Amtsblatt
der Europäischen Union

DE
Reihe L

2024/1689

12.7.2024

VERORDNUNG (EU) 2024/1689 DES EUROPÄISCHEN PARLAMENTS UND DES RATES

vom 13. Juni 2024

zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz und zur Änderung der Verordnungen (EG) Nr. 300/2008, (EU) Nr. 167/2013, (EU) Nr. 168/2013, (EU) 2018/858, (EU) 2018/1139 und (EU) 2019/2144 sowie der Richtlinien 2014/90/EU, (EU) 2016/797 und (EU) 2020/1828 (Verordnung über künstliche Intelligenz)

(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 der Europäischen Zentralbank ([2]),

nach Stellungnahme des Ausschusses der Regionen ([3]),

gemäß dem ordentlichen Gesetzgebungsverfahren ([4]),

in Erwägung nachstehender Gründe:

(1) Zweck dieser Verordnung ist es, das Funktionieren des Binnenmarkts zu verbessern, indem ein einheitlicher Rechtsrahmen insbesondere für die Entwicklung, das Inverkehrbringen, die Inbetriebnahme und die Verwendung von Systemen künstlicher Intelligenz (KI-Systeme) in der Union im Einklang mit den Werten der Union festgelegt wird, um die Einführung von menschenzentrierter und vertrauenswürdiger künstlicher Intelligenz (KI) zu fördern und gleichzeitig ein hohes Schutzniveau in Bezug auf Gesundheit, Sicherheit und der in der Charta der Grundrechte der Europäischen Union („Charta“) verankerten Grundrechte, einschließlich Demokratie, Rechtsstaatlichkeit und Umweltschutz, sicherzustellen, den Schutz vor schädlichen Auswirkungen von KI-Systemen in der Union zu gewährleisten und gleichzeitig die Innovation zu unterstützen. Diese Verordnung 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) Diese Verordnung sollte im Einklang mit den in der Charta verankerten Werten der Union angewandt werden, den Schutz von natürlichen Personen, Unternehmen, Demokratie und Rechtsstaatlichkeit sowie der Umwelt erleichtern und gleichzeitig Innovation und Beschäftigung fördern und der Union eine Führungsrolle bei der Einführung vertrauenswürdiger KI verschaffen.

(3) 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 KI vertrauenswürdig und sicher ist und im Einklang mit den Grundrechten entwickelt und verwendet wird. Unterschiedliche nationale Vorschriften können zu einer Fragmentierung des Binnenmarkts führen und können die Rechtssicherheit für Akteure, die KI-Systeme entwickeln, einführen oder verwenden, beeinträchtigen. Daher sollte in der gesamten Union ein einheitlich hohes Schutzniveau sichergestellt werden, um eine vertrauenswürdige KI zu erreichen, wobei Unterschiede, die den freien Verkehr, Innovationen, den Einsatz und die Verbreitung von KI-Systemen und damit zusammenhängenden

([1]) ABl. C 517 vom 22.12.2021, S. 56.
([2]) ABl. C 115 vom 11.3.2022, S. 5.
([3]) ABl. C 97 vom 28.2.2022, S. 60.
([4]) Standpunkt des Europäischen Parlaments vom 13. März 2024 (noch nicht im Amtsblatt veröffentlicht) und Beschluss des Rates vom 21. Mai 2024.

[sn107] Biometrische Kategorisierung

[sn206] Strafverfolgung

Produkten und Dienstleistungen im Binnenmarkt behindern, vermieden werden sollten, indem den Akteuren einheitliche Pflichten 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 Einzelpersonen im Hinblick auf die Verarbeitung personenbezogener Daten enthält, mit denen die Verwendung von KI-Systemen zur biometrischen Fernidentifizierung zu Strafverfolgungszwecken, die Verwendung von KI-Systemen für die Risikobewertung natürlicher Personen zu Strafverfolgungszwecken und die Verwendung von KI-Systemen zur biometrischen Kategorisierung zu Strafverfolgungszwecken eingeschränkt wird, ist es angezeigt, diese Verordnung in Bezug auf diese konkreten Vorschriften auf Artikel 16 AEUV zu stützen. Angesichts dieser konkreten Vorschriften und des Rückgriffs auf Artikel 16 AEUV ist es angezeigt, den Europäischen Datenschutzausschuss zu konsultieren.

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

(5) Gleichzeitig kann KI je nach den Umständen ihrer konkreten Anwendung und Nutzung sowie der technologischen Entwicklungsstufe Risiken mit sich bringen und öffentliche Interessen und grundlegende Rechte schädigen, die durch das Unionsrecht geschützt sind. Ein solcher Schaden kann materieller oder immaterieller Art sein, einschließlich physischer, psychischer, gesellschaftlicher oder wirtschaftlicher Schäden.

(6) Angesichts der großen Auswirkungen, die KI auf die Gesellschaft haben kann, und der Notwendigkeit, Vertrauen aufzubauen, ist es von entscheidender Bedeutung, dass KI und ihr Regulierungsrahmen im Einklang mit den in Artikel 2 des Vertrags über die Europäische Union (EUV) verankerten Werten der Union, den in den Verträgen und, nach Artikel 6 EUV, der Charta verankerten Grundrechten und -freiheiten entwickelt werden. Voraussetzung sollte sein, dass KI eine menschenzentrierte Technologie ist. Sie sollte den Menschen als Instrument dienen und letztendlich das menschliche Wohlergehen verbessern.

(7) Um ein einheitliches und hohes Schutzniveau in Bezug auf öffentliche Interessen im Hinblick auf Gesundheit, Sicherheit und Grundrechte zu gewährleisten, sollten für alle Hochrisiko-KI-Systeme gemeinsame Vorschriften festgelegt werden. Diese Vorschriften sollten mit der Charta im Einklang stehen, nichtdiskriminierend sein und mit den internationalen Handelsverpflichtungen der Union vereinbar sein. Sie sollten auch die Europäische Erklärung zu den digitalen Rechten und Grundsätzen für die digitale Dekade und die Ethikleitlinien für vertrauenswürdige KI der hochrangigen Expertengruppe für künstliche Intelligenz berücksichtigen.

(8) Daher ist ein Rechtsrahmen der Union mit harmonisierten Vorschriften für KI erforderlich, um die Entwicklung, Verwendung und Verbreitung von KI im Binnenmarkt zu fördern und gleichzeitig ein hohes Schutzniveau in Bezug auf öffentliche Interessen wie etwa Gesundheit und Sicherheit und den Schutz der durch das Unionsrecht anerkannten und geschützten Grundrechte, einschließlich der Demokratie, der Rechtsstaatlichkeit und des Umweltschutzes, zu gewährleisten. Zur Umsetzung dieses Ziels sollten Vorschriften für das Inverkehrbringen, die Inbetriebnahme und die Verwendung bestimmter KI-Systeme festgelegt werden, um das reibungslose Funktionieren des Binnenmarkts zu gewährleisten, sodass diesen Systemen der Grundsatz des freien Waren- und Dienstleistungsverkehrs zugutekommen kann. Diese Regeln sollten klar und robust sein, um die Grundrechte zu schützen, neue innovative Lösungen zu unterstützen und ein europäisches Ökosystem öffentlicher und privater Akteure zu ermöglichen, die KI-Systeme im Einklang mit den Werten der Union entwickeln, und um das Potenzial des digitalen Wandels in allen Regionen der Union zu erschließen. Durch die Festlegung dieser Vorschriften sowie durch Maßnahmen zur Unterstützung der Innovation mit besonderem Augenmerk auf kleinen und mittleren Unternehmen (KMU), einschließlich Start-up-Unternehmen, unterstützt diese Verordnung das vom Europäischen Rat formulierte Ziel, das europäische menschenzentrierte KI-Konzept zu fördern und bei der Entwicklung einer sicheren, vertrauenswürdigen und ethisch vertretbaren KI weltweit eine Führungsrolle einzunehmen ([5]), und sorgt für den vom Europäischen Parlament ausdrücklich geforderten Schutz von Ethikgrundsätzen ([6]).

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

([6]) 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).

(9) Es sollten harmonisierte 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 ([7]), dem Beschluss Nr. 768/2008/EG des Europäischen Parlaments und des Rates ([8]) und der Verordnung (EU) 2019/1020 des Europäischen Parlaments und des Rates ([9]) („neuer Rechtsrahmen") festgelegt werden. Die in dieser Verordnung festgelegten harmonisierten Vorschriften sollten in allen Sektoren gelten und sollten im Einklang mit dem neuen Rechtsrahmen bestehendes Unionsrecht, das durch diese Verordnung ergänzt wird, unberührt lassen, insbesondere in den Bereichen Datenschutz, Verbraucherschutz, Grundrechte, Beschäftigung, Arbeitnehmerschutz und Produktsicherheit. Daher bleiben alle Rechte und Rechtsbehelfe, die für Verbraucher und andere Personen, auf die sich KI-Systeme negativ auswirken können, gemäß diesem Unionsrecht vorgesehen sind, auch in Bezug auf einen möglichen Schadenersatz gemäß der Richtlinie 85/374/EWG des Rates ([10]) unberührt und in vollem Umfang anwendbar. Darüber hinaus und unter Einhaltung des Unionsrechts in Bezug auf Beschäftigungs- und Arbeitsbedingungen, einschließlich des Gesundheitsschutzes und der Sicherheit am Arbeitsplatz sowie der Beziehungen zwischen Arbeitgebern und Arbeitnehmern sollte diese Verordnung daher — was Beschäftigung und den Schutz von Arbeitnehmern angeht — das Unionsrecht im Bereich der Sozialpolitik und die nationalen Arbeitsrechtsvorschriften nicht berühren. Diese Verordnung sollte auch die Ausübung der in den Mitgliedstaaten und auf Unionsebene anerkannten Grundrechte, einschließlich des Rechts oder der Freiheit zum Streik oder zur Durchführung anderer Maßnahmen, die im Rahmen der spezifischen Systeme der Mitgliedstaaten im Bereich der Arbeitsbeziehungen vorgesehen sind, sowie das Recht, im Einklang mit nationalem Recht Kollektivvereinbarungen auszuhandeln, abzuschließen und durchzusetzen oder kollektive Maßnahmen zu ergreifen, nicht beeinträchtigen. Diese Verordnung sollte die in einer Richtlinie des Europäischen Parlaments und des Rates zur Verbesserung der Arbeitsbedingungen in der Plattformarbeit enthaltenen Bestimmungen nicht berühren. 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 unter Einhaltung des Unionsrechts angewandt 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, nämlich Personen unter 18 Jahren, unter Berücksichtigung der Allgemeinen Bemerkung Nr. 25 (2021) des UNCRC über die Rechte der Kinder im digitalen Umfeld von dieser Verordnung unberührt bleiben, sofern sie nicht spezifisch KI-Systeme betreffen und mit ihnen andere legitime Ziele des öffentlichen Interesses verfolgt werden.

(10) Das Grundrecht auf Schutz personenbezogener Daten wird insbesondere durch die Verordnungen (EU) 2016/679 ([11]) und (EU) 2018/1725 ([12]) des Europäischen Parlaments und des Rates und die Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates ([13]) gewahrt. Die Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates ([14]) schützt darüber hinaus die Privatsphäre und die Vertraulichkeit der Kommunikation, auch durch Bedingungen für die Speicherung personenbezogener und nicht personenbezogener Daten auf Endgeräten und den Zugang dazu. Diese Rechtsakte der Union bieten die Grundlage für eine nachhaltige und verantwortungsvolle Datenverarbeitung, auch wenn Datensätze eine Mischung aus personenbezogenen und nicht-personenbezogenen Daten enthalten. Diese Verordnung soll die Anwendung des bestehenden Unionsrechts zur Verarbeitung personenbezogener Daten, einschließlich der Aufgaben und Befugnisse der unabhängigen Aufsichtsbehörden, die für die Überwachung der Einhaltung dieser Instrumente zuständig sind, nicht berühren. Sie lässt ferner die Pflichten der Anbieter und Betreiber von KI-Systemen in ihrer Rolle als Verantwortliche oder Auftragsverarbeiter, die sich aus dem Unionsrecht oder dem nationalen Recht über den Schutz personenbezogener Daten ergeben, unberührt, soweit die Konzeption, die Entwicklung oder die Verwendung von KI-Systemen die Verarbeitung personenbezogener Daten

[sn502] Anbieter

[sn503] Betreiber

([7]) Verordnung (EG) Nr. 765/2008 des Europäischen Parlaments und des Rates vom 9. Juli 2008 über die Vorschriften für die Akkreditierung und zur Aufhebung der Verordnung (EWG) Nr. 339/93 des Rates (ABl. L 218 vom 13.8.2008, S. 30).

([8]) 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 zur Aufhebung des Beschlusses 93/465/EWG des Rates (ABl. L 218 vom 13.8.2008, S. 82).

([9]) 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).

([10]) Richtlinie 85/374/EWG des Rates vom 25. Juli 1985 zur Angleichung der Rechts- und Verwaltungsvorschriften der Mitgliedstaaten über die Haftung für fehlerhafte Produkte (ABl. L 210 vom 7.8.1985, S. 29).

([11]) 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).

([12]) 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).

([13]) 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 (ABl. L 119 vom 4.5.2016, S. 89).

([14]) Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation) (ABl. L 201 vom 31.7.2002, S. 37).

umfasst. Ferner sollte klargestellt werden, dass betroffene 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 dem Profiling. Harmonisierte Vorschriften für das Inverkehrbringen, die Inbetriebnahme und die Verwendung von KI-Systemen, die im Rahmen dieser Verordnung festgelegt werden, sollten die wirksame Durchführung erleichtern und die Ausübung der Rechte betroffener Personen und anderer Rechtsbehelfe, die im Unionsrecht über den Schutz personenbezogener Daten und anderer Grundrechte garantiert sind, ermöglichen.

[sn502] Anbieter

(11) Diese Verordnung sollte die Bestimmungen über die Verantwortlichkeit der Anbieter von Vermittlungsdiensten gemäß der Verordnung (EU) 2022/2065 des Europäischen Parlaments und des Rates ([15]) unberührt lassen.

(12) Der Begriff „KI-System“ in dieser Verordnung sollte klar definiert und eng mit der Tätigkeit internationaler Organisationen abgestimmt werden, die sich mit KI befassen, um Rechtssicherheit, mehr internationale Konvergenz und hohe Akzeptanz sicherzustellen und gleichzeitig Flexibilität zu bieten, um den raschen technologischen Entwicklungen in diesem Bereich Rechnung zu tragen. Darüber hinaus sollte die Begriffsbestimmung auf den wesentlichen Merkmalen der KI beruhen, die sie von einfacheren herkömmlichen Softwaresystemen und Programmierungsansätzen abgrenzen, und sollte sich nicht auf Systeme beziehen, die auf ausschließlich von natürlichen Personen definierten Regeln für das automatische Ausführen von Operationen beruhen. Ein wesentliches Merkmal von KI-Systemen ist ihre Fähigkeit, abzuleiten. Diese Fähigkeit bezieht sich auf den Prozess der Erzeugung von Ausgaben, wie Vorhersagen, Inhalte, Empfehlungen oder Entscheidungen, die physische und digitale Umgebungen beeinflussen können, sowie auf die Fähigkeit von KI-Systemen, Modelle oder Algorithmen oder beides aus Eingaben oder Daten abzuleiten. Zu den Techniken, die während der Gestaltung eines KI-Systems das Ableiten ermöglichen, gehören Ansätze für maschinelles Lernen, wobei aus Daten gelernt wird, wie bestimmte Ziele erreicht werden können, sowie logik- und wissensgestützte Konzepte, wobei aus kodierten Informationen oder symbolischen Darstellungen der zu lösenden Aufgabe abgeleitet wird. Die Fähigkeit eines KI-Systems, abzuleiten, geht über die einfache Datenverarbeitung hinaus, indem Lern-, Schlussfolgerungs- und Modellierungsprozesse ermöglicht werden. Die Bezeichnung „maschinenbasiert“ bezieht sich auf die Tatsache, dass KI-Systeme von Maschinen betrieben werden. Durch die Bezugnahme auf explizite oder implizite Ziele wird betont, dass KI-Systeme gemäß explizit festgelegten Zielen oder gemäß impliziten Zielen arbeiten können. Die Ziele des KI-Systems können sich — unter bestimmten Umständen — von der Zweckbestimmung des KI-Systems unterscheiden. Für die Zwecke dieser Verordnung sollten Umgebungen als Kontexte verstanden werden, in denen KI-Systeme betrieben werden, während die von einem KI-System erzeugten Ausgaben verschiedene Funktionen von KI-Systemen widerspiegeln, darunter Vorhersagen, Inhalte, Empfehlungen oder Entscheidungen. KI-Systeme sind mit verschiedenen Graden der Autonomie ausgestattet, was bedeutet, dass sie bis zu einem gewissen Grad unabhängig von menschlichem Zutun agieren und in der Lage sind, ohne menschliches Eingreifen zu arbeiten. Die Anpassungsfähigkeit, die ein KI-System nach Inbetriebnahme aufweisen könnte, bezieht sich auf seine Lernfähigkeit, durch sie es sich während seiner Verwendung verändern kann. KI-Systeme können eigenständig oder als Bestandteil eines Produkts verwendet werden, unabhängig davon, ob das System physisch in das Produkt integriert (eingebettet) ist oder der Funktion des Produkts dient, ohne darin integriert zu sein (nicht eingebettet).

[sn503] Betreiber

(13) Der in dieser Verordnung verwendete Begriff „Betreiber“ sollte als eine natürliche oder juristische Person, einschließlich Behörden, Einrichtungen oder sonstiger Stellen, die ein KI-System unter ihrer Befugnis verwenden, verstanden werden, es sei denn das KI-System wird im Rahmen einer persönlichen und nicht beruflichen Tätigkeit verwendet. Je nach Art des KI-Systems kann sich dessen Verwendung auf andere Personen als den Betreiber auswirken.

(14) Der in dieser Verordnung verwendete Begriff „biometrische Daten“ sollte im Sinne des Begriffs „biometrische Daten“ nach Artikel 4 Nummer 14 der Verordnung (EU) 2016/679, Artikel 3 Nummer 18 der Verordnung (EU) 2018/1725 und Artikel 3 Nummer 13 der Richtlinie (EU) 2016/680 ausgelegt werden. Biometrische Daten können die Authentifizierung, Identifizierung oder Kategorisierung natürlicher Personen und die Erkennung von Emotionen natürlicher Personen ermöglichen.

(15) Der Begriff „biometrische Identifizierung“ sollte gemäß dieser Verordnung als automatische Erkennung physischer, physiologischer und verhaltensbezogener menschlicher Merkmale wie Gesicht, Augenbewegungen, Körperform, Stimme, Prosodie, Gang, Haltung, Herzfrequenz, Blutdruck, Geruch, charakteristischer Tastenanschlag zum Zweck der Überprüfung der Identität einer Person durch Abgleich der biometrischen Daten der entsprechenden Person mit den in einer Datenbank gespeicherten biometrischen Daten definiert werden, unabhängig davon, ob die Einzelperson ihre Zustimmung dazu gegeben hat oder nicht. Dies umfasst keine KI-Systeme, die bestimmungsgemäß für die biometrische Verifizierung, wozu die Authentifizierung gehört, verwendet werden sollen, deren einziger Zweck darin besteht, zu bestätigen, dass eine bestimmte natürliche Person die Person ist, für die sie sich ausgibt, sowie zur Bestätigung der Identität einer natürlichen Person zu dem alleinigen Zweck Zugang zu einem Dienst zu erhalten, ein Gerät zu entriegeln oder Sicherheitszugang zu Räumlichkeiten zu erhalten.

([15]) Verordnung (EU) 2022/2065 des Europäischen Parlaments und des Rates vom 19. Oktober 2022 über einen Binnenmarkt für digitale Dienste und zur Änderung der Richtlinie 2000/31/EG (Gesetz über digitale Dienste) (ABl. L 277 vom 27.10.2022, S. 1).

[sn107] Biometrische Kategorisierung

(16) Der Begriff „biometrischen Kategorisierung“ sollte im Sinne dieser Verordnung die Zuordnung natürlicher Personen auf der Grundlage ihrer biometrischen Daten zu bestimmten Kategorien bezeichnen. Diese bestimmten Kategorien können Aspekte wie Geschlecht, Alter, Haarfarbe, Augenfarbe, Tätowierungen, Verhaltens- oder Persönlichkeitsmerkmale, Sprache, Religion, Zugehörigkeit zu einer nationalen Minderheit, sexuelle oder politische Ausrichtung betreffen. Dies gilt nicht für Systeme zur biometrischen Kategorisierung, bei denen es sich um eine reine Nebenfunktion handelt, die untrennbar mit einem anderen kommerziellen Dienst verbunden ist, d. h. die Funktion kann aus objektiven technischen Gründen nicht ohne den Hauptdienst verwendet werden und die Integration dieses Merkmals oder dieser Funktion dient nicht dazu, die Anwendbarkeit der Vorschriften dieser Verordnung zu umgehen. Beispielsweise könnten Filter zur Kategorisierung von Gesichts- oder Körpermerkmalen, die auf Online-Marktplätzen verwendet werden, eine solche Nebenfunktion darstellen, da sie nur im Zusammenhang mit der Hauptdienstleistung verwendet werden können, die darin besteht, ein Produkt zu verkaufen, indem es dem Verbraucher ermöglicht wird, zu sehen, wie das Produkt an seiner Person aussieht, und ihm so zu helfen, eine Kaufentscheidung zu treffen. Filter, die in sozialen Netzwerken eingesetzt werden und Gesichts- oder Körpermerkmale kategorisieren, um es den Nutzern zu ermöglichen, Bilder oder Videos hinzuzufügen oder zu verändern, können ebenfalls als Nebenfunktion betrachtet werden, da ein solcher Filter nicht ohne die Hauptdienstleistung sozialer Netzwerke verwendet werden kann, die in der Weitergabe von Online-Inhalten besteht.

(17) Der in dieser Verordnung verwendete Begriff „biometrisches Fernidentifizierungssystem“ sollte funktional definiert werden als KI-System, das dem Zweck dient, natürliche Personen ohne ihre aktive Einbeziehung in der Regel aus der Ferne durch Abgleich der biometrischen Daten einer Person mit den in einer Referenzdatenbank gespeicherten biometrischen Daten zu identifizieren, unabhängig davon, welche Technologie, Verfahren oder Arten biometrischer Daten dazu verwendet werden. Diese biometrischen Fernidentifizierungssysteme werden in der Regel zur zeitgleichen Erkennung mehrerer Personen oder ihrer Verhaltensweisen verwendet, um die Identifizierung natürlicher Personen ohne ihre aktive Einbeziehung erheblich zu erleichtern. Dies umfasst keine KI-Systeme, die bestimmungsgemäß für die biometrische Verifizierung, wozu die Authentifizierung gehört, verwendet werden sollen, deren einziger Zweck darin besteht, zu bestätigen, dass eine bestimmte natürliche Person die Person ist, für die sie sich ausgibt, sowie zur Bestätigung der Identität einer natürlichen Person zu dem alleinigen Zweck Zugang zu einem Dienst zu erhalten, ein Gerät zu entriegeln oder Sicherheitszugang zu Räumlichkeiten zu erhalten. Diese Ausnahme wird damit begründet, dass diese Systeme im Vergleich zu biometrischen Fernidentifizierungssystemen, die zur Verarbeitung biometrischer Daten einer großen Anzahl von Personen ohne ihre aktive Einbeziehung verwendet werden können, geringfügige Auswirkungen auf die Grundrechte natürlicher Personen haben dürften. Bei „Echtzeit-Systemen“ erfolgen die Erfassung der biometrischen Daten, der Abgleich und die Identifizierung zeitgleich, nahezu zeitgleich 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 etwa 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 etwa Bild- oder Videoaufnahmen, die von Video-Überwachungssystemen oder privaten Geräten vor der Anwendung des Systems auf die betroffenen natürlichen Personen erzeugt wurden.

