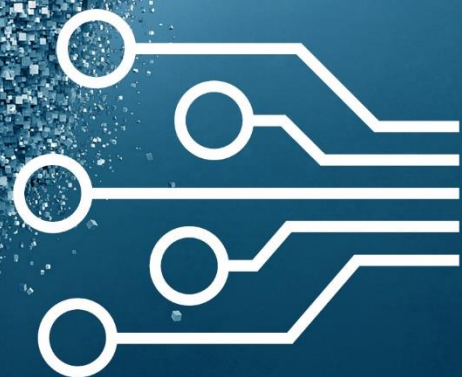


Konsolidierte Fassung der KI-Verordnung (EP-Vorschlag)

– ohne Änderungen –

Abänderungen des Europäischen Parlaments vom 14. Juni 2023 zu dem 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 (COM(2021)0206 – C9-0146/2021 – 2021/0106(COD))



Inhaltsverzeichnis

A. VORWORT	7
B. KI-VERORDNUNG	8
I. Begründung	8
II. Einleitung Verordnung.....	28
III. Erwägungsgründe	28
IV. Verordnung selbst.....	80
❖ Titel I	80
➤ Artikel 1 Gegenstand.....	80
➤ Artikel 2 Anwendungsbereich.....	81
➤ Artikel 3 Begriffsbestimmung	83
➤ Artikel 4a Allgemeine, für alle KI-Systeme geltende Grundsätze	89
➤ Artikel 4b KI-Kompetenz.....	91
❖ Titel II Verbotene Praktiken im Bereich der künstlichen Intelligenz.....	92
➤ Artikel 5.....	92
❖ Titel III Hochrisiko KI-Systeme.....	94
❖ Kapitel 1 Klassifizierung von KI-Systemen als Hochrisiko-Systeme.....	94
➤ Artikel 6 Klassifizierungsvorschriften für Hochrisiko-KI-Systeme... 	94
➤ Artikel 7 Änderungen des Anhangs III	95
❖ Kapitel 2 Anforderungen an Hochrisiko-KI-Systeme.....	97
➤ Artikel 8 Einhaltung der Anforderungen.....	97
➤ Artikel 9 Risikomanagementsystem.....	98
➤ Artikel 10 Daten und Daten-Governance	100
➤ Artikel 11 Technische Dokumentation	102
➤ Artikel 12 Aufzeichnungspflichten	103
➤ Artikel 13 Transparenz und Bereitstellung von Informationen	104
➤ Artikel 14 Menschliche Aufsicht	106
➤ Artikel 15 Genauigkeit, Robustheit und Cybersicherheit	107
❖ Kapitel 3 Pflichten der Anbieter und Betreiber von Hochrisiko-KI-Systemen und anderer Beteiligter	108
➤ Artikel 16 Pflichten der Anbieter und Betreiber von Hochrisiko-KI-Systemen und anderer Beteiligter	108
➤ Artikel 17 Qualitätsmanagementsystem	110
➤ Artikel 20 Automatisch erzeugte Protokolle.....	111
➤ Artikel 21 Korrekturmaßnahmen.....	111
➤ Artikel 22 Informationspflicht.....	112

➤ Artikel 23 Zusammenarbeit mit den zuständigen Behörden, dem Amt für künstliche Intelligenz und der Kommission	112
➤ Artikel 24 Pflichten der Produkthersteller	113
➤ Artikel 25 Bevollmächtigte	113
➤ Artikel 26 Pflichten der Einführer	114
➤ Artikel 27 Pflichten der Händler	115
➤ Artikel 28 Verantwortlichkeiten entlang der KI-Wertschöpfungskette der Anbieter, Händler, Einführer, Betreiber oder anderer Drittparteien	116
➤ Artikel 28a Missbräuchliche Vertragsklauseln, die einem KMU oder einem Startup einseitig auferlegt werden.....	117
➤ Artikel 28b Pflichten des Anbieters eines Basismodells.....	119
➤ Artikel 29 Pflichten der Nutzer von Hochrisiko-KI-Systemen.....	120
➤ Artikel 29a Folgenabschätzung im Hinblick auf die Grundrechte für Hochrisiko-KI-Systeme	123
❖ Kapitel 4 Notifizierende Behörden und notifizierte Stellen	124
➤ Artikel 30 Notifizierende Behörden.....	124
➤ Artikel 31 Antrag einer Konformitätsbewertungsstelle auf Notifizierung.....	125
➤ Artikel 32 Notifizierungsverfahren.....	126
➤ Artikel 33 Notifizierte Stellen.....	126
➤ Artikel 34 Zweigstellen notifizierter Stellen und Vergabe von Unteraufträgen durch notifizierte Stellen	128
➤ Artikel 35 Kennnummern und Verzeichnisse notifizierter Stellen ..	129
➤ Artikel 36 Änderungen der Notifizierungen	129
➤ Artikel 37 Anfechtungen der Kompetenz notifizierter Stellen	130
➤ Artikel 38 Koordinierung der notifizierten Stellen	130
➤ Artikel 39 Konformitätsbewertungsstellen in Drittländern	130
❖ Kapitel 5 Normen, Konformitätsbewertung, Bescheinigungen, Registrierung.....	131
➤ Artikel 40 Harmonisierte Normen	131
➤ Artikel 41 Gemeinsame Spezifikationen	131
➤ Artikel 42 Vermutung der Konformität mit gewissen Anforderungen	133
➤ Artikel 43 Konformitätsbewertung.....	133
➤ Artikel 44 Bescheinigungen	136
➤ Artikel 45 Einspruch gegen Entscheidungen notifizierter Stellen..	136

➤ Artikel 46 Meldepflichten der notifizierten Stellen.....	136
➤ Artikel 47 Ausnahme vom Konformitätsbewertungsverfahren.....	137
➤ Artikel 48 EU-Konformitätserklärung	138
➤ Artikel 49 CE-Konformitätskennzeichnung	139
➤ Artikel 50 Aufbewahrung von Unterlagen.....	140
➤ Artikel 51 Registrierung	140
❖ Titel IV Transparenzpflichten	141
➤ Artikel 52 Transparenzpflichten.....	141
❖ Titel V Maßnahmen zur Innovationsförderung	142
➤ Artikel 53 KI-Reallabore	142
➤ Artikel 53a Modalitäten und Funktionsweise von KI-Reallaboren ..	145
➤ Artikel 54 Weiterverarbeitung von Daten zur Entwicklung bestimmter KI-Systeme im öffentlichen Interesse im KI-Reallabor	146
➤ Artikel 54a Förderung der KI-Forschung und -Entwicklung zur Unterstützung sozial und ökologisch vorteilhafter Resultate.....	148
➤ Artikel 55 Maßnahmen für KMU, Start-up-Unternehmen und Nutzer	148
❖ Titel VI Leistungsstruktur	149
❖ Kapitel 1 Europäischer Ausschuss für Künstliche Intelligenz	149
❖ Abschnitt 1 Allgemeine Bestimmungen über das Europäische Amt für künstliche Intelligenz.....	149
➤ Artikel 56 Einrichtung des Europäischen Amts für künstliche Intelligenz	149
➤ Artikel 56a Struktur	150
➤ Artikel 56b Aufgaben des Amts für künstliche Intelligenz	150
➤ Artikel 56c Rechenschaftspflicht, Unabhängigkeit und Transparenz	153
➤ Abschnitt 2 Sekretariat	153
➤ Artikel 57 Sekretariat.....	153
➤ Abschnitt 3 Verwaltungsrat.....	154
➤ Artikel 57a Zusammensetzung des Verwaltungsrats.....	154
➤ Artikel 57b Aufgaben des Verwaltungsrats.....	155
➤ Artikel 57c Vorsitz des Verwaltungsrats.....	155
➤ Abschnitt 4 Beirat.....	155
➤ Artikel 58 Beirat	155
➤ Abschnitt 5 Europäische Benchmarking-Behörden.....	157
➤ Artikel 58a Benchmarking	157
❖ Kapitel 2 Zuständige nationale Behörden	157

➤	Artikel 59 Benennung der nationalen Aufsichtsbehörden	157
➤	Artikel 59a Mechanismus für die Zusammenarbeit zwischen nationalen Aufsichtsbehörden in Fällen, in denen zwei oder mehr Mitgliedstaaten betroffen sind	159
❖	Titel VII EU-Datenbank für Hochrisiko-KI-Systeme.....	159
➤	Artikel 60 EU-Datenbank für Hochrisiko-KI-Systeme.....	159
❖	Titel VIII Beobachtung nach dem Inverkehrbringen, Informationsaustausch, Marktüberwachung	160
❖	Kapitel 1 Beobachtung nach dem Inverkehrbringen.....	160
➤	Artikel 61 Beobachtung nach dem Inverkehrbringen durch die Anbieter und Plan für die Beobachtung nach dem Inverkehrbringen für Hochrisiko-KI-Systeme	160
❖	Kapitel 2 Austausch von Informationen über Vorfälle und Fehlfunktionen	161
➤	Artikel 62 Meldung schwerwiegender Vorfälle.....	161
❖	Kapitel 3 Durchsetzung	162
➤	Artikel 63 Marktüberwachung und Kontrolle von KI-Systemen auf dem Unionsmarkt.....	162
➤	Artikel 64 Zugang zu Daten und zur Dokumentation.....	163
➤	Artikel 65 Verfahren für den Umgang mit KI-Systemen, die ein Risiko auf nationaler Ebene bergen	164
➤	Artikel 66 Schutzklauselverfahren der Union.....	167
➤	Artikel 66a Gemeinsame Untersuchungen.....	167
➤	Artikel 67 Konforme KI-Systeme, die ein Risiko bergen.....	168
➤	Artikel 68 Formale Nichtkonformität	169
❖	Kapitel 3A Rechtsbehelfe	169
➤	Artikel 68a Recht auf Beschwerde bei einer nationalen Aufsichtsbehörde	169
➤	Artikel 68b Recht auf einen wirksamen gerichtlichen Rechtsbehelf gegen eine nationale Aufsichtsbehörde	170
➤	Artikel 68c Das Recht auf Erläuterung der individuellen Entscheidungsfindung.....	170
➤	Artikel 68d Änderung der Richtlinie (EU) 2020/1828	171
➤	Artikel 68e Meldung von Verstößen und Schutz von Hinweisgebern	171
❖	Titel IX Verhaltenskodizes	171
➤	Artikel 69 Verhaltenskodizes.....	171
❖	Titel X Vertraulichkeit und Sanktionen.....	173

➤ Artikel 70 Vertraulichkeit	173
➤ Artikel 71 Sanktionen	174
➤ Artikel 72 Verhängung von Geldbußen gegen Organe, Einrichtungen und sonstige Stellen der Union	176
❖ Titel XI Befugnisübertragung und Ausschussverfahren.....	178
➤ Artikel 73 Ausübung der Befugnisübertragung.....	178
➤ Artikel 75 Ausschussverfahren.....	179
❖ Titel XII Schlussbestimmungen	179
➤ Artikel 75 Änderung der Verordnung (EU) Nr. 300/2008	179
➤ Artikel 76 Änderung der Verordnung (EU) Nr. 167/2013	179
➤ Artikel 77 Änderung der Verordnung (EU) Nr. 168/2013	180
➤ Artikel 78 Änderung der Richtlinie 2014/90/EU	180
➤ Artikel 79 Änderung der Richtlinie (EU) 2016/797.....	180
➤ Artikel 80 Änderung der Verordnung (EU) Nr. 2018/858	180
➤ Artikel 81 Änderung der Verordnung (EU) 2018/1139	181
➤ Artikel 81a Änderung der Verordnung (EU) 2019/1020	182
➤ Artikel 82 Änderung der Verordnung (EU) Nr. 2019/2144	182
➤ Artikel 82a Bessere Rechtsetzung.....	182
➤ Artikel 82b Leitlinien der Kommission zur Durchführung dieser Verordnung	183
➤ Artikel 83 Bereits in Verkehr gebrachte oder in Betrieb genommene KI-Systeme	183
➤ Artikel 84 Bewertung und Überarbeitung	184
➤ Artikel 85 Inkrafttreten und Geltungsbeginn	186
V. Finanzbogen zu Rechtsakten	188
VI. Finanzbogen zu Rechtsakten	190
C. ANHÄNGE	210
❖ Anhang II.....	211
❖ Anhang III.....	215
❖ Anhang IV	219
❖ Anhang V	222
❖ Anhang VI	223
❖ Anhang VII	224
❖ Anhang VIII	228
❖ Anhang IX	231

A. VORWORT

Die rasanten Fortschritte künstlicher Intelligenz (KI) haben zweifellos das Potenzial, unser tägliches Leben und die Art und Weise, wie wir Technologie nutzen, zu revolutionieren. Von der Automatisierung bis hin zu personalisierten Empfehlungen hat KI bereits Einzug in verschiedene Lebensbereiche gehalten, und wird es weiter tun.

Der „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“ dürfte weitreichende Auswirkungen auf die Nutzung und Regulierung dieser Technologie haben. Nachdem das Europäische Parlament einen eigenen Vorschlag der von der Europäischen Kommission im April 2021 vorgeschlagenen KI-Verordnung einschließlich ihrer Anhänge am 14. Juni 2023 mit zahlreichen Änderungen angenommen hat,¹ soll nun im Trilog eine endgültige Fassung erarbeitet werden. Bis zu deren Finalisierung soll die vorliegende konsolidierte Version der Vorschläge des Europäischen Parlaments und der Europäischen Kommission einen kompakten Überblick über den aktuellen Stand der KI-Verordnung nach Vorstellung des Europäischen Parlaments geben.

Wir haben zwei Varianten erstellt: eine ohne und eine mit sichtbaren Änderungen. Vorliegend handelt es sich um die Variante ohne sichtbare Änderungen. Hier wurden sämtliche Änderungen des Europäischen Parlaments in den Text der Kommission integriert. Gestrichene Erwägungsgründe haben wir gänzlich aus dem Text entfernt. Seitens des Parlaments wurden noch nicht alle Teile neu nummeriert, so erklären sich kleinere Unregelmäßigkeiten (beispielsweise wurde Anhang I gestrichen, trotzdem beginnen die Anhänge mit Anhang II).



Fritz-Ulli Pieper
Technology, Media &
Telecoms
Salary Partner
+49 211 8387-240
f.pieper@taylorwessing.com



Rebecca Kehrl
Technology, Media &
Telecoms
Wissenschaftliche Mitarbeiterin



Raphaëla Pavlidou
Technology, Media &
Telecoms
Praktikantin

¹ https://www.europarl.europa.eu/doceo/document/TA-9-2023-0236_DE.html

B. KI-VERORDNUNG

I. BEGRÜNDUNG

1. KONTEXT DES VORSCHLAG

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 Dienstleistung 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“² – 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 Vertrauen³. 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

² https://ec.europa.eu/commission/sites/beta-political/files/political-guidelines-next-commission_de.pdf

³ Weißbuch zur künstlichen Intelligenz – Ein europäisches Konzept für Exzellenz und Vertrauen, COM(2020) 65 final, 2020.

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 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 Rat⁴ 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 Parlament⁵ 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“⁶. In seinen Schlussfolgerungen von 2019 zu dem koordinierten Plan für künstliche Intelligenz „Made in Europe“⁷ 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 sollten⁸.

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 erleichtern⁹.

⁴ Europäischer Rat, [Außerordentliche Tagung des Europäischen Rates \(1. und 2. Oktober 2020\) – Schlussfolgerungen](#), EUCO 13/20, 2020, S. 6.

⁵ 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).

⁶ Europäischer Rat, [Tagung des Europäischen Rates \(19. Oktober 2017\) – Schlussfolgerung](#), EUCO 14/17, 2017, S. 7.

⁷ Rat der Europäischen Union, [Künstliche Intelligenz b\) Schlussfolgerungen zu dem koordinierten Plan für künstliche Intelligenz – Annahme](#), 6177/19, 2019.

⁸ Europäischer Rat, [Außerordentliche Tagung des Europäischen Rates \(1. und 2. Oktober 2020\) – Schlussfolgerungen](#), EUCO 13/20, 2020.

⁹ Rat der Europäischen Union, [Schlussfolgerungen des Vorsitzes – Die Charta der Grundrechte im Zusammenhang mit künstlicher Intelligenz und dem digitalen Wandel](#), 11481/20, 2020.

Auch das Europäische Parlament hat sich intensiv mit dem Thema der KI befasst. Im Oktober 2020 nahm es eine Reihe von Entschlüssen zur KI an, u. a. zur Ethik¹⁰, zivilrechtlichen Haftung¹¹ und zum Urheberrecht¹². 2021 folgten weitere Entschlüsse zur KI im Strafrecht¹³ sowie in der Bildung, der Kultur und im audiovisuellen Bereich¹⁴. In seiner Entschlüsselung 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 Entschlüsselung 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 Entschlüsselung des Europäischen Parlaments unter uneingeschränkter Wahrung der Grundsätze der Verhältnismäßigkeit, Subsidiarität und besserer 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 Entschlüsse 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

¹⁰ Entschlüsselung 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 \(INL\)](#).

¹¹ Entschlüsselung des Europäischen Parlaments vom 20. Oktober 2020 mit Empfehlungen an die Kommission für eine Regelung der zivilrechtlichen Haftung beim Einsatz künstlicher Intelligenz, [2020/2014 \(INL\)](#).

¹² Entschlüsselung des Europäischen Parlaments vom 20. Oktober 2020 zu den Rechten des geistigen Eigentums bei der Entwicklung von KI-Technologien, [2020/2015 \(INI\)](#).

¹³ Europäisches Parlament – Berichtsentwurf über künstliche Intelligenz im Strafrecht und ihre Verwendung durch die Polizei und Justizbehörden in Strafsachen, [2020/2016 \(INI\)](#).

¹⁴ 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.

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 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 Wertpapierfirmen¹⁵ einzuhalten sind.

Zudem steht der Vorschlag in Einklang mit dem geltenden EU-Dienstleistungsrecht, unter das auch die in der E-Commerce-Richtlinie 2000/31/EG¹⁶ regulierten Vermittlungsdienste und der jüngste Kommissionsvorschlag für das Gesetz über digitale Dienste¹⁷ 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 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 werden¹⁸. 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**¹⁹.

¹⁵ 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).

¹⁶ 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).

¹⁷ 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.

¹⁸ Mitteilung der Kommission „Gestaltung der digitalen Zukunft Europas“, COM(2020) 67.

¹⁹ [Digitaler Kompass 2030: der europäische Weg in die digitale Dekade](#).

Darüber hinaus ist die Förderung der auf KI beruhenden Innovation eng mit dem **Daten-Governance-Gesetz**²⁰, der **Richtlinie über offene Daten**²¹ und anderen Initiativen im Rahmen der **EU-Strategie für Daten**²² 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 VERHÄLTNISSÄSSIGKEIT

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.

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.

²⁰ Vorschlag für eine Verordnung über europäische Daten-Governance (Data-Governance-Gesetz), [COM\(2020\) 767](#).

²¹ 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).

²² Mitteilung der Kommission „Eine europäische Datenstrategie“, COM(2020) 66 final.

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 Website²³ 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 Kleinunternehmen 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

²³ [Alle Ergebnisse der Konsultation finden Sie hier.](#)

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 währenden 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 befürworteten 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 Umsetzung der Strategie für Künstliche Intelligenz zu beraten. Im April 2019 unterstützte die Kommission²⁴ die zentralen Anforderungen, die die hochrangige Expertengruppe in ihre Ethik-Leitlinien für vertrauenswürdige KI²⁵ 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

²⁴ Europäische Kommission, [Schaffung von Vertrauen in eine auf den Menschen ausgerichtete künstliche Intelligenz](#), COM(2019) 168.

²⁵ HLEG, [Ethics Guidelines for Trustworthy AI](#), 2019.

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*)²⁶ erstellt.

Zudem wurde eine **KI-Allianz**²⁷ 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 eingingen²⁸. 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 unterstützen²⁹. 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**.

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

- **Option 1:** EU-Rechtsetzungsinstrument zur Einrichtung eines Systems zur freiwilligen Kennzeichnung;

²⁶ HLEG, [Assessment List for Trustworthy Artificial Intelligence \(ALTAI\) for self-assessment](#), 2020.

²⁷ Die KI-Allianz, ein Forum unterschiedlichster Interessenträger, wurde 2018 gegründet: <https://ec.europa.eu/digital-single-market/en/european-ai-alliance>.

²⁸ 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](#).

²⁹ Einzelheiten aller durchgeführten Konsultationen sind Anhang 2 der Folgenabschätzung zu entnehmen.

- **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 unterschweligen 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 Organisationen³⁰ erprobten Ethik-Leitlinien der HEG³¹ 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

³⁰ Sie wurden auch von der Kommission in ihrer Mitteilung aus dem Jahr 2019 zu einem auf den Menschen ausgerichteten Ansatz für KI gebilligt.

³¹ Hochrangige Expertengruppe für künstliche Intelligenz, [Ethics Guidelines for Trustworthy AI \(Ethik-Leitlinien für eine vertrauenswürdige KI\)](#), 2019.

einzuhaltenden Konformitätsbewertungsverfahren im Einzelnen erläutert werden. Mit dem Konzept der Konformitätsbewertung sollen die Belastungen für die Wirtschaftsakteure und notifizierte 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 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 Verfahrensweisen 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.

II. EINLEITUNG VERORDNUNG

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 Sozialausschusses³²,

nach Stellungnahme des Ausschusses der Regionen³³,

unter Hinweis auf die Stellungnahme der Europäischen Zentralbank,

unter Hinweis auf die gemeinsame Stellungnahme des Europäischen Datenschutzausschusses und des Europäischen Datenschutzbeauftragten,

gemäß dem ordentlichen Gesetzgebungsverfahren,

in Erwägung nachstehender Gründe:

III. ERWÄGUNGSRÜNDE

(1) Zweck dieser Verordnung ist es, die Einführung von menschenzentrierter und vertrauenswürdiger künstlicher Intelligenz zu fördern und ein hohes Maß an Schutz der

³² ABl. C [...] vom [...], S. [...].

³³ ABl. C [...] vom [...], S. [...].

Gesundheit, der Sicherheit, der Grundrechte, der Demokratie und der Rechtsstaatlichkeit sowie der Umwelt vor schädlichen Auswirkungen von Systemen der künstlichen Intelligenz in der Union sicherzustellen und gleichzeitig die Innovation zu fördern und das Funktionieren des Binnenmarktes zu verbessern. Diese Verordnung legt einen einheitlichen Rechtsrahmen insbesondere für die Entwicklung, das Inverkehrbringen, die Inbetriebnahme und Verwendung künstlicher Intelligenz im Einklang mit den Werten der Union fest und gewährleistet den grenzüberschreitenden freien Verkehr KI-gestützter Waren und Dienstleistungen, wodurch verhindert wird, dass die Mitgliedstaaten die Entwicklung, Vermarktung und Verwendung von Systemen künstlicher Intelligenz (KI-Systemen) beschränken, sofern dies nicht ausdrücklich durch diese Verordnung erlaubt wird. Bestimmte KI-Systeme können auch Auswirkungen auf die Demokratie und Rechtsstaatlichkeit sowie die Umwelt haben. Diese Bedenken werden in den kritischen Sektoren speziell angegangen und in den Anhängen dieser Verordnung sind Anwendungsfälle aufgeführt.

- (1a) Diese Verordnung soll die Werte der Union wahren, dazu beitragen, dass die mit der KI verbundenen Vorteile der gesamten Gesellschaft zugutekommen, Einzelpersonen, Unternehmen, Demokratie und Rechtsstaatlichkeit sowie die Umwelt vor Risiken schützen und zugleich Innovation und Beschäftigung fördern und der Union eine Führungsrolle in diesem Bereich verschaffen.
- (2) 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 vertrauenswürdig und 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, um eine vertrauenswürdige KI zu erreichen, wobei Unterschiede, die den freien Verkehr, Innovationen, den Einsatz und die Verbreitung 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 der Rechte von Personen im gesamten Binnenmarkt auf der Grundlage des Artikels 114 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV) gewährleistet wird.
- (2a) Da künstliche Intelligenz oft auf die Verarbeitung großer Datenmengen angewiesen ist und viele KI-Systeme und -Anwendungen auf der Verarbeitung personenbezogener Daten beruhen, sollte sich diese Verordnung auch auf Artikel 16 AEUV stützen, in dem das Recht auf den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten verankert ist und der den Erlass von Vorschriften zum Schutz von Privatpersonen im Hinblick auf die Verarbeitung personenbezogener Daten vorsieht.

- (2b) Das Grundrecht auf Schutz personenbezogener Daten wird insbesondere durch die Verordnungen (EU) 2016/679 und (EU) 2018/1725 und die Richtlinie (EU) 2016/680 gewahrt. Die Richtlinie 2002/58/EG schützt darüber hinaus die Privatsphäre und die Vertraulichkeit der Kommunikation und enthält Bedingungen für die Speicherung personenbezogener und nicht personenbezogener Daten auf Endgeräten und den Zugang dazu. Diese Rechtsakte bieten die Grundlage für eine nachhaltige und verantwortungsvolle Datenverarbeitung, auch wenn Datensätze eine Mischung aus personenbezogenen und nicht personenbezogenen Daten enthalten. Die Verordnung soll die Anwendung des bestehenden Unionsrechts zur Verarbeitung personenbezogener Daten, einschließlich der Aufgaben und Befugnisse der unabhängigen Aufsichtsbehörden, die für die Überwachung der Einhaltung dieser Instrumente zuständig sind, nicht berühren. Die Grundrechte auf Privatleben und den Schutz personenbezogener Daten, wie sie im Unionsrecht zum Datenschutz und zur Privatsphäre vorgesehen und in der Charta der Grundrechte der Europäischen Union (die „Charta“) verankert sind, werden von der Verordnung nicht berührt.
- (2c) Systeme der künstlichen Intelligenz unterliegen in der Union den einschlägigen Rechtsvorschriften zur Produktsicherheit, durch die ein Rahmen bereitgestellt wird, durch den Verbraucher vor gefährlichen Produkten im Allgemeinen geschützt werden, wobei solche Rechtsvorschriften weiterhin gelten sollten. Diese Verordnung lässt die Vorschriften, die in anderen Rechtsakten der Union zur Regelung des Verbraucherschutzes und der Produktsicherheit festgelegt sind, insbesondere in der Verordnung (EU) 2017/2394, der Verordnung (EU) 2019/1020 und der Richtlinie 2001/95/EG über die allgemeine Produktsicherheit sowie der Richtlinie 2013/11/EU, unberührt.
- (2d) In Übereinstimmung mit Artikel 114 Absatz 2 AEUV dient diese Verordnung als Ergänzung und sollte nicht die Rechte und Interessen von Arbeitnehmern beeinträchtigen. Diese Verordnung sollte daher nicht das Unionsrecht im Bereich der Sozialpolitik und die nationalen Arbeitsrechtsvorschriften und -gepflogenheiten berühren, d. h. jegliche gesetzlichen und vertraglichen Vorschriften über Beschäftigungs- und Arbeitsbedingungen, einschließlich der Gesundheit und Sicherheit am Arbeitsplatz sowie der Beziehung zwischen Arbeitgeber und Arbeitnehmer, einschließlich Unterrichtung, Anhörung und Beteiligung. Diese Verordnung sollte die Ausübung der in den Mitgliedstaaten und auf Unionsebene anerkannten Grundrechte, einschließlich des Rechts oder der Freiheit zum Streik oder zur Durchführung anderer Maßnahmen, die im Rahmen der spezifischen Systeme der Mitgliedstaaten im Bereich der Arbeitsbeziehungen nach ihren nationalen Rechtsvorschriften und/oder Gepflogenheiten vorgesehen sind, nicht beeinträchtigen. Sie sollte auch nicht die Konzertierungspraktiken und das Recht berühren, im Einklang mit den nationalen Rechtsvorschriften und/oder Gepflogenheiten Tarifverträge auszuhandeln, abzuschließen und durchzusetzen oder kollektive Maßnahmen zu ergreifen. Keinesfalls sollte sie die Kommission daran hindern, spezifische Rechtsvorschriften zu den Rechten und Freiheiten der Beschäftigten, die von KI-Systemen betroffen sind, vorzuschlagen.

- (2e) Diese Verordnung sollte die in der Richtlinie ... [COD 2021/414/EG] zur Verbesserung der Arbeitsbedingungen in der Plattformarbeit enthaltenen Bestimmungen nicht berühren.
- (2f) Diese Verordnung sollte dazu beitragen, Forschung und Innovation zu unterstützen, und sollte Forschungs- und Entwicklungstätigkeiten nicht beeinträchtigen und die Freiheit der wissenschaftlichen Forschung wahren. Daher müssen KI-Systeme, die eigens für den alleinigen Zweck der wissenschaftlichen Forschung und Entwicklung entwickelt werden, vom Anwendungsbereich der Verordnung ausgenommen werden, und es muss sichergestellt werden, dass sich die Verordnung nicht anderweitig auf wissenschaftliche Aktivitäten zur Forschung und Entwicklung in Bezug auf KI-Systeme auswirkt. In jedem Fall sollten jegliche Forschungs- und Entwicklungsaktivitäten in Übereinstimmung mit der Charta der Menschenrechte, dem Unionsrecht sowie den nationalen Rechtsvorschriften ausgeführt werden.
- (3) Künstliche Intelligenz bezeichnet eine Reihe von Technologien, die sich rasant entwickeln und zu vielfältigem Nutzen für Wirtschaft, Umwelt und Gesellschaft über das gesamte Spektrum industrieller und gesellschaftlicher Aktivitäten hinweg beitragen können – und dies bereits tun –, wenn sie in Übereinstimmung mit den relevanten allgemeinen Grundsätzen entwickelt werden, die der Charta und den Werten, auf denen die Union beruht, entsprechen. 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, Lebensmittelsicherheit, allgemeine und berufliche Bildung, Medien, Sport, Kultur, Infrastrukturmanagement, Energie, Verkehr und Logistik, Krisenmanagement, öffentliche Dienstleistungen, Sicherheit, Justiz, Ressourcen- und Energieeffizienz, Umweltüberwachung, die Bewahrung und Wiederherstellung der Biodiversität und der Ökosysteme sowie Klimaschutz und Anpassung an den Klimawandel
- (3a) Um dazu beizutragen, die Klimaneutralitätsziele zu erreichen, sollten europäische Unternehmen versuchen, alle verfügbaren technologischen Fortschritte zu nutzen, die hierbei hilfreich sein können. Künstliche Intelligenz ist eine Technologie, die eingesetzt werden kann, um die stets wachsende Datenmenge zu verarbeiten, die bei den Abläufen in Bereichen wie Wirtschaft, Umwelt und Gesundheit entsteht. Um Investitionen in Analyse- und Optimierungsinstrumente auf KI-Basis zu erleichtern, sollte diese Verordnung eine vorhersagbare und angemessene Umgebung für industrielle Lösungen mit geringem Risiko bereitstellen.
- (4) Gleichzeitig kann künstliche Intelligenz je nach den Umständen ihrer konkreten Anwendung und Nutzung sowie der technologischen Entwicklungsstufe Risiken mit sich bringen und öffentliche oder private Interessen und grundlegende Rechte natürlicher Personen schädigen, die durch

das Unionsrecht geschützt sind. Ein solcher Schaden kann materieller oder immaterieller Art sein, einschließlich physischer, psychischer, gesellschaftlicher oder wirtschaftlicher Schäden.

- (4a) Angesichts der großen Auswirkungen, die künstliche Intelligenz auf die Gesellschaft haben kann, und der Notwendigkeit, Vertrauen aufzubauen, ist es von entscheidender Bedeutung, dass die künstliche Intelligenz und ihr Regulierungsrahmen im Einklang mit den in Artikel 2 EUV verankerten Werten der Union und den in den Verträgen, der Charta und den internationalen Menschenrechtsnormen verankerten Grundrechten und -freiheiten entwickelt werden. Als Voraussetzung sollte künstliche Intelligenz eine menschenzentrierte Technologie sein. Sie soll weder die menschliche Autonomie ersetzen noch den Verlust individueller Freiheit voraussetzen und in erster Linie den Bedürfnissen der Gesellschaft und dem Gemeinwohl dienen. Um die Entwicklung und Nutzung ethisch eingebetteter künstlicher Intelligenz sicherzustellen, die die Werte der Union und die Charta achtet, sollten Garantien vorgesehen werden.
- (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, der Demokratie, der Rechtsstaatlichkeit, der Umwelt, der Gesundheit und Sicherheit zu gewährleisten. Zur Umsetzung dieses Ziels sollten Vorschriften für das Inverkehrbringen und die Inbetriebnahme und die Verwendung 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. Diese Regeln sollten klar und robust sein, um die Grundrechte zu schützen, neue innovative Lösungen zu unterstützen und ein europäisches Ökosystem öffentlicher und privater Akteure zu ermöglichen, die KI-Systeme im Einklang mit den Werten der Union entwickeln. Durch die Festlegung dieser Vorschriften sowie durch Maßnahmen zur Unterstützung der Innovation mit besonderem Augenmerk auf KMU und Start-up-Unternehmen unterstützt die Verordnung das vom Europäischen Rat³⁴ formulierte Ziel der Union, in Europa hergestellte KI zu fördern und bei der Entwicklung einer sicheren, vertrauenswürdigen und ethisch vertretbaren künstlichen Intelligenz weltweit eine Führungsrolle einzunehmen, und sorgt für den vom Europäischen Parlament³⁵ ausdrücklich geforderten Schutz von Ethikgrundsätzen.
- (5a) Darüber hinaus muss sich die Union – um die Entwicklung von KI-Systemen gemäß den Werten der Union zu fördern – den Hauptlücken und Hindernissen widmen, die das Potenzial des digitalen Wandels hemmen, wobei hier etwa der Mangel an in der Digitalisierung geschulten Arbeitskräften, Bedenken zur Internetsicherheit, zu wenige und zu geringer Zugang zu

³⁴ Europäischer Rat, Außerordentliche Tagung des Europäischen Rates (1. und 2. Oktober 2020) – Schlussfolgerungen, EUCO 13/20, 2020, S. 6.

³⁵ 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).

Investitionen sowie bestehende und potenzielle Lücken zwischen großen Unternehmen, KMU und Start-ups zu nennen sind. Dabei sollte besondere Aufmerksamkeit darauf gelegt werden, dass alle Regionen der Union von den Vorteilen der KI und von Innovationen in den neuen Technologien profitieren und dass ausreichende Investitionen und Ressourcen bereitgestellt werden, vor allem für Regionen, die in einigen Bereichen der Digitalisierung noch viel aufzuholen haben.

- (6) Der Begriff „KI-System“ in dieser Verordnung sollte klar definiert und eng mit der Tätigkeit internationaler Organisationen abgestimmt werden, die sich mit künstlicher Intelligenz befassen, um Rechtssicherheit, Harmonisierung und hohe Akzeptanz sicherzustellen und gleichzeitig genügend Flexibilität zu bieten, um künftigen, rapiden technologischen Entwicklungen in diesem Bereich Rechnung zu tragen. Darüber hinaus sollte die Begriffsbestimmung auf den wesentlichen Merkmalen der künstlichen Intelligenz wie ihren Lern-, Schlussfolgerungs- oder Modellierungsfähigkeiten beruhen und sie von einfacheren Softwaresystemen und Programmierungsansätzen abgrenzen. KI-Systeme sind mit verschiedenen Graden der Autonomie ausgestattet, was bedeutet, dass sie zumindest bis zu einem gewissen Grad unabhängig von menschlicher Kontrolle agieren und in der Lage sind, ohne menschliches Eingreifen zu arbeiten. Die Bezeichnung „maschinenbasiert“ bezieht sich auf die Tatsache, dass KI-Systeme von Maschinen betrieben werden. Durch die Bezugnahme auf explizite oder implizite Ziele wird betont, dass KI-Systeme gemäß expliziten – von Menschen festgelegten – Zielen oder gemäß impliziten Zielen arbeiten können. Die Ziele des KI-Systems können sich – unter bestimmten Umständen – von dem eigentlich vorgesehenen Verwendungszweck unterscheiden. Der Verweis auf Vorhersagen umfasst auch Inhalte, die in dieser Verordnung als eine Form von Vorhersage in Bezug auf eines der möglichen von einem KI-System generierten Ergebnisse hervorgebracht werden. Für die Zwecke dieser Verordnung sollten „Umgebungen“ als Kontexte verstanden werden, in denen KI-Systeme betrieben werden, während die von einem KI-System erzeugten Inhalte – also Vorhersagen, Empfehlungen oder Entscheidungen – auf der Grundlage von Eingaben aus dem genannten Umfeld als Reaktion auf die Ziele des Systems entstehen. Durch solche Ergebnisse wird das genannte Umfeld wiederum beeinflusst, auch dadurch, dass ihm neue Informationen zugeführt werden.
- (6a) KI-Systeme verfügen oft über Funktionen zum maschinellen Lernen, durch die es ihnen möglich ist, sich anzupassen und neue Aufgaben autonom auszuführen. Der Begriff „maschinelles Lernen“ bezieht sich auf den Rechenvorgang, bei dem die Parameter eines Modells auf der Grundlage von Daten optimiert werden, wobei es sich um ein mathematisches Konstrukt handelt, bei dem Ergebnisse auf der Grundlage von Eingabedaten erzeugt werden. Zu den Konzepten des maschinellen Lernens gehören z. B. beaufsichtigtes oder unbeaufsichtigtes und bestärkendes Lernen unter Verwendung einer Palette von Methoden, einschließlich des tiefen Lernens (Deep Learning) auf der Grundlage von neuronalen Netzwerken. Ziel dieser Verordnung ist es, bestimmte potenzielle Risiken anzugehen, die dadurch entstehen können, dass die Kontrolle über KI-Systeme übertragen wird, insbesondere wenn die Kontrolle auf KI-

Systeme übertragen wird, die sich nach der Einführung des Systems entwickeln. Die Funktionen und Ergebnisse vieler dieser KI-Systeme beruhen auf abstrakten mathematischen Beziehungen, die für Menschen schwer zu verstehen und zu überwachen sind bzw. schwer auf spezifische Eingaben zurückzuführen sind. Diese komplexen und undurchsichtigen Merkmale („Black-Box-Elemente“) haben Auswirkungen auf die Zurechenbarkeit und Erklärbarkeit. Vergleichsweise einfachere Techniken, wie zum Beispiel wissensgestützte Konzepte, Bayessche Schätzungen oder Entscheidungsbäume können auch zu Rechtslücken führen, die durch diese Verordnung angegangen werden müssen, insbesondere, wenn sie in Verbindung mit Konzepten des maschinellen Lernens in hybriden Systemen verwendet werden.

- (6b) KI-Systeme können als eigenständige Softwaresysteme verwendet werden, in ein physisches Produkt integriert (eingebettet) werden, der Funktion eines physischen Produkts dienen, ohne darin integriert zu sein (nicht eingebettet), oder als KI-Komponente eines größeren Systems verwendet werden. Wenn dieses größere System ohne die genannte KI-Komponente nicht funktionsfähig wäre, dann sollte das gesamte größere System im Rahmen dieser Verordnung als ein einziges KI-System angesehen werden.
- (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 Rates³⁶. „Biometrische Daten“ sind zusätzliche Daten, die sich aus der spezifischen technischen Verarbeitung physischer, physiologischer oder verhaltensbezogener Signale einer natürlichen Person ergeben, wie Gesichtsausdruck, Bewegungen, Pulsfrequenz, Stimme, Tastenanschlag oder Gang, die die eindeutige Identifizierung einer natürlichen Person ermöglichen oder bestätigen können.
- (7a) Der Begriff „biometrische Identifizierung“ sollte gemäß dieser Verordnung als automatische Erkennung physischer, physiologischer, verhaltensbezogener und psychischer menschlicher Merkmale wie Gesicht, Augenbewegungen, Gesichtsausdruck, Körperform, Stimme, Sprache, Gang, Haltung, Herzfrequenz, Blutdruck, Geruch, Tastenanschläge, psychologische Reaktionen (Wut, Kummer, Trauer usw.) zum Zweck der Überprüfung der Identität einer Person durch Abgleich der biometrischen Daten der entsprechenden Person mit den in einer Datenbank gespeicherten biometrischen Daten (1:n-Identifizierung) definiert werden, unabhängig davon, ob die Einzelperson ihre Zustimmung dazu gegeben hat oder nicht.
- (7b) Der Begriff „biometrische Kategorisierung“ im Sinne dieser Verordnung sollte die Zuordnung natürlicher Personen zu bestimmten Kategorien oder die Ableitung ihrer Merkmale und Attribute wie soziales Geschlecht, Geschlecht, Alter, Haarfarbe, Augenfarbe, Tätowierung, ethnische oder soziale Herkunft, Gesundheit, mentale oder körperliche Fähigkeiten, Persönlichkeits- oder Charaktermerkmale, Sprache, Religion oder Zugehörigkeit zu einer nationalen Minderheit oder sexuelle oder politische Ausrichtung auf der Grundlage ihrer biometrischen oder

³⁶

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).

biometriegestützten Daten oder von Daten, die aus diesen Daten abgeleitet werden können, bezeichnen.

- (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, mit Ausnahme von Verifizierungssystemen, die nur die biometrischen Daten einer Person mit den in Bezug auf diese Person zuvor gewonnenen biometrischen Daten (eindeutige Beziehung) vergleichen. 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. „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. Angesichts der Tatsache, dass das Konzept der biometrischen Identifizierung unabhängig von der Einwilligung einer Person ist, gilt diese Definition auch, wenn Warnmeldungen an dem Ort angebracht sind, der durch das biometrische Fernidentifizierungssystem überwacht wird, und ist durch die vorige Anmeldung nicht de facto ungültig.
- (8a) Bei der Identifizierung natürlicher Personen aus der Ferne wird zwischen biometrischen Fernidentifizierungssystemen und Systemen zur Überprüfung von Einzelpersonen aus der Nähe unterschieden, die biometrische Identifizierungsinstrumente verwenden und deren einziger Zweck darin besteht, zu bestätigen, ob eine bestimmte natürliche Person, die sich zur Identifizierung vorstellt, beispielsweise berechtigt ist oder nicht, Zugang zu einem Dienst, einem Gerät oder einem Gebäude zu erhalten.
- (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 und unabhängig von möglichen Kapazitätseinschränkungen. 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, Sportplätze, Schulen, Universitäten, relevante Gebäudebereiche von Krankenhäusern und Banken, Vergnügungsparks, Festivals, 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.

- (9a) Es ist wichtig, festzustellen, dass KI-Systeme so konzipiert sind, dass es ihnen möglich ist, allgemeine Grundsätze einzuhalten, mit denen ein auf den Menschen ausgerichteter Rahmen auf hoher Ebene geschaffen wird, der einen kohärenten, auf den Menschen ausgerichteten Ansatz für ethische und vertrauenswürdige KI im Einklang mit der Charta der Grundrechte der Europäischen Union und den Werten, auf denen die Union beruht, fördert, einschließlich des Schutzes der Grundrechte, der Handlungs- und Kontrollfähigkeit des Menschen, der technischen Robustheit und Sicherheit, des Schutzes der Privatsphäre und der Datenverwaltung, der Transparenz, der Nichtdiskriminierung und Fairness sowie des gesellschaftlichen und ökologischen Wohlergehens.
- (9b) Der Begriff „KI-Kompetenz“ bezieht sich auf Fähigkeiten, Kenntnisse und das Verständnis, die es Anbietern, Nutzern und Betroffenen unter Berücksichtigung ihrer jeweiligen Rechte und Pflichten im Rahmen dieser Verordnung ermöglichen, KI-Systeme in Kenntnis der Sachlage einzusetzen sowie sich der Chancen und Risiken von KI und möglicher Schäden, die sie verursachen kann, bewusst zu werden und dadurch ihre demokratische Kontrolle zu fördern. KI-Kompetenz sollte sich nicht auf das Lernen über Werkzeuge und Technologien beschränken, sondern auch darauf abzielen, Anbieter und Nutzer mit den Begriffen und Kompetenzen auszustatten, die erforderlich sind, um die Einhaltung und Durchsetzung dieser Verordnung sicherzustellen. Daher ist es notwendig, dass die Kommission, die Mitgliedstaaten sowie die Anbieter und Nutzer von KI-Systemen in Zusammenarbeit mit allen einschlägigen Interessenträgern die Entwicklung ausreichender KI-Kompetenzen bei Menschen aller Altersgruppen, einschließlich Frauen und Mädchen, in allen Bereichen der Gesellschaft fördern und dass die diesbezüglichen Fortschritte aufmerksam verfolgt werden.
- (10) Um gleiche Wettbewerbsbedingungen und einen wirksamen Schutz der Rechte und Freiheiten natürlicher Personen in der gesamten Union und auf internationaler Ebene 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 Betreiber von KI-Systemen, die in der Union ansässig oder niedergelassen sind, gelten. Damit die Union ihren Grundwerten treu bleibt, sollten KI-Systeme, die für Verfahren eingesetzt werden, die im Rahmen dieser Verordnung als unannehmbar angesehen werden, aufgrund ihrer besonders schädigenden Auswirkungen auf die in der Charta verankerten Grundrechte auch außerhalb der Union als unannehmbar gelten. Es ist daher angemessen, die Ausfuhr solcher KI-Systeme in Drittländer durch in der Union ansässige Betreiber zu verbieten.

- (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, Nutzer und Betreiber von KI-Systemen gelten, die in einem Drittland ansässig oder niedergelassen sind, soweit die von diesen Systemen erzeugten Ergebnisse für die Nutzung in der Union vorgesehen sind. 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. Diese Ausnahme sollte jedoch auf vertrauenswürdige Länder und internationale Organisationen beschränkt werden, die die Werte der Union teilen.
- (12) Diese Verordnung sollte auch für Organe, Einrichtungen und sonstige Stellen der Union gelten, wenn sie als Anbieter oder Betreiber 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.

- (12a) Software und Daten, die offen geteilt werden und die Nutzer kostenlos abrufen, nutzen, verändern und weiter verteilen können, auch in veränderter Form, können zu Forschung und Innovation auf dem Markt beitragen. Durch Forschungsprojekte der Kommission wurde auch gezeigt, dass freie und quelloffene Software im Umfang von 65 Mrd. bis 95 Mrd. EUR zum Bruttoinlandsprodukt der Europäischen Union beitragen kann und dass durch sie wesentliche Wachstumsmöglichkeiten für die europäische Wirtschaft geschaffen werden. Nutzer haben die Möglichkeit, Software und Daten zu nutzen, zu kopieren, zu verbreiten, Studien zu ihr/ihnen durchzuführen, sie zu ändern und zu verbessern, einschließlich Modellen im Rahmen von freien und quelloffenen Lizenzen. Um die Entwicklung und den Einsatz von KI zu fördern – insbesondere durch KMU, Start-ups, die wissenschaftliche Forschung und auch durch Einzelpersonen –, sollte diese Verordnung nicht für solche freien und quelloffenen KI-Komponenten gelten, es sei denn, sie werden von einem Anbieter als Teil eines Hochrisiko-KI-Systems oder eines KI-Systems, das unter Titel II oder IV dieser Verordnung fällt, in Verkehr gebracht oder in Betrieb genommen.
- (12b) Weder die gemeinsame Entwicklung von freien oder quelloffenen Softwarekomponenten noch ihr Verfügbarmachen auf offenen Portalen sollte ein Inverkehrbringen oder eine Inbetriebnahme darstellen. Eine gewerbliche Tätigkeit im Sinne der Bereitstellung auf dem Markt ist möglicherweise nicht nur dadurch gekennzeichnet, dass ein Entgelt verlangt wird, mit Ausnahme von Transaktionen zwischen Kleinstunternehmen für eine freie und quelloffene AI, sondern auch dadurch, dass für technische Unterstützungsleistungen ein Entgelt verlangt wird, dass eine Softwareplattform bereitgestellt wird, über die der Anbieter andere Dienste monetarisiert, oder dass personenbezogene Daten zu anderen Zwecken als der alleinigen Verbesserung der Sicherheit, Kompatibilität oder der Software verwendet werden.
- (12c) Die Entwickler von freien und quelloffenen KI-Komponenten sollten im Rahmen dieser Verordnung nicht verpflichtet werden, Anforderungen zu erfüllen, die auf die Produktwertschöpfungskette der KI und insbesondere auf den Anbieter abzielen, der freie und quelloffene KI-Softwarekomponenten verwendet hat. Die Entwickler von freien und quelloffenen KI-Komponenten sollten jedoch dazu angehalten werden, weit verbreitete Dokumentationsverfahren, wie z. B. Modell- und Datenkarten, als Mittel dazu einzusetzen, den Informationsaustausch entlang der KI-Wertschöpfungskette zu beschleunigen, sodass vertrauenswürdige KI-Systeme in der Union gefördert werden können.
- (13) Um einen einheitlichen und hohen Schutz öffentlicher Interessen im Hinblick auf die Gesundheit und Sicherheit sowie die Grundrechte, Demokratie, Rechtsstaatlichkeit und die Umwelt zu

gewährleisten, werden für alle Hochrisiko-KI-Systeme gemeinsame Normen vorgeschlagen. Diese Normen sollten mit der Charta dem europäischen Grünen Deal, der Gemeinsamen Erklärung zu den digitalen Rechten der Union und den Ethik-Leitlinien für vertrauenswürdige künstliche Intelligenz (KI) der hochrangigen Expertengruppe für künstliche Intelligenz 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 unannehmbare 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 missbräuchlich 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 das Ziel oder die Auswirkung haben, menschliches Verhalten maßgeblich nachteilig zu beeinflussen, und die zu physischen oder psychischen Schäden führen dürften, sollte verboten werden. Diese Einschränkung sollte so verstanden werden, dass sie Neurotechnologien einschließt, die von KI-Systemen unterstützt werden, die zur Überwachung, Nutzung oder Beeinflussung neuronaler Daten eingesetzt werden, die über Schnittstellen zwischen Gehirn und Computer gesammelt werden, da sie das Verhalten einer natürlichen Person auf eine Art maßgeblich beeinflussen, durch die wahrscheinlich dieser Person oder einer anderen Person wesentlicher Schaden zugefügt wird. Solche KI-Systeme setzen auf eine vom Einzelnen nicht zu erkennende unterschwellige Beeinflussung oder sollen die Schutzbedürftigkeit von Einzelpersonen und spezifischen Gruppen von Personen aufgrund ihrer bekannten oder vorhergesagten Persönlichkeitsmerkmale, ihres Alters oder ihrer körperlichen oder geistigen Behinderung oder ihrer sozialen oder wirtschaftlichen Situation ausnutzen. Dies geschieht mit der Absicht oder der Auswirkung, das Verhalten einer Person wesentlich zu beeinflussen, und zwar in einer Weise, die dieser oder einer anderen Person oder Gruppen von Personen wesentlichen Schaden zufügt oder zufügen kann, einschließlich Schäden, die sich im Laufe der Zeit akkumulieren. Diese Absicht, das Verhalten zu beeinflussen, 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, wie Faktoren, die nicht vernünftigerweise vorgesehen und vom Anbieter oder Betreiber des KI-Systems abgeschwächt werden können. In jedem Fall ist es nicht erforderlich, dass der Anbieter oder der Betreiber die Absicht haben, signifikanten Schaden zuzufügen, wenn dieser Schaden aufgrund von manipulativen oder ausbeuterischen KI-gestützten Praktiken entsteht. Die Verbote für solche KI-Praktiken ergänzen die Bestimmungen, die in Richtlinie 2005/29/EG enthalten sind und denen zufolge unlautere Geschäftspraktiken verboten sind – unabhängig davon, ob sie mit Rückgriff auf KI-Systeme oder auf andere Weise durchgeführt werden. In solchen Kontexten sollten zulässige Geschäftsverfahren – beispielsweise im Bereich der Werbung –, die mit dem Unionsrecht im Einklang stehen, nicht an sich als Verfahren angesehen werden, die gegen das Verbot verstoßen. 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 und auf der Grundlage der ausdrücklichen Zustimmung der Personen durchgeführt wird, die ihnen ausgesetzt sind, oder gegebenenfalls ihres gesetzlichen Vertreters.

