamen Spezifikationen zum Ausdruck kommt.

(4) Die in Absatz 2 Buchstabe d genannten Risikomanagementmaßnahmen werden so gestaltet, dass jedes mit einer bestimmten Gefahr verbundene Restrisiko sowie das Gesamtrestrisiko der Hochrisiko-KI-Systeme als vertretbar beurteilt werden kann, sofern das Hochrisiko-KI-System entsprechend seiner Zweckbestimmung oder im Rahmen einer vernünftigerweise vorhersehbaren Fehlanwendung verwendet wird. Diese Restrisiken müssen den Nutzern mitgeteilt werden.

Bei der Festlegung der am besten geeigneten Risikomanagementmaßnahmen ist Folgendes sicherzustellen:

a) weitestmögliche Beseitigung oder Verringerung der Risiken durch eine geeignete Konzeption und Entwicklung,

b) gegebenenfalls Anwendung angemessener Minderungs- und Kontrollmaßnahmen im Hinblick auf nicht auszuschließende Risiken;

c) Bereitstellung angemessener Informationen gemäß Artikel 13, insbesondere bezüglich der in Absatz 2 Buchstabe b des vorliegenden Artikels genannten Risiken, und gegebenenfalls entsprechende Schulung der Nutzer.

Bei der Beseitigung oder Verringerung der Risiken im Zusammenhang mit der Verwendung des Hochrisiko-KI-Systems werden die technischen Kenntnisse, die Erfahrungen und der Bildungsstand, die vom Nutzer erwarten werden können, sowie das Umfeld, in dem das System eingesetzt werden soll, gebührend berücksichtigt.

(5) Hochrisiko-KI-Systeme müssen getestet werden, um die am besten geeigneten Risikomanagementmaßnahmen zu ermitteln. Durch das Testen wird sichergestellt, dass Hochrisiko-KI-Systeme stets bestimmungsgemäß funktionieren und die Anforderungen dieses Kapitels erfüllen.

(6) Die Testverfahren müssen geeignet sein, die Zweckbestimmung des KI-Systems zu erfüllen, und brauchen nicht über das hierfür erforderliche Maß hinauszugehen.

(7) Das Testen von Hochrisiko-KI-Systemen erfolgt zu jedem geeigneten Zeitpunkt während des gesamten Entwicklungsprozesses und in jedem Fall vor dem Inverkehrbringen oder der Inbetriebnahme. Das Testen erfolgt anhand vorab festgelegter Parameter und probabilistischer Schwellenwerte, die für die Zweckbestimmung des Hochrisiko-KI-Systems geeignet sind.

(8) Bei der Umsetzung des in den Absätzen 1 bis 7 beschriebenen Risikomanagementsystems ist insbesondere zu berücksichtigen, ob das Hochrisiko-KI-System wahrscheinlich für Kinder zugänglich ist oder Auswirkungen auf Kinder hat.

(9) Bei Kreditinstituten, die unter die Richtlinie 2013/36/EU fallen, sind die in den Absätzen 1 bis 8 beschriebenen Aspekte Bestandteil der von diesen Instituten gemäß Artikel 74 der Richtlinie festgelegten Risikomanagementverfahren.

Artikel 10
Daten und Daten-Governance

(1) Hochrisiko-KI-Systeme, in denen Techniken eingesetzt werden, bei denen Modelle mit Daten trainiert werden, müssen mit Trainings-, Validierungs- und Testdatensätzen entwickelt werden, die den in den Absätzen 2 bis 5 genannten Qualitätskriterien entsprechen.

(2) Für Trainings-, Validierungs- und Testdatensätze gelten geeignete Daten-Governance- und Datenverwaltungsverfahren. Diese Verfahren betreffen insbesondere

a) die einschlägigen konzeptionellen Entscheidungen,

b) die Datenerfassung,

c) relevante Datenaufbereitungsvorgänge wie Kommentierung, Kennzeichnung, Bereinigung, Anreicherung und Aggregierung,

d) die Aufstellung relevanter Annahmen, insbesondere in Bezug auf die Informationen, die mit den Daten erfasst und dargestellt werden sollen,

e) eine vorherige Bewertung der Verfügbarkeit, Menge und Eignung der benötigten Datensätze,

f) eine Untersuchung im Hinblick auf mögliche Verzerrungen (Bias);

g) die Ermittlung möglicher Datenlücken oder Mängel und wie diese Lücken und Mängel behoben werden können.

(3) Die Trainings-, Validierungs- und Testdatensätze müssen relevant, repräsentativ, fehlerfrei und vollständig sein. Sie haben die geeigneten statistischen Merkmale, gegebenenfalls auch bezüglich der Personen oder Personengruppen, auf die das Hochrisiko-KI-System bestimmungsgemäß angewandt werden soll. Diese Merkmale der Datensätze können durch einzelne Datensätze oder eine Kombination solcher Datensätze erfüllt werden.

(4) Die Trainings-, Validierungs- und Testdatensätze müssen, soweit dies für die Zweckbestimmung erforderlich ist, den Merkmalen oder Elementen entsprechen, die für die besonderen geografischen, verhaltensbezogenen oder funktionalen Rahmenbedingungen, unter denen das Hochrisiko-KI-System bestimmungsgemäß verwendet werden soll, typisch sind.

(5) Soweit dies für die Beobachtung, Erkennung und Korrektur von Verzerrungen im Zusammenhang mit Hochrisiko-KI-Systemen unbedingt erforderlich ist, dürfen die Anbieter solcher Systeme besondere Kategorien personenbezogener Daten gemäß Artikel 9 Absatz 1 der Verordnung (EU) 2016/679, Artikel 10 der Richtlinie (EU) 2016/680 und Artikel 10 Absatz 1 der Verordnung (EU) 2018/1725 verarbeiten, wobei sie angemessene Vorkehrungen für den Schutz der Grundrechte und Grundfreiheiten natürlicher Personen treffen müssen, wozu auch technische Beschränkungen einer Weiterverwendung und modernste Sicherheits- und Datenschutzmaßnahmen wie Pseudonymisierung oder Verschlüsselung gehören, wenn der verfolgte Zweck durch eine Anonymisierung erheblich beeinträchtigt würde.

(6) Bei der Entwicklung von Hochrisiko-KI-Systemen, in denen keine Techniken eingesetzt werden, bei denen Modelle mit Daten trainiert werden, müssen angemessene Daten-Governance und Datenverwaltungsverfahren angewandt werden, um sicherzustellen, dass solche Hochrisiko-KI-Systeme den Vorgaben in Absatz 2 entsprechen.

Artikel 11
Technische Dokumentation

(1) Die technische Dokumentation eines Hochrisiko-KI-Systems wird erstellt, bevor dieses System in Verkehr gebracht oder in Betrieb genommen wird, und ist stets auf dem neuesten Stand zu halten.

Die technische Dokumentation wird so erstellt, dass aus ihr der Nachweis hervorgeht, wie das Hochrisiko-KI-System die Anforderungen dieses Kapitels erfüllt, und dass den zuständigen nationalen Behörden und den notifizierten Stellen alle Informationen zur Verfügung stehen, die erforderlich sind, um zu beurteilen, ob das KI-System diese Anforderungen erfüllt. Sie enthält zumindest die in Anhang IV genannten Angaben.

(2) Wird ein Hochrisiko-KI-System, das mit einem Produkt verbunden ist, das unter die in Anhang II Abschnitt A aufgeführten Rechtsakte fällt, in Verkehr gebracht oder in Betrieb genommen, so wird eine einzige technische Dokumentation erstellt, die alle in Anhang IV genannten Informationen sowie die nach diesen Rechtsakten erforderlichen Informationen enthält.

(3) Der Kommission wird die Befugnis übertragen, gemäß Artikel 73 delegierte Rechtsakte zur Änderung des Anhangs IV zu erlassen, wenn dies nötig ist, damit die technische Dokumentation in Anbetracht des technischen Fortschritts stets alle Informationen enthält, die erforderlich sind, um zu beurteilen, ob das System die Anforderungen dieses Kapitels erfüllt.

Artikel 12
Aufzeichnungspflichten

(1) Hochrisiko-KI-Systeme werden mit Funktionsmerkmalen konzipiert und entwickelt, die eine automatische Aufzeichnung von Vorgängen und Ereignissen („Protokollierung“) während des Betriebs der Hochrisiko-KI-Systeme ermöglichen. Diese Protokollierung muss anerkannten Normen oder gemeinsamen Spezifikationen entsprechen.

(2) Die Protokollierung gewährleistet, dass das Funktionieren des KI-Systems während seines gesamten Lebenszyklus in einem der Zweckbestimmung des Systems angemessenen Maße rückverfolgbar ist.

(3) Die Protokollierung ermöglicht insbesondere die Überwachung des Betriebs des Hochrisiko-KI-Systems im Hinblick auf das Auftreten von Situationen, die dazu führen können, dass das KI-System ein Risiko im Sinne des Artikels 65 Absatz 1 birgt, oder die zu einer wesentlichen Änderung führen, und erleichtert so die Beobachtung nach dem Inverkehrbringen gemäß Artikel 61.

(4) Die Protokollierungsfunktionen der in Anhang III Absatz 1 Buchstabe a genannten Hochrisiko-KI-Systeme müssen zumindest Folgendes umfassen:

a) Aufzeichnung jedes Zeitraums der Verwendung des Systems (Datum und Uhrzeit des Beginns und des Endes jeder Verwendung);

b) die Referenzdatenbank, mit der das System die Eingabedaten abgleicht;

c) die Eingabedaten, mit denen die Abfrage zu einer Übereinstimmung geführt hat;

d) die Identität der gemäß Artikel 14 Absatz 5 an der Überprüfung der Ergebnisse beteiligten natürlichen Personen.

Artikel 13
Transparenz und Bereitstellung von Informationen für die Nutzer

(1) Hochrisiko-KI-Systeme werden so konzipiert und entwickelt, dass ihr Betrieb hinreichend transparent ist, damit die Nutzer die Ergebnisse des Systems angemessen interpretieren und verwenden können. Die Transparenz wird auf eine geeignete Art und in einem angemessenen Maß gewährleistet, damit die Nutzer und Anbieter ihre in Kapitel 3 dieses Titels festgelegten einschlägigen Pflichten erfüllen können.

(2) Hochrisiko-KI-Systeme werden mit Gebrauchsanweisungen in einem geeigneten digitalen Format bereitgestellt oder auf andere Weise mit Gebrauchsanweisungen

versehen, die präzise, vollständige, korrekte und eindeutige Informationen in einer für die Nutzer relevanten, barrierefrei zugänglichen und verständlichen Form enthalten.

(3) Die in Absatz 2 genannten Informationen umfassen:

a) den Namen und die Kontaktangaben des Anbieters sowie gegebenenfalls seines Bevollmächtigten;

b) die Merkmale, Fähigkeiten und Leistungsgrenzen des Hochrisiko-KI-Systems, einschließlich

i) seiner Zweckbestimmung,

ii) des Maßes an Genauigkeit, Robustheit und Cybersicherheit gemäß Artikel 15, für das das Hochrisiko-KI-System getestet und validiert wurde und das zu erwarten ist, sowie alle bekannten und vorhersehbaren Umstände, die sich auf das erwartete Maß an Genauigkeit, Robustheit und Cybersicherheit auswirken können,

iii) aller bekannten oder vorhersehbaren Umstände im Zusammenhang mit der bestimmungsgemäßen Verwendung des Hochrisiko-KI-Systems oder einer vernünftigerweise vorhersehbaren Fehlanwendung, die zu Risiken für die Gesundheit und Sicherheit oder die Grundrechte führen können,

iv) seiner Leistung bezüglich der Personen oder Personengruppen, auf die das System bestimmungsgemäß angewandt werden soll,

v) gegebenenfalls der Spezifikationen für die Eingabedaten oder sonstiger relevanter Informationen über die verwendeten Trainings-, Validierungs- und Testdatensätze unter Berücksichtigung der Zweckbestimmung des KI-Systems;

c) etwaige Änderungen des Hochrisiko-KI-Systems und seiner Leistung, die der Anbieter zum Zeitpunkt der ersten Konformitätsbewertung vorab bestimmt hat;

d) die in Artikel 14 genannten Maßnahmen zur Gewährleistung der menschlichen Aufsicht, einschließlich der technischen Maßnahmen, die getroffen wurden, um den Nutzern die Interpretation der Ergebnisse von KI-Systemen zu erleichtern;

e) die erwartete Lebensdauer des Hochrisiko-KI-Systems und alle erforderlichen Wartungs- und Pflegemaßnahmen zur Gewährleistung des ordnungsgemäßen Funktionierens dieses KI-Systems, auch in Bezug auf Software-Updates.

Artikel 14
Menschliche Aufsicht

(1) Hochrisiko-KI-Systeme werden so konzipiert und entwickelt, dass sie während der Dauer der Verwendung des KI-Systems – auch mit geeigneten Werkzeugen einer Mensch-Maschine-Schnittstelle – von natürlichen Personen wirksam beaufsichtigt werden können.

(2) Die menschliche Aufsicht dient der Verhinderung oder Minimierung der Risiken für die Gesundheit, die Sicherheit oder die Grundrechte, die entstehen können, wenn ein Hochrisiko-KI-System bestimmungsgemäß oder unter im Rahmen einer vernünftigerweise vorhersehbaren Fehlanwendung verwendet wird, insbesondere

wenn solche Risiken trotz der Einhaltung anderer Anforderungen dieses Kapitels fortbestehen.

(3) Die menschliche Aufsicht wird durch eine oder alle der folgenden Vorkehrungen gewährleistet:

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

b) sie wird vor dem Inverkehrbringen oder der Inbetriebnahme des Hochrisiko-KI-Systems vom Anbieter bestimmt und ist dazu geeignet, vom Nutzer umgesetzt zu werden.

(4) Die in Absatz 3 genannten Maßnahmen müssen den Personen, denen die menschliche Aufsicht übertragen wurde, je nach den Umständen Folgendes ermöglichen:

a) die Fähigkeiten und Grenzen des Hochrisiko-KI-Systems vollständig zu verstehen und seinen Betrieb ordnungsgemäß zu überwachen, damit Anzeichen von Anomalien, Fehlfunktionen und unerwarteter Leistung so bald wie möglich erkannt und behoben werden können;

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

c) die Ergebnisse des Hochrisiko-KI-Systems richtig zu interpretieren, wobei insbesondere die Merkmale des Systems und die vorhandenen Interpretationswerkzeuge und -methoden zu berücksichtigen sind;

d) in einer bestimmten Situation zu beschließen, das Hochrisiko-KI-System nicht zu verwenden oder das Ergebnis des Hochrisiko-KI-Systems anderweitig 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.

(5) Bei den in Anhang III Nummer 1 Buchstabe a genannten Hochrisiko-KI-Systemen müssen die in Absatz 3 genannten Vorkehrungen so gestaltet sein, dass außerdem der Nutzer keine Maßnahmen oder Entscheidungen allein aufgrund des vom System hervorgebrachten Identifizierungsergebnisses trifft, solange dies nicht von mindestens zwei natürlichen Personen überprüft und bestätigt wurde.

Artikel 15
Genauigkeit, Robustheit und Cybersicherheit

(1) Hochrisiko-KI-Systeme werden so konzipiert und entwickelt, dass sie im Hinblick auf ihre Zweckbestimmung ein angemessenes Maß an Genauigkeit, Robustheit und Cybersicherheit erreichen und in dieser Hinsicht während ihres gesamten Lebenszyklus beständig funktionieren.

(2) Die Genauigkeitsgrade und die relevanten Genauigkeitskennzahlen von Hochrisiko-KI-Systemen werden in der ihnen beigefügten Gebrauchsanweisung angegeben.

(3) Hochrisiko-KI-Systeme müssen widerstandsfähig gegenüber Fehlern, Störungen oder Unstimmigkeiten sein, die innerhalb des Systems oder der Umgebung, in der das System betrieben wird, insbesondere wegen seiner Interaktion mit natürlichen Personen oder anderen Systemen auftreten können.

Die Robustheit von Hochrisiko-KI-Systemen kann durch technische Redundanz erreicht werden, was auch Sicherungs- oder Störungssicherheitspläne umfassen kann.

Hochrisiko-KI-Systeme, die nach dem Inverkehrbringen oder der Inbetriebnahme weiterhin dazulernen, sind so zu entwickeln, dass auf möglicherweise verzerrte Ergebnisse, die durch eine Verwendung vorheriger Ergebnisse als Eingabedaten für den künftigen Betrieb entstehen („Rückkopplungsschleifen"), angemessen mit geeigneten Risikominderungsmaßnahmen eingegangen wird.

(4) Hochrisiko-KI-Systeme müssen widerstandfähig gegen Versuche unbefugter Dritter sein, ihre Verwendung oder Leistung durch Ausnutzung von Systemschwachstellen zu verändern.

Die technischen Lösungen zur Gewährleistung der Cybersicherheit von Hochrisiko-KI-Systemen müssen den jeweiligen Umständen und Risiken angemessen sein.

Die technischen Lösungen für den Umgang mit KI-spezifischen Schwachstellen umfassen gegebenenfalls Maßnahmen zur Verhütung und Kontrolle von Angriffen, mit denen versucht wird, den Trainingsdatensatz zu manipulieren („Datenvergiftung"), von Eingabedaten, die das Modell zu Fehlern verleiten sollen („feindliche Beispiele"), oder von Modellmängeln.

KAPITEL 3

PFLICHTEN DER ANBIETER UND NUTZER VON HOCHRISIKO-KI-SYSTEMEN UND ANDERER BETEILIGTER

Artikel 16
Pflichten der Anbieter von Hochrisiko-KI-Systemen

Anbieter von Hochrisiko-KI-Systemen müssen

a) sicherstellen, dass ihre Hochrisiko-KI-Systeme die Anforderungen in Kapitel 2 dieses Titels erfüllen;

b) über ein Qualitätsmanagementsystem verfügen, das dem Artikel 17 entspricht;

c) die technische Dokumentation des Hochrisiko-KI-Systems erstellen;

d) die von ihren Hochrisiko-KI-Systemen automatisch erzeugten Protokolle aufbewahren, wenn dies ihrer Kontrolle unterliegt;

e) sicherstellen, dass das Hochrisiko-KI-System dem betreffenden Konformitätsbewertungsverfahren unterzogen wird, bevor es in Verkehr gebracht oder in Betrieb genommen wird;

f) den in Artikel 51 genannten Registrierungspflichten nachkommen;

g) die erforderlichen Korrekturmaßnahmen ergreifen, wenn das Hochrisiko-KI-System die Anforderungen in Kapitel 2 dieses Titels nicht erfüllt;

h) die zuständigen nationalen Behörden der Mitgliedstaaten, in denen sie das System bereitgestellt oder in Betrieb genommen haben, und gegebenenfalls die notifizierte

Stelle über die Nichtkonformität und bereits ergriffene Korrekturmaßnahmen informieren;

i) die CE-Kennzeichnung an ihren Hochrisiko-KI-Systemen anbringen, um die Konformität mit dieser Verordnung gemäß Artikel 49 anzuzeigen;

j) auf Anfrage einer zuständigen nationalen Behörde nachweisen, dass das Hochrisiko-KI-System die Anforderungen in Kapitel 2 dieses Titels erfüllt.

Artikel 17
Qualitätsmanagementsystem

(1) Anbieter von Hochrisiko-KI-Systemen richten ein Qualitätsmanagementsystem ein, das die Einhaltung dieser Verordnung gewährleistet. Dieses System wird systematisch und ordnungsgemäß in Form schriftlicher Regeln, Verfahren und Anweisungen dokumentiert und umfasst mindestens folgende Aspekte:

a) ein Konzept zur Einhaltung der Regulierungsvorschriften, was die Einhaltung der Konformitätsbewertungsverfahren und der Verfahren für das Management von Änderungen an den Hochrisiko-KI-Systemen miteinschließt;

b) Techniken, Verfahren und systematische Maßnahmen für den Entwurf, die Entwurfskontrolle und die Entwurfsprüfung des Hochrisiko-KI-Systems;

c) Techniken, Verfahren und systematische Maßnahmen für die Entwicklung, Qualitätskontrolle und Qualitätssicherung des Hochrisiko-KI-Systems;

d) Untersuchungs-, Test- und Validierungsverfahren, die vor, während und nach der Entwicklung des Hochrisiko-KI-Systems durchzuführen sind, und die Häufigkeit der Durchführung;

e) die technischen Spezifikationen und Normen, die anzuwenden sind, falls die einschlägigen harmonisierten Normen nicht vollständig angewandt werden, sowie die Mittel, mit denen gewährleistet werden soll, dass das Hochrisiko-KI-System die Anforderungen in Kapitel 2 dieses Titels erfüllt;

f) Systeme und Verfahren für das Datenmanagement, einschließlich Datenerfassung, Datenanalyse, Datenkennzeichnung, Datenspeicherung, Datenfilterung, Datenauswertung, Datenaggregation, Vorratsdatenspeicherung und sonstiger Vorgänge in Bezug auf die Daten, die im Vorfeld und für die Zwecke des Inverkehrbringens oder der Inbetriebnahme von Hochrisiko-KI-Systemen durchgeführt werden;

g) das in Artikel 9 genannte Risikomanagementsystem;

h) Einrichtung, Anwendung und Aufrechterhaltung eines Systems zur Beobachtung nach dem Inverkehrbringen gemäß Artikel 61;

i) Verfahren zur Meldung schwerwiegender Vorfälle und Fehlfunktionen gemäß Artikel 62;

j) Kommunikation mit zuständigen nationalen Behörden, zuständigen Behörden, auch sektoralen Behörden, die den Zugang zu Daten gewähren oder erleichtern, sowie mit notifizierten Stellen, anderen Akteuren, Kunden oder sonstigen interessierten Kreisen;

k) Systeme und Verfahren für die Aufzeichnung aller einschlägigen Unterlagen und Informationen;

l) Ressourcenmanagement, einschließlich Maßnahmen im Hinblick auf die Versorgungssicherheit;

m) einen Rechenschaftsrahmen, der die Verantwortlichkeiten der Leitung und des sonstigen Personals in Bezug auf alle in diesem Absatz aufgeführten Aspekte regelt.

(2) Die Umsetzung der in Absatz 1 genannten Aspekte erfolgt in einem angemessenen Verhältnis zur Größe der Organisation des Anbieters.

