Rat der
Europäischen Union

Brüssel, den 25. November 2022
(OR. en)

14954/22

Interinstitutionelles Dossier:
2021/0106(COD)

LIMITE

TELECOM 472
JAI 1494
COPEN 396
CYBER 374
DATAPROTECT 320
EJUSTICE 89
COSI 293
IXIM 267
ENFOPOL 569
RELEX 1556
MI 843
COMPET 918
CODEC 1773

VERMERK

Absender:	Ausschuss der Ständigen Vertreter (1. Teil)
Empfänger:	Rat
Nr. Vordok.:	14336/22
Nr. Komm.dok.:	8115/21
Betr.:	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 – Allgemeine Ausrichtung

I. EINLEITUNG

1. Die Kommission hat den Vorschlag für eine Verordnung zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz (**Gesetz über künstliche Intelligenz**) am 21. April 2021 angenommen.

2. Die Ziele des Kommissionsvorschlags bestehen in der Gewährleistung, dass die auf dem Unionsmarkt in Verkehr gebrachten und verwendeten KI-Systeme sicher sind und das geltende Recht in Bezug auf die bestehenden Grundrechte und die Werte der Union wahren, der Gewährleistung der Rechtssicherheit im Hinblick auf die Förderung von Investitionen in KI und innovativer KI, der Stärkung der Governance und der wirksamen Durchsetzung des geltenden Rechts in Bezug auf Grundrechte und Sicherheit und der Erleichterung der Entwicklung eines Binnenmarkts für rechtskonforme, sichere und vertrauenswürdige KI-Anwendungen bei gleichzeitiger Verhinderung einer Marktfragmentierung.

II. ARBEIT IN DEN ANDEREN ORGANEN

3. Im Europäischen Parlament werden die Beratungen vom Ausschuss für Binnenmarkt und Verbraucherschutz (IMCO; Berichterstatter: Brando Benifei, S&D, Italien) und dem Ausschuss für bürgerliche Freiheiten, Justiz und Inneres (LIBE; Berichterstatter: Dragos Tudorache, Renew, Rumänien) in einem Verfahren mit gemeinsamen Ausschusssitzungen geführt. Der Rechtsausschuss (JURI), der Ausschuss für Industrie, Forschung und Energie (ITRE) und der Ausschuss für Kultur und Bildung (CULT) begleiten die legislative Arbeit und verfügen über gemeinsame und/oder ausschließliche Zuständigkeiten. Die beiden Berichterstatter haben den Entwurf ihres Berichts im April 2022 vorgelegt und die Abstimmung über den gemeinsamen Bericht von IMCO und LIBE ist für das erste Quartal 2023 geplant.

4. Der Europäische Wirtschafts- und Sozialausschuss hat seine Stellungnahme zu dem Vorschlag am 22. September 2021 abgegeben, während die Stellungnahme des Europäischen Ausschusses der Regionen am 2. Dezember 2021 folgte.

5. Am 18. Juni 2021 haben der Europäische Datenschutzausschuss (EDSA) und der Europäische Datenschutzbeauftragte (EDSB) eine gemeinsame Stellungnahme zu dem Vorschlag abgegeben.

6. Die Europäische Zentralbank (EZB) hat ihre Stellungnahme am 29. Dezember 2021 abgegeben und sie der Gruppe „Telekommunikation und Informationsgesellschaft“ (im Folgenden „Gruppe TELECOM“) am 10. Februar 2022 vorgelegt.

III. STAND DER BERATUNGEN IM RAT

1. Im Rat wurde der Vorschlag von der Gruppe TELECOM geprüft. Die Gruppe TELECOM hat unter portugiesischem Vorsitz mit der Prüfung des Vorschlags begonnen und zwischen April und Juni 2021 mehrere Sitzungen und Workshops abgehalten. Die Arbeiten zu dem Vorschlag wurden unter slowenischem Vorsitz fortgesetzt, der einen ersten, teilweisen Kompromissvorschlag ausarbeitete, in dem die **Artikel 1-7 und die Anhänge I-III** behandelt werden. Zusätzlich organisierte der slowenische Vorsitz eine halbtägige informelle Ratstagung der Ministerinnen und Minister für Telekommunikation, die ausschließlich dem Vorschlag für ein KI-Gesetz gewidmet war und auf der die Ministerinnen und Minister ihre Unterstützung für den horizontalen und menschenzentrierten Ansatz bei der Regulierung von KI bekräftigten. Der französische Vorsitz setzte den Prüfungsprozess fort und am Ende seines Mandats überarbeitete er die verbleibenden Passagen des Texts (die **Artikel 8-85 und die Anhänge IV-IX**) und stellte am 17. Juni 2022 den vollständigen ersten konsolidierten Kompromissvorschlag des KI-Gesetzes vor.

2. Der tschechische Vorsitz führte am 5. Juli 2022 eine Orientierungsaussprache in der Gruppe TELECOM auf der Grundlage eines Dokuments über politische Optionen, deren Ergebnisse genutzt wurden, um **den zweiten Kompromisstext** auszuarbeiten. Auf der Grundlage der Reaktionen der Delegationen auf diesen Kompromiss bereitete der tschechische Vorsitz **den dritten Kompromisstext** vor, der in der Sitzung der Gruppe TELECOM vom 22. und 29. September 2022 vorgestellt und erörtert wurde. Nach diesen Beratungen wurden die Delegationen ersucht, weitere schriftliche Bemerkungen vorzubringen, die der tschechische Vorsitz nutzte, um **den vierten Kompromissvorschlag** auszuarbeiten. Auf der Grundlage der Beratungen zum vierten Kompromissvorschlag in den Sitzungen der Gruppe TELECOM vom 25. Oktober 2022 und 8. November 2022 sowie unter Berücksichtigung der endgültigen schriftlichen Bemerkungen der Mitgliedstaaten hat der tschechische Vorsitz **die endgültige Fassung des Kompromisstexts** ausgearbeitet, der in der Anlage enthalten ist. Der AStV hat den Kompromissvorschlag am 18. November geprüft und **einstimmig beschlossen, ihn dem Rat (Verkehr, Telekommunikation und Energie – Telekommunikation) ohne Änderungen im Hinblick auf eine allgemeine Ausrichtung** auf dessen Tagung am 6. Dezember 2022 **zu übermitteln**.

IV. WICHTIGSTE ELEMENTE DES KOMPROMISSVORSCHLAGS

1. Definition eines KI-Systems, verbotene KI-Praktiken, Liste der Anwendungsfälle von Hochrisiko-KI-Systemen in Anhang III und Klassifizierung von KI-Systemen als Hochrisiko-Systeme

1.1 Um sicherzustellen, dass die Definition eines KI-Systems ausreichend klare Kriterien für die Abgrenzung der KI von klassischeren Software-Systemen bietet, wird die Begriffsbestimmung in **Artikel 3 Absatz 1** im Kompromisstext auf Systeme eingegrenzt, die anhand von Konzepten des maschinellen Lernens sowie logik- und wissensgestützten Konzepten entwickelt wurden.

1.2 Im Hinblick auf die Übertragung von Befugnissen an die Kommission in Bezug auf die Aktualisierungen der Begriffsbestimmung eines AI-Systems wurden **Anhang I** und die entsprechende Befugnisübertragung, wonach die Kommission sie im Wege von delegierten Rechtsakten aktualisieren kann, gestrichen. Stattdessen wurden die neuen **Erwägungsgründe 6a und 6b** ergänzt, um klarzustellen, was unter Konzepten des maschinellen Lernens und unter logik- und wissensgestützten Konzepten zu verstehen ist. Um sicherzustellen, dass das KI-Gesetz flexibel und zukunftssicher bleibt, wurde in **Artikel 4** die Möglichkeit einer Annahme von Durchführungsrechtsakten zur weiteren Präzisierung und Aktualisierung von Techniken im Rahmen von Konzepten des maschinellen Lernens und von logik- und wissensgestützten Konzepten ergänzt.

1.3 Was verbotene Praktiken im Bereich der KI betrifft, so wird das Verbot, KI für die Bewertung des sozialen Verhaltens zu verwenden, in **Artikel 5** des Kompromisstexts auch auf private Akteure ausgeweitet. Darüber hinaus schließt die Bestimmung, mit der die Verwendung von KI-Systemen, die eine Schwäche oder Schutzbedürftigkeit einer bestimmten Gruppe von Personen ausnutzt, verboten wird, nun auch Personen ein, die aufgrund ihrer sozialen oder wirtschaftlichen Lage schutzbedürftig sind. Im Hinblick auf das Verbot der Verwendung biometrischer Echtzeit-Fernidentifizierungssysteme in öffentlich zugänglichen Räumen durch Strafverfolgungsbehörden werden im Kompromisstext die Ziele präzisiert, wenn eine solche Verwendung als zu Strafverfolgungszwecken streng notwendig erachtet wird, und zu denen den Strafverfolgungsbehörden die Verwendung solcher Systeme daher ausnahmsweise gestattet werden sollte.

1.4 Im Hinblick auf die Liste der Anwendungsfälle von Hochrisiko-KI-Systemen in **Anhang III** wurden drei davon gestrichen (Aufdeckung von Deepfakes durch die Strafverfolgungsbehörden, Kriminalanalyse, Überprüfung der Echtheit von Reisedokumenten), zwei ergänzt (kritische digitale Infrastruktur und Lebens- und Krankenversicherung) und andere genauer abgestimmt. Gleichzeitig wurde **Artikel 7 Absatz 1** geändert, um die Möglichkeit vorzusehen, dass Hochrisiko-Anwendungsfälle nicht nur im Wege von delegierten Rechtsakten in die Liste aufgenommen, sondern auch gestrichen werden können. Um sicherzustellen, dass die Grundrechte im Falle solcher Streichungen angemessen geschützt werden, wurden in **Artikel 7 Absatz 3** zusätzliche Bestimmungen ergänzt, in denen die Bedingungen präzisiert werden, die erfüllt werden müssten, bevor ein delegierter Rechtsakt erlassen werden kann.

1.5 Im Hinblick auf die Klassifizierung von KI-Systemen als Hochrisiko-Systeme enthält der Kompromissvorschlag nun eine zusätzliche horizontale Ebene über der Hochrisiko-Klassifizierung in **Anhang III**, um sicherzustellen, dass KI-Systeme, die wahrscheinlich keine schwerwiegenden Grundrechtsverletzungen oder andere bedeutende Risiken verursachen, nicht erfasst werden. Konkret enthält **Artikel 6 Absatz 3** neue Bestimmungen, nach denen die Bedeutung des Ergebnisses des AI-Systems in Bezug auf die zu treffende Maßnahme oder Entscheidung ebenfalls berücksichtigt werden sollte, wenn KI-Systeme als Hochrisiko-Systeme klassifiziert werden. Die Bedeutung des Ergebnisses eines KI-Systems würde auf der Grundlage bewertet werden, ob es in Bezug auf die zu treffende Maßnahme oder Entscheidung völlig unwesentlich ist oder nicht.

2. Anforderungen an Hochrisiko-KI-Systeme und Verantwortlichkeiten der verschiedenen Akteure in der KI-Wertschöpfungskette

2.1 Viele der in **Titel III Kapitel 2** des Vorschlags enthaltenen Anforderungen an Hochrisiko-KI-Systeme wurden präzisiert und so angepasst, dass sie technisch machbarer sind und ihre Einhaltung die Interessenträger weniger belastet, zum Beispiel in Bezug auf die Datenqualität oder auf die technische Dokumentation, die von KMU erstellt werden sollte, um nachzuweisen, dass ihre Hochrisiko-KI-Systeme den Anforderungen entsprechen.

2.2 Angesichts der Tatsache, dass KI-Systeme entlang komplexer Wertschöpfungsketten entwickelt und vertrieben werden, enthält der Kompromisstext Änderungen, mit denen die Zuweisung von Verantwortlichkeiten und Rollen klargestellt werden. So wurden zum Beispiel einige zusätzliche Bestimmungen in den **Artikeln 13 und 14** ergänzt, die eine wirksamere Zusammenarbeit zwischen Anbietern und Nutzern ermöglichen. Der Kompromisstext zielt auch darauf ab, die Beziehung zwischen den Verantwortlichkeiten im Rahmen des KI-Gesetzes und jenen, die bereits im Rahmen anderer Rechtsvorschriften bestehen, wie etwa die einschlägigen Datenschutz- oder sektoralen Rechtsvorschriften der Union, einschließlich des Sektors der Finanzdienstleistungen. Darüber hinaus werden im neuen **Artikel 23a** die Situationen genauer beschrieben, in denen andere Akteure in der Wertschöpfungskette verpflichtet sind, die Verantwortlichkeiten eines Anbieters zu übernehmen.

3. KI-System mit allgemeinem Verwendungszweck

3.1 Es wurde der neue **Titel IA** hinzugefügt, um den Situationen Rechnung zu tragen, in denen KI-Systeme für zahlreiche verschiedene Zwecke verwendet werden können (KI für allgemeine Zwecke) und in denen es aufgrund der Gegebenheiten zur Integration von KI-Technologie für allgemeine Zwecke in ein anderes System kommen kann, das möglicherweise zu einem Hochrisiko-System wird. Im Kompromisstext wird in **Artikel 4b Absatz 1** festgelegt, dass bestimmte Anforderungen für Hochrisiko-KI-Systeme auch für KI-Systeme mit allgemeinem Verwendungszweck gelten würden. Allerdings würde – anstelle einer direkten Anwendung dieser Anforderungen – in einem Durchführungsrechtsakt auf der Grundlage einer Konsultation und einer eingehenden Folgenabschätzung und unter Berücksichtigung spezifischer Merkmale dieser Systeme und der zugehörigen Wertschöpfungskette, der technischen Durchführbarkeit und der technologischen Entwicklungen präzisiert werden, wie sie im Verhältnis zu KI-Systemen mit allgemeinem Verwendungszweck angewendet werden sollten. Die Verwendung eines Durchführungsrechtsakts wird gewährleisten, dass die Mitgliedstaaten ordnungsgemäß eingebunden werden und nach wie vor das letzte Wort darüber haben, wie die Anforderungen in diesem Zusammenhang angewendet werden.

3.2 Darüber hinaus enthält der Kompromisstext in **Artikel 4b Absatz 5** auch die Möglichkeit, weitere Durchführungsrechtsakte zu erlassen, die die Modalitäten der Zusammenarbeit zwischen Anbietern von KI-Systemen mit allgemeinem Verwendungszweck und anderen Anbietern, die beabsichtigen, solche Systeme auf dem Unionsmarkt als Hochrisiko-KI-Systeme in Betrieb zu nehmen oder in Verkehr zu bringen, insbesondere im Hinblick auf die Bereitstellung von Informationen.

4. **Klarstellung des Anwendungsbereichs des vorgeschlagenen KI-Gesetzes und Bestimmungen über die Strafverfolgungsbehörden**

4.1 In **Artikel 2** wurde ein ausdrücklicher Verweis auf die Ausnahme von Zwecken der nationalen Sicherheit, der Verteidigung und des Militärs aus dem Anwendungsbereich des KI-Gesetzes aufgenommen. In ähnlicher Weise wurde klargestellt, dass das KI-Gesetz – mit Ausnahme der Transparenzpflichten – nicht für KI-Systeme und deren Ergebnisse, die für den ausschließlichen Zweck der Forschung und Entwicklung verwendet werden, und nicht für die Verpflichtungen von Personen, die KI zu nichtberuflichen Zwecken verwenden, die außerhalb des Anwendungsbereichs des KI-Gesetzes liegen, gelten sollte.

4.2 Um den spezifischen Besonderheiten der Strafverfolgungsbehörden Rechnung zu tragen, wurde eine Reihe von Änderungen an den Bestimmungen in Bezug auf die Verwendung von KI-Systemen zu Strafverfolgungszwecken vorgenommen. Insbesondere wurden einige der damit zusammenhängenden Begriffsbestimmungen in **Artikel 3** wie etwa die Begriffe „biometrisches Fernidentifizierungssystem“ und „Echtzeit-Fernidentifizierungssystem“ präzisiert, um klarzustellen, welche Situationen unter das entsprechende Verbot und den Anwendungsfall von Hochrisiko-KI-Systemen fallen würden und welche nicht. Der Kompromissvorschlag enthält auch andere Änderungen, die vorbehaltlich geeigneter Schutzvorkehrungen ein angemessenes Maß an Flexibilität bei der Verwendung von Hochrisiko-KI-Systemen durch Strafverfolgungsbehörden sicherstellen oder der Notwendigkeit Rechnung tragen sollen, die Vertraulichkeit sensibler operativer Daten in Bezug auf ihre Tätigkeiten zu wahren.

5. **Konformitätsbewertungen, Governance-Rahmen, Marktüberwachung, Durchsetzung und Sanktionen**

5.1 Um den Rechtsbefolgungsrahmen für das KI-Gesetz zu vereinfachen, enthält der Kompromisstext eine Reihe von Klarstellungen und Vereinfachungen der Bestimmungen über die Verfahren zur Konformitätsbewertung. Die Bestimmungen im Zusammenhang mit der Marktüberwachung wurden ebenfalls präzisiert und vereinfacht, um sie wirksamer und leichter umsetzbar zu gestalten, und dabei der Notwendigkeit eines diesbezüglich verhältnismäßigen Ansatzes Rechnung getragen. Darüber hinaus wurde **Artikel 41** gründlich geprüft, um den Ermessensspielraum der Kommission im Hinblick auf den Erlass von Durchführungsrechtsakten zur Festlegung gemeinsamer technischer Spezifikationen für die Anforderungen für Hochrisiko-KI-Systeme und KI-Systeme mit allgemeinem Verwendungszweck zu begrenzen.

5.2 Zudem werden in dem Kompromisstext die Bestimmungen über den Ausschuss für künstliche Intelligenz (im Folgenden „KI-Ausschuss“) erheblich geändert, um eine größere Autonomie des Ausschusses zu gewährleisten und seine Rolle in der Governance-Architektur des KI-Gesetzes zu stärken. In diesem Zusammenhang wurden die **Artikel 56 und 58** überarbeitet, um die Rolle des KI-Ausschusses dahingehend zu stärken, dass er besser in der Lage sein sollte, den Mitgliedstaaten bei der Umsetzung und Durchsetzung des KI-Gesetzes Unterstützung zu leisten. Konkret wurden die Aufgaben des KI-Ausschusses ausgeweitet und seine Zusammensetzung wurde festgelegt. Um die Beteiligung der Interessenträger in Bezug auf alle Fragen im Zusammenhang mit der Umsetzung des KI-Gesetzes sicherzustellen, auch in Bezug auf die Ausarbeitung von Durchführungs- und delegierten Rechtsakten, wurde eine neue Anforderung ergänzt, wonach der KI-Ausschuss eine ständige Untergruppe einrichtet, die als Plattform für eine große Bandbreite an Interessenträgern dient. Zwei weitere ständige Untergruppen für Marktüberwachungsbehörden und für notifizierende Behörden sollten ebenfalls eingerichtet werden, um die Kohärenz der Governance und der Durchsetzung des KI-Gesetzes in der gesamten Union zu stärken.

5.3 Um den Governance-Rahmen weiter zu verbessern, enthält der Kompromisstext die neuen **Artikel 68a und 68b**. **Artikel 68a** enthält eine Anforderung, wonach die Kommission eine oder mehrere Testeinrichtungen der Union im Bereich der künstlichen Intelligenz benennen muss, die auf Anfrage des KI-Ausschusses oder der Marktüberwachungsbehörden unabhängige technische oder wissenschaftliche Gutachten zur Verfügung stellen sollten; mit **Artikel 68b** wird eine Verpflichtung geschaffen, wonach die Kommission einen zentralen Pool unabhängiger Sachverständiger zur Unterstützung der im Rahmen des KI-Gesetzes erforderlichen Durchsetzungsmaßnahmen einrichten muss. Schließlich gibt es auch einen neuen **Artikel 58a**, in dem eine Verpflichtung festgelegt wird, wonach die Kommission Leitlinien für die Anwendung des KI-Gesetzes vorlegen muss.

5.4 Im Hinblick auf die Sanktionen für Verstöße gegen die Bestimmungen des KI-Gesetzes sieht der Kompromisstext in **Artikel 71** verhältnismäßigere Obergrenzen für die Beträge der Geldbußen für KMU und Start-up-Unternehmen vor. Darüber hinaus wurden in **Artikel 71 Absatz 6** vier weitere Kriterien für die Festlegung des Betrags von Geldbußen ergänzt, um deren Verhältnismäßigkeit insgesamt noch weiter zu sichern.

6. **Transparenz und sonstige Bestimmungen zu Gunsten der betroffenen Personen**

6.1 Der Kompromissvorschlag enthält eine Reihe von Änderungen, mit denen die Transparenz im Hinblick auf die Verwendung von Hochrisiko-KI-Systemen erhöht wird. Insbesondere wurde der **Artikel 51** überarbeitet, um darauf hinzuweisen, dass bestimmte Nutzer von Hochrisiko-KI-Systemen, bei denen es sich um Behörden, Einrichtungen oder sonstige Stellen handelt, ebenfalls verpflichtet sein werden, sich in der EU-Datenbank für in Anhang III aufgeführte Hochrisiko-KI-Systeme zu registrieren. Darüber hinaus wird in dem neu hinzugefügten **Artikel 52 Absatz 2a** der Schwerpunkt auf die Pflicht für Nutzer eines Emotionserkennungssystems gelegt, die natürlichen Personen, die von diesem System betroffen sind, darüber zu informieren.

6.2 In dem neu hinzugefügten **Artikel 63 Absatz 11** des Kompromissvorschlags wird außerdem klargestellt, dass eine natürliche oder juristische Person, die Grund zu der Annahme hat, dass es einen Verstoß gegen die Bestimmungen des KI-Gesetzes gegeben hat, Beschwerde bei der einschlägigen Marktüberwachungsbehörde einlegen und erwarten kann, dass eine solche Beschwerde entsprechend den zweckbestimmten Verfahren dieser Behörde bearbeitet wird.

7. **Maßnahmen zur Innovationsförderung**

7.1 Mit dem Ziel, einen innovationsfreundlicheren Rechtsrahmen zu schaffen, und um faktengestütztes regulatorisches Lernen zu fördern, wurden die Bestimmungen in Bezug auf Maßnahmen zur Innovationsförderung in **Artikel 53** im Kompromisstext maßgeblich geändert. Insbesondere wurde klargestellt, dass die regulatorischen KI-Reallabore, die eine kontrollierte Umgebung für die Entwicklung, Testung und Validierung innovativer KI-Systeme unter der direkten Aufsicht und Anleitung der zuständigen nationalen Behörden schaffen sollen, auch das Testen innovativer KI-Systeme unter realen Bedingungen ermöglichen sollten. Ferner wurden neue Bestimmungen in den **Artikeln 54a und 54b** aufgenommen, wonach KI-Systeme unter bestimmten Bedingungen und Schutzvorkehrungen unbeaufsichtigt unter realen Bedingungen erprobt werden können. In beiden Fällen wird im Kompromisstext erläutert, wie diese neuen Vorschriften im Verhältnis zu anderen bestehenden sektorspezifischen Rechtsvorschriften über Reallabore auszulegen sind.

7.2 Schließlich enthält der Kompromisstext – um den Verwaltungsaufwand für kleinere Unternehmen zu mindern – in **Artikel 55** eine Liste von Maßnahmen, die die Kommission zu ergreifen hat, um solche Akteure zu unterstützen, und sieht er in **Artikel 55a** einige begrenzte und klar festgelegte Ausnahmeregelungen vor.

V. FAZIT

1. Der Rat wird daher gebeten,
   - den in der Anlage wiedergegebenen Kompromisstext zu prüfen;
   - auf der Tagung des Rates (Verkehr, Telekommunikation und Energie – Telekommunikation) am 6. Dezember 2022 eine allgemeine Ausrichtung zum Vorschlag für eine Verordnung zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz (Gesetz über künstliche Intelligenz, KI-Gesetz) zu bestätigen.

ANLAGE

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

(Text von Bedeutung für den EWR)

DAS EUROPÄISCHE PARLAMENT UND DER RAT DER EUROPÄISCHEN UNION —

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

auf Vorschlag der Europäischen Kommission,

nach Zuleitung des Entwurfs des Gesetzgebungsakts an die nationalen Parlamente,

nach Stellungnahme des Europäischen Wirtschafts- und Sozialausschusses[1],

nach Stellungnahme des Ausschusses der Regionen[2],

nach Stellungnahme der Europäischen Zentralbank[3],

gemäß dem ordentlichen Gesetzgebungsverfahren,

in Erwägung nachstehender Gründe:

---

1 ABl. C […] vom […], S. […].
2 ABl. C […] vom […], S. […].
3 Verweis auf die Stellungnahme der EZB.

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

(2) Systeme der künstlichen Intelligenz (KI-Systeme) können problemlos in verschiedenen Bereichen der Wirtschaft und Gesellschaft, auch grenzüberschreitend, eingesetzt werden und in der gesamten Union verkehren. Einige Mitgliedstaaten haben bereits die Verabschiedung nationaler Vorschriften in Erwägung gezogen, damit künstliche Intelligenz sicher ist und unter Einhaltung der Grundrechte entwickelt und verwendet wird. Unterschiedliche nationale Vorschriften können zu einer Fragmentierung des Binnenmarkts führen und würden die Rechtssicherheit für Akteure, die KI-Systeme entwickeln, einführen oder verwenden, beeinträchtigen. Daher sollte in der gesamten Union ein einheitlich hohes Schutzniveau sichergestellt werden, wobei Unterschiede, die den freien Verkehr von KI-Systemen und damit zusammenhängenden Produkten und Dienstleistungen im Binnenmarkt behindern, vermieden werden sollten, indem den Akteuren einheitliche Verpflichtungen auferlegt werden und der gleiche Schutz der zwingenden Gründe des Allgemeininteresses und der Rechte von Personen im gesamten Binnenmarkt auf der Grundlage des Artikels 114 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV) gewährleistet wird. Soweit diese Verordnung konkrete Vorschriften zum Schutz von Privatpersonen im Hinblick auf die Verarbeitung personenbezogener Daten enthält, mit denen vor allem die Verwendung von KI-Systemen zur biometrischen Echtzeit-Fernidentifizierung in öffentlich zugänglichen Räumen zu Strafverfolgungszwecken eingeschränkt wird, sollte sich diese Verordnung in Bezug auf diese konkreten Vorschriften auch auf Artikel 16 AEUV stützen. Angesichts dieser konkreten Vorschriften und des Rückgriffs auf Artikel 16 AEUV ist es angezeigt, den Europäischen Datenschutzausschuss zu konsultieren.

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

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

(5) Daher ist ein Rechtsrahmen der Union mit harmonisierten Vorschriften für künstliche Intelligenz erforderlich, um die Entwicklung, Verwendung und Verbreitung künstlicher Intelligenz im Binnenmarkt zu fördern und gleichzeitig einen hohen Schutz öffentlicher Interessen wie Gesundheit und Sicherheit und den Schutz der durch das Unionsrecht anerkannten und geschützten Grundrechte zu gewährleisten. Zur Umsetzung dieses Ziels sollten Vorschriften für das Inverkehrbringen und die Inbetriebnahme bestimmter KI-Systeme festgelegt werden, um das reibungslose Funktionieren des Binnenmarkts zu gewährleisten, sodass diesen Systemen der Grundsatz des freien Waren- und Dienstleistungsverkehrs zugutekommen kann. Durch die Festlegung dieser Vorschriften und aufbauend auf der Arbeit der hochrangigen Expertengruppe für künstliche Intelligenz, die sich in den Leitlinien für eine vertrauenswürdige KI in der EU niedergeschlagen hat, unterstützt diese Verordnung das vom Europäischen Rat formulierte Ziel der Union, bei der Entwicklung einer sicheren, vertrauenswürdigen und ethisch vertretbaren künstlichen Intelligenz weltweit eine Führungsrolle einzunehmen[4], und sorgt für den vom Europäischen Parlament ausdrücklich geforderten Schutz von ethischen Grundsätzen[5].

---

4 Europäischer Rat, Außerordentliche Tagung des Europäischen Rates (1./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).

(5a) Die in dieser Verordnung festgelegten harmonisierten Vorschriften für das Inverkehrbringen, die Inbetriebnahme und die Verwendung von KI-Systemen sollten in allen Sektoren gelten und sollten im Einklang mit ihrem neuen Rechtsrahmen bestehendes Unionsrecht, das durch diese Verordnung ergänzt wird, unberührt lassen, insbesondere in den Bereichen Datenschutz, Verbraucherschutz, Grundrechte, Beschäftigung und Produktsicherheit. Daher bleiben alle Rechte und Rechtsbehelfe, die Verbrauchern und anderen Personen, auf die sich KI-Systeme negativ auswirken können, durch dieses Unionsrecht zuerkannt werden, auch in Bezug auf einen möglichen Schadenersatz gemäß der Richtlinie 85/374/EWG vom 25. Juli 1985 zur Angleichung der Rechts- und Verwaltungsvorschriften der Mitgliedstaaten über die Haftung für fehlerhafte Produkte, unberührt. Darüber hinaus zielt diese Verordnung darauf ab, die Wirksamkeit dieser bestehenden Rechte und Rechtsbehelfe zu stärken, indem bestimmte Anforderungen und Pflichten, auch in Bezug auf die Transparenz, die technische Dokumentation und das Führen von Aufzeichnungen von KI-Systemen, festgelegt werden. Ferner sollten die in dieser Verordnung festgelegten Pflichten der verschiedenen Akteure, die an der KI-Wertschöpfungskette beteiligt sind, unbeschadet der nationalen Rechtsvorschriften im Einklang mit dem Unionsrecht angewendet werden, wodurch die Verwendung bestimmter KI-Systeme begrenzt wird, wenn diese Rechtsvorschriften nicht in den Anwendungsbereich dieser Verordnung fallen oder mit ihnen andere legitime Ziele des öffentlichen Interesses verfolgt werden als in dieser Verordnung. So sollten etwa die nationalen arbeitsrechtlichen Vorschriften und die Rechtsvorschriften zum Schutz Minderjähriger (d. h. Personen unter 18 Jahren) unter Berücksichtigung der Allgemeinen Bemerkung Nr. 25 (2021) der Vereinten Nationen über die Rechte der Kinder von dieser Verordnung unberührt bleiben, sofern sie nicht spezifisch KI-Systeme betreffen und mit ihnen andere legitime Ziele des öffentlichen Interesses verfolgt werden.

(6) Der Begriff „KI-System“ sollte klar definiert werden, um Rechtssicherheit zu gewährleisten und gleichzeitig genügend Flexibilität zu bieten, um künftigen technologischen Entwicklungen Rechnung zu tragen. Die Begriffsbestimmung sollte auf den wesentlichen funktionalen Merkmalen der künstlichen Intelligenz wie ihre Lern-, Schlussfolgerungs- oder Modellierungsfähigkeiten beruhen und diese von einfacheren Softwaresystemen und Programmierungsansätzen abgrenzen. Insbesondere für die Zwecke dieser Verordnung sollten KI-Systeme in der Lage sein, auf der Grundlage maschineller und/oder vom Menschen erzeugter Daten und Eingaben durch maschinelles Lernen und/oder logik- und wissensgestützte Konzepte abzuleiten, wie eine Reihe von Endzielen, die vom Menschen festgelegt wurden, erreicht wird, und Ergebnisse wie Inhalte für generative KI-Systeme (z. B. Text, Video oder Bilder), Vorhersagen, Empfehlungen oder Entscheidungen hervorzubringen, die das Umfeld beeinflussen, mit dem sie interagieren, sei es physisch oder digital. Ein System, das ausschließlich von natürlichen Personen definierte Regeln anwendet, um automatisch Operationen auszuführen, sollte nicht als KI-System gelten. KI-Systeme können so konzipiert sein, dass sie mit verschiedenen Graden der Autonomie arbeiten und eigenständig oder als Bestandteil eines Produkts verwendet werden können, unabhängig davon, ob das System physisch in das Produkt integriert ist (eingebettet) oder der Funktion des Produkts dient, ohne darin integriert zu sein (nicht eingebettet). Das Konzept der Autonomie eines KI-Systems steht im Zusammenhang mit dem Grad, mit dem ein solches System ohne menschliches Zutun funktioniert.

(6a) Bei Konzepten des maschinellen Lernens liegt der Schwerpunkt auf der Entwicklung von Systemen, die lernen und anhand von Daten ableiten können, wie ein Anwendungsproblem gelöst wird, ohne dass sie ausdrücklich mit einer Anleitung der einzelnen Schritte von der Eingabe bis zu den Ergebnissen dafür programmiert wurden. Der Begriff „Lernen“ bezeichnet den Rechenvorgang, bei dem anhand von Daten die Parameter eines Modells optimiert werden, das als mathematische Konstruktion auf der Grundlage von Eingabedaten Ergebnisse hervorbringt. Zu den Problemen, die durch maschinelles Lernen bewältigt werden, gehören in der Regel Aufgaben, für die andere Ansätze erfolglos waren, entweder aufgrund einer unangemessenen Formalisierung des Problems oder aufgrund der Tatsache, dass die Lösung des Problems mithilfe von Konzepten, die kein maschinelles Lernen umfassen, nicht möglich ist. Die Konzepte des maschinellen Lernens umfassen etwa überwachtes, unüberwachtes und bestärkendes Lernen, wobei verschiedene Methoden eingesetzt werden, einschließlich Deep Learning mit neuronalen Netzwerken, statistische Lernverfahren und statistische Inferenz (etwa auch logistische Regressionen oder Bayes'sche Schätzungen) sowie Such- und Optimierungsmethoden.

(6b) Bei logik- und wissensgestützten Konzepten liegt der Schwerpunkt auf der Entwicklung von Systemen mit der Fähigkeit, in Bezug auf eine Wissensbasis Schlussfolgerungen zu ziehen, um ein Anwendungsproblem zu lösen. Solche Systeme umfassen in der Regel eine Wissensbasis und eine Inferenzmaschine, die Ergebnisse hervorbringt, indem Schlussfolgerungen auf der Grundlage der Wissensbasis gezogen werden. In der Wissensbasis, die normalerweise von menschlichen Experten kodiert wird, werden für das Anwendungsproblem relevante Entitäten und logische Zusammenhänge dargestellt, indem auf der Grundlage von Regeln, Ontologien oder Wissensgraphen Formalisierungen vorgenommen werden. Die Inferenzmaschine wendet die Wissensbasis an und extrahiert neue Informationen durch Operationen wie Sortierung, Suche, Abgleichung und Verkettung. Logik- und wissensgestützte Konzepte umfassen beispielsweise Wissensrepräsentationen, induktive (logische) Programmierung, Wissensbasen, Inferenz- und Deduktionsmaschinen, (symbolische) Schlussfolgerungs- und Expertensysteme sowie Such- und Optimierungsmethoden.

(6c) Zur Gewährleistung einheitlicher Bedingungen für die Umsetzung dieser Verordnung in Bezug auf die Konzepte des maschinellen Lernens und die logik- und wissensgestützten Konzepte und zur Berücksichtigung von Marktentwicklungen und technischen Entwicklungen, sollten der Kommission Durchführungsbefugnisse übertragen werden.

(6d) Der in dieser Verordnung verwendete Begriff „Nutzer“ sollte als eine natürliche oder juristische Person, einschließlich Behörden, Einrichtungen oder sonstige Stellen, die ein KI-System verwenden und unter deren Verantwortung das System verwendet wird, verstanden werden. Je nach Art des KI-Systems kann sich dessen Verwendung auf andere Personen als den Nutzer auswirken.

(7) Der in dieser Verordnung verwendete Begriff „biometrische Daten“ sollte im Einklang mit dem Begriff „biometrische Daten“ im Sinne von Artikel 4 Nummer 14 der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates[6], Artikel 3 Nummer 18 der Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates[7] und Artikel 3 Nummer 13 der Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates[8] ausgelegt werden.

---

6 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).

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

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

(8) Der in dieser Verordnung verwendete Begriff „biometrisches Fernidentifizierungssystem“ sollte funktional definiert werden als KI-System, das dem Zweck dient, natürliche Personen in der Regel aus der Ferne und ohne ihre aktive Einbeziehung durch Abgleich der biometrischen Daten einer Person mit den in einem Referenzdatenregister gespeicherten biometrischen Daten zu identifizieren, und unabhängig davon, welche Technik, Verfahren oder Arten biometrischer Daten dazu verwendet werden. Diese biometrischen Fernidentifizierungssysteme werden in der Regel zur zeitgleichen Erkennung (durch Scannen) mehrerer Personen oder ihrer Verhaltensweisen verwendet, um die Identifizierung einer Reihe von Personen ohne ihre aktive Einbeziehung erheblich zu erleichtern. Von dieser Definition ausgeschlossen sind Verifizierungs-/Authentifizierungssysteme, deren alleiniger Zweck darin besteht, zu bestätigen, dass eine bestimmte natürliche Person die Person ist, für die sie sich ausgibt, sowie Systeme, die zur Bestätigung der Identität einer natürlichen Person zu dem alleinigen Zweck, ihr Zugang zu einem Dienst, einem Gerät oder einer Räumlichkeit zu gewähren, verwendet werden. Diese Ausnahme wird damit begründet, dass diese Systeme im Vergleich zu biometrischen Fernidentifizierungssystemen, die zur Verarbeitung biometrischer Daten einer großen Anzahl von Personen verwendet werden können, geringfügige Auswirkungen auf die Grundrechte der natürlichen Personen haben dürften. 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.