- (16a) KI-Systeme, die natürliche Personen kategorisieren, indem sie sie nach bekannten oder vermuteten sensiblen oder geschützten Merkmalen bestimmten Kategorien zuweisen, sind besonders intrusiv, verletzen die menschliche Würde und bringen ein großes Diskriminierungsrisiko mit sich. Zu solchen Merkmalen gehören Geschlecht und Geschlechtsidentität, Rasse, ethnische Herkunft, Migrations- oder Staatsbürgerschaftsstatus, politische Ausrichtung, sexuelle Ausrichtung, Religion, Behinderung oder jegliche anderen Gründe, die nach Artikel 21 der EU-Charta der Grundrechte und nach Artikel 9 der Verordnung (EU) 2016/769 keine Diskriminierung nach sich ziehen dürfen. Solche Systeme sollten daher verboten werden.
- (17) KI-Systeme, die das soziale Verhalten natürlicher Personen für allgemeine Zwecke bewerten, können zu diskriminierenden Ergebnissen und zur Ausgrenzung bestimmter Gruppen führen. Sie verletzen die Menschenwürde und das Recht auf Nichtdiskriminierung sowie die Werte der Gleichheit und Gerechtigkeit. Solche KI-Systeme bewerten oder klassifizieren die Vertrauenswürdigkeit natürlicher Personen oder Gruppen auf der Grundlage zahlreicher Datenpunkte und des zeitlichen Auftretens bestimmter Aspekte ihres sozialen Verhaltens in verschiedenen Zusammenhängen oder aufgrund bekannter, vermuteter 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 greift besonders in die Rechte und Freiheiten der betroffenen Personen ein und kann letztendlich die Privatsphäre eines großen Teils der Bevölkerung beeinträchtigen, ein Gefühl der ständigen Überwachung wecken. Parteien, die biometrische Identifizierung in öffentlich zugänglichen Räumen einsetzen, in eine unkontrollierbare Machtposition bringen und indirekt von der Ausübung der Versammlungsfreiheit und anderer Grundrechte, die den Kern der Rechtsstaatlichkeit darstellen, abhalten. 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. 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. Die Verwendung dieser Systeme in öffentlich zugänglichen Räumen sollte daher verboten werden. Gleichzeitig sollten KI-Systeme, die für die Analyse von aufgezeichnetem Filmmaterial von öffentlich zugänglichen Räumen durch Systeme zur nachträglichen biometrischen Fernidentifizierung verwendet werden, ebenfalls verboten werden, es sei denn, es liegt eine vorgerichtliche Genehmigung für die Verwendung im Rahmen der Strafverfolgung vor, wenn dies für die gezielte Durchsuchung im Zusammenhang mit einer bestimmten schweren Straftat, die bereits stattgefunden hat, unbedingt erforderlich ist, und dies nur mit einer vorgerichtlichen Genehmigung.
- (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 im Sinne dieser Verordnung, 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 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 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.
- (26a) KI-Systeme, die von Strafverfolgungsbehörden oder in deren Auftrag eingesetzt werden, um Vorhersagen, Profile oder Risikobewertungen auf der Grundlage von Datenanalysen oder der Erstellung von Profilen von Gruppen natürlicher Personen oder Orten zu treffen bzw. zu erstellen oder um das Auftreten oder erneute Auftreten einer tatsächlichen oder potenziellen Straftat bzw. von anderem unter Strafe gestelltem Sozialverhalten vorherzusagen, bergen ein besonderes Risiko der Diskriminierung bestimmter Personen oder Personengruppen, da sie die Menschenwürde verletzen sowie gegen den zentralen Rechtsgrundsatz der Unschuldsvermutung verstoßen. Solche KI-Systeme sollten daher verboten werden.
- (26b) Das wahllose und ungezielte Auslesen biometrischer Daten aus sozialen Medien oder Überwachungsvideos, um Gesichtserkennungsdatenbanken zu schaffen oder zu erweitern, verstärkt das Gefühl der Massenüberwachung und kann zu schweren Verstößen gegen die Grundrechte führen, einschließlich des Rechts auf Privatsphäre. Die Verwendung von KI-Systemen zu diesem Zweck sollte daher verboten werden.
- (26c) Im Hinblick auf die wissenschaftliche Grundlage von KI-Systemen zur Erkennung von Emotionen, physischen oder physiologischen Merkmalen wie Gesichtsausdrücken, Bewegungen, der Pulsfrequenz oder der Stimme bestehen ernsthafte Bedenken. Emotionen oder Gefühlsausdrücke werden je nach Kultur und Situation anders wahrgenommen und selbst eine bestimmte Person zeigt in ähnlichen Situationen nicht immer dieselben Emotionen. Zu den größten Schwachstellen solcher Technologien gehören die begrenzte Zuverlässigkeit (Emotionskategorien werden weder zuverlässig durch einen gemeinsamen Satz von Gesichtsbewegungen ausgedrückt noch eindeutig damit in Verbindung gebracht), die mangelnde Spezifität (physische oder physiologische Ausdrücke stimmen nicht eins zu eins mit Emotionskategorien überein) und die begrenzte Verallgemeinerbarkeit (die Auswirkungen von Kontext und Kultur werden nicht ausreichend berücksichtigt). Probleme der Zuverlässigkeit und folglich größere Risiken für Missbrauch können insbesondere dann auftreten, wenn das System in realen Situationen in den Bereichen Strafverfolgung, Grenzverwaltung, Arbeitsplatz und Bildungseinrichtung eingesetzt wird. Daher sollte das Inverkehrbringen, die Inbetriebnahme oder die Verwendung von KI-Systemen, die in Kontexten verwendet werden sollen, um den emotionalen Zustand einer natürlichen Person auszumachen, verboten werden.

- (26d) Praktiken, die nach Unionsrecht, einschließlich Datenschutzrecht, Nichtdiskriminierungsrecht, Verbraucherschutzrecht und Wettbewerbsrecht, verboten sind, sollten von dieser Verordnung nicht betroffen sein.
- (27) Hochrisiko-KI-Systeme sollten nur dann auf dem Unionsmarkt in Verkehr gebracht oder in Betrieb genommen oder verwendet 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, einschließlich der Grundrechte, der Demokratie, der Rechtstaatlichkeit oder der Umwelt. Um die Angleichung an die sektorspezifischen Rechtsvorschriften sicherzustellen und um Doppelungen zu vermeiden, sollten hinsichtlich der Anforderungen für Hochrisiko-KI-Systeme die sektorspezifischen Rechtsvorschriften berücksichtigt werden, die im Rahmen dieser Verordnung enthalten sind, etwa die Verordnung (EU) 2017/745 über Medizinprodukte, die Verordnung (EU) 2017/746 über In-vitro-Diagnostika oder die Richtlinie 2006/42/EG über Maschinen. 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. Angesichts der rasanten technologischen Entwicklung sowie der potenziellen Veränderungen bei der Nutzung von KI-Systemen sollten die Listen von Hochrisikobereichen und -anwendungsfällen in Anhang III jedoch durch die Durchführung regelmäßiger Bewertungen einer ständigen Überprüfung unterzogen werden.
- (28) KI-Systeme könnten negative Auswirkungen auf die Gesundheit und Sicherheit von Personen haben, insbesondere wenn solche Systeme als Sicherheitskomponenten 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.
- (28a) 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, die Gleichstellung der Geschlechter, das Recht auf Bildung, der Verbraucherschutz, die Arbeitnehmerrechte, die Rechte von Menschen mit Behinderungen, Geschlechtergleichstellung, Rechte des geistigen Eigentums, das Recht auf einen wirksamen Rechtsbehelf und ein faires Gerichtsverfahren, 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 oder die Umwelt 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 Rates³⁷, der Verordnung (EU) Nr. 167/2013 des Europäischen Parlaments und des Rates³⁸, der Verordnung (EU) Nr. 168/2013 des Europäischen Parlaments und des Rates³⁹, der Richtlinie 2014/90/EU des Europäischen Parlaments und des Rates⁴⁰, der Richtlinie (EU) 2016/797 des Europäischen Parlaments und des Rates⁴¹, der Verordnung (EU) 2018/858 des Europäischen Parlaments und des Rates⁴², der Verordnung (EU) 2018/1139 des Europäischen Parlaments und des Rates⁴³ und der Verordnung (EU) 2019/2144 des

³⁷ 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).

³⁸ 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).

³⁹ 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).

⁴⁰ 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).

⁴¹ 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).

⁴² 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).

⁴³ 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).

Europäischen Parlaments und des Rates⁴⁴ 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-, Marktüberwachungs- 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 Harmonisierungsrechtsvorschriften der Union fallen, die in Anhang II aufgelistet sind, 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, um sicherzustellen, dass es die wesentlichen Sicherheitsanforderungen erfüllt. 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 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 Rates⁴⁵ und die Verordnung (EU) 2017/746 des Europäischen Parlaments und des Rates⁴⁶, 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 und die unter einem der Bereiche und Anwendungsfälle in Anhang III aufgeführt sind, ist es

⁴⁴ 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).

⁴⁵ 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).

⁴⁶ 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).

angezeigt, sie als hochriskant einzustufen, wenn sie aufgrund ihrer Zweckbestimmung ein erhebliches Risiko bergen, die Gesundheit und Sicherheit oder die Grundrechte von Personen und – wenn das KI-System als Sicherheitskomponente einer kritischen Infrastruktur verwendet wird – die Umwelt wesentlich zu schädigen. Solche erheblichen Gefahrenrisiken sollten einerseits durch die Bewertung des Risikos in Bezug auf eine Kombination von Faktoren wie dem Schweregrad, der Intensität, der Wahrscheinlichkeit des Auftretens und andererseits in Bezug darauf ermittelt werden, ob das Risiko eine Einzelperson, mehrere Personen oder eine bestimmte Gruppe von Personen beeinträchtigen kann. Eine solche Kombination von Faktoren könnte – abhängig vom Kontext – zum Beispiel zu dem Ergebnis führen, dass zwar ein hoher Schweregrad, aber eine geringe Wahrscheinlichkeit vorliegt, eine natürliche Person zu beeinträchtigen, oder eine hohe Wahrscheinlichkeit besteht, eine ganze Gruppe von Personen mit einer geringen Intensität über einen langen Zeitraum zu beeinträchtigen. Die Bestimmung dieser Systeme erfolgt nach derselben Methode und denselben Kriterien, die auch für künftige Änderungen der Liste der Hochrisiko-KI-Systeme vorgesehen sind.

- (32a) Anbieter von KI-Systemen, die unter einen der in Anhang III aufgeführten Bereiche und Anwendungsfälle fallen und die der Auffassung sind, dass ihre Systeme kein erhebliches Risiko für die Gesundheit, Sicherheit, Grundrechte oder die Umwelt darstellen, sollten die nationalen Aufsichtsbehörden informieren, indem sie eine mit Gründen versehene Notifizierung einreichen. Dies kann in Form einer einseitigen Zusammenfassung der relevanten Informationen zu dem jeweiligen KI-System erfolgen, in der auch der vorgesehene Zweck genannt wird und der Grund, warum das KI-System kein erhebliches Risiko für die Gesundheit, die Sicherheit, die Grundrechte oder die Umwelt darstellt. Die Kommission sollte die Kriterien genau spezifizieren, um den Unternehmen eine Bewertung zu ermöglichen, ob ihr System solche Risiken birgt, und damit sie ein einfach anwendbares, standardisiertes Muster für die Meldung entwickeln können. Anbieter sollten die Meldung so schnell wie möglich und in jedem Fall vor dem Inverkehrbringen des KI-Systems auf dem Markt oder seiner Inbetriebnahme einreichen – idealerweise bereits in der Entwicklungsphase –, und sie sollten die Freiheit haben, es nach der Meldung zu jedem gegebenen Zeitpunkt in Verkehr bringen. Falls das KI-System jedoch nach Einschätzung der Behörde falsch eingestuft wurde, sollte die Behörde der Meldung innerhalb eines Zeitraums von drei Monaten widersprechen. Der Widerspruch sollte begründet werden und es sollte ordnungsgemäß erklärt werden, warum das KI-System falsch eingestuft wurde. Dem Anbieter sollte das Recht vorbehalten sein, unter Angabe weiterer Argumente Rechtsmittel einzulegen. Auch wenn es drei Monate nach Einreichen der Meldung keinen Widerspruch gab, können die nationalen Aufsichtsbehörden – wie bei jedem anderen in Verkehr gebrachtem KI-System – dennoch eingreifen, wenn das KI-System auf nationaler Ebene ein Risiko darstellt. Die nationalen Aufsichtsbehörden sollten der KI-Behörde Jahresberichte einreichen, in denen die erhaltenen Notifizierungen und die getroffenen Entscheidungen detailliert aufgeführt werden.
- (33a) Da biometrische Daten in Übereinstimmung mit der Verordnung (EU) 2016/679 eine spezielle Kategorie sensibler personenbezogener Daten darstellen, ist es angemessen, bestimmte

kritische Anwendungsfälle von biometrischen und auf Biometrie beruhenden Systemen als Hochrisikofälle einzustufen. KI-Systeme, die für die biometrische Identifizierung natürlicher Personen verwendet werden sollen, sowie KI-Systeme, durch die auf der Grundlage biometrischer oder biometriegestützter Daten Rückschlüsse auf persönliche Merkmale natürlicher Personen gezogen werden, einschließlich Systemen zum Erkennen von Emotionen, sollten daher – mit Ausnahme der Systeme, die gemäß dieser Verordnung verboten sind – als Hochrisiko-Systeme klassifiziert werden. Dies sollte keine KI-Systeme umfassen, die bestimmungsgemäß für die biometrische Fernidentifizierung verwendet werden sollen, deren einziger Zweck darin besteht, zu bestätigen, dass eine bestimmte Person die Person ist, für die sie sich ausgibt, sowie Systeme, die zur Bestätigung der Identität einer natürlichen Person zu dem alleinigen Zweck verwendet werden, ihr Zugang zu einem Dienst, einem Gerät oder einer Räumlichkeit zu gewähren (Eins-zu-Eins-Überprüfung). Biometrische und auf Biometrie beruhende Systeme, die gemäß den Rechtsvorschriften der Union bereitgestellt werden, um Maßnahmen zur Cybersicherheit und zum Schutz personenbezogener Daten zu ermöglichen, sollten nicht als erhebliches Risiko für die Gesundheit, Sicherheit und die Grundrechte angesehen werden.

- (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 sowie kritische digitale Infrastruktur verwendet werden sollen, als hochriskant eingestuft werden, da ihr Ausfall oder ihre Störung die Sicherheit und Integrität solcher kritischer Infrastruktur oder 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. Sicherheitskomponenten von kritischer Infrastruktur, einschließlich kritischer digitaler Infrastruktur, sind Systeme, die eingesetzt werden, um die physische Integrität von kritischer Infrastruktur oder die Gesundheit und Sicherheit von Personen und Eigentum unmittelbar zu schützen. Ein Ausfall oder eine Störung solcher Komponenten kann direkt zu einer Gefährdung der physischen Integrität kritischer Infrastruktur und somit zu einer Gefährdung der Gesundheit und Sicherheit von Menschen und Eigentum führen. Komponenten, die für die ausschließliche Verwendung zu Zwecken der Cybersicherheit vorgesehen sind, sollten nicht als Sicherheitskomponenten gelten. Zu den Beispielen solcher Sicherheitskomponenten können Systeme zur Überwachung des Wasserdrucks oder Brandmeldekontrollsysteme in Cloud-Rechenzentren gehören.
- (35) Die Einführung von KI-Systemen im Bildungsbereich ist von wesentlicher Bedeutung, um zur Modernisierung ganzer Bildungssysteme beizutragen, die Qualität der Bildung sowohl offline als auch online zu erhöhen und die digitale Bildung zu beschleunigen und sie somit auch einem breiteren Publikum zugänglich zu machen. 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 eine Entscheidung über die Zulassung wesentlich zu beeinflussen oder um Personen im Rahmen

von Prüfungen als Teil ihrer Ausbildung oder als Voraussetzung dafür zu bewerten oder um zu bewerten, ob das Bildungsniveau einer Person angemessen ist, oder um das Niveau der Bildung und Ausbildung, das Personen erhalten oder zu dem sie Zugang erhalten, wesentlich zu beeinflussen oder zu überwachen, oder KI-Systeme, die zur Überwachung und Erkennung von verbotenem Verhalten von Schülern während Prüfungen eingesetzt werden, 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 sehr intrusiv sein und das Recht auf allgemeine und berufliche Bildung sowie das Recht auf Nichtdiskriminierung verletzen und historische Diskriminierungsmuster fortschreiben, beispielsweise gegenüber Frauen, bestimmten Altersgruppen und Menschen mit Behinderungen oder Personen mit einer bestimmten rassischen oder ethnischen Herkunft oder sexuellen Ausrichtung.

- (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 oder für die wesentliche Beeinflussung von Entscheidungen über Einstellung, Beförderung und Kündigung sowie KI-Systeme für die personalisierte Zuweisung von Arbeitsaufgaben auf der Grundlage von individuellem Verhalten, persönlichen Merkmalen oder biometrischen Daten, Überwachung oder Bewertung von Personen in Arbeitsvertragsverhältnissen, sollten ebenfalls als hochriskant eingestuft werden, da diese Systeme die künftigen Karriereaussichten und die Lebensgrundlagen dieser Personen und die Arbeitnehmerrechte spürbar beeinflussen können. Einschlägige Arbeitsvertragsverhältnisse sollten Beschäftigte und Personen sinnvoll erfassen, die Dienstleistungen über Plattformen erbringen, auf die im Arbeitsprogramm der Kommission für 2021 Bezug genommen wird. 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 auch den Kern ihrer Grundrechte auf Datenschutz und Privatsphäre unterminieren. Diese Verordnung gilt unbeschadet der Tatsache, dass es in der Zuständigkeit der Union und der Mitgliedstaaten liegt, spezifischere Vorschriften für den Einsatz von KI-Systemen im Kontext von Beschäftigungsverhältnissen festzulegen.
- (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, auch der Gesundheitsdienste und wesentlicher Dienstleistungen, einschließlich, jedoch nicht beschränkt auf, Wohnen, Strom, Heizung/Kühlung und Internet 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 rassistischen oder ethnischen Herkunft, des Geschlechts, einer Behinderung, des Alters oder der sexuellen Ausrichtung, fortschreiben oder neue Formen von Diskriminierung mit sich bringen. Jedoch sollten KI-Systeme, die nach Rechtsvorschriften der Union zur Aufdeckung von Betrug beim Angebot von Finanzdienstleistungen vorgesehen sind, nicht als Hochrisiko-Systeme gemäß dieser Verordnung angesehen werden. Natürliche Personen, die staatliche Unterstützungsleistungen und -dienste von Behörden beantragen oder erhalten, auch Gesundheitsdienste und wesentliche Dienstleistungen, einschließlich, jedoch nicht beschränkt auf, Wohnen, Strom, Heizung/Kühlung und Internet, 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. Ähnlich können KI-Systeme, die bestimmungsgemäß verwendet werden sollen, um Entscheidungen zu treffen oder erheblichen Einfluss auf Entscheidungen in Bezug auf die Anspruchsvoraussetzungen natürlicher Personen in den Bereichen Kranken- und Lebensversicherungen zu nehmen, ebenso signifikante Auswirkungen auf die Existenzgrundlage von Menschen haben und ihre Grundrechte beeinträchtigen, wie zum Beispiel den Zugang zur Gesundheitsversorgung oder durch die Fortschreibung von Diskriminierung aufgrund persönlicher Merkmale. 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 Bewertung und Einstufung von Notrufen durch natürliche Personen oder 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.

- (37a) In Anbetracht der Rolle und Verantwortung von Polizei- und Justizbehörden und der Auswirkungen von Entscheidungen, die sie zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Vollstreckung von strafrechtlichen Sanktionen treffen, muss der Einsatz von KI-Anwendungen bei der Strafverfolgung vor allem in Situationen als

hochriskant eingestuft werden, wenn die Möglichkeit besteht, dass er beträchtliche Auswirkungen auf das Leben von Einzelpersonen hat.

- (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 Leistung, 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 oder in ihrem Auftrag oder von Organen, Einrichtungen und sonstigen Stellen der Union als Lügendetektoren und ähnliche Instrumente zur Bewertung der Zuverlässigkeit von Beweismitteln in Strafverfahren, zur Erstellung eines Profils während der Aufdeckung, Untersuchung oder strafrechtlichen Verfolgung einer Straftat sowie zur Kriminalanalyse in Bezug auf natürliche Personen eingesetzt werden, sofern deren Verwendung gemäß den relevanten nationalen Rechtsvorschriften und denen der Union zugelassen ist. KI-Systeme, die speziell für Verwaltungsverfahren in Steuer- und Zollbehörden bestimmt sind, sollten nicht als Hochrisiko-KI-Systeme eingestuft werden, die von Strafverfolgungsbehörden zum Zwecke der Verhütung, Aufdeckung, Untersuchung und strafrechtlichen Verfolgung von Straftaten eingesetzt werden. Der Einsatz von KI-Instrumenten durch Strafverfolgungs- und Justizbehörden sollte nicht zu einem Faktor der Ungleichheit, der sozialen Spaltung oder der Ausgrenzung werden. Die Auswirkungen des Einsatzes von KI-Instrumenten auf die Verteidigungsrechte von Verdächtigen sollten nicht außer Acht gelassen werden, insbesondere nicht die Schwierigkeit, aussagekräftige Informationen über ihre Funktionsweise zu erhalten, und die daraus resultierende Schwierigkeit der Anfechtung ihrer Ergebnisse vor Gericht, insbesondere durch Personen, gegen die ermittelt wird.
- (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 oder den Organen, Einrichtungen und sonstigen Stellen der Union oder in ihrem Auftrag als Lügendetektoren und ähnliche Instrumente – sofern ihr Einsatz gemäß den relevanten nationalen Rechtsvorschriften oder denen der Union gestattet ist – oder zur Bewertung bestimmter Risiken eingesetzt werden, 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 und Bewertung des Wahrheitsgehalts von Nachweisen von Asyl- und Visumanträgen sowie Aufenthaltstiteln und damit verbundenen Beschwerden im Hinblick darauf, die Berechtigung der den Antrag stellenden natürlichen Personen festzustellen; zur Überwachung, Kontrolle oder Verarbeitung von personenbezogenen Daten im Zusammenhang mit Grenzkontrolltätigkeiten zur Ortung, Erkennung oder Identifizierung von natürlichen Personen; für Prognosen oder Vorhersagen von Trends im Zusammenhang mit Migrationsbewegungen und Grenzüberschreitungen. 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 Rates⁴⁷, der Verordnung (EG) Nr. 810/2009 des Europäischen Parlaments und des Rates⁴⁸ und anderen einschlägigen Rechtsvorschriften entsprechen. KI-Systeme, die in den Bereichen Migration, Asyl und Grenzkontrolle eingesetzt werden, sollten unter keinen Umständen von Mitgliedstaaten oder Organen, Einrichtungen und sonstigen Stellen der Union als Mittel zur Umgehung ihrer internationalen Verpflichtungen gemäß dem Genfer Abkommen vom 28. Juli 1951 über die Rechtsstellung der Flüchtlinge in der Fassung des Protokolls von New York vom 31. Januar 1967 genutzt noch unter Verstoß gegen den Grundsatz der Nichtzurückweisung oder zur Verweigerung sicherer und effektiver rechtmäßiger Wege in das Gebiet der Union gegenüber Asylsuchenden, auch in Bezug auf das Recht auf internationalen Schutz, verwendet werden.

- (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

⁴⁷ 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).

⁴⁸ 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).

insbesondere den Risiken möglicher Verzerrungen, Fehler und Undurchsichtigkeiten zu begegnen, sollten KI-Systeme, die von einer Justiz- oder Verwaltungsbehörde oder in ihrem Auftrag dazu eingesetzt werden, diese Justiz- oder Verwaltungsbehörde dabei zu unterstützen, Sachverhalte und Rechtsvorschriften zu ermitteln und auszulegen und das Recht auf konkrete Sachverhalte anzuwenden, oder auf ähnliche Weise in einem alternativem Streitbeilegungsverfahren eingesetzt werden, als hochriskant eingestuft werden. Der Einsatz von Instrumenten mit künstlicher Intelligenz kann die Entscheidungsgewalt von Richtern oder die Unabhängigkeit der Justiz unterstützen, sollte sie aber nicht ersetzen, da die endgültige Entscheidungsfindung eine von Menschen geleitete Tätigkeit und Entscheidung bleiben muss. 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.

- (40a) Um die Risiken eines unzulässigen externen Eingriffs in das in Artikel 39 der Charta verankerte Wahlrecht und unverhältnismäßige Auswirkungen auf demokratische Verfahren, die Demokratie und die Rechtsstaatlichkeit anzugehen, sollten KI-Systeme, die bestimmungsgemäß verwendet werden sollen, um das Ergebnis einer Wahl oder eines Referendums oder das Wahlverhalten natürlicher Personen bei der Ausübung ihres Wahlrechts in einer Wahl oder in Referenden zu beeinflussen, als Hochrisiko-KI-Systeme eingestuft werden, mit Ausnahme von KI-Systemen, deren Ergebnissen natürliche Personen nicht direkt ausgesetzt sind, wie Instrumente zur Organisation, Optimierung und Strukturierung politischer Kampagnen in administrativer und logistischer Hinsicht.
- (40b) Angesichts der Anzahl natürlicher Personen, die die Dienste nutzen, die von Social-Media-Plattformen bereitgestellt werden, die als sehr große Online-Plattformen gelten, können solche Online-Plattformen auf eine Weise eingesetzt werden, die die Online-Sicherheit stark gefährdet und die öffentliche Meinung und den öffentlichen Diskurs sowie Wahlverfahren und demokratische Prozesse oder soziale Belange stark beeinflusst. Es ist daher angezeigt, dass KI-Systeme, die von diesen Online-Plattformen in ihren Empfehlungssystemen verwendet werden, unter diese Verordnung fallen, um sicherzustellen, dass die KI-Systeme die in dieser Verordnung festgelegten Anforderungen erfüllen, einschließlich technischer Vorschriften in den Bereichen Datenverwaltung, technische Dokumentation und Rückverfolgbarkeit, Transparenz, menschliche Aufsicht, Genauigkeit und Robustheit der Daten. Durch die Einhaltung der Bestimmungen dieser Verordnung sollte es den Betreibern sehr großer Online-Plattformen möglich sein, die umfassenderen Verpflichtungen zur Risikobewertung und Risikominderung gemäß Artikel 34 und 35 der Verordnung (EU) 2022/2065 zu erfüllen. Die Verpflichtungen gemäß der vorliegenden Verordnung lassen die Bestimmungen der Verordnung (EU) 2022/2065 unberührt und sollten die gemäß der Verordnung (EU) 2022/2065 festgesetzten Verpflichtungen in Fällen, in denen die soziale Medienplattform als sehr große Online-Plattform

eingestuft wurde, ergänzen. Angesichts der europaweiten Auswirkungen von Social-Media-Plattformen, die als sehr große Online-Plattformen eingestuft wurden, sollten die nach Verordnung (EU) 2022/2065 festgelegten Behörden für die Zwecke der Durchsetzung dieser Bestimmung als Strafverfolgungsbehörden fungieren.

- (41) Die Tatsache, dass ein KI-System gemäß dieser Verordnung als hochriskantes KI-System 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 oder nicht rechtmäßig ist, beispielsweise in Bezug auf den Schutz personenbezogener Daten. Eine solche Verwendung sollte weiterhin ausschließlich im Einklang mit den geltenden Anforderungen erfolgen, die sich aus der Charta, dem anwendbaren Sekundärrecht der Union und nationalen Recht ergeben.
- (41a) Eine gewisse Anzahl von verbindlichen Rechtsvorschriften auf Unions-, nationaler und internationaler Ebene, die für KI-Systeme relevant sind, gelten bereits, unter anderem das Primärrecht der EU (die EU-Verträge und die EU-Grundrechtecharta), das Sekundärrecht der EU (etwa die Datenschutzgrundverordnung, die Produkthaftungsrichtlinie, die Verordnung über den freien Verkehr nicht personenbezogener Daten, Antidiskriminierungsrichtlinien, das Verbraucherschutzrecht sowie die Richtlinien über Sicherheit und Gesundheitsschutz am Arbeitsplatz), die UN-Menschenrechtsübereinkommen, die Konventionen des Europarats (wie die Europäische Menschenrechtskonvention) sowie zahlreiche nationale Gesetze. Neben bereichsübergreifenden gibt es auch verschiedene fachspezifische Vorschriften, die für bestimmte KI-Anwendungen gelten (etwa die Verordnung über Medizinprodukte).
- (42) Zur Minderung der Risiken für Betreiber 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 sowie der vernünftigerweise vorhersehbaren Fehlanwendung und dem vom Anbieter einzurichtenden Risikomanagementsystem Rechnung zu tragen ist. Diese Anforderungen sollten zielorientiert, zweckdienlich, angemessen und wirksam sein, ohne den Akteuren unangemessene zusätzliche regulatorische Belastungen oder Kosten aufzubürden.
- (43) Die Anforderungen sollten für Hochrisiko-KI-Systeme im Hinblick auf die Qualität und Relevanz der verwendeten Datensätze, die technische Dokumentation und die Aufzeichnungspflichten, die Transparenz und die Bereitstellung von Informationen für die Betreiber, 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 oder vernünftigerweise vorhersehbaren Fehlanwendung des Systems wirksam zu mindern, und es stehen keine anderen weniger handelsbeschränkenden Maßnahmen zur Verfügung, sodass ungerechtfertigte Handelsbeschränkungen vermieden werden.

- (44) Ein Zugang zu einer hohen Datenqualität spielt eine zentrale Rolle bei der Bereitstellung von Strukturen und für die Sicherstellung der Leistung vieler KI-Systeme, 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. Trainings- und – falls zutreffend – Validierungs- und Testdatensätze, einschließlich der Kennzeichnungen, sollten im Hinblick auf die Zweckbestimmung des Systems hinreichend relevant, repräsentativ sowie ordnungsgemäß auf Fehler überprüft und so vollständig wie möglich 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, mit besonderem Augenmerk auf die Minderung möglicher Verzerrungen in den Datensätzen, die zu Risiken für die Grundrechte oder zu diskriminierenden Ergebnissen für die von dem Hochrisiko-KI-System betroffenen Personen führen könnten. Verzerrungen können zum Beispiel, insbesondere bei Verwendung historischer Daten, den zugrunde liegenden Datensätzen innewohnen sowie von den Entwicklern der Algorithmen eingeführt oder bei der Implementierung der Systeme in der realen Welt generiert werden. Die von einem KI-System ausgegebenen Ergebnisse werden durch solche inhärenten Verzerrungen beeinflusst und haben die Tendenz, allmählich zuzunehmen und dadurch bestehende Diskriminierungen fortzusetzen und zu verstärken, insbesondere im Hinblick auf Personen, die bestimmten ethnischen Gruppen oder aufgrund von Rassismus benachteiligten Gemeinschaften angehören. 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, kontext- und 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 – ausnahmsweise und nach Anwendung aller geltenden Bedingungen, die in dieser Verordnung und in der Verordnung (EU) 2016/679, der Richtlinie (EU) 2016/680 und der Verordnung (EU) 2018/1725 festgelegt sind – angesichts des erheblichen öffentlichen Interesses auch besondere Kategorien personenbezogener Daten verarbeiten dürfen, um Verzerrungen in Hochrisiko-KI-Systemen zu erkennen und zu korrigieren. Negative Verzerrungen sollten als Verzerrungen verstanden werden, durch die direkte oder indirekte diskriminierende Auswirkungen in Bezug auf eine natürliche Person entstehen. Die Anforderungen in Bezug auf die Datenverwaltung können erfüllt werden, indem auf Dritte zurückgegriffen wird, die zertifizierte Konformitätsdienstleistungen anbieten, einschließlich der Überprüfung der Datenverwaltung, der Integrität der Datensätze und der Datenschulungs-, Validierungs- und Testverfahren.

- (45) Für die Entwicklung und Bewertung 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.
- (45a) Das Recht auf Privatsphäre und den Schutz personenbezogener Daten muss während des gesamten Lebenszyklus des KI-Systems sichergestellt sein. In dieser Hinsicht sind die Grundsätze der Datenminimierung und des Datenschutzes durch Technikgestaltung und datenschutzfreundliche Voreinstellungen, wie sie im Datenschutzrecht der Union festgelegt sind, von wesentlicher Bedeutung, wenn die Verarbeitung von Daten erhebliche Risiken für die Grundrechte natürlicher Personen birgt. Anbieter und Nutzer von KI-Systemen sollten dem Stand der Technik entsprechende technische und organisatorische Maßnahmen ergreifen, um diese Rechte zu schützen. Zu diesen Maßnahmen gehören nicht nur die Anonymisierung und Verschlüsselung, sondern auch der Einsatz zunehmend verfügbarer Technik, die es ermöglicht, Algorithmen direkt am Ort der Datenerzeugung einzusetzen und wertvolle Erkenntnisse zu gewinnen, ohne dass die Daten zwischen den Parteien übertragen bzw. die Rohdaten oder strukturierten Daten selbst unnötig kopiert werden.
- (46) Umfassende Informationen darüber, wie Hochrisiko-KI-Systeme entwickelt wurden und wie sie während ihres gesamten Lebensdauer 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 während des gesamten Lebenszyklus des KI-Systems stets auf einem angemessenen Stand gehalten werden. KI-Systeme können während

ihres gesamten Lebenszyklus wesentliche Auswirkungen auf die Umwelt und einen hohen Energieverbrauch haben. Um die Auswirkungen von KI-Systemen auf die Umwelt besser erfassen zu können, sollte die von den Anbietern erstellte technische Dokumentation Informationen zum Energieverbrauch des KI-Systems enthalten, einschließlich des Verbrauchs während der Entwicklung und des erwarteten Verbrauchs während der Nutzung. Bei diesen Informationen sollten die einschlägigen nationalen Rechtsvorschriften und Rechtsvorschriften der Union berücksichtigt werden. Die übermittelten Informationen sollten verständlich, vergleichbar und überprüfbar sein und zu diesem Zweck sollte die Kommission Leitlinien zu einer harmonisierten Methode für die Berechnung und Meldung solcher Informationen entwickeln. Um sicherzustellen, dass eine einzige technische Dokumentation erstellt werden kann, sollten die diese Dokumentation betreffenden Begriffe und Definitionen und jegliche anderen Dokumentationen in den einschlägigen Rechtsvorschriften so weit wie möglich angeglichen werden.

- (46a) Hochrisiko-KI-Systeme müssen modernste Methoden und einschlägige geltende Normen berücksichtigen, um den Energie- und Ressourcenverbrauch sowie die Abfallerzeugung zu verringern und die Energieeffizienz sowie die Gesamteffizienz des Systems zu erhöhen. Die Umweltaspekte von KI-Systemen, die für die Zwecke dieser Verordnung signifikant sind, sind der Energieverbrauch des KI-Systems während der Entwicklungs-, Trainings- und Einführungsphase sowie bei der Aufzeichnung, Meldung und Speicherung dieser Daten. Durch die Konzeption von KI-Systemen sollte es möglich sein, den Energieverbrauch und die Energieressourcen während jeder Phase der Entwicklung, des Trainings und des Einsatzes zu messen und aufzuzeichnen. Die Beobachtung und Meldung der Emissionen von KI-Systemen muss robust, transparent, kohärent und genau sein. Um eine einheitliche Anwendung dieser Verordnung und ein stabiles rechtliches Umfeld für die Anbieter und Betreiber im Binnenmarkt sicherzustellen, sollte die Kommission eine gemeinsame Spezifikation für die Methodik entwickeln, damit die Berichterstattungs- und Dokumentierungspflichten zum Energieverbrauch und den Ressourcen während der Entwicklung, des Trainings und des Einsatzes von KI-Systemen erfüllt werden. Auf der Grundlage solcher gemeinsamer Spezifikationen kann eine Messmethode zur Erstellung eines Entwurfs eines Referenzszenarios entwickelt werden, mit der die Kommission – nachdem eine Folgenabschätzung unter Berücksichtigung des geltenden Rechts durchgeführt wurde – besser darüber entscheiden kann, ob künftige regulatorische Eingriffe erforderlich sind.
- (46b) Um die Ziele dieser Verordnung zu erreichen und zu den Umweltzielen der Union beizutragen und gleichzeitig das reibungslose Funktionieren des Binnenmarkts sicherzustellen, könnte es erforderlich sein, Empfehlungen und Leitlinien zu erstellen und – letztendlich – auch Nachhaltigkeitsziele. Zu diesem Zweck ist die Kommission befugt, eine Methodik zu entwickeln, um damit zur Erstellung wesentlicher Leistungsindikatoren und eines Bezugsrahmens für die Nachhaltigkeitsziele der Vereinten Nationen beizutragen. Das Ziel sollte es vor allem sein, einen gerechten Vergleich zwischen den verschiedenen Möglichkeiten zur Umsetzung von KI zu

ermöglichen, indem Anreize geschaffen werden, um die Nutzung effizienterer KI-Technologien in den Bereichen Energie und Ressourcen zu fördern. Um diese Ziele zu erreichen, sollten durch diese Verordnung die Mittel bereitgestellt werden, um eine grundlegende Datensammlung zu den gemeldeten Daten zu Emissionen zu erstellen, die während der Entwicklung, des Trainings und des Einsatzes von KI-Systemen entstehen.

- (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.
- (47a) Solche Anforderungen an Transparenz und Nachvollziehbarkeit der KI-Entscheidungsfindung sollten auch dazu beitragen, den abschreckenden Auswirkungen digitaler Asymmetrie und sogenannter „Dark Patterns“ entgegenzuwirken, die auf Einzelpersonen und ihre Einwilligung nach Aufklärung abzielen.
- (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. Leistungskennzahlen und ihre erwarteten Genauigkeitsgrade sollten mit dem vorrangigen Ziel festgelegt werden, Risiken und negative Auswirkungen des KI-Systems zu mindern. Der erwartete Grad der Leistungskennzahlen sollte den Betreibern auf klare, transparente, leicht nachvollziehbare und verständliche Weise mitgeteilt werden. Die Angabe von Leistungskennzahlen gibt keinen Aufschluss auf die künftige Leistung, sodass entsprechende Methoden angewandt werden müssen, um eine dauerhafte Leistung während der Nutzung sicherzustellen. Es sind zwar Normungsgremien vorhanden, um Normen vorzugeben, allerdings ist eine Abstimmung beim Leistungsvergleich vonnöten, um festzulegen, wie diese Standardvorgaben und -merkmale von KI-Systemen gemessen werden sollten. Der Europäische Ausschuss für künstliche Intelligenz sollte nationale und internationale Metrologie- und Benchmarking-Behörden zusammenbringen

und Leitlinien herausgeben, um die technischen Aspekte der Messung der angemessenen Leistungs- und Robustheitsgrade anzugehen.

- (50) Die technische Robustheit ist eine wesentliche Voraussetzung für Hochrisiko-KI-Systeme. Sie sollten widerstandsfähig 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. Die Nutzer des KI-Systems sollten Maßnahmen ergreifen, um sicherzustellen, dass der mögliche Kompromiss zwischen Robustheit und Genauigkeit nicht zu diskriminierenden oder negativen Ergebnissen für Untergruppen, die Minderheiten angehören, führt.
- (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 oder Angriffe auf vertrauliche Daten) 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 sowie die notifizierten Stellen, zuständigen nationalen Behörden und Marktüberwachungsbehörden daher geeignete Maßnahmen ergreifen, wobei gegebenenfalls auch die zugrunde liegende IKT-Infrastruktur zu berücksichtigen ist. Bei Hochrisiko-KI sollten Sicherheitslösungen und Patches für die gesamte Lebensdauer des Produkts oder, falls keine Abhängigkeit von einem bestimmten Produkt besteht, für einen vom Hersteller anzugebenden Zeitraum bereitgestellt werden.
- (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 Rates⁴⁹ über die Vorschriften für die Akkreditierung und Überwachung von Produkten, dem Beschluss Nr. 768/2008/EG des Europäischen Parlaments und des Rates⁵⁰ über einen gemeinsamen Rechtsrahmen für die Vermarktung von Produkten und der Verordnung (EU) 2019/1020 des

⁴⁹ 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).

⁵⁰ 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).

Europäischen Parlaments und des Rates⁵¹ 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.
- (53a) Als Unterzeichner des Übereinkommens über die Rechte von Menschen mit Behinderungen der Vereinten Nationen (VN-BRK) sind die Union und alle Mitgliedstaaten rechtlich verpflichtet, Menschen mit Behinderungen vor Diskriminierung zu schützen und ihre Gleichstellung zu fördern, sicherzustellen, dass Menschen mit Behinderungen gleichberechtigt Zugang zu Informations- und Kommunikationstechnologien und -systemen haben, und die Achtung der Privatsphäre von Menschen mit Behinderungen sicherzustellen. Angesichts der zunehmenden Bedeutung und Nutzung von KI-Systemen sollte die strikte Anwendung der Grundsätze des universellen Designs auf alle neuen Technologien und Dienste einen vollständigen, gleichberechtigten und uneingeschränkten Zugang für alle Menschen sicherstellen, die potenziell von KI-Technologien betroffen sind oder diese nutzen, einschließlich Menschen mit Behinderungen, und zwar in einer Weise, die ihrer Würde und Vielfalt in vollem Umfang Rechnung trägt. Es ist daher von wesentlicher Bedeutung, dass die Anbieter die uneingeschränkte Einhaltung der Zugänglichkeitsanforderungen sicherstellen, einschließlich der in der Richtlinie (EU) 2016/2102 und Richtlinie (EU) 2019/882 festgelegten Anforderungen. Die Anbieter sollten die Einhaltung dieser Anforderungen durch Voreinstellungen sicherstellen. Die erforderlichen Maßnahmen sollten daher so weit wie möglich in die Konzeption von Hochrisiko-KI-Systemen integriert werden.
- (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. Für Anbieter, die bereits Qualitätsmanagementsysteme auf der Grundlage von Normen wie der Norm ISO 9001 oder anderen einschlägigen Normen eingerichtet haben, sollte nicht ein weiteres, doppeltes Qualitätsmanagementsystem eingerichtet werden, sondern eher eine Anpassung der bereits bestehenden Systeme an bestimmte Aspekte vorgenommen werden, die mit der Einhaltung der spezifischen Anforderungen dieser Verordnung zusammenhängen. Dies sollte sich – in diesem Zusammenhang – auch in künftigen Normungstätigkeiten der Kommission oder von ihr angenommenen Leitlinien niederschlagen. 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

⁵¹ 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).

als Teil des auf nationaler oder regionaler Ebene eingesetzten Qualitätsmanagementsystems annehmen und umsetzen.

- (55) Wird ein Hochrisiko-KI-System, bei dem es sich um eine Sicherheitskomponente eines Produkts handelt, das unter einschlägige sektorale Rechtsvorschriften des neuen Rechtsrahmens 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.
- (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 Betreiber festzulegen, auch im Hinblick darauf, dass eine angemessene Überwachung der Leistung eines KI-Systems unter realen Bedingungen sichergestellt werden muss. Die Betreiber 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.
- (58a) Während Risiken im Zusammenhang mit KI-Systemen einerseits aus der Art und Weise entstehen können, in der solche Systeme konzipiert sind, können sie sich andererseits auch aus der Art und Weise ergeben, in der diese Systeme verwendet werden. Betreiber von Hochrisiko-KI-Systemen spielen daher eine entscheidende Rolle bei der Gewährleistung des Schutzes der Grundrechte in Ergänzung der Pflichten der Anbieter bei der Entwicklung der KI-Systeme. Betreiber können am besten verstehen, wie das Hochrisiko-KI-System konkret eingesetzt wird, weshalb sie dank einer genaueren Kenntnis des Verwendungskontextes sowie der wahrscheinlich betroffenen Personen oder Personengruppen, einschließlich marginalisierter und schutzbedürftiger Gruppen, erhebliche potenzielle Risiken erkennen können, die in der Entwicklungsphase nicht vorausgesehen wurden. In diesem spezifischen

Nutzungskontext sollten die Betreiber geeignete Verwaltungsstrukturen ermitteln, wie Regelungen für menschliche Aufsicht, Verfahren für die Bearbeitung von Beschwerden sowie Rechtsbehelfe, weil die Auswahl der Verwaltungsstrukturen für die Minderung der Risiken für Grundrechte in konkreten Anwendungsfällen von entscheidender Bedeutung sein kann. Um auf wirksame Weise sicherzustellen, dass die Grundrechte geschützt werden, sollten Betreiber von Hochrisiko-KI-Systemen daher vor der Inbetriebnahme dieser Systeme eine Folgenabschätzung im Hinblick auf die Grundrechte durchführen. Der Folgenabschätzung sollte ein detaillierter Plan beigefügt werden, in dem die Maßnahmen oder Instrumente beschrieben werden, die zur Minderung der festgestellten Risiken für die Grundrechte beitragen, spätestens ab dem Zeitpunkt der Einführung des Systems. Wenn ein solcher Plan nicht ermittelt werden kann, sollten die Betreiber davon absehen, das System einzuführen. Bei der Durchführung dieser Folgenabschätzung sollte der Betreiber die nationale Aufsichtsbehörde und – so weit wie möglich – die einschlägigen Interessenträger sowie die Vertreter von Personengruppen, die wahrscheinlich von dem KI-System betroffen sein werden, benachrichtigen, um die relevanten Informationen einzuholen, die erforderlich sind, die Folgenabschätzung durchzuführen und den Betreibern wird nahegelegt, die Zusammenfassung ihrer Folgenabschätzung in Bezug auf die Grundrechte auf ihrer Online-Website öffentlich zugänglich zu machen. Diese Verpflichtung sollte – angesichts fehlender Ressourcen – nicht für KMU gelten, die möglicherweise Schwierigkeiten haben, eine solche Konsultation durchzuführen. Dennoch sollten auch KMU es anstreben, solche Vertreter einzubeziehen, wenn sie ihre Folgenabschätzung in Bezug auf die Grundrechte durchführen. Darüber hinaus sollten Betreiber von Hochrisiko-KI-Systemen, die öffentliche Behörden oder Organe, Einrichtungen und sonstige Stellen der Union sowie Betreiber, die nach Verordnung (EU) 2022/1925 als Torwächter benannte Unternehmen sind, angesichts der potenziellen Auswirkungen und der Notwendigkeit demokratischer Aufsicht und Kontrolle verpflichtet werden, die Nutzung von Hochrisiko-KI-Systemen in einer öffentlichen Datenbank zu registrieren. Andere Betreiber können die Nutzung ihrer Hochrisiko-KI-Systeme freiwillig registrieren.

- (59) Es ist angemessen, davon auszugehen, dass der Betreiber 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) Innerhalb der KI-Wertschöpfungskette liefern häufig mehrere Unternehmen Tools und Dienstleistungen, aber auch Komponenten oder Prozesse, die dann vom Anbieter in das KI-System integriert werden, u. a. in Bezug auf die Datenerfassung und -vorverarbeitung, das Trainieren, Umtrainieren, Testen und Bewerten von Modellen, die Integration in Software oder andere Aspekte der Modellentwicklung. Die beteiligten Unternehmen können ihr Angebot direkt oder indirekt über Schnittstellen wie Anwendungsprogrammierschnittstellen (API) kommerziell zur Verfügung stellen und unter freien und quelloffenen Lizenzen vertreiben, aber auch zunehmend über KI-Arbeitskräfteplattformen, den Weiterverkauf von trainierten Parametern,

DIY-Kits zum Bau von Modellen oder über das Angebot eines kostenpflichtigen Zugangs zu einer Modellservicearchitektur zur Entwicklung und zum Trainieren von Modellen. Angesichts dieser Komplexität der KI-Wertschöpfungskette sollten alle einschlägigen Dritten, insbesondere diejenigen, die an der Entwicklung, am Verkauf und an der kommerziellen Bereitstellung von Software-Tools, Komponenten, vortrainierten Modellen oder in das KI-System integrierten Daten beteiligt sind, oder Netzdienstbetreiber, ohne ihre eigenen Rechte an geistigem Eigentum oder Geschäftsgeheimnisse zu gefährden, die erforderlichen Informationen, Schulungen oder Fachkenntnisse zur Verfügung stellen und gegebenenfalls mit Anbietern, denen die Kontrolle über alle für die Einhaltung der Vorschriften relevanten Aspekte des KI-Systems, das unter diese Verordnung fällt, ermöglicht werden soll, zusammenarbeiten. Um eine kosteneffiziente Steuerung der KI-Wertschöpfungskette zu ermöglichen, muss der Grad der Kontrolle von jedem Dritten, der dem Anbieter ein Tool, eine Dienstleistung, eine Komponente oder ein Verfahren liefert, das später vom Anbieter in das KI-System integriert wird, ausdrücklich offengelegt werden.

- (60a) Befindet sich eine Partei in einer stärkeren Verhandlungsposition, so besteht die Gefahr, dass diese Partei diese Position zum Nachteil der anderen Vertragspartei ausnutzt, wenn sie über die Lieferung von Werkzeugen, Dienstleistungen, Komponenten oder Verfahren, die in einem Hochrisiko-KI-System verwendet oder integriert werden, oder über die Abhilfemaßnahmen im Falle der Verletzung oder der Beendigung damit verbundener Verpflichtungen verhandelt. Solche vertraglichen Ungleichgewichte schaden insbesondere Kleinstunternehmen sowie kleinen und mittleren Unternehmen sowie Start-ups, es sei denn, sie befinden sich im Besitz eines Unternehmens oder werden von einem Unternehmen unter Vertrag genommen, das den Unterauftragnehmer angemessen entschädigen kann, da sie nicht in der Lage sind, die Bedingungen der vertraglichen Vereinbarung auszuhandeln, und unter Umständen keine andere Wahl haben, als Vertragsbedingungen ohne Verhandlungsspielraum zu akzeptieren. Daher sollten missbräuchliche Vertragsklauseln, die die Lieferung von Werkzeugen, Dienstleistungen, Bauteilen oder Verfahren, die in einem Hochrisiko-KI-System verwendet oder integriert werden, oder die Abhilfemaßnahmen bei Verletzung oder Beendigung damit verbundener Verpflichtungen regeln, für solche Kleinstunternehmen, kleinen oder mittleren Unternehmen und Start-ups nicht verbindlich sein, wenn sie ihnen einseitig auferlegt wurden.
- (60b) Bei den Vorschriften über Vertragsbedingungen sollte der Grundsatz der Vertragsfreiheit als wesentliches Konzept in den Geschäftsbeziehungen zwischen Unternehmen berücksichtigt werden. Daher sollten nicht alle Vertragsklauseln einer Missbräuchlichkeitsprüfung unterzogen werden, sondern nur solche Klauseln, die einseitig Kleinst-, kleinen und mittleren Unternehmen und Start-ups auferlegt werden. Dies betrifft Situationen ohne Verhandlungsspielraum, in denen eine Partei eine bestimmte Vertragsklausel einbringt und das Kleinstunternehmen bzw. das kleine oder mittlere Unternehmen und das Start-up den Inhalt dieser Klausel trotz eines Verhandlungsversuchs nicht beeinflussen kann. Eine Vertragsklausel, die lediglich von einer Partei eingebracht und von dem Kleinstunternehmen bzw. dem kleinen oder mittleren

Unternehmen oder einem Start-up akzeptiert wird, oder eine Klausel, die zwischen den Vertragsparteien ausgehandelt und anschließend in geänderter Weise vereinbart wird, sollte nicht als einseitig auferlegt gelten.