(3) Bei Anbietern, die Kreditinstitute im Sinne der Richtlinie 2013/36/EU sind, gilt die Verpflichtung zur Einrichtung eines Qualitätsmanagementsystems als erfüllt, wenn die Vorschriften über Regelungen, Verfahren und Mechanismen der internen Unternehmensführung gemäß Artikel 74 der genannten Richtlinie eingehalten werden. Dabei werden die in Artikel 40 dieser Verordnung genannten harmonisierten Normen berücksichtigt.

Artikel 18
Pflicht zur Erstellung der technischen Dokumentation

(1) Anbieter von Hochrisiko-KI-Systemen erstellen die in Artikel 11 genannte technische Dokumentation gemäß Anhang IV.

(2) Anbieter, die Kreditinstitute im Sinne der Richtlinie 2013/36/EU sind, pflegen die technische Dokumentation als Teil ihrer Dokumentation über die Regelungen, Verfahren und Mechanismen der internen Unternehmensführung gemäß Artikel 74 der genannten Richtlinie.

Artikel 19
Konformitätsbewertung

(1) Die Anbieter von Hochrisiko-KI-Systemen stellen sicher, dass ihre Systeme vor dem Inverkehrbringen oder der Inbetriebnahme dem betreffenden Konformitätsbewertungsverfahren gemäß Artikel 43 unterzogen werden. Wurde infolge dieser Konformitätsbewertung nachgewiesen, dass die KI-Systeme die Anforderungen in Kapitel 2 dieses Titels erfüllen, erstellen die Anbieter eine EU-Konformitätserklärung gemäß Artikel 48 und bringen die CE-Konformitätskennzeichnung gemäß Artikel 49 an.

(2) Bei den in Anhang III Nummer 5 Buchstabe b genannten Hochrisiko-KI-Systemen, die von Anbietern in Verkehr gebracht oder in Betrieb genommen werden, die Kreditinstitute im Sinne der Richtlinie 2013/36/EU sind, erfolgt die Konformitätsbewertung im Rahmen des in den Artikeln 97 bis 101 der Richtlinie genannten Verfahrens.

Artikel 20
Automatisch erzeugte Protokolle

(1) Anbieter von Hochrisiko-KI-Systemen bewahren die von ihren Hochrisiko-KI-Systemen automatisch erzeugten Protokolle auf, soweit diese Protokolle aufgrund einer vertraglichen Vereinbarung mit dem Nutzer oder auf gesetzlicher Grundlage ihrer Kontrolle unterliegen. Die Protokolle werden für einen Zeitraum aufbewahrt, der der Zweckbestimmung des Hochrisiko-KI-Systems und den geltenden

rechtlichen Verpflichtungen nach Unionsrecht oder nationalem Recht angemessen ist.

(2) Anbieter, die Kreditinstitute im Sinne der Richtlinie 2013/36/EU sind, bewahren die von ihren Hochrisiko-KI-Systemen automatisch erzeugten Protokolle als Teil der Dokumentation gemäß Artikel 74 der Richtlinie auf.

Artikel 21
Korrekturmaßnahmen

Anbieter von Hochrisiko-KI-Systemen, die der Auffassung sind oder Grund zu der Annahme haben, dass ein von ihnen in Verkehr gebrachtes oder in Betrieb genommenes Hochrisiko-KI-System nicht dieser Verordnung entspricht, ergreifen unverzüglich die erforderlichen Korrekturmaßnahmen, um die Konformität dieses Systems herzustellen oder es gegebenenfalls zurückzunehmen oder zurückzurufen. Sie setzen die Händler des betreffenden Hochrisiko-KI-Systems und gegebenenfalls den Bevollmächtigten und die Einführer davon in Kenntnis.

Artikel 22
Informationspflicht

Birgt das Hochrisiko-KI-System ein Risiko im Sinne des Artikels 65 Absatz 1 und ist dem Anbieter des Systems dieses Risiko bekannt, so informiert dieser Anbieter unverzüglich die zuständigen nationalen Behörden der Mitgliedstaaten, in denen er das System bereitgestellt hat, und gegebenenfalls die notifizierte Stelle, die eine Bescheinigung für das Hochrisiko-KI-System ausgestellt hat, und macht dabei ausführliche Angaben, insbesondere zur Nichtkonformität und zu bereits ergriffenen Korrekturmaßnahmen.

Artikel 23
Zusammenarbeit mit den zuständigen Behörden

Anbieter von Hochrisiko-KI-Systemen übermitteln einer zuständigen nationalen Behörde auf deren Verlangen alle Informationen und Unterlagen, die erforderlich sind, um die Konformität des Hochrisiko-KI-Systems mit den Anforderungen in Kapitel 2 dieses Titels nachzuweisen, in einer von dem betreffenden Mitgliedstaat festgelegten Amtssprache der Union. Auf begründetes Verlangen einer zuständigen nationalen Behörde gewähren die Anbieter dieser Behörde auch Zugang zu den von ihrem Hochrisiko-KI-System automatisch erzeugten Protokollen, soweit diese Protokolle aufgrund einer vertraglichen Vereinbarung mit dem Nutzer oder auf gesetzlicher Grundlage ihrer Kontrolle unterliegen.

Artikel 24
Pflichten der Produkthersteller

Wird ein Hochrisiko-KI-System für Produkte, die unter die in Anhang II Abschnitt A aufgeführten Rechtsakte fallen, zusammen mit dem gemäß diesen Rechtsvorschriften hergestellten Produkt unter dem Namen des Produktherstellers in Verkehr gebracht oder in Betrieb genommen, so übernimmt der Hersteller des Produkts die Verantwortung für die Konformität des KI-Systems mit dieser Verordnung und hat in Bezug auf das KI-System dieselben Pflichten, die dem Anbieter durch diese Verordnung auferlegt werden.

Artikel 25
Bevollmächtigte

(1) Anbieter, die außerhalb der Union niedergelassen sind, benennen vor der Bereitstellung ihrer Systeme in der Union schriftlich einen in der Union niedergelassenen Bevollmächtigten, wenn kein Einführer festgestellt werden kann.

(2) Der Bevollmächtigte nimmt die Aufgaben wahr, die in seinem vom Anbieter erhaltenen Auftrag festgelegt sind. Der Auftrag ermächtigt den Bevollmächtigten zumindest zur Wahrnehmung folgender Aufgaben:

a) Bereithaltung eines Exemplars der EU-Konformitätserklärung und der technischen Dokumentation für die zuständigen nationalen Behörden und die in Artikel 63 Absatz 7 genannten nationalen Behörden;

b) Übermittlung aller Informationen und Unterlagen, die erforderlich sind, um die Konformität eines Hochrisiko-KI-Systems mit den Anforderungen in Kapitel 2 dieses Titels nachzuweisen, an eine zuständige nationale Behörde auf deren begründetes Verlangen, einschließlich der Gewährung des Zugangs zu den vom Hochrisiko-KI-System automatisch erzeugten Protokollen, soweit diese Protokolle aufgrund einer vertraglichen Vereinbarung mit dem Nutzer oder auf gesetzlicher Grundlage der Kontrolle des Anbieters unterliegen;

c) Zusammenarbeit mit den zuständigen nationalen Behörden auf deren begründetes Verlangen bei allen Maßnahmen, die Letztere im Zusammenhang mit dem Hochrisiko-KI-System ergreifen.

Artikel 26
Pflichten der Einführer

(1) Bevor sie ein Hochrisiko-KI-System in Verkehr bringen, stellen die Einführer solcher Systeme sicher, dass

a) der Anbieter des KI-Systems das betreffende Konformitätsbewertungsverfahren durchgeführt hat;

b) der Anbieter die technische Dokumentation gemäß Anhang IV erstellt hat;

c) das System mit der erforderlichen Konformitätskennzeichnung versehen ist und ihm die erforderlichen Unterlagen und Gebrauchsanweisungen beigefügt sind.

(2) Ist ein Einführer der Auffassung oder hat er Grund zu der Annahme, dass ein Hochrisiko-KI-System nicht dieser Verordnung entspricht, so bringt er dieses Hochrisiko-KI-System erst in Verkehr, nachdem die Konformität dieses Systems hergestellt worden ist. Birgt das Hochrisiko-KI-System ein Risiko im Sinne des Artikels 65 Absatz 1, so setzt der Einführer den Anbieter des KI-Systems und die Marktüberwachungsbehörden davon in Kenntnis.

(3) Die Einführer geben ihren Namen, ihren eingetragenen Handelsnamen oder ihre eingetragene Handelsmarke und ihre Kontaktanschrift auf dem Hochrisiko-KI-System selbst oder, wenn dies nicht möglich ist, auf der Verpackung oder in der beigefügten Dokumentation an.

(4) Solange sich ein Hochrisiko-KI-System in ihrer Verantwortung befindet, gewährleisten die Einführer, dass – soweit zutreffend – die Lagerungs- oder

Transportbedingungen dessen Konformität mit den Anforderungen in Kapitel 2 dieses Titels nicht beeinträchtigen.

(5) Die Einführer übermitteln den zuständigen nationalen Behörden auf deren begründetes Verlangen alle Informationen und Unterlagen zum Nachweis der Konformität eines Hochrisiko-KI-Systems mit den Anforderungen in Kapitel 2 dieses Titels in einer Sprache, die für die betreffende zuständige nationale Behörde leicht verständlich ist, und gewähren ihr Zugang zu den vom Hochrisiko-KI-System automatisch erzeugten Protokollen, soweit diese Protokolle aufgrund einer vertraglichen Vereinbarung mit dem Nutzer oder auf gesetzlicher Grundlage der Kontrolle des Anbieters unterliegen. Sie arbeiten außerdem mit diesen Behörden bei allen Maßnahmen zusammen, die eine zuständige nationale Behörde im Zusammenhang mit diesem System ergreift.

Artikel 27
Pflichten der Händler

(1) Bevor Händler ein Hochrisiko-KI-System auf dem Markt bereitstellen, überprüfen sie, ob das Hochrisiko-KI-System mit der erforderlichen CE-Konformitätskennzeichnung versehen ist, ob ihm die erforderliche Dokumentation und Gebrauchsanweisung beigefügt sind und ob der Anbieter bzw. gegebenenfalls der Einführer des Systems die in dieser Verordnung festgelegten Pflichten erfüllt hat.

(2) Ist ein Händler der Auffassung oder hat er Grund zu der Annahme, dass ein Hochrisiko-KI-System nicht den Anforderungen in Kapitel 2 dieses Titels entspricht, so stellt er das Hochrisiko-KI-System erst auf dem Markt bereit, nachdem die Konformität mit den Anforderungen hergestellt worden ist. Birgt das System zudem ein Risiko im Sinne des Artikels 65 Absatz 1, so setzt der Händler den Anbieter bzw. den Einführer des Systems davon in Kenntnis.

(3) Solange sich ein Hochrisiko-KI-System in ihrer Verantwortung befindet, gewährleisten die Händler, dass – soweit zutreffend – die Lagerungs- oder Transportbedingungen die Konformität des Systems mit den Anforderungen in Kapitel 2 dieses Titels nicht beeinträchtigen.

(4) Ein Händler, der der Auffassung ist oder Grund zu der Annahme hat, dass ein von ihm auf dem Markt bereitgestelltes Hochrisiko-KI-System nicht den Anforderungen in Kapitel 2 dieses Titels entspricht, ergreift die erforderlichen Korrekturmaßnahmen, um die Konformität dieses Systems mit diesen Anforderungen herzustellen, es zurückzunehmen oder zurückzurufen, oder er stellt sicher, dass der Anbieter, der Einführer oder gegebenenfalls jeder relevante Akteur diese Korrekturmaßnahmen ergreift. Birgt das Hochrisiko-KI-System ein Risiko im Sinne des Artikels 65 Absatz 1, so informiert der Händler unverzüglich die zuständigen nationalen Behörden der Mitgliedstaaten, in denen er das System bereitgestellt hat, und macht dabei ausführliche Angaben, insbesondere zur Nichtkonformität und zu bereits ergriffenen Korrekturmaßnahmen.

(5) Auf begründetes Verlangen einer zuständigen nationalen Behörde übermitteln die Händler von Hochrisiko-KI-Systemen dieser Behörde alle Informationen und Unterlagen, die erforderlich sind, um die Konformität eines Hochrisiko-KI-Systems mit den Anforderungen in Kapitel 2 dieses Titels nachzuweisen. Die Händler arbeiten außerdem mit dieser zuständigen nationalen Behörde bei allen von dieser Behörde ergriffenen Maßnahmen zusammen.

Artikel 28
Pflichten der Händler, Einführer, Nutzer oder sonstiger Dritter

(1) In den folgenden Fällen gelten Händler, Einführer, Nutzer oder sonstige Dritte als Anbieter für die Zwecke dieser Verordnung und unterliegen den Anbieterpflichten gemäß Artikel 16:

a) wenn sie ein Hochrisiko-KI-System unter ihrem Namen oder ihrer Marke in Verkehr bringen oder in Betrieb nehmen;

b) wenn sie die Zweckbestimmung eines bereits im Verkehr befindlichen oder in Betrieb genommenen Hochrisiko-KI-Systems verändern;

c) wenn sie eine wesentliche Änderung an dem Hochrisiko-KI-System vornehmen.

(2) Unter den in Absatz 1 Buchstabe b oder c genannten Umständen gilt der Anbieter, der das Hochrisiko-KI-System ursprünglich in Verkehr gebracht oder in Betrieb genommen hatte, nicht mehr als Anbieter für die Zwecke dieser Verordnung.

Artikel 29
Pflichten der Nutzer von Hochrisiko-KI-Systemen

(1) Die Nutzer von Hochrisiko-KI-Systemen verwenden solche Systeme entsprechend der den Systemen beigefügten Gebrauchsanweisung und gemäß den Absätzen 2 und 5.

(2) Die Pflichten nach Absatz 1 lassen sonstige Pflichten der Nutzer nach Unionsrecht oder nationalem Recht sowie das Ermessen der Nutzer bei der Organisation ihrer eigenen Ressourcen und Tätigkeiten zur Wahrnehmung der vom Anbieter angegebenen Maßnahmen der menschlichen Aufsicht unberührt.

(3) Unbeschadet des Absatzes 1 und soweit die Eingabedaten seiner Kontrolle unterliegen, sorgen die Nutzer dafür, dass die Eingabedaten der Zweckbestimmung des Hochrisiko-KI-Systems entsprechen.

(4) Die Nutzer überwachen den Betrieb des Hochrisiko-KI-Systems anhand der Gebrauchsanweisung. Haben sie Grund zu der Annahme, dass die Verwendung gemäß der Gebrauchsanweisung dazu führen kann, dass das Hochrisiko-KI-System ein Risiko im Sinne des Artikels 65 Absatz 1 birgt, so informieren sie den Anbieter oder Händler und setzen die Verwendung des Systems aus. Sie informieren den Anbieter oder Händler auch, wenn sie einen schwerwiegenden Vorfall oder eine Fehlfunktion im Sinne des Artikels 62 festgestellt haben, und unterbrechen die Verwendung des KI-Systems. Kann der Nutzer den Anbieter nicht erreichen, so gilt Artikel 62 entsprechend.

Bei Nutzern, die Kreditinstitute im Sinne der Richtlinie 2013/36/EU sind, gilt die in Unterabsatz 1 vorgesehene Überwachungspflicht als erfüllt, wenn die Vorschriften über Regelungen, Verfahren und Mechanismen der internen Unternehmensführung gemäß Artikel 74 der genannten Richtlinie eingehalten werden.

(5) Nutzer von Hochrisiko-KI-Systemen bewahren die von ihrem Hochrisiko-KI-System automatisch erzeugten Protokolle auf, soweit diese Protokolle ihrer Kontrolle unterliegen. Die Protokolle werden für einen Zeitraum aufbewahrt, der der Zweckbestimmung des Hochrisiko-KI-Systems und den geltenden rechtlichen Verpflichtungen nach Unionsrecht oder nationalem Recht angemessen ist.

Nutzer, die Kreditinstitute im Sinne der Richtlinie 2013/36/EU sind, bewahren die Protokolle als Teil ihrer Dokumentation über die Regelungen, Verfahren und Mechanismen der internen Unternehmensführung gemäß Artikel 74 der genannten Richtlinie auf.

(6) Die Nutzer von Hochrisiko-KI-Systemen verwenden die gemäß Artikel 13 bereitgestellten Informationen, um gegebenenfalls ihrer Verpflichtung zur Durchführung einer Datenschutz-Folgenabschätzung gemäß Artikel 35 der Verordnung (EU) 2016/679 oder Artikel 27 der Richtlinie (EU) 2016/680 nachzukommen.

KAPITEL 4

NOTIFIZIERENDE BEHÖRDEN UND NOTIFIZIERTE STELLEN

Artikel 30
Notifizierende Behörden

(1) Jeder Mitgliedstaat sorgt für die Benennung oder Schaffung einer notifizierenden Behörde, die für die Einrichtung und Durchführung der erforderlichen Verfahren zur Bewertung, Benennung und Notifizierung von Konformitätsbewertungsstellen und für deren Überwachung zuständig ist.

(2) Die Mitgliedstaaten können eine nationale Akkreditierungsstelle im Sinne der Verordnung (EG) Nr. 765/2008 als notifizierende Behörde benennen.

(3) Notifizierende Behörden werden so eingerichtet, strukturiert und in ihren Arbeitsabläufen organisiert, dass jegliche Interessenkonflikte mit Konformitätsbewertungsstellen vermieden werden und die Objektivität und die Unparteilichkeit ihrer Tätigkeiten gewährleistet sind.

(4) Notifizierende Behörden werden so strukturiert, dass Entscheidungen über die Notifizierung von Konformitätsbewertungsstellen von kompetenten Personen getroffen werden, die nicht mit den Personen identisch sind, die die Bewertung dieser Stellen durchgeführt haben.

(5) Notifizierende Behörden dürfen weder Tätigkeiten, die Konformitätsbewertungsstellen durchführen, noch Beratungsleistungen auf einer gewerblichen oder wettbewerblichen Basis anbieten oder erbringen.

(6) Notifizierende Behörden gewährleisten die Vertraulichkeit der von ihnen erlangten Informationen.

(7) Notifizierende Behörden verfügen über kompetente Mitarbeiter in ausreichender Zahl, sodass sie ihre Aufgaben ordnungsgemäß wahrnehmen können.

(8) Notifizierende Behörden gewährleisten, dass Konformitätsbewertungen in angemessener Art und Weise und ohne unnötige Belastungen für die Anbieter durchgeführt werden und dass die notifizierten Stellen bei ihren Tätigkeiten die Größe eines Unternehmens, die Branche, in der es tätig ist, seine Struktur und die Komplexität des betreffenden KI-Systems gebührend berücksichtigen.

Artikel 31
Antrag einer Konformitätsbewertungsstelle auf Notifizierung

(1) Konformitätsbewertungsstellen beantragen ihre Notifizierung bei der notifizierenden Behörde des Mitgliedstaats, in dem sie ansässig sind.

(2) Dem Antrag auf Notifizierung legen sie eine Beschreibung der Konformitätsbewertungstätigkeiten, des/der Konformitätsbewertungsverfahren(s) und der Technologien der künstlichen Intelligenz, für die diese Konformitätsbewertungsstelle Kompetenz beansprucht, sowie, falls vorhanden, eine Akkreditierungsurkunde bei, die von einer nationalen Akkreditierungsstelle ausgestellt wurde und in der bescheinigt wird, dass die Konformitätsbewertungsstelle die Anforderungen des Artikels 33 erfüllt. Sonstige gültige Dokumente in Bezug auf bestehende Benennungen der antragstellenden notifizierten Stelle im Rahmen anderer Harmonisierungsrechtsvorschriften der Union sind ebenfalls beizufügen.

(3) Kann die Konformitätsbewertungsstelle keine Akkreditierungsurkunde vorweisen, so legt sie der notifizierenden Behörde als Nachweis alle Unterlagen vor, die erforderlich sind, um zu überprüfen, festzustellen und regelmäßig zu überwachen, ob sie die Anforderungen des Artikels 33 erfüllt. Bei notifizierten Stellen, die im Rahmen anderer Harmonisierungsrechtsvorschriften der Union benannt wurden, können alle Unterlagen und Bescheinigungen im Zusammenhang mit solchen Benennungen zur Unterstützung ihres Benennungsverfahrens nach dieser Verordnung verwendet werden.

Artikel 32
Notifizierungsverfahren

(1) Die notifizierenden Behörden dürfen nur Konformitätsbewertungsstellen notifizieren, die die Anforderungen des Artikels 33 erfüllen.

(2) Die notifizierenden Behörden unterrichten die Kommission und die übrigen Mitgliedstaaten mithilfe des elektronischen Notifizierungsinstruments, das von der Kommission entwickelt und verwaltet wird.

(3) Eine Notifizierung enthält vollständige Angaben zu den Konformitätsbewertungstätigkeiten, dem/den betreffenden Konformitätsbewertungsmodul(en) und den betreffenden Technologien der künstlichen Intelligenz.

(4) Die betreffende Konformitätsbewertungsstelle darf die Aufgaben einer notifizierten Stelle nur dann wahrnehmen, wenn weder die Kommission noch die übrigen Mitgliedstaaten innerhalb von einem Monat nach der Notifizierung Einwände erhoben haben.

(5) Die notifizierenden Behörden melden der Kommission und den übrigen Mitgliedstaaten jede später eintretende Änderung der Notifizierung.

Artikel 33
Notifizierte Stellen

(1) Die notifizierten Stellen überprüfen die Konformität von Hochrisiko-KI-Systemen nach den in Artikel 43 genannten Konformitätsbewertungsverfahren.

(2) Die notifizierten Stellen müssen die Anforderungen an die Organisation, das Qualitätsmanagement, die Ressourcenausstattung und die Verfahren erfüllen, die zur Wahrnehmung ihrer Aufgaben erforderlich sind.

(3) Die Organisationsstruktur, die Zuweisung der Zuständigkeiten, die Berichtslinien und die Funktionsweise der notifizierten Stellen sind so gestaltet, dass sie die Zuverlässigkeit der Leistung der notifizierten Stelle und das Vertrauen in die Ergebnisse der von ihr durchgeführten Konformitätsbewertungstätigkeiten gewährleisten.

(4) Die notifizierten Stellen sind von dem Anbieter eines Hochrisiko-KI-Systems, zu dem sie Konformitätsbewertungstätigkeiten durchführen, unabhängig. Außerdem sind die notifizierten Stellen von allen anderen Akteuren, die ein wirtschaftliches Interesse an dem bewerteten Hochrisiko-KI-System haben, und von allen Wettbewerbern des Anbieters unabhängig.