(9) Für die Zwecke dieser Verordnung sollte der Begriff „öffentlich zugänglicher Raum“ so verstanden werden, dass er sich auf einen einer unbestimmten Anzahl natürlicher Personen zugänglichen physischen Ort bezieht, unabhängig davon, ob er sich in privatem oder öffentlichem Eigentum befindet, und unabhängig von den Tätigkeiten, für die der Ort verwendet werden kann; dazu zählen Bereiche wie Gewerbe (etwa Geschäfte, Restaurants, Cafés), Dienstleistungen (etwa Banken, berufliche Tätigkeiten, Gastgewerbe), Sport (etwa Schwimmbäder, Fitnessstudios, Stadien), Verkehr (etwa Bus- und U-Bahn-Haltestellen, Bahnhöfe, Flughäfen, Transportmittel), Unterhaltung (etwa Kinos, Theater, Museen, Konzert- und Konferenzsäle) Freizeit oder sonstiges (etwa öffentliche Straßen und Plätze, Parks, Wälder, Spielplätze). Ein Ort sollte auch als öffentlich zugänglich eingestuft werden, wenn der Zugang, unabhängig von möglichen Kapazitäts- oder Sicherheitsbeschränkungen, vorher bestimmten Bedingungen unterliegt, die von einer unbestimmten Anzahl von Personen erfüllt werden können, etwa durch den Kauf eines Fahrscheins, die vorherige Registrierung oder die Erfüllung eines Mindestalters. Dahingegen sollte ein Ort nicht als öffentlich zugänglich gelten, wenn der Zugang auf eine Anzahl natürlicher Personen beschränkt ist, die entweder im Unionsrecht oder im nationalen Recht, das direkt mit der öffentlichen Sicherheit zusammenhängt, oder im Rahmen einer eindeutigen Willenserklärung der Person, die die entsprechende Autorität über den Ort ausübt, bestimmt und definiert wird. Die tatsächliche Zugangsmöglichkeit alleine (etwa eine unversperrte Tür, ein offenes Zauntor) bedeutet nicht, dass der Ort öffentlich zugänglich ist, wenn aufgrund von Hinweisen oder Umständen das Gegenteil nahegelegt wird (etwa Schilder, die den Zugang verbieten oder einschränken). Unternehmens- und Fabrikgelände sowie Büros und Arbeitsplätze, die nur für die betreffenden Mitarbeiter und Dienstleister zugänglich sein sollen, sind Orte, die nicht öffentlich zugänglich sind. Justizvollzugsanstalten oder Grenzkontrollbereiche sollten nicht zu den öffentlich zugänglichen Orten zählen. Einige andere Gebiete können sowohl öffentlich zugängliche als auch nicht öffentlich zugängliche Bereiche umfassen, etwa Flughäfen oder die Gänge eines privaten Wohngebäudes, deren Zugang erforderlich ist, um zu einer Arztpraxis zu gelangen. Auch Online-Räume werden nicht erfasst, da es sich nicht um physische Räume handelt. Ob ein bestimmter Raum öffentlich zugänglich ist, sollte jedoch von Fall zu Fall unter Berücksichtigung der Besonderheiten der jeweiligen individuellen Situation entschieden werden.

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

(11) Angesichts ihres digitalen Charakters sollten bestimmte KI-Systeme in den Anwendungsbereich dieser Verordnung fallen, selbst wenn sie in der Union weder in Verkehr gebracht noch in Betrieb genommen oder verwendet werden. Dies ist beispielsweise der Fall, wenn ein in der Union ansässiger oder niedergelassener Akteur bestimmte Dienstleistungen an einen außerhalb der Union ansässigen oder niedergelassenen Akteur im Zusammenhang mit einer Tätigkeit vergibt, die von einem KI-System ausgeübt werden soll, das als hochriskant einzustufen wäre. Unter diesen Umständen könnte das von dem Akteur außerhalb der Union betriebene KI-System Daten verarbeiten, die rechtmäßig in der Union erhoben und aus der Union übertragen wurden, und sodann dem vertraglichen Akteur in der Union die aus dieser Verarbeitung resultierenden Ergebnisse dieses KI-Systems liefern, ohne dass dieses KI-System dabei in der Union in Verkehr gebracht, in Betrieb genommen oder verwendet wird. Um die Umgehung dieser Verordnung zu verhindern und einen wirksamen Schutz in der Union ansässiger natürlicher Personen zu gewährleisten, sollte diese Verordnung auch für Anbieter und Nutzer von KI-Systemen gelten, die in einem Drittland ansässig oder niedergelassen sind, soweit die von diesen Systemen erzeugten Ergebnisse in der Union verwendet werden. Um jedoch bestehenden Vereinbarungen und besonderen Erfordernissen für die künftige 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. Empfangende Behörden der Mitgliedstaaten und Organe, Einrichtungen und sonstige Stellen der Union sowie Stellen in der Union, die diese Ergebnisse verwenden, sind weiterhin dafür verantwortlich, sicherzustellen, dass ihre Verwendung mit Unionsrecht vereinbar ist. Wenn diese internationalen Übereinkünfte überarbeitet oder wenn künftig neue Übereinkünfte geschlossen werden, sollten die Vertragsparteien größtmögliche Anstrengungen unternehmen, um diese Übereinkünfte an die Anforderungen dieser Verordnung anzugleichen.

(12) Diese Verordnung sollte auch für Organe, Einrichtungen und sonstige Stellen der Union gelten, wenn sie als Anbieter oder Nutzer eines KI-Systems auftreten.

(-12a) Wenn und soweit KI-Systeme mit oder ohne Änderungen für Zwecke in den Bereichen Militär, Verteidigung oder nationale Sicherheit in Verkehr gebracht, in Betrieb genommen oder verwendet werden, sollten sie vom Anwendungsbereich dieser Verordnung ausgenommen werden, unabhängig von der Art der Einrichtung, die diese Tätigkeiten ausübt, etwa ob es sich um eine öffentliche oder private Einrichtung handelt. In Bezug auf die Zwecke in den Bereichen Militär und Verteidigung begründet sich die Ausnahme sowohl auf Artikel 4 Absatz 2 EUV als auch auf die Besonderheiten der Verteidigungspolitik der Mitgliedstaaten und der in Titel V Kapitel 2 des Vertrags über die Europäische Union (EUV) abgedeckten gemeinsamen Verteidigungspolitik der Union, die dem Völkerrecht unterliegen, was daher den geeigneteren Rechtsrahmen für die Regulierung von KI-Systemen im Zusammenhang mit der Anwendung tödlicher Gewalt und sonstigen KI-Systemen im Zusammenhang mit Militär- oder Verteidigungsaktivitäten darstellt. In Bezug auf die Zwecke im Bereich nationale Sicherheit begründet sich die Ausnahme sowohl auf die Tatsache, dass die nationale Sicherheit im Einklang mit Artikel 4 Absatz 2 EUV weiterhin in die alleinige Verantwortung der Mitgliedstaaten fällt, als auch auf die besondere Art und die operativen Bedürfnisse der Tätigkeiten im Bereich der nationalen Sicherheit und der spezifischen nationalen Vorschriften für diese Tätigkeiten. Wird ein KI-System, das für Zwecke in den Bereichen Militär, Verteidigung oder nationale Sicherheit entwickelt, in Verkehr gebracht, in Betrieb genommen oder verwendet wird, jedoch vorübergehend oder ständig für andere Zwecke verwendet (etwa für zivile oder humanitäre Zwecke oder für Zwecke der Strafverfolgung oder öffentlichen Sicherheit), so würde dieses System in den Anwendungsbereich dieser Verordnung fallen. In diesem Fall sollte die Einrichtung, die das System für andere Zwecke als Zwecke in den Bereichen Militär, Verteidigung oder nationale Sicherheit verwendet, die Konformität des Systems mit dieser Verordnung sicherstellen, es sei denn, das System entspricht bereits dieser Verordnung. KI-Systeme, die für einen ausgeschlossenen Zweck (d. h. Militär, Verteidigung oder nationale Sicherheit) und für einen oder mehrere nicht ausgeschlossene Zwecke (etwa zivile Zwecke, Strafverfolgung usw.) in Verkehr gebracht oder in Betrieb genommen werden, fallen in den Anwendungsbereich dieser Verordnung, und Anbieter dieser Systeme sollten die Einhaltung dieser Verordnung sicherstellen. In diesen Fällen sollte sich die Tatsache, dass ein KI-System in den Anwendungsbereich dieser Verordnung fällt, nicht darauf auswirken, dass Einrichtungen, die Tätigkeiten in Bezug auf militärische Angelegenheiten, Verteidigung und nationale Sicherheit ausüben, KI-Systeme für Zwecke in den Bereichen Militär, Verteidigung oder nationale Sicherheit – unabhängig von der Art der Einrichtung, die diese Tätigkeiten ausübt – verwenden können, wobei deren Verwendung vom Anwendungsbereich dieser Verordnung ausgenommen ist. Ein KI-System, das für zivile Zwecke oder Strafverfolgungszwecke in Verkehr gebracht wurde und mit oder ohne Änderungen für Zwecke in den Bereichen Militär, Verteidigung oder nationale Sicherheit verwendet wird, sollte nicht in den Anwendungsbereich dieser Verordnung fallen, unabhängig von der Art der Einrichtung, die diese Tätigkeiten ausübt.

(12a) 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.

(12b) Diese Verordnung sollte Aktivitäten zur Forschung und Entwicklung nicht untergraben und die Freiheit der Wissenschaft respektieren. Daher müssen KI-Systeme, die eigens für den alleinigen Zweck der wissenschaftlichen Forschung und Entwicklung entwickelt und in Betrieb genommen werden, vom Anwendungsbereich der Verordnung ausgenommen werden, und es muss sichergestellt werden, dass sich die Verordnung nicht anderweitig auf die Aktivitäten zur Forschung und Entwicklung in Bezug auf KI-Systeme auswirkt. Auch in Bezug auf produktorientierte Forschungsaktivitäten der Anbieter sollte diese Verordnung nicht gelten. Dies berührt weder die Pflicht zur Einhaltung dieser Verordnung, wenn ein KI-System, das in den Anwendungsbereich dieser Verordnung fällt, infolge von Forschungs- und Entwicklungsaktivitäten in Verkehr gebracht oder in Betrieb genommen wird, noch die Anwendung der Bestimmungen zu Reallaboren und zu Tests unter realen Bedingungen. Darüber hinaus sollte unbeschadet der Anmerkungen in Bezug auf KI-Systeme, die eigens für den alleinigen Zweck der wissenschaftlichen Forschung und Entwicklung entwickelt und in Betrieb genommen werden, jedes andere KI-System, das für die Durchführung von Forschungs- und Entwicklungsaktivitäten verwendet werden könnte, den Bestimmungen dieser Verordnung unterliegen. In jedem Fall sollten jegliche Forschungs- und Entwicklungsaktivitäten gemäß anerkannter ethischer und professioneller Grundsätze für die wissenschaftliche Forschung ausgeführt werden.

(12c) In Anbetracht der Art und Komplexität der Wertschöpfungskette von KI-Systemen ist es unerlässlich, die Rolle von Akteuren zu klären, die zur Entwicklung von KI-Systemen, vor allem von Hochrisiko-KI-Systemen, beitragen können. Es muss insbesondere klargestellt werden, dass KI-Systeme mit allgemeinem Verwendungszweck KI-Systeme sind, die vom Anbieter dazu vorgesehen sind, allgemein anwendbare Funktionen, wie Bild- oder Spracherkennung, in einer Vielzahl von Kontexten auszuführen. Sie können einzeln als Hochrisiko-KI-System verwendet werden oder Komponenten von Hochrisiko-KI-Systemen sein. Aufgrund ihrer besonderen Merkmale und zur Gewährleistung einer gerechten Verteilung der Verantwortung entlang der KI-Wertschöpfungskette sollten diese Systeme im Rahmen dieser Verordnung daher verhältnismäßigen und spezifischeren Anforderungen und Pflichten unterliegen, während ein hohes Schutzniveau in Bezug auf Grundrechte, Gesundheit und Sicherheit sichergestellt wird. Darüber hinaus sollten Anbieter von KI-Systemen mit allgemeinem Verwendungszweck, unabhängig davon, ob sie von Anbietern einzeln als Hochrisiko-KI-System oder als Komponenten von Hochrisiko-KI-Systemen verwendet werden, gegebenenfalls mit den Anbietern der entsprechenden Hochrisiko-KI-Systeme, um ihnen die Einhaltung der Verpflichtungen aus dieser Verordnung zu ermöglichen, und mit den gemäß dieser Verordnung eingerichteten zuständigen Behörden zusammenarbeiten. Um den besonderen Merkmalen von KI-Systemen mit allgemeinem Verwendungszweck und den rasanten Marktentwicklungen und technischen Entwicklungen in diesem Bereich Rechnung zu tragen, sollten der Kommission Durchführungsbefugnisse übertragen werden, um die Anwendung der Anforderungen dieser Verordnung an KI-Systeme mit allgemeinem Verwendungszweck zu präzisieren und anzupassen sowie um den Austausch von Informationen zwischen Anbietern von KI-Systemen mit allgemeinem Verwendungszweck festzulegen, damit die Anbieter des entsprechenden Hochrisiko-KI-Systems ihre Pflichten aus dieser Verordnung einhalten können.

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

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

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

(16) KI-gestützte manipulative Techniken können dazu verwendet werden, Personen zu unerwünschten Verhaltensweisen zu bewegen oder sie zu täuschen, indem sie in einer Weise zu Entscheidungen angeregt werden, die ihre Autonomie, Entscheidungsfindung und freie Auswahl untergräbt und beeinträchtigt. Das Inverkehrbringen, die Inbetriebnahme oder die Verwendung bestimmter KI-Systeme, die menschliches Verhalten wesentlich beeinflussen, und die zu physischen oder psychischen Schäden führen dürften, sind besonders gefährlich und sollten dementsprechend verboten werden. Solche KI-Systeme setzen auf eine unterschwellige Beeinflussung, beispielweise durch Reize in Form von Ton-, Bild- oder Videoinhalten, die für Menschen nicht erkennbar sind, da diese Reize außerhalb ihres Wahrnehmungsbereichs liegen, oder auf andere Arten unterschwelliger Beeinflussung, die ihre Autonomie, Entscheidungsfindung oder freie Auswahl in einer Weise untergraben und beeinträchtigen, die sich ihrer bewussten Wahrnehmung entzieht oder deren Einfluss – selbst wenn sie sich seiner bewusst sind – sie nicht kontrollieren oder widerstehen können, etwa in Fällen von Gehirn-Computer-Schnittstellen oder virtueller Realität. Ferner können KI-Systeme auch anderweitig Schwächen bestimmter Gruppen von Personen aufgrund ihres Alters oder einer Behinderung im Sinne der Richtlinie (EU) 2019/882 oder aufgrund einer bestimmten sozialen oder wirtschaftlichen Situation ausnutzen, durch die diese Personen gegenüber einer Ausnutzung anfälliger werden dürften – beispielweise Personen, die in extremer Armut leben, und ethnische oder religiöse Minderheiten. Solche KI-Systeme können in Verkehr gebracht, in Betrieb genommen oder mit dem Ziel oder der Wirkung verwendet werden, das Verhalten einer Person in einer Weise wesentlich zu beeinflussen, die dieser Person oder einer anderen Person oder Gruppen von Personen einen physischen oder psychischen Schaden zufügt oder mit hinreichender Wahrscheinlichkeit zufügen wird, einschließlich Schäden, die sich im Laufe der Zeit anhäufen können. Diese Absicht, das Verhalten zu beeinflussen, kann nicht vermutet werden, wenn die Beeinflussung auf Faktoren zurückzuführen ist, die nicht Teil des KI-Systems sind und außerhalb der Kontrolle des Anbieters oder Nutzers liegen, d. h. Faktoren, die vom Anbieter oder Nutzer des KI-Systems vernünftigerweise nicht vorhergesehen oder gemindert werden können. In jedem Fall ist es nicht erforderlich, dass der Anbieter oder der Nutzer die Absicht haben, physischen oder psychischen Schaden zuzufügen, wenn dieser Schaden aufgrund von manipulativen oder ausbeuterischen KI-gestützten Praktiken entsteht. Das Verbot solcher KI-Praktiken ergänzt die Bestimmungen der Richtlinie 2005/29/EG, insbesondere sind unlautere Geschäftspraktiken, durch die die Verbraucher wirtschaftliche oder finanzielle Schäden erleiden, unter allen Umständen verboten, unabhängig davon, ob sie durch KI-Systeme oder anderweitig umgesetzt werden. Das Verbot manipulativer und ausbeuterischer Praktiken gemäß dieser Verordnung sollte sich nicht auf rechtmäßige Praktiken im Zusammenhang mit medizinischen Behandlungen, etwa der psychologischen Behandlung einer psychischen Krankheit oder der physischen Rehabilitation, auswirken, wenn diese Praktiken im Einklang mit den geltenden Standards und Rechtsvorschriften im medizinischen Bereich erfolgen. Darüber hinaus sollten übliche und rechtmäßige Geschäftspraktiken, die im Einklang mit den geltenden Rechtsvorschriften stehen, als solche nicht als schädliche manipulative KI-Praktiken gelten.

(17) KI-Systeme, mit denen Behörden oder private Akteure das soziale Verhalten natürlicher Personen bewerten, können zu diskriminierenden Ergebnissen und zur Ausgrenzung bestimmter Gruppen führen. Sie können die Menschenwürde und das Recht auf Nichtdiskriminierung sowie die Werte der Gleichheit und Gerechtigkeit verletzen. Solche KI-Systeme bewerten oder klassifizieren natürliche Personen auf der Grundlage ihres sozialen Verhaltens in verschiedenen Zusammenhängen oder aufgrund bekannter oder vorhergesagter persönlicher Eigenschaften oder Persönlichkeitsmerkmale. Die aus solchen KI-Systemen erzielte soziale Bewertung kann zu einer Schlechterstellung oder Benachteiligung bestimmter natürlicher Personen oder ganzer Gruppen natürlicher Personen in sozialen Zusammenhängen, die in keinem Zusammenhang zu den Umständen stehen, unter denen die Daten ursprünglich erzeugt oder erfasst wurden, oder zu einer Schlechterstellung in einer Weise führen, die im Hinblick auf ihr soziales Verhalten oder dessen Tragweite ungerechtfertigt oder unverhältnismäßig ist. KI-Systeme, die solche inakzeptablen Bewertungspraktiken mit sich bringen, sollten daher verboten werden. Dieses Verbot sollte nicht die rechtmäßigen Praktiken zur Bewertung von natürlichen Personen berühren, die im Einklang mit den Rechtsvorschriften für einen oder mehrere bestimmte Zwecke durchgeführt wird.

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

(19) Die Verwendung solcher Systeme zu Strafverfolgungszwecken sollte daher untersagt werden, außer in erschöpfend aufgeführten und eng abgegrenzten Fällen, in denen die Verwendung unbedingt erforderlich ist, um einem erheblichen öffentlichen Interesse zu dienen, dessen Bedeutung die Risiken überwiegt. Zu diesen Fällen gehört die Suche nach potenziellen Opfern von Straftaten, einschließlich vermisster Kinder, bestimmte Gefahren für das Leben oder die körperliche Unversehrtheit natürlicher Personen oder die Gefahr eines Terroranschlags sowie das Erkennen, Aufspüren, Identifizieren oder Verfolgen von Tätern oder Verdächtigen von Straftaten im Sinne des Rahmenbeschlusses 2002/584/JI des Rates[9], sofern diese Straftaten in dem betreffenden Mitgliedstaat nach dessen Recht mit einer Freiheitsstrafe oder einer freiheitsentziehenden Maßregel der Sicherung im Höchstmaß von mindestens drei Jahren bedroht sind. Eine solche Schwelle für eine Freiheitsstrafe oder eine freiheitsentziehende Maßregel der Sicherung nach nationalem Recht trägt dazu bei sicherzustellen, dass die Straftat schwerwiegend genug ist, um den Einsatz biometrischer Echtzeit-Fernidentifizierungssysteme zu rechtfertigen. Darüber hinaus sind einige der 32 im Rahmenbeschluss 2002/584/JI des Rates aufgeführten Straftaten in der Praxis eher relevant als andere, da der Rückgriff auf die biometrische Echtzeit-Fernidentifizierung für die konkrete Erkennung, Aufspürung, Identifizierung oder Verfolgung eines Täters oder Verdächtigen einer der verschiedenen aufgeführten Straftaten voraussichtlich in äußerst unterschiedlichem Maße erforderlich und verhältnismäßig sein wird und da dabei die wahrscheinlichen Unterschiede in Schwere, Wahrscheinlichkeit und Ausmaß des Schadens oder möglicher negativer Folgen zu berücksichtigen sind. Darüber hinaus sollte diese Verordnung die Fähigkeit der Strafverfolgungs-, Grenzschutz-, Einwanderungs- oder Asylbehörden erhalten, im Einklang mit den im Unionsrecht und im nationalen Recht für diesen Zweck festgelegten Bedingungen die Identität der betreffenden Person in ihrer Anwesenheit festzustellen. Insbesondere sollten Strafverfolgungs-, Grenzschutz-, Einwanderungs- oder Asylbehörden im Einklang mit dem Unionsrecht und dem nationalen Recht Informationssysteme verwenden können, um eine Person zu identifizieren, die während einer Identitätsfeststellung entweder verweigert, identifiziert zu werden, oder nicht in der Lage ist, seine oder ihre Identität anzugeben oder zu belegen, wobei gemäß dieser Verordnung keine vorherige Genehmigung erlangt werden muss. Dabei könnte es sich beispielsweise um eine Person handeln, die in eine Straftat verwickelt ist und nicht gewillt oder aufgrund eines Unfalls oder des Gesundheitszustands nicht in der Lage ist, den Strafverfolgungsbehörden ihre Identität offenzulegen.

---

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

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

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

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

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

(24) Jede Verarbeitung biometrischer Daten und anderer personenbezogener Daten im Zusammenhang mit der Verwendung von KI-Systemen für die biometrische Identifizierung, ausgenommen im Zusammenhang mit der Verwendung biometrischer Echtzeit-Fernidentifizierungssysteme in öffentlich zugänglichen Räumen zu Strafverfolgungszwecken im Sinne dieser Verordnung, sollte weiterhin allen Anforderungen genügen, die sich aus Artikel 10 der Richtlinie (EU) 2016/680 ergeben. Für andere Zwecke als die Strafverfolgung ist die Verarbeitung biometrischer Daten zur eindeutigen Identifizierung einer natürlichen Person gemäß Artikel 9 Absatz 1 der Verordnung (EU) 2016/679 und Artikel 10 Absatz 1 der Verordnung (EU) 2018/1725 verboten, es sei denn, es liegt einer der Fälle vor, die in Absatz 2 des jeweiligen genannten Artikels aufgeführt sind.

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

(26) Nach den Artikeln 2 und 2a des dem EUV und dem AEUV beigefügten Protokolls Nr. 22 über die Position Dänemarks ist Dänemark durch die auf der Grundlage des Artikels 16 AEUV festgelegten Vorschriften in Artikel 5 Absatz 1 Buchstabe d und Artikel 5 Absätze 2, 3 und 4 dieser Verordnung in Bezug auf die Verarbeitung personenbezogener Daten durch die Mitgliedstaaten im Rahmen der Ausübung von Tätigkeiten, die in den Anwendungsbereich des Dritten Teils Titel V Kapitel 4 und 5 AEUV fallen, weder gebunden noch zu ihrer Anwendung verpflichtet.

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

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

(29) In Bezug auf Hochrisiko-KI-Systeme, bei denen es sich um Sicherheitskomponenten von Produkten oder Systemen oder selbst um Produkte oder Systeme handelt, die in den Anwendungsbereich der Verordnung (EG) Nr. 300/2008 des Europäischen Parlaments und des Rates[10], der Verordnung (EU) Nr. 167/2013 des Europäischen Parlaments und des Rates[11], der Verordnung (EU) Nr. 168/2013 des Europäischen Parlaments und des Rates[12], der Richtlinie 2014/90/EU des Europäischen Parlaments und des Rates[13], der Richtlinie (EU) 2016/797 des Europäischen Parlaments und des Rates[14], der Verordnung (EU) 2018/858 des Europäischen Parlaments und des Rates[15], der Verordnung (EU) 2018/1139 des Europäischen Parlaments und des Rates[16] und der Verordnung (EU) 2019/2144 des Europäischen Parlaments und des Rates[17] fallen, ist es angezeigt, diese Rechtsakte zu ändern, damit die Kommission – aufbauend auf den technischen und regulatorischen Besonderheiten des jeweiligen Sektors und ohne Beeinträchtigung bestehender Governance-, Konformitätsbewertungs- und Durchsetzungsmechanismen sowie der darin eingerichteten Behörden – beim Erlass von etwaigen künftigen delegierten Rechtsakten oder Durchführungsrechtsakten auf der Grundlage der genannten Rechtsakte die in der vorliegenden Verordnung festgelegten verbindlichen Anforderungen an Hochrisiko-KI-Systeme berücksichtigt.

---

10 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).

11 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).

12 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).

13 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).

14 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).

15 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).

16 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).

17 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).

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

(31) Die Einstufung eines KI-Systems als hochriskant gemäß dieser Verordnung sollte nicht zwangsläufig bedeuten, dass von dem Produkt, dessen Sicherheitskomponente das KI-System ist, oder dem KI-System als Produkt selbst nach den Kriterien der einschlägigen Harmonisierungsrechtsvorschriften der Union für das betreffende Produkt ein hohes Risiko ausgeht. Dies betrifft insbesondere die Verordnung (EU) 2017/745 des Europäischen Parlaments und des Rates[18] und die Verordnung (EU) 2017/746 des Europäischen Parlaments und des Rates[19], in denen für Produkte, die ein mittleres und hohes Risiko bergen, eine Konformitätsbewertung durch Dritte vorgesehen ist.

---

[18] 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).

[19] 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).

(32) Bei Hochrisiko-KI-Systemen, bei denen es sich um andere Systeme als Sicherheitskomponenten von Produkten handelt oder die selbst Produkte sind, ist es angezeigt, sie als hochriskant einzustufen, wenn sie aufgrund ihrer Zweckbestimmung ein hohes Risiko bergen, die Gesundheit und Sicherheit oder die Grundrechte von Personen zu schädigen, wobei sowohl die Schwere des möglichen Schadens als auch die Wahrscheinlichkeit seines Auftretens zu berücksichtigen sind, und sofern sie in einer Reihe von Bereichen verwendet werden, die in der Verordnung ausdrücklich festgelegt sind. Die Bestimmung dieser Systeme erfolgt nach derselben Methode und denselben Kriterien, die auch für künftige Änderungen der Liste der Hochrisiko-KI-Systeme vorgesehen sind. Ferner muss klargestellt werden, dass es innerhalb der in Anhang III aufgeführten Hochrisiko-Fälle Systeme geben kann, die – unter Berücksichtigung des von dem KI-System hervorgebrachten Ergebnisses – nicht zu einem bedeutenden Risiko für die in diesen Fällen geschützten rechtlichen Interessen führen. Daher sollte das KI-System, das ein solches Ergebnis hervorbringt, nur dann als Hochrisiko-System erachtet werden, wenn ein solches Ergebnis in Bezug auf die zu treffende Maßnahme oder Entscheidung einen hohen Bedeutungsgrad hat (d. h. nicht völlig unwesentlich ist), sodass es ein bedeutendes Risiko für die geschützten rechtlichen Interessen hervorruft. Wenn beispielsweise die dem Menschen von dem KI-System bereitgestellten Informationen aus der Erstellung von Profilen natürlicher Personen im Sinne von Artikel 4 Absatz 4 der Verordnung (EU) 2016/679 und Artikel 3 Absatz 4 der Richtlinie (EU) 2016/680 und Artikel 3 Absatz 5 der Verordnung (EU) 2018/1725 besteht, so sollten solche Informationen im Zusammenhang mit den in Anhang III aufgeführten Hochrisiko-KI-Systemen nicht typischerweise als unwesentlich erachtet werden. Wenn das Ergebnis des KI-Systems allerdings nur von unerheblicher oder geringfügiger Relevanz für menschliche Maßnahmen oder Entscheidungen ist, so kann es als völlig unwesentlich erachtet werden, einschließlich beispielsweise KI-Systeme, die für die Übersetzung zu Zwecken der Information oder der Dokumentenverwaltung verwendet werden.

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

(34) Was die Verwaltung und den Betrieb kritischer Infrastrukturen anbelangt, so sollten KI-Systeme, die als Sicherheitskomponenten für das Management und den Betrieb kritischer digitaler Infrastruktur gemäß Anhang I Punkt 8 der Richtlinie über die Resilienz kritischer Einrichtungen, des Straßenverkehrs sowie für die Wasser-, Gas-, Wärme- und Stromversorgung verwendet werden sollen, als hochriskant eingestuft werden, da ihr Ausfall oder ihre Störung in großem Umfang das Leben und die Gesundheit von Menschen gefährden und zu erheblichen Störungen bei der normalen Durchführung sozialer und wirtschaftlicher Tätigkeiten führen kann. Sicherheitskomponenten kritischer Infrastruktur, einschließlich kritischer digitaler Infrastruktur, sind Systeme, die verwendet werden, um die physische Integrität kritischer Infrastruktur oder die Gesundheit und Sicherheit von Menschen und Eigentum zu schützen, die aber nicht notwendig sind, damit das System funktioniert. 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 Beispielen von Sicherheitskomponenten solcher kritischen Infrastruktur zählen etwa Systeme für die Überwachung des Wasserdrucks oder Feuermelder-Kontrollsysteme in Cloud-Computing-Zentren.

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

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

(37) Ein weiterer Bereich, in dem der Einsatz von KI-Systemen besondere Aufmerksamkeit verdient, ist der Zugang zu und die Nutzung von bestimmten grundlegenden privaten und öffentlichen Diensten und Leistungen, die erforderlich sind, damit die Menschen uneingeschränkt an der Gesellschaft teilhaben oder ihren Lebensstandard verbessern können. Insbesondere KI-Systeme, die zur Kreditpunktebewertung oder zur Bewertung der Kreditwürdigkeit natürlicher Personen verwendet werden, sollten als Hochrisiko-KI-Systeme eingestuft werden, da sie den Zugang dieser Personen zu Finanzmitteln oder wesentlichen Dienstleistungen wie Wohnraum, Elektrizität und Telekommunikationsdienstleistungen bestimmen. KI-Systeme, die zu diesem Zweck eingesetzt werden, können zur Diskriminierung von Personen oder Gruppen führen und historische Diskriminierungsmuster, beispielsweise aufgrund der rassischen oder ethnischen Herkunft, einer Behinderung, des Alters oder der sexuellen Ausrichtung, fortschreiben oder neue Formen von Diskriminierung mit sich bringen. Angesichts des sehr begrenzten Auswirkungen und der auf dem Markt verfügbaren Alternativen ist es angezeigt, KI-Systeme zur Kreditwürdigkeitsprüfung und Kreditpunktebewertung auszunehmen, wenn sie von Kleinst- oder Kleinunternehmen im Sinne des Anhangs der Empfehlung 2003/361/EG der Kommission für den Eigenbedarf in Betrieb genommen werden. Natürliche Personen, die grundlegende staatliche Unterstützungsleistungen und -dienste von Behörden beantragen oder erhalten, sind in der Regel von diesen Leistungen und Diensten abhängig und befinden sich gegenüber den zuständigen Behörden in einer prekären Lage. Wenn KI-Systeme eingesetzt werden, um zu bestimmen, ob solche Leistungen und Dienste von den Behörden verweigert, gekürzt, widerrufen oder zurückgefordert werden sollten, einschließlich der Frage, ob Begünstigte rechtmäßig Anspruch auf solche Leistungen oder Dienste haben, können diese Systeme erhebliche Auswirkungen auf die Existenzgrundlage der Menschen haben und ihre Grundrechte wie das Recht auf sozialen Schutz, Nichtdiskriminierung, Menschenwürde oder einen wirksamen Rechtsbehelf verletzen. Solche Systeme sollten daher als hochriskant eingestuft werden. Dennoch sollte diese Verordnung die Entwicklung und Anwendung innovativer Ansätze in der öffentlichen Verwaltung nicht behindern, die von einer breiteren Verwendung konformer und sicherer KI-Systeme profitieren würde, sofern diese Systeme kein hohes Risiko für juristische und natürliche Personen bergen. Schließlich sollten KI-Systeme, die bei der Entsendung oder der Priorisierung der Entsendung von Rettungsdiensten eingesetzt werden, ebenfalls als hochriskant eingestuft werden, da sie in für das Leben und die Gesundheit von Personen und für ihr Eigentum sehr kritischen Situationen Entscheidungen treffen. KI-Systeme werden ferner zunehmend für die Risikobewertung in Bezug auf natürliche Personen und Preisbildung im Fall von Lebens- und Krankenversicherungen verwendet, was – bei nicht ordnungsgemäßer Konzeption, Entwicklung und Verwendung – schwerwiegende Konsequenzen für das Leben und die Gesundheit von Menschen haben kann, einschließlich finanzieller Ausgrenzung und Diskriminierung. Um einen kohärenten Ansatz im Finanzdienstleistungssektor zu gewährleisten, sollte die oben genannte Ausnahme für Kleinst- oder Kleinunternehmen für den Eigenbedarf gelten, sofern sie selbst ein KI-System für den Verkauf ihrer eigenen Versicherungsprodukte bereitstellen und in Betrieb nehmen.

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

(39) KI-Systeme, die in den Bereichen Migration, Asyl und Grenzkontrolle eingesetzt werden, betreffen Menschen, die sich häufig in einer besonders prekären Lage befinden und vom Ergebnis der Maßnahmen der zuständigen Behörden abhängig sind. Die Genauigkeit, der nichtdiskriminierende Charakter und die Transparenz der KI-Systeme, die in solchen Zusammenhängen eingesetzt werden, sind daher besonders wichtig, um die Achtung der Grundrechte der betroffenen Personen, insbesondere ihrer Rechte auf Freizügigkeit, Nichtdiskriminierung, den Schutz des Privatlebens und personenbezogener Daten, den internationalen Schutz und die gute Verwaltung, zu gewährleisten. Daher ist es angezeigt, KI-Systeme als hochriskant einzustufen, die von den zuständigen mit Aufgaben in den Bereichen Migration, Asyl und Grenzkontrolle betrauten Behörden für Folgendes eingesetzt werden: als Lügendetektoren und ähnliche Instrumente oder zur Ermittlung des emotionalen Zustand einer natürlichen Person; zur Bewertung bestimmter Risiken, die von natürlichen Personen ausgehen, die in das Hoheitsgebiet eines Mitgliedstaats einreisen oder ein Visum oder Asyl beantragen; zur Unterstützung der zuständigen Behörden bei der Prüfung von Asyl- und Visumanträgen sowie Aufenthaltstiteln und damit verbundenen Beschwerden im Hinblick darauf, die Berechtigung der den Antrag stellenden natürlichen Personen festzustellen. KI-Systeme im Bereich Migration, Asyl und Grenzkontrolle, die unter diese Verordnung fallen, sollten den einschlägigen Verfahrensvorschriften der Richtlinie 2013/32/EU des Europäischen Parlaments und des Rates[20], der Verordnung (EG) Nr. 810/2009 des Europäischen Parlaments und des Rates[21] und anderen einschlägigen Rechtsvorschriften entsprechen.

---

[20] 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).

[21] 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).

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

(41) Die Tatsache, dass ein KI-System gemäß dieser Verordnung als hochriskant eingestuft wird, sollte nicht dahingehend ausgelegt werden, dass die Verwendung des Systems nach anderen Rechtsakten der Union oder nach nationalen Rechtsvorschriften, die mit dem Unionsrecht vereinbar sind, rechtmäßig ist, beispielsweise in Bezug auf den Schutz personenbezogener Daten, die Verwendung von Lügendetektoren und ähnlichen Instrumenten oder anderen Systemen zur Ermittlung des emotionalen Zustand einer natürlichen Person. Eine solche Verwendung sollte weiterhin ausschließlich im Einklang mit den geltenden Anforderungen erfolgen, die sich aus der Charta, dem anwendbaren Sekundärrecht der Union und nationalen Recht ergeben. Diese Verordnung sollte nicht so verstanden werden, dass sie eine Rechtsgrundlage für die Verarbeitung personenbezogener Daten bildet, auch nicht – gegebenenfalls – für besondere Kategorien personenbezogener Daten, vorbehaltlich gegenteiliger Bestimmungen in dieser Verordnung.