(18) Der in dieser Verordnung verwendete Begriff „Emotionserkennungssystem“ sollte als ein KI-System definiert werden, das dem Zweck dient, Emotionen oder Absichten natürlicher Personen auf der Grundlage ihrer biometrischen Daten festzustellen oder daraus abzuleiten. In diesem Begriff geht es um Emotionen oder Absichten wie Glück, Trauer, Wut, Überraschung, Ekel, Verlegenheit, Aufregung, Scham, Verachtung, Zufriedenheit und Vergnügen. Dies umfasst nicht physische Zustände wie Schmerz oder Ermüdung, einschließlich beispielsweise Systeme, die zur Erkennung des Zustands der Ermüdung von Berufspiloten oder -fahrern eigesetzt werden, um Unfälle zu verhindern. Es geht dabei auch nicht um die bloße Erkennung offensichtlicher Ausdrucksformen, Gesten und Bewegungen, es sei denn, sie werden zum Erkennen oder Ableiten von Emotionen verwendet. Bei diesen Ausdrucksformen kann es sich um einfache Gesichtsausdrücke wie ein Stirnrunzeln oder ein Lächeln oder um Gesten wie Hand-, Arm- oder Kopfbewegungen oder um die Stimmmerkmale einer Person handeln, wie eine erhobene Stimme oder ein Flüstern.

(19) 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, unabhängig von den Tätigkeiten, für die der Ort verwendet werden kann; dazu zählen Bereiche wie etwa für Gewerbe, etwa Geschäfte, Restaurants, Cafés, für Dienstleistungen, etwa Banken, berufliche Tätigkeiten, Gastgewerbe, für Sport, etwa Schwimmbäder, Fitnessstudios, Stadien, für Verkehr, etwa Bus- und U-Bahn-Haltestellen, Bahnhöfe, Flughäfen, Transportmittel, für Unterhaltung, etwa Kinos, Theater, Museen, Konzert- und Konferenzsäle oder für 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, bestimmten im Voraus festgelegten 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 natürliche 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 Befugnis

über den Ort ausübt, bestimmt und festgelegt werden. Die tatsächliche Zugangsmöglichkeit allein, etwa eine unversperrte Tür oder 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 und Grenzkontrollbereiche sollten nicht zu den öffentlich zugänglichen Orten zählen. Einige andere Gebiete können sowohl öffentlich zugängliche als auch nicht öffentlich zugängliche Orte umfassen, etwa die Gänge eines privaten Wohngebäudes, deren Zugang erforderlich ist, um zu einer Arztpraxis zu gelangen, oder Flughäfen. 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.

[sn502] Anbieter

[sn503] Betreiber

[sn801] KI-Kompetenz

(20) Um den größtmöglichen Nutzen aus KI-Systemen zu ziehen und gleichzeitig die Grundrechte, Gesundheit und Sicherheit zu wahren und eine demokratische Kontrolle zu ermöglichen, sollte die KI-Kompetenz Anbieter, Betreiber und betroffene Personen mit den notwendigen Konzepten ausstatten, um fundierte Entscheidungen über KI-Systeme zu treffen. Diese Konzepte können in Bezug auf den jeweiligen Kontext unterschiedlich sein und das Verstehen der korrekten Anwendung technischer Elemente in der Entwicklungsphase des KI-Systems, der bei seiner Verwendung anzuwendenden Maßnahmen und der geeigneten Auslegung der Ausgaben des KI-Systems umfassen sowie — im Falle betroffener Personen — das nötige Wissen, um zu verstehen, wie sich mithilfe von KI getroffene Entscheidungen auf sie auswirken werden. Im Zusammenhang mit der Anwendung dieser Verordnung sollte die KI-Kompetenz allen einschlägigen Akteuren der KI-Wertschöpfungskette die Kenntnisse vermitteln, die erforderlich sind, um die angemessene Einhaltung und die ordnungsgemäße Durchsetzung der Verordnung sicherzustellen. Darüber hinaus könnten die umfassende Umsetzung von KI-Kompetenzmaßnahmen und die Einführung geeigneter Folgemaßnahmen dazu beitragen, die Arbeitsbedingungen zu verbessern und letztlich die Konsolidierung und den Innovationspfad vertrauenswürdiger KI in der Union unterstützen. Ein Europäisches Gremium für Künstliche Intelligenz (im Folgenden „KI-Gremium“) sollte die Kommission dabei unterstützen, KI-Kompetenzinstrumente sowie die Sensibilisierung und Aufklärung der Öffentlichkeit in Bezug auf die Vorteile, Risiken, Schutzmaßnahmen, Rechte und Pflichten im Zusammenhang mit der Nutzung von KI-Systeme zu fördern. In Zusammenarbeit mit den einschlägigen Interessenträgern sollten die Kommission und die Mitgliedstaaten die Ausarbeitung freiwilliger Verhaltenskodizes erleichtern, um die KI-Kompetenz von Personen, die mit der Entwicklung, dem Betrieb und der Verwendung von KI befasst sind, zu fördern.

(21) Um gleiche Wettbewerbsbedingungen und einen wirksamen Schutz der Rechte und Freiheiten von Einzelpersonen 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 Betreiber von KI-Systemen, die in der Union niedergelassen sind, gelten.

(22) 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 niedergelassener Akteur bestimmte Dienstleistungen an einen in einem Drittland 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 in einem Drittland betriebene KI-System Daten verarbeiten, die rechtmäßig in der Union erhoben und aus der Union übertragen wurden, und dem vertraglichen Akteur in der Union die aus dieser Verarbeitung resultierende Ausgabe dieses KI-Systems liefern, ohne dass dieses KI-System dabei in der Union in Verkehr gebracht, in Betrieb genommen oder verwendet würde. 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 Betreiber von KI-Systemen gelten, die in einem Drittland niedergelassen sind, soweit beabsichtigt wird, die von diesem System erzeugte Ausgabe in der Union zu verwenden. 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 der Zusammenarbeit oder internationaler Übereinkünfte tätig werden, die auf Unionsebene oder nationaler Ebene für die Zusammenarbeit mit der Union oder den Mitgliedstaaten im Bereich der Strafverfolgung und der justiziellen Zusammenarbeit geschlossen wurden, vorausgesetzt dass dieses Drittland oder diese internationale Organisationen angemessene Garantien in Bezug auf den Schutz der Grundrechte und -freiheiten von Einzelpersonen bieten. Dies kann gegebenenfalls Tätigkeiten von Einrichtungen umfassen, die von Drittländern mit der Wahrnehmung bestimmter Aufgaben zur Unterstützung dieser Zusammenarbeit im Bereich der Strafverfolgung und der justiziellen Zusammenarbeit betraut wurden. Ein solcher Rahmen für die Zusammenarbeit oder für Übereinkünfte wurde bilateral zwischen Mitgliedstaaten und Drittländern oder zwischen der Europäischen Union, Europol und anderen Agenturen der Union und Drittländern und internationalen Organisationen erarbeitet. Die Behörden, die nach dieser Verordnung für die Aufsicht über die Strafverfolgungs- und Justizbehörden zuständig sind, sollten prüfen, ob diese Rahmen für die Zusammenarbeit oder internationale Übereinkünfte angemessene Garantien in Bezug auf den Schutz der Grundrechte und -freiheiten von Einzelpersonen enthalten. Empfangende nationale Behörden und Organe, Einrichtungen sowie sonstige Stellen der Union, die diese Ausgaben in der Union verwenden, sind weiterhin dafür verantwortlich, sicherzustellen, dass ihre

[sn206] Strafverfolgung

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.

[sn502] Anbieter

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

(24) 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 gründet 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 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 Verteidigungstätigkeiten darstellt. In Bezug auf die Zwecke im Bereich nationale Sicherheit gründet sich die Ausnahme sowohl auf die Tatsache, dass die nationale Sicherheit gemäß 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 KI-System für andere Zwecke als Zwecke in den Bereichen Militär, Verteidigung oder nationale Sicherheit verwendet, die Konformität des KI-Systems mit dieser Verordnung sicherstellen, es sei denn, das System entspricht bereits dieser Verordnung. KI-Systeme, die für einen ausgeschlossenen Zweck, nämlich Militär, Verteidigung oder nationale Sicherheit, und für einen oder mehrere nicht ausgeschlossene Zwecke, etwa zivile Zwecke oder Strafverfolgungszwecke, 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 den Bereichen nationale Sicherheit, Verteidigung oder Militär ausüben, KI-Systeme für Zwecke in den Bereichen nationale Sicherheit, Militär und Verteidigung verwenden können, unabhängig von der Art der Einrichtung, die diese Tätigkeiten ausübt, wobei die 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.

[sn206] Strafverfolgung

(25) Diese Verordnung sollte die Innovation fördern, die Freiheit der Wissenschaft achten und Forschungs- und Entwicklungstätigkeiten nicht untergraben. Daher müssen KI-Systeme und -Modelle, die eigens für den alleinigen Zweck der wissenschaftlichen Forschung und Entwicklung entwickelt und in Betrieb genommen werden, vom Anwendungsbereich der Verordnung ausgenommen werden. Ferner muss sichergestellt werden, dass sich die Verordnung nicht anderweitig auf Forschungs- und Entwicklungstätigkeiten zu KI-Systemen und -Modellen auswirkt, bevor diese in Verkehr gebracht oder in Betrieb genommen werden. Hinsichtlich produktorientierter Forschungs-, Test- und Entwicklungstätigkeiten in Bezug auf KI-Systeme oder -Modelle sollten die Bestimmungen dieser Verordnung auch nicht vor der Inbetriebnahme oder dem Inverkehrbringen dieser Systeme und Modelle gelten. Diese Ausnahme berührt weder die Pflicht zur Einhaltung dieser Verordnung, wenn ein KI-System, das in den Anwendungsbereich dieser Verordnung fällt, infolge solcher Forschungs- und Entwicklungstätigkeiten in Verkehr gebracht oder in Betrieb genommen wird, noch die Anwendung der Bestimmungen zu KI-Reallaboren und zu Tests unter Realbedingungen. Darüber hinaus sollte unbeschadet der Ausnahme 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 Entwicklungstätigkeiten verwendet werden könnte, den Bestimmungen dieser Verordnung unterliegen. In jedem Fall sollten jegliche Forschungs- und Entwicklungstätigkeiten gemäß anerkannten ethischen und professionellen Grundsätzen für die wissenschaftliche Forschung und unter Wahrung des geltenden Unionsrechts ausgeführt werden.

(26) 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 inakzeptable Praktiken im Bereich der KI zu verbieten und Anforderungen an Hochrisiko-KI-Systeme und Pflichten für die betreffenden Akteure sowie Transparenzpflichten für bestimmte KI-Systeme festzulegen.

(27) Während der risikobasierte Ansatz die Grundlage für ein verhältnismäßiges und wirksames verbindliches Regelwerk bildet, muss auch auf die Ethikleitlinien für vertrauenswürdige KI von 2019 der von der Kommission eingesetzten unabhängigen hochrangigen Expertengruppe für künstliche Intelligenz verwiesen werden. In diesen Leitlinien hat die hochrangige Expertengruppe sieben unverbindliche ethische Grundsätze für KI entwickelt, die dazu beitragen sollten, dass KI vertrauenswürdig und ethisch vertretbar ist. Zu den sieben Grundsätzen gehören: menschliches Handeln und menschliche Aufsicht, technische Robustheit und Sicherheit, Privatsphäre und Daten-Governance, Transparenz, Vielfalt, Nichtdiskriminierung und Fairness, soziales und ökologisches Wohlergehen sowie Rechenschaftspflicht. Unbeschadet der rechtsverbindlichen Anforderungen dieser Verordnung und anderer geltender Rechtsvorschriften der Union tragen diese Leitlinien zur Gestaltung kohärenter, vertrauenswürdiger und menschenzentrierter KI bei im Einklang mit der Charta und den Werten, auf die sich die Union gründet. Nach den Leitlinien der hochrangigen Expertengruppe bedeutet „menschliches Handeln und menschliche Aufsicht“, dass ein KI-System entwickelt und als Instrument verwendet wird, das den Menschen dient, die Menschenwürde und die persönliche Autonomie achtet und so funktioniert, dass es von Menschen angemessen kontrolliert und überwacht werden kann. „Technische Robustheit und Sicherheit“ bedeutet, dass KI-Systeme so entwickelt und verwendet werden, dass sie im Fall von Schwierigkeiten robust sind und widerstandsfähig gegen Versuche, die Verwendung oder Leistung des KI-Systems so zu verändern, dass dadurch die unrechtmäßige Verwendung durch Dritte ermöglicht wird, und dass ferner unbeabsichtigte Schäden minimiert werden. „Privatsphäre und Daten-Governance“ bedeutet, dass KI-Systeme im Einklang mit den geltenden Vorschriften zum Schutz der Privatsphäre und zum Datenschutz entwickelt und verwendet werden und dabei Daten verarbeiten, die hohen Qualitäts- und Integritätsstandards genügen. „Transparenz“ bedeutet, dass KI-Systeme so entwickelt und verwendet werden, dass sie angemessen nachvollziehbar und erklärbar sind, wobei den Menschen bewusst gemacht werden muss, dass sie mit einem KI-System kommunizieren oder interagieren, und dass die Betreiber ordnungsgemäß über die Fähigkeiten und Grenzen des KI-Systems informieren und die betroffenen Personen über ihre Rechte in Kenntnis setzen müssen. „Vielfalt, Nichtdiskriminierung und Fairness“ bedeutet, dass KI-Systeme in einer Weise entwickelt und verwendet werden, die unterschiedliche Akteure einbezieht und den gleichberechtigten Zugang, die Geschlechtergleichstellung und die kulturelle Vielfalt fördert, wobei diskriminierende Auswirkungen und unfaire Verzerrungen, die nach Unionsrecht oder nationalem Recht verboten sind, verhindert werden. „Soziales und ökologisches Wohlergehen“ bedeutet, dass KI-Systeme in nachhaltiger und umweltfreundlicher Weise und zum Nutzen aller Menschen entwickelt und verwendet werden, wobei die langfristigen Auswirkungen auf den Einzelnen, die Gesellschaft und die Demokratie überwacht und bewertet werden. Die Anwendung dieser Grundsätze sollte, soweit möglich, in die Gestaltung und Verwendung von KI-Modellen einfließen. Sie sollten in jedem Fall als Grundlage für die Ausarbeitung von Verhaltenskodizes im Rahmen dieser Verordnung dienen. Alle Interessenträger, einschließlich der Industrie, der Wissenschaft, der Zivilgesellschaft und der Normungsorganisationen, werden aufgefordert, die ethischen Grundsätze bei der Entwicklung freiwilliger bewährter Verfahren und Normen, soweit angebracht, zu berücksichtigen.

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

(29) 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 das Ziel oder die Auswirkung haben, menschliches Verhalten maßgeblich nachteilig zu beeinflussen, und große Schäden, insbesondere erhebliche nachteilige Auswirkungen auf die physische und psychische Gesundheit oder auf die finanziellen Interessen verursachen dürften, ist besonders gefährlich und sollte 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 manipulativer oder täuschender 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. Dies könnte beispielsweise durch Gehirn-Computer-Schnittstellen oder virtuelle Realität erfolgen, da diese ein höheres Maß an Kontrolle darüber ermöglichen, welche Reize den Personen, insofern diese das Verhalten der Personen in erheblichem Maße schädlich beeinflussen können, angeboten werden. Ferner können KI-Systeme auch anderweitig die Vulnerabilität einer Person oder bestimmter Gruppen von Personen aufgrund ihres Alters oder einer Behinderung im Sinne der Richtlinie (EU) 2019/882 des Europäischen Parlaments und des Rates ([16]) 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 mit dem Ziel oder der Wirkung in Verkehr gebracht, in Betrieb genommen oder verwendet werden, das Verhalten einer Person in einer Weise wesentlich zu beeinflussen, die dieser Person oder einer anderen Person oder Gruppen von Personen einen erheblichen Schaden zufügt oder mit hinreichender Wahrscheinlichkeit

([16]) Richtlinie (EU) 2019/882 des Europäischen Parlaments und des Rates vom 17. April 2019 über die Barrierefreiheitsanforderungen für Produkte und Dienstleistungen (ABl. L 151 vom 7.6.2019, S. 70).

[sn107] Biometrische Kategorisierung

[sn502] Anbieter

[sn503] Betreiber

zufügen wird, einschließlich Schäden, die sich im Laufe der Zeit anhäufen können, und sollten daher verboten werden. 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 Betreibers liegen, d. h. Faktoren, die vom Anbieter oder Betreiber des KI-Systems vernünftigerweise nicht vorhergesehen oder gemindert werden können. In jedem Fall ist es nicht erforderlich, dass der Anbieter oder der Betreiber die Absicht haben, erheblichen 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 des Europäischen Parlaments und des Rates ([17]); insbesondere sind unlautere Geschäftspraktiken, durch 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 gemäß den geltenden Rechtsvorschriften und medizinischen Standards erfolgen, z. B mit der ausdrücklichen Zustimmung der Einzelpersonen oder ihrer gesetzlichen Vertreter. Darüber hinaus sollten übliche und rechtmäßige Geschäftspraktiken, beispielsweise im Bereich der Werbung, die im Einklang mit den geltenden Rechtsvorschriften stehen, als solche nicht als schädliche manipulative KI-gestützten Praktiken gelten.

(30) Systeme zur biometrischen Kategorisierung, die anhand der biometrischen Daten von natürlichen Personen, wie dem Gesicht oder dem Fingerabdruck einer Person, die politische Meinung, die Mitgliedschaft in einer Gewerkschaft, religiöse oder weltanschauliche Überzeugungen, die Rasse, das Sexualleben oder die sexuelle Ausrichtung einer Person erschließen oder ableiten, sollten verboten werden. Dieses Verbot sollte nicht für die rechtmäßige Kennzeichnung, Filterung oder Kategorisierung biometrischer Datensätze gelten, die im Einklang mit dem Unionsrecht oder dem nationalen Recht anhand biometrischer Daten erworben wurden, wie das Sortieren von Bildern nach Haar- oder Augenfarbe, was beispielsweise im Bereich der Strafverfolgung verwendet werden kann.

[sn108] Biometrische Echtzeit-Fernidentifizierung

(31) KI-Systeme, die eine soziale Bewertung natürlicher Personen durch öffentliche oder private Akteure bereitstellen, 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 oder Gruppen natürlicher Personen in einem bestimmten Zeitraum auf der Grundlage zahlreicher Datenpunkte in Bezug auf ihr soziales Verhalten in verschiedenen Zusammenhängen oder aufgrund bekannter, vermuteter oder vorhergesagter persönlicher Eigenschaften oder Persönlichkeitsmerkmale. Die aus solchen KI-Systemen erzielte soziale Bewertung kann zu einer Schlechterstellung oder Benachteiligung bestimmter natürlicher Personen oder ganzer Gruppen natürlicher Personen in sozialen Kontexten, die in keinem Zusammenhang mit den Umständen stehen, unter denen die Daten ursprünglich erzeugt oder erhoben wurden, oder zu einer Schlechterstellung führen, die im Hinblick auf die Tragweite ihres sozialen Verhaltens unverhältnismäßig oder ungerechtfertigt ist. KI-Systeme, die solche inakzeptablen Bewertungspraktiken mit sich bringen und zu einer solchen Schlechterstellung oder Benachteiligung führen, sollten daher verboten werden. Dieses Verbot sollte nicht die rechtmäßigen Praktiken zur Bewertung natürlicher Personen berühren, die im Einklang mit dem Unionsrecht und dem nationalen Recht zu einem bestimmten Zweck durchgeführt werden.

(32) Die Verwendung von KI-Systemen zur biometrischen Echtzeit-Fernidentifizierung natürlicher Personen in öffentlich zugänglichen Räumen zu Strafverfolgungszwecken greift besonders in die Rechte und Freiheiten der betroffenen Personen ein, 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. Technische Ungenauigkeiten von KI-Systemen, die für die biometrische Fernidentifizierung natürlicher Personen bestimmt sind, können zu verzerrten Ergebnissen führen und eine diskriminierende Wirkung haben. Solche möglichen verzerrten Ergebnisse und eine solche diskriminierende Wirkung sind von besonderer Bedeutung, wenn es um das Alter, die ethnische Herkunft, die Rasse, das Geschlecht oder Behinderungen geht. Darüber hinaus bergen die Unmittelbarkeit der Auswirkungen und die begrenzten Möglichkeiten weiterer Kontrollen oder Korrekturen im Zusammenhang mit der Verwendung solcher in Echtzeit betriebener Systeme erhöhte Risiken für die Rechte und Freiheiten der betreffenden Personen, die im Zusammenhang mit Strafverfolgungsmaßnahmen stehen oder davon betroffen sind.

(33) 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 bestimmten Opfern von Straftaten, einschließlich vermisster Personen, bestimmte Gefahren für das Leben oder die körperliche Unversehrtheit natürlicher Personen oder die Gefahr eines Terroranschlags sowie das Aufspüren oder Identifizieren von Tätern oder Verdächtigen in Bezug auf die in einem Anhang zu dieser Verordnung

([17]) Richtlinie 2005/29/EG des Europäischen Parlaments und des Rates vom 11. Mai 2005 über unlautere Geschäftspraktiken im binnenmarktinternen Geschäftsverkehr zwischen Unternehmen und Verbrauchern und zur Änderung der Richtlinie 84/450/EWG des Rates, der Richtlinien 97/7/EG, 98/27/EG und 2002/65/EG des Europäischen Parlaments und des Rates sowie der Verordnung (EG) Nr. 2006/2004 des Europäischen Parlaments und des Rates (Richtlinie über unlautere Geschäftspraktiken) (ABl. L 149 vom 11.6.2005, S. 22).