(5) Die notifizierten Stellen gewährleisten durch ihre Organisation und Arbeitsweise, dass bei der Ausübung ihrer Tätigkeit Unabhängigkeit, Objektivität und Unparteilichkeit gewahrt sind. Von den notifizierten Stellen werden eine Struktur und Verfahren dokumentiert und umgesetzt, die ihre Unparteilichkeit gewährleisten und sicherstellen, dass die Grundsätze der Unparteilichkeit in ihrer gesamten Organisation und von allen Mitarbeitern und bei allen Bewertungstätigkeiten gefördert und angewandt werden.

(6) Die notifizierten Stellen gewährleisten durch dokumentierte Verfahren, dass ihre Mitarbeiter, Ausschüsse, Zweigstellen, Unterauftragnehmer sowie alle zugeordneten Stellen oder Mitarbeiter externer Einrichtungen die Vertraulichkeit der Informationen, die bei der Durchführung der Konformitätsbewertungstätigkeiten in ihren Besitz gelangen, wahren, außer wenn die Offenlegung gesetzlich vorgeschrieben ist. Informationen, von denen Mitarbeiter der notifizierten Stellen bei der Durchführung ihrer Aufgaben gemäß dieser Verordnung Kenntnis erlangen, unterliegen der beruflichen Schweigepflicht, außer gegenüber den notifizierenden Behörden des Mitgliedstaats, in dem sie ihre Tätigkeiten ausüben.

(7) Die notifizierten Stellen verfügen über Verfahren zur Durchführung ihrer Tätigkeiten unter gebührender Berücksichtigung der Größe eines Unternehmens, der Branche, in der es tätig ist, seiner Struktur sowie der Komplexität des betreffenden KI-Systems.

(8) Die notifizierten Stellen schließen eine angemessene Haftpflichtversicherung für ihre Konformitätsbewertungstätigkeiten ab, es sei denn, diese Haftpflicht wird aufgrund nationalen Rechts von dem betreffenden Mitgliedstaat gedeckt oder dieser Mitgliedstaat ist unmittelbar für die Durchführung der Konformitätsbewertung zuständig.

(9) Die notifizierten Stellen sind in der Lage, die ihnen durch diese Verordnung zufallenden Aufgaben mit höchster beruflicher Integrität und der erforderlichen Fachkompetenz in dem betreffenden Bereich auszuführen, gleichgültig, ob diese Aufgaben von den notifizierten Stellen selbst oder in ihrem Auftrag und in ihrer Verantwortung erfüllt werden.

(10) Die notifizierten Stellen verfügen über ausreichende interne Kompetenzen, um die von externen Stellen in ihrem Namen wahrgenommen Aufgaben wirksam beurteilen zu können. Dazu müssen die notifizierten Stellen jederzeit für jedes Konformitätsbewertungsverfahren und für jede Art von Hochrisiko-KI-Systemen, für die sie benannt wurden, ständig über ausreichendes administratives, technisches und

wissenschaftliches Personal verfügen, das die entsprechenden Erfahrungen und Kenntnisse in Bezug auf einschlägige KI-Technik, Daten und Datenverarbeitung sowie die Anforderungen in Kapitel 2 dieses Titels besitzt.

(11) Die notifizierten Stellen wirken an den in Artikel 38 genannten Koordinierungstätigkeiten mit. Sie wirken außerdem unmittelbar oder mittelbar an der Arbeit der europäischen Normungsorganisationen mit oder stellen sicher, dass sie stets über den Stand der einschlägigen Normen unterrichtet sind.

(12) Die notifizierten Stellen machen der in Artikel 30 genannten notifizierenden Behörde alle einschlägigen Unterlagen, einschließlich der Unterlagen des Anbieters, zugänglich bzw. übermitteln diese auf Anfrage, damit diese ihre Bewertungs-, Benennungs-, Notifizierungs-, Überwachungs- und Kontrollaufgaben wahrnehmen kann und die Bewertung gemäß diesem Kapitel erleichtert wird.

Artikel 34

Zweigstellen notifizierter Stellen und Vergabe von Unteraufträgen durch notifizierte Stellen

(1) Vergibt die notifizierte Stelle bestimmte mit der Konformitätsbewertung verbundene Aufgaben an Unterauftragnehmer oder überträgt sie diese einer Zweigstelle, so stellt sie sicher, dass der Unterauftragnehmer oder die Zweigstelle die Anforderungen des Artikels 33 erfüllt, und setzt die notifizierende Behörde davon in Kenntnis.

(2) Die notifizierten Stellen tragen die volle Verantwortung für die Arbeiten, die von Unterauftragnehmern oder Zweigstellen ausgeführt werden, unabhängig davon, wo diese niedergelassen sind.

(3) Arbeiten dürfen nur mit Zustimmung des Anbieters an einen Unterauftragnehmer vergeben oder einer Zweigstelle übertragen werden.

(4) Die notifizierten Stellen halten für die notifizierende Behörde die einschlägigen Unterlagen über die Bewertung der Qualifikation des Unterauftragnehmers oder der Zweigstelle und die von ihnen gemäß dieser Verordnung ausgeführten Arbeiten bereit.

Artikel 35

Kennnummern und Verzeichnisse der nach dieser Verordnung benannten notifizierten Stellen

(1) Die Kommission weist den notifizierten Stelle jeweils eine Kennnummer zu. Selbst wenn eine Stelle nach mehreren Rechtsakten der Union notifiziert worden ist, erhält sie nur eine einzige Kennnummer.

(2) Die Kommission veröffentlicht das Verzeichnis der nach dieser Verordnung notifizierten Stellen samt den ihnen zugewiesenen Kennnummern und den Tätigkeiten, für die sie notifiziert wurden. Die Kommission hält das Verzeichnis stets auf dem neuesten Stand.

Artikel 36

Änderungen der Notifizierungen

(1) Falls eine notifizierende Behörde vermutet oder darüber unterrichtet wird, dass eine notifizierte Stelle die in Artikel 33 festgelegten Anforderungen nicht mehr erfüllt oder dass sie ihren Verpflichtungen nicht nachkommt, so untersucht die den Sachverhalt unverzüglich und mit äußerster Sorgfalt. In diesem Zusammenhang teilt sie der betreffenden notifizierten Stelle die erhobenen Einwände mit und gibt ihr die

Möglichkeit, dazu Stellung zu nehmen. Kommt die notifizierende Behörde zu dem Schluss, dass die überprüfte notifizierte Stelle die in Artikel 33 festgelegten Anforderungen nicht mehr erfüllt oder dass sie ihren Verpflichtungen nicht nachkommt, schränkt sie die Notifizierung gegebenenfalls ein, setzt sie aus oder widerruft sie, wobei sie das Ausmaß der Nichterfüllung oder Pflichtverletzung berücksichtigt. Sie setzt zudem die Kommission und die übrigen Mitgliedstaaten unverzüglich davon in Kenntnis.

(2) Wird die Notifizierung widerrufen, eingeschränkt oder ausgesetzt oder stellt die notifizierte Stelle ihre Tätigkeit ein, so ergreift die notifizierende Behörde geeignete Maßnahmen, um sicherzustellen, dass die Akten dieser notifizierten Stelle von einer anderen notifizierten Stelle übernommen bzw. für die zuständigen notifizierenden Behörden auf deren Verlangen bereitgehalten werden.

Artikel 37
Anfechtungen der Kompetenz notifizierter Stellen

(1) Die Kommission untersucht erforderlichenfalls alle Fälle, in denen begründete Zweifel daran bestehen, dass eine notifizierte Stelle die in Artikel 33 festgelegten Anforderungen erfüllt.

(2) Die notifizierende Behörde stellt der Kommission auf Anfrage alle Informationen über die Notifizierung der betreffenden notifizierten Stelle zur Verfügung.

(3) Die Kommission stellt sicher, dass alle im Verlauf ihrer Untersuchungen gemäß diesem Artikel erlangten vertraulichen Informationen vertraulich behandelt werden.

(4) Stellt die Kommission fest, dass eine notifizierte Stelle die in Artikel 33 festgelegten Anforderungen nicht oder nicht mehr erfüllt, so erlässt sie einen begründeten Beschluss, in dem der notifizierende Mitgliedstaat aufgefordert wird, die erforderlichen Abhilfemaßnahmen zu treffen, einschließlich eines Widerrufs der Notifizierung, sofern dies nötig ist. Dieser Durchführungsrechtsakt wird gemäß dem in Artikel 74 Absatz 2 genannten Prüfverfahren erlassen.

Artikel 38
Koordinierung der notifizierten Stellen

(1) Die Kommission sorgt dafür, dass in den von dieser Verordnung erfassten Bereichen eine zweckmäßige Koordinierung und Zusammenarbeit zwischen den an den Konformitätsbewertungsverfahren für KI-Systeme im Rahmen dieser Verordnung beteiligten notifizierten Stellen in Form einer sektoralen Gruppe notifizierter Stellen eingerichtet und ordnungsgemäß weitergeführt wird.

(2) Die Mitgliedstaaten sorgen dafür, dass sich die von ihnen notifizierten Stellen direkt oder über benannte Vertreter an der Arbeit dieser Gruppe beteiligen.

Artikel 39
Konformitätsbewertungsstellen in Drittländern

Konformitätsbewertungsstellen, die nach dem Recht eines Drittlandes errichtet wurden, mit dem die Union ein Abkommen geschlossen hat, können ermächtigt werden, die Tätigkeiten notifizierter Stellen gemäß dieser Verordnung durchzuführen.

KAPITEL 5

NORMEN, KONFORMITÄTSBEWERTUNG, BESCHEINIGUNGEN, REGISTRIERUNG

Artikel 40
Harmonisierte Normen

Bei Hochrisiko-KI-Systemen, die mit harmonisierten Normen oder Teilen davon, deren Fundstellen im *Amtsblatt der Europäischen Union* veröffentlicht wurden, übereinstimmen, wird eine Konformität mit den Anforderungen in Kapitel 2 dieses Artikels vermutet, soweit diese Anforderungen von den Normen abgedeckt sind.

Artikel 41
Gemeinsame Spezifikationen

(1) Gibt es keine harmonisierten Normen gemäß Artikel 40 oder ist die Kommission der Auffassung, dass die einschlägigen harmonisierten Normen unzureichend sind oder dass bestimmte Bedenken hinsichtlich der Sicherheit oder der Grundrechte ausgeräumt werden müssen, so kann die Kommission im Wege von Durchführungsrechtsakten gemeinsame Spezifikationen für die Anforderungen in Kapitel 2 dieses Titels festlegen. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 74 Absatz 2 genannten Prüfverfahren erlassen.

(2) Bei der Ausarbeitung der in Absatz 1 genannten gemeinsamen Spezifikationen holt die Kommission die Stellungnahmen der einschlägigen Stellen oder Expertengruppen ein, die nach den jeweiligen sektorspezifischen Rechtsvorschriften der Union eingerichtet wurden.

(3) Bei Hochrisiko-KI-Systemen, die mit den in Absatz 1 genannten gemeinsamen Spezifikationen übereinstimmen, wird eine Konformität mit den Anforderungen in Kapitel 2 dieses Artikels vermutet, soweit diese Anforderungen von den gemeinsamen Spezifikationen abgedeckt sind.

(4) Wenn Anbieter die in Absatz 1 genannten gemeinsamen Spezifikationen nicht befolgen, müssen sie hinreichend nachweisen, dass sie technische Lösungen verwenden, die den gemeinsamen Spezifikationen zumindest gleichwertig sind.

Artikel 42
Vermutung der Konformität mit gewissen Anforderungen

(1) Unter Berücksichtigung der Zweckbestimmung gilt für Hochrisiko-KI-Systeme, die mit Daten zu den besonderen geografischen, verhaltensbezogenen und funktionalen Rahmenbedingungen, unter denen sie bestimmungsgemäß verwendet werden sollen, trainiert und getestet wurden, die Vermutung, dass sie die in Artikel 10 Absatz 4 festgelegte Anforderung erfüllen.

(2) Für Hochrisiko-KI-Systeme, die im Rahmen eines der Cybersicherheitszertifizierungssysteme gemäß der Verordnung (EU) 2019/881 des

Europäischen Parlaments und des Rates[63], deren Fundstellen im *Amtsblatt der Europäischen Union* veröffentlicht wurden, zertifiziert wurden oder für die eine solche Konformitätserklärung erstellt wurde, gilt die Vermutung, dass sie die in Artikel 15 der vorliegenden Verordnung festgelegten Cybersicherheitsanforderungen erfüllen, sofern diese Anforderungen von der Cybersicherheitszertifizierung oder der Konformitätserklärung oder Teilen davon abdeckt sind.

Artikel 43
Konformitätsbewertung

(1) Hat ein Anbieter zum Nachweis, dass sein in Anhang III Nummer 1 aufgeführtes Hochrisiko-KI-System die Anforderungen in Kapitel 2 dieses Titels erfüllt, harmonisierte Normen gemäß Artikel 40 oder gegebenenfalls gemeinsame Spezifikationen gemäß Artikel 41 angewandt, so befolgt er eines der folgenden Verfahren:

(a) das Konformitätsbewertungsverfahren auf der Grundlage einer internen Kontrolle gemäß Anhang VI;

(b) das Konformitätsbewertungsverfahren auf der Grundlage der Bewertung des Qualitätsmanagementsystems und der Bewertung der technischen Dokumentation unter Beteiligung einer notifizierten Stelle gemäß Anhang VII.

Hat ein Anbieter zum Nachweis, dass sein Hochrisiko-KI-System die Anforderungen in Kapitel 2 dieses Titels erfüllt, die harmonisierten Normen gemäß Artikel 40 nicht oder nur teilweise angewandt oder gibt es solche harmonisierten Normen nicht und liegen keine gemeinsamen Spezifikationen gemäß Artikel 41 vor, so befolgt er das Konformitätsbewertungsverfahren gemäß Anhang VII.

Für die Zwecke des Konformitätsbewertungsverfahrens gemäß Anhang VII kann der Anbieter eine der notifizierten Stellen auswählen. Soll das System jedoch von Strafverfolgungs-, Einwanderungs- oder Asylbehörden oder von Organen, Einrichtungen oder sonstigen Stellen der EU in Betrieb genommen werden, so übernimmt die in Artikel 63 Absatz 5 oder 6 genannte Marktüberwachungsbehörde die Funktion der notifizierten Stelle.

(2) Bei den in Anhang III Nummern 2 bis 8 aufgeführten Hochrisiko-KI-Systemen befolgen die Anbieter das Konformitätsbewertungsverfahren auf der Grundlage einer internen Kontrolle gemäß Anhang VI, das keine Beteiligung einer notifizierten Stelle vorsieht. Bei den in Anhang III Nummer 5 Buchstabe b genannten Hochrisiko-KI-Systemen, die von Kreditinstituten im Sinne der Richtlinie 2013/36/EU in Verkehr gebracht oder in Betrieb genommen werden, erfolgt die Konformitätsbewertung im Rahmen des in den Artikeln 97 bis 101 der Richtlinie genannten Verfahrens.

(3) Bei den Hochrisiko-KI-Systemen, die unter die in Anhang II Abschnitt A aufgeführten Rechtsakte fallen, befolgt der Anbieter die einschlägigen Konformitätsbewertungsverfahren, die nach diesen Rechtsakten erforderlich sind. Die Anforderungen in Kapitel 2 dieses Titels gelten für diese Hochrisiko-KI-Systeme

[63] Verordnung (EU) 2019/881 des Europäischen Parlaments und des Rates vom 17. April 2019 über die ENISA (Agentur der Europäischen Union für Cybersicherheit) und über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik und zur Aufhebung der Verordnung (EU) Nr. 526/2013 (Rechtsakt zur Cybersicherheit) (ABl. L 151 vom 7.6.2019, S. 15).

und werden in diese Bewertung einbezogen. Anhang VII Nummern 4.3, 4.4, 4.5 und Nummer 4.6 Absatz 5 finden ebenfalls Anwendung.

Für die Zwecke dieser Bewertung sind die notifizierten Stellen, die gemäß diesen Rechtsakten benannt wurden, auch berechtigt, die Konformität der Hochrisiko-KI-Systeme mit den Anforderungen in Kapitel 2 dieses Titels zu kontrollieren, sofern im Rahmen des gemäß diesen Rechtsakten durchgeführten Notifizierungsverfahrens geprüft wurde, dass diese notifizierten Stellen die in Artikel 33 Absätze 4, 9 und 10 festgelegten Anforderungen erfüllen.

Wenn die in Anhang II Abschnitt A aufgeführten Rechtsakte es dem Hersteller des Produkts ermöglichen, auf eine Konformitätsbewertung durch Dritte zu verzichten, sofern dieser Hersteller alle harmonisierten Normen, die alle einschlägigen Anforderungen abdecken, angewandt hat, so darf dieser Hersteller nur dann von dieser Möglichkeit Gebrauch machen, wenn er auch harmonisierte Normen oder gegebenenfalls gemeinsame Spezifikationen gemäß Artikel 41, die die Anforderungen in Kapitel 2 dieses Titels abdecken, angewandt hat.

(4) Hochrisiko-KI-Systeme werden einem neuen Konformitätsbewertungsverfahren unterzogen, wenn sie wesentlich geändert werden, unabhängig davon, ob das geänderte System noch weiter in Verkehr gebracht oder vom derzeitigen Nutzer weitergenutzt werden soll.

Bei Hochrisiko-KI-Systemen, die nach dem Inverkehrbringen oder der Inbetriebnahme weiterhin dazulernen, gelten Änderungen des Hochrisiko-KI-Systems und seiner Leistung, die vom Anbieter zum Zeitpunkt der ursprünglichen Konformitätsbewertung vorab festgelegt wurden und in den Informationen der technischen Dokumentation gemäß Anhang IV Nummer 2 Buchstabe f enthalten sind, nicht als wesentliche Änderung.

(5) Der Kommission wird die Befugnis übertragen, gemäß Artikel 73 delegierte Rechtsakte zur Aktualisierung der Anhänge VI und VII zu erlassen, um Elemente der Konformitätsbewertungsverfahren einzuführen, die angesichts des technischen Fortschritts erforderlich werden.

(6) Der Kommission wird die Befugnis übertragen, delegierte Rechtsakte zur Änderung der Absätze 1 und 2 zu erlassen, um die in Anhang III Nummern 2 bis 8 genannten Hochrisiko-KI-Systeme dem Konformitätsbewertungsverfahren gemäß Anhang VII oder Teilen davon zu unterwerfen. Die Kommission erlässt solche delegierten Rechtsakte unter Berücksichtigung der Wirksamkeit des Konformitätsbewertungsverfahrens auf der Grundlage einer internen Kontrolle gemäß Anhang VI hinsichtlich der Vermeidung oder Minimierung der von solchen Systemen ausgehenden Risiken für die Gesundheit und Sicherheit und den Schutz der Grundrechte sowie hinsichtlich der Verfügbarkeit angemessener Kapazitäten und Ressourcen in den notifizierten Stellen.

Artikel 44
Bescheinigungen

(1) Die von notifizierten Stellen gemäß Anhang VII erteilten Bescheinigungen werden in einer Amtssprache der Union ausgefertigt, die der Mitgliedstaat, in dem die notifizierte Stelle niedergelassen ist, festlegt, oder in einer anderen Amtssprache der Union, mit der die notifizierte Stelle einverstanden ist.

(2) Die Bescheinigungen sind für die darin genannte Dauer gültig, die maximal fünf Jahre beträgt. Auf Antrag des Anbieters kann die Gültigkeit einer Bescheinigung auf der Grundlage einer Neubewertung gemäß den geltenden Konformitätsbewertungsverfahren um weitere Zeiträume von jeweils höchstens fünf Jahren verlängert werden.

(3) Stellt eine notifizierte Stelle fest, dass ein KI-System die Anforderungen in Kapitel 2 dieses Titels nicht mehr erfüllt, setzt sie die erteilte Bescheinigung aus oder widerruft diese oder schränkt sie ein, jeweils unter Berücksichtigung des Verhältnismäßigkeitsgrundsatzes, sofern die Einhaltung der Anforderungen nicht durch geeignete Korrekturmaßnahmen des Anbieters des Systems innerhalb einer von der notifizierten Stelle gesetzten angemessenen Frist wiederhergestellt wird. Die notifizierte Stelle begründet ihre Entscheidung.

Artikel 45
Einspruch gegen Entscheidungen notifizierter Stellen

Die Mitgliedstaaten stellen sicher, dass ein Einspruchsverfahren gegen die Entscheidungen der notifizierten Stelle für Beteiligte vorgesehen ist, die ein berechtigtes Interesse an einer solchen Entscheidung haben.

Artikel 46
Meldepflichten der notifizierten Stellen

(1) Die notifizierten Stellen melden der notifizierenden Behörde

a) alle Unionsbescheinigungen über die Bewertung der technischen Dokumentation, etwaige Ergänzungen dieser Bescheinigungen und alle Genehmigungen von Qualitätsmanagementsystemen, die gemäß den Anforderungen des Anhangs VII erteilt wurden;

b) alle Verweigerungen, Einschränkungen, Aussetzungen oder Rücknahmen von Unionsbescheinigungen über die Bewertung der technischen Dokumentation oder Genehmigungen von Qualitätsmanagementsystemen, die gemäß den Anforderungen des Anhangs VII erteilt wurden;

c) alle Umstände, die Folgen für den Anwendungsbereich oder die Bedingungen der Notifizierung haben;

d) alle Auskunftsersuchen über Konformitätsbewertungstätigkeiten, die sie von den Marktüberwachungsbehörden erhalten haben;

e) auf Anfrage, die Konformitätsbewertungstätigkeiten, denen sie im Anwendungsbereich ihrer Notifizierung nachgegangen sind, und sonstige Tätigkeiten, einschließlich grenzüberschreitender Tätigkeiten und Vergabe von Unteraufträgen, die sie durchgeführt haben.

(2) Jede notifizierte Stelle unterrichtet die anderen notifizierten Stellen über

a) die Genehmigungen von Qualitätsmanagementsystemen, die sie verweigert, ausgesetzt oder zurückgenommen hat, und auf Anfrage die Genehmigungen von Qualitätsmanagementsystemen, die sie erteilt hat;

b) die EU-Bescheinigungen über die Bewertung der technischen Dokumentation und deren etwaige Ergänzungen, die sie verweigert, ausgesetzt oder

zurückgenommen oder anderweitig eingeschränkt hat, und auf Anfrage die Bescheinigungen und/oder deren Ergänzungen, die sie ausgestellt hat.