- (60c) Darüber hinaus sollten die Vorschriften über missbräuchliche Vertragsklauseln nur für diejenigen Vertragsbestandteile gelten, die sich auf die Lieferung von Werkzeugen, Dienstleistungen, Komponenten oder Verfahren beziehen, die in einem Hochrisiko-KI-System verwendet werden oder darin integriert sind, oder auf die Abhilfemaßnahmen bei Verletzung oder Beendigung der damit verbundenen Verpflichtungen. Andere Teile desselben Vertrags, die nicht mit diesen Bestandteilen zusammenhängen, sollten nicht der in dieser Verordnung festgelegten Missbräuchlichkeitsprüfung unterliegen.
- (60d) Kriterien für die Ermittlung missbräuchlicher Vertragsklauseln sollten nur auf überzogene Vertragsbedingungen angewandt werden, bei denen eine stärkere Verhandlungsposition missbraucht wird. Die überwiegende Mehrheit der Vertragsklauseln, die in wirtschaftlicher Hinsicht für eine Partei günstiger sind als für die andere, einschließlich derjenigen, die in Verträgen zwischen Unternehmen üblich sind, sind ein normaler Ausdruck des Grundsatzes der Vertragsfreiheit und gelten weiterhin. Ist eine Vertragsbedingung nicht in der Liste der Klauseln aufgeführt, die stets als missbräuchlich gelten, findet die allgemeine Missbräuchlichkeitsbestimmung Anwendung. In diesem Zusammenhang sollten die als missbräuchlich aufgeführten Klauseln als Maßstab für die Auslegung der allgemeinen Missbräuchlichkeitsbestimmung dienen.
- (60e) Basismodelle sind eine neuere Entwicklung, bei der KI-Modelle auf der Grundlage von Algorithmen entwickelt werden, die im Hinblick auf Allgemeinheit und Vielseitigkeit der Ergebnisse optimiert wurden. Diese Modelle werden häufig auf der Grundlage eines breiten Spektrums von Datenquellen und großer Datenmengen trainiert, um eine Fülle nachgelagerter Aufgaben zu erfüllen, darunter auch solche, für die sie nicht speziell entwickelt und trainiert wurden. Das Basismodell kann unimodal oder multimodal sein und durch verschiedene Methoden wie überwachtes Lernen oder bestärkendes Lernen trainiert werden. KI-Systeme mit spezifischer Zweckbestimmung oder KI-Systeme mit allgemeinem Verwendungszweck können eine Implementierung eines Basismodells sein, was bedeutet, dass jedes Basismodell in unzähligen nachgelagerten KI-Systemen oder KI-Systemen mit allgemeinem Verwendungszweck wiederverwendet werden kann. Diese Modelle sind für viele nachgelagerte Anwendungen und Systeme von wachsender Bedeutung.
- (60f) Im Falle von Basismodellen, die als Dienstleistung, z. B. über den API-Zugang, bereitgestellt werden, sollte sich die Zusammenarbeit mit nachgeschalteten Anbietern über den gesamten Zeitraum erstrecken, in dem dieser Dienst bereitgestellt und unterstützt wird, um eine angemessene Risikominderung zu ermöglichen, es sei denn, der Anbieter des Basismodells überträgt das Trainingsmodell sowie umfassende und angemessene Informationen über die Datensätze und den Entwicklungsprozess des Systems oder schränkt den Dienst, z. B. den

API-Zugang, so ein, dass der nachgeschaltete Anbieter in der Lage ist, dieser Verordnung ohne weitere Unterstützung durch den ursprünglichen Anbieter des Basismodells vollständig zu entsprechen.

- (60g) Angesichts der Art und Komplexität der Wertschöpfungskette für KI-Systeme ist es von entscheidender Bedeutung, die Rolle der Akteure zu klären, die zur Entwicklung von KI-Systemen beitragen. Es besteht erhebliche Unsicherheit darüber, wie sich Basismodelle entwickeln werden, sowohl in Bezug auf die Typologie der Modelle als auch in Bezug auf die Selbstverwaltung. Daher muss die rechtliche Situation der Anbieter von Basismodellen unbedingt geklärt werden. Angesichts ihrer Komplexität und unerwarteten Auswirkungen, der mangelnden Kontrolle des nachgelagerten KI-Anbieters über die Entwicklung des Basismodells und des sich daraus ergebenden Machtungleichgewichts und um eine gerechte Aufteilung der Verantwortung entlang der KI-Wertschöpfungskette zu gewährleisten, sollten solche Modelle im Rahmen dieser Verordnung angemessenen und spezifischeren Anforderungen und Verpflichtungen unterliegen. Insbesondere sollten Basismodelle mögliche Risiken und Schäden durch geeignete Gestaltung, Erprobung und Analyse bewerten und mindern, Maßnahmen zur Datenverwaltung, einschließlich der Bewertung von Verzerrungen, umsetzen und technische Gestaltungsanforderungen erfüllen, um ein angemessenes Niveau an Leistung, Vorhersagbarkeit, Interpretierbarkeit, Korrigierbarkeit, Sicherheit und Cybersicherheit zu gewährleisten, und sie sollten Umweltstandards einhalten. Diese Verpflichtungen sollten durch Normen ergänzt werden. Außerdem sollten für Basismodelle Informationspflichten gelten und alle erforderlichen technischen Unterlagen für potenzielle nachgeschaltete Anbieter erstellt werden müssen, damit diese ihren Verpflichtungen aus dieser Verordnung nachkommen können. Generative Basismodelle sollten Transparenz über die Tatsache sicherstellen, dass die Inhalte von einem KI-System und nicht von Menschen erzeugt werden. Diese spezifischen Anforderungen und Verpflichtungen laufen nicht darauf hinaus, Basismodelle als Hochrisiko-KI-Systeme zu betrachten, sondern sollen sicherstellen, dass die Ziele dieser Verordnung, nämlich ein hohes Maß an Schutz der Grundrechte, Gesundheit und Sicherheit, der Umwelt, der Demokratie und der Rechtsstaatlichkeit, erreicht werden. Vortrainierte Modelle, die für eine enger gefasste, weniger allgemeine und begrenzte Reihe von Anwendungen entwickelt wurden und nicht an ein breites Spektrum von Aufgaben angepasst werden können, wie z. B. einfache Mehrzweck-KI-Systeme, sollten für die Zwecke dieser Verordnung nicht als Basismodelle betrachtet werden, da sie besser interpretierbar sind und ihr Verhalten weniger unvorhersehbar ist.
- (60h) Angesichts der Art der Basismodelle fehlt es an Fachwissen im Bereich der Konformitätsbewertung, und die Methoden zur Prüfung durch Dritte befinden sich noch in der Entwicklung. Die Branche selbst entwickelt daher neue Methoden zur Bewertung von Basismodellen, die zum Teil das Ziel der Prüfung erfüllen (z. B. Modellevaluierung, Red-Teaming oder Verifizierungs- und Validierungstechniken des maschinellen Lernens). Diese internen Bewertungen für Basismodelle sollten breit anwendbar sein (z. B. unabhängig von

Vertriebskanälen, Modalität und Entwicklungsmethoden), um die für solche Modelle spezifischen Risiken unter Berücksichtigung der modernsten Praktiken der Branche anzugehen, und sich auf die Entwicklung eines ausreichenden technischen Verständnisses und einer ausreichenden Kontrolle über das Modell, das Management vernünftigerweise vorhersehbarer Risiken und eine umfassende Analyse und Prüfung des Modells durch geeignete Maßnahmen, z. B. durch die Einbeziehung unabhängiger Gutachter, konzentrieren. Da Basismodelle eine neue und schnell voranschreitende Entwicklung im Bereich der künstlichen Intelligenz sind, ist es angebracht, dass die Kommission und das Amt für künstliche Intelligenz den Rechts- und Verwaltungsrahmen für solche Modelle und insbesondere für generative KI-Systeme, die auf solchen Modellen beruhen, überwachen und regelmäßig bewerten, da diese erhebliche Fragen im Zusammenhang mit der Erzeugung von Inhalten, die gegen das Unionsrecht und die Vorschriften zum Urheberrecht verstoßen, und mit möglichem Missbrauch aufwerfen. Es sollte klargestellt werden, dass diese Verordnung das Unionsrecht zum Urheberrecht und zu verwandten Schutzrechten, einschließlich der Richtlinien 2001/29/EG, 2004/48/EG und (EU) 2019/790 des Europäischen Parlaments und des Rates, unberührt lassen sollte.

- (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 Rates⁵² sollte den Anbietern den Nachweis der Konformität mit den Anforderungen dieser Verordnung ermöglichen. Um die Wirksamkeit von Normen als politisches Instrument für die Union sicherzustellen und angesichts der Bedeutung von Normen für die Sicherstellung der Konformität mit den Anforderungen dieser Verordnung und für die Wettbewerbsfähigkeit von Unternehmen, ist es notwendig, für eine ausgewogene Interessenvertretung zu sorgen, indem alle relevanten Interessengruppen in die Entwicklung von Normen einbezogen werden. Der Normungsprozess sollte in Bezug auf die an den Normungstätigkeiten beteiligten juristischen und natürlichen Personen transparent sein.
- (61a) Um die Einhaltung der Vorschriften zu erleichtern, sollten die ersten Normungsaufträge von der Kommission spätestens zwei Monate nach Inkrafttreten dieser Verordnung erteilt werden. Dies sollte die Rechtssicherheit verbessern und dadurch Investitionen und Innovationen im Bereich der KI sowie die Wettbewerbsfähigkeit und das Wachstum des Unionsmarktes fördern und gleichzeitig die Multi-Stakeholder-Governance voranbringen, bei der alle relevanten europäischen Interessenträger wie das Amt für KI, die europäischen Normungsorganisationen und die im Rahmen des einschlägigen sektoralen Unionsrechts eingerichteten Gremien oder Sachverständigengruppen sowie die Industrie, KMU, Start-ups, die Zivilgesellschaft, Forscher

⁵² 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 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).

und Sozialpartner vertreten sind, und sollte letztlich die globale Zusammenarbeit bei der Normung im Bereich der KI in einer Weise erleichtern, die mit den Werten der Union vereinbar ist. Bei der Ausarbeitung des Normungsauftrags sollte die Kommission das Amt für KI und das KI-Beratungsforum konsultieren, um einschlägiges Fachwissen einzuholen.

- (61b) Wenn KI-Systeme am Arbeitsplatz zum Einsatz kommen sollen, dürfen die harmonisierten Normen nur technische Spezifikationen und Verfahren betreffen.
- (61c) Die Kommission sollte in der Lage sein, unter bestimmten Bedingungen gemeinsame Spezifikationen anzunehmen, wenn es keine einschlägige harmonisierte Norm gibt oder um spezifische Grundrechtsbelange zu berücksichtigen. Während des gesamten Entwurfsprozesses sollte die Kommission regelmäßig das Amt für KI und sein Beratungsforum, die europäischen Normungsorganisationen und die im Rahmen des einschlägigen sektoralen Unionsrechts eingerichteten Gremien oder Sachverständigengruppen sowie die einschlägigen Interessenträger wie Industrie, KMU, Start-ups, Zivilgesellschaft, Forscher und Sozialpartner konsultieren.
- (61d) Bei der Annahme gemeinsamer Spezifikationen sollte die Kommission eine regulatorische Abstimmung der KI mit gleichgesinnten globalen Partnern anstreben. Dies ist der Schlüssel zur Förderung von Innovation und grenzüberschreitenden Partnerschaften im Bereich der KI, da die Koordinierung mit gleichgesinnten Partnern in internationalen Normungsgremien von großer Bedeutung ist.
- (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. Um das Vertrauen in die Wertschöpfungskette zu stärken und den Unternehmen Gewissheit über die Leistungsfähigkeit ihrer Systeme zu geben, sollten Dritte, die KI-Komponenten anbieten, die Möglichkeit haben, freiwillig eine Konformitätsbewertung durch Dritte zu beantragen.
- (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] gewährleistet 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 Komplexität von Hochrisiko-KI-Systemen und der damit verbundenen Risiken ist es unerlässlich, eine angemessenere Kapazität für die Anwendung der Konformitätsbewertung durch Dritte für Hochrisiko-KI-Systeme zu entwickeln. In Anbetracht der derzeitigen Erfahrung professioneller dem Inverkehrbringen vorgeschalteter Zertifizierer im Bereich der Produktsicherheit und der unterschiedlichen Art der damit verbundenen Risiken empfiehlt es sich jedoch, 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, oder von KI-Systemen, die dazu bestimmt sind, auf der Grundlage biometrischer oder biometriegestützter Daten Rückschlüsse auf persönliche Merkmale natürlicher Personen zu ziehen, einschließlich Systemen zur Erkennung von Emotionen, bei denen die Beteiligung einer notifizierten Stelle an der Konformitätsbewertung vorgesehen werden sollte, soweit diese Systeme nicht ganz verboten sind.
- (65) Damit KI-Systeme, falls vorgeschrieben, Konformitätsbewertungen 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 und Mindestanforderungen an die Cybersicherheit. Die Mitgliedstaaten sollten die Benennung einer ausreichenden Zahl von Konformitätsbewertungsstellen fördern, um eine zeitnahe Zertifizierung zu ermöglichen. Die Verfahren zur Bewertung, Benennung, Notifizierung und Überwachung von Konformitätsbewertungsstellen sollten in den Mitgliedstaaten so einheitlich wie möglich angewandt werden, um administrative Grenzhindernisse zu beseitigen und dafür zu sorgen, dass das Potenzial des Binnenmarktes ausgeschöpft wird.
- (65a) Im Einklang mit den Verpflichtungen der EU im Rahmen des Übereinkommens der Welthandelsorganisation über technische Handelshemmnisse ist es angemessen, die Akzeptanz von Prüfergebnissen zu erhöhen, die von den zuständigen Konformitätsbewertungsstellen unabhängig von dem Gebiet, in dem diese niedergelassen sind, erstellt werden, wenn dies für den Nachweis der Konformität mit den geltenden Anforderungen der Verordnung erforderlich ist. Die Kommission sollte aktiv mögliche internationale Instrumente zu diesem Zweck prüfen und insbesondere den Abschluss von Abkommen über die gegenseitige Anerkennung mit Ländern anstreben, die sich auf einem vergleichbaren

technischen Entwicklungsstand befinden und kompatible Konzepte für die KI und die Konformitätsbewertung haben.

- (66) Im Einklang mit dem allgemein anerkannten Begriff der wesentlichen Änderung von Produkten, für die Harmonisierungsrechtsvorschriften der Union gelten, ist es angebracht, dass ein Hochrisiko-KI-System einer neuen Konformitätsbewertung unterzogen wird, wenn eine ungeplante Änderung eintritt, die über kontrollierte oder vom Anbieter vorher festgelegte Änderungen, einschließlich kontinuierlicher Lernprozesse, hinausgeht und ein neues inakzeptables Risiko schaffen und die Einhaltung dieser Verordnung durch das Hochrisiko-KI-System erheblich 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. Aus allgemeinen Sicherheitsgründen und zum Schutz vor aufkommenden Bedrohungen infolge von Systemmanipulationen sollte das Gleiche für Aktualisierungen des KI-Systems gelten, sofern sie keine wesentliche Änderung darstellen.
- (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. Bei physischen Hochrisiko-KI-Systemen sollte eine physische CE-Kennzeichnung angebracht werden, die durch eine digitale CE-Kennzeichnung ergänzt werden kann. Bei rein digitalen Hochrisiko-KI-Systemen sollte eine digitale CE-Kennzeichnung verwendet werden. 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, die Umwelt und den Klimawandel und für die Gesellschaft insgesamt von entscheidender Bedeutung sein. Es ist daher angebracht, dass die Mitgliedstaaten aus außergewöhnlichen Gründen, des Schutzes des Lebens und der Gesundheit natürlicher Personen und des Schutzes, des Umweltschutzes und des Schutzes der kritischen Infrastruktur 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 und ihre Basismodelle in einer von der Kommission einzurichtenden und zu verwaltenden EU-Datenbank zu registrieren. Diese Datenbank sollte frei und öffentlich

zugänglich, leicht verständlich und maschinenlesbar sein. Die Datenbank sollte außerdem benutzerfreundlich und leicht navigierbar sein und zumindest Suchfunktionen enthalten, die es der Öffentlichkeit ermöglichen, die Datenbank nach bestimmten Hochrisikosystemen, Standorten, Risikokategorien gemäß Anhang IV und Schlüsselwörtern zu durchsuchen. Bereitsteller, die Behörden oder Organe, Einrichtungen, Ämter und Agenturen der Union sind, oder Bereitsteller, die in ihrem Namen handeln, sowie Bereitsteller, die Unternehmen sind, die gemäß der Verordnung (EU) 2022/1925 als Torwächter benannt wurden, sollten sich vor der ersten Inbetriebnahme oder Verwendung eines Hochrisiko-KI-Systems sowie nach jeder wesentlichen Änderung ebenfalls in der EU-Datenbank registrieren. Andere Betreiber sollten berechtigt sein, dies freiwillig zu tun. Jede wesentliche Änderung von Hochrisiko-KI-Systemen muss ebenfalls in der EU-Datenbank registriert werden. Die Kommission sollte im Einklang mit der Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates⁵³ 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. Die Kommission sollte bei der Wahrnehmung ihrer Aufgaben als Verantwortliche für die EU-Datenbank die Risiken im Zusammenhang mit Cybersicherheit und Gefährdungen berücksichtigen. Um für ein Höchstmaß an Verfügbarkeit und Nutzung der Datenbank durch die Öffentlichkeit zu sorgen, sollte die Datenbank, einschließlich der über sie zur Verfügung gestellten Informationen, den Anforderungen der Richtlinie (EU) 2019/882 entsprechen.

- (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 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.

⁵³ 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).

- (71) Künstliche Intelligenz bezeichnet eine Reihe sich rasch entwickelnder Technologien, die eine 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 Innovationen fördernden, zukunftssicheren und gegenüber Störungen widerstandsfähigen Rechtsrahmen sicherzustellen, sollten die Mitgliedstaaten mindestens ein Reallabor für künstliche Intelligenz einrichten, um die Entwicklung und Erprobung innovativer KI-Systeme vor deren Inverkehrbringen oder anderweitiger Inbetriebnahme unter strenger Regulierungsaufsicht zu erleichtern. Es ist in der Tat wünschenswert, dass die Einrichtung von Reallaboren, deren Einrichtung derzeit im Ermessen der Mitgliedstaaten liegt, in einem nächsten Schritt anhand festgelegter Kriterien verbindlich gemacht wird. Dieses obligatorische Reallabor könnte auch gemeinsam mit einem oder mehreren anderen Mitgliedstaaten eingerichtet werden, sofern dieses Reallabor die jeweilige nationale Ebene der beteiligten Mitgliedstaaten abdecken würde. Zusätzliche Reallabore können außerdem auf verschiedenen Ebenen, auch zwischen Mitgliedstaaten, eingerichtet werden, um die grenzüberschreitende Zusammenarbeit und Synergien zu erleichtern. Mit Ausnahme des obligatorischen Reallabors auf nationaler Ebene sollten die Mitgliedstaaten ferner die Möglichkeit haben, virtuelle oder hybride Reallabore einzurichten. Alle Reallabore sollten sowohl physische als auch virtuelle Produkte abdecken können. Die einrichtenden Behörden sollten auch dafür Sorge tragen, dass die Reallabore über angemessene finanzielle und personelle Ressourcen für ihren Betrieb verfügen.
- (72) Die Ziele der Reallabore sollten für die einrichtenden Behörden darin bestehen, ihr Verständnis der technischen Entwicklungen zu verbessern, die Überwachungsmethoden zu verbessern und den Entwicklern und Anbietern von KI-Systemen Leitlinien an die Hand zu geben, um die Einhaltung der Vorschriften dieser Verordnung oder gegebenenfalls anderer geltender Rechtsvorschriften der Union und der Mitgliedstaaten sowie der Charta der Grundrechte zu erreichen, und für die potenziellen Anbieter darin bestehen, die Erprobung und Entwicklung innovativer Lösungen im Zusammenhang mit KI-Systemen in der dem Inverkehrbringen vorgelagerten Phase zu ermöglichen und zu erleichtern, um die Rechtssicherheit zu verbessern, mehr regulatorisches Lernen durch die einrichtenden Behörden in einem kontrollierten Umfeld zu ermöglichen, um bessere Leitlinien zu entwickeln und mögliche künftige Verbesserungen des Rechtsrahmens im Rahmen des ordentlichen Gesetzgebungsverfahrens zu ermitteln. Alle erheblichen Risiken, die bei der Entwicklung und Erprobung solcher KI-Systeme festgestellt werden, sollten die unverzügliche Risikominderung und, falls diese fehlschlägt, die Aussetzung des Entwicklungs- und Erprobungsprozesses nach sich ziehen, bis diese Risikominderung erfolgt ist. 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 Mitgliedstaaten sollten dafür Sorge tragen, dass Reallabore in der gesamten Union weithin verfügbar sind, wobei die Teilnahme

freiwillig bleiben sollte. Insbesondere muss sichergestellt werden, dass KMU und Start-up-Unternehmen einen einfachen Zugang zu diesen Reallaboren erhalten und aktiv in die Entwicklung und Erprobung innovativer KI-Systeme einbezogen werden und sich daran beteiligen, damit sie mit ihrem Know-how und ihrer Erfahrung einen Beitrag leisten können.

- (72a) Die vorliegende Verordnung sollte nur unter bestimmten Voraussetzungen 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 potenziellen Anbieter des Reallabors 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, die Gesundheit, die Umwelt und die Grundrechte, die bei der Entwicklung und Erprobung im Reallabor auftreten können, zu mindern. Das Verhalten der potenziellen Anbieter des Reallabors sollte berücksichtigt werden, wenn die zuständigen Behörden über die vorübergehende oder dauerhafte Aussetzung ihrer Beteiligung am Reallabor entscheiden oder darüber, ob sie eine Geldbuße gemäß Artikel 83 Absatz 2 der Verordnung (EU) 2016/679 und Artikel 57 der Richtlinie (EU) 2016/680 verhängen.
- (72b) Um sicherzustellen, dass die künstliche Intelligenz für die Gesellschaft und die Umwelt von Nutzen ist, sollten die Mitgliedstaaten die Forschung und Entwicklung im Bereich von KI mit gesellschaftlichem und ökologischem Nutzen unterstützen und fördern, indem sie ausreichende Ressourcen bereitstellen, darunter staatliche Mittel und Unionsmittel, und Projekten, die von der Zivilgesellschaft getragen werden, vorrangigen Zugang zu Reallaboren gewähren. Diese Projekte sollten auf dem Grundsatz der interdisziplinären Zusammenarbeit zwischen KI-Entwicklern, Fachleuten in den Bereichen Gleichstellung und Nichtdiskriminierung, Barrierefreiheit und Verbraucher-, Umwelt- und digitale Rechte sowie Wissenschaftlern beruhen.
- (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 KI-Kompetenz, Sensibilisierungs- und Informationsmaßnahmen. Die Mitgliedstaaten nutzen entsprechende bestehende Kanäle und richten gegebenenfalls neue Kanäle für die Kommunikation mit KMU, Start-up-Unternehmen und anderen Innovatoren ein, um Orientierungshilfe zu bieten und Fragen zur Durchführung dieser Verordnung zu beantworten. Zu solchen bestehenden Kanälen könnten unter anderem die folgenden gehören: das Netzwerk von Computer-Notfallteams der Agentur der Europäischen Union für Cybersicherheit (ENISA), nationale Datenschutzbehörden, die KI-Abruf-Plattform, die europäischen Zentren für digitale

Innovation sowie andere durch EU-Programme finanzierte relevante Instrumente und die Erprobungs- und Versuchseinrichtungen, die von der Kommission und den Mitgliedstaaten auf nationaler oder EU-Ebene eingerichtet wurden/werden. Diese Kanäle arbeiten gegebenenfalls zusammen, um Synergien zu schaffen und eine Homogenität ihrer Leitlinien für Start-up-Unternehmen, KMU und Nutzer sicherzustellen. Darüber hinaus sind die besonderen Interessen und Bedürfnisse kleinerer Anbieter bei der Festlegung der Gebühren für die Konformitätsbewertung durch die notifizierten Stellen zu berücksichtigen. Die Kommission bewertet regelmäßig die Zertifizierungs- und Befolgungskosten für KMU und Start-up-Unternehmen, unter anderem durch transparente Konsultationen mit KMU, Start-up-Unternehmen und Nutzern, und arbeitet mit den Mitgliedstaaten zusammen, um diese Kosten zu senken. So können zum Beispiel 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. Mittlere Unternehmen, die kürzlich die Kategorie von der kleinen auf die mittlere Größe im Sinne des Anhangs der Empfehlung 2003/361/EG (Artikel 16) gewechselt haben, sollten während eines von den Mitgliedstaaten als angemessen erachteten Zeitraums Zugang zu diesen Initiativen und Orientierungshilfen haben, da diesen neuen mittleren Unternehmen mitunter die erforderlichen rechtlichen Mittel und Schulungsmöglichkeiten fehlen, um für ein angemessenes Verständnis und eine ordnungsgemäße Einhaltung der Bestimmungen zu sorgen.

- (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, 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 Fragmentierung zu vermeiden, für das optimale Funktionieren des Binnenmarkts zu sorgen, eine wirksame und harmonisierte Umsetzung dieser Verordnung sicherzustellen, ein hohes Maß an Vertrauenswürdigkeit und an Schutz für die Gesundheit und Sicherheit, die Grundrechte, die Umwelt, die Demokratie und die Rechtsstaatlichkeit in der gesamten Union in Bezug auf KI-Systeme zu erreichen, die nationalen Aufsichtsbehörden, die Organe, Einrichtungen, Ämter und Agenturen der Union in Angelegenheiten, die diese Verordnung betreffen, aktiv zu unterstützen und die Akzeptanz der künstlichen Intelligenz in der gesamten Union zu erhöhen, sollte ein Europäisches Amt für künstliche Intelligenz eingerichtet werden. Das Amt für künstliche Intelligenz sollte Rechtspersönlichkeit besitzen, in völliger Unabhängigkeit handeln, für eine Reihe von Beratungs- und Koordinierungsaufgaben zuständig sein und Stellungnahmen, Empfehlungen, Ratschläge oder Leitlinien zu Fragen im Zusammenhang mit der Umsetzung dieser Verordnung abgeben, und es sollte mit angemessenen Finanzmitteln und Personal ausgestattet sein. Die Mitgliedstaaten sollten gemeinsam mit der Kommission, dem EDSB, der FRA und der ENISA über den Verwaltungsrat des Amts für KI die strategische Leitung und Kontrolle des Amts für KI übernehmen. Ein Verwaltungsratsmitglied sollte für die Leitung der Tätigkeiten des Sekretariats des Amts für KI und für die Vertretung des Amts für KI verantwortlich sein. Interessenträger sollten sich im Wege eines Beratungsforums, das eine vielfältige und ausgewogene Vertretung von Interessenträgern sicherstellen und das Amt für KI in Angelegenheiten, die diese Verordnung betreffen, beraten sollte, formell an der Arbeit des Amts für KI beteiligen. Sollte sich die Einrichtung des Amts für KI als unzureichend erweisen, um eine vollständig kohärente Anwendung dieser Verordnung auf Unionsebene sowie effiziente grenzüberschreitende Durchsetzungsmaßnahmen zu gewährleisten, sollte die Einrichtung einer Agentur für KI in Betracht gezogen werden.
- (77) Jeder Mitgliedstaat sollte eine nationale Aufsichtsbehörde benennen, die die Anwendung und Umsetzung dieser Verordnung beaufsichtigt. Diese Behörde sollte zudem ihren Mitgliedstaat im Verwaltungsrat des Amts für KI vertreten, 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. Jede nationale Aufsichtsbehörde sollte bei der Erfüllung ihrer Aufgaben und Ausübung ihrer Befugnisse gemäß dieser Verordnung vollkommen unabhängig handeln.
- (77a) Die nationalen Aufsichtsbehörden sollten die Anwendung der Bestimmungen dieser Verordnung überwachen und zu ihrer einheitlichen Anwendung in der gesamten Union beitragen. Zu diesem Zweck sollten die nationalen Aufsichtsbehörden untereinander, mit den jeweils zuständigen nationalen Behörden, mit der Kommission und mit dem Amt für KI zusammenarbeiten.
- (77b) Das Mitglied oder die Bediensteten jeder nationalen Aufsichtsbehörde sollten gemäß dem Unionsrecht oder dem Recht der Mitgliedstaaten sowohl während ihrer Amts- beziehungsweise Dienstzeit als auch nach deren Beendigung verpflichtet sein, über alle vertraulichen

Informationen, die ihnen bei der Wahrnehmung ihrer Aufgaben oder der Ausübung ihrer Befugnisse bekannt geworden sind, Verschwiegenheit zu wahren. Während dieser Amtsbeziehungsweise Dienstzeit sollte diese Verschwiegenheitspflicht insbesondere für Geschäftsgeheimnisse und für die von natürlichen Personen gemeldeten Verstöße gegen diese Verordnung gelten.

- (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 oder sich weiterentwickeln, 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, einschließlich Rechtsvorschriften zum Schutz der Grundrechte und Verbraucherrechte, zu melden, die sich aus der Verwendung ihrer KI-Systeme ergeben, und geeignete Korrekturmaßnahmen zu ergreifen. Die Betreiber sollten zudem den zuständigen Behörden schwerwiegende Vorfälle oder Verstöße gegen nationales Recht und Unionsrecht, die sich aus der Verwendung ihrer KI-Systeme ergeben, melden, wenn sie Kenntnis von solchen schwerwiegenden Vorfällen oder Verstößen erlangen.
- (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. Für die Zwecke dieser Verordnung sollten die nationalen Aufsichtsbehörden als Marktüberwachungsbehörden für unter diese Verordnung fallende KI-Systeme fungieren, mit Ausnahme von KI-Systemen, die unter Anhang II dieser Verordnung fallen. Bei KI-Systemen, die unter die in Anhang II aufgeführten Rechtsakte fallen, sollten die nach diesen Rechtsakten zuständigen Behörden weiterhin die federführende Behörde sein. Die nationalen Aufsichtsbehörden und die in den in Anhang II aufgeführten Rechtsakten genannten zuständigen Behörden sollten bei Bedarf zusammenarbeiten. Gegebenenfalls sollten die in den in Anhang II aufgeführten Rechtsakten genannten zuständigen Behörden kompetente Mitarbeiter an die nationale Aufsichtsbehörde entsenden, um sie bei der Wahrnehmung ihrer Aufgaben zu unterstützen. Für die Zwecke dieser Verordnung sollten die nationalen Aufsichtsbehörden die gleichen Befugnisse und Pflichten haben wie die Marktüberwachungsbehörden gemäß der Verordnung (EU) 2019/1020. 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. Nachdem alle anderen angemessenen Möglichkeiten zur Bewertung/Überprüfung der Konformität ausgeschöpft wurden, sollte der nationalen Aufsichtsbehörde auf begründeten Antrag Zugang zu den Trainings-, Validierungs- und Testdatensätzen, dem trainierten Modell und dem Trainingsmodell des Hochrisiko-KI-Systems, einschließlich seiner relevanten Modellparameter und seiner Ausführungs-/Prozessumgebung, gewährt werden. Bei einfacheren Softwaresystemen, die unter diese Verordnung fallen und nicht auf trainierten Modellen beruhen, und wenn alle anderen Möglichkeiten zur Überprüfung der Konformität ausgeschöpft wurden, kann die nationale Aufsichtsbehörde auf begründeten Antrag hin ausnahmsweise Zugang zum Quellcode erhalten. Wurde der nationalen Aufsichtsbehörde gemäß dieser Verordnung Zugang zu den Trainings-, Validierungs- und Testdatensätzen gewährt, so sollte dieser Zugang durch geeignete technische Mittel und Instrumente erfolgen, einschließlich des Zugangs vor Ort und in Ausnahmefällen des Fernzugangs. Die nationale Aufsichtsbehörde sollte alle erhaltenen Informationen, einschließlich des Quellcodes, der Software und gegebenenfalls der Daten, als vertrauliche Informationen behandeln und die einschlägigen Rechtsvorschriften der Union zum Schutz des geistigen Eigentums und der Geschäftsgeheimnisse beachten. Die nationale Aufsichtsbehörde sollte alle erhaltenen Informationen nach Abschluss der Untersuchung löschen.

- (80) Das Unionsrecht zu Finanzdienstleistungen enthält 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 des Unionsrechts zu Finanzdienstleistungen zu gewährleisten, sollten die für die Beaufsichtigung und Durchsetzung des Unionsrechts zu 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 Rates⁵⁴ 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 Betreiber von

⁵⁴ 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).

Hochrisiko-KI-Systemen in Betracht gezogen werden, soweit diese Kreditinstitute betreffen, die unter die Richtlinie 2013/36/EU fallen.

- (80a) Angesichts der Ziele dieser Verordnung, nämlich einen gleichwertigen Schutz der Gesundheit, der Sicherheit und der Grundrechte natürlicher Personen sowie den Schutz der Rechtsstaatlichkeit und der Demokratie sicherzustellen, und unter Berücksichtigung, dass die Minderung der von KI-Systemen ausgehenden Risiken gegenüber diesen Rechten auf nationaler Ebene möglicherweise nicht ausreichend erreicht wird oder Gegenstand unterschiedlicher Auslegungen sein kann, was letztlich zu einem ungleichen Schutzniveau für natürliche Personen und zu einer Fragmentierung der Märkte führen könnte, sollten die nationalen Aufsichtsbehörden ermächtigt werden, gemeinsame Untersuchungen durchzuführen oder zur wirksamen Durchsetzung das in dieser Verordnung vorgesehene Schutzklauselverfahren der Union anzuwenden. Gemeinsame Untersuchungen sollten eingeleitet werden, wenn die nationalen Aufsichtsbehörden hinreichende Gründe zu der Annahme haben, dass es sich bei einem Verstoß gegen diese Verordnung um einen weitverbreiteten Verstoß oder einen weitverbreiteten Verstoß mit unionsweiter Dimension handelt, oder wenn das KI-System oder das Basismodell ein Risiko darstellt, das mindestens 45 Millionen Personen in mehr als einem Mitgliedstaat betrifft oder betreffen könnte.
- (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 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 für Hochrisiko-KI-Systeme 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 Rates⁵⁵ als Sicherheitsnetz dienen.

⁵⁵ 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).

- (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 Transparenz und Offenheit anstreben und gleichzeitig die Vertraulichkeit der im Rahmen der Durchführung ihrer Tätigkeiten erlangten Informationen und Daten wahren, indem sie technische und organisatorische Maßnahmen zum Schutz der Sicherheit und Vertraulichkeit der im Rahmen der Durchführung ihrer Tätigkeiten erlangten Informationen, unter anderem für Rechte des geistigen Eigentums und öffentliche und nationale Sicherheitsinteressen, ergreifen. Für den Fall, dass die Tätigkeiten der Kommission, der zuständigen nationalen Behörden und der notifizierten Stellen gemäß dieser Verordnung zu einer Verletzung von Rechten des geistigen Eigentums führen, sollten die Mitgliedstaaten geeignete Maßnahmen und Rechtsbehelfe vorsehen, um die Durchsetzung der Rechte des geistigen Eigentums in Anwendung der Richtlinie 2004/48/EG zu gewährleisten.
- (84) Die Einhaltung dieser Verordnung sollte durch die Verhängung von Geldbußen durch die nationale Aufsichtsbehörde bei der Durchführung von Verfahren nach dem in dieser Verordnung festgelegten Verfahren durchsetzbar sein. 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. Um die verwaltungsrechtlichen Sanktionen für Verstöße gegen diese Verordnung zu verschärfen und zu harmonisieren, sollten die Obergrenzen für die Festsetzung der Geldbußen bei bestimmten Verstößen festgelegt werden. Bei der Bemessung der Höhe der Geldbußen sollten die zuständigen nationalen Behörden in jedem Einzelfall alle relevanten Umstände der jeweiligen Situation berücksichtigen, insbesondere die Art, die Schwere und die Dauer des Verstoßes und seiner Folgen sowie die Größe des Anbieters, vor allem wenn es sich bei diesem um ein KMU oder ein Start-up-Unternehmen handelt. Der Europäische Datenschutzbeauftragte sollte befugt sein, gegen Organe, Einrichtungen und sonstige Stellen der Union, die in den Anwendungsbereich dieser Verordnung fallen, Geldbußen zu verhängen. Die Sanktionen und Gerichtskosten gemäß dieser Verordnung sollten nicht Gegenstand von Vertragsklauseln oder anderen Vereinbarungen sein.
- (84a) Da die Rechte und Freiheiten natürlicher und juristischer Personen und Gruppen natürlicher Personen durch KI-Systeme ernsthaft beeinträchtigt werden können, ist es von wesentlicher Bedeutung, dass natürliche und juristische Personen oder Gruppen natürlicher Personen sinnvollen Zugang zu Melde- und Rechtsbehelfsmechanismen haben und das Recht auf Zugang zu verhältnismäßigen und wirksamen Rechtsbehelfen haben. Sie sollten in der Lage sein, Verstöße gegen diese Verordnung ihrer nationalen Aufsichtsbehörde zu melden, und das Recht haben, eine Beschwerde gegen die Anbieter oder Betreiber von KI-Systemen einzureichen. Gegebenenfalls sollten die Betreiber interne Beschwerdemechanismen bereitstellen, die von natürlichen und juristischen Personen oder Gruppen von natürlichen Personen genutzt werden können. Unbeschadet anderer verwaltungsrechtlicher oder außergerichtlicher Rechtsbehelfe sollten natürliche und juristische Personen und Gruppen

natürlicher Personen auch das Recht auf einen wirksamen gerichtlichen Rechtsbehelf in Bezug auf eine sie betreffende rechtsverbindliche Entscheidung einer nationalen Aufsichtsbehörde oder, wenn die nationale Aufsichtsbehörde eine Beschwerde nicht bearbeitet, den Beschwerdeführer nicht über den Fortgang oder das vorläufige Ergebnis der eingereichten Beschwerde informiert oder ihrer Verpflichtung, eine endgültige Entscheidung zu treffen, nicht nachkommt, in Bezug auf die Beschwerde haben.

- (84b) Betroffene Personen sollten stets darüber informiert werden, dass sie dem Einsatz eines Hochrisiko-KI-Systems ausgesetzt sind, wenn Betreiber ein Hochrisiko-KI-System zur Unterstützung bei der Entscheidungsfindung einsetzen oder Entscheidungen in Bezug auf natürliche Personen treffen. Auf der Grundlage dieser Information können betroffene Personen ihr Recht auf eine Erklärung gemäß dieser Verordnung wahrnehmen. Wenn die Betreiber betroffenen Personen im Rahmen dieser Verordnung eine Erklärung bieten, sollten sie den Sachverstand und die Kenntnisse des Durchschnittsverbrauchers oder der Durchschnittsperson berücksichtigen.
- (84c) Das Unionsrecht zum Schutz von Hinweisgebern (Richtlinie (EU) 2019/1937) gilt uneingeschränkt für Wissenschaftler, Konstrukteure, Entwickler, Projektmitarbeiter, Prüfer, Produktmanager, Ingenieure und Wirtschaftsakteure, die Kenntnis von Informationen über Verstöße gegen das Unionsrecht durch einen Anbieter eines KI-Systems oder durch sein KI-System erlangen.
- (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 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 Rechtsetzung⁵⁶ niedergelegt wurden. An diesen Konsultationen sollte eine ausgewogene Auswahl von Interessenträgern teilnehmen, einschließlich Verbraucherorganisationen, Verbänden, die betroffene Personen vertreten, Vertretern von Unternehmen aus verschiedenen Sektoren und von unterschiedlicher Größe sowie Forschern und Wissenschaftlern. Um insbesondere für eine gleichberechtigte Beteiligung an der Vorbereitung delegierter Rechtsakte zu sorgen, erhalten das Europäische Parlament und der

⁵⁶ ABl. L 123 vom 12.5.2016, S. 1.

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.

- (85a) Angesichts der rasanten technologischen Entwicklungen und des erforderlichen technischen Fachwissens bei der Bewertung von Hochrisiko-KI-Systemen sollte die Kommission die Durchführung dieser Verordnung, insbesondere die verbotenen KI-Systeme, die Transparenzpflichten und die Liste der Bereiche und Anwendungsfälle mit hohem Risiko, regelmäßig, mindestens jedoch einmal jährlich, überprüfen und dabei das Amt für künstliche Intelligenz und die einschlägigen Interessenträger konsultieren.
- (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 Rates⁵⁷ 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.
- (87a) Da es nur wenige verlässliche Informationen über den Ressourcen- und Energieverbrauch, die Abfallproduktion und andere Umweltauswirkungen von KI-Systemen und der damit verbundenen IKT-Technologie, einschließlich Software, Hardware und insbesondere Rechenzentren, gibt, sollte die Kommission eine angemessene Methodik zur Messung der Umweltauswirkungen und der Wirksamkeit dieser Verordnung im Hinblick auf die Umwelt- und Klimaziele der Union einführen.
- (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

⁵⁷ 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).

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 18. Juni 2021 eine Stellungnahme abgegeben—

HABEN FOLGENDE VERORDNUNG ERLASSEN:

IV. ARTIKEL DER VERORDNUNG

TITEL I

ALLGEMEINE BESTIMMUNGEN

ARTIKEL 1

GEGENSTAND

1. Ziel dieser Verordnung ist es, die Einführung von menschenzentrierter und vertrauenswürdiger künstlicher Intelligenz zu fördern und ein hohes Maß an Schutz der Gesundheit, der Sicherheit, der Grundrechte, der Demokratie und der Rechtsstaatlichkeit sowie der Umwelt vor schädlichen Auswirkungen von Systemen der künstlichen Intelligenz in der Union sicherzustellen und gleichzeitig die Innovation zu fördern.

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;
- 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 bestimmte KI-Systeme;
- e) Vorschriften für die Marktbeobachtung sowie die Steuerung und Durchsetzung der und Marktüberwachung.
 - ea) Maßnahmen zur Innovationsförderung mit besonderem Augenmerk auf KMU und Start-ups einschließlich der Einrichtung von Reallaboren und gezielter Maßnahmen zur Verringerung des Regelungsaufwands für KMU und Start-ups;
 - eb) Vorschriften für die Einrichtung und Arbeitsweise des Amtes für künstliche Intelligenz der Union

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) Betreiber von KI-Systemen, die ihren Sitz in der Union haben oder die sich in der Union befinden;
 - c) Anbieter und Betreiber von KI-Systemen, die ihren Sitz in einem Drittland haben oder die in einem Drittland niedergelassen oder ansässig sind, in dem entweder das Recht eines Mitgliedsstaates aufgrund eines internationalen Rechts gilt oder wenn das vom System hervorgebrachte Ergebnis in der Union verwendet werden soll.
 - ca) Anbieter, die die in Artikel 5 genannten KI-Systeme außerhalb der Union in Verkehr bringen oder in Betrieb nehmen, wenn der Anbieter oder Händler dieser Systeme in der Union ansässig ist;
 - cb) Einführer und Händler von KI-Systemen sowie bevollmächtigte Vertreter von Anbietern von KI-Systemen, wenn diese Einführer, Händler oder bevollmächtigten Vertreter ihre Niederlassung in der Union haben oder dort ansässig sind;
 - cc) betroffene Personen im Sinne von Artikel 3 Absatz 8a, die in der Union ansässig sind und deren Gesundheit, Sicherheit oder Grundrechte durch die Verwendung eines KI-Systems, das in der Union in Verkehr gebracht oder in Betrieb genommen wird, beeinträchtigt werden.
- (2) Für Hochrisiko-KI-Systeme, die Sicherheitskomponenten von Produkten oder Systemen oder selbst Produkte oder Systeme sind und die in den Anwendungsbereich der in Anhang II Abschnitt B aufgeführten Harmonisierungsrechtsvorschriften fallen, gilt nur Artikel 84 dieser Verordnung.
- (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 Kooperationen oder Übereinkünfte im Bereich der Strafverfolgung und justiziellen Zusammenarbeit mit der Union oder mit einem oder mehreren Mitgliedstaaten verwenden und Gegenstand eines Beschlusses der Kommission sind, der gemäß Artikel 36 der Richtlinie (EU) 2016/680 oder Artikel 45 der Verordnung (EU) 2016/679 (Angemessenheitsbeschluss)

erlassen wurde, oder Teil eines internationalen Abkommens sind, das zwischen der Union und dem betreffenden Drittland oder der internationalen Organisation gemäß Artikel 218 AEUV geschlossen wurde und angemessene Garantien in Bezug auf den Schutz der Privatsphäre und der Grundrechte und -freiheiten natürlicher Personen bietet;

- (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 Rates⁵⁸ [*die durch die entsprechenden Bestimmungen des Gesetzes über digitale Dienste ersetzt werden sollen*] bleibt von dieser Verordnung unberührt.
- (5a) Das Unionsrecht zum Schutz personenbezogener Daten, der Privatsphäre und der Vertraulichkeit der Kommunikation gilt für die Verarbeitung personenbezogener Daten im Zusammenhang mit den in dieser Verordnung festgelegten Rechten und Pflichten. Diese Verordnung berührt nicht die Verordnungen (EU) 2016/679 und (EU) 2018/1725 sowie die Richtlinien 2002/58/EG und (EU) 2016/680, unbeschadet der in Artikel 10 Absatz 5 und Artikel 54 der vorliegenden Verordnung vorgesehenen Regelungen;
- (5b) Diese Verordnung berührt nicht die Vorschriften anderer Rechtsakte der Union zum Verbraucherschutz und zur Produktsicherheit;
- (5c) Diese Verordnung hindert die Mitgliedstaaten oder die Union nicht daran, Rechts- oder Verwaltungsvorschriften beizubehalten oder einzuführen, die für die Arbeitnehmer im Hinblick auf den Schutz ihrer Rechte bei der Verwendung von KI-Systemen durch die Arbeitgeber vorteilhafter sind, oder die Anwendung von Tarifverträgen zu fördern oder zuzulassen, die für die Arbeitnehmer vorteilhafter sind.
- (5d) Diese Verordnung gilt nicht für Forschungs-, Test- und Entwicklungstätigkeiten in Bezug auf ein KI-System, bevor dieses System in Verkehr gebracht oder in Betrieb genommen wird, vorausgesetzt, dass diese Tätigkeiten unter Wahrung der Grundrechte und des geltenden Unionsrechts durchgeführt werden. Die Kommission wird ermächtigt, delegierte Rechtsakte gemäß Artikel 73 zu erlassen, die die Anwendung dieses Absatzes präzisieren, um diese Ausnahme zu spezifizieren und ihren bestehenden und potenziellen Missbrauch zu verhindern. Das Amt für künstliche Intelligenz stellt Leitlinien für die Steuerung von Forschung und Entwicklung gemäß Artikel 56 zur Verfügung, die auch darauf abzielen, die Anwendung dieser Leitlinien durch die nationalen Aufsichtsbehörden zu koordinieren;
- (5e) Diese Verordnung gilt nicht für KI-Komponenten, die unter freien Lizenzen und Open-Source-Lizenzen bereitgestellt werden, es sei denn, sie werden von einem Anbieter als Teil eines Hochrisiko-KI-Systems oder eines KI-Systems, das unter Titel II oder IV fällt, in Verkehr gebracht oder in Betrieb genommen. Diese Ausnahmeregelung gilt nicht für Basismodelle im Sinne von Artikel 3.

⁵⁸ 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).