[sn202] Kritische Infrastruktur

[sn108] Biometrische Echtzeit-Fernidentifizierung

genannten Straftaten, sofern diese Straftaten in dem betreffenden Mitgliedstaat im Sinne des Rechts dieses Mitgliedstaats mit einer Freiheitsstrafe oder einer freiheitsentziehenden Maßregel der Sicherung im Höchstmaß von mindestens vier 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 möglicherweise zu rechtfertigen. Darüber hinaus beruht die im Anhang dieser Verordnung aufgeführte Liste der Straftaten auf den 32 im Rahmenbeschluss 2002/584/JI des Rates ([18]) aufgeführten Straftaten, unter Berücksichtigung der Tatsache, dass einige der Straftaten in der Praxis eher relevant sein können als andere, da der Rückgriff auf die biometrische Echtzeit-Fernidentifizierung für die konkrete Aufspürung oder Identifizierung eines Täters oder Verdächtigen in Bezug auf eine der verschiedenen aufgeführten Straftaten voraussichtlich in äußerst unterschiedlichem Maße erforderlich und verhältnismäßig sein könnte und da dabei die wahrscheinlichen Unterschiede in Schwere, Wahrscheinlichkeit und Ausmaß des Schadens oder möglicher negativer Folgen zu berücksichtigen sind. Eine unmittelbare Gefahr für das Leben oder die körperliche Unversehrtheit natürlicher Personen kann auch durch die schwerwiegende Störung einer kritischen Infrastruktur im Sinne des Artikels 2 Nummer 4 der Richtlinie (EU) 2022/2557 des Europäischen Parlaments und des Rates ([19]) entstehen, wenn die Störung oder Zerstörung einer solchen kritischen Infrastruktur zu einer unmittelbaren Gefahr für das Leben oder die körperliche Unversehrtheit einer Person führen würde, auch durch die schwerwiegende Beeinträchtigung der Bereitstellung der Grundversorgung für die Bevölkerung oder der Wahrnehmung der Kernfunktion des Staates. Darüber hinaus sollte diese Verordnung die Fähigkeit der Strafverfolgungs-, Grenzschutz-, Einwanderungs- oder Asylbehörden erhalten, gemäß 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 gemäß dem Unionsrecht oder 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, 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.

(34) 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 nur eingesetzt werden, um die Identität der speziell betroffenen Person zu bestätigen und sollte sich hinsichtlich des Zeitraums und des geografischen und personenbezogenen Anwendungsbereichs auf das unbedingt Notwendige beschränken, wobei insbesondere den Beweisen oder Hinweisen in Bezug auf die Bedrohungen, die Opfer oder den Täter Rechnung zu tragen ist. Die Verwendung des biometrischen Echtzeit-Fernidentifizierungssystems in öffentlich zugänglichen Räumen sollte nur genehmigt werden, wenn die zuständige Strafverfolgungsbehörde eine Grundrechte-Folgenabschätzung durchgeführt und, sofern in dieser Verordnung nichts anderes bestimmt ist, das System gemäß dieser Verordnung in der Datenbank registriert hat. Die Personenreferenzdatenbank sollte für jeden Anwendungsfall in jedem der oben genannten Fälle geeignet sein.

(35) 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, deren Entscheidung rechtsverbindlich ist, unterliegen. Eine solche Genehmigung sollte grundsätzlich vor der Verwendung des KI-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 des KI-Systems eine Genehmigung einzuholen. In solchen dringenden Fällen sollte die Verwendung des KI-Systems 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 Fällen eine solche Genehmigung beantragen und die Gründe dafür angeben, warum sie sie nicht früher, unverzüglich, spätestens jedoch innerhalb von 24 Stunden beantragen konnte. Wird eine solche Genehmigung abgelehnt, sollte die Verwendung biometrischer Echtzeit-Identifizierungssysteme, die mit dieser Genehmigung verbunden sind, mit sofortiger Wirkung eingestellt werden, und alle Daten im Zusammenhang mit dieser Verwendung sollten verworfen und gelöscht werden. Diese Daten umfassen Eingabedaten, die von einem KI-System während der Nutzung eines solchen Systems direkt erfasst werden, sowie die Ergebnisse und Ausgaben der mit dieser Genehmigung verbundenen Verwendung. Daten, die im Einklang mit anderem Unionsrecht oder nationalem Recht rechtmäßig

([18]) 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).

([19]) Richtlinie (EU) 2022/2557 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über die Resilienz kritischer Einrichtungen und zur Aufhebung der Richtlinie 2008/114/EG des Rates (ABl. L 333 vom 27.12.2022, S. 164).

erworben wurden, sollten davon nicht betroffen sein. In jedem Fall darf keine Entscheidung mit nachteiligen Rechtsfolgen für eine Person allein auf der Grundlage der Ausgaben des biometrischen Fernidentifizierungssystems getroffen werden.

(36) Damit sie ihre Aufgaben im Einklang mit den Anforderungen dieser Verordnung und der nationalen Vorschriften erfüllen können, sollte die zuständige Marktüberwachungsbehörde und die nationale Datenschutzbehörde über jede Verwendung des biometrischen Echtzeit-Identifizierungssystems unterrichtet werden. Die Marktüberwachungsbehörden und die nationalen Datenschutzbehörden, die unterrichtet wurden, sollten der Kommission jährlich einen Bericht über die Verwendung biometrischer Echtzeit-Identifizierungssysteme vorlegen.

(37) Darüber hinaus ist es angezeigt, innerhalb des durch diese Verordnung vorgegebenen erschöpfenden Rahmens festzulegen, dass eine solche Verwendung im Hoheitsgebiet eines Mitgliedstaats gemäß 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. Solche nationalen Rechtsvorschriften sollten der Kommission spätestens 30 Tage nach ihrer Annahme mitgeteilt werden.

(38) 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 des Artikels 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 den zu dieser Genehmigung anwendbaren detaillierten nationalen Rechtsvorschriften unterliegen.

(39) 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 gemäß Artikel 9 Absatz 1 der Verordnung (EU) 2016/679 und Artikel 10 Absatz 1 der Verordnung (EU) 2018/1725, vorbehaltlich der in diesen Artikeln vorgesehenen begrenzten Ausnahmefällen, verboten. In Anwendung des Artikels 9 Absatz 1 der Verordnung (EU) 2016/679 war die Verwendung biometrischer Fernidentifizierung zu anderen Zwecken als der Strafverfolgung bereits Gegenstand von Verbotsentscheidungen der nationalen Datenschutzbehörden.

(40) 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 Unterabsatz 1 Buchstabe g, soweit er auf die Verwendung von Systemen zur biometrischen Kategorisierung für Tätigkeiten im Bereich der polizeilichen Zusammenarbeit und der justiziellen Zusammenarbeit in Strafsachen Anwendung findet, Artikel 5 Absatz 1 Buchstabe d, soweit sie auf die Verwendung von KI-Systemen nach der darin festgelegten Bestimmung Anwendung finden, sowie Artikel 5 Absatz 1 Unterabsatz 1 Buchstabe h, Artikel 5 Absätze 2 bis 6 und Artikel 26 Absatz 10 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 oder 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.

(41) 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 Unterabsatz 1 Buchstabe g soweit er auf die Verwendung von Systemen zur biometrischen Kategorisierung für Tätigkeiten im Bereich der polizeilichen Zusammenarbeit und der justiziellen Zusammenarbeit in Strafsachen Anwendung findet, Artikel 5 Absatz 1 Unterabsatz 1 Buchstaben d soweit sie auf die Verwendung von KI-Systemen

nach der darin festgelegten Bestimmung Anwendung finden, sowie Artikel 5 Absatz 1 Unterabsatz 1 Buchstabe h, Artikel 5 Absätze 2 bis 6 und Artikel 26 Absatz 10 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 oder 5 AEUV fallen, weder gebunden noch zu ihrer Anwendung verpflichtet.

(42) Im Einklang mit der Unschuldsvermutung sollten natürliche Personen in der Union stets nach ihrem tatsächlichen Verhalten beurteilt werden. Natürliche Personen sollten niemals allein nach dem Verhalten beurteilt werden, das von einer KI auf der Grundlage ihres Profiling, ihrer Persönlichkeitsmerkmale oder -eigenschaften wie Staatsangehörigkeit, Geburtsort, Wohnort, Anzahl der Kinder, Schulden oder Art ihres Fahrzeugs vorhergesagt wird, ohne dass ein begründeter Verdacht besteht, dass diese Person an einer kriminellen Tätigkeit auf der Grundlage objektiver nachprüfbarer Tatsachen beteiligt ist, und ohne dass eine menschliche Überprüfung stattfindet. Daher sollten Risikobewertungen, die in Bezug auf natürliche Personen durchgeführt werden, um zu bewerten, ob sie straffällig werden oder um eine tatsächliche oder mögliche Straftat vorherzusagen, und dies ausschließlich auf dem Profiling dieser Personen oder der Bewertung ihrer Persönlichkeitsmerkmale und -eigenschaften beruht, verboten werden. In jedem Fall betrifft oder berührt dieses Verbot nicht Risikoanalysen, die nicht auf dem Profiling von Einzelpersonen oder auf Persönlichkeitsmerkmalen und -eigenschaften von Einzelpersonen beruhen, wie etwa KI-Systeme, die Risikoanalysen zur Bewertung der Wahrscheinlichkeit eines Finanzbetrugs durch Unternehmen auf der Grundlage verdächtiger Transaktionen durchführen, oder Risikoanalyseinstrumente einsetzen, um die Wahrscheinlichkeit vorherzusagen, dass Betäubungsmittel oder illegale Waren durch Zollbehörden, beispielsweise auf der Grundlage bekannter Schmuggelrouten, aufgespürt werden.

[sn502] Anbieter

(43) Das Inverkehrbringen, die Inbetriebnahme für diesen spezifischen Zweck oder die Verwendung von KI-Systemen, die Datenbanken zur Gesichtserkennung durch das ungezielte Auslesen von Gesichtsbildern aus dem Internet oder von Videoüberwachungsaufnahmen erstellen oder erweitern, sollte verboten werden, da dies das Gefühl der Massenüberwachung verstärkt und zu schweren Verstößen gegen die Grundrechte, einschließlich des Rechts auf Privatsphäre, führen kann.

(44) Im Hinblick auf die wissenschaftliche Grundlage von KI-Systemen, die darauf abzielen, Emotionen zu erkennen oder abzuleiten, bestehen ernsthafte Bedenken, insbesondere da sich Gefühlsausdrücke je nach Kultur oder Situation und selbst bei ein und derselben Person erheblich unterscheiden. Zu den größten Schwachstellen solcher Systeme gehört, dass sie beschränkt zuverlässig, nicht eindeutig und nur begrenzt verallgemeinerbar sind. Daher können KI-Systeme, die Emotionen oder Absichten natürlicher Personen auf der Grundlage ihrer biometrischen Daten erkennen oder ableiten, diskriminierende Ergebnisse hervorbringen und in die Rechte und Freiheiten der betroffenen Personen eingreifen. Angesichts des Machtungleichgewichts in den Bereichen Arbeit und Bildung in Verbindung mit dem intrusiven Charakter dieser Systeme können diese zu einer Schlechterstellung oder Benachteiligung bestimmter natürlicher Personen oder ganzer Gruppen führen. Daher sollte das Inverkehrbringen, die Inbetriebnahme oder die Verwendung von KI-Systemen, die den emotionalen Zustand von Einzelpersonen in Situationen, ableiten sollen, die mit dem Arbeitsplatz oder dem Bildungsbereich in Zusammenhang stehen, verboten werden. Dieses Verbot sollte nicht für KI-Systeme gelten, die ausschließlich aus medizinischen oder sicherheitstechnischen Gründen in Verkehr gebracht werden, wie z. B. Systeme, die für therapeutische Zwecke bestimmt sind.

(45) Praktiken, die nach Unionsrecht, einschließlich Datenschutzrecht, Nichtdiskriminierungsrecht, Verbraucherschutzrecht und Wettbewerbsrecht, verboten sind, sollten von dieser Verordnung nicht betroffen sein.

(46) Hochrisiko-KI-Systeme sollten nur dann auf dem Unionsmarkt in Verkehr gebracht, in Betrieb genommen oder verwendet werden, wenn sie bestimmte verbindliche Anforderungen erfüllen. Mit diesen Anforderungen sollte sichergestellt werden, dass Hochrisiko-KI-Systeme, die in der Union verfügbar sind oder deren Ausgabe anderweitig in der Union verwendet wird, keine unannehmbaren Risiken für wichtige öffentliche Interessen der Union bergen, wie sie im Unionsrecht anerkannt und geschützt sind. Auf der Grundlage des neuen Rechtsrahmens, wie in der Bekanntmachung der Kommission „Leitfaden für die Umsetzung der Produktvorschriften der EU 2022 (Blue Guide)“ ([20]) dargelegt, gilt als allgemeine Regel, dass mehr als ein Rechtsakt der Harmonisierungsrechtsvorschriften der Union wie die Verordnungen (EU) 2017/745 ([21]) und (EU) 2017/746 ([22]) des Europäischen Parlaments und des Rates oder die Richtlinie 2006/42/EG des Europäischen Parlaments und des Rates ([23]) auf ein Produkt anwendbar sein können, da die Bereitstellung oder Inbetriebnahme nur erfolgen kann, wenn das Produkt allen geltenden Harmonisierungsrechtsvorschriften der Union entspricht. Um Kohärenz zu gewährleisten und unnötigen

([20]) ABl. C 247 vom 29.6.2022, S. 1.
([21]) 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).
([22]) 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).
([23]) 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).

Verwaltungsaufwand oder Kosten zu vermeiden, sollten die Anbieter eines Produkts, das ein oder mehrere Hochrisiko-KI-Systeme enthält, für die die Anforderungen dieser Verordnung und der in einem Anhang dieser Verordnung aufgeführten Harmonisierungsrechtsvorschriften der Union gelten, in Bezug auf operative Entscheidungen darüber flexibel sein, wie die Konformität eines Produkts, das ein oder mehrere Hochrisiko-KI-Systeme enthält, bestmöglich mit allen geltenden Anforderungen der Harmonisierungsrechtsvorschriften der Union sichergestellt werden kann. 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, wodurch eine mögliche Beschränkung des internationalen Handels so gering wie möglich bleiben sollte.

(47) KI-Systeme könnten nachteilige Auswirkungen auf die Gesundheit und Sicherheit von Personen haben, insbesondere wenn solche Systeme als Sicherheitsbauteile 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.

(48) Das Ausmaß der nachteiligen 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, das Recht auf Nichtdiskriminierung, das Recht auf Bildung, der Verbraucherschutz, die Arbeitnehmerrechte, die Rechte von Menschen mit Behinderungen, die Gleichstellung der Geschlechter, Rechte des geistigen Eigentums, das Recht auf einen wirksamen Rechtsbehelf und ein faires Gerichtsverfahren, das Verteidigungsrecht, die Unschuldsvermutung 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 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 unter anderem in Bezug auf die Gesundheit und Sicherheit von Personen verursachen kann, ebenfalls Rechnung getragen werden.

(49) In Bezug auf Hochrisiko-KI-Systeme, die Sicherheitsbauteile von Produkten oder Systemen oder selbst Produkte oder Systeme sind, die in den Anwendungsbereich der Verordnung (EG) Nr. 300/2008 des Europäischen Parlaments und des Rates ([24]), der Verordnung (EU) Nr. 167/2013 des Europäischen Parlaments und des Rates ([25]), der Verordnung (EU) Nr. 168/2013 des Europäischen Parlaments und des Rates ([26]), der Richtlinie 2014/90/EU des Europäischen Parlaments und des Rates ([27]), der Richtlinie (EU) 2016/797 des Europäischen Parlaments und des Rates ([28]), der Verordnung (EU) 2018/858 des Europäischen Parlaments und des Rates ([29]), der Verordnung (EU) 2018/1139 des

([24]) 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).
([25]) 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).
([26]) 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).
([27]) 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).
([28]) 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).
([29]) 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).

Europäischen Parlaments und des Rates ([30]) und der Verordnung (EU) 2019/2144 des Europäischen Parlaments und des Rates ([31]) 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 delegierten Rechtsakten oder Durchführungsrechtsakten auf der Grundlage der genannten Rechtsakte die in der vorliegenden Verordnung festgelegten verbindlichen Anforderungen an Hochrisiko-KI-Systeme berücksichtigt.

(50) In Bezug auf KI-Systeme, die Sicherheitsbauteile von Produkten oder selbst Produkte sind, die in den Anwendungsbereich bestimmter, im Anhang dieser Verordnung aufgeführter 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 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, In-vitro-Diagnostika, Automobile und Flugzeuge.

(51) Die Einstufung eines KI-Systems als hochriskant gemäß dieser Verordnung sollte nicht zwangsläufig bedeuten, dass von dem Produkt, dessen Sicherheitsbauteil das KI-System ist, oder von dem KI-System als eigenständigem Produkt nach den Kriterien der einschlägigen Harmonisierungsrechtsvorschriften der Union für das betreffende Produkt ein hohes Risiko ausgeht. Dies gilt insbesondere für die Verordnungen (EU) 2017/745 und (EU) 2017/746, wo für Produkte mit mittlerem und hohem Risiko eine Konformitätsbewertung durch Dritte vorgesehen ist.

(52) Bei eigenständigen KI-Systemen, d. h. Hochrisiko-KI-Systemen, bei denen es sich um andere Systeme als Sicherheitsbauteile 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 dieser Verordnung ausdrücklich festgelegt sind. Die Bestimmung dieser Systeme erfolgt nach derselben Methodik und denselben Kriterien, die auch für künftige Änderungen der Liste der Hochrisiko-KI-Systeme vorgesehen sind, zu deren Annahme die Kommission im Wege delegierter Rechtsakte ermächtigt werden sollte, um dem rasanten Tempo der technologischen Entwicklung sowie den möglichen Änderungen bei der Verwendung von KI-Systemen Rechnung zu tragen.

(53) Ferner muss klargestellt werden, dass es bestimmte Fälle geben kann, in denen KI-Systeme für vordefinierte in dieser Verordnung festgelegte Bereiche nicht zu einem bedeutenden Risiko der Beeinträchtigung der in diesen Bereichen geschützten rechtlichen Interessen führen, da sie die Entscheidungsfindung nicht wesentlich beeinflussen oder diesen Interessen nicht erheblich schaden. Für die Zwecke dieser Verordnung sollte ein KI-System, das das Ergebnis der Entscheidungsfindung nicht wesentlich beeinflusst, als ein KI-System verstanden werden, das keine Auswirkungen auf den Inhalt und damit das Ergebnis der Entscheidungsfindung hat, unabhängig davon, ob es sich um menschliche oder automatisierte Entscheidungen handelt. Ein KI-System, das das Ergebnis der Entscheidungsfindung nicht wesentlich beeinflusst, könnte Situationen einschließen, in denen eine oder mehrere der folgenden Bedingungen erfüllt sind. Die erste dieser Bedingungen ist, dass das KI-System dazu bestimmt ist, in einem Verfahren eine eng gefasste Aufgabe zu erfüllen, wie etwa ein KI-System, das unstrukturierte Daten in strukturierte Daten umwandelt, ein KI-System, das eingehende Dokumente in Kategorien einordnet, oder ein KI-System, das zur Erkennung von Duplikaten unter einer großen Zahl von Anwendungen eingesetzt wird. Diese Aufgaben sind so eng gefasst und begrenzt, dass sie nur beschränkte Risiken darstellen, die sich durch die Verwendung eines KI-Systems in einem Kontext, der in einem Anhang dieser Verordnung als Verwendung mit hohem Risiko aufgeführt ist, nicht erhöhen.

([30]) 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).

([31]) 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).

Die zweite Bedingung sollte darin bestehen, dass die von einem KI-System ausgeführte Aufgabe das Ergebnis einer zuvor abgeschlossenen menschlichen Tätigkeit verbessert, die für die Zwecke der in einem Anhang dieser Verordnung aufgeführten Verwendungen mit hohem Risiko relevant sein kann. Unter Berücksichtigung dieser Merkmale wird eine menschliche Tätigkeit durch das KI-System lediglich durch eine zusätzliche Ebene ergänzt und stellt daher ein geringeres Risiko dar. Diese Bedingung würde beispielsweise für KI-Systeme gelten, deren Ziel es ist, die in zuvor verfassten Dokumenten verwendete Sprache zu verbessern, etwa den professionellen Ton, den wissenschaftlichen Sprachstil oder um den Text an einen bestimmten mit einer Marke verbundenen Stil anzupassen. Dritte Bedingung sollte sein, dass mit dem KI-System Entscheidungsmuster oder Abweichungen von früheren Entscheidungsmustern erkannt werden sollen. Das Risiko wäre geringer, da die Verwendung des KI-Systems einer zuvor abgeschlossenen menschlichen Bewertung folgt, die das KI-System ohne angemessene menschliche Überprüfung nicht ersetzen oder beeinflussen soll. Zu solchen KI-Systemen gehören beispielsweise solche, die in Bezug auf ein bestimmtes Benotungsmuster eines Lehrers dazu verwendet werden können, nachträglich zu prüfen, ob der Lehrer möglicherweise von dem Benotungsmuster abgewichen ist, um so auf mögliche Unstimmigkeiten oder Unregelmäßigkeiten aufmerksam zu machen. Die vierte Bedingung sollte darin bestehen, dass das KI-System dazu bestimmt ist, eine Aufgabe auszuführen, die eine Bewertung, die für die Zwecke der in einem Anhang dieser Verordnung aufgeführten KI-Systeme relevant ist, lediglich vorbereitet, wodurch die mögliche Wirkung der Ausgaben des Systems im Hinblick auf das Risiko für die folgende Bewertung sehr gering bleibt. Diese Bedingung umfasst u. a. intelligente Lösungen für die Bearbeitung von Dossiers, wozu verschiedene Funktionen wie Indexierung, Suche, Text- und Sprachverarbeitung oder Verknüpfung von Daten mit anderen Datenquellen gehören, oder KI-Systeme, die für die Übersetzung von Erstdokumenten verwendet werden. In jedem Fall sollten KI-Systeme, die in den in einem Anhang dieser Verordnung aufgeführten Anwendungsfälle mit hohem Risiko verwendet werden, als erhebliche Risiken für die Gesundheit, Sicherheit oder Grundrechte gelten, wenn das KI-System Profiling im Sinne von Artikel 4 Nummer 4 der Verordnung (EU) 2016/679 oder Artikel 3 Nummer 4 der Richtlinie (EU) 2016/680 oder Artikel 3 Nummer 5 der Verordnung (EU) 2018/1725 beinhaltet. Um die Nachvollziehbarkeit und Transparenz zu gewährleisten, sollte ein Anbieter, der der Auffassung ist, dass ein KI-System auf der Grundlage der oben genannten Bedingungen kein hohes Risiko darstellt, eine Dokumentation der Bewertung erstellen, bevor dieses System in Verkehr gebracht oder in Betrieb genommen wird, und die genannte Dokumentation den zuständigen nationalen Behörden auf Anfrage zur Verfügung stellen. Ein solcher Anbieter sollte verpflichtet sein, das KI-System in der gemäß dieser Verordnung eingerichteten EU-Datenbank zu registrieren. Um eine weitere Anleitung für die praktische Umsetzung der Bedingungen zu geben, unter denen die in einem Anhang dieser Verordnung aufgeführten Systeme ausnahmsweise kein hohes Risiko darstellen, sollte die Kommission nach Konsultation des KI-Gremiums Leitlinien bereitstellen, in denen diese praktische Umsetzung detailliert aufgeführt ist und durch eine umfassende Liste praktischer Beispiele für Anwendungsfälle von KI-Systemen, die ein hohes Risiko und Anwendungsfälle, die kein hohes Risiko darstellen, ergänzt wird.