(3) Jede notifizierte Stelle übermittelt den anderen notifizierten Stellen, die ähnlichen Konformitätsbewertungstätigkeiten für die gleiche KI-Technik nachgehen, ihre einschlägigen Informationen über negative und auf Anfrage auch über positive Konformitätsbewertungsergebnisse.

Artikel 47
Ausnahme vom Konformitätsbewertungsverfahren

(1) Abweichend von Artikel 43 kann eine Marktüberwachungsbehörde das Inverkehrbringen oder die Inbetriebnahme bestimmter Hochrisiko-KI-Systeme im Hoheitsgebiet des betreffenden Mitgliedstaats aus außergewöhnlichen Gründen der öffentlichen Sicherheit, des Schutzes des Lebens und der Gesundheit von Personen, des Umweltschutzes und des Schutzes wichtiger Industrie- und Infrastrukturanlagen genehmigen. Diese Genehmigung wird auf die Dauer der erforderlichen Konformitätsbewertungsverfahren befristet und läuft mit dem Abschluss dieser Verfahren aus. Der Abschluss dieser Verfahren erfolgt unverzüglich.

(2) Die in Absatz 1 genannte Genehmigung wird nur erteilt, wenn die Marktüberwachungsbehörde zu dem Schluss gelangt, dass das Hochrisiko-KI-System die Anforderungen in Kapitel 2 dieses Titels erfüllt. Die Marktüberwachungsbehörde unterrichtet die Kommission und die anderen Mitgliedstaaten über alle von ihr gemäß Absatz 1 erteilten Genehmigungen.

(3) Erhebt weder ein Mitgliedstaat noch die Kommission innerhalb von 15 Kalendertagen nach Erhalt der in Absatz 2 genannten Mitteilung Einwände gegen die von einer Marktüberwachungsbehörde eines Mitgliedstaats gemäß Absatz 1 erteilte Genehmigung, so gilt diese Genehmigung als gerechtfertigt.

(4) Erhebt innerhalb von 15 Kalendertagen nach Erhalt der in Absatz 2 genannten Mitteilung ein Mitgliedstaat Einwände gegen eine von einer Marktüberwachungsbehörde eines anderen Mitgliedstaats erteilte Genehmigung oder ist die Kommission der Auffassung, dass die Genehmigung mit dem Unionsrecht unvereinbar ist oder dass die Schlussfolgerung der Mitgliedstaaten in Bezug auf die Konformität des in Absatz 2 genannten Systems unbegründet ist, so nimmt die Kommission unverzüglich Konsultationen mit dem betreffenden Mitgliedstaat auf; der bzw. die betroffenen Akteur(e) werden konsultiert und erhalten Gelegenheit, dazu Stellung zu nehmen. In Anbetracht dessen entscheidet die Kommission, ob die Genehmigung gerechtfertigt ist oder nicht. Die Kommission richtet ihren Beschluss an die betroffenen Mitgliedstaaten und an den/die betroffenen Akteur(e).

(5) Wird die Genehmigung als ungerechtfertigt erachtet, so muss sie von der Marktüberwachungsbehörde des betreffenden Mitgliedstaats zurückgenommen werden.

(6) Abweichend von den Absätzen 1 bis 5 gelten für Hochrisiko-KI-Systeme, die bestimmungsgemäß als Sicherheitskomponenten von Produkten verwendet werden sollen, die unter die Verordnung (EU) 2017/745 und die Verordnung (EU) 2017/746 fallen, oder die selbst solche Produkte sind, die Ausnahmen gemäß Artikel 59 der Verordnung (EU) 2017/745 und Artikel 54 der Verordnung (EU) 2017/746 auch für die Konformitätsbewertung hinsichtlich der Erfüllung der Anforderungen in Kapitel 2 dieses Titels.

Artikel 48
EU-Konformitätserklärung

(1) Der Anbieter stellt für jedes KI-System eine schriftliche EU-Konformitätserklärung aus und hält sie für einen Zeitraum von 10 Jahren ab dem Inverkehrbringen oder der Inbetriebnahme des KI-Systems für die zuständigen nationalen Behörden bereit. Aus der EU-Konformitätserklärung geht hervor, für welches KI-System sie ausgestellt wurde. Ein Exemplar der EU-Konformitätserklärung wird den zuständigen nationalen Behörden auf Anfrage zur Verfügung gestellt.

(2) Die EU-Konformitätserklärung besagt, dass das betreffende Hochrisiko-KI-System die Anforderungen in Kapitel 2 dieses Titels erfüllt. Die EU-Konformitätserklärung enthält die in Anhang V aufgeführten Angaben und wird in eine oder mehrere Amtssprachen der Union übersetzt, die von dem/den Mitgliedstaat(en) vorgeschrieben wird/werden, in dem/denen das Hochrisiko-KI-System bereitgestellt wird.

(3) Unterliegen Hochrisiko-KI-Systeme noch anderen Harmonisierungsrechtsvorschriften der Union, die ebenfalls eine EU-Konformitätserklärung vorschreiben, so wird eine einzige EU-Konformitätserklärung ausgestellt, die sich auf alle für das Hochrisiko-KI-System geltenden Rechtsvorschriften der Union bezieht. Die Erklärung enthält alle erforderlichen Angaben zur Feststellung der Harmonisierungsrechtsvorschriften der Union, auf die sich die Erklärung bezieht.

(4) Mit der Ausstellung der EU-Konformitätserklärung übernimmt der Anbieter die Verantwortung für die Erfüllung der Anforderungen in Kapitel 2 dieses Titels. Der Anbieter hält die EU-Konformitätserklärung gegebenenfalls auf dem neuesten Stand.

(5) Der Kommission wird die Befugnis übertragen, gemäß Artikel 73 delegierte Rechtsakte zur Änderung des in Anhang V festgelegten Inhalts der EU-Konformitätserklärung zu erlassen, um Elemente einzuführen, die angesichts des technischen Fortschritts erforderlich werden.

Artikel 49
CE-Konformitätskennzeichnung

(1) Die CE-Kennzeichnung wird gut sichtbar, leserlich und dauerhaft an Hochrisiko-KI-Systemen angebracht. Falls die Art des Hochrisiko-KI-Systems dies nicht zulässt oder nicht rechtfertigt, wird sie auf der Verpackung oder gegebenenfalls den Begleitunterlagen angebracht.

(2) Für die in Absatz 1 dieses Artikels genannte CE-Kennzeichnung gelten die allgemeinen Grundsätze des Artikels 30 der Verordnung (EG) Nr. 765/2008.

(3) Wo erforderlich, wird der CE-Kennzeichnung die Kennnummer der für die Konformitätsbewertungsverfahren gemäß Artikel 43 zuständigen notifizierten Stelle hinzugefügt. Diese Kennnummer wird auch auf jeglichem Werbematerial angegeben, in dem darauf hingewiesen wird, dass das Hochrisiko-KI-System die Anforderungen für die CE-Kennzeichnung erfüllt.

Artikel 50
Aufbewahrung von Unterlagen

Der Anbieter hält für einen Zeitraum von zehn Jahren ab dem Inverkehrbringen oder der Inbetriebnahme des Hochrisiko-KI-Systems folgende Unterlagen für die zuständigen nationalen Behörden bereit:

a) die in Artikel 11 genannte technische Dokumentation,

b) die Unterlagen zu dem in Artikel 17 genannten Qualitätsmanagementsystem,

c) die Unterlagen über etwaige von notifizierten Stellen genehmigte Änderungen,

d) die Entscheidungen und etwaigen sonstigen Dokumente der notifizierten Stellen,

e) die in Artikel 48 genannte EU-Konformitätserklärung.

Artikel 51
Registrierung

Vor dem Inverkehrbringen oder der Inbetriebnahme eines in Artikel 6 Absatz 2 genannten Hochrisiko-KI-Systems registriert der Anbieter oder gegebenenfalls sein Bevollmächtigter dieses System in der in Artikel 60 genannten EU-Datenbank.

TITEL IV

TRANSPARENZPFLICHTEN FÜR BESTIMMTE KI-SYSTEME

Artikel 52
Transparenzpflichten für bestimmte KI-Systeme

(1) Die Anbieter stellen sicher, dass KI-Systeme, die für die Interaktion mit natürlichen Personen bestimmt sind, so konzipiert und entwickelt werden, dass natürlichen Personen mitgeteilt wird, dass sie es mit einem KI-System zu tun haben, es sei denn, dies ist aufgrund der Umstände und des Kontexts der Nutzung offensichtlich. Diese Vorgabe gilt nicht für gesetzlich zur Aufdeckung, Verhütung, Ermittlung und Verfolgung von Straftaten zugelassene KI-Systeme, es sei denn, diese Systeme stehen der Öffentlichkeit zur Anzeige einer Straftat zur Verfügung.

(2) Die Verwender eines Emotionserkennungssystems oder eines Systems zur biometrischen Kategorisierung informieren die davon betroffenen natürlichen Personen über den Betrieb des Systems. Diese Vorgabe gilt nicht für gesetzlich zur Aufdeckung, Verhütung, Ermittlung und Verfolgung von Straftaten zugelassene KI-Systeme, die zur biometrischen Kategorisierung verwendet werden.

(3) Nutzer eines KI-Systems, das Bild-, Ton- oder Videoinhalte erzeugt oder manipuliert, die wirklichen Personen, Gegenständen, Orten oder anderen Einrichtungen oder Ereignissen merklich ähneln und einer Person fälschlicherweise als echt oder wahrhaftig erscheinen würden („Deepfake“), müssen offenlegen, dass die Inhalte künstlich erzeugt oder manipuliert wurden.

Unterabsatz 1 gilt jedoch nicht, wenn die Verwendung zur Aufdeckung, Verhütung, Ermittlung und Verfolgung von Straftaten gesetzlich zugelassen oder für die Ausübung der durch die Charta der Grundrechte der Europäischen Union garantierten Rechte auf freie Meinungsäußerung und auf Freiheit der Kunst und

Wissenschaft erforderlich ist und geeignete Schutzvorkehrungen für die Rechte und Freiheiten Dritter bestehen.

(4) Die Absätze 1, 2 und 3 lassen die in Titel III dieser Verordnung festgelegten Anforderungen und Pflichten unberührt.

TITEL V

MAßNAHMEN ZUR INNOVATIONSFÖRDERUNG

Artikel 53
KI-Reallabore

(1) KI-Reallabore, die von den zuständigen Behörden eines oder mehrerer Mitgliedstaaten oder vom Europäischen Datenschutzbeauftragten eingerichtet werden, bieten eine kontrollierte Umgebung, um die Entwicklung, Erprobung und Validierung innovativer KI-Systeme für einen begrenzten Zeitraum vor ihrem Inverkehrbringen oder ihrer Inbetriebnahme nach einem spezifischen Plan zu erleichtern. Dies geschieht unter direkter Aufsicht und Anleitung der zuständigen Behörden, um die Einhaltung der Anforderungen dieser Verordnung und gegebenenfalls anderer Rechtsvorschriften der Union und der Mitgliedstaaten, die innerhalb des Reallabors beaufsichtigt wird, sicherzustellen.

(2) Soweit die innovativen KI-Systeme personenbezogene Daten verarbeiten oder anderweitig der Aufsicht anderer nationaler Behörden oder zuständiger Behörden unterstehen, die den Zugang zu Daten gewähren oder unterstützen, sorgen die Mitgliedstaaten dafür, dass die nationalen Datenschutzbehörden und diese anderen nationalen Behörden in den Betrieb des KI-Reallabors einbezogen werden.

(3) Die KI-Reallabore lassen die Aufsichts- und Abhilfebefugnisse der zuständigen Behörden unberührt. Alle erheblichen Risiken für die Gesundheit und Sicherheit und die Grundrechte, die bei der Entwicklung und Erprobung solcher Systeme festgestellt werden, führen zur sofortigen Risikominderung oder, falls dies nicht möglich ist, zur Aussetzung des Entwicklungs- und Erprobungsprozesses bis eine solche Risikominderung erfolgt ist.

(4) Die am KI-Reallabor Beteiligten bleiben nach geltendem Recht der Union und der Mitgliedstaaten für Schäden haftbar, die Dritten infolge der Erprobung im Reallabor entstehen.

(5) Die zuständigen Behörden der Mitgliedstaaten, die KI-Reallabore eingerichtet haben, koordinieren ihre Tätigkeiten und arbeiten im Rahmen des Europäischen Ausschusses für künstliche Intelligenz zusammen. Sie übermitteln dem Ausschuss und der Kommission jährliche Berichte über die Ergebnisse der Umsetzung dieser Systeme, einschließlich bewährter Verfahren, gewonnener Erkenntnisse und Empfehlungen zu deren Aufbau, sowie gegebenenfalls über die Anwendung dieser Verordnung und anderer Rechtsvorschriften der Union, die innerhalb des Reallabors kontrolliert werden.

(6) Die Modalitäten und Bedingungen für den Betrieb der KI-Reallabore, einschließlich Genehmigungskriterien und Verfahren für die Beantragung, Auswahl, Beteiligung und für den Ausstieg aus dem Reallabor, sowie die Rechte und Pflichten der Beteiligten werden in Durchführungsrechtsakten festgelegt. Diese

Durchführungsrechtsakte werden gemäß dem in Artikel 74 Absatz 2 genannten Prüfverfahren erlassen.

Artikel 54
Weiterverarbeitung personenbezogener Daten zur Entwicklung bestimmter KI-Systeme im öffentlichen Interesse im KI-Reallabor

(1) Im KI-Reallabor dürfen personenbezogene Daten, die rechtmäßig für andere Zwecke erhoben wurden, zur Entwicklung und Erprobung bestimmter innovativer KI-Systeme im Reallabor unter folgenden Bedingungen verarbeitet werden:

a) die innovativen KI-Systeme werden entwickelt, um ein erhebliches öffentliches Interesse in einem oder mehreren der folgenden Bereiche zu wahren:

i) Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit unter der Kontrolle und Verantwortung der zuständigen Behörden, wobei die Verarbeitung auf der Grundlage des Rechts der Mitgliedstaaten oder des Unionsrechts erfolgt,

ii) öffentliche Sicherheit und öffentliche Gesundheit, einschließlich Verhütung, Bekämpfung und Behandlung von Krankheiten,

iii) hohes Umweltschutzniveau und Verbesserung der Umweltqualität;

b) die verarbeiteten Daten sind für die Erfüllung einer oder mehrerer der in Titel III Kapitel 2 genannten Anforderungen erforderlich, soweit diese Anforderungen durch die Verarbeitung anonymisierter, synthetischer oder sonstiger nicht personenbezogener Daten nicht wirksam erfüllt werden können;

c) es bestehen wirksame Überwachungsmechanismen, um festzustellen, ob während der Erprobung im Reallabor hohe Risiken für die Grundrechte der betroffenen Personen auftreten können, sowie Reaktionsmechanismen, um diese Risiken umgehend zu mindern und erforderlichenfalls die Verarbeitung zu beenden;

d) personenbezogene Daten, die im Rahmen des Reallabors verarbeitet werden sollen, befinden sich in einer funktional getrennten, isolierten und geschützten Datenverarbeitungsumgebung unter der Kontrolle der Beteiligten, und nur befugte Personen haben Zugriff auf diese Daten;

e) es erfolgt keine Übermittlung oder Übertragung verarbeiteter personenbezogener Daten an Dritte und auch kein anderweitiger Zugriff Dritter auf diese Daten;

f) eine Verarbeitung personenbezogener Daten im Rahmen des Reallabors führt zu keinen Maßnahmen oder Entscheidungen, die Auswirkungen auf die betroffenen Personen haben;

g) personenbezogene Daten, die im Rahmen des Reallabors verarbeitet wurden, werden gelöscht, sobald die Beteiligung an dem Reallabor beendet wird oder das Ende der Speicherfrist für die personenbezogenen Daten erreicht ist;

h) die Protokolle der Verarbeitung personenbezogener Daten im Rahmen des Reallabors werden für die Dauer der Beteiligung am Reallabor und noch 1 Jahr nach deren Beendigung ausschließlich zu dem Zweck und nur so lange

aufbewahrt, wie dies zur Erfüllung der Rechenschafts- und Dokumentationspflichten nach diesem Artikel oder anderen anwendbaren Rechtsvorschriften der Union oder der Mitgliedstaaten erforderlich ist;

i) eine vollständige und detaillierte Beschreibung des Prozesses und der Gründe für das Trainieren, Testen und Validieren des KI-Systems wird zusammen mit den Testergebnissen als Teil der technischen Dokumentation gemäß Anhang IV aufbewahrt;

j) eine kurze Zusammenfassung des im KI-Reallabor entwickelten KI-Projekts, seiner Ziele und erwarteten Ergebnisse wird auf der Website der zuständigen Behörden veröffentlicht.

(2) Absatz 1 lässt die Rechtsvorschriften der Union oder der Mitgliedstaaten, die eine Verarbeitung für andere als die in diesen Rechtsvorschriften ausdrücklich genannten Zwecke ausschließen, unberührt.

Artikel 55
Maßnahmen für Kleinanbieter und Kleinnutzer

(1) Die Mitgliedstaaten ergreifen folgende Maßnahmen:

a) Gewährung eines vorrangigen Zugangs zu den KI-Reallaboren für Kleinanbieter und Start-up-Unternehmen, soweit sie die entsprechenden Voraussetzungen erfüllen;

b) Durchführung besonderer Sensibilisierungsmaßnahmen für die Anwendung dieser Verordnung, die auf die Bedürfnisse der Kleinanbieter und Kleinnutzer ausgerichtet sind;

c) gegebenenfalls Einrichtung eines eigenen Kanals für die Kommunikation mit Kleinanbietern, Kleinnutzern und anderen Innovatoren, um Orientierungen zu geben und Fragen zur Durchführung dieser Verordnung zu beantworten.

(2) Bei der Festsetzung der Gebühren für die Konformitätsbewertung gemäß Artikel 43 werden die besonderen Interessen und Bedürfnisse von Kleinanbietern berücksichtigt, indem diese Gebühren proportional zu ihrer Größe und der Größe ihres Marktes gesenkt werden.

TITEL VI

LEITUNGSSTRUKTUR

KAPITEL 1

EUROPÄISCHER AUSSCHUSS FÜR KÜNSTLICHE INTELLIGENZ

Artikel 56
Einrichtung des Europäischen Ausschusses für künstliche Intelligenz

(1) Ein „Europäischer Ausschuss für künstliche Intelligenz“ (im Folgenden „Ausschuss“) wird eingerichtet.

(2) Der Ausschuss berät und unterstützt die Kommission zu folgenden Zwecken:

a) Leisten eines Beitrags zur wirksamen Zusammenarbeit der nationalen Aufsichtsbehörden und der Kommission in Angelegenheiten, die unter diese Verordnung fallen;

b) Koordinierung und Mitwirkung an Leitlinien und Analysen der Kommission, der nationalen Aufsichtsbehörden und anderer zuständiger Behörden zu neu auftretenden Fragen in Bezug auf Angelegenheiten, die unter diese Verordnung fallen, im gesamten Binnenmarkt;

c) Unterstützung der nationalen Aufsichtsbehörden und der Kommission bei der Gewährleistung der einheitlichen Anwendung dieser Verordnung.

Artikel 57
Struktur des Ausschusses

(1) Der Ausschuss besteht aus den nationalen Aufsichtsbehörden, vertreten durch ihren Leiter oder einen gleichwertigen hochrangigen Beamten der Behörde, und dem Europäischen Datenschutzbeauftragten. Weitere nationale Behörden können zu den Sitzungen eingeladen werden, wenn die erörterten Fragen für sie von Belang sind.

(2) Der Ausschuss gibt sich mit einfacher Mehrheit seiner Mitglieder und nach Zustimmung der Kommission eine Geschäftsordnung. Die Geschäftsordnung regelt auch die operativen Aspekte der Wahrnehmung der in Artikel 58 aufgeführten Aufgaben des Ausschusses. Der Ausschuss kann gegebenenfalls Untergruppen zur Prüfung besonderer Fragen einsetzen.

(3) Den Vorsitz im Ausschuss führt die Kommission. Die Kommission beruft die Sitzungen ein und bereitet die Tagesordnung im Einklang mit den Aufgaben des Ausschusses gemäß dieser Verordnung und seiner Geschäftsordnung vor. Die Kommission leistet administrative und analytische Unterstützung für die Tätigkeiten des Ausschusses gemäß dieser Verordnung.

(4) Der Ausschuss kann externe Sachverständige und Beobachter zu seinen Sitzungen einladen und einen Meinungsaustausch mit interessierten Dritten führen, um diesen in angemessenem Umfang in seine Tätigkeiten einfließen zu lassen. Dazu kann die Kommission den Austausch zwischen dem Verwaltungsrat und anderen Einrichtungen, Ämtern, Agenturen und Beratungsgruppen der Union fördern.

Artikel 58
Aufgaben des Ausschusses

Bei der Beratung und Unterstützung der Kommission im Zusammenhang mit Artikel 56 Absatz 2 hat der Ausschuss insbesondere folgende Aufgaben:

a) Sammlung von Fachwissen und bewährten Verfahren und deren Austausch zwischen den Mitgliedstaaten;

b) Leisten eines Beitrags zu einer einheitlichen Verwaltungspraxis in den Mitgliedstaaten, auch bezüglich der Funktionsweise der in Artikel 53 genannten KI-Reallabore;

c) Abgabe von Stellungnahmen, Empfehlungen oder schriftlichen Beiträgen zu Fragen im Zusammenhang mit der Durchführung dieser Verordnung, insbesondere

i) über technische Spezifikationen oder bestehende Normen in Bezug auf die in Titel III Kapitel 2 festgelegten Anforderungen,

ii) über die Anwendung der in Artikel 40 genannten harmonisierten Normen oder der in Artikel 41 genannten gemeinsamen Spezifikationen,

iii) über die Ausarbeitung von Leitfäden, einschließlich der Leitlinien für die Festsetzung von Geldbußen gemäß Artikel 71.