(42) Zur Minderung der Risiken, die von auf dem Unionsmarkt in Verkehr gebrachten oder anderweitig in Betrieb genommenen Hochrisiko-KI-Systemen ausgehen, sollten bestimmte verbindliche Anforderungen gelten, wobei der Zweckbestimmung des Systems und dem vom Anbieter einzurichtenden Risikomanagementsystem Rechnung zu tragen ist. Insbesondere sollte das Risikomanagementsystem aus einem kontinuierlichen iterativen Prozess bestehen, der während des gesamten Lebenszyklus eines Hochrisiko-KI-Systems geplant und durchgeführt wird. Mit diesem Prozess sollte sichergestellt werden, dass der Anbieter die Risiken für die Gesundheit, die Sicherheit und die Grundrechte der Personen, die von dem System im Lichte seiner Zweckbestimmung betroffen sein könnten, einschließlich der möglichen Risiken, die sich aus der Interaktion zwischen dem KI-System und der Umgebung, in der es betrieben wird, ergeben könnten, ermittelt und analysiert und dementsprechend geeignete Risikomanagementmaßnahmen nach dem Stand der Technik ergreift.

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

(44) Eine hohe Datenqualität ist für die Leistung vieler KI-Systeme von wesentlicher Bedeutung, insbesondere wenn Techniken eingesetzt werden, bei denen Modelle mit Daten trainiert werden, um sicherzustellen, dass das Hochrisiko-KI-System bestimmungsgemäß und sicher funktioniert und nicht zur Ursache für Diskriminierung wird, die nach dem Unionsrecht verboten ist. Für hochwertige Trainings-, Validierungs- und Testdatensätze müssen geeignete Daten-Governance- und Datenverwaltungsverfahren umgesetzt werden. Die Trainings-, Validierungs- und Testdatensätze sollten hinreichend relevant und repräsentativ sein und die geeigneten statistischen Merkmale haben, auch bezüglich der Personen oder Personengruppen, auf die das Hochrisiko-KI-System bestimmungsgemäß angewandt werden soll. Diese Datensätze sollten ferner im Hinblick auf die Zweckbestimmung des KI-Systems weitestgehend fehlerfrei und so vollständig wie möglich sein, wobei der technischen Durchführbarkeit und dem Stand der Technik, der Verfügbarkeit von Daten und der Umsetzung geeigneter Risikomanagementmaßnahmen auf verhältnismäßige Weise Rechnung zu tragen ist, sodass mögliche Mängel der Datensätze angemessen behoben werden. Die Anforderung, dass die Datensätze vollständig und fehlerfrei sein müssen, sollte sich nicht auf den Einsatz von Techniken zur Wahrung der Privatsphäre im Zusammenhang mit der Entwicklung und dem Testen von KI-Systemen auswirken. Die Trainings-, Validierungs- und Testdatensätze sollten, soweit dies aufgrund der Zweckbestimmung erforderlich ist, den Eigenschaften, Merkmalen oder Elementen entsprechen, die für die besonderen geografischen, verhaltensbezogenen oder funktionalen Rahmenbedingungen oder den Zusammenhängen, in denen das KI-System bestimmungsgemäß verwendet werden soll, typisch sind. Um das Recht anderer auf Schutz vor Diskriminierung, die sich aus Verzerrungen in KI-Systemen ergeben könnte, zu wahren, sollten die Anbieter angesichts des erheblichen öffentlichen Interesses im Sinne von Artikel 9 Absatz 2 Buchstabe g der Verordnung (EU) 2016/679 und Artikel 10 Absatz 2 Buchstabe g der Verordnung (EU) 2018/1725 auch besondere Kategorien personenbezogener Daten verarbeiten dürfen, um Verzerrungen in Hochrisiko-KI-Systemen zu beobachten, zu erkennen und zu korrigieren.

(44a) Bei der Anwendung der in Artikel 5 Absatz 1 Buchstabe c der Verordnung (EU) 2016/679 und Artikel 4 Absatz 1 Buchstabe c der Verordnung (EU) 2018/1725 genannten Grundsätze, insbesondere des Grundsatzes der Datenminimierung, sollte im Hinblick auf Trainings-, Validierungs- und Testdatensätze im Rahmen der vorliegenden Verordnung der vollständige Lebenszyklus des KI-Systems gebührend berücksichtigt werden.

(45) Für die Entwicklung von Hochrisiko-KI-Systemen sollten bestimmte Akteure wie Anbieter, notifizierte Stellen und andere einschlägige Stellen wie Zentren für digitale Innovation, Test- und Versuchseinrichtungen und Forscher in der Lage sein, in ihren jeweiligen Tätigkeitsbereichen, die mit dieser Verordnung in Zusammenhang stehen, auf hochwertige Datensätze zuzugreifen und diese zu nutzen. Die von der Kommission eingerichteten gemeinsamen europäischen Datenräume und die Erleichterung des Datenaustauschs im öffentlichen Interesse zwischen Unternehmen und mit Behörden werden entscheidend dazu beitragen, einen vertrauensvollen, rechenschaftspflichtigen und diskriminierungsfreien Zugang zu hochwertigen Daten für das Training, die Validierung und das Testen von KI-Systemen zu gewährleisten. Im Gesundheitsbereich beispielsweise wird der europäische Raum für Gesundheitsdaten den diskriminierungsfreien Zugang zu Gesundheitsdaten und das Training von KI-Algorithmen mithilfe dieser Datensätze erleichtern, und zwar unter Wahrung der Privatsphäre, auf sichere, zeitnahe, transparente und vertrauenswürdige Weise und unter angemessener institutioneller Leitung. Die einschlägigen zuständigen Behörden, einschließlich sektoraler Behörden, die den Zugang zu Daten bereitstellen oder unterstützen, können auch die Bereitstellung hochwertiger Daten für das Training, die Validierung und das Testen von KI-Systemen unterstützen.

(46) Informationen darüber, wie Hochrisiko-KI-Systeme entwickelt wurden und wie sie während ihres gesamten Lebenszyklus funktionieren, sind unerlässlich, um die Einhaltung der Anforderungen dieser Verordnung überprüfen zu können. Dies erfordert die Führung von Aufzeichnungen und die Verfügbarkeit einer technischen Dokumentation, die alle erforderlichen Informationen enthält, um die Einhaltung der einschlägigen Anforderungen durch das KI-System zu beurteilen. Diese Informationen sollten die allgemeinen Merkmale, Fähigkeiten und Grenzen des Systems, die verwendeten Algorithmen, Daten, Trainings-, Test- und Validierungsverfahren sowie die Dokumentation des einschlägigen Risikomanagementsystems umfassen. Die technische Dokumentation sollte stets auf dem neuesten Stand gehalten werden. Darüber hinaus sollten Anbieter oder Nutzer die vom Hochrisiko-KI-System automatisch erzeugten Protokolle, einschließlich z. B. Ausgabedaten, Datum und Uhrzeit des Beginns usw., soweit dieses System und die zugehörigen Protokolle ihrer Kontrolle unterliegen, für einen Zeitraum aufbewahren, der angemessen ist, damit sie ihren Pflichten nachkommen können.

(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 sollten 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 der Personen, die von dem System im Lichte seiner Zweckbestimmung betroffen sein könnten. Um den Nutzern das Verständnis der Gebrauchsanweisungen zu erleichtern, sollten sie gegebenenfalls anschauliche Beispiele enthalten.

(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. Angesichts der bedeutenden Konsequenzen für Personen im Falle von falschen Treffern durch bestimmte biometrische Identifizierungssysteme ist es angezeigt, für diese Systeme eine verstärkte Anforderung im Hinblick auf die menschliche Aufsicht vorzusehen, sodass der Nutzer keine Maßnahmen oder Entscheidungen aufgrund des vom System hervorgebrachten Identifizierungsergebnisses treffen kann, solange dies nicht von mindestens zwei natürlichen Personen getrennt überprüft und bestätigt wurde. Diese Personen könnten von einer oder mehreren Einrichtungen stammen, darunter die Person, die das System betreibt oder verwendet. Diese Anforderung sollte keine unnötigen Belastungen oder Verzögerungen mit sich bringen, und es könnte ausreichen, dass die getrennten Überprüfungen durch die verschiedenen Personen automatisch in die vom System erzeugten Protokolle aufgenommen werden.

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

(50) Die technische Robustheit ist eine wesentliche Voraussetzung für Hochrisiko-KI-Systeme. Sie sollten widerstandsfähig in Bezug auf schädliches oder anderweitig unerwünschtes Verhalten sein, das sich aus Einschränkungen innerhalb der Systeme oder der Umgebung, in der die Systeme betrieben werden, ergeben kann (z. B. Fehler, Störungen, Unstimmigkeiten, unerwartete Situationen). Hochrisiko-KI-Systeme sollten daher mit geeigneten technischen Lösungen konzipiert und entwickelt werden, um dieses schädliche oder anderweitig unerwünschte Verhalten zu verhindern oder zu minimieren, wie etwa Mechanismen, die es dem System ermöglichen, seinen Betrieb bei bestimmten Anomalien oder, wenn der Betrieb außerhalb vorab festgelegter Grenzen erfolgt, sicher zu unterbrechen (Störungssicherheitspläne). Ein fehlender Schutz vor diesen Risiken könnte die Sicherheit beeinträchtigen oder sich negativ auf die Grundrechte auswirken, wenn das KI-System beispielsweise falsche Entscheidungen trifft oder falsche oder verzerrte Ergebnisse hervorbringt.

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

(52) Als Teil der Harmonisierungsrechtsvorschriften der Union sollten Vorschriften für das Inverkehrbringen, die Inbetriebnahme und die Verwendung von Hochrisiko-KI-Systemen im Einklang mit der Verordnung (EG) Nr. 765/2008 des Europäischen Parlaments und des Rates über die Vorschriften für die Akkreditierung und Überwachung von Produkten[22], dem Beschluss Nr. 768/2008/EG des Europäischen Parlaments und des Rates über einen gemeinsamen Rechtsrahmen für die Vermarktung von Produkten[23] und der Verordnung (EU) 2019/1020 des Europäischen Parlaments und des Rates über Marktüberwachung und die Konformität von Produkten[24] („neuer Rechtsrahmen für die Vermarktung von Produkten“) festgelegt werden.

(52a) Im Einklang mit den Grundsätzen des neuen Rechtsrahmens sollten besondere Pflichten für einschlägige Akteure innerhalb der KI-Wertschöpfungskette festgelegt werden, um die Rechtssicherheit zu gewährleisten und die Einhaltung dieser Verordnung zu erleichtern. In bestimmten Situationen könnten diese Akteure mehr als eine Rolle gleichzeitig wahrnehmen und sollten daher alle einschlägigen Pflichten, die mit diesen Rollen verbunden sind, kumulativ erfüllen. So könnte ein Akteur beispielsweise gleichzeitig als Händler und als Einführer auftreten.

(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.

---

22 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).

23 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).

24 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).

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

(54a) Um Rechtssicherheit zu gewährleisten, muss klargestellt werden, dass unter bestimmten Bedingungen jede natürliche oder juristische Person als Anbieter eines neuen Hochrisiko-KI-Systems betrachtet werden und daher alle einschlägigen Pflichten erfüllen sollte. Dies wäre beispielsweise der Fall, wenn die betreffende Person ihren Namen oder ihre Handelsmarke auf einem bereits in Verkehr gebrachten oder in Betrieb genommenen Hochrisiko-KI-System anbringt oder wenn diese Person die Zweckbestimmung eines KI-Systems, das kein Hochrisiko-System ist und bereits in Verkehr gebracht oder in Betrieb genommen wurde, so ändert, dass das geänderte System zu einem Hochrisiko-KI-System wird. Diese Bestimmungen sollten unbeschadet spezifischerer Bestimmungen in bestimmten sektoralen Rechtsvorschriften des neuen Rechtsrahmens gelten, mit denen diese Verordnung gemeinsam gelten sollte. So sollte beispielsweise Artikel 16 Absatz 2 der Verordnung (EU) 745/2017, wonach bestimmte Tätigkeiten nicht als eine Änderung des Produkts, die Auswirkungen auf seine Konformität mit den geltenden Anforderungen haben könnte, gelten sollten, weiterhin auf Hochrisiko-KI-Systeme angewendet werden, bei denen es sich um Medizinprodukte im Sinne der genannten Verordnung handelt.

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

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

(56a) Für nicht in der Union niedergelassene Anbieter spielt der Bevollmächtigte eine zentrale Rolle bei der Gewährleistung der Konformität der von den betreffenden Anbietern in der Union in Verkehr gebrachten oder in Betrieb genommenen Hochrisiko-KI-Systeme und in seiner Funktion als deren in der Union niedergelassener Ansprechpartner. Angesichts dieser zentralen Rolle und um sicherzustellen, dass die Verantwortung für die Zwecke der Durchsetzung dieser Verordnung übernommen wird, sollte der Bevollmächtigte gesamtschuldnerisch mit dem Anbieter für fehlerhafte Hochrisiko-KI-Systeme haftbar gemacht werden. Die Haftung des Bevollmächtigten gemäß dieser Verordnung lässt die Bestimmungen der Richtlinie 85/374/EWG über die Haftung für fehlerhafte Produkte unberührt.

(57) [gestrichen]

(58) Angesichts des Charakters von KI-Systemen und der Risiken für die Sicherheit und die Grundrechte, die mit ihrer Verwendung verbunden sein können, ist es angebracht, besondere Zuständigkeiten für die Nutzer festzulegen, auch im Hinblick darauf, dass eine angemessene Überwachung der Leistung eines KI-Systems unter realen Bedingungen sichergestellt werden muss. Die Nutzer sollten insbesondere Hochrisiko-KI-Systeme gemäß den Gebrauchsanweisungen verwenden, und es sollten bestimmte andere Pflichten in Bezug auf die Überwachung der Funktionsweise der KI-Systeme und gegebenenfalls auch Aufzeichnungspflichten festgelegt werden. Diese Pflichten sollten unbeschadet anderer Pflichten der Nutzer in Bezug auf Hochrisiko-KI-Systeme nach Unionsrecht oder nationalem Recht gelten und sollten nicht gelten, wenn die Verwendung im Rahmen einer persönlichen und nicht beruflichen Tätigkeit erfolgt.

(58a) Es sollte klargestellt werden, dass diese Verordnung die Pflichten der Anbieter und Nutzer von KI-Systemen in ihrer Rolle als Verantwortliche oder Auftragsverarbeiter, die sich aus dem Unionsrecht über den Schutz personenbezogener Daten ergeben, unberührt lässt, soweit die Konzeption, die Entwicklung oder die Verwendung von KI-Systemen die Verarbeitung personenbezogener Daten umfasst. Ferner sollte klargestellt werden, dass die betroffenen Personen weiterhin über alle Rechte und Garantien verfügen, die ihnen durch dieses Unionsrecht gewährt werden, einschließlich der Rechte im Zusammenhang mit der ausschließlich automatisierten Entscheidungsfindung im Einzelfall und der Profilerstellung. Harmonisierte Vorschriften für das Inverkehrbringen, die Inbetriebnahme und die Verwendung von KI-Systemen, die im Rahmen dieser Verordnung festgelegt werden, sollten die wirksame Umsetzung erleichtern und die Ausübung der Rechte der betroffenen Personen und anderer Rechtsbehelfe, die im Unionsrecht über den Schutz personenbezogener Daten und anderer Grundrechte garantiert sind, ermöglichen.

(59) [gestrichen]

(60) [gestrichen]

(61) Die Normung sollte eine Schlüsselrolle dabei spielen, den Anbietern technische Lösungen zur Verfügung zu stellen, um im Einklang mit dem Stand der Technik die Einhaltung dieser Verordnung zu gewährleisten. Die Einhaltung harmonisierter Normen gemäß der Verordnung (EU) Nr. 1025/2012 des Europäischen Parlaments und des Rates[25], die normalerweise den Stand der Technik widerspiegeln sollten, sollte den Anbietern den Nachweis der Konformität mit den Anforderungen dieser Verordnung ermöglichen. In Ermangelung einschlägiger Verweise auf harmonisierte Normen sollte die Kommission jedoch im Wege von Durchführungsrechtsakten gemeinsame Spezifikationen für bestimmte Anforderungen im Rahmen dieser Verordnung festlegen können, die als außergewöhnliche Ausweichlösung dienen, um die Pflicht des Anbieters zur Einhaltung der Anforderungen dieser Verordnung zu erleichtern, wenn der Normungsprozess blockiert ist oder wenn es Verzögerungen bei der Ausarbeitung einer geeigneten harmonisierten Norm gibt. Ist eine solche Verzögerung auf die technische Komplexität der betreffenden Norm zurückzuführen, sollte die Kommission dies prüfen, bevor sie die Festlegung gemeinsamer Spezifikationen in Erwägung zieht. Eine angemessene Einbeziehung kleiner und mittlerer Unternehmen in die Ausarbeitung von Normen zur Unterstützung der Umsetzung dieser Verordnung ist von wesentlicher Bedeutung, um Innovation und Wettbewerbsfähigkeit im Bereich der künstlichen Intelligenz in der Union zu fördern. Eine solche Beteiligung sollte im Einklang mit den Artikeln 5 und 6 der Verordnung (EU) Nr. 1025/2012 angemessen sichergestellt werden.

---

[25] 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).

(61a) Unbeschadet der Anwendung harmonisierter Normen und gemeinsamer Spezifikationen ist es angezeigt, dass für Anbieter eine Vermutung der Konformität mit der einschlägigen Datenanforderungen gilt, wenn ihr Hochrisiko-KI-System anhand von Daten trainiert und getestet wurde, die die spezifischen geografischen, verhaltensbezogenen oder funktionalen Rahmenbedingungen widerspiegeln, in denen das KI-System verwendet werden soll. Ebenso sollte im Einklang mit Artikel 54 Absatz 3 der Verordnung (EU) 2019/881 des Europäischen Parlaments und des Rates bei Hochrisiko-KI-Systemen, die im Rahmen eines Cybersicherheitszertifizierungssystems gemäß der genannten Verordnung zertifiziert wurden oder für die eine Konformitätserklärung ausgestellt wurde und deren Fundstellen im Amtsblatt der Europäischen Union veröffentlicht wurden, davon ausgegangen werden, dass sie die Cybersicherheitsanforderungen dieser Verordnung erfüllen. Dies gilt unbeschadet des freiwilligen Charakters dieses Cybersicherheitszertifizierungssystems.

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

(63) Damit für die Betreiber möglichst wenig Aufwand entsteht und etwaige Doppelarbeit vermieden wird, sollte bei Hochrisiko-KI-Systemen im Zusammenhang mit Produkten, die nach dem neuen Rechtsrahmen unter bestehende Harmonisierungsrechtsvorschriften der Union fallen, im Rahmen der bereits in diesen Rechtsvorschriften vorgesehenen Konformitätsbewertung bewertet werden, ob diese KI-Systeme den Anforderungen dieser Verordnung genügen. Die Anwendbarkeit der Anforderungen dieser Verordnung sollte daher die besondere Logik, die Methodik oder die allgemeine Struktur der Konformitätsbewertung gemäß den einschlägigen spezifischen Rechtsvorschriften des neuen Rechtsrahmens unberührt lassen. Dieser Ansatz spiegelt sich voll und ganz in der Wechselwirkung zwischen dieser Verordnung und der [Maschinenverordnung] wider. Bei den Anforderungen in dieser Verordnung geht es um die Sicherheitsrisiken, die von KI-Systemen ausgehen, die Sicherheitsfunktionen in Maschinen steuern, wogegen bestimmte spezifische Anforderungen der [Maschinenverordnung] gewährleisten werden, dass ein KI-System auf sichere Weise in die gesamte Maschine integriert wird, damit die Sicherheit der Maschine insgesamt nicht beeinträchtigt wird. In der [Maschinenverordnung] wird der Begriff „KI-System“ genauso wie in dieser Verordnung definiert. Im Hinblick auf Hochrisiko-KI-Systeme im Zusammenhang mit Produkten, die unter die Verordnungen (EU) 2017/746 und (EU) 2017/746 über Medizinprodukte fallen, sollte die Anwendbarkeit der Anforderungen dieser Verordnung die Logik des Risikomanagements und die Nutzen-Risiko-Bewertung, die gemäß dem Rahmen für Medizinprodukte durchgeführt werden, unberührt lassen.

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

(65) Damit KI-Systeme, die zur biometrischen Fernidentifizierung von Personen verwendet werden sollen, einer Konformitätsbewertung durch Dritte unterzogen werden können, sollten die notifizierten Stellen gemäß dieser Verordnung von den zuständigen nationalen Behörden notifiziert werden, sofern sie eine Reihe von Anforderungen erfüllen, insbesondere in Bezug auf Unabhängigkeit, Kompetenz und Nichtvorliegen von Interessenkonflikten. Die Notifizierung dieser Stellen sollte von den zuständigen nationalen Behörden der Kommission und den anderen Mitgliedstaaten mittels dem von der Kommission entwickelten und verwalteten elektronischen Notifizierungsinstrument gemäß Artikel R23 des Beschlusses 768/2008 übermittelt werden.

(66) Im Einklang mit dem allgemein anerkannten Begriff der wesentlichen Änderung von Produkten, für die Harmonisierungsvorschriften der Union gelten, ist es angebracht, dass das KI-System bei jeder Änderung, die die Einhaltung dieser Verordnung durch das Hochrisiko-KI-System beeinträchtigen könnte (z. B. Änderung des Betriebssystems oder der Softwarearchitektur), oder wenn sich die Zweckbestimmung des Systems ändert, als neues KI-System betrachtet werden sollte, das einer neuen Konformitätsbewertung unterzogen werden sollte. Änderungen, die den Algorithmus und die Leistung von KI-Systemen, die nach dem Inverkehrbringen oder der Inbetriebnahme weiterhin dazulernen (d. h. sie passen automatisch an, wie die Funktionen ausgeführt werden), sollten jedoch keine wesentliche Änderung darstellen, sofern diese Änderungen vom Anbieter vorab festgelegt und zum Zeitpunkt der Konformitätsbewertung bewertet wurden.

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

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

(69) Um die Arbeit der Kommission und der Mitgliedstaaten im Bereich der künstlichen Intelligenz zu erleichtern und die Transparenz gegenüber der Öffentlichkeit zu erhöhen, sollten Anbieter von Hochrisiko-KI-Systemen, die nicht mit Produkten in Verbindung stehen, die unter die einschlägigen Harmonisierungsrechtsvorschriften der Union fallen, dazu verpflichtet werden, sich und Informationen über ihr Hochrisiko-KI-System in einer von der Kommission einzurichtenden und zu verwaltenden EU-Datenbank zu registrieren. Vor der Verwendung eines in Anhang III aufgeführten Hochrisiko-KI-Systems registrieren sich Nutzer von Hochrisiko-KI-Systemen, die Behörden, Einrichtungen oder sonstige Stellen sind, mit Ausnahme von Strafverfolgungs-, Grenzschutz-, Einwanderungs- oder Asylbehörden, sowie Behörden, die Nutzer von Hochrisiko-KI-Systemen im Bereich der kritischen Infrastruktur sind, in einer solchen Datenbank und wählen das System aus, dessen Verwendung sie planen. Die Kommission sollte im Einklang mit der Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates[26] 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.

[26] 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).

(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 Pflichten 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 aus Sicht einer normal informierten, angemessen aufmerksamen, verständigen natürlichen Person aufgrund der Umstände und des Kontexts der Nutzung offensichtlich. Bei der Umsetzung dieser Pflicht sollten die Merkmale von Personen, die aufgrund ihres Alters oder einer Behinderung einer schutzbedürftigen Gruppe angehören, berücksichtigt werden, soweit das KI-System auch mit diesen Gruppen interagieren soll. Darüber hinaus sollten natürlichen Personen informiert werden, wenn sie Systemen ausgesetzt sind, die durch die Verarbeitung ihrer biometrischen Daten die Gefühle oder Absichten dieser Personen identifizieren oder ableiten oder sie bestimmten Kategorien zuordnen können. Solche spezifischen Kategorien können Aspekte wie Geschlecht, Alter, Haarfarbe, Augenfarbe, Tätowierungen, persönliche Merkmale, ethnische Herkunft, persönliche Vorlieben und Interessen und andere Aspekte wie sexuelle oder politische Orientierung betreffen. 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. Die Einhaltung der oben genannten Informationspflichten sollte nicht als Hinweis darauf ausgelegt werden, dass die Verwendung des Systems oder seiner Ergebnisse nach dieser Verordnung oder anderen Rechtsvorschriften der Union und der Mitgliedstaaten rechtmäßig ist, und sollte andere Transparenzpflichten für Nutzer von KI-Systemen, die im Unionsrecht oder im nationalen Recht festgelegt sind, unberührt lassen. Sie sollte ferner auch nicht so ausgelegt werden, dass sie darauf hindeutet, dass die Verwendung des Systems oder seiner Ergebnisse das Recht auf freie Meinungsäußerung und das Recht auf Freiheit der Kunst und Wissenschaft, die in der Charta der Grundrechte der EU garantiert sind, behindern, insbesondere wenn der Inhalt Teil eines offensichtlich kreativen, satirischen, künstlerischen oder fiktionalen Werks oder Programms ist, vorbehalten angemessener Schutzvorkehrungen für die Rechte und Freiheiten Dritter.

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

(72) Die Ziele der KI-Reallabore sollten darin bestehen, Innovationen im Bereich KI zu fördern, indem eine kontrollierte Versuchs- und Testumgebung für die Entwicklungsphase und die dem Inverkehrbringen vorgelagerte Phase geschaffen wird, um sicherzustellen, dass die innovativen KI-Systeme mit dieser Verordnung und anderen einschlägigen Rechtsvorschriften der Union und der Mitgliedstaaten in Einklang stehen. Darüber hinaus sollen sie die Rechtssicherheit für Innovatoren sowie die Aufsicht und das Verständnis der zuständigen Behörden in Bezug auf die Möglichkeiten, neu auftretenden Risiken und der Auswirkungen der KI-Nutzung verbessern und den Marktzugang beschleunigen, unter anderem indem Hindernisse für kleine und mittlere Unternehmen (KMU), einschließlich Start-up-Unternehmen, abgebaut werden. Die Beteiligung am KI-Reallabor sollte sich auf Fragen konzentrieren, die zu Rechtsunsicherheit für Anbieter und zukünftige Anbieter führen, damit sie Innovationen vornehmen, mit KI in der Union experimentieren und zu faktengestütztem regulatorischen Lernen beitragen. Die Beaufsichtigung der KI-Systeme im KI-Reallabor sollte sich daher auf deren Entwicklung, Training, Testen und Validierung vor dem Inverkehrbringen oder der Inbetriebnahme der Systeme sowie auf das Konzept und das Auftreten wesentlicher Änderungen erstrecken, die möglicherweise ein neues Konformitätsbewertungsverfahren erfordern. Gegebenenfalls sollten die zuständigen nationalen Behörden, die KI-Reallabore einrichten, mit anderen einschlägigen Behörden zusammenarbeiten, einschließlich denjenigen, die den Schutz der Grundrechte überwachen, und könnten die Einbeziehung anderer Akteure innerhalb des KI-Ökosystems gestatten, wie etwa nationaler oder europäischer Normungsorganisationen, notifizierter Stellen, Test- und Versuchseinrichtungen, Forschungs- und Versuchslabore, Innovationszentren und einschlägiger Interessenträger und Organisationen der Zivilgesellschaft. 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. KI-Reallabore, die im Rahmen dieser Verordnung eingerichtet wurden, sollten andere Rechtsvorschriften, die die Einrichtung anderer Reallabore ermöglichen, unberührt lassen, um die Einhaltung anderer Rechtsvorschriften als dieser Verordnung sicherzustellen. Gegebenenfalls sollten die für diese anderen Reallabore zuständigen Behörden die Vorteile der Nutzung dieser Reallabore auch zum Zweck der Gewährleistung der Konformität der KI-Systeme mit dieser Verordnung berücksichtigen. Im Einvernehmen zwischen den zuständigen nationalen Behörden und den Beteiligten des KI-Reallabors können Tests unter realen Bedingungen auch im Rahmen des KI-Reallabors durchgeführt und beaufsichtigt werden.

(-72a) Die vorliegende Verordnung sollte im Einklang mit Artikel 6 Absatz 4 und Artikel 9 Absatz 2 Buchstabe g der Verordnung (EU) 2016/679 und den Artikeln 5 und 10 der Verordnung (EU) 2018/1725 sowie unbeschadet des Artikels 4 Absatz 2 und des Artikels 10 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 durch die Beteiligten des KI-Reallabors bilden. Alle anderen Pflichten der Verantwortlichen und Rechte betroffener Personen im Rahmen der Verordnung (EU) 2016/679, Verordnung (EU) 2018/1725 und Richtlinie (EU) 2016/680 gelten weiterhin. Insbesondere sollte diese Verordnung keine Rechtsgrundlage im Sinne von Artikel 22 Absatz 2 Buchstabe b der Verordnung (EU) 2016/679 und Artikel 24 Absatz 2 Buchstabe b der Verordnung (EU) 2018/1725 bilden. Die am Reallabor Beteiligten sollten angemessene Schutzvorkehrungen treffen und mit den zuständigen Behörden zusammenarbeiten, unter anderem indem sie deren Anweisungen befolgen und zügig und nach Treu und Glauben handeln, um etwaige hohe Risiken für die Sicherheit und die Grundrechte, die bei der Entwicklung und Erprobung im Reallabor auftreten können, zu mindern. Das Verhalten der am Reallabor Beteiligten sollte berücksichtigt werden, wenn die zuständigen Behörden entscheiden, ob sie eine Geldbuße gemäß Artikel 83 Absatz 2 der Verordnung (EU) 2016/679 und Artikel 57 der Richtlinie (EU) 2016/680 verhängen.

(72a) Um den Prozess der Entwicklung und des Inverkehrbringens der in Anhang III aufgeführten Hochrisiko-KI-Systeme zu beschleunigen, ist es wichtig, dass Anbieter oder zukünftige Anbieter solcher Systeme auch von einer spezifischen Regelung für das Testen dieser Systeme unter realen Bedingungen profitieren können, ohne sich an einem KI-Reallabor zu beteiligen. In solchen Fällen und unter Berücksichtigung der möglichen Folgen solcher Tests für Einzelpersonen sollte jedoch sichergestellt werden, dass mit der Verordnung angemessene und ausreichende Garantien und Bedingungen für Anbieter oder zukünftige Anbieter eingeführt werden. Diese Garantien sollten unter anderem die Einholung der sachkundigen Einwilligung natürlicher Personen in die Beteiligung an Tests in realen Bedingungen umfassen, mit Ausnahme der Strafverfolgung in Fällen, in denen die Einholung der sachkundigen Einwilligung verhindern würde, dass das KI-System getestet wird. Die Einwilligung der Testteilnehmer zur Teilnahme an solchen Tests im Rahmen dieser Verordnung unterscheidet sich von der Einwilligung betroffener Personen in die Verarbeitung ihrer personenbezogenen Daten nach den einschlägigen Datenschutzvorschriften und lässt diese Einwilligung unberührt.

(73) Um Innovationen zu fördern und zu schützen, ist es wichtig, die Interessen von Anbietern und Nutzern von KI-Systemen, bei denen es sich um KMU handelt, besonders zu berücksichtigen. Zu diesem Zweck sollten die Mitgliedstaaten Initiativen ergreifen, die sich an diese Akteure richten, darunter auch Sensibilisierungs- und Informationsmaßnahmen. Darüber hinaus sind die besonderen Interessen und Bedürfnisse von Anbietern, bei denen es sich um KMU handelt, bei der Festlegung der Gebühren für die Konformitätsbewertung durch die notifizierten Stellen zu berücksichtigen. Übersetzungen im Zusammenhang mit der verpflichtenden Dokumentation und Kommunikation mit Behörden können für Anbieter und andere Akteure, insbesondere den kleineren unter ihnen, erhebliche Kosten verursachen. Die Mitgliedstaaten sollten möglichst dafür sorgen, dass eine der Sprachen, die sie für die einschlägige Dokumentation der Anbieter und für die Kommunikation mit den Akteuren bestimmen und akzeptieren, eine Sprache ist, die von der größtmöglichen Zahl grenzüberschreitender Nutzer weitgehend verstanden wird.

(73a) Um Innovationen zu fördern und zu schützen, sollten die KI-Abruf-Plattform, alle einschlägigen EU-Finanzierungsprogramme und -projekte, wie das Programm „Digitales Europa“ und Horizont Europa, die von der Kommission und den Mitgliedstaaten auf nationaler oder EU-Ebene durchgeführt werden, zur Verwirklichung der Ziele dieser Verordnung beitragen.

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

(74a) Um die Verhältnismäßigkeit angesichts der sehr geringen Größe einiger Akteure in Bezug auf die Innovationskosten sicherzustellen, ist es darüber hinaus angezeigt, Kleinstunternehmen von den kostspieligsten Pflichten auszunehmen, beispielsweise von der Einführung eines Qualitätsmanagementsystems, was den Verwaltungsaufwand und die Kosten für diese Unternehmen verringern würde, ohne das Schutzniveau und die Notwendigkeit der Einhaltung der Anforderungen für Hochrisiko-KI-Systeme zu beeinträchtigen.

(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 Test- und Versuchseinrichtungen erleichtert. Dies gilt insbesondere für Expertengremien, Fachlaboratorien und Referenzlaboratorien im Bereich Medizinprodukte gemäß der Verordnung (EU) 2017/745 und der Verordnung (EU) 2017/746.

(76) Um eine reibungslose, wirksame und harmonisierte Umsetzung dieser Verordnung zu erleichtern, sollte ein Europäischer Ausschuss für künstliche Intelligenz (KI-Ausschuss) eingerichtet werden. Der KI-Ausschuss sollte die verschiedenen Interessen des KI-Ökosystems widerspiegeln und sich aus Vertretern der Mitgliedstaaten zusammensetzen. Um die Einbeziehung der einschlägigen Interessenträger sicherzustellen, sollte eine ständige Untergruppe des KI-Ausschusses eingerichtet werden. Der KI-Ausschuss sollte für eine Reihe von Beratungsaufgaben zuständig sein und Stellungnahmen, Empfehlungen, Ratschläge oder Beiträge zu Leitlinien zu Fragen im Zusammenhang mit der Umsetzung dieser Verordnung abgeben, darunter zu Durchsetzungsfragen, technischen Spezifikationen oder bestehenden Normen in Bezug auf die in dieser Verordnung festgelegten Anforderungen; außerdem sollte er die Kommission und die Mitgliedstaaten und ihre zuständigen nationalen Behörden in spezifischen Fragen im Zusammenhang mit künstlicher Intelligenz beraten. Um den Mitgliedstaaten eine gewisse Flexibilität bei der Benennung ihrer Vertreter im KI-Ausschuss zu geben, können diese Vertreter alle Personen sein, die öffentlichen Stellen angehören, die über einschlägige Zuständigkeiten und Befugnisse verfügen sollten, um die Koordinierung auf nationaler Ebene zu erleichtern und zur Erfüllung der Aufgaben des KI-Ausschusses beizutragen. Der KI-Ausschuss sollte zwei ständige Untergruppen einrichten, um Marktüberwachungsbehörden und notifizierenden Behörden für die Zusammenarbeit und den Austausch in Fragen, die die Marktaufsicht bzw. notifizierende Behörden betreffen, eine Plattform zu bieten. Die ständige Untergruppe für Marktüberwachung sollte für diese Verordnung als Gruppe für die Verwaltungszusammenarbeit (ADCO-Gruppe) im Sinne des Artikels 30 der Verordnung (EU) 2019/1020 fungieren. Im Einklang mit der Rolle und den Aufgaben der Kommission gemäß Artikel 33 der Verordnung (EU) 2019/1020 sollte die Kommission die Tätigkeiten der ständigen Untergruppe für Marktüberwachung durch die Durchführung von Marktbewertungen oder -untersuchungen unterstützen, insbesondere im Hinblick auf die Ermittlung von Aspekten dieser Verordnung, die eine spezifische und dringende Koordinierung zwischen den Marktüberwachungsbehörden erfordern. Der KI-Ausschuss kann weitere ständige oder nichtständige Untergruppen einrichten, falls das für die Prüfung bestimmter Fragen zweckmäßig sein sollte. Der KI-Ausschuss sollte gegebenenfalls auch mit den einschlägigen Einrichtungen, Sachverständigengruppen und Netzwerken der EU zusammenarbeiten, die im Zusammenhang mit den einschlägigen EU-Rechtsvorschriften tätig sind, einschließlich insbesondere denjenigen, die im Rahmen der einschlägigen EU-Verordnungen über Daten, digitale Produkte und Dienstleistungen tätig sind.