[sn502] Anbieter
[sn202] Kritische Infrastruktur
[sn908] EU-Datenbank

(54) Da biometrische Daten eine besondere Kategorie personenbezogener Daten darstellen, sollten einige kritische Anwendungsfälle biometrischer Systeme als hochriskant eingestuft werden, sofern ihre Verwendung nach den einschlägigen Rechtsvorschriften der Union und den nationalen Rechtsvorschriften zulässig ist. Technische Ungenauigkeiten von KI-Systemen, die für die biometrische Fernidentifizierung natürlicher Personen bestimmt sind, können zu verzerrten Ergebnissen führen und eine diskriminierende Wirkung haben. Das Risiko solcher verzerrter Ergebnisse und solcher diskriminierender Wirkungen ist von besonderer Bedeutung, wenn es um das Alter, die ethnische Herkunft, die Rasse, das Geschlecht oder Behinderungen geht. Biometrische Fernidentifizierungssysteme sollten daher angesichts der von ihnen ausgehenden Risiken als hochriskant eingestuft werden. Diese Einstufung umfasst keine KI-Systeme, die bestimmungsgemäß für die biometrische Verifizierung, wozu die Authentifizierung gehört, verwendet werden sollen, deren einziger Zweck darin besteht, zu bestätigen, dass eine bestimmte natürliche Person die Person ist, für die sie sich ausgibt, sowie zur Bestätigung der Identität einer natürlichen Person zu dem alleinigen Zweck Zugang zu einem Dienst zu erhalten, ein Gerät zu entriegeln oder sicheren Zugang zu Räumlichkeiten zu erhalten. Darüber hinaus sollten KI-Systeme, die bestimmungsgemäß für die biometrische Kategorisierung nach sensiblen Attributen oder Merkmalen, die gemäß Artikel 9 Absatz 1 der Verordnung (EU) 2016/679 auf der Grundlage biometrischer Daten geschützt sind, und sofern sie nicht nach der vorliegenden Verordnung verboten sind, sowie Emotionserkennungssysteme, die nach dieser Verordnung nicht verboten sind, als hochriskant eingestuft werden. Biometrische Systeme, die ausschließlich dazu bestimmt sind, um Maßnahmen zur Cybersicherheit und zum Schutz personenbezogener Daten durchführen zu können, sollten nicht als Hochrisiko-KI-Systeme gelten.

[sn107] Biometrische Kategorisierung
[sn202] Kritische Infrastruktur

(55) Was die Verwaltung und den Betrieb kritischer Infrastruktur anbelangt, so ist es angezeigt, KI-Systeme, die als Sicherheitsbauteile für die Verwaltung und den Betrieb kritischer digitaler Infrastruktur gemäß Nummer 8 des Anhangs der Richtlinie (EU) 2022/2557, des Straßenverkehrs sowie für die Wasser-, Gas-, Wärme- und Stromversorgung verwendet werden sollen, als hochriskant einzustufen, da ihr Ausfall oder ihre Störung in großem Umfang ein Risiko für das Leben und die Gesundheit von Personen darstellen und zu erheblichen Störungen bei der normalen Durchführung sozialer und wirtschaftlicher Tätigkeiten führen kann. Sicherheitsbauteile kritischer Infrastruktur, einschließlich kritischer digitaler Infrastruktur, sind Systeme, die verwendet werden, um die physische Integrität kritischer Infrastruktur oder die Gesundheit und Sicherheit von Personen und Eigentum zu schützen, die aber nicht notwendig sind, damit das System funktioniert. Ausfälle oder Störungen solcher Komponenten können

[sn202] Kritische Infrastruktur

direkt zu Risiken für die physische Integrität kritischer Infrastruktur und somit zu Risiken für die Gesundheit und Sicherheit von Personen und Eigentum führen. Komponenten, die für die ausschließliche Verwendung zu Zwecken der Cybersicherheit vorgesehen sind, sollten nicht als Sicherheitsbauteile gelten. Zu Beispielen von Sicherheitsbauteilen solcher kritischen Infrastruktur zählen etwa Systeme für die Überwachung des Wasserdrucks oder Feuermelder-Kontrollsysteme in Cloud-Computing-Zentren.

(56) Der Einsatz von KI-Systemen in der Bildung ist wichtig, um eine hochwertige digitale allgemeine und berufliche Bildung zu fördern und es allen Lernenden und Lehrkräften zu ermöglichen, die erforderlichen digitalen Fähigkeiten und Kompetenzen, einschließlich Medienkompetenz und kritischem Denken, zu erwerben und auszutauschen, damit sie sich aktiv an Wirtschaft, Gesellschaft und demokratischen Prozessen beteiligen können. Allerdings sollten KI-Systeme, die in der allgemeinen oder beruflichen Bildung eingesetzt werden, um insbesondere den Zugang oder die Zulassung zum Zweck der Zuordnung von Personen zu Bildungs- und Berufsbildungseinrichtungen oder -programmen auf allen Ebenen zu bestimmen, die Lernergebnisse von Personen zu beurteilen, das angemessene Bildungsniveau einer Person zu bewerten und das Niveau der Bildung und Ausbildung, das die Person erhält oder zu dem sie Zugang erhält, wesentlich zu beeinflussen und verbotenes Verhalten von Schülern während Prüfungen zu überwachen und zu erkennen als hochriskante KI-Systeme eingestuft werden, da sie über den Verlauf der Bildung und des Berufslebens einer Person entscheiden und daher ihre Fähigkeit beeinträchtigen können, ihren Lebensunterhalt zu sichern. Bei unsachgemäßer Konzeption und Verwendung können solche Systeme sehr intrusiv sein und das Recht auf allgemeine und berufliche Bildung sowie das Recht auf Nichtdiskriminierung verletzen und historische Diskriminierungsmuster fortschreiben, beispielsweise gegenüber Frauen, bestimmten Altersgruppen und Menschen mit Behinderungen oder Personen mit einer bestimmten rassischen oder ethnischen Herkunft oder sexuellen Ausrichtung.

(57) 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 die Bedingungen des Arbeitsverhältnisses sowie die Beförderung und die Beendigung von Arbeitsvertragsverhältnissen, für die Zuweisung von Arbeitsaufgaben auf der Grundlage von individuellem Verhalten, persönlichen Eigenschaften oder Merkmalen sowie für die Überwachung oder Bewertung von Personen in Arbeitsvertragsverhältnissen sollten ebenfalls als hochriskant eingestuft werden, da diese Systeme die künftigen Karriereaussichten und die Lebensgrundlagen dieser Personen und die Arbeitnehmerrechte spürbar beeinflussen können. Einschlägige Arbeitsvertragsverhältnisse sollten in sinnvoller Weise Beschäftigte und Personen erfassen, die Dienstleistungen über Plattformen erbringen, auf die im Arbeitsprogramm der Kommission für 2021 Bezug genommen wird. Solche Systeme können während des gesamten Einstellungsverfahrens und bei der Bewertung, Beförderung oder Weiterbeschäftigung 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 solcher Personen können auch deren Grundrechte auf Datenschutz und Privatsphäre untergraben.

(58) 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 Menschen uneingeschränkt an der Gesellschaft teilhaben oder ihren Lebensstandard verbessern können. Insbesondere natürliche Personen, die grundlegende staatliche Unterstützungsleistungen und -dienste von Behörden beantragen oder erhalten, wie etwa Gesundheitsdienste, Leistungen der sozialen Sicherheit, soziale Dienste, die Schutz in Fällen wie Mutterschaft, Krankheit, Arbeitsunfall, Pflegebedürftigkeit oder Alter und Arbeitsplatzverlust sowie Sozialhilfe und Wohngeld bieten, 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 gewährt, 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 Lebensgrundlage von Personen haben und ihre Grundrechte wie etwa das Recht auf sozialen Schutz, Nichtdiskriminierung, Menschenwürde oder einen wirksamen Rechtsbehelf verletzen und sollten daher als hochriskant eingestuft werden. Dennoch sollte diese Verordnung die Entwicklung und Verwendung 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. Darüber hinaus sollten KI-Systeme, die zur Bewertung der Bonität oder Kreditwürdigkeit natürlicher Personen verwendet werden, als Hochrisiko-KI-Systeme eingestuft werden, da sie den Zugang dieser Personen zu Finanzmitteln oder wesentlichen Dienstleistungen wie etwa Wohnraum, Elektrizität und Telekommunikationsdienstleistungen bestimmen. KI-Systeme, die für diese Zwecke eingesetzt werden, können zur Diskriminierung von Personen oder Gruppen führen und historische Diskriminierungsmuster, wie etwa aufgrund der rassischen oder ethnischen Herkunft, des Geschlechts, einer Behinderung, des Alters oder der sexuellen Ausrichtung, fortschreiben oder neue Formen von Diskriminierung mit sich bringen. Allerdings sollten KI-Systeme, die nach Unionsrecht zur Aufdeckung von Betrug beim Angebot von Finanzdienstleistungen oder für Aufsichtszwecke zur Berechnung der Eigenkapitalanforderungen von Kreditinstituten und Versicherungsunternehmen vorgesehen sind, nicht als Hochrisiko-Systeme gemäß dieser Verordnung angesehen werden. Darüber hinaus

können KI-Systeme, die für die Risikobewertung und Preisbildung in Bezug auf natürliche Personen im Fall von Kranken- und Lebensversicherungen eingesetzt werden, auch erhebliche Auswirkungen auf die Existenzgrundlage der Menschen haben und bei nicht ordnungsgemäßer Konzeption, Entwicklung und Verwendung schwerwiegende Konsequenzen für das Leben und die Gesundheit von Menschen nach sich ziehen, einschließlich finanzieller Ausgrenzung und Diskriminierung. Schließlich sollten KI-Systeme, die bei der Bewertung und Einstufung von Notrufen durch natürliche Personen oder der Entsendung oder der Priorisierung der Entsendung von Not- und Rettungsdiensten wie Polizei, Feuerwehr und medizinischer Nothilfe sowie für die Triage von Patienten bei der Notfallversorgung 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.

(59) In Anbetracht der Rolle und Zuständigkeit von Strafverfolgungsbehörden sind deren Maßnahmen im Zusammenhang mit bestimmten Verwendungen von KI-Systemen durch ein erhebliches Machtungleichgewicht gekennzeichnet und können zur Überwachung, zur Festnahme oder zum Entzug der Freiheit einer natürlichen Person sowie zu anderen nachteiligen Auswirkungen auf die in der Charta verankerten Grundrechte führen. Insbesondere wenn das KI-System nicht mit hochwertigen Daten trainiert wird, die Anforderungen an seine Leistung, Genauigkeit oder Robustheit nicht erfüllt werden oder das System nicht ordnungsgemäß konzipiert und getestet wird, bevor es in Verkehr gebracht oder in anderer Weise in Betrieb genommen wird, kann es Personen in diskriminierender oder anderweitig falscher oder ungerechter Weise ausgrenzen. Darüber hinaus könnte die Ausübung wichtiger verfahrensrechtlicher Grundrechte wie etwa des Rechts auf einen wirksamen Rechtsbehelf und ein unparteiisches Gericht sowie das Verteidigungsrecht und die Unschuldsvermutung behindert werden, insbesondere wenn solche KI-Systeme nicht hinreichend transparent, erklärbar und dokumentiert sind. Daher ist es angezeigt, eine Reihe von KI-Systemen — sofern deren Einsatz nach einschlägigem Unions- oder nationalem Recht zugelassen ist —, 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 Tätigkeiten und der damit verbundenen Risiken sollten diese Hochrisiko-KI-Systeme insbesondere KI-Systeme umfassen, die von Strafverfolgungsbehörden oder in ihrem Auftrag oder von Organen, Einrichtungen und sonstigen Stellen der Union zur Unterstützung von Strafverfolgungsbehörden für folgende Zwecke eingesetzt werden: zur Bewertung des Risikos, dass eine natürliche Person Opfer von Straftaten wird, wie Lügendetektoren und ähnliche Instrumente, zur Bewertung der Zuverlässigkeit von Beweismitteln im Rahmen der Ermittlung oder Verfolgung von Straftaten und — soweit nach dieser Verordnung nicht untersagt — zur Bewertung des Risikos, dass eine natürliche Person eine Straftat begeht oder erneut begeht, nicht nur auf der Grundlage der Erstellung von Profilen natürlicher Personen oder zur Bewertung von Persönlichkeitsmerkmalen und Eigenschaften oder vergangenem kriminellen Verhalten von natürlichen Personen oder Gruppen, zur Erstellung von Profilen während der Aufdeckung, Untersuchung oder strafrechtlichen Verfolgung einer Straftat. KI-Systeme, die speziell für Verwaltungsverfahren in Steuer- und Zollbehörden sowie in Zentralstellen für Geldwäsche-Verdachtsanzeigen, die Verwaltungsaufgaben zur Analyse von Informationen gemäß dem Unionsrecht zur Bekämpfung der Geldwäsche durchführen, bestimmt sind, sollten nicht als Hochrisiko-KI-Systeme eingestuft werden, die von Strafverfolgungsbehörden zum Zweck der Verhütung, Aufdeckung, Untersuchung und strafrechtlichen Verfolgung von Straftaten eingesetzt werden. Der Einsatz von KI-Instrumenten durch Strafverfolgungsbehörden und anderen relevanten Behörden sollte nicht zu einem Faktor der Ungleichheit oder Ausgrenzung werden. Die Auswirkungen des Einsatzes von KI-Instrumenten auf die Verteidigungsrechte von Verdächtigen sollten nicht außer Acht gelassen werden, insbesondere nicht die Schwierigkeit, aussagekräftige Informationen über die Funktionsweise solcher Systeme zu erhalten, und die daraus resultierende Schwierigkeit einer gerichtlichen Anfechtung ihrer Ergebnisse, insbesondere durch natürliche Personen, gegen die ermittelt wird.

(60) KI-Systeme, die in den Bereichen Migration, Asyl und Grenzkontrolle eingesetzt werden, betreffen Personen, 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, Schutz des Privatlebens und personenbezogener Daten, internationalen Schutz und gute Verwaltung, zu gewährleisten. Daher ist es angezeigt, KI-Systeme — sofern deren Einsatz nach einschlägigem Unions- oder nationalem Recht zugelassen ist — als hochriskant einzustufen, die von den zuständigen mit Aufgaben in den Bereichen Migration, Asyl und Grenzkontrolle betrauten Behörden oder in deren Auftrag oder von Organen, Einrichtungen oder sonstigen Stellen der Union für Folgendes eingesetzt werden: als Lügendetektoren und ähnliche Instrumente; 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 — einschließlich der damit zusammenhängenden Bewertung der Zuverlässigkeit von Beweismitteln — von Asyl- und Visumanträgen sowie Aufenthaltstiteln und damit verbundenen Beschwerden im Hinblick darauf, die Berechtigung der den Antrag stellenden natürlichen Personen festzustellen; zum Zweck der Aufdeckung, Anerkennung oder Identifizierung natürlicher Personen im Zusammenhang mit Migration, Asyl und Grenzkontrolle, mit Ausnahme der Überprüfung von Reisedokumenten. KI-Systeme im Bereich Migration, Asyl und Grenzkontrolle, die unter diese Verordnung fallen, sollten den einschlägigen Verfahrensvorschriften der Verordnung (EG) Nr. 810/2009 des Europäischen

Parlaments und des Rates [32], der Richtlinie 2013/32/EU des Europäischen Parlaments und des Rates [33] und anderem einschlägigen Unionsrecht entsprechen. Der Einsatz von KI-Systemen in den Bereichen Migration, Asyl und Grenzkontrolle sollte unter keinen Umständen von den Mitgliedstaaten oder Organen, Einrichtungen oder sonstigen Stellen der Union als Mittel zur Umgehung ihrer internationalen Verpflichtungen aus dem am 28. Juli 1951 in Genf unterzeichneten Abkommen der Vereinten Nationen über die Rechtsstellung der Flüchtlinge in der durch das Protokoll vom 31. Januar 1967 geänderten Fassung genutzt werden. Die Systeme sollten auch nicht dazu genutzt werden, in irgendeiner Weise gegen den Grundsatz der Nichtzurückweisung zu verstoßen oder sichere und wirksame legale Wege in das Gebiet der Union, einschließlich des Rechts auf internationalen Schutz, zu verweigern.

(61) 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 von einer Justizbehörde oder in ihrem Auftrag dazu genutzt werden sollen, Justizbehörden bei der Ermittlung und Auslegung von Sachverhalten und Rechtsvorschriften und bei der Anwendung des Rechts auf konkrete Sachverhalte zu unterstützen, als hochriskant eingestuft werden. KI-Systeme, die von Stellen für die alternative Streitbeilegung für diese Zwecke genutzt werden sollen, sollten ebenfalls als hochriskant gelten, wenn die Ergebnisse der alternativen Streitbeilegung Rechtswirkung für die Parteien entfalten. Der Einsatz von KI-Instrumenten kann die Entscheidungsgewalt von Richtern oder die Unabhängigkeit der Justiz unterstützen, sollte sie aber nicht ersetzen; die endgültige Entscheidungsfindung muss eine von Menschen gesteuerte Tätigkeit bleiben. Die Einstufung von KI-Systemen als hochriskant sollte sich jedoch nicht auf KI-Systeme erstrecken, die für rein begleitende Verwaltungstätigkeiten bestimmt sind, die die tatsächliche Rechtspflege in Einzelfällen nicht beeinträchtigen, wie etwa die Anonymisierung oder Pseudonymisierung gerichtlicher Urteile, Dokumente oder Daten, die Kommunikation zwischen dem Personal oder Verwaltungsaufgaben.

(62) Unbeschadet der Vorschriften der Verordnung (EU) 2024/900 des Europäischen Parlaments und des Rates [34] und um den Risiken eines unzulässigen externen Eingriffs in das in Artikel 39 der Charta verankerte Wahlrecht und nachteiligen Auswirkungen auf die Demokratie und die Rechtsstaatlichkeit zu begegnen, sollten KI-Systeme, die verwendet werden sollen, um das Ergebnis einer Wahl oder eines Referendums oder das Wahlverhalten natürlicher Personen bei der Ausübung ihres Wahlrechts in einer Wahl oder in Referenden zu beeinflussen, als Hochrisiko-KI-Systeme eingestuft werden, mit Ausnahme von KI-Systemen, deren Ausgaben natürliche Personen nicht direkt ausgesetzt sind, wie Instrumente zur Organisation, Optimierung und Strukturierung politischer Kampagnen in administrativer und logistischer Hinsicht.

(63) Die Tatsache, dass ein KI-System gemäß dieser Verordnung als ein Hochrisiko-KI-System eingestuft wird, sollte nicht dahin gehend 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 Zustands natürlicher Personen. Eine solche Verwendung sollte weiterhin ausschließlich gemäß 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, gegebenenfalls einschließlich besonderer Kategorien personenbezogener Daten, bildet, es sei denn, in dieser Verordnung ist ausdrücklich etwas anderes vorgesehen.

[sn301] Risikomanagementsystem

[sn502] Anbieter

(64) Um die von in Verkehr gebrachten oder in Betrieb genommenen Hochrisiko-KI-Systemen ausgehenden Risiken zu mindern und ein hohes Maß an Vertrauenswürdigkeit zu gewährleisten, sollten für Hochrisiko-KI-Systeme bestimmte verbindliche Anforderungen gelten, wobei der Zweckbestimmung und dem Nutzungskontext des KI-Systems sowie dem vom Anbieter einzurichtenden Risikomanagementsystem Rechnung zu tragen ist. Die von den Anbietern zur Erfüllung der verbindlichen Anforderungen dieser Verordnung ergriffenen Maßnahmen sollten dem allgemein anerkannten Stand der KI Rechnung tragen, verhältnismäßig und wirksam sein, um die Ziele dieser Verordnung zu erreichen. Auf der Grundlage des neuen Rechtsrahmens, wie in der Bekanntmachung der Kommission „Leitfaden für die Umsetzung der Produktvorschriften der EU 2022 (Blue Guide)“ dargelegt, gilt als allgemeine Regel, dass mehr als ein Rechtsakt der Harmonisierungsrechtsvorschriften der Union auf ein Produkt anwendbar sein können, da die Bereitstellung oder Inbetriebnahme nur erfolgen kann, wenn das Produkt allen geltenden Harmonisierungsrechtsvorschriften der Union entspricht. Die Gefahren von KI-Systemen, die unter die Anforderungen dieser Verordnung fallen, decken andere Aspekte ab als die bestehenden Harmonisierungsrechtsvorschriften der Union, weshalb die Anforderungen dieser Verordnung das bestehende Regelwerk der Harmonisierungsrechtsvorschriften der Union ergänzen würden. So bergen etwa Maschinen oder Medizinprodukte mit einer KI-Komponente möglicherweise Risiken, die von den grundlegenden Gesundheits- und Sicherheitsan-

[32] 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).

[33] 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).

[34] Verordnung (EU) 2024/900 des Europäischen Parlaments und des Rates vom 13. März 2024 über die Transparenz und das Targeting politischer Werbung (ABl. L, 2024/900, 20.3.2024, ELI: http://data.europa.eu/eli/reg/2024/900/oj).

[sn502] Anbieter

[sn301] Risikomanagementsystem

[se301] informiert

forderungen der einschlägigen harmonisierten Rechtsvorschriften der Union nicht erfasst werden, da diese sektoralen Rechtsvorschriften keine spezifischen KI-Risiken behandeln. Dies erfordert die gleichzeitige und ergänzende Anwendung mehrerer Rechtsakte. Um Kohärenz zu gewährleisten und unnötigen Verwaltungsaufwand sowie unnötige Kosten zu vermeiden, sollten die Anbieter eines Produkts, das ein oder mehrere Hochrisiko-KI-Systeme enthält, für die die Anforderungen dieser Verordnung und der in einem Anhang dieser Verordnung aufgeführten und auf dem neuen Rechtsrahmen beruhenden Harmonisierungsvorschriften der Union gelten, in Bezug auf betriebliche Entscheidungen darüber flexibel sein, wie die Konformität eines Produkts, das ein oder mehrere Hochrisiko-KI-Systeme enthält, bestmöglich mit allen geltenden Anforderungen dieser harmonisierten Rechtsvorschriften der Union sichergestellt werden kann. Diese Flexibilität könnte beispielsweise bedeuten, dass der Anbieter beschließt, einen Teil der gemäß dieser Verordnung erforderlichen Test- und Berichterstattungsverfahren, Informationen und Unterlagen in bereits bestehende Dokumentationen und Verfahren zu integrieren, die nach den auf dem neuen Rechtsrahmen beruhenden und in einem Anhang dieser Verordnung aufgeführten geltenden Harmonisierungsrechtsvorschriften der Union erforderlich sind. Dies sollte in keiner Weise die Verpflichtung des Anbieters untergraben, alle geltenden Anforderungen zu erfüllen.