ARTIKEL 3
BEGRIFFSBESTIMMUNG

Für die Zwecke dieser Verordnung bezeichnet der Ausdruck

1. „System der künstlichen Intelligenz“ (KI-System) ein maschinengestütztes System, das so konzipiert ist, dass es mit unterschiedlichem Grad an Autonomie operieren kann und das für explizite oder implizite Ziele Ergebnisse wie Vorhersagen, Empfehlungen oder Entscheidungen hervorbringen kann, die das physische oder virtuelle Umfeld beeinflussen;
- 1a. „Risiko“ die Kombination aus der Wahrscheinlichkeit des Auftretens eines Schadens und der Schwere dieses Schadens;
- 1b. „erhebliches Risiko“ ein Risiko, das aufgrund der Kombination von Schwere, Intensität, Eintrittswahrscheinlichkeit und Dauer seiner Auswirkungen sowie seiner Eigenschaft, eine Einzelperson, eine Vielzahl von Personen oder eine bestimmte Personengruppe zu beeinträchtigen, erheblich ist;
- 1c. „Basismodell“ ein KI-Systemmodell, das auf einer breiten Datenbasis trainiert wurde, auf eine allgemeine Ausgabe ausgelegt ist und an eine breite Palette unterschiedlicher Aufgaben angepasst werden kann;
- 1d. „KI-System mit allgemeinem Verwendungszweck“ ein KI-System, das in einem breiten Spektrum von Anwendungen eingesetzt und an diese angepasst werden kann, für die es nicht absichtlich und speziell entwickelt wurde;
- 1e. „große Trainingsläufe“ den Produktionsprozess eines leistungsstarken KI-Modells, der Rechenressourcen oberhalb einer sehr hohen Schwelle erfordert;
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;
4. „Betreiber“ 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 Betreiber, den Bevollmächtigten, den Einführer und den Händler;
- 8a. „betroffene Person“ jede natürliche Person oder Personengruppe, die einem KI- System unterliegt oder anderweitig davon betroffen ist;
9. „Inverkehrbringen“ die erstmalige Bereitstellung eines KI-Systems auf dem Unionsmarkt;
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 Betreiber 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 gemäß der vom Anbieter bereitgestellten Gebrauchsanweisung entspricht, die sich aber aus einem vernünftigerweise vorhersehbaren menschlichen Verhalten oder einer vernünftigerweise vorhersehbaren Interaktion mit anderen Systemen, einschließlich anderer KI-Systeme, ergeben kann;
14. „Sicherheitskomponente eines Produkts oder Systems“ einen Bestandteil eines Produkts oder Systems gemäß den in Anhang II aufgeführten Harmonisierungsrechtsvorschriften der Union, der eine Sicherheitsfunktion für dieses Produkt oder System erfüllt oder dessen Ausfall oder Störung die Gesundheit und Sicherheit von Personen gefährdet;
15. „Gebrauchsanweisung“ die Informationen, die der Anbieter bereitstellt, um den Betreiber insbesondere über die Zweckbestimmung und die ordnungsgemäße Verwendung eines KI-Systems sowie über die zu treffende Vorsichtsmaßnahmen 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 Betreibern bereits zur Verfügung gestellten KI-Systems an den Anbieter abzielt;
17. „Rücknahme eines KI-Systems“ jede Maßnahme, mit der verhindert werden soll, dass 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 für den Nachweis, 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 notifiziert wurde;
23. „wesentliche Änderung“ eine Änderung oder eine Reihe von Änderungen des KI-Systems nach dessen Inverkehrbringen oder Inbetriebnahme, die in der ursprünglichen Risikobewertung des Anbieters nicht vorgesehen oder geplant war und durch die die Konformität des KI-Systems mit den Anforderungen in Titel III Kapitel 2 dieser Verordnung beeinträchtigt wird oder die zu einer Änderung der Zweckbestimmung führt, für die das KI-System geprüft wurde;
24. „CE-Konformitätskennzeichnung“ (CE-Kennzeichnung) eine physische oder digitale Kennzeichnung, durch die ein Anbieter erklärt, dass ein KI-System oder ein Produkt mit einem eingebetteten 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 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 Unter- oder Überanpassung zu vermeiden; der Validierungsdatensatz ist ein separater Datensatz oder Teil des Trainingsdatensatzes mit fester oder variabler Aufteilung;
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“ biometrische Daten im Sinne der Begriffsbestimmung in Artikel 4 Nummer 14 der Verordnung (EU) 2016/679;
- 33a. „biometriegestützte Daten“ Daten, die sich aus einer spezifischen technischen Verarbeitung von physischen, physiologischen oder verhaltensbezogenen Signalen einer natürlichen Person ergeben;
- 33b. „biometrische Identifizierung“ die automatisierte Erkennung physischer, physiologischer, verhaltensbezogener und psychologischer menschlicher Merkmale zum Zwecke der Feststellung der Identität einer Person durch den Vergleich biometrischer Daten dieser Person mit gespeicherten biometrischen Daten von Personen in einer Datenbank (One-to-many-Identifizierung);
- 33c. „biometrische Überprüfung“ die automatisierte Überprüfung der Identität natürlicher Personen durch den Vergleich biometrischer Daten einer Person mit zuvor bereitgestellten biometrischen Daten (Eins-zu-Eins-Überprüfung, einschließlich Authentifizierung);
- 33d. „besondere Kategorien personenbezogener Daten“ die in Artikel 9 Absatz 1 der Verordnung (EU) 2016/679 aufgeführten Kategorien personenbezogener Daten;
34. „Emotionserkennungssystem“ ein KI-System, das dem Zweck dient, Emotionen, Gedanken, Geisteszustände oder Absichten von Einzelpersonen oder Gruppen auf der Grundlage ihrer biometrischen und biometriegestützten Daten festzustellen oder daraus abzuleiten;
35. „biometrische Kategorisierung“ die Zuordnung natürlicher Personen zu bestimmten Kategorien oder die Ableitung ihrer Merkmale und Attribute auf der Grundlage ihrer biometrischen oder biometriegestützten Daten oder der Daten, die aus diesen Daten abgeleitet werden können;
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

Betreiber des KI-Systems vorher weiß, ob die Person anwesend sein wird und identifiziert werden kann, mit Ausnahme von Verifizierungssystemen;

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 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 in öffentlichem oder privatem Besitz, unabhängig davon, ob dafür bestimmte Zugangsbedingungen gelten, und unabhängig von möglichen Kapazitätsbeschränkungen;
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 oder in deren Auftrag 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“ eine öffentliche (AM 69) 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 Verwaltungsrat des Büros für künstliche Intelligenz überträgt;
43. „zuständige nationale Behörde“ eine der nationalen Behörden, die für die Durchsetzung dieser Verordnung zuständig sind;
44. „schwerwiegender Vorfall“ ein Vorkommnis oder eine Fehlfunktion eines KI-Systems, das bzw. die 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,
 - ba) einen Verstoß gegen die durch das Unionsrecht geschützten Grundrechte,
 - bb) schwere Sach- oder Umweltschäden.
- 44a. „personenbezogene Daten“ personenbezogene Daten im Sinne des Artikels 4 Nummer 1 der Verordnung (EU) 2016/679;
- 44b. „nicht personenbezogene Daten“ Daten, die keine personenbezogenen Daten sind;
- 44c. „Profiling“ jede Form der automatisierten Verarbeitung personenbezogener Daten im Sinne von Artikel 4 Nummer 4 der Verordnung (EU) 2016/679 oder – im Falle von Strafverfolgungsbehörden – in Artikel 3 Nummer 4 der Richtlinie (EU) 2016/680 oder – im Falle von Organen, Einrichtungen und sonstigen Stellen der Union – in Artikel 3 Nummer 5 der Verordnung (EU) 2018/1725;
- 44d. „Deep Fake“ manipulierte oder künstliche Audio-, Bild- oder Videoinhalte, die fälschlicherweise den Anschein erwecken, authentisch oder wahrheitsgetreu zu sein, und die Darstellungen von Personen enthalten, die scheinbar Dinge sagen oder tun, die sie nicht gesagt oder getan haben, und die mit Hilfe von KI-Techniken, einschließlich maschinellen Lernens und Deep Learning, erstellt wurden;
- 44e. „weitverbreiteter Verstoß“ jede Handlung oder Unterlassung, die gegen das Unionsrecht verstößt, das die Interessen des Einzelnen schützt,
- a) die die kollektiven Interessen von Einzelpersonen in mindestens zwei weiteren Mitgliedstaaten als dem Mitgliedstaat schädigt oder zu schädigen droht, in dem
 - i) die Handlung oder die Unterlassung ihren Ursprung hatte oder stattfand,
 - ii) der betreffende Anbieter oder gegebenenfalls sein Bevollmächtigter niedergelassen ist oder
 - iii) der Betreiber niedergelassen ist, sofern der Verstoß vom Betreiber begangen wird;
 - b) Handlungen oder Unterlassungen, die gegen das Unionsrecht verstoßen, das die Interessen des Einzelnen schützt, die die kollektiven Interessen von Einzelpersonen geschädigt haben, schädigen oder schädigen könnten und die gemeinsame Merkmale aufweisen, einschließlich derselben rechtswidrigen Praxis und desselben verletzten Interesses, und die gleichzeitig auftreten und von demselben Betreiber in mindestens drei Mitgliedstaaten begangen werden;

- 44f. „weitverbreiteter Verstoß mit unionsweiter Dimension“ ein weitverbreiteter Verstoß, der die kollektiven Interessen von Einzelpersonen in mindestens zwei Dritteln der Mitgliedstaaten, die zusammen mindestens zwei Drittel der Bevölkerung der Union ausmachen, geschädigt hat oder zu schädigen droht;
- 44g. „Reallabor“ ein von einer Behörde eingerichtetes kontrolliertes Umfeld, das die sichere Entwicklung, Erprobung und Validierung innovativer KI-Systeme für einen begrenzten Zeitraum ermöglicht, bevor diese auf den Markt gebracht oder in Betrieb genommen werden, nach einem bestimmten Plan unter behördlicher Aufsicht;
- 44h. „kritische Infrastrukturen“ Objekte, Anlagen, Ausrüstung, Netze oder Systeme oder Teile eines Objekts, einer Anlage, Ausrüstung, eines Netzes oder eines Systems, die für die Erbringung eines wesentlichen Dienstes erforderlich sind, im Sinne von Artikel 2 Nummer 4 der Richtlinie (EU) 2022/2557;
- 44i. Bislang leer
- 44j. Bislang leer
- 44k. „Bewertung des sozialen Verhaltens“ die Bewertung oder Klassifizierung natürlicher Personen auf der Grundlage ihres sozialen Verhaltens, ihres sozioökonomischen Status oder bekannter oder vorhergesagter persönlicher oder charakterlicher Merkmale;
- 44l. „soziales Verhalten“ die Art und Weise, wie eine natürliche Person mit anderen natürlichen Personen oder der Gesellschaft interagiert und diese beeinflusst;
- 44m. „Stand der Technik“ den Entwicklungsstand der technischen Leistungsfähigkeit zu einem bestimmten Zeitpunkt in Bezug auf Produkte, Verfahren und Dienstleistungen, der auf den einschlägigen konsolidierten Erkenntnissen von Wissenschaft, Technik und Erfahrung beruht;
- 44n. „Testen unter realen Bedingungen“ das zeitlich begrenzte Testen eines KI-Systems für den vorgesehenen Zweck unter realen Bedingungen außerhalb eines Labors oder einer anderweitig simulierten Umgebung;

ARTIKEL 4A

ALLGEMEINE, FÜR ALLE KI-SYSTEME GELTENDE GRUNDSÄTZE

- (1) Alle Betreiber, die unter diese Verordnung fallen, setzen alles daran, KI-Systeme oder Basismodelle im Einklang mit den folgenden allgemeinen Grundsätzen zu entwickeln und zu nutzen, mit denen ein höchste Ansprüche erfüllender Rahmen geschaffen wird, mit dem ein kohärenter, auf den Menschen ausgerichteter Ansatz der Union für ethische und vertrauenswürdige künstliche Intelligenz gefördert wird, der uneingeschränkt mit der Charta und den Werten, auf die sich die Union gründet, im Einklang steht:

- a) „Menschliches Handeln und menschliche Aufsicht“ bedeutet, dass KI-Systeme als Werkzeug entwickelt und verwendet werden, das den Menschen dient, die Menschenwürde und die persönliche Autonomie achtet und so funktioniert, dass es von Menschen angemessen kontrolliert und überwacht werden kann.
 - b) „Technische Robustheit und Sicherheit“ bedeutet, dass KI-Systeme so entwickelt und verwendet werden, dass unbeabsichtigte und unerwartete Schäden minimiert werden und dass sie im Fall unbeabsichtigter Probleme robust und widerstandsfähig gegen Versuche sind, die Verwendung oder Leistung des KI-Systems so zu verändern, dass dadurch die unrechtmäßige Verwendung durch böswillige Dritte ermöglicht wird.
 - c) „Privatsphäre und Datenqualitätsmanagement“ bedeutet, dass KI-Systeme im Einklang mit den geltenden Vorschriften zum Schutz der Privatsphäre und zum Datenschutz entwickelt und verwendet werden und dabei Daten verarbeiten, die hohen Qualitäts- und Integritätsstandards genügen.
 - d) „Transparenz“ bedeutet, dass KI-Systeme so entwickelt und verwendet werden müssen, dass sie angemessen nachvollziehbar und erklärbar sind, wobei den Menschen bewusst gemacht werden muss, dass sie mit einem KI-System kommunizieren oder interagieren, und dass die Nutzer ordnungsgemäß über die Fähigkeiten und Grenzen des KI-Systems und die betroffenen Personen über ihre Rechte informiert werden müssen.
 - e) „Vielfalt, Diskriminierungsfreiheit und Fairness“ bedeutet, dass KI-Systeme in einer Weise entwickelt und verwendet werden, die unterschiedliche Akteure einbezieht und den gleichberechtigten Zugang, die Geschlechtergleichstellung und die kulturelle Vielfalt fördert, wobei diskriminierende Auswirkungen und unfaire Verzerrungen, die nach Unionsrecht oder nationalem Recht verboten sind, verhindert werden.
 - f) „Soziales und ökologisches Wohlergehen“ bedeutet, dass KI-Systeme in nachhaltiger und umweltfreundlicher Weise und zum Nutzen aller Menschen entwickelt und verwendet werden, wobei die langfristigen Auswirkungen auf den Einzelnen, die Gesellschaft und die Demokratie überwacht und bewertet werden.
- (2) Absatz 1 lässt die Verpflichtungen unberührt, die durch geltendes Unionsrecht und nationales Recht festgelegt sind. Bei Hochrisiko-KI-Systemen werden die allgemeinen Grundsätze durch die in den Artikeln 8 bis 15 und die in Titel III Kapitel 3 dieser Verordnung festgelegten Anforderungen von den Anbietern oder Betreibern umgesetzt und von ihnen eingehalten. Bei Basismodellen werden die allgemeinen Grundsätze durch die in den Artikeln 28 bis 28b festgelegten Anforderungen von den Anbietern umgesetzt und von ihnen eingehalten. Bei allen KI-Systemen kann die Anwendung der in Absatz 1 genannten Grundsätze je nach Fall durch die Bestimmungen von Artikel 28, Artikel 52 oder die Anwendung harmonisierter Normen, technischer Spezifikationen und Verhaltenskodizes gemäß Artikel 69 erreicht werden, ohne dass dadurch neue Verpflichtungen im Rahmen dieser Verordnung entstehen.

- (3) Die Kommission und das Amt für künstliche Intelligenz lassen diese Grundsätze in Standardisierungsanträge sowie in Empfehlungen einfließen, bei denen es sich um technische Anleitungen handelt, um Anbieter und Betreiber bei der Entwicklung und Nutzung von KI-Systemen zu unterstützen. Die europäischen Normungsorganisationen berücksichtigen die in Absatz 1 dieses Artikels genannten allgemeinen Grundsätze als ergebnisorientierte Ziele, wenn sie geeignete harmonisierte Normen für AI-Systeme mit hohem Risiko im Sinne von Artikel 40 Absatz 2b entwickeln.

ARTIKEL 4B

KI-KOMPETENZ

- (1) Bei der Durchführung dieser Verordnung fördern die Union und die Mitgliedstaaten Maßnahmen zur Entwicklung eines ausreichenden Niveaus an KI-Kompetenz, und zwar sektorübergreifend und unter Berücksichtigung der unterschiedlichen Bedürfnisse der jeweiligen Gruppen von Anbietern, Betreibern und betroffenen Personen, unter anderem durch Aus- und Weiterbildungs-, Qualifizierungs- und Umschulungsprogramme und unter Sicherstellung eines ausgewogenen Verhältnisses in Bezug auf Geschlecht und Alter, um eine demokratische Kontrolle von KI-Systemen zu ermöglichen.
- (2) Anbieter und Betreiber von KI-Systemen ergreifen Maßnahmen, um sicherzustellen, dass ihr Personal und andere Personen, die in ihrem Auftrag mit dem Betrieb und der Nutzung von KI-Systemen befasst sind, über ein ausreichendes Maß an KI-Kompetenz verfügen, wobei ihre technischen Kenntnisse, ihre Erfahrung, ihre Ausbildung und Schulung und der Kontext, in dem die KI-Systeme eingesetzt werden sollen, sowie die Personen oder Personengruppen, bei denen die KI-Systeme eingesetzt werden sollen, zu berücksichtigen sind.
- (3) Solche Maßnahmen zur Kompetenzsteigerung bestehen insbesondere darin, grundlegende Konzepte und Fähigkeiten über KI-Systeme und ihre Funktionsweise zu vermitteln, einschließlich der verschiedenen Arten von Produkten und Verwendungszwecke, ihrer Risiken und Vorteile.
- (4) Ein ausreichendes Maß an KI-Kompetenz trägt – falls angezeigt – dazu bei, dass Anbieter und Betreiber in der Lage sind, die Einhaltung und Durchsetzung dieser Verordnung sicherzustellen.

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 unterschweligen Beeinflussung außerhalb des Bewusstseins einer Person oder absichtlich manipulative oder täuschende Techniken einsetzt, mit dem Ziel oder der Folge, dass das Verhalten einer Person oder einer Gruppe von Personen, indem die Fähigkeit der Person, eine fundierte Entscheidung zu treffen, spürbar beeinträchtigt wird, wodurch die Person veranlasst wird, eine Entscheidung zu treffen, die sie andernfalls nicht getroffen hätte, und zwar in einer Weise, die dieser Person, einer anderen Person oder einer Gruppe von Personen erheblichen Schaden zufügt oder zufügen kann.

Das Verbot von KI-Systemen, die gemäß Unterabsatz 1 Techniken der unterschweligen Beeinflussung einsetzen, gilt nicht für KI-Systeme, die für anerkannte therapeutische Zwecke auf der Grundlage einer ausdrücklichen, nach Aufklärung erteilten Einwilligung der ihnen ausgesetzten Personen oder gegebenenfalls ihres gesetzlichen Vertreters verwendet werden sollen;

- b) das Inverkehrbringen, die Inbetriebnahme oder die Verwendung eines KI-Systems, das eine Schwäche oder Schutzbedürftigkeit einer Person oder einer bestimmten Gruppe von Personen einschließlich der Merkmale der bekannten oder vorhergesagten Persönlichkeitsmerkmale oder der sozialen oder wirtschaftlichen Situation der Person oder Gruppe von Personen, ihres Alters oder ihrer körperlichen oder geistigen Fähigkeiten ausnutzt, mit dem Ziel oder der Folge, das Verhalten dieser Person oder einer dieser Gruppe angehörenden Person in einer Weise wesentlich zu beeinflussen, die dieser Person oder einer anderen Person einen erheblichen Schaden zufügt oder zufügen kann;
- ba) das Inverkehrbringen, die Inbetriebnahme oder die Verwendung von Systemen zur biometrischen Kategorisierung, die natürliche Personen nach sensitiven oder geschützten Attributen oder Merkmalen oder auf der Grundlage von Rückschlüssen auf diese Attribute oder Merkmale kategorisieren. Dieses Verbot gilt nicht für KI-Systeme, die für anerkannte therapeutische Zwecke auf der Grundlage einer ausdrücklichen, nach Aufklärung erteilten Einwilligung der ihnen ausgesetzten Personen oder gegebenenfalls ihres gesetzlichen Vertreters verwendet werden.
- c) das Inverkehrbringen, die Inbetriebnahme oder die Verwendung von KI-Systemen zur Bewertung des sozialen Verhaltens oder Klassifizierung natürlicher Personen oder Gruppen von natürlichen Personen über einen bestimmten Zeitraum auf der Grundlage

ihres sozialen Verhaltens oder bekannter, abgeleiteter oder vorhergesagter persönlicher Eigenschaften oder Persönlichkeitsmerkmale, wobei die soziale Bewertung zu einem oder beiden der folgenden Ergebnisse führt:

- i) Schlechterstellung oder Benachteiligung bestimmter natürlicher Personen oder 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
- da) das Inverkehrbringen, die Inbetriebnahme oder die Verwendung von KI-Systemen zur Risikobeurteilung natürlicher Personen oder von Gruppen natürlicher Personen, um das Risiko einer natürlichen Person, straffällig zu werden oder erneut straffällig zu werden, einzuschätzen oder um das Auftreten oder die Wiederholung einer tatsächlichen oder potenziellen Straftat oder Ordnungswidrigkeit auf der Grundlage von Profilen natürlicher Personen oder der Bewertung von Persönlichkeitsmerkmalen, Eigenschaften, einschließlich des Standorts der Person, oder früheren kriminellen Verhaltens von natürlichen Personen oder Gruppen von natürlichen Personen vorherzusagen;
- db) das Inverkehrbringen, die Inbetriebnahme oder die Nutzung von KI-Systemen, die Datenbanken zur Gesichtserkennung durch das ungezielte Auslesen von Gesichtsbildern aus dem Internet oder von Überwachungsaufnahmen erstellen oder erweitern;
- dc) das Inverkehrbringen, die Inbetriebnahme oder die Nutzung von KI-Systemen zur Ableitung von Emotionen einer natürlichen Person in den Bereichen Strafverfolgung, Grenzmanagement, am Arbeitsplatz und in Bildungseinrichtungen;
- dd) die Inbetriebnahme oder Nutzung von KI-Systemen zur Analyse von aufgezeichnetem Bildmaterial öffentlich zugänglicher Räume durch Systeme zur nachträglichen biometrischen Fernidentifizierung, es sei denn, sie unterliegen einer vorgerichtlichen Genehmigung im Einklang mit dem Unionsrecht und sind für die gezielte Fahndung im Zusammenhang mit einer bestimmten schweren Straftat im Sinne von Artikel 83 Absatz 1 AEUV, die bereits zum Zweck der Strafverfolgung stattgefunden hat, unbedingt erforderlich.

- (1a) Dieser Artikel berührt nicht die Verbote, die gelten, wenn eine Praxis der künstlichen Intelligenz gegen ein anderes Unionsrecht verstößt, einschließlich des Unionsrechts zum Datenschutz, zur Diskriminierungsfreiheit, zum Verbraucherschutz oder zum Wettbewerb.

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 das KI-System ist selbst ein solches Produkt;
 - b) das Produkt, dessen Sicherheitskomponente gemäß Buchstabe a das KI-System ist, oder das KI-System selbst als Produkt muss einer Konformitätsbewertung durch Dritte in Bezug auf die Risiken für Gesundheit und Sicherheit 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 KI-Systeme, die unter einen oder mehrere der in Anhang III genannten kritischen Bereiche und Anwendungsfälle fallen, als hochriskant, wenn sie ein erhebliches Risiko für die Gesundheit, die Sicherheit oder die Grundrechte von natürlichen Personen darstellen. Fällt ein KI-System unter Anhang III Nummer 2, so gilt es als hochriskant, wenn es ein erhebliches Risiko für die Umwelt birgt.

Die Kommission legt sechs Monate vor Inkrafttreten dieser Verordnung nach Anhörung des Amtes für künstliche Intelligenz und der einschlägigen Interessenträger Leitlinien vor, in denen eindeutig festgelegt ist, unter welchen Umständen die Ergebnisse der in Anhang III genannten Systeme der künstlichen Intelligenz ein erhebliches Risiko für die Gesundheit, die Sicherheit oder die Grundrechte natürlicher Personen darstellen und in welchen Fällen dies nicht der Fall ist.

- (2a) Wenn Anbieter, die unter einen oder mehrere der in Anhang III genannten kritischen Bereiche und Anwendungsfälle fallen, der Ansicht sind, dass ihr KI-System kein erhebliches Risiko im Sinne von Absatz 2 darstellt, übermitteln sie der nationalen Aufsichtsbehörde eine begründete Mitteilung, dass sie nicht den Anforderungen von Titel III Kapitel 2 dieser Verordnung unterliegen. Wenn das KI-System in zwei oder mehr Mitgliedstaaten verwendet werden soll, ist diese Mitteilung an das Büro für künstliche Intelligenz zu richten. Unbeschadet des Artikels 65 überprüft die nationale Aufsichtsbehörde die Mitteilung und antwortet innerhalb von drei Monaten direkt oder über das Büro für künstliche Intelligenz, wenn sie der Ansicht ist, dass das KI-System falsch eingestuft wurde.
- (2b) Anbieter, die ihr KI-System fälschlicherweise als nicht den Anforderungen von Titel III Kapitel 2 dieser Verordnung unterliegend einstufen und es vor Ablauf der Einspruchsfrist der nationalen Aufsichtsbehörden auf den Markt bringen, werden gemäß Artikel 71 mit Geldbußen belegt.
- (2c) Die nationalen Aufsichtsbehörden legen dem Büro für künstliche Intelligenz jährlich einen Bericht vor, in dem sie die Anzahl der eingegangenen Meldungen, die betreffenden Hochrisikobereiche und die im Zusammenhang mit den eingegangenen Mitteilungen getroffenen Entscheidungen darlegen.

ARTIKEL 7

ÄNDERUNGEN DES ANHANGS III

- (1) Der Kommission wird die Befugnis übertragen, gemäß Artikel 73 delegierte Rechtsakte zur Änderung von Anhang III zu erlassen, um Bereiche oder Anwendungsfälle von Hochrisiko-KI-Systemen hinzuzufügen oder zu ändern, wenn diese ein erhebliches Risiko für die Gesundheit und Sicherheit darstellen oder nachteilige Auswirkungen auf die Grundrechte, die Umwelt oder die Demokratie und die Rechtsstaatlichkeit nach sich ziehen und dieses Risiko hinsichtlich seiner Schwere und Eintrittswahrscheinlichkeit dem Risiko eines Schadens oder nachteiliger Auswirkungen, das von den bereits in Anhang III genannten AI-Systemen mit hohem Risiko ausgeht, entspricht oder größer ist.
- (1a) Der Kommission wird ferner die Befugnis übertragen, delegierte Rechtsakte gemäß Artikel 73 zu erlassen, um Anwendungsfälle von KI-Systemen mit hohem Risiko aus der Liste in Anhang III zu streichen, wenn die in Absatz 1 genannten Bedingungen nicht mehr gelten.
- (2) Bei der Bewertung eines KI-Systems für die Zwecke der Absätze 1 und 1a berücksichtigt die Kommission folgende Kriterien:
- a) die Zweckbestimmung des KI-Systems;
 - aa) die allgemeinen Fähigkeiten und Funktionalitäten des KI-Systems unabhängig von seinem Verwendungszweck;

- b) das Ausmaß, in dem ein KI-System verwendet wird oder voraussichtlich verwendet werden wird;
- ba) die Art und Menge der vom KI-System verarbeiteten und verwendeten Daten;
- bb) das Ausmaß, in dem das KI-System autonom handelt;
- c) das Ausmaß, in dem durch die Verwendung eines KI-Systems schon die Gesundheit geschädigt, die Sicherheit beeinträchtigt oder negative Auswirkungen auf die Grundrechte, die Umwelt, die Demokratie und die Rechtsstaatlichkeit verursacht worden sind oder beispielsweise nach Berichten oder dokumentierten Behauptungen, die den zuständigen nationalen Aufsichtsbehörden, der Kommission, dem Amt für künstliche Intelligenz, dem Europäischen Datenschutzbeauftragten oder der Agentur der Europäischen Union für Grundrechte übermittelt werden, Anlass zu erheblichen Bedenken hinsichtlich der Wahrscheinlichkeit 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 oder eine bestimmte Gruppe von Personen unverhältnismäßig stark zu beeinträchtigen;
- e) das Ausmaß, in dem potenziell geschädigte oder beeinträchtigte Personen von dem mithilfe eines KI-Systems hervorgebrachten Ergebnis abhängen und dieses Ergebnis für die zu treffende Maßnahme oder Entscheidung rein akzessorisch ist, weil es insbesondere aus praktischen oder rechtlichen Gründen nach vernünftigem Ermessen unmöglich ist, sich diesem Ergebnis zu entziehen
- ea) den möglichen Missbrauch und die böswillige Nutzung des KI-Systems und der ihm zugrunde liegenden Technologie;
- f) das Ausmaß, in dem ein Machtungleichgewicht besteht oder in dem potenziell geschädigte oder beeinträchtigte Personen gegenüber dem Nutzer eines KI-Systems schutzbedürftig sind, insbesondere aufgrund von Status, Autorität, Wissen, wirtschaftlichen oder sozialen Umständen oder Alter;
- g) das Ausmaß, in dem das mithilfe eines KI-Systems hervorgebrachte Ergebnis leicht rückgängig zu machen oder behebbar ist, wobei Ergebnisse, die sich negativ auf die Gesundheit, Sicherheit, die Grundrechte von Personen, die Umwelt oder auf Demokratie und Rechtsstaatlichkeit auswirken, nicht als leicht rückgängig zu machen gelten;
- ga) das Ausmaß der Verfügbarkeit und des Einsatzes von wirksamen technischen Lösungen und Mechanismen für die Kontrolle, Zuverlässigkeit und Korrigierbarkeit des KI-Systems;

- gb) das Ausmaß und die Wahrscheinlichkeit, dass der Einsatz des KI-Systems für Einzelpersonen, Gruppen oder die Gesellschaft im Allgemeinen, einschließlich möglicher Verbesserungen der Produktsicherheit, nützlich ist;
 - gc) das Ausmaß menschlicher Aufsicht und die Möglichkeit menschlichen Eingreifens, um eine Entscheidung oder Empfehlungen, die potenziell zu Schaden führen können, außer Kraft zu setzen;
 - h) das Ausmaß, in dem bestehende Rechtsvorschriften der Union Folgendes vorsehen:
 - i) wirksame Abhilfemaßnahmen in Bezug auf die Schäden, die von einem KI-System verursacht wurden, mit Ausnahme von Ansprüchen im Falle direkter oder indirekter Schäden,
 - ii) wirksame Maßnahmen zur Vermeidung oder wesentlichen Verringerung dieser Risiken.
- (2a) Bei der Bewertung eines KI-Systems für die Zwecke der Absätze 1 oder 1a konsultiert die Kommission das Amt für künstliche Intelligenz und gegebenenfalls Vertreter der Gruppen, auf die sich ein KI-System auswirkt, die Industrie, unabhängige Experten, die Sozialpartner und Organisationen der Zivilgesellschaft. Die Kommission führt in diesem Zusammenhang auch öffentliche Konsultationen durch und macht die Ergebnisse dieser Konsultationen und der endgültigen Bewertung öffentlich zugänglich.
- (2b) Das Amt für künstliche Intelligenz, die nationalen Aufsichtsbehörden oder das Europäische Parlament können die Kommission auffordern, die Risikokategorisierung eines KI-Systems gemäß den Absätzen 1 und 1a neu zu bewerten und neu einzustufen. Die Kommission begründet ihre Entscheidung und veröffentlicht die Begründung.

KAPITEL 2

ANFORDERUNGEN AN HOCHRISIKO-KI-SYSTEME

ARTIKEL 8

EINHALTUNG DER ANFORDERUNGEN

- (1) Hochrisiko-KI-Systeme müssen die in diesem Kapitel festgelegten Anforderungen erfüllen.
- (1a) Bei der Erfüllung der in diesem Kapitel festgelegten Anforderung sind die gemäß Artikel 82b entwickelten Leitlinien, der allgemein anerkannte Stand der Technik, einschließlich der einschlägigen harmonisierten Normen und gemeinsamen Spezifikationen gemäß den Artikeln 40 und 41 oder der bereits in den Harmonisierungsrechtsvorschriften der Union festgelegten Normen und Spezifikationen, angemessen zu berücksichtigen.
- (2) Bei der Gewährleistung der Einhaltung dieser Anforderungen wird der Zweckbestimmung des Hochrisiko-KI-Systems, den vernünftigerweise vorhersehbaren Fehlanwendungen und dem in Artikel 9 genannten Risikomanagementsystem Rechnung getragen.

- (2a) Solange die Anforderungen von Titel III Kapitel 2 und 3 oder Titel VIII Kapitel 1, 2 und 3 für Hochrisiko-KI-Systeme durch die in Anhang II Abschnitt A aufgeführten Harmonisierungsrechtsvorschriften der Union abgedeckt sind, gelten die Anforderungen oder Verpflichtungen dieser Kapitel dieser Verordnung als erfüllt, sofern sie die KI-Komponente umfassen. Die Anforderungen von Titel III Kapitel 2 und 3 oder Titel VIII Kapitel 1, 2 und 3 für Hochrisiko-KI-Systeme, die nicht unter die in Anhang II Abschnitt A aufgeführten Harmonisierungsrechtsvorschriften der Union fallen, werden gegebenenfalls in diese Harmonisierungsrechtsvorschriften der Union aufgenommen. Die entsprechende Konformitätsbewertung wird im Rahmen der Verfahren durchgeführt, die in den in Anhang II Abschnitt A aufgeführten Harmonisierungsrechtsvorschriften der Union festgelegt sind.

ARTIKEL 9

RISIKOMANAGEMENTSYSTEM

- (1) Für Hochrisiko-KI-Systeme wird während des gesamten Lebenszyklus des KI-Systems ein Risikomanagementsystem eingerichtet, angewandt, dokumentiert und aufrechterhalten. Das Risikomanagementsystem kann in bereits bestehende Risikomanagementverfahren im Zusammenhang mit dem einschlägigen sektoralen Unionsrecht integriert werden oder Teil davon sein, sofern es die Anforderungen dieses Artikels erfüllt.
- (2) Das Risikomanagementsystem versteht sich als ein kontinuierlicher iterativer Prozess während des gesamten Lebenszyklus eines KI-Systems, der eine regelmäßige Überprüfung und Aktualisierung des Risikomanagementprozesses erfordert, um seine kontinuierliche Wirksamkeit sowie eine Dokumentation aller wichtigen Entscheidungen und Maßnahmen, die gemäß diesem Artikel getroffen wurden, sicherzustellen. Es umfasst folgende Schritte:
- a) Ermittlung, Abschätzung und Bewertung der bekannten und vernünftigerweise vorhersehbaren Risiken, die das Hochrisiko-KI-System für die Gesundheit oder Sicherheit natürlicher Personen, ihre Grundrechte, einschließlich des gleichen Zugangs und der Chancengleichheit, die Demokratie und die Rechtsstaatlichkeit oder die Umwelt verursachen kann, wenn das Hochrisiko-KI-System entsprechend seiner Zweckbestimmung oder im Rahmen einer vernünftigerweise vorhersehbaren Fehlanwendung verwendet wird;
 - c) Bewertung auftretender erheblicher Risiken, wie unter Buchstabe a beschrieben und ermittelt auf der Grundlage der Auswertung der Daten aus dem in Artikel 61 genannten System zur Beobachtung nach dem Inverkehrbringen;
 - d) Ergreifung geeigneter und gezielter Risikomanagementmaßnahmen zur Bewältigung der gemäß den Buchstaben a und b dieses Absatzes ermittelten Risiken 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, um die Risiken wirksam zu mindern und gleichzeitig eine angemessene und verhältnismäßige Umsetzung der Anforderungen sicherzustellen.

- (4) Die in Absatz 2 Buchstabe d genannten Risikomanagementmaßnahmen werden so gestaltet, dass ein relevantes mit einer bestimmten Gefahr verbundenes Restrisiko sowie das Gesamtrestrisiko der Hochrisiko-KI-Systeme nach vernünftigem Ermessen als vertretbar beurteilt werden kann, sofern das Hochrisiko-KI-System entsprechend seiner Zweckbestimmung oder im Rahmen einer vernünftigerweise vorhersehbaren Fehlanwendung verwendet wird. Diese Restrisiken und die begründeten Beurteilungen müssen den Betreibern mitgeteilt werden.

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

- a) soweit technisch machbar, eine Beseitigung oder Verringerung der identifizierten Risiken durch eine geeignete Konzeption und Entwicklung des Hochrisiko-KI-Systems, gegebenenfalls unter Einbeziehung von Experten und externen Interessenträgern,
- b) gegebenenfalls Anwendung angemessener Minderungs- und Kontrollmaßnahmen für nicht auszuschließende erhebliche Risiken;
- c) Bereitstellung der erforderlichen Informationen gemäß Artikel 13, insbesondere bezüglich der in Absatz 2 Buchstabe b des vorliegenden Artikels genannten Risiken, und gegebenenfalls entsprechende Schulung der Betreiber.

Bei der Beseitigung oder Verringerung der Risiken im Zusammenhang mit der Verwendung des Hochrisiko-KI-Systems berücksichtigen die Anbieter gebührend die technischen Kenntnisse, die Erfahrungen und den Bildungsstand, die der Betreiber möglicherweise benötigt, auch in Bezug auf den voraussichtlichen Nutzungskontext.

- (5) Hochrisiko-KI-Systeme müssen getestet werden, um die am besten geeigneten und gezielten Risikomanagementmaßnahmen zu ermitteln und diese Maßnahmen in Bezug auf den potenziellen Nutzen und die beabsichtigten Ziele des Systems abzuwägen. 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-
- (7) Das Testen von Hochrisiko-KI-Systemen erfolgt in jedem Fall vor dem Inverkehrbringen oder der Inbetriebnahme. Das Testen erfolgt anhand vorab festgelegter Parameter und probabilistischer Schwellenwerte, die für die Zweckbestimmung und vernünftigerweise vorhersehbare Fehlanwendung des Hochrisiko-KI-Systems geeignet sind.

- (8) Bei der Umsetzung des in den Absätzen 1 bis 7 beschriebenen Risikomanagementsystems berücksichtigen die Anbieter insbesondere, ob das Hochrisiko-KI-System wahrscheinlich negative Auswirkungen auf gefährdete Personengruppen oder Kinder hat.
- (9) Bei Anbietern und KI-Systemen, die bereits unter das Unionsrecht fallen, das ihnen die Einrichtung eines spezifischen Risikomanagements vorschreibt, einschließlich Kreditinstituten, die unter die Richtlinie 2013/36/EU fallen, sind die in den Absätzen 1 bis 8 beschriebenen Aspekte Bestandteil der durch dieses Unionsrecht festgelegten Risikomanagementverfahren oder werden mit diesen kombiniert.

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, soweit dies je nach Marktsegment oder Anwendungsbereich technisch machbar ist.
- Techniken, die keine gekennzeichneten Eingabedaten erfordern, wie z. B. unüberwachtes Lernen und bestärkendes Lernen, werden auf der Grundlage von Datensätzen entwickelt, z. B. zum Testen und Überprüfen, die den in den Absätzen 2 bis 5 genannten Qualitätskriterien entsprechen.
- (2) Für Trainings-, Validierungs- und Testdatensätze gilt eine Daten-Governance, die dem Nutzungskontext und dem beabsichtigten Zweck des KI-Systems angemessen ist. Diese Maßnahmen betreffen insbesondere
- a) die einschlägigen konzeptionellen Entscheidungen,
 - aa) die Transparenz in Bezug auf den ursprünglichen Zweck der Datenerfassung;
 - b) die Datenerfassungsprozesse,
 - c) Datenaufbereitungsvorgänge wie Kommentierung, Kennzeichnung, Bereinigung, Aktualisierung, Anreicherung und Aggregation,
 - d) die Aufstellung von Annahmen, insbesondere in Bezug auf die Informationen, die mit den Daten erfasst und dargestellt werden sollen,
 - e) eine Bewertung der Verfügbarkeit, Menge und Eignung der benötigten Datensätze,
 - f) eine Untersuchung im Hinblick auf mögliche Verzerrungen (Bias), die die Gesundheit und Sicherheit von Personen beeinträchtigen, sich negativ auf die Grundrechte auswirken oder zu einer nach dem Unionsrecht verbotenen Diskriminierung führen könnten, insbesondere wenn die Datenoutputs die Inputs für künftige Operationen beeinflussen („Feedback-Schleifen“), sowie geeignete Maßnahmen zur Erkennung, Verhinderung und Abschwächung möglicher Verzerrungen;

- fa) geeignete Maßnahmen zur Erkennung, Verhinderung und Abschwächung möglicher Verzerrungen;
 - g) die Ermittlung relevanter Datenlücken oder Mängel, die der Einhaltung dieser Verordnung entgegenstehen, und wie diese Lücken und Mängel behoben werden können.
- (3) Die Trainingsdatensätze und, falls verwendet, die Validierungs- und Testdatensätze, einschließlich der Kennzeichnungen, müssen relevant, hinreichend repräsentativ, angemessen auf Fehler überprüft und im Hinblick auf den beabsichtigten Zweck so vollständig wie möglich sein. Sie haben die geeigneten statistischen Merkmale, gegebenenfalls auch bezüglich der Personen oder Personengruppen, für die das Hochrisiko-KI-System bestimmungsgemäß verwendet werden soll. Diese Merkmale der Datensätze müssen durch einzelne Datensätze oder eine Kombination solcher Datensätze erfüllt werden.
- (4) Die Datensätze müssen, soweit dies für die Zweckbestimmung oder den vernünftigerweise vorhersehbaren Fehlgebrauch des KI-Systems erforderlich ist, den Merkmalen oder Elementen entsprechen, die für die besonderen geografischen, kontextuellen, verhaltensbezogenen oder funktionalen Rahmenbedingungen, unter denen das Hochrisiko-KI-System bestimmungsgemäß verwendet werden soll, typisch sind.
- (5) Soweit dies für die Erkennung und Korrektur von negativen Verzerrungen im Zusammenhang mit Hochrisiko-KI-Systemen unbedingt erforderlich ist, dürfen die Anbieter solcher Systeme in Ausnahmefällen 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 gehören. Insbesondere müssen alle folgenden Bedingungen erfüllt sein, damit diese Verarbeitung stattfinden kann:
- a) die Erkennung und Korrektur von Verzerrungen kann durch die Verarbeitung künstlicher oder anonymisierter Daten nicht effektiv durchgeführt werden
 - b) die Daten sind pseudonymisiert;
 - c) der Anbieter ergreift geeignete technische und organisatorische Maßnahmen, um sicherzustellen, dass die für die Zwecke dieses Absatzes verarbeiteten Daten gesichert, geschützt und angemessenen Sicherheitsvorkehrungen unterworfen sind und nur befugte Personen mit entsprechenden Vertraulichkeitsverpflichtungen Zugriff auf diese Daten haben;
 - d) die für die Zwecke dieses Absatzes verarbeiteten Daten dürfen nicht an andere Parteien weitergegeben, übertragen oder anderweitig abgerufen werden;

- e) die für die Zwecke dieses Absatzes verarbeiteten Daten sind durch geeignete technische und organisatorische Maßnahmen geschützt und werden gelöscht, sobald die Verzerrung berichtigt wurde oder das Ende der Speicherfrist für die personenbezogenen Daten erreicht ist;
- f) wirksame und angemessene Maßnahmen sind vorhanden, um die Verfügbarkeit, Sicherheit und Widerstandsfähigkeit der Verarbeitungssysteme und -dienste gegen technische oder physische Zwischenfälle sicherzustellen;
- g) wirksame und angemessene Maßnahmen sind vorhanden, um die physische Sicherheit der Orte, an denen die Daten gespeichert und verarbeitet werden, die interne IT und die IT-Sicherheitssteuerung und -verwaltung sowie die Zertifizierung von Prozessen und Produkten sicherzustellen.

Anbieter, die sich auf diese Bestimmung berufen, erstellen eine Dokumentation, in der sie erläutern, warum die Verarbeitung besonderer Kategorien personenbezogener Daten notwendig war, um Verzerrungen aufzudecken und zu korrigieren.

- (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.
- (6a) Kann der Anbieter den in diesem Artikel festgelegten Verpflichtungen nicht nachkommen, weil er keinen Zugang zu den Daten hat und sich die Daten ausschließlich im Besitz des Betreibers befinden, kann der Betreiber auf der Grundlage eines Vertrags für jeden Verstoß gegen diesen Artikel zur Verantwortung gezogen werden.

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 nationalen Aufsichtsbehörden und den notifizierten Stellen die 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 oder im Falle von KMU und Start-ups gleichwertige Unterlagen, die dieselben Ziele verfolgen, vorbehaltlich der Genehmigung durch die zuständige nationale Behörde.

- (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 Absatz 1 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.
- (3a) 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 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 dem Stand der Technik und den anerkannten Normen oder gemeinsamen Spezifikationen entsprechen.
- (2) Um sicherzustellen, dass das Funktionieren des KI-Systems während seiner gesamten Lebensdauer in einem der Zweckbestimmung des Systems angemessenen Maße rückverfolgbar ist, müssen die Protokollierungsfunktionen die Überwachung der Vorgänge gemäß Artikel 29 Absatz 4 sowie die Überwachung nach dem Inverkehrbringen gemäß Artikel 61 erleichtern. Sie müssen insbesondere die Aufzeichnung von Ereignissen ermöglichen, die für die Identifizierung von Situationen relevant sind, die möglicherweise
 - a) dazu führen, dass das KI-System eine Gefahr im Sinne von Artikel 65 Absatz 1 darstellt, oder
 - b) zu einer wesentlichen Änderung des KI-Systems führen.
- (2a) Hochrisiko-KI-Systeme müssen so konzipiert und entwickelt werden, dass sie über Protokollierungsfunktionen verfügen, mit denen die Aufzeichnung des Energieverbrauchs, die Messung oder Berechnung des Ressourcenverbrauchs und der Umweltauswirkungen des Hochrisiko-KI-Systems während aller Phasen des Lebenszyklus des Systems möglich ist.
- (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

- (1) Hochrisiko-KI-Systeme werden so konzipiert und entwickelt, dass ihr Betrieb hinreichend transparent ist, damit die Anbieter und Nutzer die Funktionsweise des Systems hinreichend verstehen können. Eine angemessene Transparenz wird entsprechend der Zweckbestimmung des KI-Systems gewährleistet, damit die Nutzer und Anbieter ihre in Kapitel 3 dieses Titels festgelegten einschlägigen Pflichten erfüllen können.

Transparenz bedeutet somit, dass zum Zeitpunkt des Inverkehrbringens des Hochrisiko-KI-Systems alle nach dem allgemein anerkannten Stand der Technik verfügbaren technischen Mittel eingesetzt werden, um sicherzustellen, dass die Ergebnisse des KI-Systems vom Anbieter und vom Nutzer interpretierbar sind. Der Nutzer muss in die Lage versetzt werden, das KI-System angemessen zu verstehen und zu nutzen, indem er allgemein weiß, wie das KI-System funktioniert und welche Daten es verarbeitet, sodass der Nutzer die vom KI-System getroffenen Entscheidungen der betroffenen Person gemäß Artikel 68 Buchstabe c erläutern kann.

- (2) Hochrisiko-KI-Systeme werden mit verständlichen Gebrauchsanweisungen in einem geeigneten digitalen Format bereitgestellt oder auf andere Weise auf einem dauerhaften Datenträger mit Gebrauchsanweisungen versehen, die präzise, korrekte, eindeutige und möglichst vollständige Informationen, die den Betrieb und die Wartung des KI-Systems sowie die fundierte Entscheidungsfindung der Nutzer unterstützen, in einer für die Nutzer hinreichend relevanten, barrierefrei zugänglichen und verständlichen Form enthalten.
- (3) Um die in Absatz 1 genannten Ergebnisse zu erzielen, umfassen die in Absatz 2 genannten Informationen:
- a) den Namen und die Kontaktangaben des Anbieters sowie gegebenenfalls seiner Bevollmächtigten;
 - aa) wenn es sich nicht um den Anbieter handelt, die Identität und die Kontaktdaten der Stelle, die die Konformitätsbewertung durchgeführt hat, und gegebenenfalls ihres Bevollmächtigten;
 - b) gegebenenfalls 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 eindeutig bekannten und vorhersehbaren Umstände, die

sich auf das erwartete Maß an Genauigkeit, Robustheit und Cybersicherheit auswirken können,

- iii) aller eindeutig 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, die Grundrechte oder die Umwelt führen können, gegebenenfalls einschließlich anschaulicher Beispiele für solche Einschränkungen und für Szenarien, für die das System nicht verwendet werden sollte;
 - iiia) des Ausmaßes, in dem das KI-System die von ihm getroffenen Entscheidungen erklären kann;
 - iv) seiner Leistung bezüglich der Personen oder Personengruppen, auf die das System bestimmungsgemäß angewandt werden soll,
 - v) relevante Informationen über Benutzeraktionen, die die Systemleistung beeinflussen können, einschließlich Art oder Qualität der 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) alle erforderlichen Wartungs- und Pflegemaßnahmen zur Gewährleistung des ordnungsgemäßen Funktionierens dieses KI-Systems, auch in Bezug auf Software-Updates, während seiner erwarteten Lebensdauer.
 - ea) eine Beschreibung der in das KI-System integrierten Mechanismen, die es den Nutzern ermöglicht, die Protokolle im Einklang mit Artikel 12 Absatz 1 ordnungsgemäß zu erfassen, zu speichern und auszuwerten.
 - eb) Die Informationen müssen zumindest in der Sprache des Landes bereitgestellt werden, in dem das KI-System verwendet wird.
- (3a) Um den in diesem Artikel festgelegten Verpflichtungen nachzukommen, sorgen die Anbieter und die Nutzer im Einklang mit Artikel 4b für ein ausreichendes Niveau an KI-Kompetenz.

ARTIKEL 14**MENSCHLICHE AUFSICHT**

- (1) Hochrisiko-KI-Systeme werden so konzipiert und entwickelt, dass sie in einem angemessenen Verhältnis zu den Risiken, die mit diesen Systemen verbunden sind, – auch mit geeigneten Werkzeugen einer Mensch-Maschine-Schnittstelle – von natürlichen Personen wirksam beaufsichtigt werden. Natürliche Personen, die mit der Sicherstellung der menschlichen Aufsicht betraut sind, müssen über ein ausreichendes Maß an KI-Kenntnissen gemäß Artikel 4b sowie über die notwendige Unterstützung und Befugnis verfügen, um diese Funktion während der Dauer der Verwendung des KI-Systems auszuüben und um eine gründliche Untersuchung nach einem Vorfall zu ermöglichen.
- (2) Die menschliche Aufsicht dient der Verhinderung oder Minimierung der Risiken für die Gesundheit, die Sicherheit, die Grundrechte oder die Umwelt, 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 und wenn Entscheidungen, die ausschließlich auf der automatisierten Verarbeitung durch KI-Systeme beruhen, rechtliche oder anderweitig erhebliche Auswirkungen auf die Personen oder Personengruppen haben, bei denen das System eingesetzt werden soll.
- (3) Die menschliche Aufsicht berücksichtigt die spezifischen Risiken, den Automatisierungsgrad und den Kontext des KI-Systems und wird durch eine oder alle der folgenden Arten von 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) Für die Zwecke der Umsetzung der Absätze 1 bis 3 wird das Hochrisiko-KI-System dem Nutzer so zur Verfügung gestellt, dass natürlichen Personen, denen die menschliche Aufsicht übertragen wurde, soweit dies den Umständen angemessen und verhältnismäßig ist, Folgendes ermöglicht wird:
 - a) die relevanten Fähigkeiten und Grenzen des Hochrisiko-KI-Systems zu kennen und hinreichend 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, das es ermöglicht, das System in einem sicheren Zustand zum Stillstand zu bringen, es sei denn, der menschliche Eingriff erhöht die Risiken oder würde die Leistung unter Berücksichtigung des allgemein anerkannten Stands der Technik negativ beeinflussen.
- (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, die die notwendige Kompetenz, Schulung und Befugnis besitzen, überprüft und bestätigt wurde.

ARTIKEL 15

GENAUIGKEIT, ROBUSTHEIT UND CYBERSICHERHEIT

- (1) Hochrisiko-KI-Systeme werden gemäß den Grundsätzen „Sicherheit durch technische Vorkehrungen“ und „Sicherheit durch entsprechende Grundeinstellungen“ konzipiert und entwickelt. Im Hinblick auf ihre Zweckbestimmung sollten sie ein angemessenes Maß an Genauigkeit, Robustheit, Sicherheit und Cybersicherheit erreichen und in dieser Hinsicht während ihres gesamten Lebenszyklus beständig funktionieren. Die Erfüllung dieser Anforderungen muss mit der Umsetzung von Maßnahmen verbunden sein, die dem Stand der Technik und dem jeweiligen Marktsegment oder Anwendungsbereich entsprechen.
- (1a) Um den technischen Aspekten der Bestimmung des angemessenen Grads an Genauigkeit und Robustheit gemäß Absatz 1 dieses Artikels Rechnung zu tragen, bringt das Amt für künstliche Intelligenz nationale Metrologie- und Benchmarking-Behörden zusammen und stellt unverbindliche Leitlinien zu dem Gegenstand von Artikel 56 Absatz 2 Buchstabe a bereit.
 - (1b) Um aufkommende Probleme im Zusammenhang mit der Cybersicherheit im gesamten Binnenmarkt anzugehen, wird neben dem Europäischen Ausschuss für künstliche Intelligenz gemäß Artikel 56 Absatz 2 Buchstabe b auch die Agentur der Europäischen Union für Cybersicherheit (ENISA) einbezogen.

- (2) Die Genauigkeitsgrade und die relevanten Genauigkeitskennzahlen von Hochrisiko-KI-Systemen werden in der ihnen beigefügten Gebrauchsanweisung angegeben. Die verwendete Sprache muss eindeutig sein und darf keine Missverständnisse oder irreführenden Aussagen enthalten.
- (3) Es müssen technische und organisatorische Maßnahmen ergriffen werden, um sicherzustellen, dass Hochrisiko-KI-Systeme so widerstandsfähig wie möglich gegenüber Fehlern, Störungen oder Unstimmigkeiten sind, 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 dem jeweiligen Anbieter, erforderlichenfalls unter Mitwirkung des Nutzers 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 die Eingabedaten für den künftigen Betrieb beeinflussen („Rückkopplungsschleifen“), und böswillige Manipulation von Eingaben, die beim Lernen während des Betriebs verwendet werden, angemessen mit geeigneten Risikominderungsmaßnahmen eingegangen wird.

- (4) Hochrisiko-KI-Systeme müssen widerstandsfähig gegen Versuche unbefugter Dritter sein, ihre Verwendung, ihr Verhalten, ihre Ergebnisse 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, um Angriffe, mit denen versucht wird, eine Manipulation des Trainingsdatensatzes („Datenvergiftung“) oder vortrainierter Komponenten, die beim Training verwendet werden („Modellvergiftung“), vorzunehmen, Eingabedaten, die das Modell zu Fehlern verleiten sollen („feindliche Beispiele“ oder „Modellvermeidung“), Angriffe auf vertrauliche Daten oder Modellmängel, die zu einer schädlichen Entscheidungsfindung führen könnten, zu verhüten, zu erkennen, darauf zu reagieren, sie zu beseitigen und zu kontrollieren.