KAPITEL 2

ZUSTÄNDIGE NATIONALE BEHÖRDEN

Artikel 59
Benennung der zuständigen nationalen Behörden

(1) Um die Anwendung und Durchführung dieser Verordnung sicherzustellen, werden von jedem Mitgliedstaat zuständige nationale Behörden eingerichtet oder benannt. Die notifizierenden Behörden werden so organisiert, dass bei der Ausübung ihrer Tätigkeiten und der Wahrnehmung ihrer Aufgaben Objektivität und Unparteilichkeit gewahrt sind.

(2) Jeder Mitgliedstaat benennt aus der Reihe der zuständigen nationalen Behörden eine nationale Aufsichtsbehörde. Die nationale Aufsichtsbehörde fungiert als notifizierende Behörde und als Marktüberwachungsbehörde, es sei denn, der Mitgliedstaat hat organisatorische und administrative Gründe, um mehr als eine Behörde zu benennen.

(3) Die Mitgliedstaaten teilen der Kommission ihre Benennung oder Benennungen sowie gegebenenfalls ihre Gründe für die Benennung von mehr als einer Behörde mit.

(4) Die Mitgliedstaaten sorgen dafür, dass die zuständigen nationalen Behörden mit angemessenen finanziellen und personellen Ressourcen ausgestattet werden, damit sie ihre Aufgaben im Rahmen dieser Verordnung wahrnehmen können. Insbesondere müssen die zuständigen nationalen Behörden ständig über eine ausreichende Zahl von Mitarbeitern verfügen, deren Kompetenzen und Sachkenntnis ein tiefes Verständnis der Technologien der künstlichen Intelligenz, der Daten und Datenverarbeitung, der Grundrechte, der Gesundheits- und Sicherheitsrisiken sowie die Kenntnis der bestehenden Normen und rechtlichen Anforderungen einschließen.

(5) Die Mitgliedstaaten übermitteln der Kommission jährlich einen Bericht über den Stand der finanziellen und personellen Ressourcen der zuständigen nationalen Behörden, in dem sie auch deren Angemessenheit bewerten. Die Kommission leitet diese Informationen an den Ausschuss zur Erörterung und etwaigen Abgabe von Empfehlungen weiter.

(6) Die Kommission fördert den Erfahrungsaustausch zwischen den zuständigen nationalen Behörden.

(7) Die zuständigen nationalen Behörden können insbesondere auch Kleinanbietern mit Orientierung und Rat bei der Anwendung dieser Verordnung zur Seite stehen. Wenn zuständige nationale Behörden beabsichtigen, Orientierung und Rat in Bezug auf KI-Systeme in Bereichen zu geben, die unter andere Rechtsvorschriften der Union fallen, so sind gegebenenfalls die nach jenen Unionsvorschriften dafür zuständigen nationalen Behörden zu konsultieren. Mitgliedstaaten können auch eine zentrale Kontaktstelle für die Kommunikation mit den Akteuren einrichten.

(8) Soweit Organe, Einrichtungen und sonstige Stellen der Union in den Anwendungsbereich dieser Verordnung fallen, übernimmt der Europäische Datenschutzbeauftragte die Funktion der für ihre Beaufsichtigung zuständigen Behörde.

TITEL VII

EU-DATENBANK FÜR EIGENSTÄNDIGE HOCHRISIKO-KI-SYSTEME

Artikel 60
EU-Datenbank für eigenständige Hochrisiko-KI-Systeme

(1) Die Kommission errichtet und pflegt in Zusammenarbeit mit den Mitgliedstaaten eine EU-Datenbank mit den in Absatz 2 genannten Informationen über Hochrisiko-KI-Systeme nach Artikel 6 Absatz 2, die gemäß Artikel 51 registriert werden.

(2) Die in Anhang VIII aufgeführten Daten werden von den Anbietern in die EU-Datenbank eingegeben. Die Kommission leistet ihnen dabei technische und administrative Unterstützung.

(3) Die in der EU-Datenbank gespeicherten Daten sind öffentlich zugänglich.

(4) Die EU-Datenbank enthält personenbezogene Daten nur, soweit dies für die Erfassung und Verarbeitung von Informationen gemäß dieser Verordnung erforderlich ist. Zu diesen Informationen gehören die Namen und Kontaktdaten der natürlichen Personen, die für die Registrierung des Systems verantwortlich sind und die rechtlich befugt sind, den Anbieter zu vertreten.

(5) Die Kommission gilt bezüglich der EU-Datenbank als die für die Verarbeitung verantwortliche Stelle. Sie sorgt auch für eine angemessene technische und administrative Unterstützung der Anbieter.

TITEL VIII

BEOBACHTUNG NACH DEM INVERKEHRBRINGEN, INFORMATIONSAUSTAUSCH, MARKTÜBERWACHUNG

KAPITEL 1

BEOBACHTUNG NACH DEM INVERKEHRBRINGEN

Artikel 61
Beobachtung nach dem Inverkehrbringen durch die Anbieter und Plan für die Beobachtung nach dem Inverkehrbringen für Hochrisiko-KI-Systeme

(1) Anbieter müssen ein System zur Beobachtung nach dem Inverkehrbringen einrichten und dokumentieren, das im Verhältnis zur Art der KI-Technik und zu den Risiken des Hochrisiko-KI-Systems steht.

(2) Mit dem System zur Beobachtung nach dem Inverkehrbringen müssen sich die einschlägigen von den Nutzern bereitgestellten oder aus anderen Quellen

gesammelten Daten zur Leistung der Hochrisiko-KI-Systeme über deren gesamte Lebensdauer hinweg aktiv und systematisch erfassen, dokumentieren und analysieren lassen, und der Anbieter muss damit die fortdauernde Einhaltung der in Titel III Kapitel 2 genannten Anforderungen an die KI-Systeme bewerten können.

(3) Das System zur Beobachtung nach dem Inverkehrbringen muss auf einem entsprechenden Plan beruhen. Der Plan für die Beobachtung nach dem Inverkehrbringen ist Teil der in Anhang IV genannten technischen Dokumentation. Die Kommission erlässt einen Durchführungsrechtsakt, in dem sie die Bestimmungen für die Erstellung eines Musters des Plans für die Beobachtung nach dem Inverkehrbringen sowie die Liste der in den Plan aufzunehmenden Elemente detailliert festlegt.

(4) Bei Hochrisiko-KI-Systemen, die unter die in Anhang II genannten Rechtsakte fallen und für die auf der Grundlage dieser Rechtsakte bereits ein System zur Beobachtung nach dem Inverkehrbringen sowie ein entsprechender Plan festgelegt wurden, müssen die in den Absätzen 1, 2 und 3 genannten Elemente gegebenenfalls in dieses System bzw. in diesen Plan aufgenommen werden.

Unterabsatz 1 gilt auch für Hochrisiko-KI-Systeme nach Anhang III Nummer 5 Buchstabe b, die von Kreditinstituten im Sinne der Richtlinie 2013/36/EU in Verkehr gebracht oder in Betrieb genommen wurden.

KAPITEL 2

AUSTAUSCH VON INFORMATIONEN ÜBER VORFÄLLE UND FEHLFUNKTIONEN

Artikel 62
Meldung schwerwiegender Vorfälle und Fehlfunktionen

(1) Anbieter von in der Union in Verkehr gebrachten Hochrisiko-KI-Systemen, melden schwerwiegende Vorfälle oder Fehlfunktionen dieser Systeme, die einen Verstoß gegen die Bestimmungen des Unionsrechts zum Schutz der Grundrechte darstellen, den Marktüberwachungsbehörden des Mitgliedstaats, in dem der Vorfall oder der Verstoß stattgefunden hat.

Diese Meldung erfolgt unmittelbar, nachdem der Anbieter den kausalen Zusammenhang zwischen dem KI-System und dem Vorfall bzw. der Fehlfunktion oder die naheliegende Wahrscheinlichkeit eines solchen Zusammenhangs festgestellt hat, oder auf jeden Fall spätestens 15 Tage, nachdem der Anbieter Kenntnis von diesem schwerwiegenden Vorfall oder der Fehlfunktion erlangt hat.

(2) Sobald die Marktüberwachungsbehörde eine Meldung über einen Verstoß gegen die Bestimmungen des Unionsrechts zum Schutz der Grundrechte erhält, unterrichtet sie die in Artikel 64 Absatz 3 genannten nationalen Behörden oder öffentlichen Stellen. Zur leichteren Einhaltung der Pflichten nach Absatz 1 arbeitet die Kommission entsprechende Leitlinien aus. Diese Leitlinien werden spätestens 12 Monate nach dem Inkrafttreten dieser Verordnung veröffentlicht.

(3) Bei Hochrisiko-KI-Systemen nach Anhang III Nummer 5 Buchstabe b, die von Kreditinstituten im Sinne der Richtlinie 2013/36/EU in Verkehr gebracht oder in Betrieb genommen wurden, sowie bei Hochrisiko-KI-Systemen, bei denen es sich um Sicherheitskomponenten von Produkten handelt, die unter die Verordnung (EU) 2017/745 und die Verordnung (EU) 2017/746 fallen, oder die selbst solche

Produkte sind, müssen nur jene schwerwiegenden Vorfälle oder Fehlfunktionen gemeldet werden, die einen Verstoß gegen die Bestimmungen des Unionsrechts zum Schutz der Grundrechte darstellen.

KAPITEL 3

DURCHSETZUNG

Artikel 63
Marktüberwachung und Kontrolle von KI-Systemen auf dem Unionsmarkt

(1) Die Verordnung (EU) 2019/1020 gilt für KI-Systeme, die unter diese Verordnung fallen. Für die Zwecke einer wirksamen Durchsetzung dieser Verordnung gilt jedoch Folgendes:

a) Jede Bezugnahme auf einen Wirtschaftsakteur nach der Verordnung (EU) 2019/1020 gilt auch als Bezugnahme auf alle Akteure, die in Titel III Kapitel 3 dieser Verordnung genannt werden.

b) Jede Bezugnahme auf ein Produkt nach der Verordnung (EU) 2019/1020 gilt auch als Bezugnahme auf alle KI-Systeme, die unter diese Verordnung fallen.

(2) Die nationale Aufsichtsbehörde erstattet der Kommission regelmäßig über die Ergebnisse ihrer jeweiligen Marktüberwachungstätigkeiten Bericht. Die nationale Aufsichtsbehörde meldet der Kommission und den einschlägigen nationalen Wettbewerbsbehörden unverzüglich alle Informationen, die sie im Verlauf ihrer Marktüberwachungstätigkeiten erlangt hat und die für die Anwendung von Unionsrecht auf Wettbewerbsregeln von Interesse sein könnten.

(3) Bei Hochrisiko-KI-Systemen und damit in Zusammenhang stehenden Produkten, auf die die in Anhang II Abschnitt A aufgeführten Rechtsakte Anwendung finden, gilt als Marktüberwachungsbehörde für die Zwecke dieser Verordnung die in jenen Rechtsakten für die Marktüberwachung benannte Behörde.

(4) Bei KI-Systemen, die von auf der Grundlage des Finanzdienstleistungsrechts der Union regulierten Finanzinstituten in Verkehr gebracht, in Betrieb genommen oder eingesetzt werden, gilt als Marktüberwachungsbehörde für die Zwecke dieser Verordnung die in jenen Rechtsvorschriften für die Finanzaufsicht über diese Institute benannte Behörde.

(5) Für die in Absatz 1 Buchstabe a genannten KI-Systeme, sofern diese Systeme für Strafverfolgungszwecke nach Anhang III Nummern 6 und 7 eingesetzt werden, benennen die Mitgliedstaaten für die Zwecke dieser Verordnung als Marktüberwachungsbehörden entweder die für den Datenschutz nach der Richtlinie (EU) 2016/680 oder der Verordnung (EU) 2016/679 zuständigen Aufsichtsbehörden oder die zuständigen nationalen Behörden, die die Tätigkeiten der Behörden im Bereich der Strafverfolgung, Einwanderung oder Asyl, die solche Systeme in Verkehr bringen oder einsetzen, beaufsichtigen.

(6) Soweit Organe, Einrichtungen und sonstige Stellen der Union in den Anwendungsbereich dieser Verordnung fallen, übernimmt der Europäische Datenschutzbeauftragte die Funktion der für sie zuständigen Marktüberwachungsbehörde.

(7) Die Mitgliedstaaten erleichtern die Koordinierung zwischen den auf der Grundlage dieser Verordnung benannten Marktüberwachungsbehörden und anderen einschlägigen nationalen Behörden oder Stellen, die die Anwendung der in Anhang II aufgeführten Harmonisierungsrechtsvorschriften der Union oder sonstigen Unionsrechts überwachen, das für die in Anhang III aufgeführten Hochrisiko-KI-Systeme relevant sein könnte.

Artikel 64
Zugang zu Daten und zur Dokumentation

(1) Im Zusammenhang mit ihren Tätigkeiten erhalten die Marktüberwachungsbehörden uneingeschränkten Zugang zu den von den Anbietern genutzten Trainings-, Validierungs- und Testdatensätzen, auch über Anwendungsprogrammierschnittstellen (API) oder sonstige für den Fernzugriff geeignete technische Mittel und Instrumente.

(2) Sofern dies für die Bewertung der Konformität der Hochrisiko-KI-Systeme mit den in Titel III Kapitel 2 festgelegten Anforderungen notwendig ist, wird der Marktüberwachungsbehörde auf deren begründetes Verlangen Zugang zum Quellcode des KI-Systems gewährt.

(3) Nationale Behörden oder öffentliche Stellen, die die Einhaltung des Unionsrechts zum Schutz der Grundrechte in Bezug auf den Einsatz der in Anhang III aufgeführten Hochrisiko-KI-Systeme überwachen oder durchsetzen, sind befugt, alle auf der Grundlage dieser Verordnung erstellten oder geführten Unterlagen anzufordern und einzusehen, sofern der Zugang zu diesen Unterlagen für die Ausübung ihres Auftrags im Rahmen ihrer Befugnisse notwendig ist. Die jeweilige Behörde oder öffentliche Stelle unterrichtet die Marktüberwachungsbehörde des betreffenden Mitgliedstaats von jedem diesbezüglichen Verlangen.

(4) Bis drei Monate nach dem Inkrafttreten dieser Verordnung muss jeder Mitgliedstaat die in Absatz 3 genannten Behörden oder öffentlichen Stellen benannt haben und deren Liste auf einer öffentlich zugänglichen Website der nationalen Aufsichtsbehörde veröffentlichen. Die Mitgliedstaaten übermitteln die Liste der Kommission und allen anderen Mitgliedstaaten und sorgen dafür, dass die Liste stets aktuell bleibt.

(5) Sollte die in Absatz 3 genannte Dokumentation nicht ausreichen, um feststellen zu können, ob ein Verstoß gegen das Unionsrecht zum Schutz der Grundrechte vorliegt, kann die in Absatz 3 genannte Behörde oder öffentliche Stelle bei der Marktüberwachungsbehörde einen begründeten Antrag auf Durchführung technischer Tests des Hochrisiko-KI-Systems stellen. Die Marktüberwachungsbehörde führt den Test unter enger Einbeziehung der beantragenden Behörde oder öffentlichen Stelle innerhalb eines angemessenen Zeitraums nach Eingang des Antrags durch.

(6) Alle Informationen und Unterlagen, in deren Besitz eine in Absatz 3 genannte nationale Behörde oder öffentliche Stelle auf der Grundlage dieses Artikels gelangt, werden im Einklang mit den in Artikel 70 festgelegten Vertraulichkeitspflichten behandelt.

Artikel 65

Verfahren für den Umgang mit KI-Systemen, die ein Risiko auf nationaler Ebene bergen

(1) Als KI-Systeme, die ein Risiko bergen, gelten Produkte, mit denen ein Risiko im Sinne des Artikels 3 Nummer 19 der Verordnung (EU) 2019/1020 verbunden ist, sofern es sich dabei um Risiken für die Gesundheit oder Sicherheit oder den Schutz der Grundrechte von Personen handelt.

(2) Hat die Marktüberwachungsbehörde eines Mitgliedstaats hinreichende Gründe zu der Annahme, dass ein KI-System ein Risiko im Sinne des Absatzes 1 birgt, prüft sie das betreffende KI-System im Hinblick auf die Erfüllung aller in dieser Verordnung festgelegten Anforderungen und Pflichten. Bestehen Risiken für den Schutz von Grundrechten, unterrichtet die Marktüberwachungsbehörde auch die in Artikel 64 Absatz 3 genannten einschlägigen nationalen Behörden oder öffentlichen Stellen. Die betreffenden Akteure müssen im notwendigen Umfang mit den Marktüberwachungsbehörden und den in Artikel 64 Absatz 3 genannten anderen Behörden oder öffentlichen Stellen zusammenarbeiten.

Stellt die Marktüberwachungsbehörde im Verlauf dieser Prüfung fest, dass das KI-System die in dieser Verordnung festgelegten Anforderungen und Pflichten nicht erfüllt, fordert sie den betreffenden Akteur unverzüglich auf, alle von ihr möglicherweise vorgegebenen Korrekturmaßnahmen zu ergreifen, die geeignet sind, die Konformität des KI-Systems wiederherzustellen, das KI-System vom Markt zu nehmen oder es innerhalb einer der Art des Risikos angemessenen Frist zurückzurufen.

Die Marktüberwachungsbehörde unterrichtet die betreffende notifizierte Stelle entsprechend. Artikel 18 der Verordnung (EU) 2019/1020 gilt für die in Unterabsatz 2 genannten Maßnahmen.

(3) Gelangt die Marktüberwachungsbehörde zu der Auffassung, dass die Nichtkonformität nicht auf ihr nationales Hoheitsgebiet beschränkt ist, unterrichtet sie die Kommission und die anderen Mitgliedstaaten über die Ergebnisse der Prüfung und über die Maßnahmen, zu denen sie den Akteur aufgefordert hat.

(4) Der Akteur sorgt dafür, dass alle geeigneten Korrekturmaßnahmen in Bezug auf die betreffenden KI-Systeme, die er in der Union in Verkehr gebracht hat, getroffen werden.

(5) Ergreift der Akteur in Bezug auf sein KI-System keine geeigneten Korrekturmaßnahmen innerhalb der in Absatz 2 genannten Frist, trifft die Marktüberwachungsbehörde alle geeigneten vorläufigen Maßnahmen, um die Bereitstellung des KI-Systems auf ihrem nationalen Markt zu verbieten oder einzuschränken, das Produkt von diesem Markt zu nehmen oder es zurückzurufen. Diese Behörde unterrichtet die Kommission und die anderen Mitgliedstaaten unverzüglich über diese Maßnahmen.

(6) Die Unterrichtung nach Absatz 5 enthält alle vorliegenden Angaben, insbesondere die für die Identifizierung des nicht konformen Systems notwendigen Daten, den Ursprung des KI-Systems, die Art der vermuteten Nichtkonformität und das sich daraus ergebende Risiko, die Art und Dauer der ergriffenen nationalen Maßnahmen und die von dem betreffenden Akteur vorgebrachten Argumente. Die Marktüberwachungsbehörden geben insbesondere an, ob die Nichtkonformität eine oder mehrere der folgenden Ursachen hat:

a) Nichterfüllung der in Titel III Kapitel 2 aufgeführten Anforderungen durch das KI-System;

b) Mängel in den in den Artikeln 40 und 41 genannten harmonisierten Normen oder gemeinsamen Spezifikationen, die eine Konformitätsvermutung begründen.

(7) Die anderen Marktüberwachungsbehörden, die kein Verfahren eingeleitet haben, unterrichten unverzüglich die Kommission und die anderen Mitgliedstaaten von jeglichen Maßnahmen und etwaigen ihnen vorliegenden zusätzlichen Erkenntnissen über die Nichtkonformität des betreffenden KI-Systems sowie über ihre Einwände, falls sie die ihnen mitgeteilt nationale Maßnahme ablehnen.

(8) Erhebt weder ein Mitgliedstaat noch die Kommission innerhalb von drei Monaten nach Eingang der in Absatz 5 genannten Unterrichtung Einwände gegen die von einem Mitgliedstaat erlassene vorläufige Maßnahme, so gilt diese Maßnahme als gerechtfertigt. Die Verfahrensrechte des betreffenden Akteurs nach Artikel 18 der Verordnung (EU) 2019/1020 bleiben hiervon unberührt.

(9) Die Marktüberwachungsbehörden aller Mitgliedstaaten tragen dafür Sorge, dass geeignete einschränkende Maßnahmen in Bezug auf das betreffende Produkt ergriffen werden, indem sie beispielsweise das Produkt unverzüglich von ihrem Markt nehmen.

Artikel 66
Schutzklauselverfahren der Union

(1) Erhebt ein Mitgliedstaat innerhalb von drei Monaten nach Eingang der in Artikel 65 Absatz 5 genannten Unterrichtung Einwände gegen eine von einem anderen Mitgliedstaat getroffene Maßnahme oder ist die Kommission der Ansicht, dass die Maßnahme mit dem Unionsrecht unvereinbar ist, so nimmt die Kommission unverzüglich Konsultationen mit dem betreffenden Mitgliedstaat oder Akteur auf und prüft die nationale Maßnahme. Anhand der Ergebnisse dieser Prüfung entscheidet die Kommission innerhalb von neun Monaten nach Eingang der in Artikel 65 Absatz 5 genannten Unterrichtung, ob die nationale Maßnahme gerechtfertigt ist oder nicht und teilt dem betreffenden Mitgliedstaat ihre Entscheidung mit.

(2) Gilt die nationale Maßnahme als gerechtfertigt, so ergreifen alle Mitgliedstaaten die erforderlichen Maßnahmen, damit das nichtkonforme KI-System von ihrem Markt genommen wird, und unterrichten die Kommission darüber. Gilt die nationale Maßnahme als nicht gerechtfertigt, nimmt der betreffende Mitgliedstaat die Maßnahme zurück.

(3) Gilt die nationale Maßnahme als gerechtfertigt und wird die Nichtkonformität des KI-Systems auf Mängel in den in den Artikeln 40 und 41 dieser Verordnung genannten harmonisierten Normen oder gemeinsamen Spezifikationen zurückgeführt, so leitet die Kommission das in Artikel 11 der Verordnung (EU) Nr. 1025/2012 festgelegte Verfahren ein.