(65) Das Risikomanagementsystem sollte in einem kontinuierlichen iterativen Prozess bestehen, der während des gesamten Lebenszyklus eines Hochrisiko-KI-Systems geplant und durchgeführt wird. Ziel dieses Prozesses sollte es ein, die einschlägigen Risiken von KI-Systemen für Gesundheit, Sicherheit und Grundrechte zu ermitteln und zu mindern. Das Risikomanagementsystem sollte regelmäßig überprüft und aktualisiert werden, um seine dauerhafte Wirksamkeit sowie die Begründetheit und Dokumentierung aller gemäß dieser Verordnung getroffenen wesentlichen Entscheidungen und Maßnahmen zu gewährleisten. Mit diesem Prozess sollte sichergestellt werden, dass der Anbieter Risiken oder negative Auswirkungen ermittelt und Minderungsmaßnahmen ergreift in Bezug auf die bekannten und vernünftigerweise vorhersehbaren Risiken von KI-Systemen für die Gesundheit, die Sicherheit und die Grundrechte angesichts ihrer Zweckbestimmung und vernünftigerweise vorhersehbaren Fehlanwendung, einschließlich der möglichen Risiken, die sich aus der Interaktion zwischen dem KI-System und der Umgebung, in der es betrieben wird, ergeben könnten. Im Rahmen des Risikomanagementsystems sollten die vor dem Hintergrund des Stands der KI am besten geeigneten Risikomanagementmaßnahmen ergriffen werden. Bei der Ermittlung der am besten geeigneten Risikomanagementmaßnahmen sollte der Anbieter die getroffenen Entscheidungen dokumentieren und erläutern und gegebenenfalls Sachverständige und externe Interessenträger hinzuziehen. Bei der Ermittlung der vernünftigerweise vorhersehbaren Fehlanwendung von Hochrisiko-KI-Systemen sollte der Anbieter die Verwendungen von KI-Systemen erfassen, die zwar nicht unmittelbar der Zweckbestimmung entsprechen und in der Betriebsanleitung vorgesehen sind, jedoch nach vernünftigem Ermessen davon auszugehen ist, dass sie sich aus einem leicht absehbaren menschlichen Verhalten im Zusammenhang mit den spezifischen Merkmalen und der Verwendung eines bestimmten KI-Systems ergeben. Alle bekannten oder vorhersehbaren Umstände bezüglich der Verwendung des Hochrisiko-KI-Systems im Einklang mit seiner Zweckbestimmung oder einer vernünftigerweise vorhersehbaren Fehlanwendung, die zu Risiken für die Gesundheit und Sicherheit oder die Grundrechte führen können, sollten vom Anbieter in der Betriebsanleitung aufgeführt werden. Damit soll sichergestellt werden, dass der Betreiber diese Umstände bei der Nutzung des Hochrisiko-KI-Systems kennt und berücksichtigt. Die Ermittlung und Umsetzung von Risikominderungsmaßnahmen in Bezug auf vorhersehbare Fehlanwendungen im Rahmen dieser Verordnung sollte keine spezifische zusätzliche Schulung für das Hochrisiko-KI-System durch den Anbieter erfordern, um gegen vorhersehbare Fehlanwendungen vorzugehen. Die Anbieter sind jedoch gehalten, solche zusätzlichen Schulungsmaßnahmen in Erwägung zu ziehen, um einer vernünftigerweise vorhersehbare Fehlanwendung entgegenzuwirken, soweit dies erforderlich und angemessen ist.

[se301] informiert

[sn503] Betreiber

[sn303] Technische Dokumentation

[sn306] Menschliche Aufsicht

(66) Die Anforderungen sollten für Hochrisiko-KI-Systeme im Hinblick auf das Risikomanagement, die Qualität und Relevanz der verwendeten Datensätze, die technische Dokumentation und die Aufzeichnungspflichten, die Transparenz und die Bereitstellung von Informationen für die Betreiber, die menschliche Aufsicht sowie die Robustheit, Genauigkeit und Sicherheit gelten. Diese Anforderungen sind erforderlich, um die Risiken für Gesundheit, Sicherheit und Grundrechte wirksam zu mindern. Nachdem nach vernünftigem Ermessen keine anderen weniger handelsbeschränkenden Maßnahmen zur Verfügung stehen, stellen sie keine ungerechtfertigten Handelsbeschränkungen dar.

(67) Hochwertige Daten und der Zugang dazu spielen eine zentrale Rolle bei der Bereitstellung von Strukturen und für die Sicherstellung der Leistung vieler KI-Systeme, insbesondere wenn Techniken eingesetzt werden, bei denen Modelle mit Daten trainiert werden, um sicherzustellen, dass das Hochrisiko-KI-System bestimmungsgemäß und sicher funktioniert und nicht zur Ursache für Diskriminierung wird, die nach dem Unionsrecht verboten ist. Hochwertige Trainings-, Validierungs- und Testdatensätze erfordern geeignete Daten-Governance- und Datenverwaltungsverfahren. Die Trainings-, Validierungs- und Testdatensätze, einschließlich der Kennzeichnungen, sollten im Hinblick auf die Zweckbestimmung des Systems relevant, hinreichend repräsentativ und so weit wie möglich fehlerfrei und vollständig sein. Um die Einhaltung des Datenschutzrechts der Union, wie der Verordnung (EU) 2016/679, zu erleichtern, sollten Daten-Governance- und Datenverwaltungsverfahren bei personenbezogenen Daten Transparenz in Bezug auf den ursprünglichen Zweck der Datenerhebung umfassen. Die Datensätze sollten auch die geeigneten statistischen Merkmale haben, auch bezüglich der Personen oder Personengruppen, auf die das Hochrisiko-KI-System bestimmungsgemäß angewandt werden soll, unter besonderer Berücksichtigung der Minderung möglicher Verzerrungen in den Datensätzen, die die Gesundheit und Sicherheit von Personen beeinträchtigen, sich negativ auf die Grundrechte auswirken oder zu einer nach dem Unionsrecht verbotenen Diskriminierung führen könnten, insbesondere wenn die Datenausgaben die Eingaben für künftige Operationen

[se002] muss einhalten

[se102] muss einhalten

beeinflussen (Rückkopplungsschleifen). Verzerrungen können zum Beispiel — insbesondere bei Verwendung historischer Daten — den zugrunde liegenden Datensätzen innewohnen oder bei der Implementierung der Systeme in der realen Welt generiert werden. Die von einem KI-System ausgegebenen Ergebnisse könnten durch solche inhärenten Verzerrungen beeinflusst werden, die tendenziell allmählich zunehmen und dadurch bestehende Diskriminierungen fortschreiben und verstärken, insbesondere in Bezug auf Personen, die bestimmten schutzbedürftigen Gruppen wie aufgrund von Rassismus benachteiligten oder ethnischen Gruppen angehören. Die Anforderung, dass die Datensätze so weit wie möglich 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. Insbesondere sollten die Datensätze, soweit dies für die Zweckbestimmung erforderlich ist, den Eigenschaften, Merkmalen oder Elementen entsprechen, die für die besonderen geografischen, kontextuellen, verhaltensbezogenen oder funktionalen Rahmenbedingungen, unter denen das Hochrisiko-KI-System bestimmungsgemäß verwendet werden soll, typisch sind. Die Anforderungen an die Daten-Governance können durch die Inanspruchnahme Dritter erfüllt werden, die zertifizierte Compliance-Dienste anbieten, einschließlich der Überprüfung der Daten-Governance, der Datensatzintegrität und der Datenschulungs-, Validierungs- und Testverfahren, sofern die Einhaltung der Datenanforderungen dieser Verordnung gewährleistet ist.

[sn502] Anbieter

(68) Für die Entwicklung und Bewertung von Hochrisiko-KI-Systemen sollten bestimmte Akteure wie etwa Anbieter, notifizierte Stellen und andere einschlägige Einrichtungen wie etwa Europäische Digitale Innovationszentren, Test- und Versuchseinrichtungen und Forscher in der Lage sein, in den Tätigkeitsbereichen, in denen diese Akteure tätig sind und 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.

(69) Das Recht auf Privatsphäre und den Schutz personenbezogener Daten muss während des gesamten Lebenszyklus des KI-Systems sichergestellt sein. In dieser Hinsicht gelten die Grundsätze der Datenminimierung und des Datenschutzes durch Technikgestaltung und Voreinstellungen, wie sie im Datenschutzrecht der Union festgelegt sind, wenn personenbezogene Daten verarbeitet werden. Unbeschadet der in dieser Verordnung festgelegten Anforderungen an die Daten-Governance können zu den Maßnahmen, mit denen die Anbieter die Einhaltung dieser Grundsätze sicherstellen, nicht nur Anonymisierung und Verschlüsselung gehören, sondern auch der Einsatz von Technik, die es ermöglicht, Algorithmen direkt am Ort der Datenerzeugung einzusetzen und KI-Systeme zu trainieren, ohne dass Daten zwischen Parteien übertragen oder die Rohdaten oder strukturierten Daten selbst kopiert werden.

(70) Um das Recht anderer auf Schutz vor Diskriminierung, die sich aus Verzerrungen in KI-Systemen ergeben könnte, zu wahren, sollten die Anbieter ausnahmsweise und in dem unbedingt erforderlichen Ausmaß, um die Erkennung und Korrektur von Verzerrungen im Zusammenhang mit Hochrisiko-KI-Systemen sicherzustellen, vorbehaltlich angemessener Vorkehrungen für den Schutz der Grundrechte und Grundfreiheiten natürlicher Personen und nach Anwendung aller in dieser Verordnung festgelegten geltenden Bedingungen zusätzlich zu den in den Verordnungen (EU) 2016/679 und (EU) 2018/1725 sowie der Richtlinie (EU) 2016/680 festgelegten Bedingungen besondere Kategorien personenbezogener Daten als Angelegenheit von erheblichem öffentlichen Interesse im Sinne des Artikels 9 Absatz 2 Buchstabe g der Verordnung (EU) 2016/679 und des Artikels 10 Absatz 2 Buchstabe g der Verordnung (EU) 2018/1725 verarbeiten können.

[sn303] Technische Dokumentation

[sn304] Protokollierung

(71) Umfassende Informationen darüber, wie Hochrisiko-KI-Systeme entwickelt wurden und wie sie während ihrer gesamten Lebensdauer funktionieren, sind unerlässlich, um die Nachvollziehbarkeit dieser Systeme, die Überprüfung der Einhaltung der Anforderungen dieser Verordnung sowie die Beobachtung ihres Betriebs und ihre Beobachtung nach dem Inverkehrbringen zu ermöglichen. 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 und die Beobachtung nach dem Inverkehrbringen zu erleichtern. Diese Informationen sollten die allgemeinen Merkmale, Fähigkeiten und Grenzen des Systems, die verwendeten Algorithmen, Daten und Trainings-, Test- und Validierungsverfahren sowie die Dokumentation des einschlägigen Risikomanagementsystems umfassen und in klarer und umfassender Form abgefasst sein. Die technische Dokumentation sollte während der gesamten Lebensdauer des KI-Systems angemessen auf dem neuesten Stand gehalten werden. Darüber hinaus sollten die Hochrisiko-KI-Systeme technisch die automatische Aufzeichnung von Ereignissen mittels Protokollierung während der Lebensdauer des Systems ermöglichen.

[sn505] Konformitätsbewertung

[sn503] Betreiber

[sn305] Transparenz

(72) Um Bedenken hinsichtlich der Undurchsichtigkeit und Komplexität bestimmter KI-Systeme auszuräumen und die Betreiber bei der Erfüllung ihrer Pflichten gemäß dieser Verordnung zu unterstützen, sollte für Hochrisiko-KI-Systeme Transparenz vorgeschrieben werden, bevor sie in Verkehr gebracht oder in Betrieb genommen werden. Hochrisiko-KI-Systeme sollten so gestaltet sein, dass die Betreiber in der Lage sind, zu verstehen, wie das KI-System funktioniert, seine Funktionalität zu bewerten und seine Stärken und Grenzen zu erfassen. Hochrisiko-KI-Systemen sollten angemessene Informationen in Form von Betriebsanleitungen beigefügt sein. Zu diesen Informationen sollten die Merkmale, Fähigkeiten und Leistungsbeschränkungen des KI-Systems gehören. Diese würden Informationen über mögliche bekannte und vorhersehbare Umstände im Zusammenhang mit der Nutzung des Hochrisiko-KI-Systems, einschließlich Handlungen des Betreibers, die das Verhalten und die Leistung des Systems beeinflussen können, unter denen das KI-System zu Risiken in Bezug auf die Gesundheit, die Sicherheit und die Grundrechte führen kann, über die Änderungen, die vom Anbieter vorab festgelegt und auf Konformität geprüft wurden, und über die einschlägigen Maßnahmen der menschlichen Aufsicht, einschließlich der Maßnahmen, um den Betreibern die Interpretation der Ausgaben von KI-Systemen zu erleichtern, umfassen. Transparenz, einschließlich der begleitenden Betriebsanleitungen, sollte den Betreibern bei der Nutzung des Systems helfen und ihre fundierte Entscheidungsfindung unterstützen. Unter anderem sollten Betreiber besser in der Lage sein, das richtige System auszuwählen, das sie angesichts der für sie geltenden Pflichten verwenden wollen, über die beabsichtigten und ausgeschlossenen Verwendungszwecke informiert sein und das KI-System korrekt und angemessen verwenden. Um die Lesbarkeit und Zugänglichkeit der in der Betriebsanleitung enthaltenen Informationen zu verbessern, sollten diese gegebenenfalls anschauliche Beispiele enthalten, zum Beispiel zu den Beschränkungen sowie zu den beabsichtigten und ausgeschlossenen Verwendungen des KI-Systems. Die Anbieter sollten dafür sorgen, dass in der gesamten Dokumentation, einschließlich der Betriebsanleitungen, aussagekräftige, umfassende, zugängliche und verständliche Informationen enthalten sind, wobei die Bedürfnisse und vorhersehbaren Kenntnisse der Zielbetreiber zu berücksichtigen sind. Die Betriebsanleitungen sollten in einer vom betreffenden Mitgliedstaat festgelegten Sprache zur Verfügung gestellt werden, die von den Zielbetreibern leicht verstanden werden kann.

[sn502] Anbieter

[sn306] Menschliche Aufsicht

(73) Hochrisiko-KI-Systeme sollten so gestaltet und entwickelt werden, dass natürliche Personen ihre Funktionsweise überwachen und sicherstellen können, dass sie bestimmungsgemäß verwendet werden und dass ihre Auswirkungen während des Lebenszyklus des Systems berücksichtigt werden. 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. Es ist außerdem unerlässlich, gegebenenfalls dafür zu sorgen, dass in Hochrisiko-KI-Systemen Mechanismen enthalten sind, um eine natürliche Person, der die menschliche Aufsicht übertragen wurde, zu beraten und zu informieren, damit sie fundierte Entscheidungen darüber trifft, ob, wann und wie einzugreifen ist, um negative Folgen oder Risiken zu vermeiden, oder das System anzuhalten, wenn es nicht wie beabsichtigt funktioniert. Angesichts der bedeutenden Konsequenzen für Personen im Falle eines falschen Treffers durch bestimmte biometrische Identifizierungssysteme ist es angezeigt, für diese Systeme eine verstärkte Anforderung im Hinblick auf die menschliche Aufsicht vorzusehen, sodass der Betreiber 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 und die Person umfassen, die das System bedient 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. Angesichts der Besonderheiten der Bereiche Strafverfolgung, Migration, Grenzkontrolle und Asyl sollte diese Anforderung nicht gelten, wenn die Geltung dieser Anforderung nach Unionsrecht oder nationalem Recht unverhältnismäßig ist.

[sn206] Strafverfolgung

(74) Hochrisiko-KI-Systeme sollten während ihres gesamten Lebenszyklus beständig funktionieren und ein angemessenes Maß an Genauigkeit, Robustheit und Cybersicherheit angesichts ihrer Zweckbestimmung und entsprechend dem allgemein anerkannten Stand der Technik aufweisen. Die Kommission sowie einschlägige Interessenträger und Organisationen sind aufgefordert, der Minderung der Risiken und negativen Auswirkungen des KI-Systems gebührend Rechnung zu tragen. Das erwartete Leistungskennzahlenniveau sollte in der beigefügten Betriebsanleitung angegeben werden. Die Anbieter werden nachdrücklich aufgefordert, diese Informationen den Betreibern in klarer und leicht verständlicher Weise ohne Missverständnisse oder irreführende Aussagen zu übermitteln. Die Rechtsvorschriften der Union zum gesetzlichen Messwesen, einschließlich der Richtlinien 2014/31/EU ([35]) und 2014/32/EU des Europäischen Parlaments und des Rates ([36]), zielt darauf ab, die Genauigkeit von Messungen sicherzustellen und die Transparenz und Fairness im Geschäftsverkehr zu fördern. In diesem Zusammenhang sollte die Kommission in Zusammenarbeit mit einschlägigen Interessenträgern und Organisationen, wie Metrologie- und Benchmarking-Behörden, gegebenenfalls die Entwicklung von Benchmarks und Messmethoden für KI-Systeme fördern. Dabei sollte die Kommission internationale Partner, die an Metrologie und einschlägigen Messindikatoren für KI arbeiten, beachten und mit ihnen zusammenarbeiten.

([35]) Richtlinie 2014/31/EU des Europäischen Parlaments und des Rates vom 26. Februar 2014 zur Angleichung der Rechtsvorschriften der Mitgliedstaaten betreffend die Bereitstellung nichtselbsttätiger Waagen auf dem Markt (ABl. L 96 vom 29.3.2014, S. 107).

([36]) Richtlinie 2014/32/EU des Europäischen Parlaments und des Rates vom 26. Februar 2014 zur Harmonisierung der Rechtsvorschriften der Mitgliedstaaten über die Bereitstellung von Messgeräten auf dem Markt (ABl. L 96 vom 29.3.2014, S. 149).

(75) 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). Daher sollten technische und organisatorische Maßnahmen ergriffen werden, um die Robustheit von Hochrisiko-KI-Systemen sicherzustellen, indem beispielsweise geeignete technische Lösungen konzipiert und entwickelt werden, um schädliches oder anderweitig unerwünschtes Verhalten zu verhindern oder zu minimieren. Zu diesen technischen Lösungen können beispielsweise Mechanismen gehören, die es dem System ermöglichen, seinen Betrieb bei bestimmten Anomalien oder beim Betrieb außerhalb bestimmter vorab festgelegter Grenzen 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 Ausgaben hervorbringt.

[sn502] Anbieter

(76) 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 zu verändern oder ihre Sicherheitsmerkmale zu beeinträchtigen. Cyberangriffe auf KI-Systeme können KI-spezifische Ressourcen wie Trainingsdatensätze (z. B. Datenvergiftung) oder trainierte Modelle (z. B. feindliche Angriffe oder Inferenzangriffe auf Mitgliederdaten) 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, etwa Sicherheitskontrollen, ergreifen, wobei gegebenenfalls auch die zugrunde liegende IKT-Infrastruktur zu berücksichtigen ist.

(77) Unbeschadet der in dieser Verordnung festgelegten Anforderungen an Robustheit und Genauigkeit können Hochrisiko-AI-Systeme, die in den Geltungsbereich einer Verordnung des Europäischen Parlaments und des Rates über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen gemäß der genannten Verordnung fallen, die Erfüllung der Cybersicherheitsanforderungen der vorliegenden Verordnung nachweisen, indem sie die in der genannten Verordnung festgelegten grundlegenden Cybersicherheitsanforderungen erfüllen. Wenn Hochrisiko-KI-Systeme die grundlegenden Anforderungen einer Verordnung des Europäischen Parlaments und des Rates über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen erfüllen, sollten sie als die in der vorliegenden Verordnung festgelegten Cybersicherheitsanforderungen erfüllend gelten, soweit die Erfüllung der genannten Anforderungen in der gemäß der genannten Verordnung ausgestellten EU-Konformitätserklärung oder in Teilen davon nachgewiesen wird. Zu diesem Zweck sollten bei der im Rahmen einer Verordnung des Europäischen Parlaments und des Rates über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen durchgeführten Bewertung der Cybersicherheitsrisiken, die mit einem gemäß der vorliegenden Verordnung als Hochrisiko-KI-System eingestuften Produkt mit digitalen Elementen verbunden sind, Risiken für die Cyberabwehrfähigkeit eines KI-Systems in Bezug auf Versuche unbefugter Dritter, seine Verwendung, sein Verhalten oder seine Leistung zu verändern, einschließlich KI-spezifischer Schwachstellen wie Datenvergiftung oder feindlicher Angriffe, sowie gegebenenfalls Risiken für die Grundrechte gemäß der vorliegenden Verordnung berücksichtigt werden.

(78) Das in dieser Verordnung vorgesehene Konformitätsbewertungsverfahren sollte in Bezug auf die grundlegenden Cybersicherheitsanforderungen an ein Produkt mit digitalen Elementen, das unter eine Verordnung des Europäischen Parlaments und des Rates über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen fällt und gemäß der vorliegenden Verordnung als Hochrisiko-KI-System eingestuft ist, gelten. Diese Regel sollte jedoch nicht dazu führen, dass die erforderliche Vertrauenswürdigkeit für unter eine Verordnung des Europäischen Parlaments und des Rates über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen fallende kritische Produkte mit digitalen Elementen verringert wird. Daher unterliegen abweichend von dieser Regel Hochrisiko-KI-Systeme, die in den Anwendungsbereich der vorliegenden Verordnung fallen und gemäß einer Verordnung des Europäischen Parlaments und des Rates über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen als wichtige und kritische Produkte mit digitalen Elementen eingestuft werden und für die das Konformitätsbewertungsverfahren auf der Grundlage der internen Kontrolle gemäß einem Anhang der vorliegenden Verordnung gilt, den Konformitätsbewertungsbestimmungen einer Verordnung des Europäischen Parlaments und des Rates über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen, soweit die wesentlichen Cybersicherheitsanforderungen der genannten Verordnung betroffen sind. In diesem Fall sollten für alle anderen Aspekte, die unter die vorliegende Verordnung fallen, die entsprechenden Bestimmungen über die Konformitätsbewertung auf der Grundlage der internen Kontrolle gelten, die in einem Anhang der vorliegenden Verordnung festgelegt sind. Aufbauend auf den Kenntnissen und dem Fachwissen der ENISA in Bezug auf die Cybersicherheitspolitik und die der ENISA gemäß der Verordnung (EU) 2019/881 des Europäischen Parlaments und des Rates ([37]) übertragenen Aufgaben sollte die Kommission in Fragen im Zusammenhang mit der Cybersicherheit von KI-Systemen mit der ENISA zusammenarbeiten.

([37]) 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).

[sn502] Anbieter

[sn707] Bevollmächtigter

(79) Es ist angezeigt, 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.

(80) Als Unterzeichner des Übereinkommens über die Rechte von Menschen mit Behinderungen der Vereinten Nationen sind die Union und alle Mitgliedstaaten rechtlich verpflichtet, Menschen mit Behinderungen vor Diskriminierung zu schützen und ihre Gleichstellung zu fördern, sicherzustellen, dass Menschen mit Behinderungen gleichberechtigt Zugang zu Informations- und Kommunikationstechnologien und -systemen haben, und die Achtung der Privatsphäre von Menschen mit Behinderungen sicherzustellen. Angesichts der zunehmenden Bedeutung und Nutzung von KI-Systemen sollte die strikte Anwendung der Grundsätze des universellen Designs auf alle neuen Technologien und Dienste einen vollständigen und gleichberechtigten Zugang für alle Menschen sicherstellen, die potenziell von KI-Technologien betroffen sind oder diese nutzen, einschließlich Menschen mit Behinderungen, und zwar in einer Weise, die ihrer Würde und Vielfalt in vollem Umfang Rechnung trägt. Es ist daher von wesentlicher Bedeutung, dass die Anbieter die uneingeschränkte Einhaltung der Barrierefreiheitsanforderungen sicherstellen, einschließlich der in der Richtlinie (EU) 2016/2102 des Europäischen Parlaments und des Rates [38] und in der Richtlinie (EU) 2019/882 festgelegten Anforderungen. Die Anbieter sollten die Einhaltung dieser Anforderungen durch Voreinstellungen sicherstellen. Die erforderlichen Maßnahmen sollten daher so weit wie möglich in die Konzeption von Hochrisiko-KI-Systemen integriert werden.