KAPITEL 3

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

ARTIKEL 16

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

Anbieter von Hochrisiko-KI-Systemen müssen

- a) vor dem Inverkehrbringen oder der Inbetriebnahme ihrer KI-Systeme sicherstellen, dass ihre Hochrisiko-KI-Systeme die Anforderungen in Kapitel 2 dieses Titels erfüllen;
- aa) ihren Namen, ihren eingetragenen Handelsnamen oder ihre eingetragene Handelsmarke und ihre Kontaktanschrift und Kontaktinformationen auf dem Hochrisiko-KI-System selbst oder, wenn dies nicht möglich ist, in der beigefügten Dokumentation angeben;
- ab) sicherstellen, dass die natürlichen Personen, denen die menschliche Aufsicht übertragen wurde, auf das Risiko einer Automatisierungs- oder Bestätigungsverzerrung aufmerksam gemacht worden sind;
- ac) die Spezifikationen für die Eingabedaten oder sonstige relevante Informationen über die verwendeten Trainings-, Validierungs- und Testdatensätze zur Verfügung stellen, einschließlich ihrer Einschränkungen und Annahmen, unter Berücksichtigung der Zweckbestimmung und der vorhersehbaren sowie vernünftigerweise vorhersehbaren Fehlanwendungen des KI-Systems;
- b) über ein Qualitätsmanagementsystem verfügen, das dem Artikel 17 entspricht;
- c) die in Artikel 11 genannte technische Dokumentation des Hochrisiko-KI-Systems erstellen und aufbewahren;
- d) die von ihren Hochrisiko-KI-Systemen automatisch erzeugten Protokolle die erforderlich sind, um die Einhaltung dieser Verordnung sicherzustellen und nachzuweisen, gemäß Artikel 20 aufbewahren, wenn dies ihrer Kontrolle unterliegt;
- e) sicherstellen, dass das Hochrisiko-KI-System dem betreffenden Konformitätsbewertungsverfahren gemäß Artikel 43 unterzogen wird, bevor es in Verkehr gebracht oder in Betrieb genommen wird;
- ea) eine EU-Konformitätserklärung gemäß Artikel 48 ausstellen;
- eb) die CE-Kennzeichnung an das Hochrisiko-KI-System anbringen, um Konformität mit dieser Verordnung gemäß Artikel 49 anzuzeigen;
- f) den in Artikel 51 genannten Registrierungspflichten nachkommen;
- g) die erforderlichen Korrekturmaßnahmen gemäß Artikel 21 ergreifen und diesbezügliche Informationen übermitteln;
- j) auf begründeten Anfrage einer nationalen Aufsichtsbehörde nachweisen, dass das Hochrisiko-KI-System die Anforderungen in Kapitel 2 dieses Titels erfüllt.
- ja) sicherstellen, dass das Hochrisiko-KI-System die Anforderungen an die Zugänglichkeit erfüllt.

ARTIKEL 17**QUALITÄTSMANAGEMENTSYSTEM**

- (1) Anbieter von Hochrisiko-KI-Systemen verfügen über ein Qualitätsmanagement-system, das die Einhaltung dieser Verordnung gewährleistet. Es wird systematisch und ordnungsgemäß in Form schriftlicher Regeln, Verfahren oder Anweisungen dokumentiert und kann in ein bestehendes Qualitätsmanagementsystem gemäß den sektoralen Rechtsakten der Union integriert werden. Es umfasst mindestens folgende Aspekte:
- 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 oder sie nicht alle relevanten Anforderungen abdecken, 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 Datengewinnung, 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 relevanten zuständigen Behörden, auch sektoralen Behörden;
 - 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. Die Anbieter müssen in jedem Fall den Grad der Strenge und das Schutzniveau einhalten, die erforderlich sind, um die Übereinstimmung ihrer KI-Systeme mit dieser Verordnung sicherzustellen.
- (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 20

AUTOMATISCH ERZEUGTE PROTOKOLLE

- (1) Nutzer von Hochrisiko-KI-Systemen bewahren die von ihrem Hochrisiko-KI-System automatisch erzeugten Protokolle auf, soweit diese Protokolle ihrer Kontrolle unterliegen. Unbeschadet des geltenden Unionsrechts oder des nationalen Rechts werden die Protokolle mindestens 6 Monate lang aufbewahrt. Die Speicherfrist muss den Industriestandards entsprechen und der Zweckbestimmung des Hochrisiko-KI-Systems angemessen sein.
- (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

- (1) 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, zu deaktivieren oder zurückzurufen.
- (1a) In den im Absatz 1 genannten Fällen informieren die Anbieter unverzüglich
- a) die Vertreiber;
 - b) die Einführer;
 - c) die zuständigen nationalen Behörden der Mitgliedstaaten, in denen sie das KI-System zur Verfügung gestellt oder in Betrieb genommen haben; sowie
 - d) wenn möglich, den Betreiber.

- (1b) Die Anbieter informieren auch den Bevollmächtigten, falls ein solcher gemäß Artikel 25 benannt wurde, und die benannte Stelle, falls das Hochrisiko-KI-System einer Konformitätsbewertung durch Dritte gemäß Artikel 43 unterzogen werden musste. Gegebenenfalls untersuchen sie auch zusammen mit dem Betreiber die Ursachen.

ARTIKEL 22

INFORMATIONSPFLICHT

- (1) Birgt das Hochrisiko-KI-System ein Risiko im Sinne des Artikels 65 Absatz 1 und wird sich der Anbieter des Systems dieses Risikos bewusst, so informiert dieser Anbieter unverzüglich die zuständigen nationalen Aufsichtsbehörden 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 Art der Nichtkonformität und zu bereits ergriffenen relevanten Korrekturmaßnahmen.
- (1a) In den im Absatz 1 genannten Fällen informieren die Anbieter eines Hochrisiko-KI-Systems unverzüglich
- a) die Vertreiber;
 - b) die Einführer;
 - c) die zuständigen nationalen Behörden der Mitgliedstaaten, in denen sie das KI-System zur Verfügung gestellt oder in Betrieb genommen haben; sowie
 - d) wenn möglich, den Betreiber.
- (1b) Die Anbieter informieren auch den Bevollmächtigten, falls ein solcher gemäß Artikel 25 benannt wurde.

ARTIKEL 23

ZUSAMMENARBEIT MIT DEN ZUSTÄNDIGEN BEHÖRDEN, DEM AMT FÜR KÜNSTLICHE INTELLIGENZ UND DER KOMMISSION

- (1) Anbieter und gegebenenfalls Betreiber von Hochrisiko-KI-Systemen übermitteln einer zuständigen nationalen Behörde oder gegebenenfalls dem Amt für künstliche Intelligenz oder der Kommission auf deren begründetes 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.
- (1a) Auf begründetes Verlangen einer zuständigen nationalen Behörde oder gegebenenfalls der Kommission gewähren die Anbieter und gegebenenfalls die Betreiber der anfragenden zuständigen nationalen Behörde oder der Kommission auch Zugang zu den von dem Hochrisiko-KI-System automatisch erstellten Protokollen, soweit diese Protokolle ihrer Kontrolle unterliegen.

- (1b) Alle Informationen und Unterlagen, in deren Besitz eine zuständige nationale Behörde oder die Kommission auf der Grundlage dieses Artikels gelangt, werden im Einklang mit den in Artikel 70 festgelegten Vertraulichkeitspflichten behandelt.

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
- (1a) Der Bevollmächtigte muss seinen Wohnsitz oder seine Niederlassung in einem der Mitgliedstaaten haben, in denen die Tätigkeiten nach Artikel 2 Absätze 1b und 1c ausgeübt werden.
- (1b) Der Anbieter stattet seinen Bevollmächtigten mit den erforderlichen Befugnissen und Ressourcen aus, damit er seine Aufgaben gemäß dieser Verordnung erfüllen kann.
- (2) Der Bevollmächtigte nimmt die Aufgaben wahr, die in seinem vom Anbieter erhaltenen Auftrag festgelegt sind. Den Marktüberwachungsbehörden wird auf Anfrage eine Kopie des Mandats in einer von der zuständigen nationalen Behörde festgelegten Amtssprache des Organs der Union zur Verfügung gestellt. Für die Zwecke dieser Verordnung ermächtigt der Auftrag den Bevollmächtigten zumindest zur Wahrnehmung folgender Aufgaben:
- a) sicherstellen, dass die EU-Konformitätserklärung und die technische Dokumentation erstellt wurden und dass ein angemessenes Konformitätsbewertungsverfahren vom Anbieter durchgeführt wurde;
 - aa) Bereithaltung einer Kopie der EU-Konformitätserklärung, der technischen Unterlagen und gegebenenfalls der von der benannten Stelle ausgestellten Bescheinigung 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 der Kontrolle des Anbieters unterliegen;

- c) Zusammenarbeit mit den nationalen Aufsichtsbehörden auf deren begründetes Verlangen bei allen Maßnahmen, die die Behörde ergreift, um die von dem Hochrisiko-KI-System ausgehenden Risiken zu verringern und abzumildern
 - ca) gegebenenfalls die Einhaltung der Registrierungspflichten im Einklang mit Artikel 51 oder, falls die Registrierung vom Anbieter selbst vorgenommen wird, Sicherstellung der Richtigkeit der in Anhang VIII Nummer 3 genannten Angaben.
- (2a) Der Bevollmächtigte wird beauftragt, sich neben oder anstelle des Anbieters insbesondere an die nationale Aufsichtsbehörde oder die zuständigen nationalen Behörden in allen Fragen zu wenden, die die Einhaltung dieser Verordnung betreffen.
- (2b) Der Bevollmächtigte beendet den Auftrag, wenn er der Auffassung ist oder Grund zu der Annahme hat, dass der Anbieter gegen seine Verpflichtungen aus dieser Verordnung verstößt. In diesem Fall unterrichtet er ferner unverzüglich die nationale Aufsichtsbehörde des Mitgliedstaats, in dem er niedergelassen ist, und gegebenenfalls die betreffende notifizierte Stelle über die Beendigung des Auftrags und deren Gründe.

ARTIKEL 26

PFLICHTEN DER EINFÜHRER

- (1) Bevor sie ein Hochrisiko-KI-System in Verkehr bringen, stellen die Einführer solcher Systeme sicher, dass die Systeme dieser Verordnung entsprechen, indem sie sicherstellen, dass
- a) der Anbieter des KI-Systems das entsprechende Konformitätsbewertungs-verfahren nach Artikel 43 durchgeführt hat;
 - b) der Anbieter die technische Dokumentation gemäß Artikel 11 und Anhang IV erstellt hat;
 - c) das System mit der erforderlichen Konformitätskennzeichnung versehen ist und ihm die erforderlichen Unterlagen und Gebrauchsanweisungen beigelegt sind.
 - ca) gegebenenfalls der Anbieter einen bevollmächtigten Vertreter gemäß Artikel 25 Absatz 1 bestellt hat.
- (2) Ist ein Einführer der Auffassung oder hat er Grund zu der Annahme, dass ein Hochrisiko-KI-System nicht dieser Verordnung entspricht oder gefälscht ist oder diesem gefälschte Unterlagen beigelegt sind, 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 und gegebenenfalls 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 sie leicht verständlich ist, und gewähren ihr Zugang zu den vom Hochrisiko-KI-System automatisch erzeugten Protokollen, soweit diese Protokolle der Kontrolle des Anbieters gemäß Artikel 20 unterliegen.
- (5a) Die Einführer arbeiten mit den zuständigen nationalen Behörden bei allen Maßnahmen zusammen, die diese Behörden ergreifen, um die von dem Hochrisiko-KI-System ausgehenden Risiken zu verringern und abzumildern.

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 seine in Artikel 16 und Artikel 26 Absatz 3 dieser Verordnung festgelegten Pflichten erfüllt hat.
- (2) Ist ein Händler der Auffassung oder hat er aufgrund von Informationen, die ihm zur Verfügung stehen, 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 und die betreffende zuständige nationale Behörde 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 aufgrund von Informationen, die ihm zur Verfügung stehen, 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 den Anbieter bzw. den Einführer des Systems sowie 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 im Einklang mit den Pflichten der Händler gemäß Absatz 1 alle sich in ihrem Besitz befindenden oder ihnen zur Verfügung stehenden Informationen und Unterlagen, die erforderlich sind, um die Konformität eines Hochrisiko-KI-Systems mit den Anforderungen in Kapitel 2 dieses Titels nachzuweisen.
- (5a) Die Händler arbeiten mit den zuständigen nationalen Behörden bei allen Maßnahmen zusammen, die diese Behörden ergreifen, um die von dem Hochrisiko-KI-System ausgehenden Risiken zu verringern und abzumildern.

ARTIKEL 28

VERANTWORTLICHKEITEN ENTLANG DER KI-WERTSCHÖPFUNGSKETTE DER ANBIETER, HÄNDLER, EINFÜHRER, BETREIBER ODER ANDERER DRITTPARTEIEN

- (1) In den folgenden Fällen gelten Händler, Einführer, Betreiber oder sonstige Dritte als Anbieter eines Hochrisiko-KI-Systems für die Zwecke dieser Verordnung und unterliegen den Anbieterpflichten gemäß Artikel 16:
 - a) wenn sie ihren Namen oder ihr Markenzeichen auf ein Hochrisiko-KI-System setzen, das bereits in Verkehr gebracht oder in Betrieb genommen wurde;
 - b) wenn sie eine wesentliche Änderung an einem Hochrisiko-KI-System vornehmen, das bereits in Verkehr gebracht oder in Betrieb genommen wurde, und zwar so, dass es weiterhin ein Hochrisiko-KI-System im Sinne von Artikel 6 bleibt;
 - ba) wenn sie eine wesentliche Änderung an einem Hochrisiko-KI-System vornehmen, das bereits in Verkehr gebracht oder in Betrieb genommen wurde, und zwar so, dass es weiterhin ein Hochrisiko-KI-System im Sinne von Artikel 6 bleibt;
 - c) wenn sie eine wesentliche Änderung an dem Hochrisiko-KI-System vornehmen.
- (2) Unter den in Absatz 1 Buchstaben a bis ba genannten Umständen gilt der Anbieter, der das KI-System ursprünglich in Verkehr gebracht oder in Betrieb genommen hatte, nicht mehr als Anbieter dieses spezifischen KI-Systems für die Zwecke dieser Verordnung. Dieser ehemalige Anbieter stellt dem neuen Anbieter die technische Dokumentation und alle anderen relevanten und vernünftigerweise zu erwartenden Informationen und Fähigkeiten des KI-Systems, den

technischen Zugang oder sonstige Unterstützung auf der Grundlage des allgemein anerkannten Stands der Technik zur Verfügung, die für die Erfüllung der in dieser Verordnung festgelegten Verpflichtungen erforderlich sind.

Dieser Absatz gilt auch für Anbieter von Basismodellen im Sinne von Artikel 3, wenn das Basismodell direkt in ein Hochrisiko-KI-System integriert ist.

- (2a) Der Anbieter eines Hochrisiko-KI-Systems und der Dritte, der Werkzeuge, Dienste, Komponenten oder Verfahren bereitstellt, die in dem Hochrisiko-KI-System verwendet oder integriert werden, legen in einer schriftlichen Vereinbarung fest, welche Informationen, Fähigkeiten, technischen Zugang und/oder sonstige Unterstützung nach dem allgemein anerkannten Stand der Technik der Dritte bereitstellen muss, damit der Anbieter des Hochrisiko-KI-Systems die Verpflichtungen im Rahmen dieser Verordnung vollständig erfüllen kann.

Die Kommission entwickelt und empfiehlt unverbindliche Mustervertragsbedingungen zwischen Anbietern von Hochrisiko-KI-Systemen und Dritten, die Werkzeuge, Dienstleistungen, Komponenten oder Prozesse liefern, die in Hochrisiko-KI-Systemen verwendet oder integriert werden, um beide Parteien bei der Ausarbeitung und Aushandlung von Verträgen mit ausgewogenen vertraglichen Rechten und Pflichten zu unterstützen, die dem Kontrollniveau jeder Partei entsprechen. Bei der Ausarbeitung unverbindlicher Mustervertragsbedingungen berücksichtigt die Kommission mögliche vertragliche Anforderungen, die in bestimmten Sektoren oder Geschäftsfällen gelten. Die unverbindlichen Vertragsbedingungen werden auf der Website des Amts für künstliche Intelligenz veröffentlicht und sind dort kostenlos in einem leicht nutzbaren elektronischen Format verfügbar.

- (2b) Für die Zwecke dieses Artikels sind Geschäftsgeheimnisse zu wahren und werden nur offengelegt, wenn vorab alle besonderen Maßnahmen gemäß der Richtlinie (EU) 2016/943 getroffen worden sind, die erforderlich sind, um ihre Vertraulichkeit, insbesondere gegenüber Dritten, zu wahren. Bei Bedarf können geeignete technische und organisatorische Vorkehrungen getroffen werden, um geistige Eigentumsrechte oder Geschäftsgeheimnisse zu schützen.

ARTIKEL 28A

MISSBRÄUHLICHE VERTRAGSKLAUSELN, DIE EINEM KMU ODER EINEM STARTUP EINSEITIG AUFERLEGT WERDEN

- (1) Eine Vertragsklausel über die Lieferung von Werkzeugen, Dienstleistungen, Komponenten oder Verfahren, die in einem Hochrisiko-KI-System verwendet oder integriert werden, oder über die Abhilfemaßnahmen im Falle eines Verstoßes oder der Beendigung damit verbundener Verpflichtungen, die ein Unternehmen einem KMU oder einem Start-up einseitig auferlegt hat, ist für letzteres Unternehmen nicht bindend, wenn sie missbräuchlich ist.

- (2) Eine Vertragsbedingung gilt nicht als missbräuchlich, wenn sie aus anwendbarem EU-Recht hervorgeht.
- (3) Eine Vertragsklausel ist missbräuchlich, wenn sie so beschaffen ist, dass sie objektiv die Fähigkeit der Partei, der die Klausel einseitig auferlegt wurde, beeinträchtigt, ihre berechtigten geschäftlichen Interessen an den betreffenden Informationen zu schützen, oder wenn ihre Verwendung grob von der guten Geschäftspraxis bei der Lieferung von Werkzeugen, Dienstleistungen, Komponenten oder Verfahren, die in einem Hochrisiko-KI-System verwendet oder integriert werden, abweicht und gegen Treu und Glauben verstößt oder ein erhebliches Ungleichgewicht zwischen den Rechten und Pflichten der Vertragsparteien schafft. Eine Vertragsklausel ist auch dann missbräuchlich, wenn sie dazu führt, dass die in Artikel 71 genannten Vertragsstrafen oder die damit verbundenen Prozesskosten auf die Vertragsparteien verlagert werden, wie in Artikel 71 Absatz 8 beschrieben.
- (4) Eine Vertragsklausel ist missbräuchlich im Sinne dieses Artikels, wenn sie Folgendes bezweckt oder bewirkt:
- a) den Ausschluss oder die Beschränkung der Haftung der Partei, die die Klausel einseitig auferlegt hat, für vorsätzliche oder grob fahrlässige Handlungen;
 - b) den Ausschluss der Rechtsbehelfe, die der Partei, der die Klausel einseitig auferlegt wurde, bei Nichterfüllung von Vertragspflichten zur Verfügung stehen, oder den Ausschluss der Haftung der Partei, die die Klausel einseitig auferlegt hat, bei einer Verletzung solcher Pflichten;
 - c) das ausschließliche Recht der Partei, die die Klausel einseitig auferlegt hat, zu bestimmen, ob die gelieferten technischen Unterlagen und Informationen vertragsgemäß sind, oder eine Vertragsklausel auszulegen.
- (5) Eine Vertragsklausel gilt im Sinne dieses Artikels als einseitig auferlegt, wenn sie von einer Vertragspartei eingebracht wird und die andere Vertragspartei ihren Inhalt trotz des Versuchs, hierüber zu verhandeln, nicht beeinflussen kann. Die Vertragspartei, die eine Vertragsklausel eingebracht hat, trägt die Beweislast dafür, dass diese Klausel nicht einseitig auferlegt wurde.
- (6) Ist die missbräuchliche Vertragsklausel von den übrigen Bedingungen des Vertrags abtrennbar, so bleiben die übrigen Vertragsbedingungen bindend. Die Partei, die die beanstandete Klausel vorgelegt hat, kann sich nicht darauf berufen, dass es sich um eine missbräuchliche Klausel handelt.
- (7) Dieser Artikel gilt für alle neuen Verträge nach dem ... [Bitte Datum des Inkrafttretens dieser Verordnung einfügen]. Die Unternehmen überprüfen bestehende vertragliche Verpflichtungen, die unter diese Verordnung fallen, bis zum Jahr ... [drei Jahre nach Inkrafttreten dieser Verordnung].

- (8) Angesichts der Geschwindigkeit, in der Innovationen auf den Märkten auftreten, wird die Liste der missbräuchlichen Vertragsklauseln in Artikel 28 Absatz a regelmäßig von der Kommission überprüft und erforderlichenfalls entsprechend den neuen Geschäftspraktiken aktualisiert.

ARTIKEL 28B

PFLICHTEN DES ANBIETERS EINES BASISMODELLS

- (1) Ein Anbieter eines Basismodells muss, bevor er es auf dem Markt bereitstellt oder in Betrieb nimmt, sicherstellen, dass es den in diesem Artikel festgelegten Anforderungen entspricht, unabhängig davon, ob es als eigenständiges Modell oder eingebettet in ein KI-System oder ein Produkt oder unter freien und Open-Source-Lizenzen als Dienstleistung sowie über andere Vertriebskanäle bereitgestellt wird.
- (2) Für die Zwecke von Absatz 1 muss der Anbieter eines Basismodells
- a) durch geeignete Planung, Erprobung und Analyse die Identifizierung, Verringerung und Abschwächung von vernünftigerweise vorhersehbaren Risiken für Gesundheit, Sicherheit, Grundrechte, Umwelt sowie Demokratie und Rechtsstaatlichkeit vor und während der Entwicklung mit geeigneten Methoden, z. B. unter Einbeziehung unabhängiger Experten, sowie die Dokumentation der verbleibenden nicht abwendbaren Risiken nach der Entwicklung nachweisen;
 - b) nur Datensätze verarbeiten und einbeziehen, die angemessenen Data-Governance-Maßnahmen für Basismodelle unterliegen, insbesondere Maßnahmen zur Prüfung der Eignung der Datenquellen und möglicher Verzerrungen und geeigneter Abhilfemaßnahmen;
 - c) das Basismodell so konzipieren und entwickeln, dass während seines gesamten Lebenszyklus ein angemessenes Niveau an Leistung, Vorhersagbarkeit, Interpretierbarkeit, Korrigierbarkeit, Sicherheit und Cybersicherheit erreicht wird, das mit Hilfe geeigneter Methoden wie der Modellevaluierung unter Einbeziehung unabhängiger Experten, dokumentierter Analysen und umfassender Tests während der Konzeption, des Entwurfs und der Entwicklung bewertet wird;
 - d) das Basismodell unter Verwendung der geltenden Normen zur Verringerung des Energieverbrauchs, des Ressourcenverbrauchs und des Abfalls sowie zur Steigerung der Energieeffizienz und der Gesamteffizienz des Systems entwerfen und entwickeln, unbeschadet des geltenden Unionsrechts und des nationalen Rechts. Diese Verpflichtung gilt nicht vor der Veröffentlichung der in Artikel 40 genannten Normen. Basismodelle müssen so konzipiert sein, dass der Energieverbrauch sowie der Verbrauch anderer Ressourcen und andere Umweltauswirkungen, die der Einsatz und

die Nutzung der Systeme während ihres gesamten Lebenszyklus haben kann, gemessen und aufgezeichnet werden können;

- e) eine umfassende technische Dokumentation und verständliche Gebrauchsanweisungen erstellen, damit die nachgeschalteten Anbieter ihren Verpflichtungen gemäß Artikel 16 und 28 Absatz 1 nachkommen können;
- f) ein Qualitätsmanagementsystem einrichten, um die Einhaltung dieses Artikels sicherzustellen und zu dokumentieren, mit der Möglichkeit, bei der Erfüllung dieser Anforderung zu experimentieren;
- g) dieses Basismodell gemäß den Anweisungen in Anhang VIII Punkt C in der in Artikel 60 genannten EU-Datenbank registrieren.

Bei der Erfüllung dieser Anforderungen ist der allgemein anerkannte Stand der Technik zu berücksichtigen, der auch in den einschlägigen harmonisierten Normen oder gemeinsamen Spezifikationen zum Ausdruck kommt, sowie die neuesten Bewertungs- und Messmethoden, die insbesondere in den in Artikel 58 Absatz a genannten Benchmarking-Leitlinien und Fähigkeiten zum Ausdruck kommen;

- (3) Anbieter von Basismodellen halten die in Absatz 2 Buchstabe e genannten technischen Unterlagen während eines Zeitraums, der 10 Jahre nach dem Inverkehrbringen oder der Inbetriebnahme ihrer Basismodelle endet, für die zuständigen nationalen Behörden bereit.
- (4) Anbieter von Basismodellen, die in KI-Systemen verwendet werden, die speziell dazu bestimmt sind, mit unterschiedlichem Grad an Autonomie Inhalte wie komplexe Texte, Bilder, Audio- oder Videodateien zu generieren („generative KI“), sowie Anbieter, die ein Basismodell in ein generatives KI-System integrieren, müssen zusätzlich
 - a) den in Artikel 52 Absatz 1 genannten Transparenzpflichten nachkommen;
 - b) das Basismodell so gestalten und gegebenenfalls weiterentwickeln, dass ein angemessener Schutz gegen die Erzeugung von Inhalten, die gegen das Unionsrecht verstoßen, nach dem allgemein anerkannten Stand der Technik und unbeschadet der Grundrechte, einschließlich des Rechts auf freie Meinungsäußerung, sichergestellt ist;
 - c) unbeschadet der Rechtsvorschriften der Union oder der Mitgliedstaaten oder der Union zum Urheberrecht eine hinreichend detaillierte Zusammenfassung der Verwendung von urheberrechtlich geschützten Ausbildungsdaten dokumentieren und öffentlich zugänglich machen.

ARTIKEL 29

PFLICHTEN DER NUTZER VON HOCHRISIKO-KI-SYSTEMEN

- (1) Die Betreiber von Hochrisiko-KI-Systemen treffen geeignete technische und organisatorische Maßnahmen, um sicherzustellen, dass sie solche Systeme entsprechend der den Systemen

beigefügten Gebrauchsanweisungen und gemäß den Absätzen 2 und 5 dieses Artikels verwenden.

- a) In dem Maße, in dem die Betreiber die Kontrolle über das Hochrisiko-KI-System ausüben, müssen sie
 - i) eine menschliche Aufsicht gemäß den in dieser Verordnung festgelegten Anforderungen sicherstellen;
 - ii) sicherstellen, dass die mit der menschlichen Aufsicht über die Hochrisiko-KI-Systeme betrauten natürlichen Personen kompetent, angemessen qualifiziert und geschult sind und über die erforderlichen Ressourcen verfügen, um die wirksame Überwachung des KI-Systems gemäß Artikel 14 sicherzustellen;
 - iii) sicherstellen, dass die einschlägigen und angemessenen Maßnahmen zur Robustheit und Cybersicherheit regelmäßig auf ihre Wirksamkeit hin überprüft und regelmäßig angepasst oder aktualisiert werden.
- (2) Die Pflichten nach Absatz 1 und 1a lassen sonstige Pflichten der Betreiber nach Unionsrecht oder nationalem Recht sowie das Ermessen der Betreiber bei der Organisation ihrer eigenen Ressourcen und Tätigkeiten zur Wahrnehmung der vom Anbieter angegebenen Maßnahmen der menschlichen Aufsicht unberührt.
- (3) Unbeschadet der Absätze 1 und 1a und soweit die Eingabedaten seiner Kontrolle unterliegen, sorgen die Betreiber dafür, dass die Eingabedaten der Zweckbestimmung des Hochrisiko-KI-Systems relevant und ausreichend repräsentativ sind.
- (4) Die Betreiber überwachen den Betrieb des Hochrisiko-KI-Systems anhand der Gebrauchsanweisung und informieren gegebenenfalls die Anbieter gemäß Artikel 61. 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 unverzüglich den Anbieter oder Händler und die zuständigen nationalen Aufsichtsbehörden und setzen die Verwendung des Systems aus. Sie informieren unverzüglich zunächst den Anbieter und dann den Einführer oder Händler sowie die zuständigen nationalen Aufsichtsbehörden, wenn sie einen schwerwiegenden Vorfall oder eine Fehlfunktion im Sinne des Artikels 62 festgestellt haben, und unterbrechen die Verwendung des KI-Systems. Kann der Betreiber den Anbieter nicht erreichen, so gilt Artikel 62 entsprechend.

Bei Betreibern, 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) Betreiber von Hochrisiko-KI-Systemen bewahren die von ihrem Hochrisiko-KI-System automatisch erzeugten Protokolle auf, soweit diese Protokolle ihrer Kontrolle unterliegen und

erforderlich sind, um die Einhaltung dieser Verordnung sicherzustellen und nachzuweisen, um Ex-post-Prüfungen von vernünftigerweise vorhersehbaren Fehlfunktionen, Zwischenfällen oder Missbräuchen des Systems durchzuführen oder um das ordnungsgemäße Funktionieren des Systems während seines gesamten Lebenszyklus sicherzustellen und zu überwachen. Unbeschadet des geltenden Unionsrechts oder nationalen Rechts sind die Protokolle mindestens sechs Monate lang aufzubewahren. Die Speicherfrist muss den Industriestandards entsprechen und der Zweckbestimmung des Hochrisiko-KI-Systems angemessen sein.

Betreiber, 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.

- (5a) Vor der Inbetriebnahme oder Nutzung eines Hochrisiko-KI-Systems am Arbeitsplatz konsultieren die Betreiber die Arbeitnehmervertreter, um eine Vereinbarung gemäß der Richtlinie 2002/14/EG zu erzielen, und informieren die betroffenen Arbeitnehmer darüber, dass sie dem System unterliegen werden.
- (5b) Betreiber von Hochrisiko-KI-Systemen, bei denen es sich um Behörden oder Organe, Einrichtungen, Ämter und Agenturen der Union oder Unternehmen im Sinne von Artikel 51 Absatz 1a Buchstabe b handelt, müssen den Registrierungspflichten gemäß Artikel 51 nachkommen.
- (6) Gegebenenfalls verwenden Betreiber von Hochrisiko-KI-Systemen die gemäß Artikel 13 bereitgestellten Informationen, um ihrer Verpflichtung zur Durchführung einer Datenschutz-Folgenabschätzung gemäß Artikel 35 der Verordnung (EU) 2016/679 oder Artikel 27 der Richtlinie (EU) 2016/680 nachzukommen, deren Zusammenfassung unter Berücksichtigung der spezifischen Nutzung und des spezifischen Kontexts, in dem das KI-System eingesetzt werden soll, veröffentlicht wird. Betreiber können bei der Erfüllung einiger der in diesem Artikel genannten Verpflichtungen teilweise auf diese Datenschutz-Folgenabschätzungen zurückgreifen, sofern die Datenschutz-Folgenabschätzungen diese Verpflichtungen erfüllen.
- (6a) Unbeschadet des Artikels 52 informieren die Betreiber der in Anhang III genannten Hochrisiko-KI-Systeme, die Entscheidungen in Bezug auf natürliche Personen treffen oder dabei helfen, Entscheidungen zu treffen, die natürlichen Personen darüber, dass sie dem Hochrisiko-KI-System unterliegen. Die betreffenden Informationen umfassen seine Zweckbestimmung und die Art der Entscheidungen, die davon getroffen werden. Der Betreiber informiert die natürliche Person auch über ihr Recht auf eine Erklärung gemäß Artikel 68c.
- (6b) Die Betreiber arbeiten mit den zuständigen nationalen Behörden bei allen Maßnahmen zusammen, die diese Behörden im Zusammenhang mit dem Hochrisikosystem zur Umsetzung dieser Verordnung ergreifen.

ARTIKEL 29A**FOLGENABSCHÄTZUNG IM HINBLICK AUF DIE GRUNDRECHTE FÜR HOCHRISIKO-KI-SYSTEME**

- (1) Vor der Inbetriebnahme eines Hochrisiko-KI-Systems im Sinne von Artikel 6 Absatz 2, mit Ausnahme von KI-Systemen, die für den Einsatz im Bereich 2 des Anhangs III bestimmt sind, führen die Betreiber eine Bewertung der Auswirkungen des Systems in dem konkreten Kontext seiner Anwendung durch. Diese Bewertung muss mindestens Folgendes umfassen:
- a) eine klare Darstellung des beabsichtigten Verwendungszwecks des Systems;
 - b) eine klare Darstellung des geplanten geografischen und zeitlichen Anwendungsbereichs des Systems;
 - c) die Kategorisierung der natürlichen Personen und Gruppen, die von der Verwendung des Systems betroffen sein könnten;
 - d) die Prüfung und Bestätigung, dass die Verwendung des Systems dem Unionsrecht und den nationalen Rechtsvorschriften sowie den Grundrechten entspricht;
 - e) die vernünftigerweise vorhersehbaren Auswirkungen der Inbetriebnahme des Hochrisiko-KI-Systems auf die Grundrechte;
 - f) spezifische Schadensrisiken, die sich auf marginalisierte Personen oder schutzbedürftige Gruppen auswirken könnte;
 - g) die vernünftigerweise vorhersehbaren negativen Auswirkungen der Nutzung des Systems auf die Umwelt;
 - h) einen ausführlichen Plan, wie das erkannte Schadensrisiko sowie die negativen Auswirkungen auf die Grundrechte gemindert werden sollen.
 - i) das Governance-System, das der Betreiber einsetzen wird, einschließlich menschlicher Überwachung, Bearbeitung von Beschwerden und Rechtsbehelfen.
- (2) Wenn kein ausführlicher Plan zur Minderung der im Zuge der Bewertung nach Absatz 1 beschriebenen Risiken bestimmt werden kann, sieht der Betreiber von der Inbetriebnahme des Hochrisiko-KI-Systems ab und informiert unverzüglich den Anbieter und die nationale Aufsichtsbehörde. Im Einklang mit den Artikeln 65 und 67 berücksichtigen die Aufsichtsbehörden diese Informationen bei der Untersuchung von Systemen, die auf nationaler Ebene ein Risiko darstellen.
- (3) Die in Absatz 1 beschriebene Verpflichtung gilt für die erste Verwendung eines Hochrisiko-KI-Systems. Der Betreiber kann in ähnlichen Fällen auf eine zuvor durchgeführte Folgenabschätzung für die allgemeinen Grundrechte oder eine bereits vorhandene Prüfung durch die Anbieter zurückgreifen. Ist der Betreiber während des Einsatzes des Hochrisiko-KI-Systems der Ansicht, dass die in Absatz 1 genannten Kriterien nicht mehr erfüllt sind, führt er eine neue Folgenabschätzung für die allgemeinen Grundrechte durch.

- (4) Im Verlauf der Folgenabschätzung benachrichtigt der Betreiber, mit Ausnahme von KMU, die nationale Aufsichtsbehörde und die relevanten Interessenträger und bezieht so weit wie möglich Vertreter der Personen oder Personengruppen ein, die von dem Hochrisiko-KI-System gemäß Absatz 1 betroffen sein könnten, einschließlich, aber nicht beschränkt auf: Gleichstellungsstellen, Verbraucherschutzbehörden, Sozialpartner und Datenschutzbehörden, um Beiträge zur Folgenabschätzung zu erhalten. Der Betreiber räumt den Stellen eine Frist von sechs Wochen für ihre Antwort ein. KMU können die in diesem Absatz festgelegten Bestimmungen freiwillig anwenden.

In dem in Artikel 47 Absatz 1 genannten Fall können öffentliche Stellen von dieser Verpflichtung befreit werden.

- (5) Ein Betreiber, bei dem es sich um eine Behörde oder ein Unternehmen im Sinne von Artikel 51 Absatz 1a Buchstabe b handelt, veröffentlicht eine Zusammenfassung der Ergebnisse der Folgenabschätzung als Teil der Registrierung der Nutzung gemäß seiner Verpflichtung nach Artikel 51 Absatz 2.
- (6) Ist der Betreiber bereits verpflichtet, eine Datenschutz-Folgenabschätzung gemäß Artikel 35 der Verordnung (EU) 2016/679 oder Artikel 27 der Richtlinie (EU) 2016/680 durchzuführen, wird die Folgenabschätzung für die allgemeinen Grundrechte gemäß Absatz 1 in Verbindung mit der Datenschutz-Folgenabschätzung durchgeführt und als Zusatz veröffentlicht. Die Datenschutz-Folgenabschätzung wird als Nachtrag veröffentlicht.

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. Diese Verfahren werden in Zusammenarbeit zwischen den notifizierenden Behörden aller Mitgliedstaaten entwickelt.
- (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. Gegebenenfalls muss das zuständige Personal über die erforderliche Sachkenntnis, z. B. einen Abschluss in einem geeigneten Rechtsgebiet, für die Überwachung der in der Charta der Grundrechte der Europäischen Union verankerten Grundrechte verfügen.
- (8) Notifizierende Behörden gewährleisten, dass Konformitätsbewertungen in angemessener und zeitnaher 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. Besondere Aufmerksamkeit gilt der Minimierung des Verwaltungsaufwands und der Befolgungskosten für Kleinst- und Kleinunternehmen gemäß der Definition im Anhang der Empfehlung 2003/361/EG der Kommission.

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 notifizieren nur Konformitätsbewertungsstellen, 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, über jede Konformitätsbewertungsstelle gemäß Absatz 1.
- (3) Eine Notifizierung gemäß Absatz 2 enthält vollständige Angaben zu den Konformitätsbewertungstätigkeiten, dem/den betreffenden Konformitätsbewertungsmodul(en) und den betreffenden Technologien der künstlichen Intelligenz sowie die betreffende Bescheinigung der Kompetenz.
- (4) Die betreffende Konformitätsbewertungsstelle darf die Aufgaben einer notifizierten Stelle nur dann wahrnehmen, wenn weder die Kommission noch die übrigen Mitgliedstaaten innerhalb von zwei Wochen nach der Validierung der Notifizierung, sofern eine Akkreditierungsurkunde gemäß Artikel 31 Absatz 2 vorgelegt wird, oder innerhalb von zwei Monaten nach der Notifizierung, sofern beweiskräftige Unterlagen gemäß Artikel 31 Absatz 3 vorgelegt werden, Einwände erhoben haben.
 - (4a) Werden Einwände erhoben, konsultiert die Kommission unverzüglich die betreffenden Mitgliedstaaten und die Konformitätsbewertungsstelle. In Anbetracht dessen entscheidet die Kommission, ob die Genehmigung gerechtfertigt ist oder nicht. Die Kommission richtet ihren Beschluss an die betroffenen Mitgliedstaaten und an die zuständige Konformitätsbewertungsstelle.
 - (4b) Die Mitgliedstaaten teilen der Kommission und den anderen Mitgliedstaaten die Konformitätsbewertungsstellen mit.
- (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, sowie die Mindestanforderungen an die Cybersicherheit, die für öffentliche Verwaltungseinrichtungen gelten, die gemäß der Richtlinie (EU) 2022/2555 als Betreiber wesentlicher Dienste identifiziert wurden.

- (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. Dies schließt die Verwendung von bewerteten KI-Systemen, die für die Tätigkeit der Konformitätsbewertungsstelle nötig sind, oder die Verwendung solcher Systeme zum persönlichen Gebrauch nicht aus.
- (4a) Eine Konformitätsbewertung gemäß Absatz 1 wird von Mitarbeitern notifizierter Stellen durchgeführt, die in den 12 Monaten vor der Bewertung weder für den Anbieter eines Hochrisiko-KI-Systems noch für eine mit diesem Anbieter verbundene juristische Person eine andere Dienstleistung im Zusammenhang mit dem bewerteten Sachverhalt erbracht haben und sich verpflichtet haben, in den 12 Monaten nach Abschluss der Bewertung keine derartigen Dienstleistungen für sie zu erbringen.
- (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. Alle Informationen und Unterlagen, in deren Besitz eine notifizierte Stelle auf der Grundlage dieses Artikels gelangt, werden im Einklang mit den in Artikel 70 festgelegten Vertraulichkeitspflichten behandelt.

- (7) Die notifizierte 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 notifizierte 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 notifizierte 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 notifizierte Stellen selbst oder in ihrem Auftrag und in ihrer Verantwortung erfüllt werden.
- (10) Die notifizierte Stellen verfügen über ausreichende interne Kompetenzen, um die von externen Stellen in ihrem Namen wahrgenommenen Aufgaben wirksam beurteilen zu können. Dazu müssen die notifizierte 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 notifizierte 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 notifizierte 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 notifizierte 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. Die benannten Stellen machen eine Liste ihrer Zweigstellen öffentlich zugänglich.
- (4) Die notifizierte Stellen halten für die notifizierende Behörde die einschlägigen Unterlagen über die Überprüfung der Qualifikation des Unterauftragnehmers oder der Zweigstelle und die von ihnen gemäß dieser Verordnung ausgeführten Arbeiten bereit.

ARTIKEL 35

KENNNUMMERN UND VERZEICHNISSE NOTIFIZierter STELLEN

- (1) Die Kommission weist den notifizierte 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 notifizierte 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 notifizierte Stelle die erhobenen Einwände mit und gibt ihr die Möglichkeit, dazu Stellung zu nehmen. Kommt die notifizierende Behörde zu dem Schluss, dass die 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 notifizierte Stelle von einer anderen notifizierte Stelle übernommen bzw. für die zuständigen notifizierenden Behörden und die Marktüberwachungsbehörde auf deren Verlangen bereitgehalten werden.

ARTIKEL 37**ANFECHTUNGEN DER KOMPETENZ NOTIFIZierter STELLEN**

- (1) Die Kommission untersucht erforderlichenfalls alle Fälle, in denen begründete Zweifel an der Kompetenz einer notifizierten Stelle oder daran bestehen, dass eine notifizierte Stelle die geltenden Anforderungen und Pflichten weiterhin erfüllt.
- (2) Die notifizierende Behörde stellt der Kommission auf Anfrage alle Informationen über die Notifizierung oder das Fortbestehen der betreffenden notifizierten Stelle zur Verfügung.
- (3) Die Kommission stellt sicher, dass alle im Verlauf ihrer Untersuchungen gemäß diesem Artikel erlangten sensiblen Informationen vertraulich behandelt werden.
- (4) Stellt die Kommission fest, dass eine notifizierte Stelle die Anforderungen für ihre Notifizierung nicht oder nicht mehr erfüllt, so setzt sie den notifizierenden Mitgliedstaat davon in Kenntnis und fordert ihn auf, die erforderlichen Abhilfemaßnahmen zu treffen, einschließlich eines Widerrufs der Notifizierung, sofern dies nötig ist. Versäumt es ein Mitgliedstaat, die erforderlichen Korrekturmaßnahmen zu ergreifen, kann die Kommission die Benennung mittels Durchführungsrechtsakt aussetzen, einschränken oder zurückziehen. 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.
- (2a) Die Kommission sorgt für den Austausch von Wissen und bewährten Verfahren zwischen den nationalen Behörden der Mitgliedstaaten, die für die Notifizierungspolitik zuständig sind.

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**

- (1) Bei Hochrisiko-KI-Systemen und Basismodellen, die mit harmonisierten Normen oder Teilen davon, deren Fundstellen gemäß der Verordnung (EU) 1025/2012 im Amtsblatt der Europäischen Union veröffentlicht wurden, übereinstimmen, wird eine Konformität mit den Anforderungen in Kapitel 2 dieses Artikels oder in Artikel 28b vermutet, soweit diese Anforderungen von den Normen abgedeckt sind.
- (1a) Die Kommission erteilt gemäß Artikel 10 der Verordnung (EU) 1025/2012 spätestens [zwei Monate nach Inkrafttreten dieser Verordnung] Normungsaufträge für alle Anforderungen, die in der Verordnung gestellt werden. Bei der Ausarbeitung des Normungsauftrags konsultiert die Kommission das Amt für KI und das KI-Beratungsforum.
- (1b) Bei der Erteilung eines Normungsauftrags an die europäischen Normungsorganisationen gibt die Kommission an, dass die Normen mit den in Anhang II aufgeführten sektoralen Rechtsvorschriften übereinstimmen müssen und sicherstellen sollen, dass die in der Union in Verkehr gebrachten oder in Betrieb genommenen KI-Systeme oder Basismodelle die in dieser Verordnung festgelegten einschlägigen Anforderungen erfüllen;
- (1c) Die am Normungsprozess beteiligten Akteure berücksichtigen die in Artikel 4 Buchstabe a dargelegten allgemeinen Grundsätze für vertrauenswürdige KI, bemühen sich um die Förderung von Investitionen und Innovationen im Bereich der KI sowie der Wettbewerbsfähigkeit und des Wachstums des Unionsmarktes und tragen zur Stärkung der weltweiten Zusammenarbeit bei der Normung und zur Berücksichtigung bestehender internationaler Normen im Bereich der KI bei, die mit den Werten, Grundrechten und Interessen der Union im Einklang stehen, und stellen eine ausgewogene Vertretung der Interessen und eine wirksame Beteiligung aller relevanten Interessenträger gemäß den Artikeln 5, 6 und 7 der Verordnung (EU) Nr. 1025/2012 sicher.

ARTIKEL 41**GEMEINSAME SPEZIFIKATIONEN**

- (1a) Die Kommission kann im Wege eines Durchführungsrechtsakts, der nach dem Prüfverfahren gemäß Artikel 74 Absatz 2 und nach Anhörung des Amtes für künstliche Intelligenz und des Beratungsforums für künstliche Intelligenz erlassen wird, gemeinsame Spezifikationen für die in Kapitel 2 dieses Titels oder in Artikel 28b genannten Anforderungen festlegen, wenn alle folgenden Bedingungen erfüllt sind:
- a) Es gibt keinen Verweis auf bereits im Amtsblatt der Europäischen Union veröffentlichte harmonisierte Normen, die sich auf die wesentliche(n) Anforderung(en) beziehen, es

sei denn, die betreffende harmonisierte Norm ist eine bestehende Norm, die überarbeitet werden muss;

- b) Die Kommission hat eine oder mehrere europäische Normungsorganisationen mit der Erarbeitung einer harmonisierten Norm für die in Kapitel 2 genannte(n) grundlegende(n) Anforderung(en) beauftragt;
 - c) Der unter Buchstabe b) genannte Auftrag ist bisher von keiner europäischen Normungsorganisation angenommen worden; oder es kommt zu unangemessenen Verzögerungen bei der Festlegung einer geeigneten harmonisierten Norm; oder die bereitgestellte Norm erfüllt nicht die Anforderungen des einschlägigen Unionsrechts oder entspricht nicht der Forderung der Kommission.
- (1b) Wenn die Kommission der Auffassung ist, dass besondere Grundrechtsbelange berücksichtigt werden müssen, müssen die von der Kommission gemäß Absatz 1a angenommenen gemeinsamen Spezifikationen auch diese besonderen Grundrechtsbelange berücksichtigen.
- (1c) Die Kommission entwickelt gemeinsame Spezifikationen für die Methodik zur Erfüllung der Berichterstattungs- und Dokumentationspflicht über den Energie- und Ressourcenverbrauch während der Entwicklung, Trainings und Einführung des Hochrisiko-KI-Systems.
- (2) Bei der Ausarbeitung der in den Absätzen 1a und 1b genannten gemeinsamen Spezifikationen konsultiert die Kommission regelmäßig das Amt für KI und das Beratungsforum, die europäischen Normungsorganisationen und die im Rahmen des einschlägigen sektoralen Unionsrechts eingerichteten Gremien oder Expertengruppen sowie andere relevante Interessenträger. Die Kommission hat die in Artikel 40 Absatz 1c genannten Ziele zu erfüllen und ordnungsgemäß zu begründen, warum sie beschlossen hat, auf gemeinsame Spezifikationen zurückzugreifen.
- Beabsichtigt die Kommission, gemeinsame Spezifikationen gemäß Absatz 1a des vorliegenden Artikels zu erlassen, so gibt sie auch klar an, welches spezifische Grundrechtsanliegen behandelt werden soll.
- Bei der Annahme gemeinsamer Spezifikationen gemäß den Absätzen 1a und 1b des vorliegenden Artikels berücksichtigt die Kommission die Stellungnahme des in Artikel 56e Buchstabe b der vorliegenden Verordnung genannten Amtes für KI. Beschließt die Kommission, der Stellungnahme des Amtes für KI nicht zu folgen, so legt sie dem Amt für KI eine begründete Erklärung vor.
- (3) Bei Hochrisiko-KI-Systemen, die mit den in den Absätzen 1a und 1b 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.
- (3a) Wird eine harmonisierte Norm von einer europäischen Normungsorganisation angenommen und der Kommission zur Veröffentlichung ihrer Fundstelle im Amtsblatt der Europäischen

Union vorgeschlagen, so bewertet die Kommission die harmonisierte Norm gemäß der Verordnung (EU) Nr. 1025/2012. Wird die Fundstelle einer harmonisierten Norm im Amtsblatt der Europäischen Union veröffentlicht, so hebt die Kommission die in den Absätzen 1 und 1b genannten Rechtsakte oder Teile davon auf, die dieselben Anforderungen gemäß Kapitel 2 dieses Titels betreffen.

- (4) Wenn Anbieter von Hochrisiko-KI-Systemen die in Absatz 1 genannten gemeinsamen Spezifikationen nicht befolgen, müssen sie hinreichend nachweisen, dass sie technische Lösungen verwenden, die den in Kapitel II genannten Anforderungen 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, kontextuellen und funktionalen Rahmenbedingungen, unter denen sie bestimmungsgemäß verwendet werden sollen, trainiert und getestet wurden, die Vermutung, dass sie die in Artikel 10 Absatz 4 festgelegten jeweiligen Anforderungen erfüllen.
- (2) Für Hochrisiko-KI-Systeme, die im Rahmen eines der Cybersicherheitszertifizierungssysteme gemäß der Verordnung (EU) 2019/881 des Europäischen Parlaments und des Rates⁵⁹, 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 entscheidet er sich für eines der folgenden Verfahren:
 - (a) das Konformitätsbewertungsverfahren auf der Grundlage einer internen Kontrolle gemäß Anhang VI; oder

⁵⁹ 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).

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

Zum Nachweis, dass sein Hochrisiko-KI-System die Anforderungen in Kapitel 2 dieses Titels erfüllt, muss der Anbieter in den folgenden Fällen das Konformitätsbewertungsverfahren gemäß Anhang VII anwenden:

- (a) Wenn es keine harmonisierten Normen gemäß Artikel 40 gibt, deren Fundstelle im Amtsblatt der Europäischen Union veröffentlicht wurde und die alle relevanten Sicherheitsanforderungen für das KI-System abdecken, und keine gemeinsamen Spezifikationen gemäß Artikel 41 vorliegen;
- (b) Wenn die unter Buchstabe a genannten technischen Spezifikationen zwar vorliegen, der Anbieter sie aber nicht oder nur teilweise angewandt hat;
- (c) Wenn eine oder mehrere der unter Buchstabe a genannten technischen Spezifikationen mit einer Einschränkung und nur für den eingeschränkten Teil der Norm veröffentlicht wurden;
- (d) Wenn der Anbieter der Ansicht ist, dass Art, Gestaltung, Konstruktion oder Zweckbestimmung des KI-Systems eine Überprüfung durch Dritte erfordern, unabhängig von seinem Risikoniveau.