(76a) Die Kommission sollte die Mitgliedstaaten und Akteure aktiv bei der Umsetzung und Durchsetzung dieser Verordnung unterstützen. In diesem Hinblick sollte sie Leitlinien zu bestimmten Themen ausarbeiten, um die Anwendung dieser Verordnung zu erleichtern, wobei den Bedürfnissen von KMU und Start-up-Unternehmen in den am wahrscheinlichsten betroffenen Sektoren besondere Aufmerksamkeit zu widmen ist. Um eine angemessene Durchsetzung und die Kapazitäten der Mitgliedstaaten zu unterstützen, sollten Unionsprüfeinrichtungen zu KI und ein Pool einschlägiger Sachverständiger eingerichtet und den Mitgliedstaaten zur Verfügung gestellt werden.

(77) Den Mitgliedstaaten kommt bei der Anwendung und Durchsetzung dieser Verordnung eine Schlüsselrolle zu. Dazu sollte jeder Mitgliedstaat eine oder mehrere zuständige nationale Behörden benennen, die die Anwendung und Umsetzung dieser Verordnung beaufsichtigen. Die Mitgliedstaaten können beschließen, öffentliche Einrichtungen jeder Art zu benennen, die die Aufgaben der zuständigen nationalen Behörden im Sinne dieser Verordnung im Einklang mit ihren spezifischen nationalen organisatorischen Merkmalen und Bedürfnissen wahrnehmen.

(78) Damit Anbieter von Hochrisiko-KI-Systemen die Erfahrungen mit der Verwendung von Hochrisiko-KI-Systemen bei der Verbesserung ihrer Systeme und im Konzeptions- und Entwicklungsprozess berücksichtigen oder rechtzeitig etwaige Korrekturmaßnahmen ergreifen können, sollten alle Anbieter über ein System zur Beobachtung nach dem Inverkehrbringen verfügen. Dieses System ist auch wichtig, damit den möglichen Risiken, die von KI-Systemen ausgehen, die nach dem Inverkehrbringen oder der Inbetriebnahme dazulernen, wirksamer und zeitnah begegnet werden kann. In diesem Zusammenhang sollten die Anbieter auch verpflichtet sein, ein System einzurichten, um den zuständigen Behörden schwerwiegende Vorfälle zu melden, die sich aus der Verwendung ihrer KI-Systeme ergeben.

(79) Zur Gewährleistung einer angemessenen und wirksamen Durchsetzung der Anforderungen und Pflichten 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. Die gemäß dieser Verordnung benannten Marktüberwachungsbehörden sollten über alle Durchsetzungsbefugnisse gemäß dieser Verordnung und der Verordnung (EU) 2019/1020 verfügen und ihre Befugnisse und Aufgaben unabhängig, unparteiisch und unvoreingenommen wahrnehmen. Obwohl die meisten KI-Systeme keinen spezifischen Anforderungen und Pflichten gemäß dieser Verordnung unterliegen, können die Marktüberwachungsbehörden Maßnahmen in Bezug auf alle KI-Systeme ergreifen, wenn sie ein Risiko gemäß dieser Verordnung darstellen. Aufgrund des spezifischen Charakters der Organe, Einrichtungen und sonstigen Stellen der Union, die in den Anwendungsbereich dieser Verordnung fallen, ist es angezeigt, dass der Europäische Datenschutzbeauftragte als eine zuständige Marktüberwachungsbehörde für sie benannt wird. Die Benennung zuständiger nationaler Behörden durch die Mitgliedstaaten sollte davon unberührt bleiben. Die Marktüberwachungstätigkeiten sollten die Fähigkeit der beaufsichtigen Unternehmen, ihre Aufgaben unabhängig wahrzunehmen, nicht beeinträchtigen, wenn eine solche Unabhängigkeit nach dem Unionsrecht erforderlich ist.

(79a) Diese Verordnung berührt nicht die Zuständigkeiten, Aufgaben, Befugnisse und Unabhängigkeit der einschlägigen nationalen Behörden oder Stellen, die die Anwendung des Unionsrechts zum Schutz der Grundrechte überwachen, einschließlich Gleichstellungsstellen und Datenschutzbehörden. Sofern dies für die Erfüllung ihres Auftrags erforderlich ist, sollten auch diese nationalen Behörden oder Stellen Zugang zu der gesamten im Rahmen dieser Verordnung erstellten Dokumentation haben. Es sollte ein spezifisches Schutzklauselverfahren festgelegt werden, um eine angemessene und zeitnahe Durchsetzung gegenüber KI-Systemen, die ein Risiko für die Gesundheit, Sicherheit und Grundrechte bergen, sicherzustellen. Das Verfahren für solche KI-Systeme, die ein Risiko bergen, sollte auf Hochrisiko-KI-Systeme, von denen ein Risiko ausgeht, auf verbotene Systeme, die unter Verstoß gegen die in dieser Verordnung festgelegten verbotenen Praktiken in Verkehr gebracht, in Betrieb genommen oder verwendet wurden, sowie auf KI-Systeme, die unter Verstoß der Transparenzanforderungen dieser Verordnung bereitgestellt wurden und ein Risiko bergen, angewandt werden.

(80) Die Rechtsvorschriften der Union über Finanzdienstleistungen enthalten Vorschriften und Anforderungen für die interne Unternehmensführung und das Risikomanagement, die für regulierte Finanzinstitute bei der Erbringung solcher Dienstleistungen gelten, auch wenn sie KI-Systeme verwenden. Um eine kohärente Anwendung und Durchsetzung der Pflichten aus dieser Verordnung sowie der einschlägigen Vorschriften und Anforderungen der Rechtsvorschriften der Union für Finanzdienstleistungen zu gewährleisten, sollten die für die Beaufsichtigung und Durchsetzung der Rechtsvorschriften im Bereich der Finanzdienstleistungen zuständigen Behörden auch als zuständige Behörden für die Überwachung der Umsetzung dieser Verordnung, einschließlich der Marktüberwachungstätigkeiten, in Bezug auf von regulierten und beaufsichtigten Finanzinstituten bereitgestellte oder verwendete KI-Systeme benannt werden, es sei denn, die Mitgliedstaaten beschließen, eine andere Behörde zu benennen, um diese Marktüberwachungsaufgaben wahrzunehmen. Diese zuständigen Behörden sollten alle Befugnisse gemäß dieser Verordnung und der Verordnung (EU) 2019/1020 über die Marktüberwachung haben, um die Anforderungen und Pflichten der vorliegenden Verordnung durchzusetzen, einschließlich Befugnisse zur Durchführung von Ex-post-Marktüberwachungstätigkeiten, die gegebenenfalls in ihre bestehenden Aufsichtsmechanismen und -verfahren im Rahmen der einschlägigen Rechtsvorschriften der Union über Finanzdienstleistungen integriert werden können. Es ist angezeigt, vorzusehen, dass die nationalen Behörden, die auf der Grundlage der Richtlinie 2013/36/EU für die Aufsicht über regulierte Kreditinstitute zuständig sind und die an dem mit der Verordnung (EU) Nr. 1024/2013 des Rates eingerichteten einheitlichen Aufsichtsmechanismus teilnehmen, in ihrer Funktion als Marktüberwachungsbehörden gemäß der vorliegenden Verordnung der Europäischen Zentralbank unverzüglich alle im Zuge ihrer Marktüberwachungstätigkeiten ermittelten Informationen übermitteln, die für die in der genannten Verordnung festgelegten Aufsichtsaufgaben der Europäischen Zentralbank von Belang sein könnten. Um die Kohärenz zwischen dieser Verordnung und den Vorschriften für Kreditinstitute, die unter die Richtlinie 2013/36/EU des Europäischen Parlaments und des Rates[27] fallen, weiter zu verbessern, ist es ferner angezeigt, einige verfahrenstechnische Anbieterpflichten in Bezug auf das Risikomanagement, die Beobachtung nach dem Inverkehrbringen und die Dokumentation in die bestehenden Pflichten und Verfahren gemäß der Richtlinie 2013/36/EU aufzunehmen. Zur Vermeidung von Überschneidungen sollten auch begrenzte Ausnahmen in Bezug auf das Qualitätsmanagementsystem der Anbieter und die Beobachtungspflichten der Nutzer von Hochrisiko-KI-Systemen in Betracht gezogen

[27] 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).

werden, soweit diese Kreditinstitute betreffen, die unter die Richtlinie 2013/36/EU fallen. Die gleiche Regelung sollte für Versicherungs- und Rückversicherungsunternehmen und Versicherungsholdinggesellschaften gemäß der Richtlinie 2009/138/EG (Solvabilität II) und Versicherungsvermittler gemäß der Richtlinie 2016/97/EU sowie für andere Arten von Finanzinstituten gelten, die Anforderungen in Bezug ihre Regelungen oder Verfahren der internen Unternehmensführung unterliegen, die gemäß den einschlägigen Rechtsvorschriften der Union über Finanzdienstleistungen festgelegt wurden, um Kohärenz und Gleichbehandlung im Finanzsektor sicherzustellen.

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

(82) Es ist wichtig, dass KI-Systeme im Zusammenhang mit Produkten, die gemäß dieser Verordnung kein hohes Risiko bergen und daher nicht die in dieser Verordnung festgelegten Anforderungen erfüllen müssen, dennoch sicher sind, wenn sie in Verkehr gebracht oder in Betrieb genommen werden. Um zu diesem Ziel beizutragen, würde die Richtlinie 2001/95/EG des Europäischen Parlaments und des Rates[28] als Sicherheitsnetz dienen.

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

---

28 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).

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

(85) Damit der Rechtsrahmen erforderlichenfalls angepasst werden kann, sollte der Kommission die Befugnis übertragen werden, gemäß Artikel 290 AEUV Rechtsakte zur Änderung der in Anhang II aufgeführten Harmonisierungsrechtsvorschriften der Union, der in Anhang III aufgeführten Hochrisiko-KI-Systeme, der Bestimmungen über die technische Dokumentation in Anhang IV, des Inhalts der EU-Konformitätserklärung in Anhang V, der Bestimmungen über die Konformitätsbewertungsverfahren in den Anhängen VI und VII und der Bestimmungen zur Festlegung der Hochrisiko-KI-Systeme zu erlassen, für die das Konformitätsbewertungsverfahren auf der Grundlage der Bewertung des Qualitätsmanagementsystems und der technischen Dokumentation gelten sollte. Es ist von besonderer Bedeutung, dass die Kommission im Zuge ihrer Vorbereitungsarbeit angemessene Konsultationen, auch auf der Ebene von Sachverständigen, durchführt, die mit den Grundsätzen in Einklang stehen, die in der Interinstitutionellen Vereinbarung vom 13. April 2016 über bessere Rechtsetzung[29] niedergelegt wurden. Um insbesondere für eine gleichberechtigte Beteiligung an der Vorbereitung delegierter Rechtsakte zu sorgen, erhalten das Europäische Parlament und der Rat alle Dokumente zur gleichen Zeit wie die Sachverständigen der Mitgliedstaaten, und ihre Sachverständigen haben systematisch Zugang zu den Sitzungen der Sachverständigengruppen der Kommission, die mit der Vorbereitung der delegierten Rechtsakte befasst sind. Solche Konsultationen und beratende Unterstützung sollten auch im Rahmen der Tätigkeiten des KI-Ausschusses und seiner Untergruppen durchgeführt werden.

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

(86) Zur Gewährleistung einheitlicher Bedingungen für die Umsetzung dieser Verordnung sollten der Kommission Durchführungsbefugnisse übertragen werden. Diese Befugnisse sollten im Einklang mit der Verordnung (EU) Nr. 182/2011 des Europäischen Parlaments und des Rates[30] ausgeübt werden. Es ist von besonderer Bedeutung, dass die Kommission im Einklang mit den Grundsätzen, die in der Interinstitutionellen Vereinbarung vom 13. April 2016 über bessere Rechtsetzung niedergelegt sind, in Fällen, in denen für die frühzeitige Ausarbeitung von Entwürfen von Durchführungsrechtsakten umfassenderes Fachwissen erforderlich ist, Sachverständigengruppen einsetzt, anvisierte Interessenträger konsultiert oder gegebenenfalls öffentliche Konsultationen durchführt. Solche Konsultationen und beratende Unterstützung sollten auch im Rahmen der Tätigkeiten des KI-Ausschusses und seiner Untergruppen durchgeführt werden, einschließlich der Ausarbeitung von Durchführungsrechtsakten im Zusammenhang mit den Artikeln 4, 4b und 6.

(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) Um Rechtssicherheit zu gewährleisten, einen angemessenen Anpassungszeitraum für die Akteure sicherzustellen und Marktstörungen zu vermeiden, unter anderem durch Gewährleistung der Kontinuität der Verwendung von KI-Systemen, ist es angezeigt, dass diese Verordnung nur dann für die Hochrisiko-KI-Systeme, die vor dem allgemeinen Anwendungsbeginn dieser Verordnung in Verkehr gebracht oder in Betrieb genommen wurden, gilt, wenn diese Systeme ab diesem Datum erheblichen Veränderungen in Bezug auf ihre Konzeption oder Zweckbestimmung unterliegen. Es sollte klargestellt werden, dass der Begriff der erhebliche Veränderung in diesem Hinblick als gleichwertig mit dem Begriff der wesentlichen Änderung verstanden werden sollte, der nur in Bezug auf Hochrisiko-KI-Systeme im Sinne dieser Verordnung verwendet wird.

---

[30] 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).

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

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

HABEN FOLGENDE VERORDNUNG ERLASSEN:

TITEL I

ALLGEMEINE BESTIMMUNGEN

Artikel 1

Gegenstand

In dieser Verordnung wird Folgendes festgelegt:

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

a) Verbote bestimmter Praktiken im Bereich der künstlichen Intelligenz;

b) besondere Anforderungen an Hochrisiko-KI-Systeme und Verpflichtungen für Akteure in Bezug auf solche Systeme;

c) harmonisierte Transparenzvorschriften für bestimmte KI-Systeme;

d) Vorschriften für die Marktbeobachtung, Marktüberwachung und Governance;

e) Maßnahmen zur Innovationsförderung.

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 physisch anwesend oder niedergelassen sind;

b) Nutzer von KI-Systemen, die in der Union physisch anwesend oder niedergelassen sind;

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

d) Einführer und Händler von KI-Systemen;

e) Produkthersteller, die KI-Systeme zusammen mit ihrem Produkt unter ihrem Namen oder ihrer Handelsmarke in Verkehr bringen oder in Betrieb nehmen;

f) Bevollmächtigte von Anbietern, die in der Union niedergelassen sind.

(2) Für KI-Systeme, die als Hochrisiko-KI-Systeme gemäß Artikel 6 Absätze 1 und 2 eingestuft sind und sich auf Produkte beziehen, die unter die in Anhang II Abschnitt B aufgeführten Harmonisierungsrechtsvorschriften der Union fallen, gilt nur Artikel 84 dieser Verordnung. Artikel 53 gilt nur, soweit die Anforderungen an Hochrisiko-KI-Systeme gemäß dieser Verordnung im Rahmen der genannten Harmonisierungsrechtsvorschriften der Union eingebunden wurden.

(3) Diese Verordnung gilt nicht für KI-Systeme, wenn und soweit sie mit oder ohne Änderungen für die Zwecke von Tätigkeiten, die nicht in den Anwendungsbereich des Unionsrechts fallen, in Verkehr gebracht, in Betrieb genommen oder verwendet werden, und in keinem Fall für Tätigkeiten in Bezug auf militärische Angelegenheiten, Verteidigung und nationale Sicherheit, unabhängig von der Art der Einrichtung, die diese Tätigkeiten ausübt.

Darüber hinaus gilt diese Verordnung nicht für KI-Systeme, die nicht in der Union in Verkehr gebracht oder in Betrieb genommen werden, wenn die Ergebnisse in der Union für die Zwecke von Tätigkeiten, die nicht in den Anwendungsbereich des Unionsrechts fallen, verwendet werden, und in keinem Fall für Tätigkeiten in Bezug auf militärische Angelegenheiten, Verteidigung und nationale Sicherheit, unabhängig von der Art der Einrichtung, die diese Tätigkeiten ausübt.

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

(5) Die Anwendung der Bestimmungen über die Verantwortlichkeit der Vermittler in Kapitel II Abschnitt 4 der Richtlinie 2000/31/EG des Europäischen Parlaments und des Rates[31] [*die durch die entsprechenden Bestimmungen des Gesetzes über digitale Dienste ersetzt werden sollen*] bleibt von dieser Verordnung unberührt.

(6) Diese Verordnung gilt nicht für KI-Systeme und deren Ergebnisse, die eigens für den alleinigen Zweck der wissenschaftlichen Forschung und Entwicklung entwickelt und in Betrieb genommen werden.

(7) Diese Verordnung gilt nicht für Forschungs- und Entwicklungsaktivitäten zu KI-Systemen.

(8) Diese Verordnung gilt nicht für die Pflichten von Nutzern, die natürliche Personen sind und KI-Systeme im Rahmen einer ausschließlich persönlichen und nicht beruflichen Tätigkeit verwenden, mit Ausnahme von Artikel 52.

---

[31] 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

Begriffsbestimmungen

Für die Zwecke dieser Verordnung bezeichnet der Ausdruck

1. „System der künstlichen Intelligenz“ (KI-System) ein System, das so konzipiert ist, dass es mit Elementen der Autonomie arbeitet, und das auf der Grundlage maschineller und/oder vom Menschen erzeugter Daten und Eingaben durch maschinelles Lernen und/oder logik- und wissensgestützte Konzepte ableitet, wie eine Reihe von Zielen erreicht wird, und systemgenerierte Ergebnisse wie Inhalte (generative KI-Systeme), Vorhersagen, Empfehlungen oder Entscheidungen hervorbringt, die das Umfeld beeinflussen, mit dem die KI-Systeme interagieren;

1a. „Lebenszyklus eines KI-Systems“ die Laufzeit eines KI-Systems von der Konzeption bis zur Stilllegung. Unbeschadet der Befugnisse der Marktüberwachungsbehörden kann diese Stilllegung auf Beschluss des Anbieters zu jedem Zeitpunkt während der Beobachtungsphase nach dem Inverkehrbringen erfolgen; die Stilllegung bedeutet, dass das System nicht weiter verwendet werden darf. Ferner endet der Lebenszyklus eines KI-Systems durch eine wesentliche Änderung des KI-Systems, die vom Anbieter oder einer anderen natürlichen oder juristischen Person vorgenommen wurde; in diesem Fall gilt das wesentlich geänderte KI-System als ein neues KI-System;

1b. „KI-System mit allgemeinem Verwendungszweck“ ein KI-System, das – unabhängig davon, wie es in Verkehr gebracht oder in Betrieb genommen wird, auch in Form quelloffener Software – vom Anbieter dazu vorgesehen ist, allgemein anwendbare Funktionen wie Bild- oder Spracherkennung, Audio- und Videogenerierung, Mustererkennung, Beantwortung von Fragen, Übersetzung und Sonstiges auszuführen; dabei kann ein KI-System mit allgemeinem Verwendungszweck in einer Vielzahl von Kontexten eingesetzt und in eine Vielzahl anderer KI-Systeme integriert werden;

2. „Anbieter“ eine natürliche oder juristische Person, Behörde, Einrichtung oder sonstige Stelle, die ein KI-System entwickelt oder entwickeln lässt und dieses System unter dem eigenen Namen oder der eigenen Marke in Verkehr bringt oder in Betrieb nimmt, sei es entgeltlich oder unentgeltlich;

3. [gestrichen];

3a. „kleine und mittlere Unternehmen“ (KMU) Unternehmen im Sinne des Anhangs der Empfehlung 2003/361/EG der Kommission betreffend die Definition der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen;

4. „Nutzer“ eine natürliche oder juristische Person, einschließlich Behörden, Einrichtungen oder sonstige Stellen, unter deren Verantwortung das System verwendet wird;

5. „Bevollmächtigter“ eine in der Union physisch anwesende oder niedergelassene natürliche oder juristische Person, die vom Anbieter eines KI-Systems schriftlich dazu bevollmächtigt wurde und sich damit einverstanden erklärt hat, in seinem Namen die in dieser Verordnung festgelegten Pflichten zu erfüllen bzw. Verfahren durchzuführen;

5a. „Produkthersteller“ einen Hersteller im Sinne der in Anhang II aufgelisteten Harmonisierungsrechtsvorschriften der Union;

6. „Einführer“ eine in der Union physisch anwesende oder niedergelassene natürliche oder juristische Person, die ein KI-System, das den Namen oder die Marke einer außerhalb der Union niedergelassenen natürlichen oder juristischen Person trägt, in der Union in Verkehr bringt;

7. „Händler“ eine natürliche oder juristische Person in der Lieferkette, die ein KI-System auf dem Unionsmarkt bereitstellt, mit Ausnahme des Anbieters oder des Einführers;

8. „Akteur“ den Anbieter, den Produkthersteller, den Nutzer, den Bevollmächtigten, den Einführer oder den Händler;

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 in der Union zum Erstgebrauch direkt an den Nutzer oder zum Eigengebrauch entsprechend seiner Zweckbestimmung;

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

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

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

15. „Gebrauchsanweisungen“ die Informationen, die der Anbieter bereitstellt, um den Nutzer insbesondere über die Zweckbestimmung und die ordnungsgemäße Verwendung eines KI-Systems zu informieren;

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

17. „Rücknahme eines KI-Systems“ jede Maßnahme, mit der verhindert werden soll, dass ein in der Lieferkette befindliches KI-System auf dem Markt bereitgestellt wird;

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

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

20. „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;

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

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

23. „wesentliche Änderung“ eine Änderung des KI-Systems nach dessen Inverkehrbringen oder Inbetriebnahme, die sich auf die Konformität des KI-Systems mit den Anforderungen in Titel III Kapitel 2 dieser Verordnung auswirkt, oder eine Änderung der Zweckbestimmung, für die das KI-System geprüft wurde. 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;

24. „CE-Konformitätskennzeichnung“ (CE-Kennzeichnung) eine Kennzeichnung, durch die ein Anbieter erklärt, dass ein KI-System die Anforderungen erfüllt, die in Titel III Kapitel 2 oder in Artikel 4b dieser Verordnung und in anderen einschlägigen Rechtsakten der Union zur Harmonisierung der Bedingungen für die Vermarktung von Produkten („Harmonisierungsrechtsvorschriften der Union“), die die Anbringung dieser Kennzeichnung vorsehen, festgelegt sind;

25. „System zur Beobachtung nach dem Inverkehrbringen“ alle Tätigkeiten, die Anbieter von KI-Systemen zur Sammlung und Überprüfung von Erfahrungen mit der Verwendung 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 Spezifikation“ eine Reihe technischer Spezifikationen im Sinne von Artikel 2 Nummer 4 der Verordnung (EU) Nr. 1025/2012, deren Befolgung es ermöglicht, bestimmte Anforderungen 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 Überanpassung zu vermeiden; der Validierungsdatensatz kann ein separater Datensatz oder Teil des Trainingsdatensatzes mit fester oder variabler Aufteilung sein;

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

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

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

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

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

36. „biometrisches Fernidentifizierungssystem“ ein KI-System, das dem Zweck dient, natürliche Personen in der Regel aus der Ferne und ohne ihre aktive Einbeziehung durch Abgleich der biometrischen Daten einer Person mit den in einem Referenzdatenregister gespeicherten biometrischen Daten zu identifizieren;

37. „biometrisches Echtzeit-Fernidentifizierungssystem“ ein biometrisches Fernidentifizierungssystem, bei dem die Erfassung biometrischer Daten, der Abgleich und die Identifizierung zeitgleich oder nahezu zeitgleich erfolgen;

38. [gestrichen];

39. „öffentlich zugänglicher Raum“ einen einer unbestimmten Anzahl natürlicher Personen zugänglichen physischen Ort in privatem oder öffentlichem Eigentum, unabhängig davon, ob vorher bestimmte Bedingungen oder Umstände für den Zugang festgelegt wurden, 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. [gestrichen];

43. „zuständige nationale Behörde“ die folgenden Behörden: die notifizierende Behörde und die Marktüberwachungsbehörde. In Bezug auf KI-Systeme, die von Organen, Einrichtungen und sonstigen Stellen der EU in Betrieb genommen oder verwendet werden, übernimmt der Europäische Datenschutzbeauftragte die Zuständigkeiten, die in den Mitgliedstaaten den zuständigen nationalen Behörden zugewiesen werden, und jede Bezugnahme auf die zuständigen nationalen Behörden oder Marktüberwachungsbehörden in dieser Verordnung ist gegebenenfalls als Bezugnahme auf den Europäischen Datenschutzbeauftragten zu verstehen;

44. „schwerwiegender Vorfall“ ein Vorkommnis oder eine Fehlfunktion eines KI-Systems, das bzw. die direkt oder indirekt eine der nachstehenden Folgen hat:

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

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

c) den Verstoß gegen die Verpflichtungen aus den Bestimmungen des Unionsrechts zum Schutz der Grundrechte,

d) schwere Sach- oder Umweltschäden;

45. „kritische Infrastruktur“ einen Vermögenswert, ein System oder einen Teil davon, der bzw. das zur Bereitstellung einer Dienstleistung erforderlich ist, die zur Aufrechterhaltung der grundlegenden gesellschaftlichen Funktionen oder wirtschaftlichen Aktivitäten im Sinne von Artikel 2 Absätze 4 und 5 der Richtlinie XXXX/XXXX über die Resilienz kritischer Einrichtungen von wesentlicher Bedeutung ist;

46. „personenbezogene Daten“ Daten im Sinne von Artikel 4 Nummer 1 der Verordnung (EU) 2016/679;

47. „nicht personenbezogene Daten“ Daten, die keine personenbezogenen Daten im Sinne des Artikels 4 Nummer 1 der Verordnung (EU) 2016/679 sind;

48. „Test unter realen Bedingungen“ den befristeten Test eines KI-Systems auf seine Zweckbestimmung, der unter realen Bedingungen außerhalb eines Labors oder einer anderweitig simulierten Umgebung erfolgt, um zuverlässige und belastbare Daten zu erheben und die Konformität des KI-Systems mit den Anforderungen dieser Verordnung zu bewerten und zu überprüfen. Tests unter realen Bedingungen gelten nicht als Inverkehrbringen oder Inbetriebnahme des KI-Systems im Sinne dieser Verordnung, sofern alle Bedingungen nach Artikel 53 oder Artikel 54a erfüllt sind;

49. „Plan für Tests unter realen Bedingungen“ ein Dokument, in dem die Ziele, die Methode, der geografische, bevölkerungsbezogene und zeitliche Umfang, die Überwachung, Organisation und Durchführung von Tests unter realen Bedingungen beschrieben werden;

50. „Testteilnehmer“ für die Zwecke der Tests unter realen Bedingungen eine natürliche Person, die an den Tests unter realen Bedingungen teilnimmt;

51. „sachkundige Einwilligung“ eine aus freien Stücken erfolgende, freiwillige Erklärung der Bereitschaft, an einem bestimmten Test unter realen Bedingungen teilzunehmen, durch einen Testteilnehmer, nachdem dieser über alle Aspekte des Tests, die für die Entscheidungsfindung bezüglich der Teilnahme relevant sind, aufgeklärt wurde; im Falle von Minderjährigen und nicht einwilligungsfähigen Personen wird die sachkundige Einwilligung von ihrem gesetzlichen Vertreter erteilt;

52. „KI-Reallabor“ einen konkreten Rahmen, der von einer zuständigen nationalen Behörde geschaffen wird und den Anbieter oder zukünftige Anbieter von KI-Systemen nach einem spezifischen Plan für einen begrenzten Zeitraum und unter regulatorischer Aufsicht nutzen können, um ein innovatives KI-System zu entwickeln, zu trainieren, zu validieren und – gegebenenfalls unter realen Bedingungen – zu testen.

Artikel 4

Durchführungsrechtsakte

Zur Gewährleistung einheitlicher Bedingungen für die Umsetzung dieser Verordnung in Bezug auf die Konzepte des maschinellen Lernens und die logik- und wissensgestützten Konzepte, die in Artikel 3 Absatz 1 genannt werden, kann die Kommission Durchführungsrechtsakte erlassen, um unter Berücksichtigung von Marktentwicklungen und technischen Entwicklungen die technischen Elemente dieser Konzepte festzulegen. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 74 Absatz 2 genannten Prüfverfahren erlassen.

TITEL IA

KI-SYSTEM MIT ALLGEMEINEM VERWENDUNGSZWECK

Artikel 4a

Konformität mit dieser Verordnung von KI-Systemen mit allgemeinem Verwendungszweck

(1) Unbeschadet der Artikel 5, 52, 53 und 69 dieser Verordnung erfüllen KI-Systeme mit allgemeinem Verwendungszweck lediglich die Anforderungen und Verpflichtungen nach Artikel 4b.

(2) Diese Anforderungen und Verpflichtungen gelten unabhängig davon, ob das KI-System mit allgemeinem Verwendungszweck als vortrainiertes Modell in Verkehr gebracht oder in Betrieb genommen wird und ob die Feinabstimmung des Modells durch den Nutzer des KI-Systems mit allgemeinem Verwendungszweck erfolgt.

Artikel 4b

Anforderungen an KI-Systeme mit allgemeinem Verwendungszweck und Pflichten der Anbieter solcher Systeme

(1) KI-Systeme mit allgemeinem Verwendungszweck, die als Hochrisiko-KI-Systeme oder als Komponenten von Hochrisiko-KI-Systemen im Sinne von Artikel 6 verwendet werden können, erfüllen die in Titel III Kapitel 2 dieser Verordnung festgelegten Anforderungen ab dem Datum der Anwendung der Durchführungsrechtsakte, die von der Kommission im Einklang mit dem in Artikel 74 Absatz 2 genannten Prüfverfahren erlassen werden, spätestens jedoch 18 Monate nach Inkrafttreten dieser Verordnung. In diesen Durchführungsrechtsakten wird die Anwendung der in Titel III Kapitel 2 festgelegten Anforderungen präzisiert und an KI-Systeme mit allgemeinem Verwendungszweck angepasst, und zwar im Hinblick auf ihre Merkmale, die technische Durchführbarkeit, die Besonderheiten der KI-Wertschöpfungskette sowie die Marktentwicklungen und technischen Entwicklungen. Bei der Erfüllung dieser Anforderungen wird dem allgemein anerkannten Stand der Technik Rechnung getragen.

(2) Anbieter von KI-Systemen mit allgemeinem Verwendungszweck nach Absatz 1 erfüllen die in den Artikeln 16aa, 16e, 16f, 16g, 16i, 16j, 25, 48 und 61 festgelegten Verpflichtungen ab dem Datum der Anwendung der in Absatz 1 genannten Durchführungsrechtsakte.

(3) Für die Zwecke der Erfüllung der Verpflichtungen nach Artikel 16e wenden Anbieter das in Anhang VI Nummern 3 und 4 festgelegte Konformitätsbewertungsverfahren auf der Grundlage einer internen Kontrolle an.

(4) Anbieter solcher Systeme halten die in Artikel 11 genannte technische Dokumentation für einen Zeitraum von zehn Jahren ab dem Inverkehrbringen oder der Inbetriebnahme des KI-Systems mit allgemeinem Verwendungszweck in der Union für die zuständigen nationalen Behörden bereit.

(5) Anbieter von KI-Systemen mit allgemeinem Verwendungszweck arbeiten mit anderen Anbietern zusammen, die beabsichtigen, solche Systeme als Hochrisiko-KI-Systeme oder als Komponenten von Hochrisiko-KI-Systemen in der Union in Betrieb zu nehmen oder in Verkehr zu bringen, und stellen ihnen die erforderlichen Informationen zur Verfügung, damit sie ihren Verpflichtungen aus dieser Verordnung nachkommen können. Bei dieser Zusammenarbeit zwischen Anbietern werden gegebenenfalls die Rechte des geistigen Eigentums sowie Betriebs- oder Geschäftsgeheimnisse gemäß Artikel 70 gewahrt. Zur Gewährleistung einheitlicher Bedingungen für die Umsetzung dieser Verordnung in Bezug auf den Austausch von Informationen zwischen Anbietern von KI-Systemen mit allgemeinem Verwendungszweck, kann die Kommission gemäß dem in Artikel 74 Absatz 2 genannten Prüfverfahren Durchführungsrechtsakte erlassen.

(6) Bei der Erfüllung der in den Absätzen 1, 2 und 3 genannten Anforderungen und Verpflichtungen

– ist jede Bezugnahme auf die Zweckbestimmung als Bezugnahme auf die mögliche Verwendung von KI-Systemen mit allgemeinem Verwendungszweck als Hochrisiko-KI-Systeme oder als Komponenten von Hochrisiko-KI-Systemen im Sinne von Artikel 6 zu verstehen;

– ist jede Bezugnahme auf die Anforderungen an Hochrisiko-KI-Systeme in Titel III Kapitel 2 so zu verstehen, dass sie sich nur auf die in diesem Artikel festgelegten Anforderungen bezieht.

Artikel 4c
Ausnahmen von Artikel 4b

(1) Artikel 4b gilt nicht, wenn der Anbieter in den Gebrauchsanweisungen oder in den Begleitdokumenten des KI-Systems mit allgemeinem Verwendungszweck ausdrücklich jegliche Verwendung mit hohem Risiko ausgeschlossen hat.

(2) Ein solcher Ausschluss erfolgt in gutem Glauben und gilt nicht als gerechtfertigt, wenn der Anbieter hinreichende Gründe für die Annahme hat, dass es zu einer Fehlanwendung des Systems kommen könnte.

(3) Stellt der Anbieter eine Fehlanwendung auf dem Markt fest oder wird darüber informiert, so ergreift er alle erforderlichen und verhältnismäßigen Maßnahmen, um eine weitere Fehlanwendung zu verhindern, wobei er insbesondere dem Umfang der Fehlanwendung und der Schwere der damit zusammenhängenden Risiken Rechnung trägt.

TITEL II

VERBOTENE PRAKTIKEN IM BEREICH DER KÜNSTLICHEN INTELLIGENZ

Artikel 5

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

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

b) das Inverkehrbringen, die Inbetriebnahme oder die Verwendung eines KI-Systems, das eine Schwäche oder Schutzbedürftigkeit einer bestimmten Gruppe von Personen aufgrund ihres Alters, einer Behinderung oder einer bestimmten sozialen oder wirtschaftlichen Situation mit dem Ziel oder der Wirkung ausnutzt, das Verhalten einer dieser Gruppe angehörenden Person in einer Weise wesentlich zu beeinflussen, die dieser Person oder einer anderen Person einen physischen oder psychischen Schaden zufügt oder mit hinreichender Wahrscheinlichkeit zufügen wird;

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

i) Schlechterstellung oder Benachteiligung bestimmter natürlicher Personen oder 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 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 durch Strafverfolgungsbehörden oder in deren Auftrag zu Strafverfolgungszwecken, außer wenn und insoweit dies im Hinblick auf eines der folgenden Ziele unbedingt erforderlich ist:

i) gezielte Suche nach bestimmten potenziellen Opfern von Straftaten;

ii) Abwenden einer konkreten und erheblichen Gefahr für kritische Infrastrukturen sowie für das Leben, die Gesundheit oder die körperliche Unversehrtheit natürlicher Personen oder Verhinderung von Terroranschlägen;

iii) Aufspüren und Identifizieren einer natürlichen Person zur strafrechtlichen Ermittlung, Verfolgung oder Vollstreckung einer Strafe für Straftaten, die in Artikel 2 Absatz 2 des Rahmenbeschlusses 2002/584/JI des Rates[32] aufgeführt und in dem betreffenden Mitgliedstaat nach dessen Recht mit einer Freiheitsstrafe oder einer freiheitsentziehenden Maßregel der Sicherung im Höchstmaß von mindestens drei Jahren bedroht sind, oder andere spezifische Straftaten, die in dem betreffenden Mitgliedstaat nach dessen Recht mit einer Freiheitsstrafe oder einer freiheitsentziehenden Maßregel der Sicherung im Höchstmaß von mindestens fünf Jahren bedroht sind.

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

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

---

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

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

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

(3) Im Hinblick auf Absatz 1 Buchstabe d und Absatz 2 ist für jede Verwendung eines biometrischen Echtzeit-Fernidentifizierungssystems in öffentlich zugänglichen Räumen zu Strafverfolgungszwecken eine vorherige Genehmigung erforderlich, die von einer Justizbehörde oder einer unabhängigen Verwaltungsbehörde des Mitgliedstaats, in dem die Verwendung erfolgen soll, auf begründeten Antrag und im Einklang mit den in Absatz 4 genannten detaillierten Vorschriften des nationalen Rechts erteilt wird. In hinreichend begründeten dringenden Fällen kann jedoch mit der Verwendung des Systems zunächst ohne Genehmigung begonnen werden, sofern diese Genehmigung unverzüglich während der Verwendung des KI-Systems beantragt wird; wird diese Genehmigung abgelehnt, so wird die Verwendung mit sofortiger Wirkung eingestellt.