[sn507] Beobachtung nach dem Inverkehrbringen

(81) 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. Anbieter von Hochrisiko-KI-Systemen, die Pflichten in Bezug auf Qualitätsmanagementsysteme gemäß den einschlägigen sektorspezifischen Rechtsvorschriften der Union unterliegen, sollten die Möglichkeit haben, die Elemente des in dieser Verordnung vorgesehenen Qualitätsmanagementsystems als Teil des bestehenden, in diesen anderen sektoralen Rechtsvorschriften der Union vorgesehen Qualitätsmanagementsystems aufzunehmen. Auch bei künftigen Normungstätigkeiten oder Leitlinien, die von der Kommission angenommen werden, sollte der Komplementarität zwischen dieser Verordnung und den bestehenden sektorspezifischen Rechtsvorschriften der Union Rechnung getragen werden. 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 besagten Behörde die Vorschriften für das Qualitätsmanagementsystem als Teil des auf nationaler oder regionaler Ebene eingesetzten Qualitätsmanagementsystems annehmen und umsetzen.

[sn707] Bevollmächtigter

(82) 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 niedergelassene Person den Behörden alle erforderlichen Informationen über die Konformität eines KI-Systems zur Verfügung stellen kann. Daher sollten Anbieter, die in Drittländern niedergelassen sind, vor der Bereitstellung ihrer KI-Systeme in der Union schriftlich einen in der Union niedergelassenen Bevollmächtigten benennen. Dieser Bevollmächtigte spielt eine zentrale Rolle bei der Gewährleistung der Konformität der von den betreffenden Anbietern, die nicht in der Union niedergelassen sind, in der Union in Verkehr gebrachten oder in Betrieb genommenen Hochrisiko-KI-Systeme und indem er als ihr in der Union niedergelassener Ansprechpartner dient.

[sn503] Betreiber

(83) Angesichts des Wesens und der Komplexität der Wertschöpfungskette für KI-Systeme und im Einklang mit dem neuen Rechtsrahmen ist es von wesentlicher Bedeutung, Rechtssicherheit zu gewährleisten und die Einhaltung dieser Verordnung zu erleichtern. Daher müssen die Rolle und die spezifischen Pflichten der relevanten Akteure entlang dieser Wertschöpfungskette, wie Einführer und Händler, die zur Entwicklung von KI-Systemen beitragen können, präzisiert werden. 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.

(84) Um Rechtssicherheit zu gewährleisten, muss präzisiert werden, dass unter bestimmten spezifischen Bedingungen jeder Händler, Einführer, Betreiber oder andere Dritte als Anbieter eines Hochrisiko-KI-Systems betrachtet werden und daher alle einschlägigen Pflichten erfüllen sollte. Dies wäre auch der Fall, wenn diese Partei ein bereits in Verkehr gebrachtes oder in Betrieb genommenes Hochrisiko-KI-System mit ihrem Namen oder ihrer Handelsmarke versieht, unbeschadet vertraglicher Vereinbarungen, die eine andere Aufteilung der Pflichten vorsehen, oder wenn sie eine wesentliche Veränderung des Hochrisiko-KI-Systems, das bereits in Verkehr gebracht oder bereits in Betrieb genommen wurde, so vornimmt, dass es ein Hochrisiko-KI-System im Sinne dieser Verordnung bleibt, oder wenn sie die Zweckbestimmung eines KI-Systems, einschließlich eines KI-Systems mit allgemeinem Verwendungszweck, das nicht als Hochrisiko-KI-System eingestuft wurde und bereits in Verkehr gebracht oder in Betrieb genommen wurde, so verändert, dass das KI-System zu einem Hochrisiko-KI-System im Sinne dieser Verordnung wird. Diese Bestimmungen sollten unbeschadet spezifischerer Bestimmungen in bestimmten Harmonisierungsrechtsvorschriften der Union auf Grundlage des neuen Rechtsrahmens gelten, mit denen diese Verordnung zusammen gelten sollte. So

[38] Richtlinie (EU) 2016/2102 des Europäischen Parlaments und des Rates vom 26. Oktober 2016 über den barrierefreien Zugang zu den Websites und mobilen Anwendungen öffentlicher Stellen (ABl. L 327 vom 2.12.2016, S. 1).

sollte beispielsweise Artikel 16 Absatz 2 der Verordnung (EU) 2017/745, wonach bestimmte Änderungen nicht als eine Änderung des Produkts, die Auswirkungen auf seine Konformität mit den geltenden Anforderungen haben könnte, gelten sollten, weiterhin auf Hochrisiko-KI-Systeme angewandt werden, bei denen es sich um Medizinprodukte im Sinne der genannten Verordnung handelt.

[sn502] Anbieter

(85) KI-Systeme mit allgemeinem Verwendungszweck können als eigenständige Hochrisiko-KI-Systeme eingesetzt werden oder Komponenten anderer Hochrisiko-KI-Systemen sein. Daher sollten, aufgrund der besonderen Merkmale dieser KI-Systeme und um für eine gerechte Verteilung der Verantwortlichkeiten entlang der KI-Wertschöpfungskette zu sorgen, Anbieter solcher Systeme, unabhängig davon, ob sie von anderen Anbietern als eigenständige Hochrisiko-KI-Systeme oder als Komponenten von Hochrisiko-KI-Systemen verwendet werden können, und sofern in dieser Verordnung nichts anderes bestimmt ist, eng mit den Anbietern der relevanten Hochrisiko-KI-Systeme, um ihnen die Einhaltung der entsprechenden Pflichten aus dieser Verordnung zu ermöglichen, und mit den gemäß dieser Verordnung eingerichteten zuständigen Behörden zusammenarbeiten.

[sn505] Konformitätsbewertung

(86) Sollte der Anbieter, der das KI-System ursprünglich in Verkehr gebracht oder in Betrieb genommen hat, unter den in dieser Verordnung festgelegten Bedingungen nicht mehr als Anbieter im Sinne dieser Verordnung gelten und hat jener Anbieter die Änderung des KI-Systems in ein Hochrisiko-KI-System nicht ausdrücklich ausgeschlossen, so sollte der erstgenannte Anbieter dennoch eng zusammenarbeiten, die erforderlichen Informationen zur Verfügung stellen und den vernünftigerweise erwarteten technischen Zugang und sonstige Unterstützung leisten, die für die Erfüllung der in dieser Verordnung festgelegten Pflichten, insbesondere in Bezug auf die Konformitätsbewertung von Hochrisiko-KI-Systemen, erforderlich sind.

(87) Zusätzlich sollte, wenn ein Hochrisiko-KI-System, bei dem es sich um ein Sicherheitsbauteil eines Produkts handelt, das in den Geltungsbereich von Harmonisierungsrechtsvorschriften der Union auf Grundlage des neuen Rechtsrahmens fällt, nicht unabhängig von dem Produkt in Verkehr gebracht oder in Betrieb genommen wird, der Produkthersteller im Sinne der genannten Rechtsvorschriften die in der vorliegenden Verordnung festgelegten Anbieterpflichten erfüllen und sollte insbesondere sicherstellen, dass das in das Endprodukt eingebettete KI-System den Anforderungen dieser Verordnung entspricht.

(88) Entlang der KI-Wertschöpfungskette liefern häufig mehrere Parteien KI-Systeme, Instrumente und Dienstleistungen, aber auch Komponenten oder Prozesse, die vom Anbieter zu diversen Zwecken in das KI-System integriert werden; dazu gehören das Trainieren, Neutrainieren, Testen und Bewerten von Modellen, die Integration in Software oder andere Aspekte der Modellentwicklung. Diese Parteien haben eine wichtige Rolle in der Wertschöpfungskette gegenüber dem Anbieter des Hochrisiko-KI-Systems, in das ihre KI-Systeme, Instrumente, Dienste, Komponenten oder Verfahren integriert werden, und sollten in einer schriftlichen Vereinbarung die Informationen, die Fähigkeiten, den technischen Zugang und die sonstige Unterstützung nach dem allgemein anerkannten Stand der Technik bereitstellen, die erforderlich sind, damit der Anbieter die in dieser Verordnung festgelegten Pflichten vollständig erfüllen kann, ohne seine eigenen Rechte des geistigen Eigentums oder Geschäftsgeheimnisse zu gefährden.

(89) Dritte, die Instrumente, Dienste, Verfahren oder Komponenten, bei denen es sich nicht um KI-Modelle mit allgemeinem Verwendungszweck handelt, öffentlich zugänglich machen, sollten nicht dazu verpflichtet werden, Anforderungen zu erfüllen, die auf die Verantwortlichkeiten entlang der KI-Wertschöpfungskette ausgerichtet sind, insbesondere gegenüber dem Anbieter, der sie genutzt oder integriert hat, wenn diese Instrumente, Dienste, Verfahren oder KI-Komponenten im Rahmen einer freien und quelloffenen Lizenz zugänglich gemacht werden. Die Entwickler von freien und quelloffenen Instrumenten, Diensten, Verfahren oder KI-Komponenten, bei denen es sich nicht um KI-Modelle mit allgemeinem Verwendungszweck handelt, sollten dazu ermutigt werden, weit verbreitete Dokumentationsverfahren, wie z. B. Modellkarten und Datenblätter, als Mittel dazu einzusetzen, den Informationsaustausch entlang der KI-Wertschöpfungskette zu beschleunigen, sodass vertrauenswürdige KI-Systeme in der Union gefördert werden können.

[sn503] Betreiber

(90) Die Kommission könnte freiwillige Mustervertragsbedingungen für Verträge zwischen Anbietern von Hochrisiko-KI-Systemen und Dritten ausarbeiten und empfehlen, in deren Rahmen Instrumente, Dienste, Komponenten oder Verfahren bereitgestellt werden, die für Hochrisiko-KI-Systeme verwendet oder in diese integriert werden, um die Zusammenarbeit entlang der Wertschöpfungskette zu erleichtern. Bei der Ausarbeitung dieser freiwilligen Mustervertragsbedingungen sollte die Kommission auch mögliche vertragliche Anforderungen berücksichtigen, die in bestimmten Sektoren oder Geschäftsfällen gelten.

(91) Angesichts des Charakters von KI-Systemen und der Risiken für die Sicherheit und die Grundrechte, die mit ihrer Verwendung verbunden sein können, ist es angezeigt, besondere Zuständigkeiten für die Betreiber festzulegen, auch im Hinblick darauf, dass eine angemessene Beobachtung der Leistung eines KI-Systems unter Realbedingungen sichergestellt werden muss. Die Betreiber sollten insbesondere geeignete technische und organisatorische Maßnahmen treffen, um sicherzustellen, dass sie Hochrisiko-KI-Systeme gemäß den Betriebsanleitungen verwenden, und es sollten bestimmte andere Pflichten in Bezug auf die Überwachung der Funktionsweise der KI-Systeme und gegebenenfalls auch Aufzeichnungspflichten festgelegt werden. Darüber hinaus sollten die Betreiber sicherstellen, dass die Personen, denen die Umsetzung der Betriebsanleitungen und die menschliche Aufsicht gemäß dieser

[sn801] KI-Kompetenz

[sn503] Betreiber

Verordnung übertragen wurde, über die erforderliche Kompetenz verfügen, insbesondere über ein angemessenes Niveau an KI-Kompetenz, Schulung und Befugnis, um diese Aufgaben ordnungsgemäß zu erfüllen. Diese Pflichten sollten sonstige Pflichten des Betreibers in Bezug auf Hochrisiko-KI-Systeme nach Unionsrecht oder nationalem Recht unberührt lassen.

(92) Diese Verordnung lässt Pflichten der Arbeitgeber unberührt, Arbeitnehmer oder ihre Vertreter nach dem Unionsrecht oder nationalem Recht und nationaler Praxis, einschließlich der Richtlinie 2002/14/EG des Europäischen Parlaments und des Rates ([39]) über Entscheidungen zur Inbetriebnahme oder Nutzung von KI-Systemen zu unterrichten oder zu unterrichten und anzuhören. Es muss nach wie vor sichergestellt werden, dass Arbeitnehmer und ihre Vertreter über die geplante Einführung von Hochrisiko-KI-Systemen am Arbeitsplatz unterrichtet werden, wenn die Bedingungen für diese Pflichten zur Unterrichtung oder zur Unterrichtung und Anhörung gemäß anderen Rechtsinstrumenten nicht erfüllt sind. Darüber hinaus ist dieses Recht, unterrichtet zu werden, ein Nebenrecht und für das Ziel des Schutzes der Grundrechte, das dieser Verordnung zugrunde liegt, erforderlich. Daher sollte in dieser Verordnung eine entsprechende Unterrichtungsanforderung festgelegt werden, ohne bestehende Arbeitnehmerrechte zu beeinträchtigen.

(93) Während Risiken im Zusammenhang mit KI-Systemen einerseits aus der Art und Weise entstehen können, in der solche Systeme konzipiert sind, können sie sich andererseits auch aus der Art und Weise ergeben, in der diese Systeme verwendet werden. Betreiber von Hochrisiko-KI-Systemen spielen daher eine entscheidende Rolle bei der Gewährleistung des Schutzes der Grundrechte in Ergänzung der Pflichten der Anbieter bei der Entwicklung der KI-Systeme. Betreiber können am besten verstehen, wie das Hochrisiko-KI-System konkret eingesetzt wird, und können somit dank einer genaueren Kenntnis des Verwendungskontextes sowie der wahrscheinlich betroffenen Personen oder Personengruppen, einschließlich schutzbedürftiger Gruppen, erhebliche potenzielle Risiken erkennen, die in der Entwicklungsphase nicht vorausgesehen wurden. Betreiber der in einem Anhang dieser Verordnung aufgeführten Hochrisiko-KI-Systeme spielen ebenfalls eine entscheidende Rolle bei der Unterrichtung natürlicher Personen und sollten, wenn sie natürliche Personen betreffende Entscheidungen treffen oder bei solchen Entscheidungen Unterstützung leisten, gegebenenfalls die natürlichen Personen darüber unterrichten, dass sie Gegenstand des Einsatzes des Hochrisiko-KI-Systems sind. Diese Unterrichtung sollte die Zweckbestimmung und die Art der getroffenen Entscheidungen umfassen. Der Betreiber sollte die natürlichen Personen auch über ihr Recht auf eine Erklärung gemäß dieser Verordnung unterrichten. Bei Hochrisiko-KI-Systemen, die zu Strafverfolgungszwecken eingesetzt werden, sollte diese Pflicht im Einklang mit Artikel 13 der Richtlinie (EU) 2016/680 umgesetzt werden.

(94) Jede Verarbeitung biometrischer Daten im Zusammenhang mit der Verwendung von KI-Systemen für die biometrische Identifizierung zu Strafverfolgungszwecken muss im Einklang mit Artikel 10 der Richtlinie (EU) 2016/680, demzufolge eine solche Verarbeitung nur dann erlaubt ist, wenn sie unbedingt erforderlich ist, vorbehaltlich angemessener Vorkehrungen für den Schutz der Rechte und Freiheiten der betroffenen Person, und sofern sie nach dem Unionsrecht oder dem Recht der Mitgliedstaaten zulässig ist, erfolgen. Bei einer solchen Nutzung, sofern sie zulässig ist, müssen auch die in Artikel 4 Absatz 1 der Richtlinie (EU) 2016/680 festgelegten Grundsätze geachtet werden, einschließlich Rechtmäßigkeit, Fairness und Transparenz, Zweckbindung, sachliche Richtigkeit und Speicherbegrenzung.

[sn706] Grundrechte-Folgenabschätzung

(95) Unbeschadet des geltenden Unionsrechts, insbesondere der Verordnung (EU) 2016/679 und der Richtlinie (EU) 2016/680, sollte die Verwendung von Systemen zur nachträglichen biometrischen Fernidentifizierung in Anbetracht des intrusiven Charakters von Systemen zur nachträglichen biometrischen Fernidentifizierung Schutzvorkehrungen unterliegen. Systeme zur nachträglichen biometrischen Fernidentifizierung sollten stets auf verhältnismäßige, legitime und unbedingt erforderliche Weise eingesetzt werden und somit zielgerichtet sein, was die zu identifizierenden Personen, den Ort und den zeitlichen Anwendungsbereich betrifft, und auf einem geschlossenen Datensatz rechtmäßig erworbener Videoaufnahmen basieren. In jedem Fall sollten Systeme zur nachträglichen biometrischen Fernidentifizierung im Rahmen der Strafverfolgung nicht so verwendet werden, dass sie zu willkürlicher Überwachung führen. Die Bedingungen für die nachträgliche biometrische Fernidentifizierung sollten keinesfalls eine Grundlage dafür bieten, die Bedingungen des Verbots und der strengen Ausnahmen für biometrische Echtzeit-Fernidentifizierung zu umgehen.

(96) Um wirksam sicherzustellen, dass die Grundrechte geschützt werden, sollten Betreiber von Hochrisiko-KI-Systemen, bei denen es sich um Einrichtungen des öffentlichen Rechts oder private Einrichtungen, die öffentliche Dienste erbringen, handelt, und Betreiber, die bestimmte Hochrisiko-KI-Systemen gemäß einem Anhang dieser Verordnung betreiben, wie Bank- oder Versicherungsunternehmen, vor der Inbetriebnahme eine Grundrechte-Folgenabschätzung durchführen. Für Einzelpersonen wichtige Dienstleistungen öffentlicher Art können auch von privaten Einrichtungen erbracht werden. Private Einrichtungen, die solche öffentliche Dienstleistungen erbringen, sind mit Aufgaben im öffentlichen Interesse verknüpft, etwa in den Bereichen Bildung, Gesundheitsversorgung, Sozialdienste, Wohnungswesen und Justizverwaltung. Ziel der Grundrechte-Folgenabschätzung ist es, dass der Betreiber die spezifischen Risiken für die Rechte von Einzelpersonen oder Gruppen von Einzelpersonen, die wahrscheinlich betroffen sein werden, ermittelt und Maßnahmen ermittelt, die im Falle eines Eintretens dieser Risiken zu ergreifen sind. Die

([39]) Richtlinie 2002/14/EG des Europäischen Parlaments und des Rates vom 11. März 2002 zur Festlegung eines allgemeinen Rahmens für die Unterrichtung und Anhörung der Arbeitnehmer in der Europäischen Gemeinschaft (ABl. L 80 vom 23.3.2002, S. 29).

[se801] berücksichtigt

[sn706] Grundrechte-Folgenabschätzung

[sn503] Betreiber

[sn502] Anbieter

Folgenabschätzung sollte vor dem erstmaligen Einsatz des Hochrisiko-KI-Systems durchgeführt werden, und sie sollte aktualisiert werden, wenn der Betreiber der Auffassung ist, dass sich einer der relevanten Faktoren geändert hat. In der Folgenabschätzung sollten die einschlägigen Verfahren des Betreibers, bei denen das Hochrisiko-KI-System im Einklang mit seiner Zweckbestimmung verwendet wird, genannt werden, und sie sollte eine Beschreibung des Zeitraums und der Häufigkeit, innerhalb dessen bzw. mit der das Hochrisiko-KI-System verwendet werden soll, sowie der Kategorien der natürlichen Personen und Gruppen, die im spezifischen Verwendungskontext betroffen sein könnten, enthalten. Die Abschätzung sollte außerdem die spezifischen Schadensrisiken enthalten, die sich auf die Grundrechte dieser Personen oder Gruppen auswirken können. Bei der Durchführung dieser Bewertung sollte der Betreiber Informationen Rechnung tragen, die für eine ordnungsgemäße Abschätzung der Folgen relevant sind, unter anderem die vom Anbieter des Hochrisiko-KI-Systems in der Betriebsanleitung angegebenen Informationen. Angesichts der ermittelten Risiken sollten die Betreiber Maßnahmen festlegen, die im Falle eines Eintretens dieser Risiken zu ergreifen sind, einschließlich beispielsweise Unternehmensführungsregelungen in diesem spezifischen Verwendungskontext, etwa Regelungen für die menschliche Aufsicht gemäß den Betriebsanleitungen oder Verfahren für die Bearbeitung von Beschwerden und Rechtsbehelfsverfahren, da sie dazu beitragen könnten, Risiken für die Grundrechte in konkreten Anwendungsfällen zu mindern. Nach Durchführung dieser Folgenabschätzung sollte der Betreiber die zuständige Marktüberwachungsbehörde unterrichten. Um einschlägige Informationen einzuholen, die für die Durchführung der Folgenabschätzung erforderlich sind, könnten die Betreiber von Hochrisiko-KI-Systemen, insbesondere wenn KI-Systeme im öffentlichen Sektor verwendet werden, relevante Interessenträger, unter anderem Vertreter von Personengruppen, die von dem KI-System betroffen sein könnten, unabhängige Sachverständige und Organisationen der Zivilgesellschaft, in die Durchführung solcher Folgenabschätzungen und die Gestaltung von Maßnahmen, die im Falle des Eintretens der Risiken zu ergreifen sind, einbeziehen. Das Europäische Büro für Künstliche Intelligenz (im Folgenden „Büro für Künstliche Intelligenz“) sollte ein Muster für einen Fragebogen ausarbeiten, um den Betreibern die Einhaltung der Vorschriften zu erleichtern und den Verwaltungsaufwand für sie zu verringern.

(97) Der Begriff „KI-Modelle mit allgemeinem Verwendungszweck“ sollte klar bestimmt und vom Begriff der KI-Systeme abgegrenzt werden, um Rechtssicherheit zu schaffen. Die Begriffsbestimmung sollte auf den wesentlichen funktionalen Merkmalen eines KI-Modells mit allgemeinem Verwendungszweck beruhen, insbesondere auf der allgemeinen Verwendbarkeit und der Fähigkeit, ein breites Spektrum unterschiedlicher Aufgaben kompetent zu erfüllen. Diese Modelle werden in der Regel mit großen Datenmengen durch verschiedene Methoden, etwa überwachtes, unüberwachtes und bestärkendes Lernen, trainiert. KI-Modelle mit allgemeinem Verwendungszweck können auf verschiedene Weise in Verkehr gebracht werden, unter anderem über Bibliotheken, Anwendungsprogrammierschnittstellen (API), durch direktes Herunterladen oder als physische Kopie. Diese Modelle können weiter geändert oder zu neuen Modellen verfeinert werden. Obwohl KI-Modelle wesentliche Komponenten von KI-Systemen sind, stellen sie für sich genommen keine KI-Systeme dar. Damit KI-Modelle zu KI-Systemen werden, ist die Hinzufügung weiterer Komponenten, zum Beispiel einer Nutzerschnittstelle, erforderlich. KI-Modelle sind in der Regel in KI-Systeme integriert und Teil davon. Diese Verordnung enthält spezifische Vorschriften für KI-Modelle mit allgemeinem Verwendungszweck und für KI-Modelle mit allgemeinem Verwendungszweck, die systemische Risiken bergen; diese sollten auch gelten, wenn diese Modelle in ein KI-System integriert oder Teil davon sind. Es sollte klar sein, dass die Pflichten für die Anbieter von KI-Modellen mit allgemeinem Verwendungszweck gelten sollten, sobald die KI-Modelle mit allgemeinem Verwendungszweck in Verkehr gebracht werden. Wenn der Anbieter eines KI-Modells mit allgemeinem Verwendungszweck ein eigenes Modell in sein eigenes KI-System integriert, das auf dem Markt bereitgestellt oder in Betrieb genommen wird, sollte jenes Modell als in Verkehr gebracht gelten und sollten daher die Pflichten aus dieser Verordnung für Modelle weiterhin zusätzlich zu den Pflichten für KI-Systeme gelten. Die für Modelle festgelegten Pflichten sollten in jedem Fall nicht gelten, wenn ein eigenes Modell für rein interne Verfahren verwendet wird, die für die Bereitstellung eines Produkts oder einer Dienstleistung an Dritte nicht wesentlich sind, und die Rechte natürlicher Personen nicht beeinträchtigt werden. Angesichts ihrer potenziellen in erheblichem Ausmaße negativen Auswirkungen sollten KI-Modelle mit allgemeinem Verwendungszweck mit systemischem Risiko stets den einschlägigen Pflichten gemäß dieser Verordnung unterliegen. Die Begriffsbestimmung sollte nicht für KI-Modelle gelten, die vor ihrem Inverkehrbringen ausschließlich für Forschungs- und Entwicklungstätigkeiten oder die Konzipierung von Prototypen verwendet werden. Dies gilt unbeschadet der Pflicht, dieser Verordnung nachzukommen, wenn ein Modell nach solchen Tätigkeiten in Verkehr gebracht wird.