Für die Zwecke der Durchführung 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 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, die bereits Gegenstand eines Konformitätsbewertungsverfahrens gewesen sind, werden einem neuen Konformitätsbewertungsverfahren unterzogen, wenn sie wesentlich geändert werden, unabhängig davon, ob das geänderte System noch weiter in Verkehr gebracht oder vom derzeitigen Betreiber 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.

- (4a) Bei der Festsetzung der Gebühren für die Konformitätsbewertung durch Dritte nach diesem Artikel werden die besonderen Interessen und Bedürfnisse von KMU berücksichtigt, indem diese Gebühren proportional zu ihrer Größe und der Größe ihres Marktes gesenkt werden.
- (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. Bei der Vorbereitung solcher delegierten Rechtsakte konsultiert die Kommission das Amt für KI und die betroffenen Interessenträger.
- (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. Bei der Vorbereitung solcher delegierten Rechtsakte konsultiert die Kommission das Amt für KI und die betroffenen Interessenträger.

ARTIKEL 44**BESCHEINIGUNGEN**

- (1) Die von notifizierten Stellen gemäß Anhang VII erteilten Bescheinigungen werden in einer oder mehreren Amtssprachen der Union ausgefertigt, die der Mitgliedstaat, in dem die notifizierte Stelle niedergelassen ist, festlegt, oder in einer oder mehreren anderen Amtssprachen der Union, mit der die notifizierte Stelle einverstanden ist.
- (2) Die Bescheinigungen sind für die darin genannte Dauer gültig, die maximal vier 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 vier 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, 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 – auch in Bezug auf ausgestellte Konformitätsbescheinigungen – 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 Auskunftersuchen 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 notifizierte 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 notifizierte Stellen, die ähnlichen Konformitätsbewertungstätigkeiten 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 nationale Aufsichtsbehörde von einer Justizbehörde fordern, das Inverkehrbringen oder die Inbetriebnahme bestimmter Hochrisiko-KI-Systeme im Hoheitsgebiet des betreffenden Mitgliedstaats aus außergewöhnlichen Gründen des Schutzes des Lebens und der Gesundheit von Personen, des Umweltschutzes und des Schutzes kritischer Infrastruktur zu 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 nationale Aufsichtsbehörde und die Justizbehörde zu dem Schluss gelangen, dass das Hochrisiko-KI-System die Anforderungen in Kapitel 2 dieses Titels erfüllt. Die nationale Aufsichtsbehörde unterrichtet die Kommission, das Amt für künstliche Intelligenz und die anderen Mitgliedstaaten über alle gestellten Anträge und alle diesbezüglichen 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 den Antrag der nationalen Aufsichtsbehörde auf eine von einer nationalen Aufsichtsbehörde 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 einen von einer nationalen Aufsichtsbehörde eines anderen Mitgliedstaats gestellten Antrag 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 und dem Amt für künstliche Intelligenz 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 nationalen Aufsichtsbehörde 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 Hochrisiko-KI-System eine schriftliche maschinenlesbare, physische oder elektronische EU-Konformitätserklärung aus und hält sie für einen Zeitraum von 10 Jahren ab dem Inverkehrbringen oder der Inbetriebnahme des Hochrisiko-KI-Systems für die nationale Aufsichtsbehörde und die zuständigen nationalen Behörden bereit. Ein Exemplar der EU-Konformitätserklärung wird der nationalen Aufsichtsbehörde und den zuständigen nationalen Behörden auf Anfrage übermittelt
- (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 in Verkehr gebracht oder bereitgestellt wird.
- (3) Unterliegen Hochrisiko-KI-Systeme noch anderen Harmonisierungsrechtsvorschriften der Union, die ebenfalls eine EU-Konformitätserklärung vorschreiben, so kann eine einzige EU-Konformitätserklärung ausgestellt werden, 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) Nach Anhörung des Amts für künstliche Intelligenz wird der Kommission 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 physische CE-Kennzeichnung wird gut sichtbar, leserlich und dauerhaft an Hochrisiko-KI-Systemen angebracht, bevor das Hochrisiko-KI-System in Verkehr gebracht wird. Falls die Art des Hochrisiko-KI-Systems dies nicht zulässt oder nicht rechtfertigt, wird sie auf der Verpackung oder gegebenenfalls den Begleitunterlagen angebracht. Dahinter kann ein Piktogramm oder ein anderes Zeichen stehen, das eine besondere Verwendungsgefahr angibt .
- (1a) Bei ausschließlich digitalen Hochrisiko-KI-Systemen wird eine digitale CE-Kennzeichnung nur dann verwendet, wenn sie über die Schnittstelle, von der aus auf das KI-System zugegriffen wird, oder über einen maschinenlesbaren Code oder andere elektronische Mittel angezeigt werden kann.
- (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 der notifizierten Stelle ist entweder von der Stelle selbst oder nach ihren Anweisungen durch den Bevollmächtigten des Anbieters anzubringen. 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.
- (3a) Falls Hochrisiko-KI-Systeme ferner unter andere Rechtsvorschriften der Union fallen, in denen die CE-Kennzeichnung auch vorgesehen ist, bedeutet die CE-Kennzeichnung, dass das Hochrisiko-KI-System auch die Anforderungen dieser anderen Rechtsvorschriften 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 nationale Aufsichtsbehörde und 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**

- (1) 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 gemäß Artikel 60 Absatz 2 in der in Artikel 60 genannten EU-Datenbank .
- (1a) Vor der Inbetriebnahme oder der Nutzung eines Hochrisiko-KI-Systems gemäß Artikel 6 Absatz 2 registrieren die folgenden Kategorien von Betreibern die Nutzung dieses KI-Systems in der in Artikel 60 genannten EU-Datenbank:
 - a) Betreiber, die Behörden oder Organe, Einrichtungen und sonstige Stellen der Union sind, oder Betreiber, die in deren Namen handeln;
 - b) Betreiber, die nach Verordnung (EU) 2022/1925 als Gatekeeper benannte Unternehmen sind.
- (1b) Betreiber, die nicht unter Unterabsatz 1 a fallen, sind berechtigt, die Verwendung eines Hochrisiko-KI-Systems im Sinne von Artikel 6 Absatz 2 freiwillig in der EU-Datenbank gemäß Artikel 60 zu registrieren.
- (1c) Unmittelbar nach jeder wesentlichen Änderung muss ein aktualisierter Registrierungseintrag vorgenommen werden.

TITEL IV
TRANSPARENZPFLICHTEN

ARTIKEL 52
TRANSPARENZPFLICHTEN

- (1) Die Anbieter stellen sicher, dass KI-Systeme, die für die Interaktion mit natürlichen Personen bestimmt sind, so konzipiert und entwickelt werden, dass das KI-System, der Anbieter selbst oder der Nutzer die natürliche Person, die einem KI-System ausgesetzt ist, rechtzeitig, klar und verständlich darüber informiert, dass sie es mit einem KI-System zu tun hat, es sei denn, dies ist aufgrund der Umstände und des Kontexts der Nutzung offensichtlich.

Soweit angemessen und sachdienlich, umfassen diese Informationen auch, welche Funktionen KI-gestützt sind, ob es eine menschliche Aufsicht gibt und wer für den Entscheidungsprozess verantwortlich ist, sowie die bestehenden Rechte und Verfahren, die es natürlichen Personen oder ihren Vertretern nach dem Unionsrecht und dem nationalen Recht ermöglichen, gegen die Anwendung solcher Systeme auf sie Einspruch zu erheben und gerichtlichen Rechtsbehelf gegen Entscheidungen, die von KI-Systemen getroffen wurden, oder gegen Schäden, die durch sie verursacht wurden, einzulegen, einschließlich ihres Rechts, eine Erklärung zu verlangen. 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, das nicht gemäß Artikel 5 verboten ist, informieren die davon betroffenen natürlichen Personen rechtzeitig, klar und verständlich über den Betrieb des Systems und holen ihre Einwilligung vor der Verarbeitung ihrer biometrischen und sonstigen personenbezogenen Daten gemäß der Verordnung (EU) 2016/679, der Verordnung (EU) 2016/1725 bzw. der Richtlinie (EU) 2016/280 ein. 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 Text-, Audio- oder visuelle Inhalte erzeugt oder manipuliert, die fälschlicherweise als echt oder wahrhaftig erscheinen würden und in denen Personen ohne ihre Zustimmung dargestellt werden, die scheinbar Dinge sagen oder tun, die sie nicht gesagt oder getan haben („Deepfake“), müssen in angemessener, zeitnaher, klarer und sichtbarer Weise offenlegen, dass die Inhalte künstlich erzeugt oder manipuliert wurden, sowie, wann immer möglich, den Namen der natürlichen oder juristischen Person, die sie erstellt oder manipuliert hat. Offenlegung bedeutet, dass der Inhalt in einer Weise gekennzeichnet wird, die darüber informiert, dass der Inhalt nicht echt ist, und die für den Empfänger dieses Inhalts deutlich sichtbar ist. Bei der Kennzeichnung der Inhalte berücksichtigen die Nutzer den

allgemein anerkannten Stand der Technik und die einschlägigen harmonisierten Normen und Spezifikationen.

- (3a) Absatz 3 gilt nicht, wenn die Verwendung eines KI-Systems, das Text-, Audio- oder visuelle Inhalte erzeugt oder manipuliert, 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. Wenn der Inhalt Teil eines offensichtlich kreativen, satirischen, künstlerischen oder fiktionalen Filmwerks, Videospiele, visuellen Werks oder analogen Programms ist, so beschränken sich die Transparenzpflichten gemäß Absatz 3 darauf, das Vorhandensein solcher generierten oder manipulierten Inhalte in geeigneter, klarer und sichtbarer Weise offenzulegen, die die Darstellung des Werks nicht beeinträchtigt, und gegebenenfalls die geltenden Urheberrechte offenzulegen. Sie hindern die Strafverfolgungsbehörden auch nicht daran, KI-Systeme zu verwenden, die dazu bestimmt sind, Deepfakes aufzudecken und Straftaten im Zusammenhang mit ihrer Verwendung zu verhindern, zu untersuchen und zu verfolgen.(4)

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

- (3b) Die in den Absätzen 1 bis 3 genannten Informationen werden den natürlichen Personen spätestens zum Zeitpunkt der ersten Interaktion oder Aussetzung bereitgestellt. Sie sind schutzbedürftigen Personen, etwa Menschen mit Behinderungen oder Kindern, zugänglich, und, sofern relevant und möglich, sind ergänzende Verfahren für die Intervention sowie die Meldung und Kennzeichnung von Inhalten seitens der betroffenen natürlichen Personen unter Berücksichtigung des allgemein anerkannten Stands der Technik und der einschlägigen harmonisierten Normen und gemeinsamen Spezifikationen vorzusehen.

TITEL V

MAßNAHMEN ZUR INNOVATIONSFÖRDERUNG

ARTIKEL 53

KI-REALLABORE

- (1) Die Mitgliedstaaten richten mindestens ein KI-Reallabor auf nationaler Ebene ein, das spätestens am Tag des Inkrafttretens dieser Verordnung betriebsbereit ist. Dieses Reallabor kann auch gemeinsam mit einem oder mehreren anderen Mitgliedstaaten eingerichtet werden.
- (1a) Es können auch zusätzliche KI-Reallabore auf regionaler oder lokaler Ebene oder gemeinsam mit anderen Mitgliedstaaten eingerichtet werden;

- (1b) Die Kommission und der Europäische Datenschutzbeauftragte können, entweder allein, gemeinsam oder in Zusammenarbeit mit einem oder mehreren Mitgliedstaaten, ebenfalls KI-Reallabore auf Unionsebene einrichten;
- (1c) Die einrichtenden Behörden stellen ausreichende Mittel bereit, um diesem Artikel wirksam und rechtzeitig nachzukommen;
- (1d) KI-Reallabore bieten gemäß den in Artikel 53 a festgelegten Kriterien eine kontrollierte Umgebung, um Innovation zu fördern und die Entwicklung, Erprobung und Validierung innovativer KI-Systeme für einen begrenzten Zeitraum vor ihrem Inverkehrbringen oder ihrer Inbetriebnahme nach einem bestimmten zwischen den zukünftigen Anbietern und der einrichtenden Behörde vereinbarten Plan zu erleichtern;
- (1e) Die Einrichtung von KI-Reallaboren soll zu den folgenden Zielen beitragen:
 - a) dass die zuständigen Behörden den zukünftigen Anbietern von KI-Systemen Anleitung bieten, um die Einhaltung dieser Verordnung oder gegebenenfalls anderer geltender Rechtsvorschriften der Union und der Mitgliedstaaten sicherzustellen;
 - b) dass die zukünftigen Anbieter die Erprobung und Entwicklung innovativer Lösungen im Zusammenhang mit KI-Systemen ermöglichen und erleichtern;
 - c) regulatorisches Lernen in einem kontrollierten Umfeld.
- (1f) Die einrichtenden Behörden bieten Anleitung und Aufsicht innerhalb des Reallabors, um Risiken, insbesondere für die Grundrechte, die Demokratie und die Rechtsstaatlichkeit, die Gesundheit und die Sicherheit sowie die Umwelt zu ermitteln, Maßnahmen zur Minderung ermittelter Risiken und deren Wirksamkeit zu prüfen und nachzuweisen und die Einhaltung der Anforderungen dieser Verordnung und gegebenenfalls anderer Rechtsvorschriften der Union und der Mitgliedstaaten sicherzustellen;
- (1g) Die einrichtenden Behörden bieten den zukünftigen Anbietern von Reallaboren, die Hochrisiko-KI-Systeme entwickeln, Anleitung und Aufsicht bei der Erfüllung der in dieser Verordnung festgelegten Anforderungen, sodass die KI-Systeme unter Annahme der Konformität mit den spezifischen Anforderungen dieser Verordnung, die im Reallabor bewertet wurden, aussteigen können. Sofern das KI-System beim Ausstieg aus dem Reallabor die Anforderungen erfüllt, wird von einer Konformität mit dieser Verordnung ausgegangen. In diesem Zusammenhang werden die von der einrichtenden Behörde erstellten Ausstiegsberichte je nach Fall von den Marktüberwachungsbehörden oder den notifizierten Stellen im Rahmen von Konformitätsbewertungsverfahren oder Marktüberwachungsprüfungen berücksichtigt.
- (2) Soweit die innovativen KI-Systeme personenbezogene Daten verarbeiten oder anderweitig der Aufsicht anderer nationaler Behörden oder zuständiger Behörden unterstehen, die den Zugang zu personenbezogenen Daten gewähren oder unterstützen, sorgen die einrichtenden Behörden dafür, dass die nationalen Datenschutzbehörden oder in den in Absatz 1 b

genannten Fällen der EDSB und diese anderen nationalen Behörden in den Betrieb des KI-Reallabors sowie in die Überwachung dieser Aspekte im vollen Umfang ihrer entsprechenden Aufgaben und Befugnisse einbezogen werden.

- (3) Die KI-Reallabore lassen die Aufsichts- und Abhilfebefugnisse der zuständigen Behörden, einschließlich auf regionaler oder lokaler Ebene, unberührt. Alle erheblichen Risiken für die Grundrechte, Demokratie und Rechtsstaatlichkeit, Gesundheit und Sicherheit oder die Umwelt, die bei der Entwicklung und Erprobung solcher KI-Systeme festgestellt werden, führen zur sofortigen und angemessenen Risikominderung. Die zuständigen Behörden sind befugt, den Erprobungsprozess oder die Teilnahme am Reallabor vorübergehend oder dauerhaft auszusetzen, wenn keine wirksame Risikominderung möglich ist, und unterrichten das Amt für künstliche Intelligenz über diese Entscheidung
- (4) Die zukünftigen Anbieter im KI-Reallabor bleiben nach geltendem Recht der Union und der Mitgliedstaaten für Schäden haftbar, die Dritten infolge der Erprobung im Reallabor entstehen. Sofern die zukünftigen Anbieter den in Absatz 1c genannten spezifischen Plan und die Bedingungen für ihre Beteiligung beachten und in gutem Glauben die von den einrichtenden Behörden bereitgestellten Anleitung befolgen, werden jedoch von den Behörden keine Geldbußen für Verstöße gegen diese Verordnung verhängt.
- (5) Die einrichtenden Behörden koordinieren ihre Tätigkeiten und arbeiten im Rahmen des Amts für künstliche Intelligenz zusammen.
- (5a) Die einrichtenden Behörden unterrichten das Amt für künstliche Intelligenz über die Einrichtung eines Reallabors und können um Unterstützung und Anleitung bitten. Eine Liste der geplanten und bestehenden Reallabore wird vom Amt für künstliche Intelligenz öffentlich zugänglich gemacht und auf dem neuesten Stand gehalten, um eine stärkere Interaktion in den Reallaboren und die transnationale Zusammenarbeit zu fördern.
- (5b) Die einrichtenden Behörden übermitteln dem Amt für künstliche Intelligenz und, sofern die Kommission nicht die einzige einrichtende Behörde ist, der Kommission jährliche Berichte, und zwar erstmals ein Jahr nach der Einrichtung des Reallabors und dann jedes Jahr bis zu dessen Beendigung sowie einen Abschlussbericht. Diese Berichte informieren über den Fortschritt und die Ergebnisse der Umsetzung dieser Reallabore, einschließlich bewährter Verfahren, Vorfällen, gewonnener Erkenntnisse und Empfehlungen zu deren Aufbau, sowie gegebenenfalls über die Anwendung und mögliche Überarbeitung dieser Verordnung und anderen Rechtsvorschriften der Union, die innerhalb des Reallabors kontrolliert werden. Diese jährlichen Berichte oder Zusammenfassungen davon werden der Öffentlichkeit im Internet zur Verfügung gestellt.
- (6) Die Kommission richtet eine eigene Schnittstelle, die alle relevanten Informationen zu den Reallaboren enthält, sowie eine zentrale Kontaktstelle auf Unionsebene ein, um mit den Reallaboren zu interagieren und den Interessenträgern die Möglichkeit zu geben, Anfragen an

die zuständigen Behörden zu richten und unverbindliche Beratung zur Konformität innovativer Produkte, Dienstleistungen und Geschäftsmodelle mit integrierter KI-Technologie einzuholen;

Die Kommission stimmt sich proaktiv mit den nationalen, regionalen und gegebenenfalls auch lokalen Behörden ab.

- (6a) Für die Zwecke der Absätze 1 und 1a übernimmt die Kommission eine ergänzende Rolle, indem sie einerseits den Mitgliedstaaten die Möglichkeit gibt, auf ihrem Fachwissen aufzubauen, und andererseits jenen Mitgliedstaaten, die sich bei der Einrichtung und dem Betrieb dieser Reallabore beraten lassen wollen, mit technischen Schulungen und Ressourcen zur Seite steht.

ARTIKEL 53A

MODALITÄTEN UND FUNKTIONSWEISE VON KI-REALLABOREN

- (1) Um eine Zersplitterung in der Union zu vermeiden, erlässt die Kommission in Absprache mit dem Amt für künstliche Intelligenz einen delegierten Rechtsakt, in dem die Modalitäten für die Einrichtung, Entwicklung, Umsetzung, Funktionsweise und Überwachung der KI-Reallabore, einschließlich der Genehmigungskriterien und des Verfahrens für die Beantragung, die Auswahl, die Beteiligung und den Ausstieg aus dem Reallabor sowie der Rechte und Pflichten der Teilnehmer auf der Grundlage der Bestimmungen dieses Artikels festgelegt werden.
- (2) Der Kommission wird die Befugnis übertragen, delegierte Rechtsakte gemäß dem Verfahren in Artikel 73 innerhalb von 12 Monaten nach Inkrafttreten dieser Verordnung zu erlassen, und sie sorgt dafür, dass
- a) Reallabore allen zukünftigen Anbietern eines KI-Systems, die einen Antrag stellen und die Eignungs- und Auswahlkriterien erfüllen, offen stehen. Die Kriterien für den Zugang zu den Reallaboren sind transparent und fair, und die einrichtenden Behörden teilen den Antragstellern ihre Entscheidung innerhalb von drei Monaten nach der Antragstellung mit;
 - b) die Reallabore einen breiten und gleichberechtigten Zugang ermöglichen und mit der Nachfrage nach Beteiligung Schritt halten;
 - c) der Zugang zu KI-Reallaboren für KMU und Start-ups kostenlos ist, unbeschadet außergewöhnlicher Kosten, die einrichtende Behörden in einer fairen und verhältnismäßigen Weise einfordern können;
 - d) Reallabore die Einbeziehung anderer relevanter Akteure innerhalb des KI-Ökosystems, wie etwa notifizierte Stellen und Normungsorganisationen (KMU, Start-ups, Unternehmen, Innovatoren, Erprobungs- und Versuchseinrichtungen, Forschungs- und Versuchslabore und digitale Innovationszentren, Kompetenzzentren, einzelne

Forscher) begünstigen, um die Zusammenarbeit mit dem öffentlichen und privaten Sektor zu ermöglichen und zu erleichtern;

- e) sie zukünftigen Anbietern ermöglichen, ihren Verpflichtungen zur Konformitätsbewertung nach dieser Verordnung oder der freiwilligen Anwendung der in Artikel 69 genannten Verhaltenskodizes in einem kontrollierten Umfeld nachzukommen;
 - f) die Verfahren, Prozesse und administrativen Anforderungen für die Antragstellung, die Auswahl, die Teilnahme und den Ausstieg aus dem Reallabor einfach, leicht verständlich und klar kommuniziert sind, um die Teilnahme von KMU und Start-ups mit begrenzten rechtlichen und administrativen Kapazitäten zu erleichtern, und unionsweit gestrafft sind, um eine Zersplitterung zu vermeiden, und dass die Teilnahme an einem von einem Mitgliedstaat, der Kommission oder dem EDSB eingerichteten Reallabor gegenseitig und einheitlich anerkannt wird und in der gesamten Union die gleiche Rechtswirkung hat;
 - g) die Beteiligung an dem KI-Reallabor auf einen der Komplexität und dem Umfang des Projekts entsprechenden Zeitraum beschränkt ist;
 - h) die Reallabore die Entwicklung von Tools und Infrastruktur für die Erprobung, das Benchmarking, die Bewertung und die Erklärung der Dimensionen von KI-Systemen, die für Reallabore von Bedeutung sind, etwa Genauigkeit, Robustheit und Cybersicherheit, sowie die Minimierung der Risiken für die Grundrechte, die Umwelt und die Gesellschaft als Ganzes, erleichtern.
- (3) Zukünftige Anbieter in den Reallaboren, insbesondere KMU und Start-ups, Zugang zu im Voraus bereitgestellten Dienstleistungen erhalten, z. B. zu Leitlinien für die Umsetzung dieser Verordnung, zu anderen wertvollen Dienstleistungen wie Hilfe bei Normungsdokumenten und Zertifizierungen und Konsultation sowie zu weiteren Initiativen des digitalen Binnenmarkts wie Erprobungs- und Versuchseinrichtungen, digitalen Knotenpunkten, Kompetenzzentren und EU-Benchmarking-Fähigkeiten.

ARTIKEL 54

WEITERVERARBEITUNG VON DATEN ZUR ENTWICKLUNG BESTIMMTER KI-SYSTEME IM ÖFFENTLICHEN INTERESSE IM KI-REALLABOR

- (1) Im KI-Reallabor können personenbezogene Daten, die rechtmäßig für andere Zwecke erhoben wurden, ausschließlich zur Entwicklung und Erprobung bestimmter KI-Systeme im Reallabor verarbeitet werden, wenn alle nachstehenden Bedingungen erfüllt sind:
 - a) KI-Systeme werden entwickelt, um ein erhebliches öffentliches Interesse in einem oder mehreren der folgenden Bereiche zu wahren:
 - ii) öffentliche Sicherheit und öffentliche Gesundheit, einschließlich Erkennung, Diagnose, Verhütung, Bekämpfung und Behandlung von Krankheiten,

- iii) hohes Umweltschutzniveau und Verbesserung der Umweltqualität, Schutz der biologischen Vielfalt, Umweltverschmutzung sowie Klimaschutz und Anpassung an den Klimawandel;
 - iiia) Sicherheit und Widerstandsfähigkeit von Verkehrssystemen, kritischen Infrastrukturen und Netzen.
- 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 Rechte und Freiheiten der betroffenen Personen gemäß Artikel 35 der Verordnung (EU) 2016/679 und gemäß Artikel 39 der Verordnung (EU) 2018/1725 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 zukünftigen Anbieter, 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, und berührt nicht die Anwendung ihrer Rechte gemäß den Rechtsvorschriften der Union über den Schutz personenbezogener Daten;
- g) personenbezogene Daten, die im Rahmen des Reallabors verarbeitet wurden, sind durch geeignete technische und organisatorische Maßnahmen geschützt und 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 aufbewahrt;
- 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-Systems, seiner Ziele, Hypothesen 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 54A

FÖRDERUNG DER KI-FORSCHUNG UND -ENTWICKLUNG ZUR UNTERSTÜTZUNG SOZIAL UND ÖKOLOGISCH VORTEILHAFTER RESULTATE

- (1) Die Mitgliedstaaten fördern die Forschung und Entwicklung von KI-Lösungen, die sozial und ökologisch vorteilhafte Ergebnisse unterstützen, einschließlich, aber nicht beschränkt auf die Entwicklung von KI-basierten Lösungen zur Verbesserung der Zugänglichkeit für Menschen mit Behinderungen, zur Beseitigung sozioökonomischer Ungleichheiten und zur Erfüllung von Nachhaltigkeits- und Umweltzielen, durch:
- a) vorrangigen Zugang relevanter Projekte zu den KI-Reallaboren, sofern sie die Voraussetzungen für die Auswahlkriterien erfüllen;
 - b) Bereitstellung öffentlicher Mittel, auch aus den einschlägigen EU-Fonds, für die KI-Forschung und -Entwicklung zur Unterstützung sozial und ökologisch vorteilhafter Resultate;
 - c) Organisation spezifischer Sensibilisierungsmaßnahmen über die Anwendung dieser Verordnung, die Verfügbarkeit von und die Antragsverfahren für gezielte Finanzierung, die auf die Bedürfnisse dieser Projekte zugeschnitten sind;
 - d) gegebenenfalls die Einrichtung zugänglicher gezielter Kanäle, auch innerhalb der Reallabore, für die Kommunikation mit den Projekten, um Anleitungen zu geben und Anfragen zur Umsetzung dieser Verordnung zu beantworten.
- (2) Die Mitgliedstaaten unterstützen die Zivilgesellschaft und die gesellschaftlichen Akteure bei der Leitung von oder der Beteiligung an solchen Projekten.

ARTIKEL 55

MAßNAHMEN FÜR KMU, START-UP-UNTERNEHMEN UND NUTZER

- (1) Die Mitgliedstaaten ergreifen folgende Maßnahmen:

- a) Gewährung eines vorrangigen Zugangs zu den KI-Reallaboren für in der Union niedergelassene KMU und Start-up-Unternehmen, soweit sie die entsprechenden Voraussetzungen erfüllen;
 - b) Durchführung besonderer Sensibilisierungsmaßnahmen für die Anwendung dieser Verordnung, die auf die Bedürfnisse von KMU, Start-up-Unternehmen und Nutzern ausgerichtet sind;
 - c) Nutzung der entsprechenden bestehenden Kanäle und gegebenenfalls Einrichtung neuer eigener Kanäle für die Kommunikation mit KMU, Start-up-Unternehmen, Nutzern und anderen Innovatoren, um Orientierungen zu geben und Fragen zur Durchführung dieser Verordnung zu beantworten;
 - ca) Förderung der Beteiligung von KMU und anderen einschlägigen Interessenträgern an der Entwicklung von Normen.
- (2) Bei der Festsetzung der Gebühren für die Konformitätsbewertung gemäß Artikel 43 werden die besonderen Interessen und Bedürfnisse von KMU, Start-up-Unternehmen und Nutzern berücksichtigt, indem diese Gebühren proportional zum Entwicklungsstadium, zu ihrer Größe, der Größe ihres Marktes und der Marktnachfrage gesenkt werden. Die Kommission bewertet regelmäßig die Zertifizierungs- und Befolgungskosten für KMU und Start-up-Unternehmen, unter anderem durch transparente Konsultationen mit KMU, Start-up-Unternehmen und Nutzern, und arbeitet mit den Mitgliedstaaten zusammen, um diese Kosten nach Möglichkeit zu senken. Die Kommission erstattet dem Europäischen Parlament und dem Rat im Rahmen des Berichts über die Bewertung und Überarbeitung dieser Verordnung gemäß Artikel 84 Absatz 2 Bericht über diese Ergebnisse.

TITEL VI

LEISTUNGSSTRUKTUR

KAPITEL 1

EUROPÄISCHER AUSSCHUSS FÜR KÜNSTLICHE INTELLIGENZ

ABSCHNITT 1

ALLGEMEINE BESTIMMUNGEN ÜBER DAS EUROPÄISCHE AMT FÜR KÜNSTLICHE INTELLIGENZ

ARTIKEL 56

EINRICHTUNG DES EUROPÄISCHEN AMTS FÜR KÜNSTLICHE INTELLIGENZ

- (1) Das „Europäische Amt für künstliche Intelligenz“ (im Folgenden „Amt für künstliche Intelligenz“) wird hiermit eingerichtet. Das Amt für künstliche Intelligenz ist eine selbständige Einrichtung der Union. Es besitzt Rechtspersönlichkeit.

- (2) Das Amt für künstliche Intelligenz hat ein Sekretariat und wird angemessen mit Mitteln und Personal ausgestattet, um seine Aufgaben gemäß dieser Verordnung wahrzunehmen.
- 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.
- (2a) Das Amt für künstliche Intelligenz hat seinen Sitz in Brüssel.

ARTIKEL 56A

STRUKTUR

Die Verwaltungs- und Leitungsstruktur des Amts für künstliche Intelligenz umfasst

- a) einen Verwaltungsrat, einschließlich eines Vorsitzes,
- b) ein von einem Verwaltungsdirektor geleitetes Sekretariat
- c) einen Beirat.

ARTIKEL 56B

AUFGABEN DES AMTS FÜR KÜNSTLICHE INTELLIGENZ

Das Amt für künstliche Intelligenz nimmt folgende Aufgaben wahr:

- a) Unterstützung, Beratung und Zusammenarbeit mit den Mitgliedstaaten, den nationalen Aufsichtsbehörden, der Kommission und anderen Organen, Einrichtungen, Ämtern und Agenturen der Union bei der Durchführung dieser Verordnung;
- b) Überwachung und Sicherstellung der wirksamen und einheitlichen Anwendung dieser Verordnung unbeschadet der Aufgaben der nationalen Aufsichtsbehörden;
- c) Beteiligung an der Koordinierung zwischen den für die Anwendung dieser Verordnung zuständigen nationalen Aufsichtsbehörden;
- d) Vermittlerfunktion bei Diskussionen über schwerwiegende Meinungsverschiedenheiten, die sich zwischen den zuständigen Behörden hinsichtlich der Anwendung der Verordnung ergeben können;
- e) Koordinierung der gemeinsamen Untersuchungen gemäß Artikel 66a;

- f) Beitrag zur wirksamen Zusammenarbeit mit den zuständigen Behörden von Drittstaaten und mit internationalen Organisationen;
- g) Sammlung von Fachwissen und bewährten Verfahren und deren Austausch zwischen den Mitgliedstaaten sowie Unterstützung der nationalen Aufsichtsbehörden der Mitgliedstaaten und der Kommission bei der Entwicklung des für die Umsetzung dieser Verordnung erforderlichen organisatorischen und technischen Fachwissens, unter anderem durch die Förderung der Schaffung und Pflege eines Expertenpools der Union;
- h) Sammlung von Fachwissen und bewährten Verfahren und deren Austausch zwischen den Mitgliedstaaten sowie Unterstützung der nationalen Aufsichtsbehörden der Mitgliedstaaten und der Kommission bei der Entwicklung des für die Umsetzung dieser Verordnung erforderlichen organisatorischen und technischen Fachwissens, unter anderem durch die Förderung der Schaffung und Pflege eines Expertenpools der Union;
 - i) technische Spezifikation oder bestehende Normen;
 - ii) die Leitlinien der Kommission
 - iii) Verhaltenskodizes und deren Anwendung in enger Zusammenarbeit mit der Industrie und anderen einschlägigen Interessenträgern;
 - iv) die mögliche Überarbeitung der Verordnung, die Ausarbeitung der delegierten Rechtsakte und mögliche Anpassungen dieser Verordnung an die in Anhang II aufgeführten Rechtsakte;
 - v) Trends, wie z. B. die globale Wettbewerbsfähigkeit Europas im Bereich der künstlichen Intelligenz, die Übernahme von künstlicher Intelligenz in der Union, die Entwicklung digitaler Fähigkeiten und neu auftretende systemische Bedrohungen im Zusammenhang mit künstlicher Intelligenz;
 - vi) Empfehlungen, wie diese Verordnung auf die sich ständig weiterentwickelnde Typologie der KI-Wertschöpfungsketten, insbesondere auf die sich daraus ergebenden Auswirkungen auf die Rechenschaftspflicht aller beteiligten Stellen, Anwendung findet.
- i) Veröffentlichung
 - i) eines jährlichen Berichts mit einer Bewertung der Durchführung dieser Verordnung, einer Überprüfung der Meldungen schwerwiegender Vorfälle gemäß Artikel 62 und das Funktionieren der in Artikel 60 genannten Datenbank sowie
 - ii) von Empfehlungen an die Kommission zur Einstufung von verbotenen Praktiken, zu den in Anhang III genannten Hochrisiko-KI-Systemen, zu den in Artikel 69 genannten Verhaltenskodizes und zur Anwendung der in Artikel 4a dargelegten allgemeinen Grundsätze.
- j) Unterstützung der Behörden bei der Einrichtung und Entwicklung von Reallaboren und Erleichterung der Zusammenarbeit zwischen den Reallaboren;

- k) Veranstaltung von Sitzungen mit Agenturen und leitenden Organen der Union, deren Aufgaben mit künstlicher Intelligenz und der Durchführung dieser Verordnung zu tun haben;
- l) Abhaltung von vierteljährlichen Anhörungen mit dem Beirat und gegebenenfalls von öffentlichen Anhörungen mit anderen Interessenträgern sowie Veröffentlichung der Ergebnisse dieser Anhörungen auf seiner Website;
- m) Sensibilisierung und Aufklärung der Öffentlichkeit in Bezug auf die Vorteile, Risiken, Schutzmaßnahmen, Rechte und Pflichten im Zusammenhang mit der Nutzung von KI-Systemen;
- n) Erleichterung der Entwicklung gemeinsamer Kriterien und eines gemeinsamen Verständnisses der Marktteilnehmer und der zuständigen Behörden in Bezug auf die in dieser Verordnung vorgesehenen einschlägigen Konzepte;
- o) Überwachung von Basismodellen und Veranstaltung eines regelmäßigen Dialogs mit den Entwicklern von Basismodellen in Bezug auf deren Konformität sowie von KI-Systemen, die solche KI-Modelle nutzen;
- p) Bereitstellung eines Auslegungsleitfadens, wie das Gesetz über künstliche Intelligenz Anwendung auf die sich ständig weiterentwickelnde Typologie der KI-Wertschöpfungsketten findet und welche Auswirkungen sich daraus für die Rechenschaftspflicht aller beteiligten Stellen im Rahmen der verschiedenen Szenarien auf der Grundlage des allgemein anerkannten Stand der Technik ergeben, wie er auch in einschlägigen harmonisierten Normen zum Ausdruck kommt;
- q) Besondere Aufsicht und Überwachung sowie Institutionalisierung eines regelmäßigen Dialogs mit den Anbietern von Basismodellen über die Erfüllung des Artikels 28b dieser Verordnung von Basismodellen und KI-Systemen, die solche KI-Modelle nutzen, sowie über bewährte Verfahren der Branche für die Selbstverwaltung. Die nationalen Aufsichtsbehörden, die notifizierten Stellen und die Marktüberwachungsbehörden können an jeder solchen Sitzung teilnehmen und Beiträge leisten.
- r) Veröffentlichung und regelmäßige Aktualisierung von Leitlinien zu den Schwellenwerten, ab denen das Trainieren eines Basismodells als großer Trainingslauf gilt, Aufzeichnung und Überwachung bekannter Fälle von großen Trainingsläufen sowie Veröffentlichung eines jährlichen Berichts über den Stand der Entwicklung, Verbreitung und Nutzung von Basismodellen zusammen mit politischen Optionen zur Bewältigung der spezifischen Risiken und Chancen von Basismodellen.
- s) Förderung der KI-Kompetenz gemäß Artikel 4b.

ARTIKEL 56C**RECHENSCHAFTSPFLICHT, UNABHÄNGIGKEIT UND TRANSPARENZ**

- (1) Das Amt für künstliche Intelligenz
 - a) ist im Einklang mit dieser Verordnung gegenüber dem Europäischen Parlament und dem Rat rechenschaftspflichtig;
 - b) handelt bei der Erfüllung seiner Aufgaben oder der Ausübung seiner Befugnisse unabhängig; und
 - c) stellt ein hohes Maß an Transparenz für seine Tätigkeiten sicher und entwickelt diesbezüglich gute Verwaltungspraktiken.
- (2) Für die Dokumente des Amts für künstliche Intelligenz findet die Verordnung (EG) Nr. 1049/2001 Anwendung.

ABSCHNITT 2**SEKRETARIAT****ARTIKEL 57****SEKRETARIAT**

- (1) Die Tätigkeiten des Sekretariats werden von einem Exekutivdirektor geleitet. Der Exekutivdirektor ist dem Verwaltungsrat gegenüber rechenschaftspflichtig. Unbeschadet der jeweiligen Befugnisse des Verwaltungsrats und der Organe der Union darf der Exekutivdirektor Weisungen von Regierungen oder sonstigen Stellen weder einholen noch entgegennehmen.
- (2) Der Exekutivdirektor nimmt an Anhörungen zu allen Fragen im Zusammenhang mit den Tätigkeiten des Amts für künstliche Intelligenz teil und erstattet auf Aufforderung des Europäischen Parlaments oder des Rates Bericht über die Erfüllung seiner Aufgaben.
- (3) Der Exekutivdirektor vertritt das Amt für künstliche Intelligenz, einschließlich in internationalen Gremien für die Zusammenarbeit im Bereich der künstlichen Intelligenz;
- (4) Das Sekretariat leistet dem Verwaltungsrat und dem Beirat die analytische, administrative und logistische Unterstützung, die zur Erfüllung der Aufgaben des Amts für künstliche Intelligenz erforderlich ist, unter anderem durch
 - a) die Umsetzung der vom Verwaltungsrat angenommenen Beschlüsse, Programme und Maßnahmen;
 - b) die alljährliche Erstellung des Entwurfs des einheitlichen Programmplanungsdokuments, des Entwurfs des Haushaltsplans, des jährlichen Bericht über die Tätigkeiten des Amts für künstliche Intelligenz, der Entwürfe von

Stellungnahmen und Standpunkten des Amts für künstliche Intelligenz und deren Übermittlung an den Verwaltungsrat;

- c) die Koordinierung mit internationalen Foren für die Zusammenarbeit im Bereich der künstlichen Intelligenz;

ABSCHNITT 3

VERWALTUNGSRAT

ARTIKEL 57A

ZUSAMMENSETZUNG DES VERWALTUNGSRATS

- (1) Dem Verwaltungsrat gehören die folgenden Mitglieder an:
 - a) ein Vertreter der nationalen Aufsichtsbehörde eines jeden Mitgliedstaats;
 - b) ein Vertreter der Kommission;
 - c) ein Vertreter des Europäischen Datenschutzbeauftragten (EDSB);
 - d) ein Vertreter der Agentur der Europäischen Union für Cybersicherheit (ENISA);
 - e) ein Vertreter der Agentur für Grundrechte (FRA)

Jeder Vertreter einer nationalen Aufsichtsbehörde hat eine Stimme. Die Vertreter der Kommission, des EDSB, der ENISA und der FRA haben kein Stimmrecht. Jedes Mitglied hat einen Stellvertreter. Bei der Ernennung der Mitglieder und der stellvertretenden Mitglieder des Verwaltungsrats wird auf ein ausgewogenes Verhältnis zwischen den Geschlechtern geachtet. Die Mitglieder des Verwaltungsrats und ihre stellvertretenden Mitglieder werden öffentlich bekannt gemacht.

- (2) Die Mitglieder und stellvertretenden Mitglieder des Verwaltungsrats dürfen keine im Konflikt stehenden Funktionen oder geschäftlichen Interessen in Bezug auf Themen im Zusammenhang mit der Anwendung dieser Verordnung innehaben bzw. haben.
- (3) Die Regeln für die Sitzungen und Abstimmungen des Verwaltungsrats sowie für die Ernennung und Abberufung des Exekutivdirektors werden in der in Artikel 57 b Buchstabe a genannten Geschäftsordnung festgelegt.

ARTIKEL 57B

AUFGABEN DES VERWALTUNGSRATS

Der Verwaltungsrat hat folgende Aufgaben:

- a) Verabschiedung strategischer Entscheidungen über die Tätigkeiten des Amts für künstliche Intelligenz und Erlass seiner Geschäftsordnung mit einer Mehrheit von zwei Dritteln seiner Mitglieder;
- b) Umsetzung seiner Geschäftsordnung;
- c) Annahme des einheitlichen Programmplanungsdokuments des Amts für künstliche Intelligenz sowie seines öffentlichen Jahresberichts und Übermittlung beider an das Europäische Parlament, den Rat, die Kommission und den Rechnungshof;
- d) Verabschiedung des Haushalts des Amts für künstliche Intelligenz;
- e) Ernennung des Exekutivdirektors und gegebenenfalls Verlängerung seiner Amtszeit oder seine Abberufung;
- f) Beschlussfassung über die Festlegung der internen Strukturen des Amts für künstliche Intelligenz und erforderlichenfalls über die Änderung dieser internen Strukturen, die für die Erfüllung der Aufgaben des Amts für künstliche Intelligenz erforderlich sind.

ARTIKEL 57C

VORSITZ DES VERWALTUNGSRATS

- (1) Der Verwaltungsrat wählt aus dem Kreis seiner stimmberechtigten Mitglieder mit einfacher Mehrheit einen Vorsitz und zwei stellvertretende Vorsitze.
- (2) Die Amtszeit des Vorsitzes und des stellvertretenden Vorsitzes beträgt vier Jahre. Die Amtszeit des Vorsitzes und der stellvertretenden Vorsitze kann einmal verlängert werden.

ABSCHNITT 4

BEIRAT

ARTIKEL 58

BEIRAT

- (1) Der Beirat liefert dem Amt für künstliche Intelligenz Beiträge der Interessenträger zu Fragen im Zusammenhang mit dieser Verordnung, insbesondere im Hinblick auf die in Artikel 56b Buchstabe I genannten 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.
- (2) Die Mitglieder des Beirats vertreten eine ausgewogene Auswahl von Interessenträgern, darunter die Industrie, Start-up-Unternehmen, KMU, die Zivilgesellschaft, die Sozialpartner und die Wissenschaft. Bei der Zusammensetzung des Beirats wird auf ein ausgewogenes Verhältnis zwischen gewerblichen und nicht-gewerblichen Interessen und innerhalb der Kategorie der gewerblichen Interessen zwischen KMU und anderen Unternehmen geachtet.
- (3) Der Verwaltungsrat ernennt die Mitglieder des Beirats nach dem in der Geschäftsordnung des Amts für künstliche Intelligenz festgelegten Auswahlverfahren und unter Berücksichtigung des Bedarfs an Transparenz sowie gemäß den in Absatz 2 genannten Kriterien.
- (4) Die Amtszeit der Mitglieder des Beirats beträgt zwei Jahre; sie kann um höchstens vier Jahre verlängert werden.
- (5) Das Europäische Komitee für Normung (CEN), das Europäische Komitee für elektrotechnische Normung (CENELEC) und das Europäische Institut für Telekommunikationsnormen (ETSI) sind ständige Mitglieder des Beirats. Die Gemeinsame Forschungsstelle ist ein ständiges Mitglied ohne Stimmrecht.
- (6) Der Beirat gibt sich eine Geschäftsordnung. Er wählt gemäß den in Absatz 2 festgelegten Kriterien zwei Ko-Vorsitzende unter seinen Mitgliedern. Die Amtszeit der Ko-Vorsitzenden beträgt zwei Jahre und kann einmal verlängert werden.
- (7) Der Beirat hält mindestens viermal pro Jahr Sitzungen ab. Der Beirat kann Experten und andere Interessenträger zu seinen Sitzungen einladen. Der Exekutivdirektor kann von Amts wegen an den Sitzungen des Beirats teilnehmen..
- (8) Zur Wahrnehmung seiner Aufgaben gemäß Absatz 1 kann der Beirat Stellungnahmen, Empfehlungen und schriftliche Beiträge ausarbeiten.
- (9) Der Beirat kann gegebenenfalls ständige oder zeitweilige Untergruppen einsetzen, um spezifische Fragen im Zusammenhang mit den Zielen dieser Verordnung zu prüfen
- (10) Der Beirat erstellt jährlich einen Bericht über seine Tätigkeit. Dieser Bericht wird veröffentlicht..

ABSCHNITT 5
EUROPÄISCHE BENCHMARKING-BEHÖRDEN

ARTIKEL 58A
BENCHMARKING

Die in Artikel 15 Absatz 1a genannten europäischen Benchmarking-Behörden und das Amt für künstliche Intelligenz entwickeln in enger Zusammenarbeit mit internationalen Partnern gemeinsam kosteneffiziente Leitlinien und Kapazitäten zur Messung und zum Vergleich von Aspekten von KI-Systemen und KI-Komponenten und insbesondere von Basismodellen, die für die Einhaltung und Durchsetzung dieser Verordnung relevant sind, und zwar auf der Grundlage des allgemein anerkannten Stands der Technik, wie er auch in einschlägigen harmonisierten Normen zum Ausdruck kommt.

KAPITEL 2
ZUSTÄNDIGE NATIONALE BEHÖRDEN

ARTIKEL 59
BENENNUNG DER NATIONALEN AUFSICHTSBEHÖRDEN

- (1) Jeder Mitgliedstaat benennt bis zum ... [drei Monate nach dem Datum des Inkrafttretens dieser Verordnung] eine nationale Aufsichtsbehörde, die so organisiert ist, dass bei der Ausübung ihrer Tätigkeiten und der Wahrnehmung ihrer Aufgaben Objektivität und Unparteilichkeit gewahrt sind.
- (2) Die nationale Aufsichtsbehörde ist dafür verantwortlich, die Anwendung und Durchführung dieser Verordnung sicherzustellen. Hinsichtlich der Hochrisiko-AI-Systeme, die sich auf Produkte beziehen, für die die in Anhang II aufgeführten Rechtsakte gelten, führen die nach diesen Rechtsakten benannten zuständigen Behörden weiterhin die Verwaltungsverfahren durch. Soweit ein Fall jedoch Aspekte betrifft, die ausschließlich unter diese Verordnung fallen, sind die zuständigen Behörden an die von der gemäß dieser Verordnung benannten nationalen Aufsichtsbehörde erlassenen Maßnahmen gebunden. Die nationale Aufsichtsbehörde fungiert als Marktaufsichtsbehörde.
- (3) Die Mitgliedstaaten machen die nationale Aufsichtsbehörde sowie Informationen darüber, wie sie kontaktiert werden kann, bis zum ... [drei Monate nach dem Datum des Inkrafttretens dieser Verordnung] öffentlich zugänglich und setzen das Amt für künstliche Intelligenz und die Kommission darüber in Kenntnis. Die nationale Aufsichtsbehörde fungiert als zentrale Kontaktstelle für diese Verordnung und sollte über elektronische Kommunikationsmittel erreichbar sein.
- (4) Die Mitgliedstaaten sorgen dafür, dass die nationale Aufsichtsbehörde mit angemessenen technischen, finanziellen und personellen Ressourcen und Infrastrukturen ausgestattet wird,

damit sie ihre Aufgaben wirksam im Rahmen dieser Verordnung wahrnehmen kann. Insbesondere muss die nationale Aufsichtsbehörde ständig über eine ausreichende Zahl von Mitarbeitern verfügen, deren Kompetenzen und Sachkenntnis ein tiefes Verständnis der Technologien der künstlichen Intelligenz, der Daten und Datenverarbeitung, des Schutzes personenbezogener Daten, der Cybersicherheit, des Wettbewerbsrechts, der Grundrechte, der Gesundheits- und Sicherheitsrisiken sowie die Kenntnis der bestehenden Normen und rechtlichen Anforderungen einschließen. Die Mitgliedstaaten bewerten und aktualisieren, falls erforderlich, jährlich die in diesem Absatz genannten Anforderungen an die Kompetenzen und die Ressourcen.

- (4a) Jede nationale Aufsichtsbehörde ist bei der Ausübung ihrer Befugnisse und der Wahrnehmung ihrer Aufgaben unabhängig, unparteiisch und unvoreingenommen. Die Mitglieder jeder nationalen Aufsichtsbehörde holen bei der Erfüllung ihrer Aufgaben und der Ausübung ihrer Befugnisse gemäß dieser Verordnung weder Weisungen von Stellen ein noch nehmen sie Weisungen entgegen und sehen von allen mit den Aufgaben ihres Amtes nicht zu vereinbarenden Handlungen ab.
- (4b) Die nationalen Aufsichtsbehörden erfüllen die Mindestanforderungen an die Cybersicherheit, die für als Betreiber wesentlicher Dienste eingestufte Einrichtungen der öffentlichen Verwaltung gemäß der Richtlinie (EU) 2022/2555 festgelegt wurden.
- (4c) Bei der Erfüllung ihrer Aufgaben hält sich die nationale Aufsichtsbehörde an in Artikel 70 festgelegten Vertraulichkeitspflichten.
- (5) Die Mitgliedstaaten übermitteln der Kommission jährlich einen Bericht über den Stand der finanziellen und personellen Ressourcen der nationalen Aufsichtsbehörde, in dem sie auch deren Angemessenheit bewerten. Die Kommission leitet diese Informationen an das Amt für künstliche Intelligenz zur Erörterung und etwaigen Abgabe von Empfehlungen weiter..
- (7) Die nationalen Aufsichtsbehörden können insbesondere auch KMU und Start-up-Unternehmen unter Berücksichtigung der Leitlinien und Empfehlungen des Amtes für künstliche Intelligenz oder der Kommission mit Orientierung und Rat bei der Anwendung dieser Verordnung zur Seite stehen. Wenn die nationale Aufsichtsbehörde beabsichtigt, Orientierung und Rat in Bezug auf KI-Systeme in Bereichen zu geben, die unter andere Rechtsvorschriften der Union fallen, werden die Leitlinien in Absprache mit den zuständigen nationalen Behörden gegebenenfalls nach jenen Unionsvorschriften entworfen.
- (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 und Koordinierung zuständigen Behörde.

ARTIKEL 59A**MECHANISMUS FÜR DIE ZUSAMMENARBEIT ZWISCHEN NATIONALEN AUFSICHTSBEHÖRDEN IN FÄLLEN, IN DENEN ZWEI ODER MEHR MITGLIEDSTAATEN BETROFFEN SIND**

- (1) Jede nationale Aufsichtsbehörde nimmt die ihr gemäß dieser Verordnung übertragenen Aufgaben und Befugnisse im Hoheitsgebiet ihres eigenen Mitgliedstaats wahr
- (2) In Fällen, in denen zwei oder mehr nationale Aufsichtsbehörden betroffen sind, gilt die nationale Aufsichtsbehörde des Mitgliedstaats, in dem der Verstoß begangen wurde, als federführende nationale Aufsichtsbehörde.
- (3) In den in Absatz 2 genannten Fällen arbeiten die betreffenden Aufsichtsbehörden zusammen und tauschen zu gegebener Zeit alle zweckdienlichen Informationen aus. Die nationalen Aufsichtsbehörden arbeiten zusammen, um einen Konsens zu erzielen.