Die zuständige Justiz- oder Verwaltungsbehörde erteilt die Genehmigung nur dann, wenn sie auf der Grundlage objektiver Nachweise oder eindeutiger Hinweise, die ihr vorgelegt werden, davon überzeugt ist, dass die Verwendung des betreffenden biometrischen Echtzeit-Fernidentifizierungssystems für das Erreichen eines der in Absatz 1 Buchstabe d genannten Ziele – wie im Antrag angegeben – notwendig und verhältnismäßig ist. Bei ihrer Entscheidung über den Antrag berücksichtigt die zuständige Justiz- oder Verwaltungsbehörde die in Absatz 2 genannten Elemente.

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

TITEL III

HOCHRISIKO-KI-SYSTEME

KAPITEL 1

KLASSIFIZIERUNG VON KI-SYSTEMEN ALS HOCHRISIKO-SYSTEME

Artikel 6

Klassifizierungsvorschriften für Hochrisiko-KI-Systeme

(1) Ein KI-System, das selbst ein Produkt ist, das unter die in Anhang II aufgeführten Harmonisierungsrechtsvorschriften der Union fällt, gilt als hochriskant, wenn es hinsichtlich seines Inverkehrbringens oder seiner Inbetriebnahme gemäß den genannten Rechtsvorschriften einer Konformitätsbewertung durch Dritte unterzogen werden muss.

(2) Ein KI-System, das als Sicherheitskomponente eines Produkts verwendet werden soll, das unter die in Absatz 1 genannten Rechtsvorschriften fällt, gilt als hochriskant, wenn es hinsichtlich seines Inverkehrbringens oder seiner Inbetriebnahme gemäß den genannten Rechtsvorschriften einer Konformitätsbewertung durch Dritte unterzogen werden muss. Diese Bestimmung gilt ungeachtet dessen, ob das KI-System unabhängig von dem jeweiligen Produkt in Verkehr gebracht oder in Betrieb genommen wird.

(3) Die in Anhang III genannten KI-Systeme gelten als hochriskant, es sei denn, das Ergebnis des Systems ist in Bezug auf die zu treffende Maßnahme oder Entscheidung völlig unwesentlich und führt daher wahrscheinlich nicht zu einem erheblichen Risiko für Gesundheit, Sicherheit oder Grundrechte.

Zur Gewährleistung einheitlicher Bedingungen für die Umsetzung dieser Verordnung erlässt die Kommission spätestens ein Jahr nach Inkrafttreten dieser Verordnung Durchführungsrechtsakte, um festzulegen, unter welchen Umständen das Ergebnis der in Anhang III genannten KI-Systeme in Bezug auf die zu treffende Maßnahme oder Entscheidung völlig unwesentlich ist. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 74 Absatz 2 genannten Prüfverfahren erlassen.

Artikel 7

Änderungen des Anhangs III

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

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

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

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

a) die Zweckbestimmung des KI-Systems;

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

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

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

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

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

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

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

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

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

i) den Umfang und die Wahrscheinlichkeit eines Nutzens, den Einzelpersonen, Gruppen oder die Gesellschaft insgesamt aus der KI-Verwendung ziehen.

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

a) das/die betreffende(n) Hochrisiko-KI-System(e) weist bzw. weisen unter Berücksichtigung der in Absatz 2 aufgeführten Kriterien keine erheblichen Risiken mehr für Grundrechte, Gesundheit oder Sicherheit auf;

b) durch die Streichung wird das allgemeine Schutzniveau in Bezug auf Gesundheit, Sicherheit und Grundrechte im Rahmen des Unionsrechts nicht gesenkt.

KAPITEL 2

ANFORDERUNGEN AN HOCHRISIKO-KI-SYSTEME

Artikel 8

Einhaltung der Anforderungen

(1) Hochrisiko-KI-Systeme erfüllen die in diesem Kapitel festgelegten Anforderungen und tragen dabei dem allgemein anerkannten Stand der Technik Rechnung.

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

Artikel 9

Risikomanagementsystem

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

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

a) Ermittlung und Analyse der bekannten und vorhersehbaren Risiken, die mit Blick auf die Zweckbestimmung des Hochrisiko-KI-Systems höchstwahrscheinlich die Gesundheit, Sicherheit und Grundrechte beeinträchtigen;

b) [gestrichen];

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

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

Die in diesem Absatz genannten Risiken betreffen nur solche Risiken, die durch die Entwicklung oder Konzeption des hochriskanten KI-Systems oder durch die Bereitstellung ausreichender technischer Informationen angemessen gemindert oder behoben werden können.

(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 wirksamer zu minimieren und gleichzeitig ein angemessenes Gleichgewicht bei der Durchführung der Maßnahmen zur Erfüllung dieser Anforderungen sicherzustellen.

(4) Die in Absatz 2 Buchstabe d genannten Risikomanagementmaßnahmen werden so gestaltet, dass jedes mit einer bestimmten Gefahr verbundene Restrisiko sowie das Gesamtrestrisiko der Hochrisiko-KI-Systeme als vertretbar beurteilt werden kann.

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

a) weitestmögliche Beseitigung oder Verringerung der nach Absatz 2 ermittelten und bewerteten Risiken durch eine geeignete Konzeption und Entwicklung des Hochrisiko-KI-Systems;

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

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

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

(5) Durch das Testen der Hochrisiko-KI-Systeme ist sicherzustellen, dass sie entsprechend ihrer Zweckbestimmung funktionieren und die Anforderungen dieses Kapitels erfüllen.

(6) Die Testverfahren können das Testen unter realen Bedingungen gemäß Artikel 54a umfassen.

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

(8) In Bezug auf das in den Absätzen 1 bis 7 beschriebene Risikomanagementsystem ist insbesondere zu berücksichtigen, ob das Hochrisiko-KI-System wahrscheinlich für Personen unter 18 Jahren zugänglich ist oder Auswirkungen auf diese Personen hat.

(9) Bei Anbietern von Hochrisiko-KI-Systemen, die den Anforderungen an interne Risikomanagementprozesse gemäß den sektorspezifischen Rechtsvorschriften der Union unterliegen, sind die in den Absätzen 1 bis 8 beschriebenen Aspekte Bestandteil der nach den genannten Rechtsvorschriften festgelegten Risikomanagementverfahren.

Artikel 10

Daten und Daten-Governance

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

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

a) die einschlägigen konzeptionellen Entscheidungen,

b) die Datenerfassungsprozesse,

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

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

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

f) eine Untersuchung im Hinblick auf mögliche Verzerrungen (Bias), die die Gesundheit und Sicherheit von natürlichen Personen beeinträchtigen oder zu einer nach dem Unionsrecht verbotenen Diskriminierung führen können,

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

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

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

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

(6) Bei der Entwicklung von Hochrisiko-KI-Systemen, in denen keine Techniken eingesetzt werden, bei denen Modelle trainiert werden, gelten die Absätze 2 bis 5 nur für Testdatensätze.

Artikel 11

Technische Dokumentation

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

Die technische Dokumentation wird so erstellt, dass aus ihr der Nachweis hervorgeht, wie das Hochrisiko-KI-System die Anforderungen dieses Kapitels erfüllt, und dass den zuständigen nationalen Behörden und den notifizierten Stellen alle Informationen in klarer und verständlicher Form 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-up-Unternehmen – alle gleichwertigen Unterlagen, die denselben Zwecken dienen, sofern die zuständige Behörde dies nicht als unangemessen erachtet.

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

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

Artikel 12

Aufzeichnungspflichten

(1) Die Technik der Hochrisiko-KI-Systeme ermöglicht die automatische Aufzeichnung von Vorgängen und Ereignissen („Protokollierung“) während des Lebenszyklus des Systems.

(2) Zur Gewährleistung, dass das Funktionieren des KI-Systems in einem der Zweckbestimmung des Systems angemessenen Maße rückverfolgbar ist, ermöglicht die Protokollierung die Aufzeichnung von Vorgängen und Ereignissen, die für Folgendes relevant sind:

i) die Ermittlung von Situationen, die dazu führen können, dass das KI-System ein Risiko im Sinne von Artikel 65 Absatz 1 birgt oder dass es zu einer wesentlichen Änderung kommt;

ii) die Erleichterung der Beobachtung nach dem Inverkehrbringen gemäß Artikel 61; und

iii) die Überwachung des Betriebs der Hochrisiko-KI-Systeme gemäß Artikel 29 Absatz 4.

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

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

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

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

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

Artikel 13

Transparenz und Bereitstellung von Informationen für die Nutzer

(1) Hochrisiko-KI-Systeme werden so konzipiert und entwickelt, dass ihr Betrieb hinreichend transparent ist, damit die Nutzer und Anbieter ihre in Kapitel 3 dieses Titels festgelegten einschlägigen Pflichten erfüllen können und damit die Nutzer das System angemessen verstehen und verwenden können.

(2) Hochrisiko-KI-Systeme werden mit Gebrauchsanweisungen in einem geeigneten digitalen Format bereitgestellt oder auf andere Weise mit Gebrauchsanweisungen versehen, die präzise, vollständige, korrekte und eindeutige Informationen in einer für die Nutzer relevanten, barrierefrei zugänglichen und verständlichen Form enthalten.

(3) Die in Absatz 2 genannten Informationen umfassen:

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

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

i) seiner Zweckbestimmung, auch der besonderen geografischen, verhaltensbezogenen oder funktionalen Rahmenbedingungen, unter denen ein Hochrisiko-KI-System bestimmungsgemäß verwendet werden soll,

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

iii) aller bekannten oder vorhersehbaren Umstände im Zusammenhang mit der bestimmungsgemäßen Verwendung des Hochrisiko-KI-Systems, die zu den in Artikel 9 Absatz 2 genannten Risiken für die Gesundheit und Sicherheit, die Grundrechte oder die Umwelt führen können,

iv) gegebenenfalls seines Verhaltens gegenüber bestimmten Personen oder Personengruppen, auf die das System bestimmungsgemäß angewandt werden soll,

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

vi) gegebenenfalls der Beschreibung des erwarteten Ergebnisses des Systems.

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

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

e) die erforderlichen Rechen- und Hardware-Ressourcen, die erwartete Lebensdauer des Hochrisiko-KI-Systems und alle erforderlichen Wartungs- und Pflegemaßnahmen sowie deren Häufigkeit zur Gewährleistung des ordnungsgemäßen Funktionierens dieses KI-Systems, auch in Bezug auf Software-Updates;

f) eine Beschreibung des in das KI-System integrierten Mechanismus, der es den Nutzern gegebenenfalls ermöglicht, die Protokolle ordnungsgemäß zu erfassen, zu speichern und auszuwerten.

Artikel 14

Menschliche Aufsicht

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

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

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

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

b) Vorkehrungen, die vor dem Inverkehrbringen oder der Inbetriebnahme des Hochrisiko-KI-Systems vom Anbieter bestimmt werden und dazu geeignet sind, vom 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 die natürlichen Personen, denen die menschliche Aufsicht übertragen wurde, je nach den Umständen und sofern verhältnismäßig in der Lage sind,

a) die Fähigkeiten und Grenzen des Hochrisiko-KI-Systems zu verstehen und seinen Betrieb ordnungsgemäß zu überwachen;

b) sich einer möglichen Neigung zu einem automatischen oder übermäßigen Vertrauen in das von einem Hochrisiko-KI-System hervorgebrachte Ergebnis („Automatisierungsbias“) bewusst zu bleiben;

c) die Ergebnisse des Hochrisiko-KI-Systems richtig zu interpretieren, wobei beispielsweise 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 außer Acht zu lassen, außer Kraft zu setzen oder rückgängig zu machen;

e) in den Betrieb des Hochrisiko-KI-Systems einzugreifen oder den Systembetrieb mit einer „Stopptaste“ oder einem ähnlichen Verfahren zu unterbrechen.

(5) Bei den in Anhang III Nummer 1 Buchstabe a genannten Hochrisiko-KI-Systemen müssen die in Absatz 3 genannten Vorkehrungen so gestaltet sein, dass außerdem der Nutzer keine Maßnahmen oder Entscheidungen allein aufgrund des vom System hervorgebrachten Identifizierungsergebnisses trifft, solange dies nicht von mindestens zwei natürlichen Personen getrennt überprüft und bestätigt wurde. Die Anforderung einer getrennten Überprüfung durch mindestens zwei natürliche Personen gilt nicht für Hochrisiko-KI-Systeme, die für Zwecke in den Bereichen Strafverfolgung, Migration, Grenzkontrolle oder Asyl verwendet werden, wenn die Anwendung dieser Anforderung nach Unionsrecht oder nationalem Recht unverhältnismäßig ist.

Artikel 15

Genauigkeit, Robustheit und Cybersicherheit

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

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

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

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

Hochrisiko-KI-Systeme, die nach dem Inverkehrbringen oder der Inbetriebnahme weiterhin dazulernen, sind so zu entwickeln, dass das Risiko möglicherweise verzerrter Ergebnisse, die den künftigen Betrieb beeinflussen („Rückkopplungsschleifen“), angemessen mit geeigneten Risikominderungsmaßnahmen beseitigt oder so gering wie möglich gehalten wird.

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

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

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

KAPITEL 3

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

Artikel 16

Pflichten der Anbieter von Hochrisiko-KI-Systemen

Anbieter von Hochrisiko-KI-Systemen müssen

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

aa) ihren Namen, ihren eingetragenen Handelsnamen oder ihre eingetragene Handelsmarke und ihre Kontaktanschrift auf dem Hochrisiko-KI-System selbst oder, wenn dies nicht möglich ist, auf der Verpackung oder in der beigefügten Dokumentation angeben;

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

c) die in Artikel 18 genannte Dokumentation aufbewahren;

d) die von ihren Hochrisiko-KI-Systemen in Übereinstimmung mit Artikel 20 automatisch erzeugten Protokolle aufbewahren, wenn dies ihrer Kontrolle unterliegt;

e) sicherstellen, dass das Hochrisiko-KI-System dem betreffenden Konformitätsbewertungsverfahren nach Artikel 43 unterzogen wird, bevor es in Verkehr gebracht oder in Betrieb genommen wird;

f) den in Artikel 51 Absatz 1 genannten Registrierungspflichten nachkommen;

g) die erforderlichen Korrekturmaßnahmen gemäß Artikel 21 ergreifen, wenn das Hochrisiko-KI-System die Anforderungen in Kapitel 2 dieses Titels nicht erfüllt;

h) die betreffende zuständige nationale Behörde der Mitgliedstaaten, in denen sie das System bereitgestellt oder in Betrieb genommen haben, und gegebenenfalls die notifizierte Stelle über die Nichtkonformität und bereits ergriffene Korrekturmaßnahmen informieren;

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

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

Artikel 17

Qualitätsmanagementsystem

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

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

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

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

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

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

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

g) das in Artikel 9 genannte Risikomanagementsystem;

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

i) Verfahren zur Meldung eines schwerwiegenden Vorfalls gemäß Artikel 62;

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

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

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

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

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

(2a) Bei Anbietern von Hochrisiko-KI-Systemen, die Verpflichtungen in Bezug auf Qualitätsmanagementsysteme gemäß den sektorspezifischen Rechtsvorschriften der Union unterliegen, können die in Absatz 1 beschriebenen Aspekte Bestandteil der nach den genannten Rechtsvorschriften festgelegten Qualitätsmanagementsysteme sein.

(3) Bei Anbietern, die Finanzinstitute sind und gemäß den Rechtsvorschriften der Union im Bereich der Finanzdienstleistungen Anforderungen in Bezug auf ihre Regelungen oder Verfahren der internen Unternehmensführung unterliegen, gilt die Verpflichtung zur Einrichtung eines Qualitätsmanagementsystems – mit Ausnahme von Absatz 1 Buchstaben g, h und i – als erfüllt, wenn die Vorschriften über Regelungen oder Verfahren der internen Unternehmensführung gemäß den einschlägigen Rechtsvorschriften der Union im Bereich der Finanzdienstleistungen eingehalten werden. Dabei werden die in Artikel 40 dieser Verordnung genannten harmonisierten Normen berücksichtigt.

Artikel 18

Aufbewahrung von Dokumentation

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

a) die in Artikel 11 genannte technische Dokumentation,

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

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

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

e) die in Artikel 48 genannte EU-Konformitätserklärung.

(1a) Jeder Mitgliedstaat legt die Bedingungen fest, unter denen die in Absatz 1 genannte Dokumentation für die zuständigen nationalen Behörden für den in dem genannten Absatz angegebenen Zeitraum bereitgehalten wird, für den Fall, dass ein Anbieter oder sein in demselben Hoheitsgebiet niedergelassener Bevollmächtigter vor Ende dieses Zeitraums in Konkurs geht oder seine Tätigkeit aufgibt.

(2) Anbieter, die Finanzinstitute sind und gemäß den Rechtsvorschriften der Union im Bereich der Finanzdienstleistungen Anforderungen in Bezug auf ihre Regelungen oder Verfahren der internen Unternehmensführung unterliegen, pflegen die technische Dokumentation als Teil der gemäß den einschlägigen Rechtsvorschriften der Union im Bereich der Finanzdienstleistungen aufzubewahrenden Dokumentation.

Artikel 19

Konformitätsbewertung

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

(2) [gestrichen]

Artikel 20

Automatisch erzeugte Protokolle

(1) Anbieter von Hochrisiko-KI-Systemen bewahren die von ihren Hochrisiko-KI-Systemen gemäß Artikel 12 Absatz 1 automatisch erzeugten Protokolle auf, soweit diese Protokolle aufgrund einer vertraglichen Vereinbarung mit dem Nutzer oder auf gesetzlicher Grundlage ihrer Kontrolle unterliegen. Sofern im geltenden Unionsrecht oder im nationalen Recht, insbesondere im Unionsrecht zum Schutz personenbezogener Daten, nichts anderes vorgesehen ist, bewahren sie sie mindestens sechs Monate lang auf.

(2) Anbieter, die Finanzinstitute sind und gemäß den Rechtsvorschriften der Union im Bereich der Finanzdienstleistungen Anforderungen in Bezug auf ihre Regelungen oder Verfahren der internen Unternehmensführung unterliegen, bewahren die von ihren Hochrisiko-KI-Systemen automatisch erzeugten Protokolle als Teil der gemäß den einschlägigen Rechtsvorschriften der Union im Bereich der Finanzdienstleistungen aufzubewahrenden Dokumentation auf.

Artikel 21

Korrekturmaßnahmen

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

Artikel 22

Informationspflicht

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

Artikel 23

Zusammenarbeit mit den zuständigen Behörden

Anbieter von Hochrisiko-KI-Systemen übermitteln einer zuständigen nationalen Behörde auf deren Anfrage 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 Sprache, die für die Behörde des betreffenden Mitgliedstaats leicht verständlich ist. Auf begründete Anfrage einer zuständigen nationalen Behörde gewähren die Anbieter dieser Behörde auch Zugang zu den von ihrem Hochrisiko-KI-System gemäß Artikel 12 Absatz 1 automatisch erzeugten Protokollen, soweit diese Protokolle aufgrund einer vertraglichen Vereinbarung mit dem Nutzer oder auf gesetzlicher Grundlage ihrer Kontrolle unterliegen.

Artikel 23a

Anforderungen an andere Personen, die den Pflichten eines Anbieters unterliegen

(1) In den folgenden Fällen gelten natürliche oder juristische Personen für die Zwecke dieser Verordnung als Anbieter eines neuen Hochrisiko-KI-Systems und unterliegen den Pflichten der Anbieter nach Artikel 16, nämlich wenn

a) sie ein bereits in Verkehr gebrachtes oder in Betrieb genommenes Hochrisiko-AI-System mit ihrem Namen oder ihrer Handelsmarke versehen, unbeschadet vertraglicher Vereinbarungen, die eine andere Aufteilung der Pflichten vorsehen;

b) [gestrichen]

c) sie eine wesentliche Änderung an einem bereits in Verkehr gebrachten oder in Betrieb genommenen Hochrisiko-KI-System vornehmen;

d) sie die Zweckbestimmung eines bereits in Verkehr gebrachten oder in Betrieb genommenen KI-Systems, das kein hohes Risiko darstellt, auf eine Art und Weise ändern, dass das geänderte System zu einem Hochrisiko-KI-System wird;

e) sie ein KI-System mit allgemeinem Verwendungszweck als ein Hochrisiko-KI-System oder als eine Komponente eines Hochrisiko-KI-Systems in Verkehr bringen oder in Betrieb nehmen.

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

(3) Bei Hochrisiko-KI-Systemen, bei denen es sich um Sicherheitskomponenten von Produkten handelt, für die die in Anhang II Abschnitt A aufgeführten Rechtsakte gelten, gilt der Hersteller dieser Produkte als Anbieter des Hochrisiko-KI-Systems und unterliegt in den beiden nachfolgenden Fällen den Pflichten nach Artikel 16:

i) das Hochrisiko-KI-System wird zusammen mit dem Produkt unter dem Namen oder der Handelsmarke des Produktherstellers in Verkehr gebracht;

ii) das Hochrisiko-KI-System wird unter dem Namen oder der Handelsmarke des Produktherstellers in Betrieb genommen wird, nachdem das Produkt in Verkehr gebracht wurde.

Artikel 24

[gestrichen]

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.

(2) Der Bevollmächtigte nimmt die Aufgaben wahr, die in seinem vom Anbieter erhaltenen Auftrag festgelegt sind. Für die Zwecke dieser Verordnung wird der Bevollmächtigte durch den Auftrag nur zur Wahrnehmung folgender Aufgaben ermächtigt:

-a) Überprüfung, dass die EU-Konformitätserklärung und die technische Dokumentation erstellt wurden und dass der Anbieter ein angemessenes Konformitätsbewertungsverfahren durchgeführt hat;

a) Bereithaltung für einen Zeitraum von zehn Jahren ab dem Inverkehrbringen oder der Inbetriebnahme des Hochrisiko-KI-Systems der Kontaktdaten des Anbieters, der den Bevollmächtigten benannt hat, eines Exemplars der EU-Konformitätserklärung, der technischen Dokumentation und gegebenenfalls der von der notifizierten Stelle ausgestellten Bescheinigung für die zuständigen nationalen Behörden und die in Artikel 63 Absatz 7 genannten nationalen Behörden;

b) Übermittlung aller – auch der nach Buchstabe b bereitgehaltenen – 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 begründete Anfrage, einschließlich der Gewährung des Zugangs zu den vom Hochrisiko-KI-System gemäß Artikel 12 Absatz 1 automatisch erzeugten Protokollen, soweit diese Protokolle aufgrund einer vertraglichen Vereinbarung mit dem Nutzer oder auf gesetzlicher Grundlage der Kontrolle des Anbieters unterliegen;

c) Zusammenarbeit mit den zuständigen nationalen Behörden auf deren begründete Anfrage bei allen Maßnahmen, die diese im Zusammenhang mit dem Hochrisiko-KI-System ergreifen;

d) Erfüllung der in Artikel 51 Absatz 1 genannten Registrierungspflichten und, wenn das System vom Anbieter selbst registriert wird, Überprüfung der Korrektheit der in Anhang VIII Teil II Nummern 1 bis 11 genannten Informationen.

Der Bevollmächtigte beendet den Auftrag, wenn er hinreichende Gründe zu der Annahme hat, dass der Anbieter gegen die in dieser Verordnung festgelegten Pflichten verstößt. In diesem Fall unterrichtet er ferner unverzüglich die Marktüberwachungsbehörde des Mitgliedstaats, in dem er niedergelassen ist, und gegebenenfalls die betreffende notifizierte Stelle über die Beendigung des Auftrags und deren Gründe.

Der Bevollmächtigte ist auf derselben Grundlage wie der Anbieter in Bezug auf seine mögliche Haftbarkeit gemäß der Richtlinie 85/374/EWG des Rates für fehlerhafte KI-Systeme rechtlich und gesamtschuldnerisch mit diesem haftbar.

Artikel 26

Pflichten der Einführer

(1) Bevor sie ein Hochrisiko-KI-System in Verkehr bringen, stellen die Einführer solcher Systeme sicher, dass ein solches System dieser Verordnung entspricht, indem sie überprüfen, ob

a) der Anbieter des KI-Systems das entsprechende Konformitätsbewertungsverfahren nach Artikel 43 durchgeführt hat;

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

c) das System mit der erforderlichen CE-Konformitätskennzeichnung versehen ist und ihm die EU-Konformitätserklärung und Gebrauchsanweisungen beigefügt sind;

d) der in Artikel 25 genannte Bevollmächtigte vom Anbieter benannt wurde.

(2) Hat ein Einführer hinreichende Gründe zu der Annahme, dass ein Hochrisiko-KI-System nicht dieser Verordnung entspricht oder gefälscht ist oder diesem gefälschte Unterlagen beigefügt 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, die Bevollmächtigten und die Marktüberwachungsbehörden davon in Kenntnis.

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

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

(4a) Die Einführer halten für einen Zeitraum von zehn Jahren ab dem Inverkehrbringen oder der Inbetriebnahme des KI-Systems ein Exemplar der von der notifizierten Stelle ausgestellten Bescheinigung sowie gegebenenfalls die Gebrauchsanweisungen und die EU-Konformitätserklärung bereit.

(5) Die Einführer übermitteln den zuständigen nationalen Behörden auf deren begründete Anfrage alle – auch die nach Absatz 5 bereitgehaltenen – Informationen und Unterlagen, die erforderlich sind, um die Konformität des Hochrisiko-KI-Systems mit den Anforderungen in Kapitel 2 dieses Titels nachzuweisen, in einer Sprache, die für diese zuständige nationale Behörde leicht verständlich ist. Zu diesem Zweck stellen sie auch sicher, dass diesen Behörden die technische Dokumentation zur Verfügung gestellt werden kann.

(5a) Die Einführer arbeiten mit den zuständigen nationalen Behörden bei allen Maßnahmen zusammen, die diese Behörden im Zusammenhang mit einem von dem Einführer eingeführten KI-System ergreifen.

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 eine EU-Konformitätserklärung und Gebrauchsanweisungen beigefügt sind und ob der Anbieter bzw. gegebenenfalls der Einführer des Systems die in Artikel 16 Buchstabe b bzw. Artikel 26 Absatz 3 festgelegten Pflichten erfüllt hat.

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

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

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

(5) Auf begründete Anfrage einer zuständigen nationalen Behörde übermitteln die Händler von Hochrisiko-KI-Systemen dieser Behörde alle Informationen und Unterlagen in Bezug auf ihre in den Absätzen 1 bis 4 beschriebenen Tätigkeiten.

(5a) Die Händler arbeiten mit den zuständigen nationalen Behörden bei allen Maßnahmen zusammen, die diese Behörden im Zusammenhang mit einem von dem Händler bereitgestellten KI-System ergreifen.

Artikel 28

[gestrichen]

Artikel 29

Pflichten der Nutzer von Hochrisiko-KI-Systemen

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

(1a) Die Nutzer übertragen natürlichen Personen, die über die erforderliche Kompetenz, Ausbildung und Befugnis verfügen, die menschliche Aufsicht.

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

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

(4) Die Nutzer richten eine menschliche Aufsicht ein und überwachen den Betrieb des Hochrisiko-KI-Systems anhand der Gebrauchsanweisungen. Haben sie Grund zu der Annahme, dass die Verwendung gemäß den Gebrauchsanweisungen dazu führen kann, dass das Hochrisiko-KI-System ein Risiko im Sinne des Artikels 65 Absatz 1 birgt, so informieren sie den Anbieter oder Händler und setzen die Verwendung des Systems aus. Sie informieren den Anbieter oder Händler auch, wenn sie einen schwerwiegenden Vorfall festgestellt haben, und unterbrechen die Verwendung des KI-Systems. Kann der Nutzer den Anbieter nicht erreichen, so gilt Artikel 62 entsprechend. Diese Pflicht gilt nicht für sensible operative Daten von Nutzern von KI-Systemen, die Strafverfolgungsbehörden sind.

Bei Nutzern, die Finanzinstitute sind und gemäß den Rechtsvorschriften der Union im Bereich der Finanzdienstleistungen Anforderungen in Bezug auf ihre Regelungen oder Verfahren der internen Unternehmensführung unterliegen, gilt die in Unterabsatz 1 aufgeführte Überwachungspflicht als erfüllt, wenn die Vorschriften über Regelungen, Verfahren oder Mechanismen der internen Unternehmensführung gemäß den einschlägigen Rechtsvorschriften der Union im Bereich der Finanzdienstleistungen eingehalten werden.

(5) Nutzer von Hochrisiko-KI-Systemen bewahren die von ihrem Hochrisiko-KI-System gemäß Artikel 12 Absatz 1 automatisch erzeugten Protokolle auf, soweit diese Protokolle ihrer Kontrolle unterliegen. Sofern im geltenden Unionsrecht oder im nationalen Recht, insbesondere im Unionsrecht zum Schutz personenbezogener Daten, nichts anderes vorgesehen ist, bewahren sie sie mindestens sechs Monate lang auf.

Nutzer, die Finanzinstitute sind und gemäß den Rechtsvorschriften der Union im Bereich der Finanzdienstleistungen Anforderungen in Bezug auf ihre Regelungen oder Verfahren der internen Unternehmensführung unterliegen, bewahren die Protokolle als Teil der gemäß den einschlägigen Rechtsvorschriften der Union im Bereich der Finanzdienstleistungen aufzubewahrenden Dokumentation auf.

(5a) Nutzer von Hochrisiko-KI-Systemen, die Behörden, Einrichtungen oder sonstige Stellen sind, mit Ausnahme von Strafverfolgungs-, Grenzschutz-, Einwanderungs- oder Asylbehörden, erfüllen die in Artikel 51 genannten Registrierungspflichten. Stellen sie fest, dass das System, dessen Verwendung sie planen, nicht in der in Artikel 60 genannten EU-Datenbank registriert wurde, sehen sie von der Verwendung dieses Systems ab und unterrichten den Anbieter oder den Händler.

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

(6a) Die Nutzer arbeiten mit den zuständigen nationalen Behörden bei allen Maßnahmen zusammen, die diese Behörden im Zusammenhang mit einem von dem Nutzer verwendeten KI-System ergreifen.

KAPITEL 4

NOTIFIZIERENDE BEHÖRDEN UND NOTIFIZIERTE STELLEN

Artikel 30

Notifizierende Behörden

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

(2) Die Mitgliedstaaten können entscheiden, dass die Bewertung und Überwachung nach Absatz 1 von einer nationalen Akkreditierungsstelle im Sinne von und im Einklang mit der Verordnung (EG) Nr. 765/2008 erfolgt.

(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 im Einklang mit Artikel 70 die Vertraulichkeit der von ihnen erlangten Informationen.

(7) Notifizierende Behörden verfügen über eine angemessene Anzahl kompetenter Mitarbeiter, sodass sie ihre Aufgaben ordnungsgemäß wahrnehmen können.

(8) [gestrichen]

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 bzw. der Konformitätsbewertungsmoduls bzw. - module und der KI-Systeme, 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. Die notifizierte Stelle aktualisiert die in Absätzen 2 und 3 genannten Unterlagen immer dann, wenn sich relevante Änderungen ergeben, damit die für notifizierte Stellen zuständige Behörde überwachen und überprüfen kann, ob die in Artikel 33 genannten Anforderungen kontinuierlich eingehalten werden.

Artikel 32

Notifizierungsverfahren

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

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

(3) Eine Notifizierung gemäß Absatz 2 enthält vollständige Angaben zu den Konformitätsbewertungstätigkeiten, dem betreffenden Konformitätsbewertungsmodul oder den betreffenden Konformitätsbewertungsmodulen und des betreffenden KI-Systems sowie die einschlägige Bestätigung der Kompetenz. Beruht eine Notifizierung nicht auf einer Akkreditierungsurkunde gemäß Artikel 31 Absatz 2, so legt die notifizierende Behörde der Kommission und den anderen Mitgliedstaaten die Unterlagen, die die Kompetenz der Konformitätsbewertungsstelle nachweisen, sowie die Vereinbarungen vor, die getroffen wurden, um sicherzustellen, dass die Stelle regelmäßig überwacht wird und weiter stets den Anforderungen nach Artikel 33 genügt.

(4) Die betreffende Konformitätsbewertungsstelle darf die Tätigkeiten einer notifizierten Stelle nur dann wahrnehmen, wenn weder die Kommission noch die anderen Mitgliedstaaten innerhalb von zwei Wochen nach einer Notifizierung durch eine notifizierende Behörde, wenn eine Akkreditierungsurkunde gemäß Artikel 31 Absatz 2 vorgelegt wird, oder innerhalb von zwei Monaten nach einer Notifizierung durch eine notifizierende Behörde, wenn als Nachweis Unterlagen gemäß Artikel 31 Absatz 3 vorgelegt werden, Einwände erhoben haben.

(5) [gestrichen]

Artikel 33

Anforderungen an notifizierte Stellen

(1) Eine notifizierte Stelle muss nach nationalem Recht gegründet und mit Rechtspersönlichkeit ausgestattet sein.

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

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

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

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

(6) Die notifizierten Stellen gewährleisten durch dokumentierte Verfahren, dass ihre Mitarbeiter, Ausschüsse, Zweigstellen, Unterauftragnehmer sowie alle zugeordneten Stellen oder Mitarbeiter externer Einrichtungen im Einklang mit Artikel 70 die Vertraulichkeit der Informationen, die bei der Durchführung der Konformitätsbewertungstätigkeiten in ihren Besitz gelangen, wahren, außer wenn die Offenlegung gesetzlich vorgeschrieben ist. Informationen, von denen Mitarbeiter der notifizierten Stellen bei der Durchführung ihrer Aufgaben gemäß dieser Verordnung Kenntnis erlangen, unterliegen der beruflichen Schweigepflicht, außer gegenüber den notifizierenden Behörden des Mitgliedstaats, in dem sie ihre Tätigkeiten ausüben.

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

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

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

(10) Die notifizierten Stellen verfügen über ausreichende interne Kompetenzen, um die von externen Stellen in ihrem Namen wahrgenommen Aufgaben wirksam beurteilen zu können. Die notifizierten Stellen verfügen ständig über ausreichendes administratives, technisches, juristisches und wissenschaftliches Personal, das die entsprechenden Erfahrungen und Kenntnisse in Bezug auf einschlägige KI-Technik, Daten und Datenverarbeitung sowie die Anforderungen in Kapitel 2 dieses Titels besitzt.

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

(12) [gestrichen]

Artikel 33a

Vermutung der Konformität mit den Anforderungen an notifizierte Stellen

Weist eine Konformitätsbewertungsstelle nach, dass sie die Kriterien der einschlägigen harmonisierten Normen, deren Fundstellen im Amtsblatt der Europäischen Union veröffentlicht wurden, oder Teile dieser Normen erfüllt, wird davon ausgegangen, dass sie die in Artikel 33 genannten Anforderungen, soweit diese von den geltenden harmonisierten Normen erfasst werden, erfüllt.

Artikel 34

Zweigstellen notifizierter Stellen und Vergabe von Unteraufträgen durch notifizierte Stellen

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

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

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

(4) Die einschlägigen Unterlagen über die Bewertung der Qualifikation des Unterauftragnehmers oder der Zweigstelle und die von ihnen gemäß dieser Verordnung ausgeführten Arbeiten werden für einen Zeitraum von fünf Jahren ab dem Datum der Beendigung der Vergabe von Unteraufträgen für die notifizierende Behörde bereitgehalten.

Artikel 34a

Operative Pflichten der notifizierten Stellen

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

(2) Die notifizierten Stellen führen ihre Tätigkeiten ohne unnötige Belastungen für die Anbieter und unter gebührender Berücksichtigung der Größe eines Unternehmens, der Branche, in der es tätig ist, seiner Struktur sowie der Komplexität des betreffenden Hochrisiko-KI-Systems durch Hierbei geht die notifizierte Stelle jedoch so streng vor und hält ein solches Schutzniveau ein, wie es für die Konformität des Hochrisiko-KI-Systems mit den Anforderungen dieser Verordnung erforderlich ist.

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

Artikel 35

Kennnummern und Verzeichnisse der nach dieser Verordnung benannten notifizierten Stellen

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

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

Artikel 36

Änderungen der Notifizierungen

(1) Die notifizierende Behörde unterrichtet die Kommission und die anderen Mitgliedstaaten mithilfe des in Artikel 32 Absatz 2 genannten elektronischen Notifizierungsinstruments über alle relevanten Änderungen der Notifizierung einer notifizierten Stelle.

(2) Für Erweiterungen des Geltungsbereichs der Notifizierung gilt das Verfahren gemäß den Artikeln 31 und 32. Für andere Änderungen der Notifizierung als Erweiterungen ihres Geltungsbereichs gelten die in den folgenden Absätzen dargelegten Verfahren.