(98) Die allgemeine Verwendbarkeit eines Modells könnte zwar unter anderem auch durch eine bestimmte Anzahl von Parametern bestimmt werden, doch sollten Modelle mit mindestens einer Milliarde Parametern, die mit einer großen Datenmenge unter umfassender Selbstüberwachung trainiert werden, als Modelle gelten, die eine erhebliche allgemeine Verwendbarkeit aufweisen und ein breites Spektrum unterschiedlicher Aufgaben kompetent erfüllen.

(99) Große generative KI-Modelle sind ein typisches Beispiel für ein KI-Modell mit allgemeinem Verwendungszweck, da sie eine flexible Erzeugung von Inhalten ermöglichen, etwa in Form von Text- Audio-, Bild- oder Videoinhalten, die leicht ein breites Spektrum unterschiedlicher Aufgaben umfassen können.

(100) Wenn ein KI-Modell mit allgemeinem Verwendungszweck in ein KI-System integriert oder Teil davon ist, sollte dieses System als KI-System mit allgemeinem Verwendungszweck gelten, wenn dieses System aufgrund dieser Integration in der Lage ist, einer Vielzahl von Zwecken zu dienen. Ein KI-System mit allgemeinem Verwendungszweck kann direkt eingesetzt oder in andere KI-Systeme integriert werden.

[sn502] Anbieter

(101) Anbieter von KI-Modellen mit allgemeinem Verwendungszweck nehmen entlang der KI-Wertschöpfungskette eine besondere Rolle und Verantwortung wahr, da die von ihnen bereitgestellten Modelle die Grundlage für eine Reihe nachgelagerter Systeme bilden können, die häufig von nachgelagerten Anbietern bereitgestellt werden und ein gutes Verständnis der Modelle und ihrer Fähigkeiten erfordern, sowohl um die Integration solcher Modelle in ihre Produkte zu ermöglichen als auch ihre Pflichten im Rahmen dieser oder anderer Verordnungen zu erfüllen. Daher sollten verhältnismäßige Transparenzmaßnahmen festgelegt werden, einschließlich der Erstellung und Aktualisierung von Dokumentation und der Bereitstellung von Informationen über das KI-Modell mit allgemeinem Verwendungszweck für dessen Nutzung durch die nachgelagerten Anbieter. Der Anbieter von KI-Modellen mit allgemeinem Verwendungszweck sollte technische Dokumentation erarbeiten und aktualisieren, damit sie dem Büro für Künstliche Intelligenz und den zuständigen nationalen Behörden auf Anfrage zur Verfügung gestellt werden kann. Welche Elemente mindestens in eine solche Dokumentation aufzunehmen sind, sollte in bestimmten Anhängen dieser Verordnung festgelegt werden. Der Kommission sollte die Befugnis übertragen werden, diese Anhänge im Wege delegierter Rechtsakte vor dem Hintergrund sich wandelnder technologischer Entwicklungen zu ändern.

[sn901] Büro für Künstliche Intelligenz

(102) Software und Daten, einschließlich Modellen, die im Rahmen einer freien und quelloffenen Lizenz freigegeben werden, die ihre offene Weitergabe erlaubt und die Nutzer kostenlos abrufen, nutzen, verändern und weiter verteilen können, auch in veränderter Form, können zu Forschung und Innovation auf dem Markt beitragen und der Wirtschaft der Union erhebliche Wachstumschancen eröffnen. KI-Modelle mit allgemeinem Verwendungszweck, die im Rahmen freier und quelloffener Lizenzen freigegeben werden, sollten als ein hohes Maß an Transparenz und Offenheit sicherstellend gelten, wenn ihre Parameter, einschließlich Gewichte, Informationen über die Modellarchitektur und Informationen über die Modellnutzung, öffentlich zugänglich gemacht werden. Die Lizenz sollte auch als freie quelloffene Lizenz gelten, wenn sie es den Nutzern ermöglicht, Software und Daten zu betreiben, zu kopieren, zu verbreiten, zu untersuchen, zu ändern und zu verbessern, einschließlich Modelle, sofern der ursprüngliche Anbieter des Modells genannt und identische oder vergleichbare Vertriebsbedingungen eingehalten werden.

(103) Zu freien und quelloffenen KI-Komponenten zählen Software und Daten, einschließlich Modelle und KI-Modelle mit allgemeinem Verwendungszweck, Instrumente, Dienste oder Verfahren eines KI-Systems. Freie und quelloffene KI-Komponenten können über verschiedene Kanäle bereitgestellt werden, einschließlich ihrer Entwicklung auf offenen Speichern. Für die Zwecke dieser Verordnung sollten KI-Komponenten, die gegen einen Preis bereitgestellt oder anderweitig monetarisiert werden, einschließlich durch die Bereitstellung technischer Unterstützung oder anderer Dienste — einschließlich über eine Softwareplattform — im Zusammenhang mit der KI-Komponente oder durch die Verwendung personenbezogener Daten aus anderen Gründen als der alleinigen Verbesserung der Sicherheit, Kompatibilität oder Interoperabilität der Software, mit Ausnahme von Transaktionen zwischen Kleinstunternehmen, nicht unter die Ausnahmen für freie und quelloffene KI-Komponenten fallen. Die Bereitstellung von KI-Komponenten über offene Speicher sollte für sich genommen keine Monetarisierung darstellen.

(104) Für die Anbieter von KI-Modellen mit allgemeinem Verwendungszweck, die im Rahmen einer freien und quelloffenen Lizenz freigegeben werden und deren Parameter, einschließlich Gewichte, Informationen über die Modellarchitektur und Informationen über die Modellnutzung, öffentlich zugänglich gemacht werden, sollten Ausnahmen in Bezug auf die Transparenzanforderungen für KI-Modelle mit allgemeinem Verwendungszweck gelten, es sei denn, sie können als Modelle gelten, die ein systemisches Risiko bergen; in diesem Fall sollte der Umstand, dass das Modell transparent ist und mit einer quelloffenen Lizenz einhergeht, nicht als ausreichender Grund gelten, um sie von der Einhaltung der Pflichten aus dieser Verordnung auszunehmen. Da die Freigabe von KI-Modellen mit allgemeinem Verwendungszweck im Rahmen einer freien und quelloffenen Lizenz nicht unbedingt wesentliche Informationen über den für das Trainieren oder die Feinabstimmung des Modells verwendeten Datensatz und die Art und Weise, wie damit die Einhaltung des Urheberrechts sichergestellt wurde, offenbart, sollte die für KI-Modelle mit allgemeinem Verwendungszweck vorgesehene Ausnahme von der Einhaltung der Transparenzanforderungen in jedem Fall nicht die Pflicht zur Erstellung einer Zusammenfassung der für das Training des Modells verwendeten Inhalte und die Pflicht, eine Strategie zur Einhaltung des Urheberrechts der Union, insbesondere zur Ermittlung und Einhaltung der gemäß Artikel 4 Absatz 3 der Richtlinie (EU) 2019/790 des Europäischen Parlaments und des Rates ([40]) geltend gemachten Rechtsvorbehalte, auf den Weg zu bringen, betreffen.

(105) KI-Modelle mit allgemeinem Verwendungszweck, insbesondere große generative KI-Modelle, die Text, Bilder und andere Inhalte erzeugen können, bedeuten einzigartige Innovationsmöglichkeiten, aber auch Herausforderungen für Künstler, Autoren und andere Kreative sowie die Art und Weise, wie ihre kreativen Inhalte geschaffen, verbreitet, genutzt und konsumiert werden. Für die Entwicklung und das Training solcher Modelle ist der Zugang zu riesigen Mengen an Text, Bildern, Videos und anderen Daten erforderlich. In diesem Zusammenhang können Text-und-Data-Mining-Techniken in großem Umfang für das Abrufen und die Analyse solcher Inhalte, die urheberrechtlich und durch verwandte Schutzrechte geschützt sein können, eingesetzt werden. Für jede Nutzung urheberrechtlich geschützter Inhalte ist die Zustimmung des betreffenden Rechteinhabers erforderlich, es sei denn, es gelten einschlägige Ausnahmen und Beschränkungen des Urheberrechts. Mit der Richtlinie (EU) 2019/790 wurden Ausnahmen und Beschränkungen eingeführt, um unter bestimmten Bedingungen Vervielfältigungen und Entnahmen

([40]) Richtlinie (EU) 2019/790 des Europäischen Parlaments und des Rates vom 17. April 2019 über das Urheberrecht und die verwandten Schutzrechte im digitalen Binnenmarkt und zur Änderung der Richtlinien 96/9/EG und 2001/29/EG (ABl. L 130 vom 17.5.2019, S. 92).

[se900] überwacht

[sn502] Anbieter

von Werken oder sonstigen Schutzgegenständen für die Zwecke des Text und Data Mining zu erlauben. Nach diesen Vorschriften können Rechteinhaber beschließen, ihre Rechte an ihren Werken oder sonstigen Schutzgegenständen vorzubehalten, um Text und Data Mining zu verhindern, es sei denn, es erfolgt zum Zwecke der wissenschaftlichen Forschung. Wenn die Vorbehaltsrechte ausdrücklich und in geeigneter Weise vorbehalten wurden, müssen Anbieter von KI-Modellen mit allgemeinem Verwendungszweck eine Genehmigung von den Rechteinhabern einholen, wenn sie Text und Data Mining bei solchen Werken durchführen wollen.

(106) Anbieter, die KI-Modelle mit allgemeinem Verwendungszweck in der Union in Verkehr bringen, sollten die Erfüllung der einschlägigen Pflichten aus dieser Verordnung gewährleisten. Zu diesem Zweck sollten Anbieter von KI-Modellen mit allgemeinem Verwendungszweck eine Strategie zur Einhaltung des Urheberrechts der Union und der verwandten Schutzrechte einführen, insbesondere zur Ermittlung und Einhaltung des gemäß Artikel 4 Absatz 3 der Richtlinie (EU) 2019/790 durch die Rechteinhaber geltend gemachten Rechtsvorbehalts. Jeder Anbieter, der ein KI-Modell mit allgemeinem Verwendungszweck in der Union in Verkehr bringt, sollte diese Pflicht erfüllen, unabhängig davon, in welchem Hoheitsgebiet die urheberrechtlich relevanten Handlungen, die dem Training dieser KI-Modelle mit allgemeinem Verwendungszweck zugrunde liegen, stattfinden. Dies ist erforderlich, um gleiche Wettbewerbsbedingungen für Anbieter von KI-Modellen mit allgemeinem Verwendungszweck sicherzustellen, unter denen kein Anbieter in der Lage sein sollte, durch die Anwendung niedrigerer Urheberrechtsstandards als in der Union einen Wettbewerbsvorteil auf dem Unionsmarkt zu erlangen.

[se900] überwacht

[sn901] Büro für Künstliche Intelligenz

(107) Um die Transparenz in Bezug auf die beim Vortraining und Training von KI-Modellen mit allgemeinem Verwendungszweck verwendeten Daten, einschließlich urheberrechtlich geschützter Texte und Daten, zu erhöhen, ist es angemessen, dass die Anbieter solcher Modelle eine hinreichend detaillierte Zusammenfassung der für das Training des KI-Modells mit allgemeinem Verwendungszweck verwendeten Inhalte erstellen und veröffentlichen. Unter gebührender Berücksichtigung der Notwendigkeit, Geschäftsgeheimnisse und vertrauliche Geschäftsinformationen zu schützen, sollte der Umfang dieser Zusammenfassung allgemein weitreichend und nicht technisch detailliert sein, um Parteien mit berechtigtem Interesse, einschließlich der Inhaber von Urheberrechten, die Ausübung und Durchsetzung ihrer Rechte nach dem Unionsrecht zu erleichtern, beispielsweise indem die wichtigsten Datenerhebungen oder Datensätze aufgeführt werden, die beim Training des Modells verwendet wurden, etwa große private oder öffentliche Datenbanken oder Datenarchive, und indem eine beschreibende Erläuterung anderer verwendeter Datenquellen bereitgestellt wird. Es ist angebracht, dass das Büro für Künstliche Intelligenz eine Vorlage für die Zusammenfassung bereitstellt, die einfach und wirksam sein sollte und es dem Anbieter ermöglichen sollte, die erforderliche Zusammenfassung in beschreibender Form bereitzustellen.

(108) In Bezug auf die den Anbietern von KI-Modellen mit allgemeinem Verwendungszweck auferlegten Pflichten, eine Strategie zur Einhaltung des Urheberrechts der Union einzuführen und eine Zusammenfassung der für das Training verwendeten Inhalte zu veröffentlichen, sollte das Büro für Künstliche Intelligenz überwachen, ob der Anbieter diese Pflichten erfüllt hat, ohne dies zu überprüfen oder die Trainingsdaten im Hinblick auf die Einhaltung des Urheberrechts Werk für Werk zu bewerten. Diese Verordnung berührt nicht die Durchsetzung der Urheberrechtsvorschriften des Unionsrechts.

(109) Die Einhaltung der für die Anbieter von KI-Modellen mit allgemeinem Verwendungszweck geltenden Pflichten sollte der Art des Anbieters von Modellen angemessen und verhältnismäßig sein, wobei Personen, die Modelle für nicht berufliche oder wissenschaftliche Forschungszwecke entwickeln oder verwenden, ausgenommen sind, jedoch ermutigt werden sollten, diese Anforderungen freiwillig zu erfüllen. Unbeschadet des Urheberrechts der Union sollte bei der Einhaltung dieser Pflichten der Größe des Anbieters gebührend Rechnung getragen und für KMU, einschließlich Start-up-Unternehmen, vereinfachte Verfahren zur Einhaltung ermöglicht werden, die keine übermäßigen Kosten verursachen und nicht von der Verwendung solcher Modelle abhalten sollten. Im Falle einer Änderung oder Feinabstimmung eines Modells sollten die Pflichten der Anbieter von KI-Modellen mit allgemeinem Verwendungszweck auf diese Änderung oder Feinabstimmung beschränkt sein, indem beispielsweise die bereits vorhandene technische Dokumentation um Informationen über die Änderungen, einschließlich neuer Trainingsdatenquellen, ergänzt wird, um die in dieser Verordnung festgelegten Pflichten in der Wertschöpfungskette zu erfüllen.

(110) KI-Modelle mit allgemeinem Verwendungszweck könnten systemische Risiken bergen, unter anderem tatsächliche oder vernünftigerweise vorhersehbare negative Auswirkungen im Zusammenhang mit schweren Unfällen, Störungen kritischer Sektoren und schwerwiegende Folgen für die öffentliche Gesundheit und Sicherheit; alle tatsächlichen oder vernünftigerweise vorhersehbaren negativen Auswirkungen auf die demokratischen Prozesse und die öffentliche und wirtschaftliche Sicherheit; die Verbreitung illegaler, falscher oder diskriminierender Inhalte. Bei systemischen Risiken sollte davon ausgegangen werden, dass sie mit den Fähigkeiten und der Reichweite des Modells zunehmen, während des gesamten Lebenszyklus des Modells auftreten können und von Bedingungen einer Fehlanwendung, der Zuverlässigkeit des Modells, der Modellgerechtigkeit und der Modellsicherheit, dem Grad der Autonomie des Modells, seinem Zugang zu Instrumenten, neuartigen oder kombinierten Modalitäten, Freigabe- und Vertriebsstrategien, dem Potenzial zur Beseitigung von Leitplanken und anderen Faktoren beeinflusst werden. Insbesondere bei internationalen Ansätzen wurde bisher festgestellt, dass folgenden Risiken Rechnung getragen werden muss: den Risiken einer möglichen vorsätzlichen Fehlanwendung oder unbeabsichtigter Kontrollprobleme im Zusammenhang mit der Ausrichtung auf menschliche Absicht; chemischen, biologischen, radiologischen und

nuklearen Risiken, zum Beispiel Möglichkeiten zur Verringerung der Zutrittsschranken, einschließlich für Entwicklung, Gestaltung, Erwerb oder Nutzung von Waffen; offensiven Cyberfähigkeiten, zum Beispiel die Art und Weise, wie Entdeckung, Ausbeutung oder operative Nutzung von Schwachstellen ermöglicht werden können; den Auswirkungen der Interaktion und des Einsatzes von Instrumenten, einschließlich zum Beispiel der Fähigkeit, physische Systeme zu steuern und in kritische Infrastrukturen einzugreifen; Risiken, dass Modelle sich selbst vervielfältigen, oder der „Selbstreplikation" oder des Trainings anderer Modelle; der Art und Weise, wie Modelle zu schädlichen Verzerrungen und Diskriminierung mit Risiken für Einzelpersonen, Gemeinschaften oder Gesellschaften führen können; der Erleichterung von Desinformation oder der Verletzung der Privatsphäre mit Gefahren für demokratische Werte und Menschenrechte; dem Risiko, dass ein bestimmtes Ereignis zu einer Kettenreaktion mit erheblichen negativen Auswirkungen führen könnte, die sich auf eine ganze Stadt, eine ganze Tätigkeit in einem Bereich oder eine ganze Gemeinschaft auswirken könnten.

(111) Es ist angezeigt, eine Methodik für die Einstufung von KI-Modellen mit allgemeinem Verwendungszweck als KI-Modelle mit allgemeinem Verwendungszweck mit systemischen Risiken festzulegen. Da sich systemische Risiken aus besonders hohen Fähigkeiten ergeben, sollte ein KI-Modell mit allgemeinem Verwendungszweck als Modell mit systemischen Risiken gelten, wenn es über auf der Grundlage geeigneter technischer Instrumente und Methoden bewertete Fähigkeiten mit hoher Wirkkraft verfügt oder aufgrund seiner Reichweite erhebliche Auswirkungen auf den Binnenmarkt hat. „Fähigkeiten mit hoher Wirkkraft" bei KI-Modellen mit allgemeinem Verwendungszweck bezeichnet Fähigkeiten, die den bei den fortschrittlichsten KI-Modellen mit allgemeinem Verwendungszweck festgestellten Fähigkeiten entsprechen oder diese übersteigen. Das gesamte Spektrum der Fähigkeiten eines Modells könnte besser verstanden werden, nachdem es in Verkehr gebracht wurde oder wenn die Betreiber mit dem Modell interagieren. Nach dem Stand der Technik zum Zeitpunkt des Inkrafttretens dieser Verordnung ist die kumulierte Menge der für das Training des KI-Modells mit allgemeinem Verwendungszweck verwendeten Berechnungen, gemessen in Gleitkommaoperationen, einer der einschlägigen Näherungswerte für Modellfähigkeiten. Die kumulierte Menge der für das Training verwendeten Berechnungen umfasst die kumulierte Menge der für die Tätigkeiten und Methoden, mit denen die Fähigkeiten des Modells vor der Einführung verbessert werden sollen, wie zum Beispiel Vortraining, Generierung synthetischer Daten und Feinabstimmung, verwendeten Berechnungen. Daher sollte ein erster Schwellenwert der Gleitkommaoperationen festgelegt werden, dessen Erreichen durch ein KI-Modell mit allgemeinem Verwendungszweck zu der Annahme führt, dass es sich bei dem Modell um ein KI-Modell mit allgemeinem Verwendungszweck mit systemischen Risiken handelt. Dieser Schwellenwert sollte im Laufe der Zeit angepasst werden, um technologischen und industriellen Veränderungen, wie zum Beispiel algorithmischen Verbesserungen oder erhöhter Hardwareeffizienz, Rechnung zu tragen, und um Benchmarks und Indikatoren für die Modellfähigkeit ergänzt werden. Um die Grundlage dafür zu schaffen, sollte das Büro für Künstliche Intelligenz mit der Wissenschaftsgemeinschaft, der Industrie, der Zivilgesellschaft und anderen Sachverständigen zusammenarbeiten. Schwellenwerte sowie Instrumente und Benchmarks für die Bewertung von Fähigkeiten mit hoher Wirkkraft sollten zuverlässig die allgemeine Verwendbarkeit, die Fähigkeiten und die mit ihnen verbundenen systemischen Risikos von KI-Modellen mit allgemeinem Verwendungszweck vorhersagen können und könnten die Art und Weise, wie das Modell in Verkehr gebracht wird, oder die Zahl der Nutzer, auf die es sich auswirken könnte, berücksichtigen. Ergänzend zu diesem System sollte die Kommission Einzelentscheidungen treffen können, mit denen ein KI-Modell mit allgemeinem Verwendungszweck als KI-Modell mit allgemeinem Verwendungszweck mit systemischem Risiko eingestuft wird, wenn festgestellt wurde, dass dieses Modell Fähigkeiten oder Auswirkungen hat, die den von dem festgelegten Schwellenwert erfassten entsprechen. Die genannte Entscheidung sollte auf der Grundlage einer Gesamtbewertung der in einem Anhang dieser Verordnung festgelegten Kriterien für die Benennung von KI-Modellen mit allgemeinem Verwendungszweck mit systemischem Risiko getroffen werden, etwa Qualität oder Größe des Trainingsdatensatzes, Anzahl der gewerblichen Nutzer und Endnutzer, seine Ein- und Ausgabemodalitäten, sein Grad an Autonomie und Skalierbarkeit oder die Instrumente, zu denen es Zugang hat. Stellt der Anbieter, dessen Modell als KI-Modell mit allgemeinem Verwendungszweck mit systemischem Risiko benannt wurde, einen entsprechenden Antrag, sollte die Kommission den Antrag berücksichtigen, und sie kann entscheiden, erneut zu prüfen, ob beim KI-Modell mit allgemeinem Verwendungszweck immer noch davon ausgegangen werden kann, dass es systemische Risiken aufweist.