Artikel 67
Konforme KI-Systeme, die ein Risiko bergen

(1) Stellt die Marktüberwachungsbehörde nach der gemäß Artikel 65 durchgeführten Prüfung fest, dass ein KI-System dieser Verordnung entspricht, jedoch trotzdem ein Risiko für die Gesundheit oder Sicherheit von Personen, für die Einhaltung der Pflichten aus dem Unionsrecht oder dem nationalen Recht zum Schutz der Grundrechte oder für andere Aspekte des Schutzes öffentlicher Interessen darstellt, fordert sie den betreffenden Akteur auf, alle geeigneten und von ihr möglicherweise vorgegebenen Maßnahmen zu treffen, damit das betreffende KI-System zum Zeitpunkt des Inverkehrbringens oder der Inbetriebnahme dieses Risiko nicht mehr birgt, oder das KI-System vom Markt zu nehmen oder es innerhalb einer der Art des Risikos angemessenen Frist zurückzurufen.

(2) Der Anbieter oder andere einschlägige Akteure müssen dafür sorgen, dass in Bezug auf alle betroffenen KI-Systeme, die sie in der Union in Verkehr gebracht haben, innerhalb der Frist, die von der Marktüberwachungsbehörde des in Absatz 1 genannten Mitgliedstaats vorgegeben wurde, Korrekturmaßnahmen ergriffen werden.

(3) Der Mitgliedstaat unterrichtet die Kommission und die übrigen Mitgliedstaaten unverzüglich davon. Diese Unterrichtung enthält alle vorliegenden Angaben, insbesondere die für die Identifizierung des betreffenden KI-Systems notwendigen Daten, den Ursprung und die Lieferkette des KI-Systems, die Art des sich daraus ergebenden Risikos sowie die Art und Dauer der ergriffenen nationalen Maßnahmen.

(4) Die Kommission nimmt unverzüglich mit den Mitgliedstaaten und den betreffenden Akteuren Konsultationen auf und prüft die ergriffenen nationalen Maßnahmen. Anhand der Ergebnisse dieser Prüfung entscheidet die Kommission, ob die Maßnahme gerechtfertigt ist oder nicht, und schlägt, falls erforderlich, geeignete Maßnahmen vor.

(5) Die Kommission richtet diese Entscheidung an die Mitgliedstaaten.

Artikel 68
Formale Nichtkonformität

(1) Gelangt die Marktüberwachungsbehörde eines Mitgliedstaats zu einer der folgenden Feststellungen, fordert sie den jeweiligen Anbieter auf, die betreffende Nichtkonformität zu beheben:

a) die Konformitätskennzeichnung wurde nicht nach Artikel 49 angebracht;

b) die Konformitätskennzeichnung wurde nicht angebracht;

c) die EU-Konformitätserklärung wurde nicht ausgestellt;

d) die EU-Konformitätserklärung wurde nicht ordnungsgemäß ausgestellt;

e) die Kennnummer der gegebenenfalls am Konformitätsbewertungsverfahren beteiligten notifizierten Stelle wurde nicht angebracht.

(2) Besteht die Nichtkonformität nach Absatz 1 weiter, so ergreift der betreffende Mitgliedstaat alle geeigneten Maßnahmen, um die Bereitstellung des Hochrisiko-KI-Systems auf dem Markt zu beschränken oder zu untersagen oder um dafür zu sorgen, dass es zurückgerufen oder vom Markt genommen wird.

TITEL IX

VERHALTENSKODIZES

Artikel 69
Verhaltenskodizes

(1) Die Kommission und die Mitgliedstaaten fördern und erleichtern die Aufstellung von Verhaltenskodizes, mit denen erreicht werden soll, dass die in Titel III Kapitel 2 genannten Anforderungen auf KI-Systeme Anwendung finden, die kein hohes Risiko bergen, und zwar auf der Grundlage technischer Spezifikationen und Lösungen, die geeignet sind, die Einhaltung dieser Anforderungen mit Blick auf die Zweckbestimmung der Systeme zu gewährleisten.

(2) Die Kommission und der Ausschuss fördern und erleichtern die Aufstellung von Verhaltenskodizes, mit denen erreicht werden soll, dass KI-Systeme freiwillig weitere Anforderungen erfüllen, die sich beispielsweise auf die ökologische Nachhaltigkeit, die barrierefreie Zugänglichkeit für Personen mit Behinderungen, die Beteiligung von Interessenträgern an der Konzeption und Entwicklung von KI-Systemen und die Vielfalt der Entwicklungsteams beziehen, wobei die Erreichung dieser Ziele anhand klarer Vorgaben und wesentlicher Leistungsindikatoren gemessen wird.

(3) Verhaltenskodizes können von einzelnen KI-System-Anbietern oder von Interessenvertretungen dieser Anbieter oder von beiden aufgestellt werden, auch unter Einbeziehung von Nutzern und Interessenträgern sowie deren Interessenvertretungen. Verhaltenskodizes können sich auf mehrere KI-Systeme erstrecken, um ähnlichen Zweckbestimmungen der jeweiligen Systeme Rechnung zu tragen.

(4) Die Kommission und der Ausschuss berücksichtigen die besonderen Interessen und Bedürfnisse von Kleinanbietern und Startups bei der Förderung und Erleichterung der Aufstellung von Verhaltenskodizes.

TITEL X

VETRAULICHKEIT UND SANKTIONEN

Artikel 70
Vertraulichkeit

(1) Die an der Anwendung dieser Verordnung beteiligten zuständigen nationalen Behörden und notifizierten Stellen wahren die Vertraulichkeit der Informationen und Daten, von denen sie in Ausübung ihrer Aufgaben und Tätigkeiten Kenntnis erlangen und dabei insbesondere Folgendes schützen:

a) Rechte des geistigen Eigentums, vertrauliche Geschäftsinformationen oder Geschäftsgeheimnisse natürlicher oder juristischer Personen, auch Quellcodes, mit Ausnahme der in Artikel 5 der Richtlinie 2016/943 über den Schutz vertraulichen Know-hows und vertraulicher Geschäftsinformationen (Geschäftsgeheimnisse) vor rechtswidrigem Erwerb sowie rechtswidriger Nutzung und Offenlegung genannten Fälle;

b) die wirksame Durchführung dieser Verordnung, insbesondere für die Zwecke von Inspektionen, Untersuchungen oder Audits,

c) öffentliche und nationale Sicherheitsinteressen;

d) die Integrität von Straf- oder Verwaltungsverfahren.

(2) Unbeschadet des Absatzes 1 darf der Austausch vertraulicher Informationen zwischen den zuständigen nationalen Behörden untereinander sowie zwischen den zuständigen nationalen Behörden und der Kommission nicht ohne vorherige Rücksprache mit der zuständigen nationalen Behörde und dem Nutzer, von denen die Informationen stammen, offengelegt werden, sofern die Hochrisiko-KI-Systeme nach Anhang III Nummern 1, 6 und 7 von Strafverfolgungs-, Einwanderungs- oder Asylbehörden verwendet werden und eine solche Offenlegung die öffentlichen und nationalen Sicherheitsinteressen gefährden könnte.

Handeln Strafverfolgungs-, Einwanderungs- oder Asylbehörden als Anbieter von Hochrisiko-KI-Systemen, wie sie in Anhang III Nummern 1, 6 und 7 aufgeführt sind, verbleibt die technische Dokumentation nach Anhang IV in den Räumlichkeiten dieser Behörden. Diese Behörden müssen dafür sorgen, dass die Artikel 63 Absätze 5 bzw. 6 genannten Marktüberwachungsbehörden auf Verlangen unverzüglich Zugang zu dieser Dokumentation oder eine Kopie davon erhalten. Zugang zu dieser Dokumentation oder zu einer Kopie davon darf nur das Personal der Marktüberwachungsbehörde erhalten, das über eine entsprechende Sicherheitsfreigabe verfügt.

(3) Die Absätze 1 und 2 dürfen sich weder auf die Rechte und Pflichten der Kommission, der Mitgliedstaaten und notifizierten Stellen in Bezug auf den Informationsaustausch und die Weitergabe von Warnungen noch auf die Pflichten der betreffenden Parteien auswirken, Informationen auf der Grundlage des Strafrechts der Mitgliedstaaten bereitzustellen.

(4) Die Kommission und die Mitgliedstaaten können mit Regulierungsbehörden von Drittstaaten, mit denen sie bilaterale oder multilaterale Vertraulichkeitsvereinbarungen getroffen haben und die ein angemessenes Niveau an Vertraulichkeit gewährleisten, erforderlichenfalls vertrauliche Informationen austauschen.

Artikel 71
Sanktionen

(1) Entsprechend den Vorgaben dieser Verordnung erlassen die Mitgliedstaaten Vorschriften für Sanktionen, beispielsweise in Form von Geldbußen, die bei Verstößen gegen diese Verordnung Anwendung finden, und ergreifen alle Maßnahmen, die für deren ordnungsgemäße und wirksame Durchsetzung notwendig sind. Die vorgesehenen Sanktionen müssen wirksam, verhältnismäßig und abschreckend sein. Sie berücksichtigen insbesondere die Interessen von Kleinanbietern und Startups sowie deren wirtschaftliches Überleben.

(2) Die Mitgliedstaaten teilen der Kommission diese Vorschriften und Maßnahmen mit und melden ihr unverzüglich alle diesbezüglichen Änderungen.

(3) Bei folgenden Verstößen werden Geldbußen von bis zu 30 000 000 EUR oder – im Falle von Unternehmen – von bis zu 6 % des gesamten weltweiten Jahresumsatzes

des vorangegangenen Geschäftsjahres verhängt, je nachdem, welcher Betrag höher ist:

a) Missachtung des Verbots der in Artikel 5 genannten KI-Praktiken;

b) Nichtkonformität des KI-Systems mit den in Artikel 10 festgelegten Anforderungen.

(4) Verstoßen KI-Systeme gegen die in dieser Verordnung festgelegten Anforderungen oder Pflichten, mit Ausnahme der in den Artikeln 5 und 10 genannten, werden Geldbußen von bis zu 20 000 000 EUR oder – im Falle von Unternehmen – von bis zu 4 % des gesamten weltweiten Jahresumsatzes des vorangegangenen Geschäftsjahres verhängt, je nachdem, welcher Betrag höher ist.

(5) Werden gegenüber notifizierten Stellen und zuständigen nationalen Behörden auf deren Auskunftsverlangen hin falsche, unvollständige oder irreführende Angaben gemacht, werden Geldbußen von bis zu 10 000 000 EUR oder – im Falle von Unternehmen – von bis zu 2 % des gesamten weltweiten Jahresumsatzes des vorangegangenen Geschäftsjahres verhängt, je nachdem, welcher Betrag höher ist.

(6) Bei der Festsetzung der Geldbuße werden in jedem Einzelfall alle relevanten Umstände der konkreten Situation sowie Folgendes gebührend berücksichtigt:

a) Art, Schwere und Dauer des Verstoßes und dessen Folgen;

b) ob bereits andere Marktüberwachungsbehörden demselben Akteur für denselben Verstoß Geldbußen auferlegt haben;

c) Größe und Marktanteil des Akteurs, der den Verstoß begangen hat.

(7) Jeder Mitgliedstaat erlässt Vorschriften darüber, ob und in welchem Umfang gegen Behörden und öffentliche Stellen, die in dem betreffenden Mitgliedstaat niedergelassen sind, Geldbußen verhängt werden können.

(8) In Abhängigkeit vom Rechtssystem des betreffenden Mitgliedstaats können die Vorschriften über Geldbußen je nach den dort geltenden Regeln so angewandt werden, dass die Geldbußen von den zuständigen nationalen Gerichten oder von sonstigen Stellen verhängt werden. Die Anwendung dieser Vorschriften in diesen Mitgliedstaaten muss eine gleichwertige Wirkung haben.

Artikel 72

Verhängung von Geldbußen gegen Organe, Einrichtungen und sonstige Stellen der Union

(1) Der Europäische Datenschutzbeauftragte kann gegen Organe, Einrichtungen und sonstige Stellen der Union, die in den Anwendungsbereich dieser Verordnung fallen, Geldbußen verhängen. Bei der Entscheidung, ob eine Geldbuße verhängt wird, und bei der Festsetzung der Geldbuße werden in jedem Einzelfall alle relevanten Umstände der konkreten Situation sowie Folgendes gebührend berücksichtigt:

a) Art, Schwere und Dauer des Verstoßes und dessen Folgen;

b) die Zusammenarbeit mit dem Europäischen Datenschutzbeauftragten bei der Behebung des Verstoßes und der Minderung seiner möglichen Auswirkungen, einschließlich der Befolgung von Maßnahmen, die der Europäische Datenschutzbeauftragte dem Organ, der der Einrichtung oder der sonstigen Stelle der Union im Hinblick auf denselben Gegenstand zuvor bereits auferlegt hatte;

c) ähnliche frühere Verstöße des Organs, der Einrichtung oder der sonstigen Stelle der Union.

(2) Bei folgenden Verstößen werden Geldbußen von bis zu 500 000 EUR verhängt:

a) Missachtung des Verbots der in Artikel 5 genannten KI-Praktiken;

b) Nichtkonformität des KI-Systems mit den in Artikel 10 festgelegten Anforderungen.

(3) Verstoßen KI-Systeme gegen die in dieser Verordnung festgelegten Anforderungen oder Pflichten, mit Ausnahme der in den Artikeln 5 und 10 genannten, werden Geldbußen von bis zu 250 000 EUR verhängt.

(4) Bevor der Europäische Datenschutzbeauftragte Entscheidungen nach diesem Artikel trifft, gibt er dem Organ, der Einrichtung oder der sonstigen Stelle der Union, gegen das/die sich das von ihm geführte Verfahren richtet, Gelegenheit, sich zum Vorwurf des Verstoßes zu äußern. Der Europäische Datenschutzbeauftragte stützt seine Entscheidungen nur auf die Elemente und Umstände, zu denen sich die betreffenden Parteien äußern können. Beschwerdeführer, soweit vorhanden, müssen in das Verfahren eng einbezogen werden.

(5) Die Verteidigungsrechte der betroffenen Parteien werden während des Verfahrens in vollem Umfang gewahrt. Vorbehaltlich der legitimen Interessen von Einzelpersonen oder Unternehmen im Hinblick auf den Schutz ihrer personenbezogenen Daten oder Geschäftsgeheimnisse haben sie Anspruch auf Einsicht in die Unterlagen des Europäischen Datenschutzbeauftragten.

(6) Das Aufkommen aus den nach diesem Artikel verhängten Geldbußen zählt zu den Einnahmen des Gesamthaushalts der Union.

TITEL XI

BEFUGNISÜBERTRAGUNG UND AUSSCHUSSVERFAHREN

Artikel 73
Ausübung der Befugnisübertragung

(1) Die Befugnis zum Erlass delegierter Rechtsakte wird der Kommission unter den in diesem Artikel festgelegten Bedingungen übertragen.

(2) Die Befugnis zum Erlass delegierter Rechtsakte nach Artikel 4, Artikel 7 Absatz 1, Artikel 11 Absatz 3, Artikel 43 Absatz 5 und 6 und Artikel 48 Absatz 5 wird der Kommission auf unbestimmte Zeit ab dem [*Datum des Inkrafttretens dieser Verordnung*] übertragen.

(3) Die Befugnis zum Erlass delegierter Rechtsakte nach Artikel 4, Artikel 7 Absatz 1, Artikel 11 Absatz 3, Artikel 43 Absatz 5 und 6 und Artikel 48 Absatz 5 kann vom Europäischen Parlament oder vom Rat jederzeit widerrufen werden. Der Beschluss über den Widerruf beendet die Übertragung der in diesem Beschluss angegebenen Befugnis. Er wird am Tag nach seiner Veröffentlichung im *Amtsblatt der Europäischen Union* oder zu einem darin angegebenen späteren Zeitpunkt wirksam. Die Gültigkeit von delegierten Rechtsakten, die bereits in Kraft sind, wird von dem Beschluss über den Widerruf nicht berührt.

(4) Sobald die Kommission einen delegierten Rechtsakt erlässt, übermittelt sie ihn gleichzeitig dem Europäischen Parlament und dem Rat.

(5) Ein delegierter Rechtsakt, der nach Artikel 4, Artikel 7 Absatz 1, Artikel 11 Absatz 3, Artikel 43 Absatz 5 und 6 und Artikel 48 Absatz 5 erlassen wurde, tritt nur in Kraft, wenn weder das Europäische Parlament noch der Rat innerhalb einer Frist von drei Monaten nach Übermittlung dieses Rechtsakts an das Europäische Parlament und den Rat Einwände erhoben haben oder wenn vor Ablauf dieser Frist das Europäische Parlament und der Rat beide der Kommission mitgeteilt haben, dass sie keine Einwände erheben werden. Auf Initiative des Europäischen Parlaments oder des Rates wird diese Frist um drei Monate verlängert.

Artikel 74
Ausschussverfahren

(1) Die Kommission wird von einem Ausschuss unterstützt. Dieser Ausschuss ist ein Ausschuss im Sinne der Verordnung (EU) Nr. 182/2011.

(2) Wird auf diesen Absatz Bezug genommen, gilt Artikel 5 der Verordnung (EU) Nr. 182/2011.

TITEL XII

SCHLUSSBESTIMMUNGEN

Artikel 75
Änderung der Verordnung (EU) Nr. 300/2008

In Artikel 4 Absatz 3 der Verordnung (EG) Nr. 300/2008 wird folgender Unterabsatz angefügt:

„Beim Erlass detaillierter Maßnahmen, die technische Spezifikationen und Verfahren für die Genehmigung und den Einsatz von Sicherheitsausrüstung betreffen, bei der auch Systeme der künstlichen Intelligenz im Sinne der Verordnung (EU) YYY/XX [über Künstliche Intelligenz] des Europäischen Parlaments und des Rates* zum Einsatz kommen, werden die in Titel III Kapitel 2 jener Verordnung festgelegten Anforderungen berücksichtigt.

_____

* Verordnung (EU) YYY/XX [über Künstliche Intelligenz] (ABl...)“

Artikel 76
Änderung der Verordnung (EU) Nr. 167/2013

In Artikel 17 Absatz 5 der Verordnung (EG) Nr. 167/2013 wird folgender Unterabsatz angefügt:

„Beim Erlass delegierter Rechtsakte nach Unterabsatz 1, die sich auf Systeme der künstlichen Intelligenz beziehen, bei denen es sich um Sicherheitskomponenten im Sinne der Verordnung (EU) YYY/XX [über Künstliche Intelligenz] des Europäischen Parlaments und des Rates* handelt, werden die in Titel III Kapitel 2 jener Verordnung festgelegten Anforderungen berücksichtigt.

_____

* Verordnung (EU) YYY/XX [über Künstliche Intelligenz] (ABl...)“

Artikel 77
Änderung der Verordnung (EU) Nr. 168/2013

In Artikel 22 Absatz 5 der Verordnung (EG) Nr. 168/2013 wird folgender Unterabsatz angefügt:

„Beim Erlass delegierter Rechtsakte nach Unterabsatz 1, die sich auf Systeme der künstlichen Intelligenz beziehen, bei denen es sich um Sicherheitskomponenten im Sinne der Verordnung (EU) YYY/XX [über Künstliche Intelligenz] des Europäischen Parlaments und des Rates* handelt, werden die in Titel III Kapitel 2 jener Verordnung festgelegten Anforderungen berücksichtigt.

_____

* Verordnung (EU) YYY/XX [über Künstliche Intelligenz] (ABl...)“

Artikel 78
Änderung der Richtlinie 2014/90/EU

In Artikel 8 der Richtlinie 2014/90/EU wird folgender Absatz angefügt:

„(4) Bei Systemen der künstlichen Intelligenz, bei denen es sich um Sicherheitskomponenten im Sinne der Verordnung (EU) YYY/XX [über Künstliche Intelligenz] des Europäischen Parlaments und des Rates* handelt, berücksichtigt die Kommission bei der Ausübung ihrer Tätigkeiten nach Absatz 1 und bei Erlass technischer Spezifikationen und Prüfnormen nach den Absätzen 2 und 3 die in Titel III Kapitel 2 jener Verordnung festgelegten Anforderungen.

_____

* Verordnung (EU) YYY/XX [über Künstliche Intelligenz] (ABl...)“.

Artikel 79
Änderung der Richtlinie (EU) 2016/797

In Artikel 5 der Richtlinie (EU) 2016/797 wird folgender Absatz angefügt:

„(12) „Beim Erlass von delegierten Rechtsakten nach Unterabsatz 1 und von Durchführungsrechtsakten nach Absatz 11, die sich auf Systeme der künstlichen Intelligenz beziehen, bei denen es sich um Sicherheitskomponenten im Sinne der Verordnung (EU) YYY/XX [über Künstliche Intelligenz] des Europäischen Parlaments und des Rates* handelt, werden die in Titel III Kapitel 2 jener Verordnung festgelegten Anforderungen berücksichtigt.

_____

* Verordnung (EU) YYY/XX [über Künstliche Intelligenz] (ABl...)“.

Artikel 80
Änderung der Verordnung (EU) Nr. 2018/858

In Artikel 5 der Verordnung (EU) 2018/858 wird folgender Absatz angefügt:

„(4) „Beim Erlass delegierter Rechtsakte nach Absatz 3, die sich auf Systeme der künstlichen Intelligenz beziehen, bei denen es sich um Sicherheitskomponenten im Sinne der Verordnung (EU) YYY/XX [über Künstliche Intelligenz] des Europäischen Parlaments und des Rates* handelt, werden die in Titel III Kapitel 2 jener Verordnung festgelegten Anforderungen berücksichtigt.

_____

* Verordnung (EU) YYY/XX [über Künstliche Intelligenz] (ABl...)“.

Artikel 81
Änderung der Verordnung (EU) 2018/1139

Die Verordnung (EU) 2018/1139 wird wie folgt geändert:

1. In Artikel 17 wird folgender Absatz angefügt:

„(3) „Unbeschadet des Absatzes 2 werden beim Erlass von Durchführungsrechtakten nach Absatz 1, die sich auf Systeme der künstlichen Intelligenz beziehen, bei denen es sich um Sicherheitskomponenten im Sinne der Verordnung (EU) YYY/XX [über Künstliche Intelligenz] des Europäischen Parlaments und des Rates* handelt, die in Titel III Kapitel 2 jener Verordnung festgelegten Anforderungen berücksichtigt.