Beschließt eine notifizierte Stelle die Einstellung ihrer Konformitätsbewertungstätigkeiten, so teilt sie dies der betreffenden notifizierenden Behörde und den betreffenden Anbietern so bald wie möglich und im Falle einer geplanten Einstellung ihrer Tätigkeiten ein Jahr vor deren Beendigung mit. Die Bescheinigungen können für einen befristeten Zeitraum von neun Monaten nach Einstellung der Tätigkeiten der notifizierten Stelle gültig bleiben, sofern eine andere notifizierte Stelle schriftlich bestätigt hat, dass sie die Verantwortung für die von diesen Bescheinigungen abgedeckten KI-Systeme übernimmt. Die neue notifizierte Stelle führt vor Ablauf dieser Frist eine vollständige Bewertung der betroffenen KI-Systeme durch, bevor sie für diese neue Bescheinigungen ausstellt. Stellt die notifizierte Stelle ihre Tätigkeit ein, so widerruft die notifizierende Behörde die Benennung.

(3) Hat die notifizierende Behörde hinreichende Gründe zu der Annahme, dass die notifizierte Stelle die in Artikel 33 festgelegten Anforderungen nicht mehr erfüllt oder dass sie ihren Verpflichtungen nicht nachkommt, so schränkt die notifizierenden Behörde – sofern die notifizierte Stelle Möglichkeit zur Stellungnahme hatte – die Notifizierung gegebenenfalls ein, setzt sie aus oder widerruft sie, wobei sie das Ausmaß der Nichterfüllung dieser Anforderungen oder Pflichtverletzung berücksichtigt. Sie setzt die Kommission und die anderen Mitgliedstaaten unverzüglich davon in Kenntnis.

(4) Wird die Benennung einer notifizierten Stelle ausgesetzt, eingeschränkt oder vollständig oder teilweise widerrufen, so setzt die notifizierte Stelle die betreffenden Hersteller spätestens innerhalb von zehn Tagen davon in Kenntnis.

(5) Wird eine Notifizierung eingeschränkt, ausgesetzt oder widerrufen, so ergreift die notifizierende Behörde geeignete Maßnahmen, um sicherzustellen, dass die Akten der betreffenden notifizierten Stelle für die notifizierenden Behörden in anderen Mitgliedstaaten und die Marktüberwachungsbehörden bereitgehalten und ihnen auf deren Anfrage zur Verfügung gestellt werden.

(6) Wird eine Benennung ausgesetzt, eingeschränkt oder widerrufen, so geht die notifizierende Behörde wie folgt vor:

a) Sie bewertet die Auswirkungen auf die von der notifizierten Stelle ausgestellten Bescheinigungen;

b) sie legt der Kommission und den anderen Mitgliedstaaten innerhalb von drei Monaten nach Meldung der Änderungen der Notifizierung einen Bericht über ihre diesbezüglichen Ergebnisse vor;

c) sie weist die notifizierte Stelle zur Gewährleistung der Konformität der im Verkehr befindlichen KI-Systeme an, sämtliche nicht ordnungsgemäß ausgestellten Bescheinigungen innerhalb einer von der Behörde festgelegten angemessenen Frist auszusetzen oder zu widerrufen;

d) sie informiert die Kommission und die anderen Mitgliedstaaten über Bescheinigungen, deren Aussetzung oder Widerruf sie angewiesen hat;

e) sie stellt den zuständigen nationalen Behörden des Mitgliedstaats, in dem der Anbieter seine eingetragene Niederlassung hat, alle relevanten Informationen über Bescheinigungen, deren Aussetzung oder Widerruf sie angewiesen hat, zur Verfügung. Die zuständige Behörde ergreift erforderlichenfalls geeignete Maßnahmen, um ein mögliches Risiko für Gesundheit, Sicherheit oder Grundrechte zu verhindern.

(7) Abgesehen von den Fällen, in denen Bescheinigungen nicht ordnungsgemäß ausgestellt wurden und in denen eine Notifizierung ausgesetzt oder eingeschränkt wurde, bleiben die Bescheinigungen unter folgenden Umständen gültig:

a) Die notifizierende Behörde hat innerhalb eines Monats nach der Aussetzung oder Einschränkung bestätigt, dass im Zusammenhang mit den von der Aussetzung oder Einschränkung betroffenen Bescheinigungen kein Risiko für Gesundheit, Sicherheit oder Grundrechte besteht, und die notifizierende Behörde hat einen Zeitplan sowie Maßnahmen genannt, die voraussichtlich dazu führen werden, dass die Aussetzung oder Einschränkung aufgehoben werden kann, oder

b) die notifizierende Behörde hat bestätigt, dass keine von der Aussetzung betroffenen Bescheinigungen während der Dauer der Aussetzung oder Einschränkung ausgestellt, geändert oder erneut ausgestellt werden, und gibt an, ob die notifizierte Stelle in der Lage ist, bestehende ausgestellte Bescheinigungen während der Dauer der Aussetzung oder Einschränkung weiterhin zu überwachen und die Verantwortung dafür zu übernehmen. Falls die für notifizierte Stellen zuständige Behörde feststellt, dass die notifizierte Stelle nicht in der Lage ist, bestehende Bescheinigungen weiterzuführen, so bestätigt der Anbieter der zuständigen nationalen Behörde des Mitgliedstaats, in dem der Anbieter des von der Bescheinigung abgedeckten Systems seine eingetragene Niederlassung hat, innerhalb von drei Monaten nach der Aussetzung oder Einschränkung schriftlich, dass eine andere qualifizierte notifizierte Stelle vorübergehend die Aufgaben der notifizierten Stelle zur Überwachung der Bescheinigungen übernimmt und dass sie während der Dauer der Aussetzung oder Einschränkung für die Bescheinigungen verantwortlich bleibt.

(8) Abgesehen von den Fällen, in denen Bescheinigungen nicht ordnungsgemäß ausgestellt wurden und in denen eine Benennung widerrufen wurde, bleiben die Bescheinigungen unter folgenden Umständen für eine Dauer von neun Monaten gültig:

a) Die zuständige nationale Behörde des Mitgliedstaats, in dem der Anbieter des von der Bescheinigung abgedeckten KI-Systems seine eingetragene Niederlassung hat, bestätigt, dass im Zusammenhang mit den betreffenden Systemen kein Risiko für Gesundheit, Sicherheit oder Grundrechte besteht, und

b) eine andere notifizierte Stelle hat schriftlich bestätigt, dass sie die unmittelbare Verantwortung für diese Systeme übernehmen und deren Bewertung innerhalb von zwölf Monaten ab dem Widerruf der Benennung abgeschlossen haben wird.

Unter den in Unterabsatz 1 genannten Umständen kann die zuständige nationale Behörde des Mitgliedstaats, in dem der Anbieter des von der Bescheinigung abgedeckten Systems seine Niederlassung hat, die vorläufige Gültigkeit der Bescheinigungen um weitere Zeiträume von je drei Monaten, zusammengenommen jedoch nicht um mehr als zwölf Monate, verlängern.

Die zuständige nationale Behörde oder die notifizierte Stelle, die die Aufgaben der von der Notifizierungsänderung betroffenen notifizierten Stelle übernimmt, teilt dies unverzüglich der Kommission, den anderen Mitgliedstaaten und den anderen notifizierten Stellen mit.

Artikel 37

Anfechtungen der Kompetenz notifizierter Stellen

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

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

(3) Die Kommission stellt sicher, dass alle im Verlauf ihrer Untersuchungen gemäß diesem Artikel erlangten vertraulichen Informationen im Einklang mit Artikel 70 vertraulich behandelt werden.

(4) Stellt die Kommission fest, dass eine notifizierte Stelle die in Artikel 33 festgelegten Anforderungen nicht oder nicht mehr erfüllt, so unterrichtet sie die notifizierende Behörde über die Gründe dieser Feststellung und fordert sie auf, die erforderlichen Korrekturmaßnahmen zu ergreifen, einschließlich der Aussetzung, der Einschränkung oder des Widerrufs der Benennung, sofern dies nötig ist. Versäumt es eine notifizierende Behörde, die erforderlichen Korrekturmaßnahmen zu ergreifen, kann die Kommission die Notifizierung mittels Durchführungsrechtsakten aussetzten, einschränken oder widerrufen. 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 Bezug auf Hochrisiko-KI-Systeme eine zweckmäßige Koordinierung und Zusammenarbeit zwischen den an den Konformitätsbewertungsverfahren im Rahmen dieser Verordnung beteiligten notifizierten Stellen in Form einer sektoralen Gruppe notifizierter Stellen eingerichtet und ordnungsgemäß weitergeführt wird.

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

Artikel 39

Konformitätsbewertungsstellen in Drittländern

Konformitätsbewertungsstellen, die nach dem Recht eines Drittlandes errichtet wurden, mit dem die Union ein Abkommen geschlossen hat, können ermächtigt werden, die Tätigkeiten notifizierter Stellen gemäß dieser Verordnung durchzuführen, sofern sie die in Artikel 33 festgelegten Anforderungen erfüllen.

KAPITEL 5

NORMEN, KONFORMITÄTSBEWERTUNG, BESCHEINIGUNGEN, REGISTRIERUNG

Artikel 40

Harmonisierte Normen

(1) Bei Hochrisiko-KI-Systemen oder KI-Systemen mit allgemeinem Verwendungszweck, die die harmonisierten Normen, deren Fundstellen im Amtsblatt der Europäischen Union veröffentlicht wurden, oder Teile dieser Normen erfüllen, wird eine Konformität mit den Anforderungen in Kapitel 2 dieses Titels oder gegebenenfalls mit den Anforderungen gemäß Artikel 4a und Artikel 4b vermutet, soweit diese Anforderungen von den Normen abgedeckt sind.

(2) Bei der Erteilung eines Normungsauftrags an die europäischen Normungsorganisationen gemäß Artikel 10 der Verordnung (EU) Nr. 1025/2012 gibt die Kommission an, dass die Normen kohärent, eindeutig und so abgefasst sind, dass sie insbesondere die folgenden Ziele erfüllen:

a) Sicherstellung, dass KI-Systeme, die in der Union in Verkehr gebracht oder in Betrieb genommen werden, sicher sind und die Werte der Union achten und die offene strategische Autonomie der Union stärken;

b) Förderung von Investitionen und Innovationen im Bereich der KI, auch durch die Steigerung der Rechtssicherheit, sowie der Wettbewerbsfähigkeit und des Wachstums des Unionsmarktes;

c) Verbesserung der Multi-Stakeholder-Governance, die alle relevanten europäischen Interessengruppen repräsentiert (z. B. Industrie, KMU, Zivilgesellschaft, Forschung);

d) Unterstützung der Stärkung der weltweiten Zusammenarbeit bei der Normung im Bereich der KI, die mit den Werten und Interessen der Union im Einklang steht.

Die Kommission fordert die europäischen Normungsorganisationen auf, nachzuweisen, dass sie sich nach besten Kräften bemühen, die genannten Ziele zu erreichen.

Artikel 41

Gemeinsame Spezifikationen

(1) Der Kommission wird die Befugnis übertragen, nach Anhörung des in Artikel 56 genannten KI-Ausschusses gemäß dem in Artikel 74 Absatz 2 genannten Prüfverfahren Durchführungsrechtsakte zu erlassen, um gemeinsame technische Spezifikationen für die Anforderungen in Kapitel 2 dieses Titels oder gegebenenfalls für die Anforderungen gemäß Artikel 4a und Artikel 4b festzulegen, wenn die folgenden Bedingungen erfüllt sind:

a) Im Amtsblatt der Europäischen Union sind im Einklang mit der Verordnung (EU) Nr. 1025/2012 keine Fundstellen zu harmonisierten Normen veröffentlicht, die die einschlägigen wesentlichen Bedenken in Bezug auf Sicherheit oder Grundrechte abdecken;

b) die Kommission hat gemäß Artikel 10 Absatz 1 der Verordnung (EU) Nr. 1025/2012 eine oder mehrere europäische Normungsorganisationen damit beauftragt, eine harmonisierte Norm für die Anforderungen in Kapitel 2 dieses Titels zu erarbeiten;

c) der in Buchstabe b genannte Auftrag wurde von keiner europäischen Normungsorganisation angenommen oder die für den Auftrag erarbeiteten harmonisierten Normen werden nicht innerhalb der gemäß Artikel 10 Absatz 1 der Verordnung (EU) Nr. 1025/2012 gesetzten Frist vorgelegt oder diese Normen genügen dem Auftrag nicht.

(1a) Vor der Ausarbeitung des Entwurfs eines Durchführungsrechtsakts teilt die Kommission dem in Artikel 22 der Verordnung (EU) Nr. 1025/2012 genannten Ausschuss mit, dass sie die Bedingungen nach Absatz 1 als erfüllt erachtet.

(2) In der frühen Ausarbeitungsphase des Entwurfs eines Durchführungsrechtsakts zur Festlegung einer gemeinsamen Spezifikation erfüllt die Kommission die in Artikel 40 Absatz 2 genannten Ziele und holt die Stellungnahmen der einschlägigen Stellen oder Expertengruppen ein, die nach den jeweiligen sektorspezifischen Rechtsvorschriften der Union eingerichtet wurden. Auf der Grundlage dieser Anhörung arbeitet die Kommission den Entwurf eines Durchführungsrechtsakts aus.

(3) Bei Hochrisiko-KI-Systemen oder KI-Systemen mit allgemeinem Verwendungszweck, die mit den in Absatz 1 genannten gemeinsamen Spezifikationen übereinstimmen, wird eine Konformität mit den Anforderungen in Kapitel 2 dieses Titels oder gegebenenfalls mit den Anforderungen gemäß Artikel 4a und Artikel 4b vermutet, soweit diese Anforderungen von den gemeinsamen Spezifikationen abgedeckt sind.

(4) Werden Fundstellen zu einer harmonisierten Norm im Amtsblatt der Europäischen Union veröffentlicht, so werden die in Absatz 1 genannten Durchführungsrechtsakte, die die Anforderungen in Kapitel 2 dieses Titels oder die Anforderungen gemäß Artikel 4a und Artikel 4b abdecken, gegebenenfalls aufgehoben.

(5) Ist ein Mitgliedstaat der Ansicht, dass eine gemeinsame Spezifikation nicht vollständig den Anforderungen in Kapitel 2 dieses Titels oder gegebenenfalls den Anforderungen gemäß Artikel 4a und Artikel 4b genügt, so setzt er die Kommission mit einer ausführlichen Erläuterung hiervon in Kenntnis, und die Kommission bewertet diese Informationen und ändert gegebenenfalls den betreffenden Durchführungsrechtsakt zur Festlegung einer gemeinsamen Spezifikation.

Artikel 42

Vermutung der Konformität mit bestimmten Anforderungen

(1) Für Hochrisiko-KI-Systeme, die mit Daten, in denen sich die besonderen geografischen, verhaltensbezogenen oder funktionalen Rahmenbedingungen niederschlagen, unter denen sie verwendet werden sollen, trainiert und getestet wurden, gilt die Vermutung, dass sie die entsprechenden in Artikel 10 Absatz 4 festgelegten Anforderungen erfüllen.

(2) Für Hochrisiko-KI-Systeme oder KI-Systeme mit allgemeinem Verwendungszweck, die im Rahmen eines Schemas für die Cybersicherheitszertifizierung gemäß der Verordnung (EU) 2019/881 des Europäischen Parlaments und des Rates[33], 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

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

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

---

[33] 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).

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

(2) Bei den in Anhang III Nummern 2 bis 8 aufgeführten Hochrisiko-KI-Systemen und bei den in Titel 1a genannten KI-Systemen mit allgemeinem Verwendungszweck befolgen die Anbieter das Konformitätsbewertungsverfahren auf der Grundlage einer internen Kontrolle gemäß Anhang VI, das keine Beteiligung einer notifizierten Stelle vorsieht.

(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) [gestrichen]

(5) Der Kommission wird die Befugnis übertragen, gemäß Artikel 73 delegierte Rechtsakte zu erlassen, um die Anhänge VI und VII angesichts des technischen Fortschritts zu aktualisieren.

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

Artikel 44

Bescheinigungen

(1) Die von notifizierten Stellen gemäß Anhang VII ausgestellten Bescheinigungen werden in einer Sprache ausgefertigt, die für die einschlägigen Behörden des Mitgliedstaats, in dem die notifizierte Stelle niedergelassen ist, leicht verständlich ist.

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

(3) Stellt eine notifizierte Stelle fest, dass ein KI-System die Anforderungen in Kapitel 2 dieses Titels nicht mehr erfüllt, setzt sie die ausgestellte Bescheinigung aus oder widerruft diese oder schränkt sie ein, jeweils unter Berücksichtigung des Grundsatzes der Verhältnismäßigkeit, 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

Es muss ein Einspruchsverfahren gegen die Entscheidungen der notifizierten Stellen vorgesehen sein.

Artikel 46

Meldepflichten der notifizierten Stellen

(1) Die notifizierten Stellen melden der notifizierenden Behörde

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

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

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

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

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

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

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

b) die EU-Bescheinigungen über die Bewertung der technischen Dokumentation und deren etwaige Ergänzungen, die sie verweigert, ausgesetzt oder zurückgenommen oder anderweitig eingeschränkt hat, und auf Anfrage die Bescheinigungen und/oder deren Ergänzungen, die sie ausgestellt hat.

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

(4) Die in den Absätzen 1 bis 3 dargelegten Pflichten werden im Einklang mit Artikel 70 erfüllt.

Artikel 47

Ausnahme vom Konformitätsbewertungsverfahren

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

(1a) In hinreichend begründeten dringenden Fällen aus außergewöhnlichen Gründen der öffentlichen Sicherheit oder in Fällen einer konkreten, erheblichen und unmittelbaren Gefahr für das Leben oder die körperliche Unversehrtheit natürlicher Personen können Strafverfolgungsbehörden oder Katastrophenschutzbehörden ein bestimmtes Hochrisiko-KI-System ohne die in Absatz 1 genannte Genehmigung in Betrieb nehmen, sofern diese Genehmigung während der Verwendung oder im Anschluss daran unverzüglich beantragt wird; falls diese Genehmigung abgelehnt wird, wird seine Verwendung mit sofortiger Wirkung eingestellt und sämtliche Ergebnisse dieser Verwendung werden unverzüglich verworfen.

(2) Die in Absatz 1 genannte Genehmigung wird nur erteilt, wenn die Marktüberwachungsbehörde zu dem Schluss gelangt, dass das Hochrisiko-KI-System die Anforderungen in Kapitel 2 dieses Titels erfüllt. Die Marktüberwachungsbehörde unterrichtet die Kommission und die anderen Mitgliedstaaten über alle von ihr gemäß Absatz 1 erteilten Genehmigungen. Diese Verpflichtung erstreckt sich nicht auf sensible operative Daten zu den Tätigkeiten von Strafverfolgungsbehörden.

(3) [gestrichen]

(4) [gestrichen]

(5) [gestrichen]

(6) Für Hochrisiko-KI-Systeme in Verbindung mit Produkten, die unter die in Anhang II Abschnitt A aufgeführten Harmonisierungsrechtsvorschriften der Union fallen, gelten nur die in den genannten Rechtsvorschriften festgelegten Ausnahmen von den Konformitätsbewertungsverfahren.

Artikel 48

EU-Konformitätserklärung

(1) Der Anbieter stellt für jedes KI-System eine schriftliche oder elektronisch unterzeichnete EU-Konformitätserklärung aus und hält sie für einen Zeitraum von 10 Jahren ab dem Inverkehrbringen oder der Inbetriebnahme des KI-Systems für die zuständigen nationalen Behörden bereit. Aus der EU-Konformitätserklärung geht hervor, für welches KI-System sie ausgestellt wurde. Ein Exemplar der EU-Konformitätserklärung wird den zuständigen nationalen Behörden auf Anfrage 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 Sprache übersetzt, die für die zuständigen nationalen Behörden des Mitgliedstaats bzw. der Mitgliedstaaten, in dem bzw. in denen das Hochrisiko-KI-System bereitgestellt wird, leicht verständlich ist.

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

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

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

Artikel 49

CE-Konformitätskennzeichnung

(1) Für die CE-Konformitätskennzeichnung gelten die allgemeinen Grundsätze des Artikels 30 der Verordnung (EG) Nr. 765/2008.

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

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

Artikel 50

[gestrichen]

Artikel 51

Registrierung betreffender Akteure und in Anhang III aufgeführter Hochrisiko-KI-Systeme

(1) Vor dem Inverkehrbringen oder der Inbetriebnahme eines in Anhang III aufgeführten Hochrisiko-KI-Systems, mit Ausnahme der in Anhang III Nummern 1, 6 und 7 genannten Hochrisiko-KI-Systeme in den Bereichen Strafverfolgung, Migration, Asyl und Grenzkontrolle und der in Anhang III Nummer 2 genannten Hochrisiko-KI-Systeme, registrieren sich der Anbieter und gegebenenfalls der Bevollmächtigte in der in Artikel 60 genannten EU-Datenbank. Der Anbieter oder gegebenenfalls der Bevollmächtigte registrieren ferner ihre Systeme in dieser Datenbank.

(2) Vor der Verwendung eines in Anhang III aufgeführten Hochrisiko-KI-Systems registrieren sich Nutzer von Hochrisiko-KI-Systemen, die Behörden, Einrichtungen oder sonstige Stellen sind, oder in ihrem Namen handelnde Einrichtungen in der in Artikel 60 genannten EU-Datenbank und wählen das System aus, dessen Verwendung sie planen.

Die in Unterabsatz 1 festgelegten Pflichten gelten weder für Behörden, Einrichtungen oder sonstige Stellen in den Bereichen Strafverfolgung, Grenzschutz, Einwanderung oder Asyl noch für Behörden, Einrichtungen oder sonstige Stellen, die die in Anhang III Nummer 2 genannten Hochrisiko-KI-Systeme verwenden, noch für in ihrem Namen handelnde Einrichtungen.

TITEL IV

TRANSPARENZPFLICHTEN FÜR ANBIETER UND NUTZER BESTIMMTER KI-SYSTEME

Artikel 52

Transparenzpflichten für Anbieter und Nutzer bestimmter KI-Systeme

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

(2) Die Nutzer eines Systems zur biometrischen Kategorisierung informieren die davon betroffenen natürlichen Personen über den Betrieb des Systems. Diese Vorgabe gilt nicht für gesetzlich zur Aufdeckung, Verhütung, Ermittlung und Verfolgung von Straftaten zugelassene KI-Systeme, die zur biometrischen Kategorisierung verwendet werden, wenn geeignete Schutzvorkehrungen für die Rechte und Freiheiten Dritter bestehen.

(2a) Die Nutzer eines Emotionserkennungssystems informieren die davon betroffenen natürlichen Personen über den Betrieb des Systems. Diese Vorgabe gilt nicht für gesetzlich zur Aufdeckung, Verhütung, Ermittlung und Verfolgung von Straftaten zugelassene KI-Systeme, die als Emotionserkennungssysteme eingesetzt werden, wenn geeignete Schutzvorkehrungen für die Rechte und Freiheiten Dritter bestehen.

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

Unterabsatz 1 gilt jedoch nicht, wenn die Verwendung zur Aufdeckung, Verhütung, Ermittlung und Verfolgung von Straftaten gesetzlich zugelassen oder der Inhalt Teil eines offensichtlich kreativen, satirischen, künstlerischen oder fiktionalen Werks oder Programms ist und geeignete Schutzvorkehrungen für die Rechte und Freiheiten Dritter bestehen.

(3a) Die in den Absätzen 1 bis 3 genannten Informationen werden den natürlichen Personen spätestens zum Zeitpunkt der ersten Interaktion oder Aussetzung in klarer und eindeutiger Weise bereitgestellt.

(4) Die Absätze 1, 2, 2a, 3 und 3a lassen die in Titel III dieser Verordnung festgelegten Anforderungen und Pflichten sowie andere im Unionsrecht oder im einzelstaatlichen Recht festlegte Transparenzpflichten für Nutzer von KI-Systemen unberührt.

TITEL V

MAßNAHMEN ZUR INNOVATIONSFÖRDERUNG

Artikel 53

KI-Reallabore

(-1a) Die zuständigen nationalen Behörden können KI-Reallabore einrichten, um unter ihrer direkten Aufsicht, Anleitung und Unterstützung innovative KI-Systeme zu entwickeln, zu trainieren, zu testen und zu validieren, bevor diese in Verkehr gebracht oder in Betrieb genommen werden. In diesen Reallaboren können unter der Aufsicht der zuständigen nationalen Behörden auch Tests unter realen Bedingungen durchgeführt werden.

(-1b) [gestrichen]

(-1c) Gegebenenfalls arbeiten die zuständigen nationalen Behörden mit anderen einschlägigen Behörden zusammen und können die Einbeziehung anderer Akteure des KI-Ökosystems gestatten.

(-1d) Andere Reallabore, die im Rahmen des nationalen Rechts oder des Unionsrechts eingerichtet wurden, bleiben von diesem Artikel unberührt; das gilt auch für Reallabore, in deren Fall die getesteten Produkte oder Dienste mit der Verwendung innovativer KI-Systeme in Zusammenhang stehen. Die Mitgliedstaaten sorgen dafür, dass die diese anderen Reallabore beaufsichtigenden Behörden und die zuständigen nationalen Behörden angemessen zusammenarbeiten.

(1) [gestrichen]

(1a) [gestrichen]

(1b) Die Einrichtung von KI-Reallaboren im Rahmen dieser Verordnung ist auf eine oder mehrere der folgenden Zielsetzungen ausgerichtet:

a) Förderung von Wettbewerbsfähigkeit und Innovation sowie Erleichterung der Entwicklung eines KI-Systems;
b) Erleichterung und Beschleunigung des Zugangs von KI-Systemen zum Unionsmarkt, insbesondere, wenn sie von kleinen und mittleren Unternehmen (KMU) und Start-up-Unternehmen angeboten werden;
c) Verbesserung der Rechtssicherheit und Förderung des Austauschs bewährter Verfahren durch Zusammenarbeit mit den am KI-Reallabor beteiligten Behörden, um für die künftige Einhaltung dieser Verordnung sowie gegebenenfalls die Einhaltung der Rechtsvorschriften der Union und der Mitgliedstaaten zu sorgen;
d) Leisten eines Beitrags zum faktengestützten regulatorischen Lernen.

(2) [gestrichen]

(2a) Der Zugang zu den KI-Reallaboren steht allen Anbietern oder zukünftigen Anbietern von KI-Systemen offen, die die in Absatz 6 Buchstabe a genannten Voraussetzungen und Auswahlkriterien erfüllen und von den zuständigen nationalen Behörden nach dem in Absatz 6 Buchstabe b genannten Auswahlverfahren ausgewählt wurden. Anbieter oder zukünftige Anbieter können den Antrag auch zusammen mit Nutzern oder einschlägigen Dritten, die ihre Partner sind, stellen.

Die Beteiligung an dem KI-Reallabor beschränkt sich auf einen der Komplexität und dem Umfang des Projekts entsprechenden Zeitraum. Dieser Zeitraum kann von den zuständigen nationalen Behörden verlängert werden.

Die Beteiligung an dem KI-Reallabor erfolgt auf der Grundlage eines besonderen Plans gemäß Absatz 6 und wird gegebenenfalls zwischen den/dem Beteiligten und den zuständigen nationalen Behörden vereinbart.

(3) Die Aufsichts- und Abhilfebefugnisse der das KI-Reallabor beaufsichtigenden Behörden bleiben von der Beteiligung an KI-Reallaboren unberührt. Um Innovationen im Bereich KI in der Union zu unterstützen, üben die betreffenden Behörden ihre Aufsichtsbefugnisse im Rahmen der geltenden Rechtsvorschriften flexibel aus, indem sie bei der Anwendung der Rechtsvorschriften auf ein bestimmtes KI-Reallabor ihren Ermessensspielraum nutzen.

Wenn der/die Beteiligte(n) den Plan für das Reallabor und die in Absatz 6 Buchstabe c genannten Anforderungen und Bedingungen für die Beteiligung erfüllt bzw. erfüllen und der Anleitung durch die Behörden in gutem Glauben folgt bzw. folgen, werden bei Verletzung der für das im Reallabor beaufsichtigte KI-System geltenden Rechtsvorschriften der Union oder der Mitgliedstaaten, einschließlich der Bestimmungen dieser Verordnung, keine Geldbußen verhängt.

(4) Die Beteiligten bleiben nach geltendem Recht der Union und der Mitgliedstaaten für Schäden haftbar, die während ihrer Beteiligung an einem KI-Reallabor entstehen.

(4a) Die zuständige nationale Behörde legt dem Anbieter oder zukünftigen Anbieter des KI-Systems auf dessen Anfrage gegebenenfalls einen schriftlichen Nachweis für die im Reallabor erfolgreich durchgeführten Tätigkeiten vor. Außerdem legt die zuständige nationale Behörde einen Abschlussbericht vor, in dem sie die im Reallabor durchgeführten Tätigkeiten, deren Ergebnisse und die gewonnenen Erkenntnisse im Einzelnen darlegt. Dieser schriftliche Nachweis und der Abschlussbericht sollten je nach Sachlage von den Marktüberwachungsbehörden oder den notifizierten Stellen bei Konformitätsbewertungsverfahren oder Marktüberwachungskontrollen berücksichtigt werden.

Vorbehaltlich der in Artikel 70 festgelegten Bestimmungen über die Vertraulichkeit und im Einklang mit der Vereinbarung der an dem Reallabor Beteiligten, sind die Europäische Kommission und der KI-Ausschuss befugt, die Abschlussberichte einzusehen und tragen diesen gegebenenfalls bei der Wahrnehmung ihrer Aufgaben gemäß dieser Verordnung Rechnung. Wenn der Beteiligte und die zuständige nationale Behörde dies ausdrücklich vereinbaren, kann der Abschlussbericht über die zentrale Informationsplattform im Sinne von Artikel 55 Absatz 3 Buchstabe b veröffentlicht werden.

(4b) Die KI-Reallabore sind so konzipiert und werden so umgesetzt, dass sie gegebenenfalls die grenzüberschreitende Zusammenarbeit zwischen zuständigen nationalen Behörden erleichtern.

(5) Die zuständigen nationalen Behörden veröffentlichen jährliche Berichte über die Umsetzung der KI-Reallabore, einschließlich bewährter Verfahren, gewonnener Erkenntnisse und Empfehlungen zu deren Aufbau, sowie gegebenenfalls über die Anwendung dieser Verordnung und anderer Rechtsvorschriften der Union, die innerhalb des Reallabors kontrolliert werden. Diese jährlichen Berichte werden dem KI-Ausschuss vorgelegt, der eine Übersicht mit allen bewährten Verfahren, gewonnenen Erkenntnissen und Empfehlungen veröffentlicht. Diese Pflicht zur Veröffentlichung der jährlichen Berichte erstreckt sich nicht auf sensible operative Daten zu den Tätigkeiten von Strafverfolgungs-, Grenzschutz-, Einwanderungs- oder Asylbehörden. Die Kommission und der KI-Ausschuss tragen den jährlichen Berichten gegebenenfalls bei der Wahrnehmung ihrer Aufgaben gemäß dieser Verordnung Rechnung.

(5b) Die Kommission stellt sicher, dass über die KI-Reallabore, einschließlich der nach diesem Artikel eingerichteten Reallabore, über die zentrale Informationsplattform im Sinne von Artikel 55 Absatz 3 Buchstabe b Informationen verfügbar sind.

(6) Die Modalitäten und Bedingungen für die Einrichtung und den Betrieb der KI-Reallabore im Sinne dieser Verordnung werden im Wege von Durchführungsrechtsakten gemäß dem in Artikel 74 Absatz 2 genannten Prüfverfahren erlassen.

Diese Modalitäten und Bedingungen tragen so weit wie möglich dazu bei, dass zuständige nationale Behörden über die Flexibilität verfügen, eigene KI-Reallabore einzurichten und zu betreiben, und dass Innovationen und regulatorisches Lernen gefördert werden, und sie tragen den besonderen Umständen und Kapazitäten beteiligter KMU, einschließlich Start-up-Unternehmen, Rechnung.

In den Durchführungsrechtsakten sind gemeinsame Grundsätze zu den folgenden Aspekten festgelegt:

a) Voraussetzungen und Auswahl für eine Beteiligung am KI-Reallabor;
b) Verfahren für Antragstellung, Beteiligung, Überwachung, Ausstieg und Beendigung bezüglich des KI-Reallabors, einschließlich Plan und Abschlussbericht für das Reallabor;
c) für Beteiligte geltende Anforderungen und Bedingungen.

(7) Wenn zuständige nationale Behörden die Genehmigung von Tests unter realen Bedingungen, die im Rahmen eines nach diesem Artikel eingerichteten KI-Reallabors beaufsichtigt werden, in Betracht zieht, vereinbaren sie mit den Beteiligten ausdrücklich die Anforderungen und Bedingungen für diese Tests und insbesondere geeignete Schutzvorkehrungen für die Grundrechte sowie für Gesundheit und Sicherheit. Gegebenenfalls arbeiten sie mit anderen zuständigen nationalen Behörden zusammen, um für unionsweit einheitliche Verfahrensweisen zu sorgen.

Artikel 54

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

(1) Rechtmäßig für andere Zwecke erhobene personenbezogene Daten dürfen im KI-Reallabor für die Zwecke der Entwicklung, der Tests und des Trainings innovativer KI-Systeme im Reallabor verarbeitet werden, wenn die folgenden kumulativen Bedingungen erfüllt sind:

a) Die innovativen KI-Systeme werden zur Wahrung eines erheblichen öffentlichen Interesses durch eine Behörde oder eine andere natürliche oder juristische Person des öffentlichen Rechts oder des Privatrechts und in einem oder mehreren der folgenden Bereiche entwickelt:

i) [gestrichen]

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

iii) Schutz und Verbesserung der Umweltqualität, einschließlich grüner Wandel, Klimaschutz und Anpassung an den Klimawandel,

iv) nachhaltige Energie, Verkehr und Mobilität,

v) Effizienz und Qualität der öffentlichen Verwaltung und öffentlicher Dienste,

vi) Cybersicherheit und Resilienz kritischer Infrastrukturen;

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, mit deren Hilfe festgestellt wird, ob während der Reallaborversuche hohe Risiken für die Rechte und Freiheiten von betroffenen Personen gemäß Artikel 35 der Verordnung (EU) 2016/679 und gemäß Artikel 39 der Verordnung (EU) 2018/1725 auftreten können, sowie Reaktionsmechanismen, mit deren Hilfe diese Risiken umgehend eingedämmt werden können und die Verarbeitung bei Bedarf beendet werden kann;

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

e) verarbeitete personenbezogene Daten werden an Dritte, die nicht an dem Reallabor beteiligt sind, nicht übermittelt oder übertragen, noch haben diese Dritten anderweitig Zugang zu diesen Daten, es sei denn, diese Offenlegung erfolgt im Einklang mit der Verordnung (EU) 2016/679 oder gegebenenfalls gemäß der Verordnung (EU) 2018/725 und mit der Zustimmung aller Beteiligten;

f) die Verarbeitung personenbezogener Daten im Rahmen des Reallabors wirkt sich nicht auf die Anwendung der in den Rechtsvorschriften der Union über den Schutz personenbezogener Daten, insbesondere in Artikel 22 der Verordnung (EU) 2016/679 und in Artikel 24 der Verordnung (EU) 2018/1725, festgelegten Rechte von betroffenen Personen aus;

g) im Rahmen des Reallabors verarbeitete personenbezogene Daten sind durch geeignete technische und organisatorische Maßnahmen geschützt und werden gelöscht, sobald die Beteiligung an dem Reallabor endet 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, es sei denn, im Unionsrecht oder im einzelstaatlichen Recht ist etwas anderes bestimmt;

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

j) eine kurze Zusammenfassung des im KI-Reallabor entwickelten KI-Projekts, seiner Ziele und erwarteten Ergebnisse wird auf der Website der zuständigen Behörden veröffentlicht. Diese Pflicht erstreckt sich nicht auf sensible operative Daten zu den Tätigkeiten von Strafverfolgungs-, Grenzschutz-, Einwanderungs- oder Asylbehörden.

(1a) Für die Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung – einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit – unter der Kontrolle und Verantwortung der Strafverfolgungsbehörden, erfolgt die Verarbeitung personenbezogener Daten im Rahmen von KI-Reallaboren auf der Grundlage des Rechts des betreffenden Mitgliedstaats oder des Unionsrechts und unterliegt den kumulativen Bedingungen des Absatzes 1.

(2) Die Rechtsvorschriften der Union oder der Mitgliedstaaten, in denen die Grundlagen für eine für die Zwecke der Entwicklung, der Tests und des Trainings innovativer KI-Systeme notwendige Verarbeitung personenbezogener Daten festgelegt sind, oder jegliche anderen dem Unionsrecht zum Schutz personenbezogener Daten entsprechenden Rechtsgrundlagen bleiben von Absatz 1 unberührt.

Artikel 54a

Tests von Hochrisiko-KI-Systemen unter realen Bedingungen außerhalb von KI-Reallaboren

(1) Tests von KI-Systemen unter realen Bedingungen können von den in Anhang III aufgeführten Anbietern oder zukünftigen Anbietern von Hochrisiko-KI-Systemen außerhalb von KI-Reallaboren im Einklang mit den Bestimmungen dieses Artikels und dem in diesem Artikel genannten Plan für Tests unter realen Bedingungen durchgeführt werden.