TITEL VII**EU-DATENBANK FÜR HOCHRISIKO-KI-SYSTEME****ARTIKEL 60****EU-DATENBANK FÜR HOCHRISIKO-KI-SYSTEME**

- (1) Die Kommission errichtet und pflegt in Zusammenarbeit mit den Mitgliedstaaten eine öffentliche EU-Datenbank mit den in Absatz 2 und 2 a genannten Informationen über Hochrisiko-KI-Systeme nach Artikel 6 Absatz 2, die gemäß Artikel 51 registriert werden.
- (2) Die in Anhang VIII Abschnitt A aufgeführten Daten werden von den Anbietern in die EU-Datenbank eingegeben. Die Kommission leistet ihnen dabei technische und administrative Unterstützung.
- (2a) Die in Anhang VIII Abschnitt B aufgeführten Daten werden von den Betreibern, die Behörden oder Organe, Einrichtungen oder sonstige Stellen der Union sind oder in deren Namen handeln, sowie von Betreibern, die in Artikel 51 (1a) und (1b) genannte Unternehmen sind, in die EU-Datenbank eingegeben.
- (3) Die in der EU-Datenbank gespeicherten Daten sind frei für die Öffentlichkeit verfügbar, benutzerfreundlich und zugänglich, einfach navigierbar und maschinenlesbar und enthalten strukturierte digitale Daten auf der Grundlage eines standardisierten Protokolls.
- (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 oder den Betreiber, der eine Behörde, ein Organ, eine Einrichtung, ein Amt oder eine Agentur der

Union oder ein in deren Namen handelnder Betreiber oder ein in Artikel 51 (1a) und (1b) genanntes Unternehmen ist, 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 und Betreiber.

Die Datenbank erfüllt die Zugänglichkeitsanforderungen von Anhang I der Richtlinie (EU) 2019/882.

TITEL VIII

BEOBSACHTUNG NACH DEM INVERKEHRBRINGEN, INFORMATIONSAUSTAUSCH, MARKTÜBERWACHTUNG

KAPITEL 1

BEOBSACHTUNG NACH DEM INVERKEHRBRINGEN

ARTIKEL 61

BEOBSACHTUNG NACH DEM INVERKEHRBRINGEN DURCH DIE ANBIETER UND PLAN FÜR DIE BEOBSACHTUNG 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 Betreibern 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. Soweit erforderlich, umfasst die Beobachtung nach dem Inverkehrbringen eine Analyse der Interaktion mit dem Umfeld anderer KI-Systeme, wozu auch andere Geräte und Software gehören, unter Berücksichtigung der Vorschriften aus Bereichen wie Datenschutz, Rechte des geistigen Eigentums und Wettbewerbsrecht.
- (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 bis zum [zwölf Monate nach dem Datum des Inkrafttretens dieser Verordnung] 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

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

Diese Meldung erfolgt unverzüglich, nachdem der Anbieter oder gegebenenfalls der Betreiber den kausalen Zusammenhang zwischen dem KI-System und dem Vorfall oder die naheliegende Wahrscheinlichkeit eines solchen Zusammenhangs festgestellt hat, oder auf jeden Fall spätestens 72 Stunden, nachdem der Anbieter oder gegebenenfalls der Betreiber Kenntnis von diesem schwerwiegenden Vorfall erlangt hat.

- (1a) Nach Feststellung eines kausalen Zusammenhangs zwischen dem KI-System und dem schwerwiegenden Vorfall oder der naheliegenden Wahrscheinlichkeit eines solchen Zusammenhangs ergreift der Anbieter angemessene Korrekturmaßnahmen gemäß Artikel 21.
- (2) Sobald die nationale Aufsichtsbehörde 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 bis zum [Inkrafttreten dieser Verordnung] veröffentlicht und regelmäßig bewertet.
- (2a) Die nationale Aufsichtsbehörde ergreift innerhalb von sieben Tagen nach Eingang der in Absatz 1 genannten Meldung geeignete Maßnahmen. Findet der Verstoß in anderen Mitgliedstaaten statt oder ist damit zu rechnen, dass er in anderen Mitgliedstaaten stattfindet, unterrichtet die nationale Aufsichtsbehörde das Amt für künstliche Intelligenz und die jeweiligen nationalen Aufsichtsbehörden dieser Mitgliedstaaten.

- (3) Bei Hochrisiko-KI-Systemen nach Anhang III, die von Anbietern in Verkehr gebracht oder in Betrieb genommen wurden, die Rechtsinstrumenten der Union mit gleichwertigen Meldepflichten wie jenen in dieser Verordnung festgesetzten unterliegen, wird die Meldung schwerwiegender Vorfälle, die nach dem Unionsrecht einen Verstoß gegen die Grundrechte darstellen, auf die nationale Aufsichtsbehörde übertragen.
- (3a) Die nationalen Aufsichtsbehörden melden dem Amt für künstliche Intelligenz jährlich die schwerwiegenden Vorfälle, die ihnen gemäß diesem Artikel gemeldet werden.

KAPITEL 3 DURCHSETZUNG

ARTIKEL 63

MARKTÜBERWACHUNG UND KONTROLLE VON KI-SYSTEMEN AUF DEM UNIONSMARKT

- (1) Die Verordnung (EU) 2019/1020 gilt für KI-Systeme und Basismodelle, 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.
 - ba) Die nationalen Aufsichtsbehörden fungieren im Rahmen dieser Verordnung als Marktaufsichtsbehörden und haben die gleichen Befugnisse und Pflichten wie Marktaufsichtsbehörden gemäß der Verordnung (EU) 2019/1020.
- (2) Die nationale Aufsichtsbehörde erstattet der Kommission und dem Amt für künstliche Intelligenz jährlich 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.
- (3a) Zum Zweck einer wirksamen Durchsetzung dieser Verordnung können die nationalen Aufsichtsbehörden

- a) unangekündigte Vor-Ort- und Ferninspektionen von Hochrisiko-KI-Systemen durchführen;
 - b) Stichproben von Hochrisiko-KI-Systemen nehmen, auch durch Ferninspektionen, um die KI-Systeme zurückzuentwickeln und Beweise für die Nichteinhaltung der Vorschriften zu sammeln.
- (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 KI-Systeme, die für Strafverfolgungszwecke eingesetzt werden, benennen die Mitgliedstaaten für die Zwecke dieser Verordnung als Marktüberwachungsbehörden die für den Datenschutz nach der Richtlinie (EU) 2016/680 zuständigen Aufsichtsbehörden.
- (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 auf der Grundlage dieser Verordnung benannten nationalen Aufsichtsbehörden stimmen sich mit anderen einschlägigen nationalen Behörden oder Stellen ab, die die Anwendung der in Anhang II aufgeführten Harmonisierungsrechtsvorschriften der Union oder sonstiger Rechtsvorschriften der Union überwachen, die für die in Anhang III aufgeführten Hochrisiko-KI-Systeme relevant sein könnten.

ARTIKEL 64

ZUGANG ZU DATEN UND ZUR DOKUMENTATION

- (1) Im Zusammenhang mit ihren Tätigkeiten und auf ihren begründeten Antrag erhält die nationale Aufsichtsbehörde oder gegebenenfalls der Betreiber über für den Fernzugriff geeignete technische Mittel und Instrumente uneingeschränkter Zugang zu den von den Anbietern genutzten Trainings-, Validierungs- und Testdatensätzen, die für den Zweck ihres Antrags relevant und unbedingt erforderlich sind.
- (2) Sofern dies für die Bewertung der Konformität der Hochrisiko-KI-Systeme mit den in Titel III Kapitel 2 festgelegten Anforderungen notwendig ist, und nachdem alle anderen sinnvollen Möglichkeiten der Überprüfung der Konformität einschließlich Absatz 1 ausgeschöpft sind oder sich als unzureichend erwiesen haben, wird der nationalen Aufsichtsbehörde auf deren begründetes Verlangen Zugang zu den Trainingsmodellen und trainierten Modellen des KI-Systems, einschließlich seiner relevanten Modellparameter, gewährt. Alle nach Artikel 70 erlangten Informationen werden als vertrauliche Informationen behandelt und unterliegen dem geltenden Unionsrecht zum Schutz des geistigen Eigentums und von Geschäftsgeheimnissen

und werden nach Abschluss der Untersuchung, für die die Informationen angefordert wurden, gelöscht.

- (2a) Absatz 1 und 2 lassen die Verfahrensrechte des betreffenden Akteurs nach Artikel 18 der Verordnung (EU) 2019/1020 unberührt.
- (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 nationale Aufsichtsbehörde 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 nationalen Aufsichtsbehörden übermitteln die Liste der Kommission, dem Amt für künstliche Intelligenz und allen anderen nationalen Aufsichtsbehörden und sorgen dafür, dass die Liste stets aktuell bleibt. Die Kommission veröffentlicht auf einer dafür eigens angelegten Website die Liste aller von den Mitgliedstaaten gemäß diesem Artikel benannten zuständigen Behörden.
- (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 nationalen Aufsichtsbehörde einen begründeten Antrag auf Durchführung technischer Tests des Hochrisiko-KI-Systems stellen. Die nationale Aufsichtsbehörde 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 KI-Systeme, die die Gesundheit und Sicherheit, die Grundrechte von Personen im Allgemeinen, auch am Arbeitsplatz, den Verbraucherschutz, die Umwelt, die öffentliche Sicherheit oder Demokratie oder Rechtsstaatlichkeit und andere öffentliche Interessen, die durch die geltenden Harmonisierungsrechtsvorschriften der Union geschützt sind, in einem Maße beeinträchtigen können, das über das hinausgeht, was im Hinblick auf den beabsichtigten Zweck oder unter

den normalen oder vernünftigerweise vorhersehbaren Bedingungen für die Nutzung des betreffenden Systems, einschließlich der Dauer der Nutzung und gegebenenfalls der Anforderungen an Inbetriebnahme, Installation und Wartung, als vernünftig und annehmbar gilt.

- (2) Hat die nationale Aufsichtsbehörde 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 die Grundrechte, unterrichtet die nationale Aufsichtsbehörde auch umgehend die in Artikel 64 Absatz 3 genannten einschlägigen nationalen Behörden oder öffentlichen Stellen und arbeitet uneingeschränkt mit ihnen zusammen. Dort wo hinreichender Grund zu der Annahme besteht, dass ein KI-System die Schutzbedürftigkeit von gefährdeten Gruppe ausnutzt oder ihre Rechte absichtlich oder unabsichtlich verletzt, ist die nationale Aufsichtsbehörde verpflichtet, die Gestaltungsziele, die Dateneingabe, die Modellauswahl, die Umsetzung und die Ergebnisse des KI-Systems zu untersuchen. Die betreffenden Akteure müssen im notwendigen Umfang mit der nationalen Aufsichtsbehörde und den in Artikel 64 Absatz 3 genannten anderen Behörden oder öffentlichen Stellen zusammenarbeiten.

Stellt die nationale Aufsichtsbehörde oder gegebenenfalls die in Artikel 64 (3) genannte nationale Behörde 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 und in jedem Falle innerhalb von fünfzehn Werktagen oder wie in den einschlägigen Harmonisierungsrechtsvorschriften der Union vorgesehen zurückzurufen.

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

- (3) Gelangt die nationale Aufsichtsbehörde zu der Auffassung, dass die Nichtkonformität nicht auf ihr nationales Hoheitsgebiet beschränkt ist, unterrichtet sie die Kommission das Amt für künstliche Intelligenz und die nationalen Aufsichtsbehörden der 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 nationale Aufsichtsbehörde alle geeigneten

vorläufigen Maßnahmen, um die Bereitstellung des KI-Systems auf ihrem nationalen Markt oder die Inbetriebnahme zu verbieten oder einzuschränken, das KI-System von diesem Markt zu nehmen oder es zurückzurufen. Diese Behörde unterrichtet die Kommission, das Amt für künstliche Intelligenz und die nationalen Aufsichtsbehörden der anderen Mitgliedstaaten umgehend 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 und die Lieferkette, 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 nationale Aufsichtsbehörde gibt insbesondere an, ob die Nichtkonformität eine oder mehrere der folgenden Ursachen hat:
- a) Nichterfüllung der in dieser Verordnung aufgeführten Anforderungen durch das Hochrisiko-KI-System;
 - b) Mängel in den in den Artikeln 40 und 41 genannten harmonisierten Normen oder gemeinsamen Spezifikationen, die eine Konformitätsvermutung begründen;
 - ba) Missachtung des Verbots der in Artikel 5 genannten KI-Praktiken;
 - bb) Nichterfüllung der Bestimmungen von Artikel 52.
- (7) Die anderen nationalen Aufsichtsbehörden, die kein Verfahren eingeleitet haben, unterrichten unverzüglich die Kommission, das Amt für künstliche Intelligenz 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 eine nationale Aufsichtsbehörde eines Mitgliedstaates noch die Kommission innerhalb von drei Monaten nach Eingang der in Absatz 5 genannten Unterrichtung Einwände gegen die von einer nationalen Aufsichtsbehörde eines anderen Mitgliedstaates 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. Die im ersten Satz dieses Absatzes genannte Frist wird bei Missachtung des Verbots der in Artikel 5 genannten KI-Praktiken auf dreißig Tage gekürzt.
- (9) Die nationalen Aufsichtsbehörden aller Mitgliedstaaten tragen dafür Sorge, dass geeignete einschränkende Maßnahmen in Bezug auf das betreffende KI-System ergriffen werden, indem sie beispielsweise das KI-System unverzüglich von ihrem Markt nehmen.
- (9a) Die nationalen Aufsichtsbehörden erstatten dem Amt für künstliche Intelligenz jährlich Bericht über die Anwendung verbotener Praktiken, die im Laufe des Jahres vorgekommen sind, sowie über die zur Abwendung oder Minderung der Risiken gemäß diesem Artikel ergriffenen Maßnahmen.

ARTIKEL 66**SCHUTZKLAUSELVERFAHREN DER UNION**

- (1) Erhebt ein Mitgliedstaat innerhalb von drei Monaten nach Eingang der in Artikel 65 Absatz 5 genannten Unterrichtung bzw. innerhalb von 30 Tagen im Falle der Missachtung des Verbots der in Artikel 5 genannten KI-Praktiken Einwände gegen eine von der nationalen Aufsichtsbehörde eines anderen Mitgliedstaats getroffene Maßnahme oder ist die Kommission der Ansicht, dass die Maßnahme mit dem Unionsrecht unvereinbar ist, so nimmt die Kommission unverzüglich Konsultationen mit der nationalen Aufsichtsbehörde des betreffenden Mitgliedstaats oder Akteur auf und prüft die nationale Maßnahme. Anhand der Ergebnisse dieser Prüfung entscheidet die Kommission innerhalb von drei Monaten bzw. 60 Tagen im Falle der Missachtung des Verbots der in Artikel 5 genannten KI-Praktiken nach Eingang der in Artikel 65 Absatz 5 genannten Unterrichtung, ob die nationale Maßnahme gerechtfertigt ist oder nicht und teilt der nationalen Aufsichtsbehörde des betreffenden Mitgliedstaats ihre Entscheidung mit. Die Kommission unterrichtet auch alle übrigen nationalen Aufsichtsbehörden über diese Entscheidung.
- (2) Gilt die nationale Maßnahme als gerechtfertigt, so ergreifen alle auf der Grundlage dieser Verordnung benannten nationalen Aufsichtsbehörden die erforderlichen Maßnahmen, damit das nichtkonforme KI-System unverzüglich von ihrem Markt genommen wird, und unterrichten die Kommission und das Amt für künstliche Intelligenz darüber. Gilt die nationale Maßnahme als nicht gerechtfertigt, nimmt die nationale Aufsichtsbehörde des betreffenden Mitgliedstaats 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 66A**GEMEINSAME UNTERSUCHUNGEN**

Hat eine nationale Aufsichtsbehörde Grund zu der Annahme, dass es sich bei dem Verstoß eines Anbieters oder eines Betreibers eines Hochrisiko-KI-Systems oder Basismodells gegen diese Verordnung um einen weitverbreiteten Verstoß mit unionsweiter Dimension handelt, der mindestens 45 Millionen Personen in der EU betrifft oder betreffen könnte, unterrichtet die betreffende nationale Aufsichtsbehörde das Amt für künstliche Intelligenz und kann die nationalen Aufsichtsbehörden der Mitgliedstaaten, in denen der Verstoß begangen wurde, auffordern, eine gemeinsame Untersuchung einzuleiten. Das Amt für künstliche Intelligenz sorgt für eine zentrale Koordinierung der gemeinsamen Untersuchung. Die Untersuchungsbefugnisse fallen in die Zuständigkeit der nationalen Aufsichtsbehörden.

ARTIKEL 67**KONFORME KI-SYSTEME, DIE EIN RISIKO BERGEN**

- (1) Stellt die nationale Aufsichtsbehörde nach der gemäß Artikel 65 durchgeführten Prüfung in uneingeschränkter Zusammenarbeit mit der in Artikel 64 Absatz 3 genannten betreffenden nationalen Behörde 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 der Umwelt oder der Demokratie und Rechtsstaatlichkeit 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.
- (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 nationalen Aufsichtsbehörde des in Absatz 1 genannten Mitgliedstaats vorgegeben wurde, Korrekturmaßnahmen ergriffen werden.
- (2a) Versäumen es der Anbieter oder andere einschlägige Akteure, die in Absatz 2 genannten Korrekturmaßnahmen zu ergreifen, und stellt das KI-System weiterhin ein Risiko im Sinne von Absatz 1 dar, kann die nationale Aufsichtsbehörde verlangen, dass der einschlägige Betreiber das KI-System innerhalb einer angemessenen, der Art des Risikos entsprechenden Frist vom Markt nimmt oder zurückruft.
- (3) Die nationale Aufsichtsbehörde unterrichtet die Kommission, das Amt für künstliche Intelligenz und die übrigen nationalen Aufsichtsbehörden 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 in Absprache mit dem Amt für künstliche Intelligenz unverzüglich mit den betroffenen nationalen Aufsichtsbehörden und den betreffenden Akteuren Konsultationen auf und prüft die ergriffenen nationalen Maßnahmen. Anhand der Ergebnisse dieser Prüfung entscheidet das Amt für künstliche Intelligenz, ob die Maßnahme gerechtfertigt ist oder nicht, und schlägt, falls erforderlich, geeignete Maßnahmen vor. Anhand der Ergebnisse dieser Prüfung entscheidet der Ausschuss, ob die Maßnahme gerechtfertigt ist oder nicht, und schlägt, falls erforderlich, geeignete Maßnahmen vor.
- (5) Die Kommission teilt diese Entscheidung in Absprache mit dem Amt für künstliche Intelligenz umgehend den nationalen Aufsichtsbehörden der betroffenen Mitgliedstaaten und den einschlägigen Akteuren mit. Sie unterrichtet auch alle anderen nationalen Aufsichtsbehörden über die Entscheidung.

- (5a) Die Kommission verabschiedet Leitlinien, die die zuständigen nationalen Behörden dabei unterstützen sollen, ähnliche Sachverhalte, die in anderen KI-Systemen auftreten, zu erkennen und gegebenenfalls zu beheben.

ARTIKEL 68

FORMALE NICHTKONFORMITÄT

- (1) Gelangt die nationale Aufsichtsbehörde eines Mitgliedstaats zu einer der folgenden Feststellungen, fordert sie den jeweiligen Anbieter auf, die betreffende Nichtkonformität zu beheben:
- a) die CE-Kennzeichnung wurde nicht nach Artikel 49 angebracht;
 - b) die CE-Kennzeichnung 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.
 - ea) die technische Dokumentation ist nicht verfügbar;
 - eb) die Registrierung in der EU-Datenbank wurde nicht vorgenommen;
 - ec) der Bevollmächtigte, soweit erforderlich, wurde nicht ernannt.
- (2) Besteht die Nichtkonformität nach Absatz 1 weiter, so ergreift die nationale Aufsichtsbehörde des betreffenden Mitgliedstaats geeignete und angemessene Maßnahmen, um die Bereitstellung des Hochrisiko-KI-Systems auf dem Markt zu beschränken oder zu untersagen oder um dafür zu sorgen, dass es unverzüglich zurückgerufen oder vom Markt genommen wird. Die nationale Aufsichtsbehörde des betreffenden Mitgliedstaats unterrichtet das Amt für künstliche Intelligenz umgehend über die Nichtkonformität und die ergriffenen Maßnahmen.

KAPITEL 3A

RECHTSBEHELFE

ARTIKEL 68A

RECHT AUF BESCHWERDE BEI EINER NATIONALEN AUFSICHTSBEHÖRDE

- (1) Jede natürliche Person oder Gruppe von natürlichen Personen hat unbeschadet eines anderweitigen verwaltungsrechtlichen oder gerichtlichen Rechtsbehelfs das Recht auf Beschwerde bei einer nationalen Aufsichtsbehörde, insbesondere in dem Mitgliedstaat ihres gewöhnlichen Aufenthaltsorts, ihres Arbeitsplatzes oder des Orts des mutmaßlichen

Verstoßes, wenn sie der Ansicht ist, dass das sie betreffende KI-System gegen diese Verordnung verstößt.

- (2) Die nationale Aufsichtsbehörde, bei der die Beschwerde eingereicht wurde, unterrichtet den Beschwerdeführer über den Stand und die Ergebnisse der Beschwerde einschließlich der Möglichkeit eines gerichtlichen Rechtsbehelfs nach Artikel 78.

ARTIKEL 68B

RECHT AUF EINEN WIRKSAMEN GERICHTLICHEN RECHTSBEHELFB GEGEN EINE NATIONALE AUF SICHTSBEHÖRDE

- (1) Jede natürliche oder juristische Person hat unbeschadet eines anderweitigen verwaltungsrechtlichen oder außergerichtlichen Rechtsbehelfs das Recht auf einen wirksamen gerichtlichen Rechtsbehelf gegen einen sie betreffenden rechtsverbindlichen Beschluss einer nationalen Aufsichtsbehörde.
- (2) Unbeschadet anderer verwaltungsrechtlicher oder außergerichtlicher Rechtsbehelfe hat jede natürliche oder juristische Person das Recht auf einen wirksamen gerichtlichen Rechtsbehelf, wenn die nach Artikel 59 zuständige nationale Aufsichtsbehörde eine Beschwerde nicht bearbeitet oder die betroffene Person nicht innerhalb von drei Monaten über den Fortgang oder das Ergebnis der gemäß Artikel 68a eingereichten Beschwerde unterrichtet.
- (3) Für Verfahren gegen eine nationale Aufsichtsbehörde sind die Gerichte des Mitgliedstaats zuständig, in dem die nationale Aufsichtsbehörde ihren Sitz hat.
- (4) Kommt es zu einem Verfahren gegen den Beschluss einer nationalen Aufsichtsbehörde, dem eine Stellungnahme oder ein Beschluss der Kommission im Rahmen des Schutzklauselverfahrens der Union vorangegangen ist, so leitet die nationale Aufsichtsbehörde diese Stellungnahme oder diesen Beschluss dem Gericht zu.

ARTIKEL 68C

DAS RECHT AUF ERLÄUTERUNG DER INDIVIDUELLEN ENTSCHEIDUNGSFINDUNG

- (1) Personen, die von einer Entscheidung betroffen sind, die der Betreiber auf der Grundlage der Daten aus einem Hochrisiko-KI-System getroffen hat und die rechtliche Auswirkungen hat oder sie in ähnlicher Art erheblich auf eine Weise beeinträchtigt, die ihrer Ansicht nach ihre Gesundheit, ihre Sicherheit, ihre Grundrechte, ihr sozioökonomisches Wohlergehen oder andere Rechte, die sich aus den in dieser Verordnung festgelegten Verpflichtungen ergeben, beeinträchtigt, haben das Recht, vom Betreiber eine klare und aussagekräftige Erläuterung gemäß Artikel 13 Absatz 1 zur Rolle des KI-Systems im Entscheidungsprozess, zu den wichtigsten Parametern der getroffenen Entscheidung und zu den zugehörigen Eingabedaten zu verlangen.

- (2) Absatz 1 gilt nicht für den Einsatz von KI-Systemen, für die sich Ausnahmen von oder Beschränkungen der Verpflichtung nach Absatz 1 aus dem Unionsrecht oder nationalen Recht ergeben, sofern diese Ausnahmen oder Beschränkungen den Wesensgehalt der Grundrechte und Grundfreiheiten wahren und ein notwendiges und angemessenes Mittel in einer demokratischen Gesellschaft darstellen.
- (3) Dieser Artikel gilt unbeschadet der Artikel 13, 14, 15 und 22 der Verordnung 2016/679..

ARTIKEL 68D

ÄNDERUNG DER RICHTLINIE (EU) 2020/1828

In Anhang I der Richtlinie (EU) 2020/1828 des Europäischen Parlaments und des Rates^{1a} wird die folgende Nummer angefügt:

„(67a) Verordnung xxxx/xxxx des Europäischen Parlaments und des Rates [zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz (Gesetz über künstliche Intelligenz) und zur Änderung bestimmter Rechtsakte der Union (ABl. L ...)]“.

^{1a}Richtlinie (EU) 2020/1828 des Europäischen Parlaments und des Rates vom 25. November 2020 über Verbandsklagen zum Schutz der Kollektivinteressen der Verbraucher und zur Aufhebung der Richtlinie 2009/22/EG (ABl. L 409 vom 4.12.2020, S. 1).

ARTIKEL 68E

MELDUNG VON VERSTÖßEN UND SCHUTZ VON HINWEISGEBERN

Für die Meldung von Verstößen gegen diese Verordnung und den Schutz von Personen, die solche Verstöße melden, gilt die Richtlinie (EU) 2019/1937 des Europäischen Parlaments und des Rates.

TITEL IX

VERHALTENSKODIZES

ARTIKEL 69

VERHALTENSKODIZES

- (1) Die Kommission, das Amt für künstliche Intelligenz 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, auch wenn die Verhaltenskodizes aufgestellt werden, um aufzuzeigen, inwiefern KI-Systeme die in Artikel 4a dargelegten Grundsätze achten und somit als

vertrauenswürdig erachtet werden können, 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) In Verhaltenskodizes, mit denen erreicht werden soll, dass die Grundsätze für vertrauenswürdige KI-Systeme freiwillig erfüllt werden, muss insbesondere
- a) das Ziel verfolgt werden, dass das Personal und andere Personen, die mit dem Betrieb und der Nutzung von KI-Systemen befasst sind, über ein ausreichendes Maß an Kompetenzen im Bereich KI verfügen, um diese Grundsätze zu wahren;
 - b) bewertet werden, in welchem Umfang sich ihre KI-Systeme auf schutzbedürftige Personen oder Personengruppen, darunter Kinder, ältere Menschen, Migranten und Menschen mit Behinderungen, auswirken können und welche Maßnahmen ergriffen werden können, um die Zugänglichkeit zu verbessern oder um diese Personen oder Personengruppen auf andere Weise zu unterstützen;
 - c) berücksichtigt werden, wie sich die Nutzung ihrer KI-Systeme auf die Vielfalt, das Geschlechterverhältnis und die Gleichstellung auswirken oder diese verbessern kann;
 - d) darauf geachtet werden, ob die KI-Systeme in einer Weise genutzt werden können, die direkt oder indirekt bestehende Voreingenommenheit oder Ungleichheiten nachhaltig oder erheblich verstärken kann;
 - e) abgewogen werden, ob es erforderlich und wichtig ist, über vielfältige Entwicklungsteams zu verfügen, um eine inklusive Gestaltung ihrer Systeme sicherzustellen;
 - f) sorgfältig abgewogen werden, ob die Systeme negative gesellschaftliche Auswirkungen haben können, insbesondere in Bezug auf politische Institutionen und demokratische Prozesse;
 - g) bewertet werden, wie KI-Systeme zur ökologischen Nachhaltigkeit und insbesondere zu den Verpflichtungen im Rahmen des europäischen Grünen Deals und der Europäischen Erklärung zu den digitalen Rechten und Grundsätzen beitragen können.
- (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 einschließlich Wissenschaftlern, sowie deren Interessenvertretungen, insbesondere Gewerkschaften und Verbraucherorganisationen. Verhaltenskodizes können sich auf mehrere KI-Systeme erstrecken, um ähnlichen Zweckbestimmungen der jeweiligen Systeme Rechnung zu tragen. Anbieter, die Verhaltenskodizes annehmen, benennen mindestens eine natürliche Person, die für die interne Überwachung verantwortlich ist.

- (4) Die Kommission und das Amt für künstliche Intelligenz berücksichtigen die besonderen Interessen und Bedürfnisse von KMU und Startups bei der Förderung und Erleichterung der Aufstellung von Verhaltenskodizes.

TITEL X

VERTRAULICHKEIT UND SANKTIONEN

ARTIKEL 70

VERTRAULICHKEIT

- (1) Die an der Anwendung dieser Verordnung beteiligte Kommission, zuständigen nationalen Behörden und notifizierten Stellen, das Amt für künstliche Intelligenz und jede andere natürliche oder juristische Person 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, gemäß den Bestimmungen der Verordnungen 2004/48/EG und 2016/943/EG, 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,
 - ba) öffentliche und nationale Sicherheitsinteressen;
 - c) öffentliche und nationale Sicherheitsinteressen;
 - d) die Integrität von Straf- oder Verwaltungsverfahren.
- (1a) Die an der Anwendung dieser Verordnung gemäß Absatz 1 beteiligten Behörden beschränken die Menge der zur Offenlegung angeforderten Daten auf die Daten, die für das wahrgenommene Risiko und die Bewertung dieses Risikos unbedingt erforderlich sind. Sie löschen die Daten, sobald diese für den Zweck, für den sie angefordert wurden, nicht mehr benötigt werden. Sie ergreifen angemessene und wirksame Cybersicherheitsmaßnahmen sowie technische und organisatorische Maßnahmen, um die Sicherheit und Vertraulichkeit der Informationen und Daten zu schützen, die sie bei der Wahrnehmung ihrer Aufgaben und Tätigkeiten erhalten.
- (2) Unbeschadet der Absätze 1 und 1 a 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 Betreiber, 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 öffentliche oder nationale Sicherheit 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, 1a 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, wenn dies unbedingt erforderlich ist und im Einklang mit den einschlägigen Bestimmungen internationaler und Handelsabkommen, 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, die bei Verstößen gegen diese Verordnung Anwendung finden, und ergreifen alle Maßnahmen, die für deren ordnungsgemäße und wirksame Durchsetzung und Anpassung an die von der Kommission und vom Amt für künstlich Intelligenz ausgearbeiteten Leitlinien nach Artikel 82b notwendig sind. Die vorgesehenen Sanktionen müssen wirksam, verhältnismäßig und abschreckend sein. Sie berücksichtigen die Interessen von KMU und Startups sowie deren wirtschaftliches Überleben.
- (2) Die Mitgliedstaaten teilen der Kommission diese Vorschriften und Maßnahmen bis zum ... [12 Monate nach Inkrafttreten dieser Verordnung] mit und melden ihr unverzüglich alle diesbezüglichen Änderungen.
- (3) Bei Missachtung des Verbots der in Artikel 5 genannten Praktiken im Bereich der künstlichen Intelligenz werden Geldbußen von bis zu 40 000 000 EUR oder – im Falle von Unternehmen

- von bis zu 7 % des gesamten weltweiten Jahresumsatzes des vorangegangenen Geschäftsjahres verhängt, je nachdem, welcher Betrag höher ist.
- (3a) Verstoßen KI-Systeme gegen die in Artikel 10 und 13 festgelegten Anforderungen, 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.
- (4) Verstoßen KI-Systeme oder Basismodelle gegen die in dieser Verordnung festgelegten Anforderungen oder Pflichten, mit Ausnahme der in den Artikeln 5, 10 und 13 genannten, 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.
- (5) Werden gegenüber notifizierten Stellen und zuständigen nationalen Behörden auf deren Auskunftsverlangen hin falsche, unvollständige oder irreführende Angaben gemacht, werden Geldbußen von bis zu 5 000 000 EUR oder – im Falle von Unternehmen – von bis zu 1 % des gesamten weltweiten Jahresumsatzes des vorangegangenen Geschäftsjahres verhängt, je nachdem, welcher Betrag höher ist.
- (6) Geldbußen können zusätzlich zu oder anstelle von nichtmonetären Maßnahmen wie Anordnungen oder Verwarnungen verhängt werden. 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 unter Berücksichtigung des Zwecks des KI-Systems sowie gegebenenfalls der Zahl der betroffenen Personen und des Ausmaßes des von ihnen erlittenen Schadens;
 - b) ob bereits andere nationale Aufsichtsbehörden eines oder mehrerer Mitgliedstaaten demselben Akteur für denselben Verstoß Geldbußen auferlegt haben;
 - c) Größe und Jahresumsatz des Akteurs, der den Verstoß begangen hat,
 - ca) alle Maßnahmen, die der Akteur ergriffen hat, um den Schaden, der den betroffenen Personen zugefügt wird, zu mindern;
 - cb) Vorsätzlichkeit oder Fahrlässigkeit des Verstoßes;
 - cc) den Grad der Zusammenarbeit mit den zuständigen nationalen Behörden zu dem Zweck, den Verstoß abzustellen und die möglichen nachteiligen Auswirkungen des Verstoßes abzumildern;
 - cd) Grad an Verantwortung des Akteurs unter Berücksichtigung der von ihm ergriffenen technischen und organisatorischen Maßnahmen;

- ce) Art und Weise, wie der Verstoß den zuständigen nationalen Behörden bekannt wurde, insbesondere ob und gegebenenfalls in welchem Umfang der Akteur den Verstoß gemeldet hat;
 - cf) Einhaltung genehmigter Verhaltensregeln oder genehmigter Zertifizierungsverfahren;
 - cg) etwaige einschlägige frühere Verstöße des Akteurs;
 - ch) andere erschwerende oder mildernde Umstände im jeweiligen Fall:
- (7) Jeder Mitgliedstaat erlässt Vorschriften über die Geldbußen, die gegen Behörden und öffentliche Stellen, die in dem betreffenden Mitgliedstaat niedergelassen sind, zu verhängen sind;
- (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.
- (8a) Die in diesem Artikel genannten Sanktionen sowie die damit verbundenen Prozesskosten und Entschädigungsansprüche sind nicht Gegenstand von Vertragsklauseln oder anderen Formen von Lastenteilungsvereinbarungen zwischen Anbietern und Händlern, Einführern, Betreibern oder sonstigen Dritten.
- (8b) Die nationalen Aufsichtsbehörden erstatten dem Amt für künstliche Intelligenz jährlich Bericht über die Geldbußen, die sie im Laufe des entsprechenden Jahres nach Maßgabe dieses Artikels verhängt haben.
- (8c) Für die Ausübung der Befugnisse nach diesem Artikel durch die zuständigen Behörden gelten geeignete Verfahrensgarantien nach Unionsrecht und nationalem Recht, einschließlich gerichtlicher Rechtsbehelfe und ordnungsgemäßer Verfahren.

ARTIKEL 72

VERHÄNGUNG VON GELDBÜßEN 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 unter Berücksichtigung des Zwecks des betreffenden KI-Systems sowie gegebenenfalls der Zahl der betroffenen Personen und des Ausmaßes des von ihnen erlittenen Schadens sowie etwaiger einschlägiger früherer Verstöße;

- aa) alle Maßnahmen, die das Organ, die Einrichtung oder die sonstige Stelle der Union zur Minderung des von den betroffenen Personen erlittenen Schadens ergriffen hat;
 - ab) Grad der Verantwortung des Organs, der Einrichtung oder der sonstigen Stelle der Union unter Berücksichtigung der von diesen ergriffenen technischen und organisatorischen Maßnahmen;
 - b) Grad der 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.
 - ca) Art und Weise, wie der Verstoß dem Europäischen Datenschutzbeauftragten bekannt wurde, insbesondere ob und – wenn ja – in welchem Umfang das Organ oder die Einrichtung der Union den Verstoß gemeldet hat;
 - cb) die jährliche Mittelausstattung der Stelle.
- (2) Bei Missachtung des Verbots der in Artikel 5 genannten Praktiken im Bereich der
- (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 750 000 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 fließt in den Gesamthaushalt der Union. Die Geldbußen dürfen sich nicht auf den wirksamen Betrieb des Organs, der Einrichtung oder sonstigen Stelle der Union auswirken, denen die Geldbuße auferlegt wurde.

- (6a) Der Europäische Datenschutzbeauftragte macht dem Amt für künstliche Intelligenz jährlich Mitteilung über die Geldbußen, die er nach Maßgabe dieses Artikels verhängt hat.

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 für einen Zeitraum von fünf Jahren ab dem ... [Datum des Inkrafttretens dieser Verordnung] übertragen. Die Kommission erstellt spätestens neun Monate vor Ablauf des Zeitraums von fünf Jahren einen Bericht über die Befugnisübertragung. Die Befugnisübertragung verlängert sich stillschweigend um Zeiträume gleicher Länge, es sei denn, das Europäische Parlament oder der Rat widersprechen einer solchen Verlängerung spätestens drei Monate vor Ablauf des jeweiligen Zeitraums.
- (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.
- (3a) Vor dem Erlass eines delegierten Rechtsakts konsultiert die Kommission die einschlägigen Organe, das Amt, den Beirat und andere einschlägige Interessenträger im Einklang mit den in der Interinstitutionellen Vereinbarung vom 13. April 2016 über bessere Rechtsetzung enthaltenen Grundsätzen.
- Sobald die Kommission beschließt, einen delegierten Rechtsakt auszuarbeiten, teilt sie dies dem Europäischen Parlament mit. Diese Mitteilung verpflichtet die Kommission nicht dazu, diesen Rechtsakt zu erlassen.
- (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 75

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 81A

ÄNDERUNG DER VERORDNUNG (EU) 2019/1020

Die Verordnung (EU) 2019/1020 wird wie folgt geändert:

In Artikel 14 Absatz 4 wird folgender Absatz angefügt:

„l) die Befugnis, die in diesem Artikel geregelten Befugnisse gegebenenfalls aus der Ferne zu erteilen;“.

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 82A

BESSERE RECHTSETZUNG

Bei der Berücksichtigung der Anforderungen dieser Verordnung gemäß Artikeln 75, 76, 77, 78, 79, 80, 81 und 82 führt die Kommission eine Analyse durch und konsultiert die einschlägigen Interessenträger, um potenzielle Lücken sowie Überschneidungen der bestehenden sektorspezifischen Rechtsvorschriften und der Bestimmungen dieser Verordnung festzustellen.

ARTIKEL 82B**LEITLINIEN DER KOMMISSION ZUR DURCHFÜHRUNG DIESER VERORDNUNG**

- (1) Die Kommission erarbeitet in Absprache mit dem Amt für künstliche Intelligenz Leitlinien für die praktische Umsetzung dieser Verordnung, insbesondere zu folgenden Punkten:
- a) die Anwendung der Vorschriften nach Artikel 8 bis 15 und Artikel 28 bis 28b;
 - b) die in Artikel 5 genannten die verbotenen Praktiken;
 - c) die praktische Umsetzung der Bestimmungen über wesentliche Änderungen;
 - d) die praktischen Umstände, unter denen die Ergebnisse eines in Anhang III genannten KI-Systems ein erhebliches Risiko für die Gesundheit, die Sicherheit oder die Grundrechte natürlicher Personen gemäß Artikel 6 Absatz 2 darstellen würden, einschließlich Beispielen in Bezug auf die in Anhang III genannten Hochrisiko-KI-Systeme;
 - e) die praktische Umsetzung der in Artikel 52 festgelegten Transparenzanforderungen;
 - f) die Erstellung der in Artikel 69 genannten Verhaltenskodizes;
 - g) das Verhältnis dieser Verordnung zu anderen einschlägigen Rechtsvorschriften der Union, auch in Bezug auf deren einheitliche Durchsetzung;
 - h) die praktische Umsetzung von Artikel 12, Artikel 28b über die Umweltauswirkungen von Basismodellen und Anhang IV Nummer 3 Buchstabe b, insbesondere die Mess- und Aufzeichnungsverfahren für die Berechnung und Meldung der Umweltauswirkungen von Systemen zur Erfüllung der in dieser Verordnung festgelegten Verpflichtungen, einschließlich des CO₂-Fußabdrucks und der Energieeffizienz, unter Berücksichtigung des Stands der Technik und von Skaleneffekten.

Wenn die Kommission Leitlinien herausgibt, widmet sie den Bedürfnissen von KMU, einschließlich Start-up-Unternehmen, lokalen Behörden und der höchstwahrscheinlich von dieser Verordnung betroffenen Sektoren besondere Aufmerksamkeit.

- (2) Auf Ersuchen der Mitgliedstaaten oder des Amts für künstliche Intelligenz oder von sich aus aktualisiert die Kommission bereits verabschiedete Leitlinien, wenn dies als notwendig erachtet wird.

ARTIKEL 83**BEREITS IN VERKEHR GEBRACHTE ODER IN BETRIEB GENOMMENE KI-SYSTEME**

- (1) Betreiber der 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 des Inkrafttretens dieser Verordnung] in Verkehr gebracht oder in Betrieb genommen wurden,

treffen die erforderlichen Maßnahmen, um die Anforderungen dieser Verordnung bis zum... [vier Jahren nach dem Inkrafttreten dieser Verordnung] zu erfüllen.

Die in dieser Verordnung festgelegten Anforderungen werden 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 und entsprechend den jeweils gültigen Vorgaben, wenn diese Rechtsakte ersetzt oder geändert werden, erfolgt.

- (2) Diese Verordnung gilt – mit Ausnahme der in Absatz 1 genannten Systeme – für Betreiber von Hochrisiko-KI-Systemen, 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 gemäß der Definition in Artikel 3 Absatz 23 wesentlich geändert wurden. Im Falle von Hochrisiko-KI-Systemen, die bestimmungsgemäß von Behörden verwendet werden sollen, treffen die Anbieter und Betreiber solcher Systeme die erforderlichen Maßnahmen für die Erfüllung der Anforderungen dieser Verordnung [zwei Jahre nach dem Inkrafttreten dieser Verordnung].

ARTIKEL 84

BEWERTUNG UND ÜBERARBEITUNG

- (1) Nach Anhörung des Amtes für künstliche Intelligenz prüft die Kommission nach dem Inkrafttreten dieser Verordnung einmal jährlich und auf Empfehlung des Amtes, ob eine Änderung der Liste in Anhang III, einschließlich der Ausweitung der Rubriken oder der Aufnahme neuer Rubriken, der Liste verbotener KI-Praktiken des Artikels 5 und der Liste der KI-Systeme, die zusätzliche Transparenzmaßnahmen nach Artikel 52 erfordern, notwendig ist.

Die Kommission übermittelt die Schlussfolgerungen dieser Bewertungen dem Europäischen Parlament und dem Rat.

- (2) Bis zum [Datum zwei Jahre nach dem Datum der Anwendung dieser Verordnung nach Artikel 85 Absatz 2] und danach alle zwei Jahre legt die Kommission gemeinsam mit dem Amt für künstliche Intelligenz 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, technischen 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,

- ba) der Entwicklungsstand harmonisierter Normen und gemeinsamer Spezifikationen für künstliche Intelligenz;
 - bb) der Umfang von Investitionen in Forschung, Entwicklung und Einsatz von KI-Systemen in der Union;
 - bc) die Wettbewerbsfähigkeit des zusammengefassten europäischen KI-Sektors im Vergleich zu den KI-Sektoren in Drittländern;
 - bd) die Auswirkung der Verordnung hinsichtlich des Ressourcen- und Energieverbrauchs sowie des Abfallaufkommens und anderer Umweltauswirkungen;
 - be) die Umsetzung des koordinierten Plans für künstliche Intelligenz, wobei das unterschiedliche Ausmaß des Fortschritts unter den Mitgliedstaaten zu berücksichtigen ist und bestehende Hindernisse für Innovationen im Bereich der KI zu ermitteln sind;
 - bf) die Aktualisierung der spezifischen Anforderungen an die Nachhaltigkeit von KI-Systemen und Basismodellen ausgehend von der Melde- und Dokumentationspflicht in Anhang IV und in Artikel 28b;
 - bg) der Rechtsrahmen zur Regelung von Basismodellen;
 - bh) die Liste der missbräuchlichen Vertragsklauseln in Artikel 28a, wobei erforderlichenfalls neue Geschäftspraktiken berücksichtigt werden.
- (3a) Bis zum ... [zwei Jahre nach Inkrafttreten dieser Verordnung gemäß Artikel 85 Absatz 2] bewertet die Kommission die Arbeitsweise des Amts für künstliche Intelligenz und prüft, ob das Amt mit ausreichenden Befugnissen und Zuständigkeiten zur Erfüllung seiner Aufgaben ausgestattet wurde, und ob es für die ordnungsgemäße Durchführung und Durchsetzung dieser Verordnung zweckmäßig und erforderlich wäre, das Büro und seine Durchsetzungskompetenzen zu erweitern und seine Ressourcen aufzustocken. Die Kommission übermittelt diesen Evaluierungsbericht dem Europäischen Parlament und dem Rat.
- (4) Innerhalb von [*eines Jahres nach dem Datum der Anwendung dieser Verordnung nach Artikel 85 Absatz 2*] und danach alle zwei 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 das Amt für künstliche Intelligenz, die Mitgliedstaaten und die zuständigen nationalen Behörden der Kommission auf Anfrage unverzüglich die gewünschten Informationen.
- (6) Bei den in den Absätzen 1 und 4 genannten Bewertungen und Überprüfungen berücksichtigt die Kommission die Standpunkte und Feststellungen des Amts für künstliche Intelligenz, des Europäischen Parlaments, des Rates und anderer einschlägiger Stellen oder Quellen und

konsultieren die einschlägigen Interessenträger. Das Ergebnis dieser Konsultation wird dem Bericht beigefügt.

- (7) Die Kommission legt erforderlichenfalls geeignete Vorschläge zur Änderung dieser Verordnung vor und berücksichtigt dabei insbesondere die technischen Entwicklungen, die Auswirkungen von KI-Systemen auf die Gesundheit und Sicherheit, die Grundrechte, die Umwelt, die Gleichstellung und Barrierefreiheit für Personen mit Behinderung, die Demokratie und Rechtsstaatlichkeit und die Fortschritte in der Informationsgesellschaft.
- (7a) Als Anleitung für die in Absatz 1 bis 4 dieses Artikels genannten Bewertungen und Überprüfungen entwickelt das Amt ein Ziel und eine partizipative Methode für die Bewertung des Risikoniveaus anhand der Kriterien gemäß den maßgeblichen Artikeln und für die Einbeziehung neuer Systeme in die Liste in Anhang III, einschließlich der Erweiterung bestehender Rubriken oder der Aufnahme neuer Rubriken; die Liste der verbotenen Praktiken in Artikel 5; und die Liste der KI-Systeme, die zusätzliche Transparenzmaßnahmen gemäß Artikel 52 erfordern.
- (7b) Eine Änderung dieser Verordnung im Sinne des Absatzes 7 oder künftige delegierte oder Durchführungsrechtsakte, die sektorspezifische Rechtsvorschriften gemäß Anhang II Abschnitt B betreffen, berücksichtigen die regulatorischen Besonderheiten des jeweiligen Sektors und die in der Verordnung festgelegten bestehenden Governance-, Konformitätsbewertungs- und Durchsetzungsmechanismen und -behörden.
- (7c) Bis zum ... [fünf Jahre nach dem Beginn der Anwendung dieser Verordnung] nimmt die Kommission unter Berücksichtigung der ersten Jahre der Anwendung der Verordnung eine Bewertung der Durchsetzung dieser Verordnung vor und erstattet dem Europäischen Parlament, dem Rat und dem Europäischen Wirtschafts- und Sozialausschuss darüber Bericht. Auf Grundlage der Ergebnisse wird dem Bericht gegebenenfalls ein Abänderung für diese Verordnung beigefügt, der die Struktur der Durchsetzung und die Notwendigkeit einer Unionsagentur für die Behebung nicht erkannter Mängel betrifft.

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
Der Präsident

Im Namen des Rates
Der Präsident

V. 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. VERWALTUNGSMABNAHMEN

- 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. *Finanzierungsbeitrag Dritter*

3.3. Geschätzte Auswirkungen auf die Einnahme

VI. 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

eine neue Maßnahme

eine neue Maßnahme im Anschluss an ein Pilotprojekt/eine vorbereitende Maßnahme⁶⁰

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

⁶⁰ Im Sinne des Artikels 54 Absatz 2 Buchstabe a oder b der Haushaltsordnung.

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.

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

unbefristete Laufzeit

- Anlaufphase von **ein/zwei Jahren (zu bestätigen)**,
- anschließend reguläre Umsetzung.

1.7. Vorgeschlagene Methode(n) der Mittelverwaltung⁶¹

- Direkte Mittelverwaltung** durch die Kommission

⁶¹ 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.

- 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

2. VERWALTUNGSMABNAHMEN

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 notifizierte 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 ⁶²	von EFTA-Ländern ⁶³	von Kandidatenländer ⁶⁴	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.
- Für den Vorschlag/die Initiative werden die folgenden operativen Mittel benötigt:

in Mio. EUR (3 Dezimalstellen)

Rubrik des Mehrjährigen Finanzrahmens	1	
--	---	--

⁶² GM = Getrennte Mittel/NGM = Nichtgetrennte Mittel.

⁶³ EFTA: Europäische Freihandelsassoziation.

⁶⁴ Kandidatenländer und gegebenenfalls potenzielle Kandidaten des Westbalkans.

GD: CNECT				Jahr 2022	Ja hr 20 23	Ja hr 20 24	Ja hr 20 25	Ja hr 20 26	Ja hr 20 27 ⁶⁵	INSGESAMT
• Operative Mittel										
Haushaltslinie ⁶⁶ 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 ⁶⁷										
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	=1 a+ 1b +3		1,240		0,240	0,240	0,240		2,200
	Zahlungen	=2 a+ 2b +3		0,840	0,340	0,340	0,340	0,340		2,200

⁶⁵ Vorläufig und abhängig von der Verfügbarkeit von Haushaltsmitteln.

⁶⁶ Gemäß dem offiziellen Eingliederungsplan.

⁶⁷ Technische und/oder administrative Hilfe und Ausgaben zur Unterstützung der Durchführung von Programmen bzw. Maßnahmen der EU (vormalige BA-Linien), indirekte Forschung, direkte Forschung.

•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
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 ⁶⁸	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)

⁶⁸ Alle Zahlen in dieser Spalte sind vorläufig und von der Fortführung der Programme und der Verfügbarkeit von Mitteln abhängig.

		Jahr 2022	Ja hr 20 23	Ja hr 20 24	Jahr 202 5	Jahr 2026	Jahr 2027		INSGES AMT
Mittel INSGESAMT unter RUBRIKEN 1 bis 7 des mehrjährigen Finanzrahmens	Verpflichtun gen		2,7 70	1,7 70	1,77 0	1,770	1,770		9,850
	Zahlungen		2,3 70	1,8 70	1,87 0	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 ⁶⁹		INSGESAMT	
			Anzahl	Kosten	Anzahl	Kosten	Anzahl	Kosten	Anzahl	Kosten	Anzahl	Kosten	Anzahl	Kosten	Anzahl	Kosten		
ERGEBNISSE																		
	Art	Durchschnittskosten	Anzahl	Kosten	Anzahl	Kosten	Anzahl	Kosten	Anzahl	Kosten	Anzahl	Kosten	Anzahl	Kosten	Anzahl	Kosten	Gesamtzahl	Gesamtkosten
EINZELZIEL Nr. 1 ⁷⁰ ...																		
Datenbank				1	1,0	1		1		1		1		1	0,1	1	1,00	
Sitzungserge				10	0,2	10	0,200	10	0,2	1	0,2	1	0,2	1	0,2	50	1,00	
Kommunikations-				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	

⁶⁹ Alle Zahlen in dieser Spalte sind vorläufig und von der Fortführung der Programme und der Verfügbarkeit von Mitteln abhängig.