_____

* Verordnung (EU) YYY/XX [über Künstliche Intelligenz] (ABl...)“

2. In Artikel 19 wird folgender Absatz angefügt:

„(4) „Beim Erlass delegierter Rechtsakte nach den Absätzen 1 und 2, die sich auf Systeme der künstlichen Intelligenz beziehen, bei denen es sich um Sicherheitskomponenten im Sinne der Verordnung (EU) YYY/XX [über Künstliche Intelligenz] des Europäischen Parlaments und des Rates* handelt, werden die in Titel III Kapitel 2 jener Verordnung festgelegten Anforderungen berücksichtigt.“

3. In Artikel 43 wird folgender Absatz angefügt:

„(4) „Beim Erlass von Durchführungsrechtsakten nach Absatz 1, die sich auf Systeme der künstlichen Intelligenz beziehen, bei denen es sich um Sicherheitskomponenten im Sinne der Verordnung (EU) YYY/XX [über Künstliche Intelligenz] des Europäischen Parlaments und des Rates* handelt, werden die in Titel III Kapitel 2 jener Verordnung festgelegten Anforderungen berücksichtigt.“

4. In Artikel 47 wird folgender Absatz angefügt:

„(3) „Beim Erlass delegierter Rechtsakte nach den Absätzen 1 und 2, die sich auf Systeme der künstlichen Intelligenz beziehen, bei denen es sich um Sicherheitskomponenten im Sinne der Verordnung (EU) YYY/XX [über Künstliche Intelligenz] des Europäischen Parlaments und des Rates* handelt, werden die in Titel III Kapitel 2 jener Verordnung festgelegten Anforderungen berücksichtigt.“

5. In Artikel 57 wird folgender Absatz angefügt:

„Beim Erlass solcher Durchführungsrechtsakte, die sich auf Systeme der künstlichen Intelligenz beziehen, bei denen es sich um Sicherheitskomponenten im Sinne der Verordnung (EU) YYY/XX [über Künstliche Intelligenz] des Europäischen Parlaments und des Rates* handelt, werden die in Titel III Kapitel 2 jener Verordnung festgelegten Anforderungen berücksichtigt.“

6. In Artikel 58 wird folgender Absatz angefügt:

„(3) Beim Erlass delegierter Rechtsakte nach den Absätzen 1 und 2, die sich auf Systeme der künstlichen Intelligenz beziehen, bei denen es sich um Sicherheitskomponenten im Sinne der Verordnung (EU) YYY/XX [über Künstliche Intelligenz] des Europäischen Parlaments und

des Rates* handelt, werden die in Titel III Kapitel 2 jener Verordnung festgelegten Anforderungen berücksichtigt.“

Artikel 82
Änderung der Verordnung (EU) Nr. 2019/2144

In Artikel 11 der Verordnung (EU) 2019/2144 wird folgender Absatz angefügt:

„(3) Beim Erlass von Durchführungsrechtsakten nach Absatz 2, die sich auf Systeme der künstlichen Intelligenz beziehen, bei denen es sich um Sicherheitskomponenten im Sinne der Verordnung (EU) YYY/XX [über Künstliche Intelligenz] des Europäischen Parlaments und des Rates* handelt, werden die in Titel III Kapitel 2 jener Verordnung festgelegten Anforderungen berücksichtigt.

_____

* Verordnung (EU) YYY/XX [über Künstliche Intelligenz] (ABl...)“.

Artikel 83
Bereits in Verkehr gebrachte oder in Betrieb genommene KI-Systeme

(1) Diese Verordnung gilt nicht für KI-Systeme, bei denen es sich um Komponenten von IT-Großsystemen handelt, die mit den in Anhang IX genannten Rechtsakten festgelegt wurden und vor dem [*Datum 12 Monate nach dem Datum der Anwendung dieser Verordnung nach Artikel 85 Absatz 2*] in Verkehr gebracht oder in Betrieb genommen wurden, sofern der Ersatz oder die Änderung jener Rechtsakte nicht zu einer wesentlichen Änderung der Konzeption oder Zweckbestimmung des betreffenden KI-Systems führt.

Die in dieser Verordnung festgelegten Anforderungen werden gegebenenfalls bei der Bewertung jedes IT-Großsystems, das auf der Grundlage der in Anhang IX aufgeführten Rechtsakte eingerichtet wurde, berücksichtigt, wobei die Bewertung entsprechend den Vorgaben der jeweiligen Rechtsakte erfolgt.

(2) Diese Verordnung gilt – mit Ausnahme der in Absatz 1 genannten Systeme – für Hochrisiko-KI-Systeme, die vor dem [*Datum der Anwendung dieser Verordnung nach Artikel 85 Absatz 2*] in Verkehr gebracht oder in Betrieb genommen wurden, nur dann, wenn diese Systeme danach in ihrer Konzeption oder Zweckbestimmung wesentlich geändert wurden.

Artikel 84
Bewertung und Überarbeitung

(1) Die Kommission prüft nach dem Inkrafttreten dieser Verordnung einmal jährlich, ob eine Änderung der Liste in Anhang III erforderlich ist.

(2) Bis zum [*Datum drei Jahre nach dem Datum der Anwendung dieser Verordnung nach Artikel 85 Absatz 2*] und danach alle vier Jahre legt die Kommission dem Europäischen Parlament und dem Rat einen Bericht über die Bewertung und Überprüfung dieser Verordnung vor. Die Berichte werden veröffentlicht.

(3) In den in Absatz 2 genannten Berichten wird insbesondere auf folgende Aspekte eingegangen:

a) Stand der finanziellen und personellen Ressourcen der zuständigen nationalen Behörden im Hinblick auf deren Fähigkeit, die ihnen auf der Grundlage dieser Verordnung übertragenen Aufgaben wirksam zu erfüllen;

b) Stand der Sanktionen, insbesondere der Bußgelder nach Artikel 71 Absatz 1, die Mitgliedstaaten bei Verstößen gegen diese Verordnung verhängt haben.

(4) Innerhalb von [*drei Jahren nach dem Datum der Anwendung dieser Verordnung nach Artikel 85 Absatz 2*] und danach alle vier Jahre führt die Kommission eine Bewertung der Folgen und Wirksamkeit der Verhaltenskodizes durch, mit denen die Anwendung der Anforderungen in Titel III Kapitel 2 und möglicherweise auch zusätzlicher Anforderungen an andere KI-Systeme als Hochrisiko-KI-Systeme gefördert werden soll.

(5) Für die Zwecke der Absätze 1 bis 4 übermitteln der Ausschuss, die Mitgliedstaaten und die zuständigen nationalen Behörden der Kommission auf Anfrage die gewünschten Informationen.

(6) Bei den in den Absätzen 1 und 4 genannten Bewertungen und Überprüfungen berücksichtigt die Kommission die Standpunkte und Feststellungen des Ausschusses, des Europäischen Parlaments, des Rates und anderer einschlägiger Stellen oder Quellen.

(7) Die Kommission legt erforderlichenfalls geeignete Vorschläge zur Änderung dieser Verordnung vor und berücksichtigt dabei insbesondere die technischen Entwicklungen und die Fortschritte in der Informationsgesellschaft.

Artikel 85
Inkrafttreten und Geltungsbeginn

(1) Diese Verordnung tritt am zwanzigsten Tag nach ihrer Veröffentlichung im *Amtsblatt der Europäischen Union* in Kraft.

(2) Diese Verordnung gilt ab dem [24 Monate nach Inkrafttreten der Verordnung].

(3) Abweichend von Absatz 2 gilt Folgendes:

a) Titel III Kapitel 4 und Titel VI gelten ab dem [*drei Monate nach Inkrafttreten der Verordnung*];

b) Artikel 71 gilt ab dem [*12 Monate nach Inkrafttreten der Verordnung*].

Diese Verordnung ist in allen ihren Teilen verbindlich und gilt unmittelbar in jedem Mitgliedstaat.

Geschehen zu Brüssel am […]

Im Namen des Europäischen Parlaments	*Im Namen des Rates*
Der Präsident	*Der Präsident*

FINANZBOGEN ZU RECHTSAKTEN

1. RAHMEN DES VORSCHLAGS/DER INITIATIVE

1.1. Bezeichnung des Vorschlags/der Initiative

1.2. Politikbereich(e)

1.3. Der Vorschlag/Die Initiative betrifft

1.4. Ziel(e)

1.4.1. Allgemeine(s) Ziel(e)

1.4.2. Einzelziel(e)

1.4.3. Erwartete Ergebnisse und Auswirkungen

1.4.4. Leistungsindikatoren

1.5. Begründung des Vorschlags/der Initiative

1.5.1. Kurz- oder langfristig zu deckender Bedarf, einschließlich einer detaillierten Zeitleiste für die Durchführung der Initiative

1.5.2. Mehrwert aufgrund des Tätigwerdens der Union (kann sich aus unterschiedlichen Faktoren ergeben, z. B. Vorteile durch Koordinierung, Rechtssicherheit, größerer Wirksamkeit oder Komplementarität). Für die Zwecke dieser Nummer bezeichnet der Ausdruck „Mehrwert aufgrund des Tätigwerdens der Union“ den Wert, der sich aus dem Tätigwerden der Union ergibt und den Wert ergänzt, der andernfalls allein von den Mitgliedstaaten geschaffen worden wäre.

1.5.3. Aus früheren ähnlichen Maßnahmen gewonnene Erkenntnisse

1.5.4. Vereinbarkeit mit dem Mehrjährigen Finanzrahmen sowie mögliche Synergieeffekte mit anderen geeigneten Instrumenten

1.5.5 Bewertung der verschiedenen verfügbaren Finanzierungsoptionen, einschließlich der Möglichkeiten für eine Umschichtung

1.6. Laufzeit und finanzielle Auswirkungen des Vorschlags/der Initiative

1.7. Vorgeschlagene Methode(n) der Mittelverwaltung

2. VERWALTUNGSMAßNAHMEN

2.1. Überwachung und Berichterstattung

2.2. Verwaltungs- und Kontrollsystem

2.2.1. Begründung der Methode(n) der Mittelverwaltung, des Durchführungsmechanismus/der Durchführungsmechanismen für die Finanzierung, der Zahlungsmodalitäten und der Kontrollstrategie, wie vorgeschlagen

2.2.2. Angaben zu den ermittelten Risiken und dem/den zu deren Eindämmung eingerichteten System(en) der internen Kontrolle

2.2.3. Schätzung und Begründung der Kosteneffizienz der Kontrollen (Verhältnis zwischen den Kontrollkosten und dem Wert der betreffenden verwalteten Mittel) sowie Bewertung des erwarteten Ausmaßes des Fehlerrisikos (bei Zahlung und beim Abschluss)

2.3. Prävention von Betrug und Unregelmäßigkeiten

3. GESCHÄTZTE FINANZIELLE AUSWIRKUNGEN DES VORSCHLAGS/DER INITIATIVE

3.1. Betroffene Rubrik(en) des Mehrjährigen Finanzrahmens und Ausgabenlinie(n) im Haushaltsplan

3.2. Geschätzte finanzielle Auswirkungen des Vorschlags auf die Mittel

3.2.1. Übersicht über die geschätzten Auswirkungen auf die operativen Mittel

3.2.2. Geschätzte Ergebnisse, die mit operativen Mitteln finanziert werden

3.2.3. Übersicht über die geschätzten Auswirkungen auf die Verwaltungsmittel

3.2.4. Vereinbarkeit mit dem Mehrjährigen Finanzrahmen

3.2.5. Finanzierungsbeteiligung Dritter

3.3. Geschätzte Auswirkungen auf die Einnahmen

FINANZBOGEN ZU RECHTSAKTEN

1. RAHMEN DES VORSCHLAGS/DER INITIATIVE

1.1. Bezeichnung des Vorschlags/der Initiative

Verordnung des Europäischen Parlaments und des Rates zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz (Gesetz über künstliche Intelligenz) und zur Änderung bestimmter Rechtsakte der Union

1.2. Politikbereich(e)

Kommunikationsnetze, Inhalte und Technologien;

Binnenmarkt, Industrie, Unternehmertum und KMU;

Die finanziellen Auswirkungen betreffen die neuen Aufgaben, mit denen die Kommission betraut wird, einschließlich der Unterstützung des KI-Ausschusses der EU;

Tätigkeit: Gestaltung der digitalen Zukunft Europas.

1.3. Der Vorschlag/Die Initiative betrifft

X **eine neue Maßnahme**

☐ **eine neue Maßnahme im Anschluss an ein Pilotprojekt/eine vorbereitende Maßnahme**[64]

☐ **die Verlängerung einer bestehenden Maßnahme**

☐ **eine neu ausgerichtete Maßnahme**

1.4. Ziel(e)

1.4.1. Allgemeine(s) Ziel(e)

Übergeordnetes Ziel der Maßnahme ist die Gewährleistung des reibungslosen Funktionierens des Binnenmarkts, indem die Voraussetzungen für die Entwicklung und Verwendung vertrauenswürdiger künstlicher Intelligenz in der Union geschaffen werden.

1.4.2. Einzelziel(e)

Einzelziel Nr. 1

Festlegung konkreter Anforderungen an und Pflichten für alle an der Wertschöpfungskette Beteiligten, um zu gewährleisten, dass die auf dem Markt in Verkehr gebrachten und verwendeten KI-Systeme sicher sind und die bestehenden Grundrechte und die Werte der Union wahren.

Einzelziel Nr. 2

Gewährleistung von Rechtssicherheit, um Investitionen und Innovationen im Bereich KI zu fördern, indem klargestellt wird, welchen grundlegenden Anforderungen und Pflichten nachgekommen werden muss sowie welche Konformitäts- und Einhaltungsverfahren befolgt werden müssen, um ein KI-System auf dem Unionsmarkt in Verkehr zu bringen oder zu verwenden.

[64] Im Sinne des Artikels 54 Absatz 2 Buchstabe a oder b der Haushaltsordnung.

Einzelziel Nr. 3

Stärkung der Leitungsstruktur und der wirksamen Durchsetzung des geltenden Rechts zur Wahrung der Grundrechte sowie der Sicherheitsanforderungen für KI-Systeme durch Erteilung neuer Befugnisse sowie Bereitstellung von Ressourcen und klaren Regeln für die zuständigen Behörden in Bezug auf Konformitätsbewertungsverfahren und nachträgliche Beobachtungsverfahren sowie die Aufteilung der Leitungs- und Überwachungsaufgaben zwischen der nationalen und der EU-Ebene.

Einzelziel Nr. 4

Erleichterung der Entwicklung eines Binnenmarkts für rechtskonforme, sichere und vertrauenswürdige KI-Anwendungen und Verhinderung einer Marktfragmentierung, indem die EU Maßnahmen ergreift, um Mindestanforderungen für KI-Systeme festzulegen, die im Einklang mit den bestehenden Grundrechten und Sicherheitsvorschriften auf dem Unionsmarkt in Verkehr gebracht und verwendet werden sollen.

1.4.3. Erwartete Ergebnisse und Auswirkungen

Bitte geben Sie an, wie sich der Vorschlag/die Initiative auf die Begünstigten/Zielgruppen auswirken dürfte.

Minimale, aber klare Anforderungen sollten sich positiv auf KI-Lieferanten auswirken, indem sie Rechtssicherheit schaffen und den Zugang zum gesamten Binnenmarkt gewährleisten.

KI-Nutzern sollte die Rechtssicherheit zugutekommen, dass die von ihnen erworbenen Hochrisiko-KI-Systeme mit den europäischen Rechtsvorschriften und Werten im Einklang stehen.

Die Verbraucherinnen und Verbraucher sollten davon profitieren, dass das Risiko von Verletzungen ihrer Sicherheit oder ihrer Grundrechte eingedämmt wird.

1.4.4. Leistungsindikatoren

Bitte geben Sie an, anhand welcher Indikatoren sich die Realisierung des Vorschlags/der Initiative verfolgen lässt.

Indikator 1

Zahl der schwerwiegenden Vorfälle oder KI-Leistungen, die einen schwerwiegenden Vorfall oder eine Verletzung der Pflicht zur Wahrung der Grundrechte darstellen, (halbjährlich) nach Anwendungsbereichen und berechnet a) in absoluten Zahlen, b) als Anteil der eingesetzten Anwendungen und c) Anteil der betroffenen Bürger.

Indikator 2

a) Gesamtinvestitionen in KI in der EU (pro Jahr)

b) Gesamtinvestitionen in KI nach Mitgliedstaat (pro Jahr)

c) Anteil von Unternehmen, die KI nutzen (pro Jahr)

d) Anteil von KMU, die KI nutzen (pro Jahr)

Buchstaben a und b werden auf der Grundlage amtlicher Quellen berechnet und mit Schätzungen des privaten Sektors verglichen.

Buchstaben c und d werden durch regelmäßige Unternehmenserhebungen erfasst.

1.5. Begründung des Vorschlags/der Initiative

1.5.1. Kurz- oder langfristig zu deckender Bedarf, einschließlich einer detaillierten Zeitleiste für die Durchführung der Initiative

Die Verordnung sollte eineinhalb Jahre nach ihrer Annahme uneingeschränkt anwendbar sein. Die Elemente der Leitungsstruktur sollten jedoch bereits vor diesem Zeitpunkt eingerichtet sein. Insbesondere müssen die Mitgliedstaaten bereits bestehende Behörden benannt und/oder neue Behörden eingerichtet haben, die die in den Rechtsvorschriften festgelegten Aufgaben bereits früher wahrnehmen, und der KI-Ausschuss der EU sollte eingerichtet und arbeitsbereit sein. Zum Zeitpunkt der Anwendbarkeit sollte die europäische Datenbank der KI-Systeme voll funktionsfähig sein. Parallel zum Annahmeverfahren ist daher die Datenbank zu entwickeln, damit ihre Entwicklung zum Zeitpunkt des Inkrafttretens der Verordnung abgeschlossen ist.

1.5.2. Mehrwert aufgrund des Tätigwerdens der Union (kann sich aus unterschiedlichen Faktoren ergeben, z. B. Vorteile durch Koordinierung, Rechtssicherheit, größerer

Wirksamkeit oder Komplementarität). Für die Zwecke dieser Nummer bezeichnet der Ausdruck „Mehrwert aufgrund des Tätigwerdens der Union“ den Wert, der sich aus dem Tätigwerden der Union ergibt und den Wert ergänzt, der andernfalls allein von den Mitgliedstaaten geschaffen worden wäre.

Die reibungslose unionsweite Bereitstellung von KI-Systemen wird durch das Entstehen eines Flickenteppichs potenziell abweichender nationaler Vorschriften behindert, die zudem die Sicherheit und den Schutz der Grundrechte sowie die Einhaltung der Werte der Union länderübergreifend nur unzureichend gewährleisten. Eine gemeinsame Legislativmaßnahme der EU im KI-Bereich könnte den Binnenmarkt ankurbeln und verfügt über großes Potenzial, der europäischen Industrie auf der Weltbühne einen Wettbewerbsvorteil und Größenvorteile zu verschaffen, die von einzelnen Mitgliedstaaten allein nicht erzielt werden können.

1.5.3. Aus früheren ähnlichen Maßnahmen gewonnene Erkenntnisse

Die Richtlinie über den elektronischen Geschäftsverkehr (2000/31/EG) setzt den übergeordneten Rahmen für das Funktionieren des Binnenmarktes und die Aufsicht über digitale Dienste und legt die Grundstruktur für ein System der Zusammenarbeit zwischen den Mitgliedstaaten. Sie deckt im Prinzip alle Anforderungen an digitale Dienste ab. Die Bewertung der Richtlinie brachte mehrere Mängel in diesem System der Zusammenarbeit zu Tage, darunter wichtige Verfahrensaspekte, wie fehlende klare Fristen für Antworten aus den Mitgliedstaaten, gepaart mit einer allgemeinen mangelnden Bereitschaft zur Beantwortung von Anfragen. Dies hat im Laufe der Jahre zu einem Mangel an Vertrauen zwischen den Mitgliedstaaten geführt, wenn es darum geht, Bedenken in Bezug auf grenzüberschreitender Anbieter digitaler Dienste auszuräumen. Die Bewertung der Richtlinie hat gezeigt, dass auf europäischer Ebene differenzierte Regeln und Anforderungen festgelegt werden müssen. Aus diesem Grund würde die Umsetzung der in dieser Verordnung festgelegten besonderen Verpflichtungen einen spezifischen Kooperationsmechanismus auf EU-Ebene mit einer Leitungsstruktur erfordern, die die Koordinierung der jeweils zuständigen Stellen auf EU-Ebene gewährleistet.

1.5.4. Vereinbarkeit mit dem Mehrjährigen Finanzrahmen sowie mögliche Synergieeffekte mit anderen geeigneten Instrumenten

In der Verordnung zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz und zur Änderung bestimmter Rechtsakte der Union wird ein neuer gemeinsamer Rahmen von Anforderungen für KI-Systeme eingeführt, der weit über den Rahmen der bestehenden Rechtsvorschriften hinausgeht. Aus diesem Grund muss mit diesem Vorschlag eine neue nationale und europäische Regulierungs- und Koordinierungsfunktion geschaffen werden. Was mögliche Synergien mit anderen geeigneten Instrumenten anbelangt, so kann die Rolle der notifizierenden Behörden auf nationaler Ebene von nationalen Behörden wahrgenommen werden, die ähnliche Aufgaben im Rahmen anderer EU-Verordnungen wahrnehmen. Durch die Stärkung des Vertrauens in KI und damit die Förderung von Investitionen in die Entwicklung und Einführung von KI ergänzt sie darüber hinaus das Programm „Digitales Europa“, zu dessen fünf Prioritäten die Förderung der Verbreitung der KI gehört.

1.5.5. Bewertung der verschiedenen verfügbaren Finanzierungsoptionen, einschließlich der Möglichkeiten für eine Umschichtung

Personal wird umgesetzt. Die übrigen Kosten werden aus dem Finanzrahmen des Programms „Digitales Europa“ finanziert, da das Ziel dieser Verordnung – Gewährleistung einer vertrauenswürdigen KI – unmittelbar zu einem Kernziel des Programms „Digitales Europa“ beiträgt, nämlich der Beschleunigung der Entwicklung und Einführung von KI in Europa.

1.6. Laufzeit und finanzielle Auswirkungen des Vorschlags/der Initiative

☐ **befristete Laufzeit**

– ☐ Laufzeit: [TT.MM.]JJJJ bis [TT.MM.]JJJJ

– ☐ Finanzielle Auswirkungen auf die Mittel für Verpflichtungen von JJJJ bis JJJJ und auf die Mittel für Zahlungen von JJJJ bis JJJJ

X **unbefristete Laufzeit**

– Anlaufphase von ein/zwei Jahren (zu bestätigen),

– anschließend reguläre Umsetzung.