Die einzelnen Elemente des Plans für Tests unter realen Bedingungen werden in Durchführungsrechtsakten festgelegt, die von der Kommission gemäß dem in Artikel 74 Absatz 2 genannten Prüfverfahren erlassen werden.

Die im Falle von Hochrisiko-KI-Systemen in Verbindung mit Produkten, die unter die in Anhang II aufgeführten Rechtsvorschriften fallen, für Tests unter realen Bedingungen geltenden Rechtsvorschriften der Union oder der Mitgliedstaaten bleiben von dieser Bestimmung unberührt.

(2) Anbieter oder zukünftige Anbieter können in Anhang III aufgeführte Hochrisiko-KI-Systeme vor deren Inverkehrbringen oder Inbetriebnahme jederzeit selbst oder in Partnerschaft mit einem oder mehreren zukünftigen Nutzern unter realen Bedingungen testen.

(3) Tests von KI-Systemen unter realen Bedingungen gemäß diesem Artikel lassen nach dem nationalen Recht oder dem Unionsrecht gegebenenfalls vorgeschriebene Ethikprüfungen unberührt.

(4) Tests unter realen Bedingungen dürfen von Anbietern oder zukünftigen Anbietern nur durchgeführt werden, wenn alle der folgenden Bedingungen erfüllt sind:

a) Der Anbieter oder der zukünftige Anbieter hat einen Plan für Tests unter realen Bedingungen erstellt und diesen bei der Marktüberwachungsbehörde in dem/den Mitgliedstaat(en) eingereicht, in dem/denen der Test unter realen Bedingungen stattfinden soll;

b) die Marktüberwachungsbehörde in dem/den Mitgliedstaat(en), in dem/denen der Test unter realen Bedingungen stattfinden soll, hat binnen 30 Tagen nach der Einreichung keine Einwände gegen den Test erhoben;

c) der Anbieter oder der zukünftige Anbieter von KI-Systemen, mit Ausnahme der in Anhang III Nummern 1, 6 und 7 genannten Hochrisiko-KI-Systeme in den Bereichen Strafverfolgung, Migration, Asyl und Grenzkontrolle und der in Anhang III Nummer 2 genannten Hochrisiko-KI-Systeme, hat den Test unter realen Bedingungen unter Angabe einer unionsweit einmaligen Kennnummer und der in Anhang VIIIa festgelegten Informationen in der EU-Datenbank gemäß Artikel 60 Absatz 5a registriert;

d) der Anbieter oder der zukünftige Anbieter, der den Test unter realen Bedingungen durchführt, ist in der Union niedergelassen oder hat für die Zwecke des Tests unter realen Bedingungen einen in der Union niedergelassenen gesetzlichen Vertreter bestellt;

e) die für die Zwecke von Tests unter realen Bedingungen erhobenen und verarbeiteten Daten werden nicht an Länder außerhalb der Union übertragen, es sei denn, bei der Übertragung und der Verarbeitung greifen Schutzvorkehrungen, die jenen des Unionsrechts gleichwertig sind;

f) der Test unter realen Bedingungen dauert nicht länger als zur Erfüllung seiner Zielsetzungen nötig und in keinem Fall länger als 12 Monate;

g) Personen, die aufgrund ihres Alters oder einer körperlichen oder geistigen Behinderung einer schutzbedürftigen Gruppe angehören, sind angemessen geschützt;

h) [gestrichen]

i) wenn ein Anbieter oder zukünftiger Anbieter den Test unter realen Bedingungen in Zusammenarbeit mit einem oder mehreren zukünftigen Nutzern organisiert, wird bzw. werden Letztere(r) vorab über alle für ihre Teilnahmeentscheidung relevanten Aspekte des Tests informiert und erhalten die einschlägigen, in Artikel 13 genannten Gebrauchsanweisungen für das KI-System. Der Anbieter oder der zukünftige Anbieter und der/die Nutzer schließen eine Vereinbarung, in der ihre Aufgaben und Zuständigkeiten festgelegt sind, um für die Einhaltung der nach dieser Verordnung und anderen Rechtsvorschriften der Union und der Mitgliedstaaten für Tests unter realen Bedingungen geltenden Bestimmungen zu sorgen;

j) die Teilnehmer an Tests unter realen Bedingungen erteilen ihre sachkundige Einwilligung gemäß Artikel 54b, oder, wenn im Fall der Strafverfolgung die Einholung einer sachkundigen Einwilligung einen Test des KI-Systems verhindern würde, dürfen sich der Test und die Ergebnisse des Tests unter realen Bedingungen nicht negativ auf den Testteilnehmer auswirken;

k) der Anbieter oder zukünftige Anbieter und der/die Nutzer lassen den Test unter realen Bedingungen von Personen überwachen, die auf dem betreffenden Gebiet angemessen qualifiziert sind und über die Kapazitäten, die Ausbildung und die Befugnisse verfügen, die für die Wahrnehmung ihrer Aufgaben erforderlich sind;

l) die Vorhersagen, Empfehlungen oder Entscheidungen des KI-Systems können effektiv außer Acht gelassen oder rückgängig gemacht werden.

(5) Jeder Teilnehmer an einem Test unter realen Bedingungen oder gegebenenfalls dessen gesetzlicher Vertreter kann seine Teilnahme an dem Test jederzeit durch Widerruf seiner sachkundigen Einwilligung beenden, ohne dass ihm daraus Nachteile entstehen und er dies in irgendeiner Weise begründen müsste. Der Widerruf der sachkundigen Einwilligung wirkt sich nicht auf bereits durchgeführte Tätigkeiten und die Nutzung von Daten aus, die aufgrund der sachkundigen Einwilligung vor deren Widerrufung erhoben wurden.

(6) Jegliche schwerwiegenden Vorfälle im Verlauf des Tests unter realen Bedingungen sind den Marktüberwachungsbehörden gemäß Artikel 62 dieser Verordnung zu melden. Der Anbieter oder zukünftige Anbieter trifft Sofortmaßnahmen zur Schadensbegrenzung, andernfalls setzt er den Test unter realen Bedingen so lange aus, bis eine Schadensbegrenzung stattgefunden hat, oder bricht ihn ab. Im Fall eines solchen Abbruchs des Tests unter realen Bedingungen richtet der Anbieter oder zukünftige Anbieter ein Verfahren für den sofortigen Rückruf des KI-Systems ein.

(7) Anbieter oder zukünftige Anbieter setzen die Marktüberwachungsbehörde in dem/den Mitgliedstaat(en), in dem/denen der Test unter realen Bedingungen stattfindet, über die Aussetzung oder den Abbruch des Tests unter realen Bedingungen und die Endergebnisse in Kenntnis.

(8) Der Anbieter oder zukünftige Anbieter sind nach geltendem Recht der Union und der Mitgliedstaaten für Schäden haftbar, die während ihrer Teilnahme an einem Test unter realen Bedingungen entstehen.

Artikel 54b

Sachkundige Einwilligung zur Teilnahme an Tests unter realen Bedingungen außerhalb von KI-Reallaboren

(1) Für die Zwecke der Tests unter realen Bedingungen gemäß Artikel 54a erteilt der Testteilnehmer freiwillig seine sachkundige Einwilligung, bevor er an dem Test teilnimmt und nachdem er mit präzisen, klaren, relevanten und verständlichen Informationen über Folgendes ordnungsgemäß aufgeklärt wurde:

i) die Art und die Zielsetzungen des Tests unter realen Bedingungen und etwaige mit der Teilnahme verbundene Unannehmlichkeiten;

ii) die Bedingungen, unter denen der Test unter realen Bedingungen erfolgen soll, einschließlich der voraussichtlichen Dauer der Teilnahme;

iii) die Rechte und Garantien, die ihm bezüglich der Teilnahme zustehen, insbesondere sein Recht, die Teilnahme an dem Test zu verweigern oder diese Teilnahme jederzeit zu beenden, ohne dass ihm daraus Nachteile entstehen und er dies in irgendeiner Weise begründen müsste;

iv) die Modalitäten, unter denen die Außerachtlassung oder Rückgängigmachung der Vorhersagen, Empfehlungen oder Entscheidungen des KI-Systems beantragt werden kann;

v) die unionsweit einmalige Kennnummer des Tests unter realen Bedingungen gemäß Artikel 54a Absatz 4 Buchstabe c und die Kontaktdaten des Anbieters oder seines gesetzlichen Vertreters, bei dem weitere Informationen eingeholt werden können.

(2) Die sachkundige Einwilligung ist zu datieren und zu dokumentieren, und eine Fassung wird dem Testteilnehmer oder seinem gesetzlichen Vertreter ausgehändigt.

Artikel 55

Unterstützungsmaßnahmen für Akteure, insbesondere KMU, einschließlich Start-up-Unternehmen

(1) Die Mitgliedstaaten ergreifen die folgenden Maßnahmen:

a) Sie gewähren KMU, einschließlich Start-up-Unternehmen, soweit sie die entsprechenden Voraussetzungen und Auswahlkriterien erfüllen, vorrangigen Zugang zu den KI-Reallaboren.

b) Sie führen besondere Sensibilisierungs- und Schulungsmaßnahmen für die Anwendung dieser Verordnung durch, die auf die Bedürfnisse von KMU, einschließlich Start-up-Unternehmen, sowie gegebenenfalls lokaler Behörden ausgerichtet sind.

c) Sie richten gegebenenfalls einen eigenen Kanal für die Kommunikation mit KMU, einschließlich Start-up-Unternehmen, sowie gegebenenfalls mit lokalen Behörden, ein, um Orientierung zu geben und Fragen zur Umsetzung dieser Verordnung, auch bezüglich der Beteiligung an KI-Reallaboren, zu beantworten.

(2) Bei der Festsetzung der Gebühren für die Konformitätsbewertung gemäß Artikel 43 werden die besonderen Interessen und Bedürfnisse von Anbietern, die KMU oder auch Start-up-Unternehmen sind, berücksichtigt, indem diese Gebühren proportional zur Größe der Unternehmen, der Größe ihres Marktes und anderen einschlägigen Kennzahlen gesenkt werden.

(3) Die Kommission ergreift die folgenden Maßnahmen:

a) Sie stellt auf Anfrage des KI-Ausschusses standardisierte Muster für die unter diese Verordnung fallenden Bereiche bereit.

b) Sie entwickelt und führt eine zentrale Informationsplattform, über die allen Akteuren in der Union leicht nutzbare Informationen zu dieser Verordnung bereitgestellt werden.

c) Sie veranstaltet entsprechende Informationskampagnen, um für die aus dieser Verordnung erwachsenden Pflichten zu sensibilisieren.

d) Sie bewertet und fördert die Zusammenführung bewährter Verfahren im Bereich der mit KI-Systemen verbundenen Vergabeverfahren.

Artikel 55a

Ausnahmen für bestimmte Akteure

(1) Für Kleinstunternehmen im Sinne von Artikel 2 Absatz 3 des Anhangs der Empfehlung 2003/361/EG der Kommission betreffend die Definition der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen gelten die Pflichten gemäß Artikel 17 dieser Verordnung nicht, wenn diese Unternehmen keine Partnerunternehmen oder verbundenen Unternehmen im Sinne von Artikel 3 des genannten Anhangs haben.

(2) Absatz 1 ist nicht dahingehend auszulegen, dass diese Akteure auch von anderen Anforderungen und Pflichten dieser Verordnung, einschließlich der nach den Artikeln 9, 61 und 62 geltenden, befreit sind.

(3) Für Kleinstunternehmen und für kleine und mittlere Unternehmen gelten die Anforderungen und Pflichten für KI-Systeme mit allgemeinem Verwendungszweck gemäß Artikel 4b nicht, wenn sie keine Partnerunternehmen oder verbundenen Unternehmen im Sinne von Artikel 3 des Anhangs der Empfehlung 2003/361/EG der Kommission betreffend die Definition der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen haben.

TITEL VI

LEITUNGSSTRUKTUR

KAPITEL 1

EUROPÄISCHER AUSSCHUSS FÜR KÜNSTLICHE INTELLIGENZ

Artikel 56

Einrichtung und Struktur des Europäischen Ausschusses für künstliche Intelligenz

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

(2) Der KI-Ausschuss setzt sich aus einem Vertreter je Mitgliedstaat zusammen. Der Europäische Datenschutzbeauftragte nimmt als Beobachter teil. Die Kommission nimmt ebenfalls an den Sitzungen des KI-Ausschusses teil, ohne sich jedoch an den Abstimmungen zu beteiligen.

Behörden, Gremien oder Sachverständige der Mitgliedstaaten und der Union können im Einzelfall zu den Sitzungen des KI-Ausschusses eingeladen werden, wenn die erörterten Fragen für sie von Belang sind.

(2a) Die Vertreter werden von ihren Mitgliedstaaten für einen Zeitraum von drei Jahren benannt, der einmal verlängert werden kann.

(2aa) Die Mitgliedstaaten sorgen dafür, dass ihre Vertreter im KI-Ausschuss

i) in ihrem Mitgliedstaat über die einschlägigen Kompetenzen und Befugnisse verfügen, sodass sie aktiv zur Bewältigung der in Artikel 58 genannten Aufgaben des KI-Ausschusses beitragen können;

ii) gegenüber dem KI-Ausschuss sowie gegebenenfalls, unter Berücksichtigung der Erfordernisse der Mitgliedstaaten, gegenüber Interessenträgern als zentrale Ansprechpartner fungieren;

iii) ermächtigt sind, auf die Kohärenz und die Abstimmung zwischen den zuständigen nationalen Behörden in ihrem Mitgliedstaat bei der Umsetzung dieser Verordnung hinzuwirken, auch durch Erhebung einschlägiger Daten und Informationen für die Zwecke der Erfüllung ihrer Aufgaben im KI-Ausschuss.

(3) Die benannten Vertreter der Mitgliedstaaten nehmen die Geschäftsordnung des KI-Ausschusses mit einer Zweidrittelmehrheit an.

In der Geschäftsordnung sind insbesondere die Vorgehensweise für das Auswahlverfahren, die Dauer des Mandats und die genauen Aufgaben des Vorsitzes, die Abstimmungsmodalitäten und die Organisation der Tätigkeiten des KI-Ausschusses und seiner Untergruppen festgelegt.

Der KI-Ausschuss richtet eine ständige Untergruppe ein, die Interessenträgern als Plattform zur Beratung des KI-Ausschusses in allen mit der Umsetzung dieser Verordnung verbundenen Fragen, einschließlich der Ausarbeitung von Durchführungsrechtsakten und delegierten Rechtsakten, dient. Für diese Zwecke werden Organisationen, die die Interessen der Anbieter und der Nutzer von KI-Systemen vertreten, einschließlich KMU und Start-up-Unternehmen, sowie Organisationen der Zivilgesellschaft, Vertreter betroffener Personen, Wissenschaftler, Normungsgremien, notifizierte Stellen, Labore sowie Test- und Versuchseinrichtungen zur Mitarbeit in dieser Untergruppe eingeladen. Der KI-Ausschuss richtet zwei ständige Untergruppen ein, um Marktüberwachungsbehörden und notifizierenden Behörden für die Zusammenarbeit und den Austausch in Fragen, die die Marktaufsicht bzw. notifizierende Behörden betreffen, eine Plattform zu bieten.

Der KI-Ausschuss kann weitere ständige oder nichtständige Untergruppen einrichten, falls das für die Prüfung bestimmter Fragen zweckmäßig sein sollte. Die im vorangehenden Unterabsatz genannten Interessenträger können gegebenenfalls in solche Untergruppen oder zu bestimmten Sitzungen dieser Untergruppen als Beobachter eingeladen werden.

(3a) Der KI-Ausschuss gewährleistet durch seine Organisation und Arbeitsweise, dass bei seinen Tätigkeiten Objektivität und Unparteilichkeit gewahrt sind.

(4) Den Vorsitz im KI-Ausschuss führt einer der Vertreter der Mitgliedstaaten. Die Kommission beruft auf Anfrage des Vorsitzes die Sitzungen ein und erstellt die Tagesordnung im Einklang mit den Aufgaben des KI-Ausschusses gemäß dieser Verordnung und seiner Geschäftsordnung. Die Kommission leistet bezüglich der Tätigkeiten des KI-Ausschusses gemäß dieser Verordnung administrative und analytische Unterstützung.

Artikel 57

[gestrichen]

Artikel 58

Aufgaben des KI-Ausschusses

Der KI-Ausschuss berät und unterstützt die Kommission und die Mitgliedstaaten, um der einheitlichen und wirksamen Anwendung dieser Verordnung den Weg zu ebnen. Für diese Zwecke kann der KI-Ausschuss insbesondere

a) technisches und regulatorisches Fachwissen und bewährte Verfahren zusammentragen und unter den Mitgliedstaaten verbreiten;

b) zur Harmonisierung der Verwaltungspraxis in den Mitgliedstaaten beitragen, auch bezüglich der Ausnahme vom Konformitätsbewertungsverfahren gemäß Artikel 47 und der Funktionsweise von KI-Reallaboren und Tests unter realen Bedingungen gemäß den Artikeln 53, 54 und 54a;

c) auf Anfrage der Kommission oder in Eigeninitiative Empfehlungen und schriftliche Stellungnahmen zu einschlägigen Fragen der Umsetzung dieser Verordnung und ihrer einheitlichen und wirksamen Anwendung abgeben, unter anderem

   i) zu technischen Spezifikationen oder geltenden Normen in Bezug auf die in Titel III Kapitel 2 festgelegten Anforderungen,

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

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

d) die Kommission unter Berücksichtigung der einschlägigen Erkenntnisse und der aktuellen technologischen Entwicklungen bezüglich der möglicherweise notwendigen Änderung von Anhang III gemäß den Artikeln 4 und 7 beraten;

e) die Kommission bezüglich der Ausarbeitung von Durchführungsrechtsakten und delegierten Rechtsakten gemäß dieser Verordnung beraten;

f) gegebenenfalls mit einschlägigen Einrichtungen, Sachverständigengruppen und Netzwerken der EU insbesondere in den Bereichen Produktsicherheit, Cybersicherheit, Wettbewerb, digitale und Mediendienste, Finanzdienstleistungen, Kryptowährungen, Verbraucherschutz, Datenschutz und Schutz der Grundrechte zusammenarbeiten;

g) zur Erarbeitung der in Artikel 58a genannten Leitlinien beitragen und die Kommission diesbezüglich beraten bzw. die Erarbeitung entsprechender Leitlinien verlangen;

h) die Marktüberwachungsbehörden bei der Arbeit unterstützen sowie – in Zusammenarbeit und vorbehaltlich der Zustimmung der betreffenden Marktüberwachungsbehörden – grenzüberschreitende Marktüberwachungsermittlungen, auch zu von KI-Systemen ausgehenden systemischen Risiken, fördern und unterstützen;

i) zur Einschätzung des Schulungsbedarfs des Personals der Mitgliedstaaten, das an der Umsetzung dieser Verordnung beteiligt ist, beitragen;

j) die Kommission zu internationalen Angelegenheiten im Bereich der künstlichen Intelligenz beraten.

KAPITEL 1A

LEITLINIEN DER KOMMISSION

Artikel 58a

Leitlinien der Kommission zur Umsetzung dieser Verordnung

(1) Die Kommission gibt auf Anfrage der Mitgliedstaaten oder des KI-Ausschusses oder in Eigeninitiative Leitlinien zur praktischen Umsetzung dieser Verordnung heraus, die sich insbesondere auf Folgendes beziehen:

i) die Anwendung der in den Artikeln 8 bis 15 genannten Anforderungen;

ii) die in Artikel 5 genannten verbotenen Praktiken;

iii) die praktische Umsetzung der Bestimmungen über wesentliche Änderungen;

iv) die praktische Umsetzung einheitlicher Bedingungen gemäß Artikel 6 Absatz 3, einschließlich Beispiele für die in Anhang III aufgeführten Hochrisiko-KI-Systeme;

v) die praktische Umsetzung der Transparenzpflichten gemäß Artikel 52;

vi) das Verhältnis dieser Verordnung zu anderen einschlägigen Rechtsvorschriften der Union, auch in Bezug auf deren einheitliche Durchsetzung.

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.

KAPITEL 2

ZUSTÄNDIGE NATIONALE BEHÖRDEN

Artikel 59

Benennung der zuständigen nationalen Behörden

(1) [gestrichen]

(2) Jeder Mitgliedstaat muss für die Zwecke dieser Verordnung mindestens eine notifizierende Behörde und mindestens eine Marktüberwachungsbehörde einrichten und als zuständige nationale Behörden benennen. Diese zuständigen nationalen Behörden gewährleisten durch ihre Organisation, dass bei ihren Tätigkeiten und Aufgaben Objektivität und Unparteilichkeit gewahrt sind. Sofern diese Grundsätze gewahrt werden, können die betreffenden Tätigkeiten und Aufgaben im Einklang mit den organisatorischen Erfordernissen des Mitgliedstaats von einer oder mehreren benannten Behörden wahrgenommen werden.

(3) Die Mitgliedstaaten teilen der Kommission ihre Benennung oder Benennungen mit.

(4) Die Mitgliedstaaten sorgen dafür, dass die zuständigen nationalen Behörden mit entsprechenden finanziellen Mitteln, technischer Ausrüstung und hochqualifiziertem Personal ausgestattet werden, damit sie ihre Aufgaben im Rahmen dieser Verordnung wirksam wahrnehmen können.

(5) Die Mitgliedstaaten unterrichten die Kommission bis zum *[ein Jahr nach Inkrafttreten dieser Verordnung]* und anschließend sechs Monate vor Ablauf der in Artikel 84 Absatz 2 genannten Frist über den Sachstand bezüglich der finanziellen Mittel, der technischen Ausrüstung und des Personals der zuständigen nationalen Behörden und geben in diesem Rahmen eine Einschätzung über deren Angemessenheit ab. Die Kommission leitet diese Informationen zur Erörterung und etwaigen Abgabe von Empfehlungen an den KI-Ausschuss weiter.

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

(7) Die zuständigen nationalen Behörden können zur Umsetzung dieser Verordnung Beratung anbieten, einschließlich Beratung, die auf Anbieter ausgerichtet ist, die KMU oder auch Start-up-Unternehmen sind. Wenn zuständige nationale Behörden beabsichtigen, Orientierung und Beratung in Bezug auf KI-Systeme in Bereichen anzubieten, die unter andere Rechtsvorschriften der Union fallen, so sind gegebenenfalls die nach jenen Unionsvorschriften dafür zuständigen nationalen Behörden zu konsultieren. Mitgliedstaaten können auch eine zentrale Kontaktstelle für die Kommunikation mit den Akteuren einrichten.

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

TITEL VII

EU-DATENBANK FÜR DIE IN ANHANG III AUFGEFÜHRTEN HOCHRISIKO-KI-SYSTEME

Artikel 60

EU-Datenbank für die in Anhang III aufgeführten Hochrisiko-KI-Systeme

(1) Die Kommission errichtet und führt in Zusammenarbeit mit den Mitgliedstaaten eine EU-Datenbank mit den in Absatz 2 genannten Informationen zu einschlägigen Akteuren und in Anhang III aufgeführten Hochrisiko-KI-Systemen, die nach den Artikeln 51 und 54a registriert werden. Bei der Festlegung der Funktionsspezifikationen der Datenbank konsultiert die Kommission den KI-Ausschuss.

(2) Die in Anhang VIII Teil I aufgeführten Daten werden bei ihrer Registrierung gegebenenfalls von den Anbietern, Bevollmächtigten und einschlägigen Nutzern in die EU-Datenbank eingegeben. Die in Anhang VIII Teil II Nummern 1 bis 11 aufgeführten Daten werden von den Anbietern oder gegebenenfalls von den Bevollmächtigten gemäß Artikel 51 in die EU-Datenbank eingegeben. Die in Anhang VIII Teil II Nummer 12 aufgeführten Daten werden auf der Grundlage der gemäß Artikel 51 Absatz 2 von einschlägigen Nutzern bereitgestellten Informationen automatisch durch die Datenbank generiert. Die in Anhang VIIIa aufgeführten Daten werden gemäß Artikel 54a von den zukünftigen Anbietern oder den Anbietern in die EU-Datenbank eingegeben.

(3) [gestrichen]

(4) Die EU-Datenbank enthält mit Ausnahme der in Anhang VIII aufgeführten Informationen keine personenbezogenen Daten und lässt Artikel 70 unberührt.

(5) Die Kommission gilt bezüglich der EU-Datenbank als die für die Verarbeitung verantwortliche Stelle. Sie stellt Anbietern, zukünftigen Anbietern und Nutzern angemessene technische und administrative Unterstützung bereit.

(5a) Die in der EU-Datenbank gemäß Artikel 51 registrierten Informationen sind öffentlich zugänglich. Auf die gemäß Artikel 54a registrierten Informationen können nur Marktüberwachungsbehörden und die Kommission zugreifen, es sei denn, der Anbieter oder der zukünftige Anbieter hat seine Zustimmung dafür erteilt, dass die Informationen auch öffentlich zugänglich sind.

TITEL VIII

BEOBACHTUNG NACH DEM INVERKEHRBRINGEN, INFORMATIONSAUSTAUSCH, MARKTÜBERWACHUNG

KAPITEL 1

BEOBACHTUNG NACH DEM INVERKEHRBRINGEN

Artikel 61

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

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

(2) Damit der Anbieter die Einhaltung der in Titel III Kapitel 2 genannten Anforderungen an KI-Systeme über deren gesamten Lebenszyklus hinweg bewerten kann, werden mit dem System zur Beobachtung nach dem Inverkehrbringen einschlägige Daten zur Leistung von Hochrisiko-KI-Systemen erfasst, dokumentiert und analysiert, die von Nutzern bereitgestellt oder aus anderen Quellen zusammengetragen werden können. Diese Pflicht gilt nicht für sensible operative Daten von Nutzern von KI-Systemen, die Strafverfolgungsbehörden sind.

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

(4) Bei Hochrisiko-KI-Systemen, die unter die in Anhang II Abschnitt A 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, gilt die gemäß diesen Rechtsakten erstellte Dokumentation nach dem Inverkehrbringen als ausreichend, sofern das in Absatz 3 genannte Muster verwendet wird.

Unterabsatz 1 gilt auch für Hochrisiko-KI-Systeme nach Anhang III Nummer 5, die von Finanzinstituten in Verkehr gebracht oder in Betrieb genommen wurden, die bezüglich der Regelungen oder Verfahren der internen Unternehmensführung Anforderungen gemäß den Rechtsvorschriften der Union über Finanzdienstleistungen unterliegen.

KAPITEL 2

AUSTAUSCH VON INFORMATIONEN ÜBER SCHWERWIEGENDE VORFÄLLE

Artikel 62

Meldung schwerwiegender Vorfälle

(1) Anbieter von in der Union in Verkehr gebrachten Hochrisiko-KI-Systemen melden schwerwiegende Vorfälle den Marktüberwachungsbehörden der Mitgliedstaaten, in denen der Vorfall stattgefunden hat.

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

(2) Sobald die Marktüberwachungsbehörde eine Meldung über einen schwerwiegenden Vorfall im Sinne von Artikel 3 Nummer 44 Buchstabe c erhält, unterrichtet sie die in Artikel 64 Absatz 3 genannten nationalen Behörden oder öffentlichen Stellen. Zur leichteren Einhaltung der Pflichten nach Absatz 1 arbeitet die Kommission entsprechende Leitlinien aus. Diese Leitlinien werden spätestens 12 Monate nach dem Inkrafttreten dieser Verordnung veröffentlicht.

(3) Bei Hochrisiko-KI-Systemen nach Anhang III Nummer 5, die von Anbietern in Verkehr gebracht oder in Betrieb genommen wurden, bei denen es sich um Finanzinstitute handelt, die bezüglich der Regelungen oder Verfahren der internen Unternehmensführung Anforderungen gemäß den Rechtsvorschriften der Union über Finanzdienstleistungen unterliegen, müssen nur die in Artikel 3 Nummer 44 Buchstabe c genannten schwerwiegenden Vorfälle gemeldet werden.

(4) Bei Hochrisiko-KI-Systemen, bei denen es sich um Sicherheitskomponenten von Produkten handelt, die unter die Verordnung (EU) 2017/745 und die Verordnung (EU) 2017/746 fallen, oder die selbst solche Produkte sind, müssen nur die in Artikel 3 Nummer 44 Buchstabe c genannten schwerwiegenden Vorfälle gemeldet werden, und zwar der zuständigen nationalen Behörde, die für diese Zwecke von den Mitgliedstaaten, in denen der Vorfall stattgefunden hat, ausgewählt wurde.

KAPITEL 3

DURCHSETZUNG

Artikel 63

Marktüberwachung und Kontrolle von KI-Systemen auf dem Unionsmarkt

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

a) Jede Bezugnahme auf einen Wirtschaftsakteur nach der Verordnung (EU) 2019/1020 gilt auch als Bezugnahme auf alle Akteure, die in Artikel 2 dieser Verordnung genannt werden.

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

(2) Die Marktüberwachungsbehörden erstatten der Kommission im Rahmen ihrer Meldepflichten gemäß Artikel 34 Absatz 4 der Verordnung (EU) 2019/1020 über die Ergebnisse ihrer jeweiligen Marktüberwachungstätigkeiten gemäß dieser Verordnung Bericht.

(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 oder – in begründeten Fällen und wenn für Abstimmung gesorgt ist – eine andere von dem Mitgliedstaat benannte einschlägige Behörde.

Die Verfahren gemäß den Artikeln 65, 66, 67 und 68 dieser Verordnung gelten nicht für KI-Systeme für Produkte, die unter die in Anhang II Abschnitt A aufgeführten Rechtsakte fallen, wenn in diesen Rechtsakten bereits Verfahren mit demselben Ziel vorgesehen sind. In diesem Fall kommen die sektorspezifischen Verfahren zur Anwendung.

(4) Bei Hochrisiko-KI-Systemen, die von auf der Grundlage des Finanzdienstleistungsrechts der Union regulierten Finanzinstituten in Verkehr gebracht, in Betrieb genommen oder verwendet werden, gilt die in jenen Rechtsvorschriften für die Finanzaufsicht über diese Institute benannte nationale Behörde als Marktüberwachungsbehörde für die Zwecke dieser Verordnung, sofern das Inverkehrbringen, die Inbetriebnahme oder die Verwendung des KI-Systems mit der Erbringung dieser Finanzdienstleistungen in direktem Zusammenhang steht.

Abweichend vom vorangehenden Unterabsatz kann der Mitgliedstaat – in begründeten Fällen und wenn für Abstimmung gesorgt ist – eine andere einschlägige Behörde als Marktüberwachungsbehörde für die Zwecke dieser Verordnung benennen.

Nationale Marktüberwachungsbehörden, die auf der Grundlage der Richtlinie 2013/36/EU regulierte Kreditinstitute, die an dem mit der Verordnung (EU) Nr. 1042/2013 des Rates eingerichteten einheitlichen Aufsichtsmechanismus teilnehmen, beaufsichtigen, sollten der Europäischen Zentralbank unverzüglich alle im Zuge ihrer Marktüberwachungstätigkeiten ermittelten Informationen übermitteln, die für die in der genannten Verordnung festgelegten Aufsichtsaufgaben der Europäischen Zentralbank von Belang sein könnten.

(5) Für die in Absatz 1 Buchstabe a genannten Hochrisiko-KI-Systeme, sofern diese Systeme für Strafverfolgungszwecke nach Anhang III Nummern 6, 7 und 8 verwendet werden, benennen die Mitgliedstaaten entweder die nationalen Behörden, die die Tätigkeiten der Strafverfolgungs-, Grenzschutz-, Einwanderungs-, Asyl- oder Justizbehörden beaufsichtigen, oder die für den Datenschutz nach der Richtlinie (EU) 2016/680 oder der Verordnung (EU) 2016/679 zuständigen Aufsichtsbehörden als Marktüberwachungsbehörden für die Zwecke dieser Verordnung. Marktüberwachungstätigkeiten dürfen in keiner Weise Auswirkungen auf die Unabhängigkeit von Justizbehörden haben oder deren Handlungen im Rahmen ihrer justiziellen Tätigkeit anderweitig beeinflussen.

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

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

(8) Der Anbieter gewährt den Marktüberwachungsbehörden unbeschadet der Befugnisübertragung gemäß der Verordnung (EU) 2019/1020, sofern dies relevant ist und beschränkt auf das zur Wahrnehmung der Aufgaben dieser Behörden erforderliche Maß, uneingeschränkten Zugang zur Dokumentation sowie zu den für die Entwicklung des Hochrisiko-KI-Systems verwendeten Trainings-, Validierungs- und Testdatensätzen, einschließlich, sofern dies relevant ist und im Rahmen der Sicherheitsmaßnahmen, über die Anwendungsprogrammierschnittstellen (API) oder andere einschlägige technische Mittel und Tools, die den Fernzugriff ermöglichen.

(9) Zum Quellcode des Hochrisiko-KI-Systems erhalten Marktüberwachungsbehörden auf begründete Anfrage und nur dann Zugang, wenn die folgenden kumulativen Bedingungen erfüllt sind:

a) Der Zugang zum Quellcode ist zur Bewertung der Konformität eines Hochrisiko-KI-Systems mit den in Titel III Kapitel 2 festgelegten Anforderungen notwendig, und

b) die Test-/Prüfverfahren und Überprüfungen aufgrund der vom Anbieter bereitgestellten Daten und Dokumentation wurden ausgeschöpft oder haben sich als unzureichend erwiesen.

(10) Jegliche Informationen und Dokumentation, in deren Besitz die Marktüberwachungsbehörden gelangt, werden im Einklang mit den in Artikel 70 festgelegten Vertraulichkeitspflichten behandelt.

(11) Natürliche oder juristische Personen, die Grund zu der Annahme haben, dass gegen die Bestimmungen dieser Verordnung verstoßen wurde, können bei der betreffenden Marktüberwachungsbehörde Beschwerde einlegen.

Gemäß Artikel 11 Absatz 3 Buchstabe e und Absatz 7 Buchstabe a der Verordnung (EU) 2019/1020 werden Beschwerden für die Zwecke der Durchführung von Marktüberwachungstätigkeiten berücksichtigt und nach den einschlägigen, von den Marktüberwachungsbehörden dafür eingerichteten Verfahren behandelt.

Artikel 63a

Beaufsichtigung von Tests unter realen Bedingungen durch Marktüberwachungsbehörden

(1) Marktüberwachungsbehörden verfügen über die Kompetenzen und Befugnisse, um sicherzustellen, dass Tests unter realen Bedingungen im Einklang mit dieser Verordnung erfolgen.

(2) Wenn Tests unter realen Bedingungen für KI-Systeme durchgeführt werden, die in einem KI-Reallabor gemäß Artikel 54 beaufsichtigt werden, überprüfen die Marktüberwachungsbehörden im Rahmen ihrer Aufsichtsaufgaben für das KI-Reallabor die Einhaltung der Bestimmungen von Artikel 54a. Die Behörden können gegebenenfalls gestatten, dass der Anbieter oder der zukünftige Anbieter den Test unter realen Bedingungen in Abweichung von den in Artikel 54a Absatz 4 Buchstaben f und g festgelegten Bedingungen durchführt.

(3) Wenn eine Marktüberwachungsbehörde vom zukünftigen Anbieter, vom Anbieter oder von einem Dritten über einen schwerwiegenden Vorfall informiert wurde oder Grund zu der Annahme hat, dass die in den Artikeln 54a und 54b festgelegten Bedingungen nicht erfüllt sind, kann sie in ihrem Hoheitsgebiet gegebenenfalls entscheiden,

a) den Test unter realen Bedingungen auszusetzen oder abzubrechen, oder

b) den Anbieter oder zukünftigen Anbieter und den/die Nutzer zur Änderung eines jeglichen Aspekts des Tests unter realen Bedingungen zu verpflichten.

(4) Wenn eine Marktüberwachungsbehörde eine Entscheidung im Sinne des Absatzes 3 getroffen oder Einwände im Sinne des Artikels 54a Absatz 4 Buchstabe b erhoben hat, sind im Rahmen der Entscheidung oder der Einwände die Gründe dafür sowie die Modalitäten und Bedingungen anzugeben, nach denen der Anbieter oder der zukünftige Anbieter die Entscheidung oder die Einwände anfechten kann.

(5) Wenn eine Marktüberwachungsbehörde eine Entscheidung im Sinne des Absatzes 3 getroffen hat, teilt sie ihre Gründe dafür gegebenenfalls der Marktüberwachungsbehörde des anderen Mitgliedstaats mit, in dem das KI-System im Einklang mit dem Plan für den Test getestet wurde.

Artikel 64

Befugnisse der für den Schutz der Grundrechte zuständigen Behörden

(1) [gestrichen]

(2) [gestrichen]

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

(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 veröffentlichen. Die Mitgliedstaaten übermitteln die Liste der Kommission und allen anderen Mitgliedstaaten und sorgen dafür, dass die Liste stets aktuell bleibt.