⁷⁰ 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.
- 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 ⁷¹	INSGESA MT
--	--------------	--------------	--------------	--------------	--------------	--------------	--	---------------

RUBRIK 7 des mehrjährigen Finanzrahmens								
Personal		1,520	1,520	1,520	1,520	1,520	1,520	7,600
Sonstige Verwaltungsausga ben		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 7⁷²des mehrjährigen Finanzrahmens								
Personal								
Sonstige Verwaltungsausga ben		0,240	0,240	0,240	0,240	0,240	0,240	1,20
Zwischensumme außerhalb der		0,240	0,240	0,240	0,240	0,240	0,240	1,20

⁷¹ Alle Zahlen in dieser Spalte sind vorläufig und von der Fortführung der Programme und der Verfügbarkeit von Mitteln abhängig.

⁷² Technische und/oder administrative Hilfe und Ausgaben zur Unterstützung der Durchführung von Programmen bzw. Maßnahmen der EU (vormalige BA-Linien), indirekte Forschung, direkte Forschung.

RUBRIK 7 des mehrjährigen Finanzrahmens								
--	--	--	--	--	--	--	--	--

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.

3.2.3.1. Geschätzter Personalbedarf

- Für den Vorschlag/die Initiative wird kein Personal benötigt.
- Für den Vorschlag/die Initiative wird folgendes Personal benötigt:

Schätzung in Vollzeitäquivalenten

		Jahr 2023	Jahr 2024	Jahr 2025	202 6	202 7	Nach 2027 <small>73</small>	
• 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)⁷⁴								
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 ⁷⁵	- 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.

⁷³ Alle Zahlen in dieser Spalte sind vorläufig und von der Fortführung der Programme und der Verfügbarkeit von Mitteln abhängig.

⁷⁴ VB = Vertragsbedienstete, ÖB = örtliche Bedienstete, ANS = abgeordnete nationale Sachverständige, LAK = Leiharbeitskräfte, JFD = Juniorfachkräfte in Delegationen.

⁷⁵ Teilobergrenze für aus operativen Mitteln finanziertes externes Personal (vormalige BA-Linien).

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	<p>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.</p> <p>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.</p>
Externes Personal	

3.2.4. *Vereinbarkeit mit dem Mehrjährigen Finanzrahmen*

Der Vorschlag/Die Initiative

- 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. *Finanzierungsbeitrag Dritter*

Der Vorschlag/Die Initiative

- sieht keine Kofinanzierung durch Dritte vor.
- sieht folgende Kofinanzierung durch Dritte vor:

Mittel in Mio. EUR (3 Dezimalstellen)

	Jahr N ⁷⁶	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								

⁷⁶ 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 ⁷⁷								
		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).

⁷⁷ Bei den traditionellen Eigenmitteln (Zölle, Zuckerabgaben) sind die Beträge netto, d. h. abzüglich 20 % für Erhebungskosten, anzugeben.

C. ANHÄNGE

ANHANG II**LISTE DER HARMONISIERUNGSVORSCHRIFTEN DER UNION****Abschnitt A – Liste der Harmonisierungsrechtsvorschriften der Union auf der Grundlage des neuen Rechtsrahmens**

1. Richtlinie 2006/42/EG des Europäischen Parlaments und des Rates vom 17. Mai 2006 über Maschinen und zur Änderung der Richtlinie 95/16/EG (ABl. L 157 vom 9.6.2006, S. 24) [aufgehoben durch die Maschinenverordnung];
2. Richtlinie 2009/48/EG des Europäischen Parlaments und des Rates vom 18. Juni 2009 über die Sicherheit von Spielzeug (ABl. L 170 vom 30.6.2009, S. 1);
3. Richtlinie 2013/53/EU des Europäischen Parlaments und des Rates vom 20. November 2013 über Sportboote und Wassermotorräder und zur Aufhebung der Richtlinie 94/25/EG (ABl. L 354 vom 28.12.2013, S. 90);
4. Richtlinie 2014/33/EU des Europäischen Parlaments und des Rates vom 26. Februar 2014 zur Angleichung der Rechtsvorschriften der Mitgliedstaaten über Aufzüge und Sicherheitsbauteile für Aufzüge (ABl. L 96 vom 29.3.2014, S. 251);
5. Richtlinie 2014/34/EU des Europäischen Parlaments und des Rates vom 26. Februar 2014 zur Harmonisierung der Rechtsvorschriften der Mitgliedstaaten für Geräte und Schutzsysteme zur bestimmungsgemäßen Verwendung in explosionsgefährdeten Bereichen (ABl. L 96 vom 29.3.2014, S. 309);
6. Richtlinie 2014/53/EU des Europäischen Parlaments und des Rates vom 16. April 2014 über die Harmonisierung der Rechtsvorschriften der Mitgliedstaaten über die Bereitstellung von Funkanlagen auf dem Markt und zur Aufhebung der Richtlinie 1999/5/EG (ABl. L 153 vom 22.5.2014, S. 62);
7. Richtlinie 2014/68/EU des Europäischen Parlaments und des Rates vom 15. Mai 2014 zur Harmonisierung der Rechtsvorschriften der Mitgliedstaaten über die Bereitstellung von Druckgeräten auf dem Markt (ABl. L 189 vom 27.6.2014, S. 164);
8. Verordnung (EU) 2016/424 des Europäischen Parlaments und des Rates vom 9. März 2016 über Seilbahnen und zur Aufhebung der Richtlinie 2000/9/EG (ABl. L 81 vom 31.3.2016, S. 1);
9. Verordnung (EU) 2016/425 des Europäischen Parlaments und des Rates vom 9. März 2016 über persönliche Schutzausrüstungen und zur Aufhebung der Richtlinie 89/686/EWG des Rates (ABl. L 81 vom 31.3.2016, S. 51);
10. Verordnung (EU) 2016/426 des Europäischen Parlaments und des Rates vom 9. März 2016 über Geräte zur Verbrennung gasförmiger Brennstoffe und zur Aufhebung der Richtlinie 2009/142/EG (ABl. L 81 vom 31.3.2016, S. 99);

11. 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);
12. 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).

Abschnitt B – Liste der Harmonisierungsrechtsvorschriften der Union

1. 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);
2. 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);
3. 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);
4. 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);
5. 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);
6. 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);
3. 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);
7. 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), insoweit die Konstruktion, Herstellung und Vermarktung von Luftfahrzeugen gemäß Artikel 2 Absatz 1 Buchstaben a und b in Bezug auf unbemannte Luftfahrzeuge sowie deren Motoren, Propeller, Teile und Ausrüstung zur Fernsteuerung betroffen sind.

ANHANG III**HOCHRISIKO-KI-SYSTEME GEMÄß ARTIKEL 6 ABSATZ 2**

Die spezifisch unter den Nummern 1 bis 8a aufgeführten KI-Systeme stehen für kritische Anwendungsfälle und gelten als Hochrisiko-KI-Systeme gemäß Artikel 6 Absatz 2, sofern sie die in diesem Artikel festgelegten Kriterien erfüllen:

1. Biometrische Identifizierung und auf Biometrie beruhende Systeme:
 - a) KI-Systeme, die bestimmungsgemäß für die biometrische Identifizierung natürlicher Personen verwendet werden sollen, mit Ausnahme der in Artikel 5 genannten Systeme;
 - aa) KI-Systeme, durch die auf der Grundlage biometrischer oder biometriegestützter Daten Rückschlüsse auf persönliche Merkmale natürlicher Personene gezogen werden, einschließlich Systeme zum Erkennen von Emotionen, mit Ausnahme der in Artikel 5 genannten Systeme;

Nummer 1 sollte keine KI-Systeme umfassen die bestimmungsgemäß für die biometrische Verifizierung verwendet werden sollen, deren einziger Zweck darin besteht, zu bestätigen, dass eine bestimmte Person die Person ist, für die sie sich ausgibt.
2. Verwaltung und Betrieb kritischer Infrastrukturen:
 - a) KI-Systeme, die bestimmungsgemäß als Sicherheitskomponenten in der Verwaltung und im Betrieb des Straßen-, Schienen und Luftverkehrs verwendet werden sollen, es sei denn, diese werden im Rahmen von Harmonisierungs- oder sektorspezifischen Rechtsvorschriften geregelt.
 - aa) KI-Systeme, die bestimmungsgemäß als Sicherheitskomponenten in der Verwaltung und im Betrieb der Wasser-, Gas-, Wärme- und Stromversorgung sowie kritischer digitaler Infrastruktur verwendet werden sollen;
3. Allgemeine und berufliche Bildung:
 - a) KI-Systeme, die bestimmungsgemäß für Entscheidungen über den Zugang oder zur erheblichen Einflussnahme auf Entscheidungen über die Zulassung oder die Zuweisung natürlicher Personen zu Einrichtungen der allgemeinen und beruflichen Bildung verwendet werden sollen;
 - b) KI-Systeme, die bestimmungsgemäß für die Bewertung von Schülern in Einrichtungen der allgemeinen und beruflichen Bildung und für die Bewertung der Teilnehmer an üblicherweise für die Zulassung zu diesen Einrichtungen erforderlichen Tests verwendet werden sollen;
 - ba) KI-Systeme, die bestimmungsgemäß für die Bewertung des angemessenen Bildungsniveaus einer Person verwendet werden sollen und das Niveau der Bildung

und Ausbildung, das die Person erhält oder zu dem sie Zugang erhält, wesentlich beeinflussen;

- bb) KI-Systeme, die bestimmungsgemäß zur Überwachung und Erkennung von unzulässigem Verhalten von Schülern und Studierenden bei Prüfungen im Rahmen von/in Einrichtungen der allgemeinen und beruflichen Bildung verwendet werden sollen;

4. Beschäftigung, Personalmanagement und Zugang zur Selbstständigkeit:

- a) KI-Systeme, die bestimmungsgemäß für die Einstellung oder Auswahl natürlicher Personen verwendet werden sollen, insbesondere für die Bekanntmachung gezielter Stellenausschreibungen, das Sichten oder Filtern von Bewerbungen und das Bewerten von Bewerbern in Vorstellungsgesprächen oder Tests;
- b) KI-Systeme, die bestimmungsgemäß für Entscheidungen oder zur erheblichen Einflussnahme auf Entscheidungen betreffend die Einstellung, Beförderung und Kündigung von Arbeitsvertragsverhältnissen, die Aufgabenzuweisung auf der Grundlage des individuellen Verhaltens oder persönlicher Eigenschaften oder Merkmale oder für die Überwachung und Bewertung der Leistung und des Verhaltens von Personen in solchen Beschäftigungsverhältnissen verwendet werden sollen;

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

- a) KI-Systeme, die bestimmungsgemäß von Behörden oder im Namen von Behörden verwendet werden sollen, um zu beurteilen, ob natürliche Personen Anspruch auf öffentliche Unterstützungsleistungen und -dienste haben, einschließlich Gesundheitsdienstleistungen und wesentlicher Dienstleistungen, jedoch nicht beschränkt auf Wohnen, Strom, Heizung/Kühlung und Internet, und ob solche Leistungen und Dienste zu gewähren, einzuschränken, zu widerrufen, zu erhöhen oder zurückzufordern sind;
- b) KI-Systeme, die bestimmungsgemäß für die Kreditwürdigkeitsprüfung und Kreditpunktebewertung natürlicher Personen verwendet werden sollen, mit Ausnahme von KI-Systemen, die zur Aufdeckung von Finanzbetrug verwendet werden;
- ba) KI-Systeme, die bestimmungsgemäß für Entscheidungen oder zur wesentlichen Einflussnahme auf Entscheidungen darüber, ob eine natürliche Person für eine Kranken- oder Lebensversicherung in Frage kommt, verwendet werden sollen;
- c) KI-Systeme, die bestimmungsgemäß zur Bewertung und Klassifizierung von Notrufen von natürlichen Personen oder für die Entsendung oder Priorisierung des Einsatzes von Not- und Rettungsdiensten, einschließlich Polizei und Strafverfolgungsbehörden, Feuerwehr und medizinischer Nothilfe, sowie für Systeme für die Triage von Patienten bei der Notfallversorgung verwendet werden sollen;

6. Strafverfolgung:

- b) KI-Systeme, die bestimmungsgemäß von Strafverfolgungsbehörden oder in deren Namen oder von Organen, Einrichtungen oder sonstigen Stellen der Union als Lügendetektoren und ähnliche Instrumente – sofern deren Verwendung gemäß den relevanten nationalen Rechtsvorschriften und denen der Union zugelassen ist – verwendet werden sollen;
- d) KI-Systeme, die bestimmungsgemäß von Strafverfolgungsbehörden oder in deren Namen oder von Organen, Einrichtungen und sonstigen Stellen der Union zur Unterstützung von Strafverfolgungsbehörden zur Bewertung der Verlässlichkeit von Beweismitteln im Zuge der Ermittlung oder Verfolgung von Straftaten verwendet werden sollen;
- f) KI-Systeme, die bestimmungsgemäß von Strafverfolgungsbehörden oder in deren Namen oder von Organen, Einrichtungen und sonstigen Stellen der Union zur Unterstützung von Strafverfolgungsbehörden zur Erstellung von Profilen natürlicher Personen gemäß Artikel 3 Absatz 4 der Richtlinie (EU) 2016/680 im Zuge der Aufdeckung, Ermittlung oder Verfolgung von Straftaten oder im Falle von Organen, Einrichtungen oder sonstigen Stellen der Union gemäß Artikel 3 Nummer 5 der Verordnung (EU) 2018/1725 verwendet werden sollen;
- g) KI-Systeme, die bestimmungsgemäß von Strafverfolgungsbehörden oder in ihrem Auftrag oder von Organen, Einrichtungen und sonstigen Stellen der Union zur Unterstützung von Strafverfolgungsbehörden zur Kriminalanalyse natürlicher Personen eingesetzt werden sollen und es den Strafverfolgungsbehörden ermöglichen, große komplexe verknüpfte und unverknüpfte Datensätze aus verschiedenen Datenquellen oder in verschiedenen Datenformaten zu durchsuchen, um unbekannte Muster zu erkennen oder verdeckte Beziehungen in den Daten aufzudecken;

7. Migration, Asyl und Grenzkontrolle:

- a) KI-Systeme, die bestimmungsgemäß von zuständigen Behörden oder in deren Namen oder von Organen, Einrichtungen und sonstigen Stellen der Union als Lügendetektoren und ähnliche verwendet werden sollen, sofern ihre Verwendung gemäß den einschlägigen Rechtsvorschriften der Union oder den einschlägigen nationalen Rechtsvorschriften zugelassen ist;
- b) KI-Systeme, die bestimmungsgemäß von zuständigen Behörden oder in deren Namen oder von Organen, Einrichtungen und sonstigen Stellen der Union zur Bewertung eines Risikos verwendet werden sollen, einschließlich eines Sicherheitsrisikos, eines Risikos der irregulären Einwanderung oder eines Gesundheitsrisikos, das von einer natürlichen Person ausgeht, die in das Hoheitsgebiet eines Mitgliedstaats einzureisen beabsichtigt oder eingereist ist;
- c) KI-Systeme, die bestimmungsgemäß von zuständigen Behörden oder in deren Namen oder von Organen, Einrichtungen und sonstigen Stellen der Union zur Überprüfung der

Echtheit von Reisedokumenten und Nachweisunterlagen natürlicher Personen und zur Erkennung unechter Dokumente durch Prüfung ihrer Sicherheitsmerkmale verwendet werden sollen;

- d) KI-Systeme, die bestimmungsgemäß von zuständigen Behörden oder in deren Namen oder von Organen, Einrichtungen und sonstigen Stellen der Union verwendet werden sollen, um zuständige Behörden bei der Prüfung und Bewertung des Wahrheitsgehalts von Nachweisen von Asyl- und Visumanträgen sowie Aufenthaltstiteln und damit verbundenen Beschwerden im Hinblick auf die Feststellung der Berechtigung der den Antrag stellenden natürlichen Personen zu unterstützen;
- da) KI-Systeme, die bestimmungsgemäß von zuständigen Behörden oder in deren Namen oder von Organen, Einrichtungen und sonstigen Stellen der Union in den Bereichen Migration, Asyl und Grenzkontrolle für die Überwachung, Kontrolle oder Verarbeitung von Daten im Zusammenhang mit Grenzkontrolltätigkeiten zur Detektion, Erkennung oder Identifizierung von natürlichen Personen verwendet werden sollen;
- db) KI-Systeme, die bestimmungsgemäß von zuständigen Behörden oder in deren Namen oder von Organen, Einrichtungen und sonstigen Stellen der Union in den Bereichen Migration, Asyl und Grenzkontrolle für die Vorhersage und Prognose von Trends im Hinblick auf Migration, Bewegungen und Grenzübertritte verwendet werden sollen;

8. Rechtspflege und demokratische Prozesse:

- a) KI-Systeme, die bestimmungsgemäß von Justiz- oder Verwaltungsbehörden oder in deren Namen zur Unterstützung einer Justiz- oder Verwaltungsbehörde bei der Ermittlung und Auslegung von Sachverhalten und Rechtsvorschriften und bei der Anwendung des Rechts auf konkrete Sachverhalte verwendet oder auf ähnliche Weise in einem alternativen Streitbeilegungsverfahren eingesetzt werden sollen.
- aa) KI-Systeme, die bestimmungsgemäß verwendet werden sollen, um das Ergebnis einer Wahl oder eines Referendums oder das Wahlverhalten natürlicher Personen bei der Ausübung ihres Wahlrechts bei einer Wahl oder einem Referendum zu beeinflussen. Dies umfasst keine KI-Systeme, deren Ergebnissen natürliche Personen nicht direkt ausgesetzt sind, wie Instrumente zur Organisation, Optimierung und Strukturierung politischer Kampagnen in administrativer und logistischer Hinsicht.
- ab) KI-Systeme die bestimmungsgemäß von Social-Media- Plattformen, die im Sinne des Artikels 33 der Verordnung (EU) Nr. 2022/2065 als sehr große Online-Plattformen gelten, in ihren Empfehlungssystemen verwendet werden sollen, um dem Empfänger der Dienstleistung auf der Plattform verfügbare nutzergenerierte Inhalte zu empfehlen.

ANHANG IV**TECHNISCHE DOKUMENTATION GEMÄß ARTIKEL 11 ABSATZ 1**

Die in Artikel 11 Absatz 1 genannte technische Dokumentation muss mindestens die folgenden Informationen enthalten, soweit sie für das betreffende KI-System von Belang sind:

1. Allgemeine Beschreibung des KI-Systems einschließlich:
 - a) Zweckbestimmung, Name des Anbieters und Version des Systems mit Angaben dazu, in welcher Beziehung sie zu vorherigen und gegebenenfalls neueren Versionen in den aufeinanderfolgenden Systemüberarbeitungen steht;
 - aa) die Art der Daten, die wahrscheinlich vom System verarbeitet werden oder verarbeitet werden sollen, und im Fall von personenbezogenen Daten die Kategorien natürlicher Personen und Gruppen, die wahrscheinlich betroffen sind oder betroffen sein sollen;
 - b) gegebenenfalls die Art und Weise der Interaktion oder Verwendung des KI-Systems mit Hardware oder Software, einschließlich anderer KI-Systeme, die nicht Teil des KI-Systems selbst sind;
 - c) Versionen der betreffenden Software oder Firmware und gegebenenfalls Informationen für den Betreiber über etwaige Anforderungen in Bezug auf die Aktualisierung der Versionen;
 - d) Beschreibung der verschiedenen Konfigurationen und Varianten des KI-Systems, die in Verkehr gebracht oder in Betrieb genommen werden sollen;
 - e) Beschreibung der Hardware, auf der das KI-System betrieben werden soll;
 - f) falls das KI-System Bestandteil von Produkten ist: Fotografien oder Abbildungen, die äußere Merkmale, Kennzeichnungen und den inneren Aufbau dieser Produkte zeigen;
 - fa) Beschreibung der Schnittstelle des Betreibers;
 - g) Gebrauchsanweisungen für die Betreiber gemäß Artikel 13 Absätze 2 und 3 sowie Artikel 14 Absatz 4 Buchstabe e und gegebenenfalls Aufbau- oder Installationsanweisungen;
 - ga) detaillierte und leicht verständliche Beschreibung des wichtigen Optimierungsziels bzw. der wichtigsten Optimierungsziele des Systems;
 - gb) detaillierte und leicht verständliche Beschreibung der erwarteten Ausgabe und der erwarteten Ausgabequalität des Systems;
 - gc) detaillierte und leicht verständliche Anweisungen für die Interpretation der Ausgabe des Systems;
 - gd) Beispiele von Szenarien, für die das System nicht verwendet werden sollte;

2. Detaillierte Beschreibung der Bestandteile des KI-Systems und seines Entwicklungsprozesses einschließlich:
- a) Methoden und Schritte zur Entwicklung des KI-Systems, gegebenenfalls einschließlich des Einsatzes von Dritten bereitgestellter vortrainierter Systeme oder Werkzeuge, und wie diese vom Anbieter benutzt, integriert oder verändert wurden;
 - b) Beschreibung der Architektur, Entwurfsspezifikationen, Algorithmen und Datenstrukturen, einschließlich einer Aufgliederung seiner Komponenten und Schnittstellen, wie sie miteinander in Beziehung stehen und wie sie für die allgemeine Verarbeitung oder Logik des KI-Systems sorgen; wichtigste Entwurfsentscheidungen mit den Gründen und Annahmen, auch in Bezug auf Personen oder Personengruppen, auf die das System angewandt werden soll; hauptsächliche Klassifizierungsentscheidungen; was das System optimieren soll und welche Bedeutung den verschiedenen Parametern dabei zukommt; Entscheidungen über mögliche Kompromisse in Bezug auf die technischen Lösungen, mit denen die Anforderungen in Titel III Kapitel 2 erfüllt werden sollen;
 - d) gegebenenfalls Datenanforderungen in Form von Datenblättern, in denen die Trainingsmethoden und -techniken und die verwendeten Trainingsdatensätze beschrieben werden, mit Angaben zu Herkunft, Umfang und Hauptmerkmalen dieser Datensätze; Angaben zur Beschaffung und Auswahl der Daten; Kennzeichnungsverfahren (z. B. für überwachtes Lernen), Datenbereinigungsmethoden (z. B. Erkennung von Ausreißern);
 - e) Bewertung der nach Artikel 14 erforderlichen Maßnahmen der menschlichen Aufsicht, mit einer Bewertung der technischen Maßnahmen, die erforderlich sind, um den Betreibern gemäß Artikel 13 Absatz 3 Buchstabe d die Interpretation der Ergebnisse von KI-Systemen zu erleichtern;
 - f) gegebenenfalls detaillierte Beschreibung der vorab bestimmten Änderungen an dem KI-System und seiner Leistung mit allen einschlägigen Angaben zu den technischen Lösungen, mit denen sichergestellt wird, dass das KI-System die einschlägigen Anforderungen nach Titel III Kapitel 2 weiterhin dauerhaft erfüllt;
 - g) verwendete Validierungs- und Testverfahren, mit Angaben zu den verwendeten Validierungs- und Testdaten und deren Hauptmerkmalen; Parameter, die zur Messung der Genauigkeit, Robustheit und der Erfüllung anderer einschlägiger Anforderungen nach Titel III Kapitel 2 sowie potenziell diskriminierender Auswirkungen verwendet werden; Testprotokolle und alle von den verantwortlichen Personen datierten und unterzeichneten Testberichte, auch in Bezug auf die in Buchstabe f genannten vorab bestimmten Änderungen.
 - ga) mit Blick auf die Cybersicherheit ergriffene Maßnahmen.

3. Detaillierte Informationen über die Überwachung, Funktionsweise und Kontrolle des KI-Systems, insbesondere in Bezug auf: seine Fähigkeiten und Leistungsgrenzen, mit dem Genauigkeitsgrad für bestimmte Personen oder Personengruppen, auf die das System angewandt werden soll, und dem insgesamt erwarteten Genauigkeitsgrad in Bezug auf seine Zweckbestimmung; vorhersehbare unbeabsichtigte Ergebnisse und Risikoquellen für die Gesundheit und Sicherheit, die Grundrechte und eine etwaige Diskriminierung angesichts der Zweckbestimmung des KI-Systems; die nach Artikel 14 erforderlichen Maßnahmen der menschlichen Aufsicht, einschließlich der technischen Maßnahmen, die getroffen wurden, um den Betreibern die Interpretation der Ergebnisse von KI-Systemen zu erleichtern; gegebenenfalls Spezifikationen für die Eingabedaten;
 - 3a. Darlegungen zur Eignung der Leistungsparameter für das spezifische KI-System;
 - 3b. Informationen über den Energieverbrauch des KI-Systems während der Entwicklungsphase und den erwarteten Energieverbrauch während der Nutzung, wobei etwaige einschlägige Rechtsvorschriften der Union und nationale Rechtsvorschriften zu berücksichtigen sind;
4. Detaillierte Beschreibung des Risikomanagementsystems gemäß Artikel 9;
5. Beschreibung aller relevanten vom Anbieter an dem System während seines Lebenszyklus vorgenommenen Änderungen;
6. Aufstellung der vollständig oder teilweise angewandten harmonisierten Normen, deren Fundstellen im *Amtsblatt der Europäischen Union* veröffentlicht worden sind; falls keine solchen harmonisierten Normen angewandt werden, eine detaillierte Beschreibung der Lösungen, mit denen die Anforderungen in Titel III Kapitel 2 erfüllt werden sollen, mit einer Aufstellung anderer einschlägiger Normen oder gemeinsamer Spezifikationen;
7. Kopie der EU-Konformitätserklärung;
8. Detaillierte Beschreibung des Systems zur Bewertung der Leistung des KI-Systems in der Phase nach dem Inverkehrbringen gemäß Artikel 61, mit dem in Artikel 61 Absatz 3 genannten Plan für die Beobachtung nach dem Inverkehrbringen.

ANHANG V**EU-KONFORMITÄTSERKLÄRUNG**

Die EU-Konformitätserklärung gemäß Artikel 48 enthält alle folgenden Angaben:

1. Name und Art des KI-Systems und etwaige zusätzliche eindeutige Angaben, die die Identifizierung und Rückverfolgbarkeit des KI-Systems ermöglichen;
2. Name und Anschrift des Anbieters und gegebenenfalls seines Bevollmächtigten;
3. Erklärung darüber, dass der Anbieter die alleinige Verantwortung für die Ausstellung der EU-Konformitätserklärung trägt;
4. Versicherung, dass das betreffende KI-System der vorliegenden Verordnung sowie gegebenenfalls weiteren einschlägigen Rechtsvorschriften der Union, in denen die Ausstellung einer EU-Konformitätserklärung vorgesehen ist, entspricht;
- 4a. Wenn ein KI-System die Verarbeitung personenbezogener Daten erfordert, eine Erklärung darüber, dass das KI-System den Verordnungen (EU) 2016/679 und (EU) 2018/1725 sowie der Richtlinie (EU) 2016/680 entspricht.
5. Verweise auf die verwendeten einschlägigen harmonisierten Normen oder sonstigen gemeinsamen Spezifikationen, für die die Konformität erklärt wird;
6. gegebenenfalls Name und Kennnummer der notifizierten Stelle, Beschreibung des durchgeführten Konformitätsbewertungsverfahrens und Kennnummer der ausgestellten Bescheinigung;
7. Ort und Datum der Ausstellung der Erklärung, Unterschrift, Name und Funktion des Unterzeichners sowie Angabe, für wen und in wessen Namen diese Person unterzeichnet hat, Unterschrift.

ANHANG VI**KONFORMITÄTBEWERTUNGSVERFAHREN AUF DER GRUNDLAGE EINER INTERNEN KONTROLLE**

1. Das Konformitätsbewertungsverfahren auf der Grundlage einer internen Kontrolle ist das Konformitätsbewertungsverfahren gemäß den Nummern 2 bis 4.
2. Der Anbieter überprüft, ob das bestehende Qualitätsmanagementsystem den Anforderungen des Artikels 17 entspricht.
3. Der Anbieter prüft die in der technischen Dokumentation enthaltenen Informationen, um zu beurteilen, ob das KI-System den einschlägigen grundlegenden Anforderungen in Titel III Kapitel 2 entspricht.
4. Der Anbieter überprüft ferner, ob der Entwurfs- und Entwicklungsprozess des KI-Systems und seine Beobachtung nach dem Inverkehrbringen gemäß Artikel 61 mit der technischen Dokumentation im Einklang stehen.

ANHANG VII**KONFORMITÄT AUF DER GRUNDLAGE DER BEWERTUNG DES QUALITÄTSMANAGEMENTSYSTEMS UND DER BEWERTUNG DER TECHNISCHEN DOKUMENTATION**

1. Einleitung

Das Konformitätsbewertungsverfahren auf der Grundlage der Bewertung des Qualitätsmanagementsystems und der Bewertung der technischen Dokumentation ist das Konformitätsbewertungsverfahren gemäß den Nummern 2 bis 5.

2. Überblick

Das genehmigte Qualitätsmanagementsystem für die Konzeption, die Entwicklung und das Testen von KI-Systemen nach Artikel 17 wird gemäß Nummer 3 geprüft und unterliegt der Überwachung gemäß Nummer 5. Die technische Dokumentation des KI-Systems wird gemäß Nummer 4 geprüft.

3. Qualitätsmanagementsystem

3.1. Der Antrag des Anbieters muss Folgendes enthalten:

- a) den Namen und die Anschrift des Anbieters sowie, wenn der Antrag vom Bevollmächtigten eingereicht wird, auch dessen Namen und Anschrift;
- b) die Liste der unter dasselbe Qualitätsmanagementsystem fallenden KI-Systeme;
- c) die technische Dokumentation für jedes unter dasselbe Qualitätsmanagementsystem fallende KI-System;
- d) die Dokumentation über das Qualitätsmanagementsystem mit allen in Artikel 17 aufgeführten Aspekten;
- e) eine Beschreibung der bestehenden Verfahren, mit denen sichergestellt wird, dass das Qualitätsmanagementsystem geeignet und wirksam bleibt;
- f) eine schriftliche Erklärung, dass derselbe Antrag bei keiner anderen notifizierten Stelle eingereicht worden ist.

3.2. Das Qualitätssicherungssystem wird von der notifizierten Stelle bewertet, um festzustellen, ob es die in Artikel 17 genannten Anforderungen erfüllt.

Die Entscheidung wird dem Anbieter oder dessen Bevollmächtigten mitgeteilt.

Die Mitteilung enthält die Ergebnisse der Bewertung des Qualitätsmanagementsystems und die begründete Bewertungsentscheidung.

3.3. Das genehmigte Qualitätsmanagementsystem wird vom Anbieter weiter angewandt und gepflegt, damit es stets sachgemäß und effizient funktioniert.

- 3.4. Der Anbieter unterrichtet die notifizierte Stelle über jede beabsichtigte Änderung des genehmigten Qualitätsmanagementsystems oder der Liste der unter dieses System fallenden KI-Systeme.

Die notifizierte Stelle prüft die vorgeschlagenen Änderungen und entscheidet, ob das geänderte Qualitätsmanagementsystem die in Nummer 3.2 genannten Anforderungen weiterhin erfüllt oder ob eine erneute Bewertung erforderlich ist.

Die notifizierte Stelle teilt dem Anbieter ihre Entscheidung mit. Die Mitteilung enthält die Ergebnisse der Prüfung der Änderungen und die begründete Bewertungsentscheidung.

4. Kontrolle der technischen Dokumentation
- 4.1. Zusätzlich zu dem in Nummer 3 genannten Antrag stellt der Anbieter bei der notifizierten Stelle seiner Wahl einen Antrag auf Bewertung der technischen Dokumentation für das KI-System, das er in Verkehr zu bringen oder in Betrieb zu nehmen beabsichtigt und das unter das in Nummer 3 genannte Qualitätsmanagementsystem fällt.
- 4.2. Der Antrag enthält:
- a) den Namen und die Anschrift des Anbieters,
 - b) eine schriftliche Erklärung, dass derselbe Antrag bei keiner anderen notifizierten Stelle eingereicht worden ist,
 - c) die in Anhang IV genannte technische Dokumentation.
- 4.3. Die technische Dokumentation wird von der notifizierten Stelle geprüft. Dazu erhält die notifizierte Stelle uneingeschränkten Zugang zu den vom Anbieter verwendeten Trainings- und Testdatensätzen, auch über Anwendungsprogrammierschnittstellen (API) oder sonstige für den Fernzugriff geeignete Mittel und Instrumente.
- 4.4. Bei der Prüfung der technischen Dokumentation kann die notifizierte Stelle vom Anbieter weitere Nachweise verlangen oder weitere Tests durchführen, um eine ordnungsgemäße Bewertung der Konformität des KI-Systems mit den Anforderungen in Titel III Kapitel 2 zu ermöglichen. Ist die notifizierte Stelle mit den vom Anbieter durchgeführten Tests nicht zufrieden, so führt sie gegebenenfalls unmittelbar selbst angemessene Tests durch.
- 4.5. Sofern dies für die Bewertung der Konformität des Hochrisiko-KI-Systems mit den in Titel III Kapitel 2 festgelegten Anforderungen notwendig ist, und nachdem alle anderen sinnvollen Möglichkeiten der Überprüfung der Konformität ausgeschöpft sind oder sich als unzureichend erwiesen haben, wird der notifizierten Stelle auf deren begründetes Verlangen Zugang zu den Trainingsmodelln und trainierten Modellen des KI-Systems, einschließlich seiner relevanten Parameter, gewährt. Ein solcher Zugang unterliegt den bestehenden EU-Rechtsvorschriften zum Schutz von geistigem Eigentum und Geschäftsgeheimnissen. Sie treffen technische und organisatorische Maßnahmen, um den Schutz des geistigen Eigentums und der Betriebsgeheimnisse zu wahren.

- 4.6. Die Entscheidung wird dem Anbieter oder dessen Bevollmächtigten mitgeteilt. Die Mitteilung enthält die Ergebnisse der Bewertung der technischen Dokumentation und die begründete Bewertungsentscheidung.

Erfüllt das KI-System die Anforderungen in Titel III Kapitel 2, so stellt die notifizierte Stelle eine EU-Bescheinigung über die Bewertung der technischen Dokumentation aus. Diese Bescheinigung enthält den Namen und die Anschrift des Anbieters, die Ergebnisse der Prüfung, etwaige Bedingungen für ihre Gültigkeit und die für die Identifizierung des KI-Systems notwendigen Daten.

Die Bescheinigung und ihre Anhänge enthalten alle zweckdienlichen Angaben für die Beurteilung der Konformität des KI-Systems und gegebenenfalls für die Kontrolle des KI-Systems während seiner Verwendung.

Entspricht das KI-System nicht den Anforderungen in Titel III Kapitel 2, so verweigert die notifizierte Stelle die Ausstellung einer EU-Bescheinigung über die Bewertung der technischen Dokumentation und unterrichtet den Antragsteller darüber, wobei sie ihre Weigerung ausführlich begründet.

Erfüllt das KI-System nicht die Anforderung in Bezug auf seine verwendeten Trainingsdaten, so muss das KI-System vor der Beantragung einer neuen Konformitätsbewertung erneut trainiert werden. In diesem Fall enthält die begründete Bewertungsentscheidung der notifizierten Stelle, mit der die Ausstellung der EU-Bescheinigung über die Bewertung der technischen Dokumentation verweigert wird, besondere Erläuterungen zu den zum Trainieren des KI-Systems verwendeten Qualitätsdaten und insbesondere zu den Gründen für die Nichtkonformität.

- 4.7. Jede Änderung des KI-Systems, die sich auf die Konformität des KI-Systems mit den Anforderungen oder auf seine Zweckbestimmung auswirken könnte, bedarf der Genehmigung der notifizierten Stelle, die die EU-Bescheinigung über die Bewertung der technischen Dokumentation ausgestellt hat. Der Anbieter unterrichtet die notifizierte Stelle über seine Absicht, die oben genannten Änderungen vorzunehmen, oder wenn er auf andere Weise Kenntnis vom Eintreten solcher Änderungen erhält. Die notifizierte Stelle bewertet die beabsichtigten Änderungen und entscheidet, ob diese Änderungen eine neue Konformitätsbewertung gemäß Artikel 43 Absatz 4 erforderlich machen oder ob ein Nachtrag zu der EU-Bescheinigung über die Bewertung der technischen Dokumentation ausgestellt werden könnte. In letzterem Fall bewertet die notifizierte Stelle die beabsichtigten Änderungen, teilt dem Anbieter ihre Entscheidung mit und stellt ihm, sofern die Änderungen genehmigt wurden, einen Nachtrag zu der EU-Bescheinigung über die Bewertung der technischen Dokumentation aus.

5. Überwachung des genehmigten Qualitätsmanagementsystems

- 5.1. Mit der in Nummer 3 genannten Überwachung durch die notifizierte Stelle soll sichergestellt werden, dass der Anbieter die Anforderungen und Bedingungen des genehmigten Qualitätsmanagementsystems ordnungsgemäß einhält.
- 5.2. Zu Bewertungszwecken gewährt der Anbieter der notifizierten Stelle Zugang zu den Räumlichkeiten, in denen die Konzeption, die Entwicklung und das Testen der KI-Systeme stattfindet. Außerdem übermittelt der Anbieter der notifizierten Stelle alle erforderlichen Informationen.
- 5.3. Die notifizierte Stelle führt regelmäßig Audits durch, um sicherzustellen, dass der Anbieter das Qualitätsmanagementsystem pflegt und anwendet, und übermittelt ihm einen entsprechenden Prüfbericht. Im Rahmen dieser Audits kann die notifizierte Stelle die KI-Systeme, für die eine EU-Bescheinigung über die Bewertung der technischen Dokumentation ausgestellt wurde, zusätzlichen Tests unterziehen.

ANHANG VIII**BEI DER REGISTRIERUNG DES HOCHRISIKO-KI-SYSTEMS GEMÄß ARTIKEL 51
BEREITZUSTELLENDEN INFORMATIONEN**

Abschnitt A - Für Hochrisiko-KI-Systeme, die gemäß Artikel 51 Absatz 1 zu registrieren sind, werden folgende Informationen bereitgestellt und danach auf dem neuesten Stand gehalten:

1. Name, Anschrift und Kontaktdaten des Anbieters;
2. bei Vorlage von Informationen durch eine andere Person im Namen des Anbieters: Name, Anschrift und Kontaktdaten dieser Person;
3. Name, Anschrift und Kontaktdaten des Bevollmächtigten, falls zutreffend;
4. Handelsname des KI-Systems und etwaige zusätzliche eindeutige Angaben, die die Identifizierung und Rückverfolgbarkeit des KI-Systems ermöglichen;
- 4a. Handelsname des Basismodells und etwaige zusätzliche eindeutige Angaben, die die Identifizierung und Rückverfolgbarkeit ermöglichen;
5. Eine einfache und verständliche Beschreibung
 - a) der Zweckbestimmung des KI-Systems;
 - b) der KI-unterstützten Komponenten und Funktionen;
 - c) eine grundlegende Erklärung der Logik des KI-Systems
- 5a. Gegebenfalls die Kategorien und die Art der Daten, die wahrscheinlich oder voraussichtlich vom KI-System verarbeitet werden
6. Status des KI-Systems (in Verkehr/in Betrieb; nicht mehr in Verkehr/in Betrieb, zurückgerufen);
7. Art, Nummer und Ablaufdatum der von der notifizierten Stelle ausgestellten Bescheinigung und gegebenenfalls Name oder Kennnummer dieser notifizierten Stelle;
8. gegebenenfalls eine gescannte Kopie der in Nummer 7 genannten Bescheinigung;
9. Mitgliedstaaten, in denen das KI-System in der Union in Verkehr gebracht, in Betrieb genommen oder bereitgestellt wird/wurde;
10. eine Kopie der in Artikel 48 genannten EU-Konformitätserklärung;

12. URL-Adresse für zusätzliche Informationen (fakultativ).

Abschnitt B - Für Hochrisiko-KI-Systeme, die gemäß Artikel 51 Absatz 1a und 1b zu registrieren sind, werden folgende Informationen bereitgestellt und danach auf dem neuesten Stand gehalten:

1. Name, Anschrift und Kontaktdaten des Betreibers;
2. Name, Anschrift und Kontaktdaten der Person, die im Namen des Betreibers Informationen übermittelt;
3. Handelsname des Hochrisiko-KI-Systems und etwaige zusätzliche eindeutige Angaben, die die Identifizierung und Rückverfolgbarkeit des verwendeten KI-Systems ermöglichen;
4.
 - a) Eine einfache und verständliche Beschreibung der bestimmungsgemäßen Verwendung des KI-Systems, einschließlich der spezifischen Ergebnisse, die durch die Nutzung des Systems angestrebt werden, sowie des geographischen und zeitlichen Anwendungsbereichs;
 - b) gegebenenfalls die Kategorien und die Art der Daten, die vom KI-System verarbeitet werden sollen;
 - c) Regelung für menschliche Aufsicht und Verwaltung;
 - d) gegebenenfalls die Stellen oder natürlichen Personen, die für die von einem KI-System getroffenen oder unterstützten Entscheidungen verantwortlich sind;
5. eine Zusammenfassung der Ergebnisse der Folgenabschätzung im Hinblick auf die Grundrechte, die gemäß Artikel 29a durchgeführt wurde;
6. die URL des Eintrags des KI-Systems in der EU-Datenbank durch seinen Anbieter;
7. gegebenenfalls eine Zusammenfassung der gemäß Artikel 35 der Verordnung (EU) 2016/679 oder Artikel 27 der Richtlinie (EU) 2016/680 durchgeführten Folgenabschätzung im Hinblick auf den Datenschutz, wie in Artikel 29 Absatz 6 dieser Verordnung festgehalten.

Abschnitt C - Für Für Basismodelle, die gemäß Artikel 28b Buchstabe e zu registrieren sind, werden folgende Informationen bereitgestellt und danach auf dem neuesten Stand gehalten:

1. Name, Anschrift und Kontaktdaten des Anbieters;
2. bei Vorlage von Informationen durch eine andere Person im Namen des Anbieters: Name, Anschrift und Kontaktdaten dieser Person;
3. Name, Anschrift und Kontaktdaten des Bevollmächtigten, falls zutreffend;
4. Handelsname und etwaige zusätzliche eindeutige Angaben, die die Identifizierung des Basismodells ermöglichen;
5. Beschreibung der Datenquelle, die bei der Entwicklung des BAismodells verwendet wurden;
6. Beschreibung der Fähigkeiten und Leistungsgrenzen des Baismodells, einschließlich der vernünftigerweise vorhersehbaren Risiken und der ergriffenen Maßnahmen zu ihrer Minderung sowie der nicht geminderten Restrisiken mit einer Erklärung, warum sie nicht gemindert werden können;
7. Beschreibung der vom Basismodell verwendeten Trainingsressourcen, einschließlich der erforderlichen Rechenleistung, der Trainingszeit und anderer einschlägiger Angaben im Zusammenhang mit der Größe und der Leistung des Modells 8. Beschreibung der Leistung des Modells, einschließlich bei öffentlichen oder branchenspezifischen Benchmarks nach dem neuesten Stand der Technik;
8. Beschreibung der Ergebnisse einschlägiger interner und externer Erprobungen sowie der Optimierung des Modells;
- ~~9.~~ Mitgliedsstaaten, in denen das Basismodell in der Union in Verkehr gebracht, in Betrieb genommen oder bereitgestellt wird/wurde;
10. URL-Adresse für zusätzliche Informationen (fakultati

ANHANG IX

RECHTSVORSCHRIFTEN DER UNION ÜBER IT-GROßSYSTEME IM RAUM DER FREIHEIT, DER SICHERHEIT UND DES RECHTS

1. Schengener Informationssystem
 - a) Verordnung (EU) 2018/1860 des Europäischen Parlaments und des Rates vom 28. November 2018 über die Nutzung des Schengener Informationssystems für die Rückkehr illegal aufhältiger Drittstaatsangehöriger (ABl. L 312 vom 7.12.2018, S. 1);
 - b) Verordnung (EU) 2018/1861 des Europäischen Parlaments und des Rates vom 28. November 2018 über die Einrichtung, den Betrieb und die Nutzung des Schengener Informationssystems (SIS) im Bereich der Grenzkontrollen, zur Änderung des Übereinkommens zur Durchführung des Übereinkommens von Schengen und zur Änderung und Aufhebung der Verordnung (EG) Nr. 1987/2006 (ABl. L 312 vom 7.12.2018, S. 14);
 - c) Verordnung (EU) 2018/1862 des Europäischen Parlaments und des Rates vom 28. November 2018 über die Einrichtung, den Betrieb und die Nutzung des Schengener Informationssystems (SIS) im Bereich der polizeilichen Zusammenarbeit und der justiziellen Zusammenarbeit in Strafsachen, zur Änderung und Aufhebung des Beschlusses 2007/533/JI des Rates und zur Aufhebung der Verordnung (EG) Nr. 1986/2006 des Europäischen Parlaments und des Rates und des Beschlusses 2010/261/EU der Kommission (ABl. L 312 vom 7.12.2018, S. 56).
2. Visa-Informationssystem
 - a) Vorschlag für eine VERORDNUNG DES EUROPÄISCHEN PARLAMENTS UND DES RATES zur Änderung der Verordnung (EG) Nr. 767/2008, der Verordnung (EG) Nr. 810/2009, der Verordnung (EU) 2017/2226, der Verordnung (EU) 2016/399, der Verordnung (EU) 2018/XX [Interoperabilitäts-Verordnung] und der Entscheidung 2004/512/EG sowie zur Aufhebung des Beschlusses 2008/633/JI des Rates, COM(2018) 302 final; zu aktualisieren, sobald die Verordnung von den beiden gesetzgebenden Organen erlassen wurde (April/Mai 2021).
3. Eurodac
 - a) Geänderter Vorschlag für eine VERORDNUNG DES EUROPÄISCHEN PARLAMENTS UND DES RATES über die Einrichtung von Eurodac für den Abgleich biometrischer Daten zum Zwecke der effektiven Anwendung der Verordnung (EU) XXX/XXX [Verordnung über Asyl- und Migrationsmanagement] und der Verordnung (EU) XXX/XXX [Neuansiedlungsverordnung], für die Feststellung der Identität illegal aufhältiger Drittstaatsangehöriger oder Staatenloser und über der Gefahrenabwehr und Strafverfolgung dienende Anträge der Gefahrenabwehr- und Strafverfolgungsbehörden

der Mitgliedstaaten und Europol auf den Abgleich mit Eurodac-Daten sowie zur Änderung der Verordnungen (EU) 2018/1240 und (EU) 2019/818, COM(2020) 614 final.

4. Einreise-/Ausreisensystem

- a) Verordnung (EU) 2017/2226 des Europäischen Parlaments und des Rates vom 30. November 2017 über ein Einreise-/Ausreisensystem (EES) zur Erfassung der Ein- und Ausreisedaten sowie der Einreiseverweigerungsdaten von Drittstaatsangehörigen an den Außengrenzen der Mitgliedstaaten und zur Festlegung der Bedingungen für den Zugang zum EES zu Gefahrenabwehr- und Strafverfolgungszwecken und zur Änderung des Übereinkommens von Schengen sowie der Verordnungen (EG) Nr. 767/2008 und (EU) Nr. 1077/2011 (ABl. L 327 vom 9.12.2017, S. 20).

5. Europäisches Reiseinformations- und -genehmigungssystem

- a) Verordnung (EU) 2018/1240 des Europäischen Parlaments und des Rates vom 12. September 2018 über die Einrichtung eines Europäischen Reiseinformations- und -genehmigungssystems (ETIAS) und zur Änderung der Verordnungen (EU) Nr. 1077/2011, (EU) Nr. 515/2014, (EU) 2016/399, (EU) 2016/1624 und (EU) 2017/2226 (ABl. L 236 vom 19.9.2018, S. 1);
- b) Verordnung (EU) 2018/1241 des Europäischen Parlaments und des Rates vom 12. September 2018 zur Änderung der Verordnung (EU) 2016/794 für die Zwecke der Einrichtung eines Europäischen Reiseinformations- und -genehmigungssystems (ETIAS) (ABl. L 236 vom 19.9.2018, S. 72).

6. Europäisches Strafregisterinformationssystem über Drittstaatsangehörige und Staatenlose

- a) Verordnung (EU) 2019/816 des Europäischen Parlaments und des Rates vom 17. April 2019 zur Einrichtung eines zentralisierten Systems für die Ermittlung der Mitgliedstaaten, in denen Informationen zu Verurteilungen von Drittstaatsangehörigen und Staatenlosen (ECRIS-TCN) vorliegen, zur Ergänzung des Europäischen Strafregisterinformationssystems und zur Änderung der Verordnung (EU) 2018/1726 (ABl. L 135 vom 22.5.2019, S. 1).

7. Interoperabilität

- a) Verordnung (EU) 2019/817 des Europäischen Parlaments und des Rates vom 20. Mai 2019 zur Errichtung eines Rahmens für die Interoperabilität zwischen EU-Informationssystemen in den Bereichen Grenzen und Visa und zur Änderung der Verordnungen (EG) Nr. 767/2008, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1726 und (EU) 2018/1861 des Europäischen Parlaments und des Rates, der Entscheidung 2004/512/EG des Rates und des Beschlusses 2008/633/JI des Rates (ABl. L 135 vom 22.5.2019, S. 27);

- b) Verordnung (EU) 2019/818 des Europäischen Parlaments und des Rates vom 20. Mai 2019 zur Errichtung eines Rahmens für die Interoperabilität zwischen EU-Informationssystemen (polizeiliche und justizielle Zusammenarbeit, Asyl und Migration) und zur Änderung der Verordnungen (EU) 2018/1726, (EU) 2018/1862 und (EU) 2019/816 (ABl. L 135 vom 22.5.2019, S. 85).

Ihre Ansprechpartner:innen



Detlef Klett
Technology, Media &
Telecoms
Partner
+49 211 8387-170
d.klett@taylorwessing.com



Mareike Gehrman
Technology, Media &
Telecoms
Partnerin
+49 211 8387-162
m.gehrman@taylorwessing.com



Fritz-Ulli Pieper
Technology, Media &
Telecoms
Salary Partner
+49 211 8387-240
f.pieper@taylorwessing.com



Dr. Benedikt Kohn, CIPP/E
Technology, Media &
Telecoms
Associate
+49 211 8387-256
b.kohn@taylorwessing.com

1100+ lawyers
300+ partners
29 offices
17 jurisdictions

Austria	Klagenfurt Vienna
Belgium	Brussels
China	Beijing Hong Kong Shanghai
Czech Republic	Brno Prague
France	Paris
Germany	Berlin Düsseldorf Frankfurt Hamburg Munich
Hungary	Budapest
Netherlands	Amsterdam Eindhoven
Poland	Warsaw
Republic of Ireland	Dublin
Slovakia	Bratislava
South Korea	Seoul*
UAE	Dubai
Ukraine	Kyiv
United Kingdom	Cambridge Liverpool London London TechFocus
USA	New York Silicon Valley

* In association with DR & AJU LLC

© Taylor Wessing 2023

This publication is not intended to constitute legal advice. Taylor Wessing entities operate under one brand but are legally distinct, either being or affiliated to a member of Taylor Wessing Verein. Taylor Wessing Verein does not itself provide legal or other services. Further information can be found on our regulatory page at:

[taylorwessing.com](https://www.taylorwessing.com)

TaylorWessing