1.7. Vorgeschlagene Methode(n) der Mittelverwaltung[65]

X **Direkte Mittelverwaltung** durch die Kommission

– ☐ durch ihre Dienststellen, einschließlich ihres Personals in den Delegationen der Union

– ☐ durch Exekutivagenturen

☐ **Geteilte Mittelverwaltung** mit Mitgliedstaaten

☐ **Indirekte Mittelverwaltung** durch Übertragung von Haushaltsvollzugsaufgaben an:

– ☐ Drittländer oder die von ihnen benannten Einrichtungen

– ☐ internationale Einrichtungen und deren Agenturen (bitte angeben)

– ☐ die EIB und den Europäischen Investitionsfonds

– ☐ Einrichtungen im Sinne der Artikel 70 und 71 der Haushaltsordnung

– ☐ öffentlich-rechtliche Körperschaften

– ☐ privatrechtliche Einrichtungen, die im öffentlichen Auftrag tätig werden, sofern sie ausreichende finanzielle Garantien bieten

– ☐ privatrechtliche Einrichtungen eines Mitgliedstaats, die mit der Einrichtung einer öffentlich-privaten Partnerschaft betraut werden und die ausreichende finanzielle Garantien bieten

– ☐ Personen, die mit der Durchführung bestimmter Maßnahmen im Bereich der GASP im Rahmen des Titels V EUV betraut und in dem maßgeblichen Basisrechtsakt benannt sind

– *Falls mehrere Methoden der Mittelverwaltung angegeben werden, ist dies unter „Bemerkungen“ näher zu erläutern.*

Bemerkungen

[65] Erläuterungen zu den Methoden der Mittelverwaltung und Verweise auf die Haushaltsordnung enthält die Website BudgWeb (in französischer und englischer Sprache): http://www.cc.cec/budg/man/budgmanag/budgmanag_en.html.

2. VERWALTUNGSMAßNAHMEN

2.1. Überwachung und Berichterstattung

Bitte geben Sie an, wie oft und unter welchen Bedingungen diese Tätigkeiten erfolgen.

Die Verordnung wird fünf Jahre nach ihrem Inkrafttreten überprüft und bewertet. Die Kommission wird dem Europäischen Parlament, dem Rat sowie dem Europäischen Wirtschafts- und Sozialausschuss über die Ergebnisse der Bewertung Bericht erstatten.

2.2. Verwaltungs- und Kontrollsystem(e)

2.2.1. Begründung der Methode(n) der Mittelverwaltung, des Durchführungsmechanismus/der Durchführungsmechanismen für die Finanzierung, der Zahlungsmodalitäten und der Kontrollstrategie, wie vorgeschlagen

Mit der Verordnung wird eine neue Politik in Bezug auf harmonisierte Vorschriften für die Bereitstellung von Systemen der künstlichen Intelligenz im Binnenmarkt unter Wahrung der Sicherheit und der Grundrechte festgelegt. Diese neuen Vorschriften erfordern ein Kohärenzverfahren für die grenzüberschreitende Anwendung der Verpflichtungen aus dieser Verordnung in Form einer neuen Beratergruppe, die die Tätigkeiten der nationalen Behörden koordiniert.

Um diesen neuen Aufgaben gerecht zu werden, müssen die Dienststellen der Kommission angemessen mit Ressourcen ausgestattet werden. Die Durchsetzung der neuen Verordnung erfordert schätzungsweise 10 VZÄ (5 VZÄ für die Unterstützung der Tätigkeiten des Ausschusses und 5 VZÄ für den Europäischen Datenschutzbeauftragten, der als notifizierende Stelle für KI-Systeme fungiert, die von einer Einrichtung der Europäischen Union eingesetzt werden).

2.2.2. Angaben zu den ermittelten Risiken und dem/den zu deren Eindämmung eingerichteten System(en) der internen Kontrolle

Um sicherzustellen, dass die Mitglieder des Ausschusses auf der Grundlage von Fakten fundierte Analysen durchführen können, ist vorgesehen, dass der Ausschuss durch die Verwaltungsstruktur der Kommission unterstützt wird und dass eine Expertengruppe eingesetzt wird, die erforderlichenfalls zusätzliches Fachwissen zur Verfügung stellt.

2.2.3. Schätzung und Begründung der Kosteneffizienz der Kontrollen (Verhältnis zwischen den Kontrollkosten und dem Wert der betreffenden verwalteten Mittel) sowie Bewertung des erwarteten Ausmaßes des Fehlerrisikos (bei Zahlung und beim Abschluss)

Für die Sitzungskosten erscheinen angesichts des geringen Werts pro Transaktion (z. B. Erstattung der Reisekosten eines Delegierten für eine Sitzung) die üblichen Kontrollverfahren ausreichend. In Bezug auf die Entwicklung der Datenbank verfügt die GD CNECT durch zentrale Vergabetätigkeiten bei der öffentlichen Auftragsvergabe über ein starkes internes Kontrollsystem.

2.3. Prävention von Betrug und Unregelmäßigkeiten

Bitte geben Sie an, welche Präventions- und Schutzmaßnahmen, z. B. im Rahmen der Betrugsbekämpfungsstrategie, bereits bestehen oder angedacht sind.

Die für die Kommission geltenden Betrugsbekämpfungsmaßnahmen gelten auch für die zusätzlichen Mittel, die für diese Verordnung erforderlich werden.

3. GESCHÄTZTE FINANZIELLE AUSWIRKUNGEN DES VORSCHLAGS/DER INITIATIVE

3.1. Betroffene Rubrik(en) des Mehrjährigen Finanzrahmens und Ausgabenlinie(n) im Haushaltsplan

- Bestehende Haushaltslinien

In der Reihenfolge der Rubriken des Mehrjährigen Finanzrahmens und der Haushaltslinien.

Rubrik des Mehrjährigen Finanzrahmens	Haushaltslinie	Art der Ausgabe	Finanzierungsbeiträge			
	Nummer	GM/NGM [66]	von EFTA-Ländern [67]	von Kandidatenländern [68]	von Drittländern	nach Artikel 21 Absatz 2 Buchstabe b der Haushaltsordnung
7	20 02 06 Verwaltungsausgaben	NGM	NEIN	NEIN	NEIN	NEIN
1	02 04 03 Künstliche Intelligenz	GM	JA	NEIN	NEIN	NEIN
1	02 01 30 01 Unterstützungsausgaben für das Programm „Digitales Europa“	NGM	JA	NEIN	NEIN	NEIN

3.2. Geschätzte finanzielle Auswirkungen des Vorschlags auf die Mittel

3.2.1. Übersicht über die geschätzten Auswirkungen auf die Ausgaben für operative Mittel

– ☐ Für den Vorschlag/die Initiative werden keine operativen Mittel benötigt.

– X Für den Vorschlag/die Initiative werden die folgenden operativen Mittel benötigt:

in Mio. EUR (3 Dezimalstellen)

[66] GM = Getrennte Mittel/NGM = Nichtgetrennte Mittel.

[67] EFTA: Europäische Freihandelsassoziation.

[68] Kandidatenländer und gegebenenfalls potenzielle Kandidaten des Westbalkans.

Rubrik des Mehrjährigen Finanzrahmens	1	

GD: CNECT				Jahr **2022**	Jahr **2023**	Jahr **2024**	Jahr **2025**	Jahr **2026**	Jahr **2027**[69]	**INSGESAMT**	
• Operative Mittel											
Haushaltslinie[70] 02 04 03		Verpflichtungen	(1a)		1,000						**1,000**
		Zahlungen	(2a)		0,600	0,100	0,100	0,100	0,100		**1,000**
Haushaltslinie		Verpflichtungen	(1b)								
		Zahlungen	(2b)								
Aus der Dotation bestimmter spezifischer Programme finanzierte Verwaltungsausgaben[71]											
Haushaltslinie 02 01 30 01			(3)		0,240	0,240	0,240	0,240	0,240		**1,200**
Mittel INSGESAMT für die GD CNECT		Verpflichtungen	=1a+1b +3		**1,240**		**0,240**	**0,240**	**0,240**		**2,200**
		Zahlungen	=2a+2b +3		**0,840**	**0,340**	**0,340**	**0,340**	**0,340**		**2,200**

•Operative Mittel INSGESAMT	Verpflichtungen	(4)		1,000						**1,000**
	Zahlungen	(5)		0,600	0,100	0,100	0,100	0,100		**1,000**
•Aus der Dotation bestimmter spezifischer Programme finanzierte Verwaltungsausgaben INSGESAMT		(6)		**0,240**	**0,240**	**0,240**	**0,240**	**0,240**		**1,200**

69 Vorläufig und abhängig von der Verfügbarkeit von Haushaltsmitteln.

70 Gemäß dem offiziellen Eingliederungsplan.

71 Technische und/oder administrative Hilfe und Ausgaben zur Unterstützung der Durchführung von Programmen bzw. Maßnahmen der EU (vormalige BA-Linien), indirekte Forschung, direkte Forschung.

Mittel INSGESAMT unter RUBRIK 1 des mehrjährigen Finanzrahmens	Verpflichtungen	=4+ 6		1,240	0,240	0,240	0,240	0,240		**2,200**
	Zahlungen	=5+ 6		0,840	0,340	0,340	0,340	0,340		**2,200**

Wenn der Vorschlag/die Initiative mehrere Rubriken betrifft, ist der vorstehende Abschnitt zu wiederholen:

•Operative Mittel INSGESAMT (alle operativen Rubriken)	Verpflichtungen	(4)								
	Zahlungen	(5)								
• Aus der Dotation bestimmter spezifischer Programme finanzierte Verwaltungsausgaben INSGESAMT (alle operativen Rubriken)		(6)								
Mittel INSGESAMT unter RUBRIKEN 1 bis 6 des mehrjährigen Finanzrahmens (Referenzbetrag)	Verpflichtungen	=4+ 6								
	Zahlungen	=5+ 6								

Rubrik des Mehrjährigen Finanzrahmens	**7**	Verwaltungsausgaben

Zum Ausfüllen dieses Teils ist die „Tabelle für Verwaltungsausgaben“ zu verwenden, die zuerst in den Anhang des Finanzbogens zu Rechtsakten (Anhang V der Internen Vorschriften), der für die dienststellenübergreifende Konsultation in DECIDE hochgeladen wird, aufgenommen wird.

in Mio. EUR (3 Dezimalstellen)

		Jahr **2023**	Jahr **2024**	Jahr **2025**	Jahr **2026**	Jahr **2027**	**Nach 2027**[72]	**INSGESAMT**
GD: CNECT								
• Personal		0,760	0,760	0,760	0,760	0,760	0,760	**3,800**
• Sonstige Verwaltungsausgaben		**0,010**	**0,010**	**0,010**	**0,010**	**0,010**	**0,010**	**0,050**
GD CNECT INSGESAMT	**Mittel**	**0,760**	**0,760**	**0,760**	**0,760**	**0,760**	**0,760**	**3,850**
Europäischer Datenschutzbeauftragter								
• Personal		0,760	0,760	0,760	0,760	0,760	0,760	**3,800**
• Sonstige Verwaltungsausgaben								
GESAMT EDSB	**Mittel**	**0,760**	**0,760**	**0,760**	**0,760**	**0,760**	**0,760**	**3,800**
Mittel INSGESAMT unter der RUBRIK 7 des Mehrjährigen Finanzrahmens	(Verpflichtungen insges. = Zahlungen insges.)	1,530	1,530	1,530	1,530	1,530	1,530	**7,650**

in Mio. EUR (3 Dezimalstellen)

	Jahr **2022**	Jahr **2023**	Jahr **2024**	Jahr **2025**	Jahr **2026**	Jahr **2027**		**INSGESAMT**

[72] Alle Zahlen in dieser Spalte sind vorläufig und von der Fortführung der Programme und der Verfügbarkeit von Mitteln abhängig.

Mittel INSGESAMT unter RUBRIKEN 1 bis 7 des mehrjährigen Finanzrahmens	Verpflichtungen		2,770	1,770	1,770	1,770	1,770		**9,850**
	Zahlungen		2,370	1,870	1,870	1,870	1,870		**9,850**

3.2.2. Geschätzte Ergebnisse, die mit operativen Mitteln finanziert werden

Mittel für Verpflichtungen in Mio. EUR (3 Dezimalstellen)

Ziele und Ergebnisse angeben ⇩			Jahr **2022**		Jahr **2023**		Jahr **2024**		Jahr **2025**		Jahr **2026**		Jahr **2027**		Nach **2027**[73]		**INSGESAMT**	
	ERGEBNISSE																	
	Art	Durchschnittskosten	Anzahl	Kosten	Anzahl	Kosten	Anzahl	Kosten	Anzahl	Kosten	Anzahl	Kosten	Anzahl	Kosten	Anzahl	Kosten	Gesamtzahl	Gesamtkosten
EINZELZIEL Nr. 1[74]…																		
Datenbank					1	1,000	1		1		1		1		1	0,100	1	1,000
Sitzungsergebnisse					10	0,200	10	0,200	10	0,200	10	0,200	10	0,200	10	0,200	50	1,000
Kommunikations-maßnahmen					2	0,040	2	0,040	2	0,040	2	0,040	2	0,040	2	0,040	10	0,040
Zwischensumme für Einzelziel Nr. 1																		
EINZELZIEL Nr. 2 ...																		
- Ergebnis																		
Zwischensumme für Einzelziel Nr. 2																		
INSGESAMT					13	0,240	13	0,240	13	0,240	13	0,240	13	0,240	13	0,100	65	2,200

[73] Alle Zahlen in dieser Spalte sind vorläufig und von der Fortführung der Programme und der Verfügbarkeit von Mitteln abhängig.

[74] Wie unter 1.4.2. („Einzelziel(e)…“) beschrieben.

3.2.3. Übersicht über die geschätzten Auswirkungen auf die Verwaltungsmittel

– ☐ Für den Vorschlag/die Initiative werden keine Verwaltungsmittel benötigt.

– X Für den Vorschlag/die Initiative werden die folgenden Verwaltungsmittel benötigt:

in Mio. EUR (3 Dezimalstellen)

	Jahr **2022**	Jahr **2023**	Jahr **2024**	Jahr **2025**	Jahr **2026**	Jahr **2027**	**Jährlich nach 2027**[75]	**INSGESAMT**
RUBRIK 7 des mehrjährigen Finanzrahmens								
Personal		1,520	1,520	1,520	1,520	1,520	**1,520**	**7,600**
Sonstige Verwaltungsausgaben		0,010	0,010	0,010	0,010	0,010	**0,010**	**0,050**
Zwischensumme RUBRIK 7 des Mehrjährigen Finanzrahmens		1,530	1,530	1,530	1,530	1,530	**1,530**	**7,650**
Außerhalb der RUBRIK 7[76]**des mehrjährigen Finanzrahmens**								
Personal								
Sonstige Verwaltungsausgaben		0,240	0,240	0,240	0,240	0,240	**0,240**	**1,20**
Zwischensumme außerhalb der RUBRIK 7 des mehrjährigen Finanzrahmens		0,240	0,240	0,240	0,240	0,240	**0,240**	**1,20**
INSGESAMT		**1,770**	**1,770**	**1,770**	**1,770**	**1,770**	**1,770**	**8,850**

Der Mittelbedarf für Personal- und sonstige Verwaltungsausgaben wird durch der Verwaltung der Maßnahme zugeordnete Mittel der GD oder GD-interne Personalumschichtung gedeckt. Hinzu kommen etwaige zusätzliche Mittel, die der für die Verwaltung der Maßnahme zuständigen GD nach Maßgabe der verfügbaren Mittel im Rahmen der jährlichen Mittelzuweisung zugeteilt werden.

75 Alle Zahlen in dieser Spalte sind vorläufig und von der Fortführung der Programme und der Verfügbarkeit von Mitteln abhängig.

76 Technische und/oder administrative Hilfe und Ausgaben zur Unterstützung der Durchführung von Programmen bzw. Maßnahmen der EU (vormalige BA-Linien), indirekte Forschung, direkte Forschung.

3.2.3.1. Geschätzter Personalbedarf

– ☐ Für den Vorschlag/die Initiative wird kein Personal benötigt.

– X Für den Vorschlag/die Initiative wird folgendes Personal benötigt:

Schätzung in Vollzeitäquivalenten

		Jahr **2023**	Jahr **2024**	Jahr **2025**	**2026**	**2027**	**Nach 2027**[77]	
• Im Stellenplan vorgesehene Planstellen (Beamte und Bedienstete auf Zeit)								
20 01 02 01 (am Sitz und in den Vertretungen der Kommission)		10	10	10	10	10	10	
20 01 02 03 (in den Delegationen)								
01 01 01 01 (indirekte Forschung)								
01 01 01 11 (direkte Forschung)								
Sonstige Haushaltslinien (bitte angeben)								
• Externes Personal (in Vollzeitäquivalenten – VZÄ)[78]								
20 02 01 (VB, ANS und LAK der Globaldotation)								
20 02 03 (VB, ÖB, ANS, LAK und JFD in den Delegationen)								
XX 01 xx **yy zz**[79]	- am Sitz							
	- in den Delegationen							
01 01 01 02 (VB, ANS und LAK – indirekte Forschung)								
01 01 01 12 (VB, ANS und LAK – direkte Forschung)								
Sonstige Haushaltslinien (bitte angeben)								
INSGESAMT		**10**	**10**	**10**	**10**	**10**	**10**	

XX steht für den jeweiligen Politikbereich bzw. Haushaltstitel.

Der Personalbedarf wird durch der Verwaltung der Maßnahme zugeordnetes Personal der GD oder GD-interne Personalumschichtung gedeckt. Hinzu kommen etwaige zusätzliche Mittel, die der für die Verwaltung der Maßnahme zuständigen GD nach Maßgabe der verfügbaren Mittel im Rahmen der jährlichen Mittelzuweisung zugeteilt werden.

Der EDSB wird voraussichtlich die Hälfte der erforderlichen Ressourcen bereitstellen.

Beschreibung der auszuführenden Aufgaben:

Beamte und Zeitbedienstete	Zur Vorbereitung von insgesamt 13–16 Sitzungen, zum Entwurf von Berichten, zur Fortsetzung der politischen Arbeit, z. B. in Bezug auf künftige Änderungen der Liste der Hochrisiko-KI-Anwendungen, und zur Pflege der Beziehungen zu den Behörden der Mitgliedstaaten werden vier AD VZÄ und ein AST VZÄ erforderlich sein. Für KI-Systeme, die von den EU-Organen entwickelt werden, ist der Europäische Datenschutzbeauftragte zuständig. Auf der Grundlage der bisherigen Erfahrungen kann davon ausgegangen werden, dass für die Wahrnehmung der Aufgaben des EDSB im Rahmen des Gesetzesentwurfs fünf AD VZÄ benötigt werden.
Externes Personal	

[77] Alle Zahlen in dieser Spalte sind vorläufig und von der Fortführung der Programme und der Verfügbarkeit von Mitteln abhängig.

[78] VB = Vertragsbedienstete, ÖB = örtliche Bedienstete, ANS = abgeordnete nationale Sachverständige, LAK = Leiharbeitskräfte, JFD = Juniorfachkräfte in Delegationen.

[79] Teilobergrenze für aus operativen Mitteln finanziertes externes Personal (vormalige BA-Linien).

3.2.4. Vereinbarkeit mit dem Mehrjährigen Finanzrahmen

Der Vorschlag/Die Initiative

– X kann durch Umschichtungen innerhalb der entsprechenden Rubrik des Mehrjährigen Finanzrahmens (MFR) in voller Höhe finanziert werden.

Keine Anpassung erforderlich.

– ☐ erfordert die Inanspruchnahme des verbleibenden Spielraums unter der einschlägigen Rubrik des MFR und/oder den Einsatz der besonderen Instrumente im Sinne der MFR-Verordnung.

Bitte erläutern Sie den Bedarf unter Angabe der betreffenden Rubriken und Haushaltslinien, der entsprechenden Beträge und der vorgeschlagenen einzusetzenden Instrumente.

– ☐ erfordert eine Revision des MFR.

Bitte erläutern Sie den Bedarf unter Angabe der betreffenden Rubriken und Haushaltslinien sowie der entsprechenden Beträge.

3.2.5. Finanzierungsbeteiligung Dritter

Der Vorschlag/Die Initiative

– X sieht keine Kofinanzierung durch Dritte vor.

– ☐ sieht folgende Kofinanzierung durch Dritte vor:

Mittel in Mio. EUR (3 Dezimalstellen)

	Jahr **N**[80]	Jahr **N+1**	Jahr **N+2**	Jahr **N+3**	Bei länger andauernden Auswirkungen (siehe 1.6.) bitte weitere Spalten einfügen			Insgesamt
Kofinanzierende Einrichtung								
Kofinanzierung INSGESAMT								

[80] Das Jahr N ist das Jahr, in dem mit der Umsetzung des Vorschlags/der Initiative begonnen wird. Bitte ersetzen Sie „N“ durch das voraussichtlich erste Jahr der Umsetzung (z. B. 2021). Dasselbe gilt für die folgenden Jahre.

3.3. Geschätzte Auswirkungen auf die Einnahmen

– ☐ Der Vorschlag/Die Initiative wirkt sich auf die Einnahmen aus, und zwar:

– ☐ Der Vorschlag/Die Initiative wirkt sich auf die Einnahmen aus, und zwar:

  – ☐ auf die übrigen Einnahmen

  – ☐ auf die übrigen Einnahmen

  – Bitte geben Sie an, ob die Einnahmen bestimmten Ausgabenlinien zugewiesen sind. ☐

in Mio. EUR (3 Dezimalstellen)

Einnahmenlinie:	Für das laufende Haushaltsjahr zur Verfügung stehende Mittel	Auswirkungen des Vorschlags/der Initiative[81]						
		Jahr **N**	Jahr **N+1**	Jahr **N+2**	Jahr **N+3**	Bei länger andauernden Auswirkungen (siehe 1.6.) bitte weitere Spalten einfügen.		
Artikel ….								

Bitte geben Sie für die zweckgebundenen Einnahmen die betreffende(n) Ausgabenlinie(n) im Haushaltsplan an.

Sonstige Anmerkungen (bei der Ermittlung der Auswirkungen auf die Einnahmen verwendete Methode/Formel oder weitere Informationen).

[81] Bei den traditionellen Eigenmitteln (Zölle, Zuckerabgaben) sind die Beträge netto, d. h. abzüglich 20 % für Erhebungskosten, anzugeben.