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

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

Artikel 65

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

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

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

Stellt die Marktüberwachungsbehörde im Verlauf dieser Prüfung fest, dass das KI-System die in dieser Verordnung festgelegten Anforderungen und Pflichten nicht erfüllt, so 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 Frist, die sie bestimmen kann, zurückzurufen.

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

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

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

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

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

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

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

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

c) Nichterfüllung der Bestimmungen von Artikel 52;

d) Nichtkonformität von KI-Systemen mit allgemeinem Verwendungszweck mit den in Artikel 4a festgelegten Anforderungen und Pflichten.

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

(8) Erhebt weder ein Mitgliedstaat noch die Kommission innerhalb von drei Monaten nach Eingang der in Absatz 5 genannten Notifizierung Einwände gegen die von einem Mitgliedstaat erlassene vorläufige Maßnahme, so gilt diese Maßnahme als gerechtfertigt. Die Verfahrensrechte des betreffenden Akteurs nach Artikel 18 der Verordnung (EU) 2019/1020 bleiben hiervon unberührt. Die im ersten Satz dieses Absatzes genannte Frist wird bei Missachtung des Verbots der in Artikel 5 genannten KI-Praktiken auf 30 Tage gekürzt.

(9) In diesem Fall tragen die Marktüberwachungsbehörden aller Mitgliedstaaten dafür Sorge, dass geeignete einschränkende Maßnahmen in Bezug auf das betreffende KI-System ergriffen werden, indem sie beispielsweise das Produkt unverzüglich von ihrem Markt nehmen.

Artikel 66

Schutzklauselverfahren der Union

(1) Erhebt ein Mitgliedstaat innerhalb von drei Monaten nach Eingang der in Artikel 65 Absatz 5 genannten Notifizierung oder – bei Missachtung des Verbots der in Artikel 5 genannten KI-Praktiken – binnen 30 Tagen Einwände gegen eine von einem anderen Mitgliedstaat getroffene Maßnahme oder ist die Kommission der Ansicht, dass die Maßnahme mit dem Unionsrecht unvereinbar ist, so nimmt die Kommission unverzüglich Konsultationen mit der Marktüberwachungsbehörde des betreffenden Mitgliedstaats und des Akteurs bzw. der Akteure auf und prüft die nationale Maßnahme. Anhand der Ergebnisse dieser Prüfung entscheidet die Kommission innerhalb von neun Monaten oder – bei Missachtung des Verbots der in Artikel 5 genannten KI-Praktiken – binnen 60 Tagen nach Eingang der in Artikel 65 Absatz 5 genannten Notifizierung, ob die nationale Maßnahme gerechtfertigt ist. Ihre Entscheidung teilt sie dem betreffenden Mitgliedstaat mit. Die Kommission unterrichtet auch alle anderen Mitgliedstaaten über diese Entscheidung.

(2) Wenn die Kommission die Maßnahme der Marktüberwachungsbehörde des betreffenden Mitgliedstaats als gerechtfertigt erachtet, tragen die Marktüberwachungsbehörden aller Mitgliedstaaten 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, und setzen die Kommission davon entsprechend in Kenntnis. Wenn die Kommission die nationale Maßnahme als nicht gerechtfertigt erachtet, nimmt die Marktüberwachungsbehörde des betreffenden Mitgliedstaats die Maßnahme zurück und setzt die Kommission davon entsprechend in Kenntnis.

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

Artikel 67

Konforme Hochrisiko-KI-Systeme oder KI-Systeme mit allgemeinem Verwendungszweck, die ein Risiko bergen

(1) Stellt die Marktüberwachungsbehörde eines Mitgliedstaats nach der gemäß Artikel 65 durchgeführten Prüfung fest, dass ein Hochrisiko-KI-System oder KI-System mit allgemeinem Verwendungszweck zwar dieser Verordnung entspricht, aber ein Risiko für die Gesundheit oder Sicherheit von Personen oder die Grundrechte darstellt, so fordert sie den betreffenden Akteur auf, alle geeigneten Maßnahmen zu treffen, damit das betreffende KI-System zum Zeitpunkt des Inverkehrbringens oder der Inbetriebnahme dieses Risiko nicht mehr birgt, oder das KI-System vom Markt zu nehmen oder es innerhalb einer Frist, die sie bestimmen kann, unverzüglich zurückzurufen.

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

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

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

(5) Die Kommission richtet ihren Beschluss an die betreffenden Mitgliedstaaten und setzt alle anderen Mitgliedstaaten davon in Kenntnis.

Artikel 68

Formale Nichtkonformität

(1) Wenn die Marktüberwachungsbehörde eines Mitgliedstaats eine der folgenden Nichtkonformitäten feststellt, fordert sie den jeweiligen Anbieter auf, diese binnen einer Frist, die sie bestimmen kann, zu beheben:

a) die Konformitätskennzeichnung wurde nicht nach Artikel 49 angebracht;

b) die Konformitätskennzeichnung wurde nicht angebracht;

c) die EU-Konformitätserklärung wurde nicht ausgestellt;

d) die EU-Konformitätserklärung wurde nicht ordnungsgemäß ausgestellt;

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

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

Artikel 68a

Unionsprüfeinrichtungen im Bereich künstliche Intelligenz

(1) Die Kommission benennt eine oder mehrere Unionsprüfeinrichtungen im Sinne des Artikels 21 der Verordnung (EU) 1020/2019 im Bereich künstliche Intelligenz.

(2) Unbeschadet der in Artikel 21 Absatz 6 der Verordnung (EU) 1020/2019 genannten Aufgaben von Unionsprüfeinrichtungen leisten die in Absatz 1 genannten Unionsprüfeinrichtungen auf Anfrage des KI-Ausschusses oder der Marktüberwachungsbehörden auch unabhängige technische oder wissenschaftliche Beratung.

Artikel 68b

Der zentrale Pool unabhängiger Sachverständiger

(1) Die Kommission sorgt auf Anfrage des KI-Ausschusses im Wege eines Durchführungsrechtsakts für die Einrichtung, Führung und Finanzierung eines zentralen Pools unabhängiger Sachverständiger, um die Durchsetzungstätigkeiten im Rahmen dieser Verordnung zu unterstützen.

(2) Die Sachverständigen werden von der Kommission ausgewählt und auf der Grundlage aktueller wissenschaftlicher oder technischer Fachkenntnisse auf dem Gebiet der künstlichen Intelligenz in den zentralen Pool aufgenommen, wobei den Fachgebieten, auf die sich die Anforderungen und Pflichten in dieser Verordnung und die Tätigkeiten der Marktüberwachungsbehörden gemäß Artikel 11 der Verordnung (EU) 1020/2019 erstrecken, entsprechend Rechnung getragen wird. Die Anzahl der Sachverständigen in dem Pool wird von der Kommission nach Maßgabe der jeweiligen Erfordernisse festgelegt.

(3) Die Sachverständigen können folgende Aufgaben haben:

a) Beratung und Unterstützung der Marktüberwachungsbehörden auf deren Anfrage bei ihrer Arbeit;

b) Unterstützung grenzüberschreitender Marktüberwachungsermittlungen gemäß Artikel 58 Buchstabe h, ohne dass die Befugnisse der Marktüberwachungsbehörden berührt werden;

c) Beratung und Unterstützung der Kommission bei der Wahrnehmung ihrer Aufgaben im Rahmen des Schutzklauselverfahrens gemäß Artikel 66.

(4) Die Sachverständigen führen ihre Aufgaben nach den Grundsätzen der Unparteilichkeit und der Objektivität aus und gewährleisten die Vertraulichkeit der Informationen und Daten, in deren Besitz sie bei der Ausführung ihrer Aufgaben und Tätigkeiten gelangen. Jeder Sachverständige gibt eine Interessenerklärung ab, die öffentlich zugänglich gemacht wird. Die Kommission richtet Systeme und Verfahren ein, mit denen mögliche Interessenkonflikte aktiv bewältigt und verhindert werden können.

(5) Die Mitgliedstaaten können verpflichtet werden, für die Beratung und Unterstützung der Sachverständigen Gebühren zu entrichten. Struktur und Höhe der Gebühren sowie Umfang und Struktur erstattungsfähiger Kosten werden von der Kommission durch Erlass der in Absatz 1 genannten Durchführungsrechtsakte festgelegt, wobei die Zielsetzung berücksichtigt wird, für die angemessene Umsetzung dieser Verordnung, für Kosteneffizienz sowie dafür zu sorgen, dass alle Mitgliedstaaten effektiven Zugang zu Sachverständigen haben müssen.

(6) Die Kommission ermöglicht Mitgliedstaaten bei Bedarf einen rechtzeitigen Zugang zu Sachverständigen und sorgt dafür, dass die Kombination aus unterstützenden Tätigkeiten der Unionsprüfeinrichtungen gemäß Artikel 68a und der Sachverständigen gemäß diesem Artikel effizient organisiert ist und den bestmöglichen zusätzlichen Nutzen bringt.

TITEL IX

VERHALTENSKODIZES

Artikel 69

Verhaltenskodizes für die freiwillige Anwendung bestimmter Anforderungen

(1) Die Kommission und die Mitgliedstaaten erleichtern die Aufstellung von Verhaltenskodizes, mit denen bewirkt werden soll, dass die in Titel III Kapitel 2 dieser Verordnung genannten Anforderungen bei KI-Systemen, die keine Hochrisiko-KI-Systeme sind, bestmöglich, unter Berücksichtigung der zur Anwendung dieser Anforderungen verfügbaren, technischen Lösungen, freiwillig angewendet werden.

(2) Die Kommission und die Mitgliedstaaten erleichtern die Aufstellung von Verhaltenskodizes, mit denen bewirkt werden soll, dass bestimmte Anforderungen, die sich beispielsweise auf die ökologische Nachhaltigkeit, einschließlich energieeffizientes Programmieren, die barrierefreie Zugänglichkeit für Personen mit Behinderungen, die Beteiligung von Interessenträgern an der Konzeption und Entwicklung der KI-Systeme und die Vielfalt der Entwicklungsteams beziehen, bei allen KI-Systemen auf der Grundlage klarer Vorgaben sowie wesentlicher Leistungsindikatoren zur Messung der Erfüllung dieser Vorgaben freiwillig angewendet werden. Außerdem erleichtern die Kommission und die Mitgliedstaaten gegebenenfalls die Aufstellung von Verhaltenskodizes zu den Pflichten der Nutzer in Bezug auf KI-Systeme, deren Anwendung freiwillig ist.

(3) Einzelne Anbieter von KI-Systemen oder Interessenvertretungen dieser Anbieter oder beide können, auch unter Einbeziehung von Nutzern und Interessenträgern sowie deren Interessenvertretungen, freiwillige Verhaltenskodizes aufstellen, oder Nutzer können gegebenenfalls freiwillige Verhaltenskodizes zu den eigenen Pflichten aufstellen. Verhaltenskodizes können sich auf einen oder mehrere KI-Systeme erstrecken, um ähnlichen Zweckbestimmungen der jeweiligen Systeme Rechnung zu tragen.

(4) Die Kommission und die Mitgliedstaaten berücksichtigen bei der Förderung und Erleichterung der Aufstellung der in diesem Artikel genannten Verhaltenskodizes die besonderen Interessen und Bedürfnisse von Anbietern, die KMU oder auch Start-up-Unternehmen sind.

TITEL X

VERTRAULICHKEIT UND SANKTIONEN

Artikel 70

Vertraulichkeit

(1) Die zuständigen nationalen Behörden, die notifizierten Stellen, die Kommission, der KI-Ausschuss und alle anderen natürlichen oder juristischen Personen, die an der Anwendung dieser Verordnung beteiligt sind, ergreifen im Einklang mit dem Unionsrecht oder dem nationalen Recht geeignete technische und organisatorische Maßnahmen, um die Vertraulichkeit der Informationen und Daten, in deren Besitz sie bei der Ausführung ihrer Aufgaben und Tätigkeiten gelangen, sicherzustellen, sodass insbesondere Folgendes geschützt ist:

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

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

c) öffentliche und nationale Sicherheitsinteressen;

d) die Integrität von Straf- oder Verwaltungsverfahren.

e) die Integrität von gemäß dem Unionsrecht oder dem nationalen Recht als Verschlusssachen eingestuften Informationen.

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

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

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

Artikel 71

Sanktionen

(1) Entsprechend den Vorgaben dieser Verordnung erlassen die Mitgliedstaaten Vorschriften für Sanktionen, beispielsweise in Form von Geldbußen, die bei Verstößen gegen diese Verordnung Anwendung finden, und ergreifen alle Maßnahmen, die für deren ordnungsgemäße und wirksame Durchsetzung notwendig sind. Die vorgesehenen Sanktionen müssen wirksam, verhältnismäßig und abschreckend sein. Sie berücksichtigen insbesondere die Größe und die Interessen von Anbietern, die KMU oder auch Start-up-Unternehmen sind, sowie deren wirtschaftliches Überleben. Darüber hinaus berücksichtigen sie, ob das KI-System im Rahmen einer persönlichen und nicht beruflichen Tätigkeit verwendet wird.

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

(3) Bei Missachtung des Verbots der in Artikel 5 genannten KI-Praktiken werden Geldbußen von bis zu 30 000 000 EUR oder – im Falle von Unternehmen – von bis zu 6 % des gesamten weltweiten Jahresumsatzes des vorangegangenen Geschäftsjahres verhängt, je nachdem, welcher Betrag höher ist. Handelt es sich um KMU, einschließlich Start-up-Unternehmen, so belaufen sich die Geldbußen auf bis zu 3 % ihres gesamten weltweiten Jahresumsatzes des vorangegangenen Geschäftsjahres.

(4) Bei Verstößen gegen die folgenden für Akteure oder notizifierte Stellen geltenden Bestimmungen 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:

-a) Pflichten der Anbieter gemäß den Artikeln 4b und 4c;

a) Pflichten der Anbieter gemäß Artikel 16;

b) Anforderungen an andere Personen gemäß Artikel 23a;

c) Pflichten Bevollmächtigter gemäß Artikel 25;

d) Pflichten der Einführer gemäß Artikel 26;

e) Pflichten der Händler gemäß Artikel 27;

f) Pflichten der Nutzer gemäß Artikel 29 Absätze 1 bis 6a;

g) für notifizierte Stellen geltende Anforderungen und Pflichten gemäß Artikel 33, Artikel 34 Absätze 1, 3 und 4 und Artikel 34a;

h) Transparenzpflichten für Anbieter und Nutzer gemäß Artikel 52.

Handelt es sich um KMU, einschließlich Start-up-Unternehmen, so belaufen sich die Geldbußen auf bis zu 2 % ihres gesamten weltweiten Jahresumsatzes des vorangegangenen Geschäftsjahres.

(5) Werden gegenüber notifizierten Stellen und zuständigen nationalen Behörden auf deren Auskunftsersuchen hin falsche, unvollständige oder irreführende Angaben gemacht, werden Geldbußen von bis zu 10 000 000 EUR oder – im Falle von Unternehmen – von bis zu 2 % des gesamten weltweiten Jahresumsatzes des vorangegangenen Geschäftsjahres verhängt, je nachdem, welcher Betrag höher ist. Handelt es sich um KMU, einschließlich Start-up-Unternehmen, so belaufen sich die Geldbußen auf bis zu 1 % ihres gesamten weltweiten Jahresumsatzes des vorangegangenen Geschäftsjahres.

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

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

aa) Vorsätzlichkeit oder Fahrlässigkeit des Verstoßes;

ab) Maßnahmen, die der Akteur ergriffen hat, um dem Verstoß abzuhelfen und seine möglichen nachteiligen Auswirkungen zu mindern;

b) ob demselben Akteur bereits von Marktüberwachungsbehörden in anderen Mitgliedstaaten für denselben Verstoß Geldbußen auferlegt wurden;

ba) ob demselben Akteur bereits von anderen Behörden für Verstöße gegen das Unionsrecht oder das nationale Recht Geldbußen auferlegt wurden, wenn diese Verstöße auf dieselbe Handlung oder Unterlassung zurückzuführen sind, die einen einschlägigen Verstoß gegen diesen Rechtsakt darstellt;

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

d) jegliche anderen erschwerenden oder mildernden Umstände im jeweiligen Fall, wie unmittelbar oder mittelbar durch den Verstoß erlangte finanzielle Vorteile oder vermiedene Verluste.

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

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

(9) Die Ausübung der eigenen Befugnisse durch eine Marktüberwachungsbehörde gemäß diesem Artikel muss angemessenen Verfahrensgarantien gemäß dem Unionsrecht und dem Recht der Mitgliedstaaten, einschließlich wirksamer gerichtlicher Rechtsbehelfe und ordnungsgemäßer Verfahren, unterliegen.

Artikel 72

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

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

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

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

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

(2) Bei Missachtung des Verbots der in Artikel 5 genannten KI-Praktiken werden Geldbußen von bis zu 500 000 EUR verhängt.

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

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

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

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

TITEL XI

BEFUGNISÜBERTRAGUNG UND AUSSCHUSSVERFAHREN

Artikel 73

Ausübung der Befugnisübertragung

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

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

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

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

Artikel 74

Ausschussverfahren

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

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

TITEL XII

SCHLUSSBESTIMMUNGEN

Artikel 75

Änderung der Verordnung (EU) Nr. 300/2008

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

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

_____

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

Artikel 76

Änderung der Verordnung (EU) Nr. 167/2013

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

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

_____

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

Artikel 77

Änderung der Verordnung (EU) Nr. 168/2013

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

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

_____

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

Artikel 78

Änderung der Richtlinie 2014/90/EU

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

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

_____

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

Artikel 79

Änderung der Richtlinie (EU) 2016/797

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

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

_____

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

Artikel 80

Änderung der Verordnung (EU) Nr. 2018/858

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

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

_____

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

Artikel 81

Änderung der Verordnung (EU) Nr. 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 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, die in Titel III Kapitel 2 jener Verordnung festgelegten Anforderungen berücksichtigt.

_____

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

2. In Artikel 19 wird folgender Absatz angefügt:

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

3. In Artikel 43 wird folgender Absatz angefügt:

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

4. In Artikel 47 wird folgender Absatz angefügt:

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

5. In Artikel 57 wird folgender Absatz angefügt:

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

6. In Artikel 58 wird folgender Absatz angefügt:

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

Artikel 82

Änderung der Verordnung (EU) 2019/2144

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

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

_____

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

Artikel 83

Bereits in Verkehr gebrachte oder in Betrieb genommene KI-Systeme

(1) Diese Verordnung gilt nicht für KI-Systeme, bei denen es sich um Komponenten von IT-Großsystemen handelt, die mit den in Anhang IX genannten Rechtsakten festgelegt wurden und vor dem [*Datum 12 Monate nach dem Datum der Anwendung dieser Verordnung nach Artikel 85 Absatz 2*] in Verkehr gebracht oder in Betrieb genommen wurden, sofern der Ersatz oder die Änderung jener Rechtsakte nicht zu einer erheblichen Veränderung der Konzeption oder Zweckbestimmung des betreffenden KI-Systems führt.

Die in dieser Verordnung festgelegten Anforderungen werden gegebenenfalls bei der Bewertung jedes IT-Großsystems, das auf der Grundlage der in Anhang IX aufgeführten Rechtsakte eingerichtet wurde, berücksichtigt, wobei die Bewertung entsprechend den Vorgaben der jeweiligen Rechtsakte erfolgt.

(2) Diese Verordnung gilt – mit Ausnahme der in Absatz 1 genannten Systeme – für Hochrisiko-KI-Systeme, die vor dem [*Datum der Anwendung dieser Verordnung nach Artikel 85 Absatz 2*] in Verkehr gebracht oder in Betrieb genommen wurden, nur dann, wenn diese Systeme danach in ihrer Konzeption oder Zweckbestimmung erheblich verändert wurden.

Artikel 84

Bewertung und Überarbeitung

(1) [gestrichen]

(1b) Die Kommission prüft nach Inkrafttreten dieser Verordnung und bis zum Ende der Befugnisübertragung alle 24 Monate, ob eine Änderung der Liste in Anhang III erforderlich ist. Die Ergebnisse dieser Prüfung werden dem Europäischen Parlament und dem Rat vorgelegt.

(2) Bis zum [*Datum drei Jahre nach dem Datum der Anwendung dieser Verordnung nach Artikel 85 Absatz 2*] und danach alle vier Jahre legt die Kommission dem Europäischen Parlament und dem Rat einen Bericht über die Bewertung und Überprüfung dieser Verordnung vor. Die Berichte werden veröffentlicht.

(3) In den in Absatz 2 genannten Berichten wird insbesondere auf folgende Aspekte eingegangen:

a) Sachstand bezüglich der finanziellen Mittel, der technischen Ausrüstung und des Personals der zuständigen nationalen Behörden im Hinblick auf deren Fähigkeit, die ihnen auf der Grundlage dieser Verordnung übertragenen Aufgaben wirksam zu erfüllen;

b) Stand der Sanktionen, insbesondere der Bußgelder nach Artikel 71 Absatz 1, die Mitgliedstaaten bei Verstößen gegen diese Verordnung verhängt haben.

(4) Innerhalb von [*drei Jahren nach dem Datum der Anwendung dieser Verordnung nach Artikel 85 Absatz 2*] und danach alle vier Jahre führt die Kommission gegebenenfalls eine Bewertung der Folgen und der Wirksamkeit der freiwilligen Verhaltenskodizes durch, mit denen die Anwendung der gemäß Titel III Kapitel 2 geltenden Anforderungen an andere KI-Systeme als Hochrisiko-KI-Systeme und möglicherweise auch zusätzlicher Anforderungen an KI-Systeme, auch in Bezug auf deren ökologische Nachhaltigkeit, gefördert werden soll.

(5) Für die Zwecke der Absätze 1a bis 4 übermitteln der KI-Ausschuss, die Mitgliedstaaten und die zuständigen nationalen Behörden der Kommission auf Anfrage die gewünschten Informationen.

(6) Bei den in den Absätzen 1a und 4 genannten Bewertungen und Überprüfungen berücksichtigt die Kommission die Standpunkte und Feststellungen des KI-Ausschusses, des Europäischen Parlaments, des Rates und anderer einschlägiger Stellen oder Quellen.

(7) Die Kommission legt erforderlichenfalls geeignete Vorschläge zur Änderung dieser Verordnung vor und berücksichtigt dabei insbesondere die technischen Entwicklungen und die Fortschritte in der Informationsgesellschaft.

Artikel 85

Inkrafttreten und Geltungsbeginn

(1) Diese Verordnung tritt am zwanzigsten Tag nach ihrer Veröffentlichung im *Amtsblatt der Europäischen Union* in Kraft.

(2) Diese Verordnung gilt ab dem [36 Monate nach Inkrafttreten der Verordnung].

(3) Abweichend von Absatz 2 gilt Folgendes:

a) Titel III Kapitel 4 und Titel VI gelten ab dem [12 Monate nach Inkrafttreten der Verordnung];

b) Artikel 71 gilt ab dem [12 Monate nach Inkrafttreten der Verordnung].

Diese Verordnung ist in allen ihren Teilen verbindlich und gilt unmittelbar in jedem Mitgliedstaat.

Geschehen zu Brüssel am […]

Im Namen des Europäischen Parlaments	*Im Namen des Rates*
Der Präsident / Die Präsidentin	*Der Präsident / Die Präsidentin*

ANHANG I

[gestrichen]

ANHANG II

LISTE DER HARMONISIERUNGSRECHTSVORSCHRIFTEN 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)

7. 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)

8. 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 3

Als Hochrisiko-KI-Systeme gemäß Artikel 6 Absatz 3 gelten die KI-Systeme, die in den Buchstaben unter den Bereichen der Nummern 1 bis 8 ausdrücklich genannt werden:

1. Biometrik

   a) Biometrische Fernidentifizierungssysteme

2. Kritische Infrastruktur

   a) KI-Systeme, die im Rahmen der Verwaltung und des Betriebs kritischer digitaler Infrastruktur, des Straßenverkehrs sowie der Wasser-, Gas-, Wärme- und Stromversorgung bestimmungsgemäß als Sicherheitskomponenten verwendet werden sollen

3. Allgemeine und berufliche Bildung

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

   b) KI-Systeme, die bestimmungsgemäß für die Bewertung von Lernergebnissen verwendet werden sollen, auch wenn diese Ergebnisse dazu dienen, den Lernprozess natürlicher Personen in Einrichtungen und Programmen aller Ebenen der allgemeinen und beruflichen Bildung zu steuern

4. Beschäftigung, Personalmanagement und Zugang zur Selbstständigkeit

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

b) KI-Systeme, die bestimmungsgemäß verwendet werden sollen, um über Beförderungen und Kündigungen von Arbeitsvertragsverhältnissen zu entscheiden, aufgrund des individuellen Verhaltens oder persönlicher Merkmale oder Eigenschaften Aufgaben zuzuweisen sowie die Leistung und das Verhalten von Personen in entsprechenden Beschäftigungsverhältnissen zu beobachten und zu bewerten

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 grundlegende öffentliche Unterstützungsleistungen und -dienste haben und ob solche Leistungen und Dienste zu gewähren, einzuschränken, zu widerrufen oder zurückzufordern sind

b) KI-Systeme, die bestimmungsgemäß für die Kreditwürdigkeitsprüfung oder Kreditpunktebewertung natürlicher Personen verwendet werden sollen, mit Ausnahme von KI-Systemen, die von Anbietern, die Kleinstunternehmen oder kleine Unternehmen im Sinne der Begriffsbestimmung im Anhang der Empfehlung 2003/361/EG der Kommission sind, für den Eigengebrauch in Betrieb genommen werden

c) KI-Systeme, die bestimmungsgemäß für die Entsendung oder Priorisierung des Einsatzes von Not- und Rettungsdiensten, einschließlich Feuerwehr und medizinischer Nothilfe, verwendet werden sollen

d) KI-Systeme, die bestimmungsgemäß bei Lebens- und Krankenversicherungen für die Risikobewertung in Bezug auf natürliche Personen und die Preisbildung verwendet werden sollen, mit Ausnahme von KI-Systemen, die von Anbietern, die Kleinstunternehmen oder kleine Unternehmen im Sinne der Begriffsbestimmung im Anhang der Empfehlung 2003/361/EG der Kommission sind, für den Eigengebrauch in Betrieb genommen werden

6. Strafverfolgung

a) KI-Systeme, die bestimmungsgemäß von Strafverfolgungsbehörden oder in deren Namen verwendet werden sollen, um das Risiko abzuschätzen, dass eine natürliche Person eine Straftat begeht oder erneut begeht oder dass eine Person zum Opfer möglicher Straftaten wird

b) KI-Systeme, die bestimmungsgemäß von Strafverfolgungsbehörden oder in deren Namen als Lügendetektoren und vergleichbare Instrumente oder zur Ermittlung des emotionalen Zustands einer natürlichen Person verwendet werden sollen

c) [gestrichen]

d) KI-Systeme, die bestimmungsgemäß von Strafverfolgungsbehörden oder in deren Namen zur Bewertung der Verlässlichkeit von Beweismitteln im Zuge der Ermittlung oder Verfolgung von Straftaten verwendet werden sollen

e) KI-Systeme, die bestimmungsgemäß von Strafverfolgungsbehörden oder in deren Namen zur Vorhersage des Auftretens oder erneuten Auftretens einer tatsächlichen oder potenziellen Straftat auf der Grundlage des Profils natürlicher Personen gemäß Artikel 3 Absatz 4 der Richtlinie (EU) 2016/680 oder zur Bewertung von Persönlichkeitsmerkmalen und Eigenschaften oder vergangenen kriminellen Verhaltens natürlicher Personen oder von Gruppen verwendet werden sollen

f) KI-Systeme, die bestimmungsgemäß von Strafverfolgungsbehörden oder in deren Namen zur Erstellung von Profilen natürlicher Personen gemäß Artikel 3 Absatz 4 der Richtlinie (EU) 2016/680 im Zuge der Aufdeckung, Ermittlung oder Verfolgung von Straftaten verwendet werden sollen

g) [gestrichen]

7. Migration, Asyl und Grenzkontrolle

a) KI-Systeme, die bestimmungsgemäß von zuständigen Behörden oder in deren Namen als Lügendetektoren und vergleichbare Instrumente oder zur Ermittlung des emotionalen Zustands einer natürlichen Person verwendet werden sollen

b) KI-Systeme, die bestimmungsgemäß von zuständigen Behörden oder in deren Namen 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) [gestrichen]

d) KI-Systeme, die bestimmungsgemäß von zuständigen Behörden oder in deren Namen zur Prüfung von Asyl- und Visumanträgen sowie Aufenthaltstiteln und damit verbundenen Beschwerden im Hinblick auf die Feststellung der Berechtigung der den Antrag stellenden natürlichen Personen verwendet werden sollen

8. Rechtspflege und demokratische Prozesse

a) KI-Systeme, die bestimmungsgemäß von Justizbehörden oder in deren Namen zur Ermittlung und Auslegung von Sachverhalten und Rechtsvorschriften und zur Anwendung des Rechts auf konkrete Sachverhalte verwendet werden sollen

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, das System entwickelnde Person(en), Datum und Version des Systems

   b) gegebenenfalls Interaktion oder Verwendung des KI-Systems mit Hardware oder Software, die nicht Teil des KI-Systems selbst sind

   c) Versionen der betreffenden Software oder Firmware und etwaige Anforderungen in Bezug auf die Aktualisierung der Versionen

   d) Beschreibung aller Formen, in denen das KI-System in Verkehr gebracht oder in Betrieb genommen wird (z. B. in Hardware eingebettetes Softwarepaket, herunterladbar, API)

   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

   g) Gebrauchsanweisungen für die Nutzer und gegebenenfalls Aufbau- oder Installationsanweisungen

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) Entwurfsspezifikationen des Systems, insbesondere die allgemeine Logik des KI-Systems und der Algorithmen; 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; Beschreibung des erwarteten Ergebnisses des Systems; Entscheidungen über mögliche Kompromisse in Bezug auf die technischen Lösungen, mit denen die Anforderungen in Titel III Kapitel 2 erfüllt werden sollen

c) Beschreibung der Systemarchitektur, aus der hervorgeht, wie Softwarekomponenten aufeinander aufbauen oder einander zuarbeiten und in die Gesamtverarbeitung integriert sind; zum Entwickeln, Trainieren, Testen und Validieren des KI-Systems verwendete Rechenressourcen

d) gegebenenfalls Datenanforderungen in Form von Datenblättern, in denen die Trainingsmethoden und -techniken und die verwendeten Trainingsdatensätze beschrieben werden, einschließlich einer allgemeinen Beschreibung dieser Datensätze sowie Angaben zu deren Herkunft, Umfang und Hauptmerkmalen; 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 Nutzern 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, Cybersicherheit 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

3. Detaillierte Informationen über die Überwachung, Funktionsweise und Kontrolle des KI-Systems, insbesondere in Bezug auf: die Fähigkeiten und Leistungsgrenzen des Systems, einschließlich seines Genauigkeitsgrads bei bestimmten Personen oder Personengruppen, auf die es bestimmungsgemäß angewandt werden soll, sowie des in Bezug auf seine Zweckbestimmung insgesamt erwarteten Genauigkeitsgrads; angesichts der Zweckbestimmung des KI-Systems vorhersehbare unbeabsichtigte Ergebnisse und Risikoquellen für die Gesundheit und Sicherheit, die Grundrechte und eine etwaige Diskriminierung; die nach Artikel 14 erforderlichen Maßnahmen der menschlichen Aufsicht, einschließlich der technischen Maßnahmen, die getroffen wurden, um den Nutzern die Interpretation der Ergebnisse von KI-Systemen zu erleichtern; gegebenenfalls Spezifikationen zu Eingabedaten

4. Detaillierte Beschreibung des Risikomanagementsystems gemäß Artikel 9

5. Beschreibung einschlägiger Änderungen, die der Anbieter während des Lebenszyklus an dem System vorgenommen hat

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 und technischer 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

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, Name und Funktion des Unterzeichners sowie Angabe, für wen und in wessen Namen diese Person unterzeichnet hat, Unterschrift

ANHANG VI

KONFORMITÄTSBEWERTUNGSVERFAHREN 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, sofern dies relevant ist und beschränkt auf das zur Wahrnehmung der Aufgaben dieser Behörden erforderliche Maß, uneingeschränkten Zugang zu den verwendeten Trainings-, Validierungs- und Testdatensätzen, einschließlich, sofern dies relevant ist und im Rahmen der Sicherheitsmaßnahmen, über die Anwendungsprogrammierschnittstellen (API) oder andere einschlägige technische Mittel und Tools, die den Fernzugriff ermöglichen.

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. Zum Quellcode des KI-Systems erhalten notifizierte Stellen auf begründete Anfrage und nur dann Zugang, wenn die folgenden kumulativen Bedingungen erfüllt sind:

a) Der Zugang zum Quellcode ist zur Bewertung der Konformität des Hochrisiko-KI-Systems mit den in Titel III Kapitel 2 festgelegten Anforderungen notwendig, und

b) die Test-/Prüfverfahren und Überprüfungen aufgrund der vom Anbieter bereitgestellten Daten und Dokumentation wurden ausgeschöpft oder haben sich als unzureichend erwiesen.

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 VON AKTEUREN UND HOCHRISIKO-KI-SYSTEMEN GEMÄß ARTIKEL 51 BEREITZUSTELLENDE INFORMATIONEN

Anbieter, Bevollmächtigte und Nutzer, bei denen es sich um Behörden, oder öffentliche Einrichtungen oder Stellen handelt, reichen die in Teil I genannten Informationen ein. Anbieter oder gegebenenfalls Bevollmächtigte stellen sicher, dass die in Teil II Nummern 1 bis 11 genannten Angaben zu ihren Hochrisiko-KI-Systemen vollständig und richtig sind und auf dem aktuellen Stand gehalten werden. Die in Teil II Nummer 12 genannten Informationen werden von der Datenbank automatisch generiert.

Teil I: Informationen zu Akteuren (bei der Registrierung des Akteurs)

-1. Art des Akteurs (Anbieter, Bevollmächtigter oder Nutzer)

1. Name, Anschrift und Kontaktdaten des Anbieters

2. bei Vorlage von Informationen durch eine andere Person im Namen des Akteurs: Name, Anschrift und Kontaktdaten dieser Person

Teil II: Informationen zu dem Hochrisiko-KI-System

1. Name, Anschrift und Kontaktdaten des Anbieters

2. gegebenenfalls Name, Anschrift und Kontaktdaten des Bevollmächtigten

3. Handelsname des KI-Systems und etwaige zusätzliche eindeutige Angaben, die die Identifizierung und Rückverfolgbarkeit des KI-Systems ermöglichen

4. Beschreibung der Zweckbestimmung des KI-Systems

5. Status des KI-Systems (in Verkehr/in Betrieb; nicht mehr in Verkehr/in Betrieb, zurückgerufen)

6. Art, Nummer und Ablaufdatum der von der notifizierten Stelle ausgestellten Bescheinigung und gegebenenfalls Name oder Kennnummer dieser notifizierten Stelle

7. gegebenenfalls eine gescannte Kopie der in Nummer 6 genannten Bescheinigung

8. Mitgliedstaaten, in denen das KI-System in der Union in Verkehr gebracht, in Betrieb genommen oder bereitgestellt wird/wurde

9. eine Kopie der in Artikel 48 genannten EU-Konformitätserklärung

10. elektronische Gebrauchsanweisungen

11. URL-Adresse für zusätzliche Informationen (fakultativ)

12. Name, Anschrift und Kontaktdaten der Nutzer

ANHANG VIIIa

BEZÜGLICH TESTS UNTER REALEN BEDINGUNGEN GEMÄß ARTIKEL 54A BEI DER REGISTRIERUNG VON IN ANHANG III AUFGEFÜHRTEN HOCHRISIKO-KI-SYSTEMEN BEREITZUSTELLENDE INFORMATIONEN

Bezüglich Tests unter realen Bedingungen, die gemäß Artikel 54a zu registrieren sind, werden folgende Informationen bereitgestellt und danach auf dem neuesten Stand gehalten:

1. die unionsweit einmalige Kennnummer des Tests unter realen Bedingungen

2. Name und Kontaktdaten des Anbieters oder des zukünftigen Anbieters und der Nutzer, die an dem Test unter realen Bedingungen teilgenommen haben

3. eine kurze Beschreibung des KI-Systems, seine Zweckbestimmung und andere zu seiner Identifizierung erforderliche Informationen

4. eine Übersicht über die Hauptmerkmale des Plans für Tests unter realen Bedingungen

5. Informationen über die Aussetzung oder des Abbruchs des Tests unter realen Bedingungen

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

4. Einreise-/Ausreisesystem

a) Verordnung (EU) 2017/2226 des Europäischen Parlaments und des Rates vom 30. November 2017 über ein Einreise-/Ausreisesystem (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 (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) (ABl. L 135 vom 22.5.2019, S. 85)