[sn901] Büro für Künstliche Intelligenz

[sn502] Anbieter

(112) Außerdem muss das Verfahren für die Einstufung eines KI-Modell mit allgemeinem Verwendungszweck mit systemischem Risiko präzisiert werden. Bei einem KI-Modell mit allgemeinem Verwendungszweck, das den geltenden Schwellenwert für Fähigkeiten mit hoher Wirkkraft erreicht, sollte angenommen werden, dass es sich um ein KI-Modell mit allgemeinem Verwendungszweck mit systemischem Risiko handelt. Der Anbieter sollte spätestens zwei Wochen, nachdem die Bedingungen erfüllt sind oder bekannt wird, dass ein KI-Modell mit allgemeinem Verwendungszweck die Bedingungen, die die Annahme bewirken, erfüllen wird, dies dem Büro für Künstliche Intelligenz mitteilen. Dies ist insbesondere im Zusammenhang mit dem Schwellenwert der Gleitkommaoperationen relevant, da das Training von KI-Modellen mit allgemeinem Verwendungszweck eine erhebliche Planung erfordert, die die vorab durchgeführte Zuweisung von Rechenressourcen umfasst, sodass die Anbieter von KI-Modellen mit allgemeinem Verwendungszweck vor Abschluss des Trainings erfahren können, ob ihr Modell den Schwellenwert erreichen wird. Im Rahmen dieser Mitteilung sollte der Anbieter nachweisen können, dass ein KI-Modell mit allgemeinem Verwendungszweck aufgrund seiner besonderen Merkmale außerordentlicherweise keine systemischen Risiken birgt und daher nicht als KI-Modell mit allgemeinem Verwendungszweck mit systemischem Risiko eingestuft werden sollte. Diese Informationen sind für das Büro für Künstliche Intelligenz wertvoll, um das Inverkehrbringen von KI-Modellen mit allgemeinem Verwendungszweck mit systemischem Risiko zu antizipieren, und die Anbieter können frühzeitig mit der Zusammenarbeit mit dem Büro für Künstliche Intelligenz beginnen. Diese Informationen

sind besonders wichtig im Hinblick auf KI-Modell mit allgemeinem Verwendungszweck, die als quelloffene Modelle bereitgestellt werden sollen, da nach der Bereitstellung von quelloffenen Modellen die erforderlichen Maßnahmen zur Gewährleistung der Einhaltung der Pflichten gemäß dieser Verordnung möglicherweise schwieriger umzusetzen sind.

[sn502] Anbieter

[sn901] Büro für Künstliche Intelligenz

(113) Erhält die Kommission Kenntnis davon, dass ein KI-Modell mit allgemeinem Verwendungszweck die Anforderungen für die Einstufung als KI-Modell mit allgemeinem Verwendungszweck mit systemischem Risiko erfüllt, das zuvor nicht bekannt war oder das der betreffende Anbieter nicht der Kommission gemeldet hat, sollte die Kommission befugt sein, es als solches auszuweisen. Zusätzlich zu den Überwachungstätigkeiten des Büros für Künstliche Intelligenz sollte ein System qualifizierter Warnungen sicherstellen, dass das Büro für Künstliche Intelligenz von dem wissenschaftlichen Gremium von KI-Modelle mit allgemeinem Verwendungszweck in Kenntnis gesetzt wird, die möglicherweise als KI-Modelle mit allgemeinem Verwendungszweck mit systemischem Risiko eingestuft werden sollten, was zu den hinzukommt.

(114) Anbieter von KI-Modellen mit allgemeinem Verwendungszweck, die systemische Risiken bergen, sollten zusätzlich zu den Pflichten für Anbieter von KI-Modellen mit allgemeinem Verwendungszweck Pflichten unterliegen, die darauf abzielen, diese Risiken zu ermitteln und zu mindern und ein angemessenes Maß an Cybersicherheit zu gewährleisten, unabhängig davon, ob es als eigenständiges Modell bereitgestellt wird oder in ein KI-System oder ein Produkt eingebettet ist. Um diese Ziele zu erreichen, sollten die Anbieter in dieser Verordnung verpflichtet werden, die erforderlichen Bewertungen des Modells — insbesondere vor seinem ersten Inverkehrbringen — durchzuführen, wozu auch die Durchführung und Dokumentation von Angriffstests bei Modellen gehören, gegebenenfalls auch im Rahmen interner oder unabhängiger externer Tests. Darüber hinaus sollten KI-Modellen mit allgemeinem Verwendungszweck mit systemischem Risiko fortlaufend systemische Risiken bewerten und mindern, unter anderem durch die Einführung von Risikomanagementstrategien wie Verfahren der Rechenschaftspflicht und Governance-Verfahren, die Umsetzung der Beobachtung nach dem Inverkehrbringen, die Ergreifung geeigneter Maßnahmen während des gesamten Lebenszyklus des Modells und die Zusammenarbeit mit einschlägigen Akteuren entlang der KI-Wertschöpfungskette.

(115) Anbieter von KI-Modellen mit allgemeinem Verwendungszweck mit systemischem Risiko sollten mögliche systemische Risiken bewerten und mindern. Wenn trotz der Bemühungen um Ermittlung und Vermeidung von Risiken im Zusammenhang mit einem KI-Modell mit allgemeinem Verwendungszweck, das systemische Risiken bergen könnte, die Entwicklung oder Verwendung des Modells einen schwerwiegenden Vorfall verursacht, so sollte der Anbieter des KI-Modells mit allgemeinem Verwendungszweck unverzüglich dem Vorfall nachgehen und der Kommission und den zuständigen nationalen Behörden alle einschlägigen Informationen und mögliche Korrekturmaßnahmen mitteilen. Zudem sollten die Anbieter während des gesamten Lebenszyklus des Modells ein angemessenes Maß an Cybersicherheit für das Modell und seine physische Infrastruktur gewährleisten. Beim Schutz der Cybersicherheit im Zusammenhang mit systemischen Risiken, die mit böswilliger Nutzung oder böswilligen Angriffen verbunden sind, sollte der unbeabsichtigte Modelldatenverlust, die unerlaubte Bereitstellung, die Umgehung von Sicherheitsmaßnahmen und der Schutz vor Cyberangriffen, unbefugtem Zugriff oder Modelldiebstahl gebührend beachtet werden. Dieser Schutz könnte durch die Sicherung von Modellgewichten, Algorithmen, Servern und Datensätzen erleichtert werden, z. B. durch Betriebssicherheitsmaßnahmen für die Informationssicherheit, spezifische Cybersicherheitsstrategien, geeignete technische und etablierte Lösungen sowie Kontrollen des physischen Zugangs und des Cyberzugangs, die den jeweiligen Umständen und den damit verbundenen Risiken angemessen sind.

(116) Das Büro für Künstliche Intelligenz sollte die Ausarbeitung, Überprüfung und Anpassung von Praxisleitfäden unter Berücksichtigung internationaler Ansätze fördern und erleichtern. Alle Anbieter von KI-Modellen mit allgemeinem Verwendungszweck könnten ersucht werden, sich daran zu beteiligen. Um sicherzustellen, dass die Praxisleitfäden dem Stand der Technik entsprechen und unterschiedlichen Perspektiven gebührend Rechnung tragen, sollte das Büro für Künstliche Intelligenz bei der Ausarbeitung solcher Leitfäden mit den einschlägigen zuständigen nationalen Behörden zusammenarbeiten und könnte dabei gegebenenfalls Organisationen der Zivilgesellschaft und andere einschlägige Interessenträger und Sachverständige, einschließlich des wissenschaftlichen Gremiums, konsultieren. Die Praxisleitfäden sollten die Pflichten für Anbieter von KI-Modellen mit allgemeinem Verwendungszweck und von KI-Modellen mit allgemeinem Verwendungszweck, die systemische Risiken bergen, abdecken. Ferner sollten Praxisleitfäden im Zusammenhang mit systemischen Risiken dazu beitragen, dass eine Risikotaxonomie für Art und Wesen der systemischen Risiken auf Unionsebene, einschließlich ihrer Ursachen, festgelegt wird. Bei den Praxisleitfäden sollten auch auf spezifische Maßnahmen zur Risikobewertung und -minderung im Mittelpunkt stehen.

(117) Die Verhaltenskodizes sollten ein zentrales Instrument für die ordnungsgemäße Einhaltung der in dieser Verordnung für Anbieter von KI-Modellen mit allgemeinem Verwendungszweck vorgesehenen Pflichten darstellen. Die Anbieter sollten sich auf Verhaltenskodizes stützen können, um die Einhaltung der Pflichten nachzuweisen. Die Kommission kann im Wege von Durchführungsrechtsakten beschließen, einen Praxisleitfaden zu genehmigen und ihm eine allgemeine Gültigkeit in der Union zu verleihen oder alternativ gemeinsame Vorschriften für die Umsetzung der einschlägigen Pflichten festzulegen, wenn ein Verhaltenskodex bis zum Zeitpunkt der Anwendbarkeit dieser Verordnung nicht fertiggestellt werden kann oder dies vom Büro für Künstliche Intelligenz für nicht angemessen

erachtet wird. Sobald eine harmonisierte Norm veröffentlicht und als geeignet bewertet wurde, um die einschlägigen Pflichten des Büros für Künstliche Intelligenz abzudecken, sollte die Einhaltung einer harmonisierten europäischen Norm den Anbietern die Konformitätsvermutung begründen. Anbieter von KI-Modellen mit allgemeinem Verwendungszweck sollten darüber hinaus in der Lage sein, die Konformität mit angemessenen alternativen Mitteln nachzuweisen, wenn Praxisleitfäden oder harmonisierte Normen nicht verfügbar sind oder sie sich dafür entscheiden, sich nicht auf diese zu stützen.

(118) Mit dieser Verordnung werden KI-Systeme und KI-Modelle reguliert, indem einschlägigen Marktteilnehmern, die sie in der Union in Verkehr bringen, in Betrieb nehmen oder verwenden, bestimmte Anforderungen und Pflichten auferlegt werden, wodurch die Pflichten für Anbieter von Vermittlungsdiensten ergänzt werden, die solche Systeme oder Modelle in ihre unter die Verordnung (EU) 2022/2065 fallenden Dienste integrieren. Soweit solche Systeme oder Modelle in als sehr groß eingestufte Online-Plattformen oder als sehr groß eingestufte Online-Suchmaschinen eingebettet sind, unterliegen sie dem in der Verordnung (EU) 2022/2065 vorgesehenen Rahmen für das Risikomanagement. Folglich sollte angenommen werden, dass die entsprechenden Verpflichtungen dieser Verordnung erfüllt sind, es sei denn, in solchen Modellen treten erhebliche systemische Risiken auf, die nicht unter die Verordnung (EU) 2022/2065 fallen, und werden dort ermittelt. Im vorliegenden Rahmen sind Anbieter sehr großer Online-Plattformen und sehr großer Online-Suchmaschinen verpflichtet, potenzielle systemische Risiken, die sich aus dem Entwurf, dem Funktionieren und der Nutzung ihrer Dienste ergeben, einschließlich der Frage, wie der Entwurf der in dem Dienst verwendeten algorithmischen Systeme zu solchen Risiken beitragen kann, sowie systemische Risiken, die sich aus potenziellen Fehlanwendungen ergeben, zu bewerten. Diese Anbieter sind zudem verpflichtet, unter Wahrung der Grundrechte geeignete Risikominderungsmaßnahmen zu ergreifen.

(119) Angesichts des raschen Innovationstempos und der technologischen Entwicklung digitaler Dienste, die in den Anwendungsbereich verschiedener Instrumente des Unionsrechts fallen, können insbesondere unter Berücksichtigung der Verwendung durch ihre Nutzer und deren Wahrnehmung die dieser Verordnung unterliegenden KI-Systeme als Vermittlungsdienste oder Teile davon im Sinne der Verordnung (EU) 2022/2065 bereitgestellt werden, was technologieneutral ausgelegt werden sollte. Beispielsweise können KI-Systeme als Online-Suchmaschinen verwendet werden, insbesondere wenn ein KI-System wie ein Online-Chatbot grundsätzlich alle Websites durchsucht, die Ergebnisse anschließend in sein vorhandenes Wissen integriert und das aktualisierte Wissen nutzt, um eine einzige Ausgabe zu generieren, bei der verschiedene Informationsquellen zusammengeführt wurden.

(120) Zudem sind die Pflichten, die Anbietern und Betreibern bestimmter KI-Systeme mit dieser Verordnung auferlegt werden, um die Feststellung und Offenlegung zu ermöglichen, dass die Ausgaben dieser Systeme künstlich erzeugt oder manipuliert werden, von besonderer Bedeutung für die Erleichterung der wirksamen Umsetzung der Verordnung (EU) 2022/2065. Dies gilt insbesondere für die Pflichten der Anbieter sehr großer Online-Plattformen oder sehr großer Online-Suchmaschinen, systemische Risiken zu ermitteln und zu mindern, die aus der Verbreitung von künstlich erzeugten oder manipulierten Inhalten entstehen können, insbesondere das Risiko tatsächlicher oder vorhersehbarer negativer Auswirkungen auf demokratische Prozesse, den gesellschaftlichen Diskurs und Wahlprozesse, unter anderem durch Desinformation.

[sn909] Beratungsforum

(121) 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 und Innovation sowie Wettbewerbsfähigkeit und Wachstum im Binnenmarkt zu fördern. Die Einhaltung harmonisierter Normen im Sinne von Artikel 2 Nummer 1 Buchstabe c der Verordnung (EU) Nr. 1025/2012 des Europäischen Parlaments und des Rates ([41]), die normalerweise den Stand der Technik widerspiegeln sollten, sollte den Anbietern den Nachweis der Konformität mit den Anforderungen der vorliegenden Verordnung ermöglichen. Daher sollte eine ausgewogene Interessenvertretung unter Einbeziehung aller relevanten Interessenträger, insbesondere KMU, Verbraucherorganisationen sowie ökologischer und sozialer Interessenträger, bei der Entwicklung von Normen gemäß den Artikeln 5 und 6 der Verordnung (EU) Nr. 1025/2012, gefördert werden. Um die Einhaltung der Vorschriften zu erleichtern, sollten die Normungsaufträge von der Kommission unverzüglich erteilt werden. Bei der Ausarbeitung des Normungsauftrags sollte die Kommission das Beratungsforum und das KI-Gremium konsultieren, um einschlägiges Fachwissen einzuholen. In Ermangelung einschlägiger Fundstellen zu harmonisierten Normen sollte die Kommission jedoch im Wege von Durchführungsrechtsakten und nach Konsultation des Beratungsforums gemeinsame Spezifikationen für bestimmte Anforderungen im Rahmen dieser Verordnung festlegen können. Die gemeinsame Spezifikation sollte eine außergewöhnliche Ausweichlösung sein, um die Pflicht des Anbieters zur Einhaltung der Anforderungen dieser Verordnung zu erleichtern, wenn der Normungsauftrag von keiner der europäischen Normungsorganisationen angenommen wurde oder die einschlägigen harmonisierten Normen den Bedenken im Bereich der Grundrechte nicht ausreichend Rechnung tragen oder die harmonisierten Normen dem Auftrag nicht entsprechen oder es Verzögerungen bei der Annahme einer geeigneten harmonisierten Norm gibt. Ist eine solche Verzögerung bei der Annahme einer harmonisierten Norm auf die technische Komplexität dieser Norm

([41]) 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).

[se005] fällt unter

[se006] erfordert

zurückzuführen, so sollte die Kommission dies prüfen, bevor sie die Festlegung gemeinsamer Spezifikationen in Erwägung zieht. Die Kommission wird ermutigt, bei der Entwicklung gemeinsamer Spezifikationen mit internationalen Partnern und internationalen Normungsgremien zusammenzuarbeiten.

(122) Unbeschadet der Anwendung harmonisierter Normen und gemeinsamer Spezifikationen ist es angezeigt, dass für Anbieter von Hochrisiko-KI-Systemen, die mit Daten, in denen sich die besonderen geografischen, verhaltensbezogenen, kontextuellen oder funktionalen Rahmenbedingungen niederschlagen, unter denen sie verwendet werden sollen, trainiert und getestet wurden, die Vermutung der Konformität mit der einschlägigen Maßnahme gilt, die im Rahmen der in dieser Verordnung festgelegten Anforderungen an die Daten-Governance vorgesehen ist. Unbeschadet der in dieser Verordnung festgelegten Anforderungen an Robustheit und Genauigkeit sollte gemäß Artikel 54 Absatz 3 der Verordnung (EU) 2019/881 bei Hochrisiko-KI-Systemen, die im Rahmen eines Schemas für die Cybersicherheit gemäß der genannten Verordnung zertifiziert wurden oder für die eine Konformitätserklärung ausgestellt wurde und deren Fundstellen im *Amtsblatt der Europäischen Union* veröffentlicht wurden, vermutet werden, dass eine Übereinstimmung mit den Cybersicherheitsanforderungen der vorliegenden Verordnung gegeben ist, sofern das Cybersicherheitszertifikat oder die Konformitätserklärung oder Teile davon die Cybersicherheitsanforderungen dieser Verordnung abdecken. Dies gilt unbeschadet des freiwilligen Charakters dieses Schemas für die Cybersicherheit.

[sn505] Konformitätsbewertung

(123) 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.

(124) Damit für Akteure möglichst wenig Aufwand entsteht und etwaige Doppelarbeit vermieden wird, ist es angezeigt, dass bei Hochrisiko-KI-Systemen im Zusammenhang mit Produkten, die auf der Grundlage des neuen Rechtsrahmens unter bestehende Harmonisierungsrechtsvorschriften der Union fallen, im Rahmen der bereits in den genannten Rechtsvorschriften vorgesehenen Konformitätsbewertung bewertet wird, ob diese KI-Systeme den Anforderungen dieser Verordnung genügen. Die Anwendbarkeit der Anforderungen dieser Verordnung sollte daher die besondere Logik, Methodik oder allgemeine Struktur der Konformitätsbewertung gemäß den einschlägigen Harmonisierungsrechtsvorschriften der Union unberührt lassen.

[sn201] Biometrie

(125) Angesichts der Komplexität von Hochrisiko-KI-Systemen und der damit verbundenen Risiken ist es wichtig, ein angemessenes Konformitätsbewertungsverfahren für Hochrisiko-KI-Systeme, an denen notifizierte Stellen beteiligt sind, — die sogenannte Konformitätsbewertung durch Dritte — zu entwickeln. In Anbetracht der derzeitigen Erfahrung professioneller dem Inverkehrbringen vorgeschalteter Zertifizierer im Bereich der Produktsicherheit und der unterschiedlichen Art der damit verbundenen Risiken empfiehlt es sich jedoch, zumindest während der anfänglichen Anwendung dieser Verordnung für Hochrisiko-KI-Systeme, die nicht mit Produkten in Verbindung stehen, den Anwendungsbereich der Konformitätsbewertung durch Dritte einzuschränken. Daher sollte die Konformitätsbewertung solcher Systeme in der Regel vom Anbieter in eigener Verantwortung durchgeführt werden, mit Ausnahme von KI-Systemen, die für die Biometrie verwendet werden sollen.

(126) Damit KI-Systeme, falls vorgeschrieben, Konformitätsbewertungen 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, Nichtvorliegen von Interessenkonflikten und geeignete Anforderungen an die Cybersicherheit. Die Notifizierung dieser Stellen sollte von den zuständigen nationalen Behörden der Kommission und den anderen Mitgliedstaaten mittels des von der Kommission entwickelten und verwalteten elektronischen Notifizierungsinstruments gemäß Anhang I Artikel R23 des Beschlusses Nr. 768/2008/EG übermittelt werden.

(127) Im Einklang mit den Verpflichtungen der Union im Rahmen des Übereinkommens der Welthandelsorganisation über technische Handelshemmnisse ist es angemessen, die gegenseitige Anerkennung von Konformitätsbewertungsergebnissen zu erleichtern, die von den zuständigen Konformitätsbewertungsstellen unabhängig von dem Gebiet, in dem sie niedergelassen sind, generiert wurden, sofern diese nach dem Recht eines Drittlandes errichteten Konformitätsbewertungsstellen die geltenden Anforderungen dieser Verordnung erfüllen und die Union ein entsprechendes Abkommen geschlossen hat. In diesem Zusammenhang sollte die Kommission aktiv mögliche internationale Instrumente zu diesem Zweck prüfen und insbesondere den Abschluss von Abkommen über die gegenseitige Anerkennung mit Drittländern anstreben.

(128) Im Einklang mit dem allgemein anerkannten Begriff der wesentlichen Änderung von Produkten, für die Harmonisierungsvorschriften der Union gelten, ist es angezeigt, 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 betreffen, die nach dem Inverkehrbringen oder der Inbetriebnahme weiterhin dazulernen — d. h., sie passen automatisch an, wie die Funktionen ausgeführt werden —, sollten jedoch keine wesentliche Veränderung darstellen, sofern diese Änderungen vom Anbieter vorab festgelegt und zum Zeitpunkt der Konformitätsbewertung bewertet wurden.

[sn509] CE-Kennzeichnung

[sn202] Kritische Infrastruktur

(129) Hochrisiko-KI-Systeme sollten grundsätzlich mit der CE-Kennzeichnung versehen sein, aus der ihre Konformität mit dieser Verordnung hervorgeht, sodass sie frei im Binnenmarkt verkehren können. Bei in ein Produkt integrierten Hochrisiko-KI-Systemen sollte eine physische CE-Kennzeichnung angebracht werden, die durch eine digitale CE-Kennzeichnung ergänzt werden kann. Bei Hochrisiko-KI-Systemen, die nur digital bereitgestellt werden, sollte eine digitale CE-Kennzeichnung verwendet werden. Die Mitgliedstaaten sollten keine ungerechtfertigten Hindernisse für das Inverkehrbringen oder die Inbetriebnahme von Hochrisiko-KI-Systemen schaffen, die die in dieser Verordnung festgelegten Anforderungen erfüllen und mit der CE-Kennzeichnung versehen sind.

(130) Unter bestimmten Bedingungen kann die rasche Verfügbarkeit innovativer Technik für die Gesundheit und Sicherheit von Menschen, den Schutz der Umwelt und vor dem Klimawandel und die Gesellschaft insgesamt von entscheidender Bedeutung sein. Es ist daher angezeigt, dass die Aufsichtsbehörden aus außergewöhnlichen Gründen der öffentlichen Sicherheit, des Schutzes des Lebens und der Gesundheit natürlicher Personen, des Umweltschutzes und des Schutzes wichtiger Industrie- und Infrastrukturanlagen das Inverkehrbringen oder die Inbetriebnahme von KI-Systemen, die keiner Konformitätsbewertung unterzogen wurden, genehmigen könnten. In hinreichend begründeten Fällen gemäß dieser Verordnung können Strafverfolgungs- oder Katastrophenschutzbehörden ein bestimmtes Hochrisiko-KI-System ohne Genehmigung der Marktüberwachungsbehörde in Betrieb nehmen, sofern diese Genehmigung während der Verwendung oder im Anschluss daran unverzüglich beantragt wird.

[sn908] EU-Datenbank

[sn503] Betreiber

(131) Um die Arbeit der Kommission und der Mitgliedstaaten im KI-Bereich zu erleichtern und die Transparenz gegenüber der Öffentlichkeit zu erhöhen, sollten Anbieter von Hochrisiko-KI-Systemen, die nicht im Zusammenhang mit Produkten stehen, welche in den Anwendungsbereich einschlägiger Harmonisierungsrechtsvorschriften der Union fallen, und Anbieter, die der Auffassung sind, dass ein KI-System, das in den in einem Anhang dieser Verordnung aufgeführten Anwendungsfällen mit hohem Risiko aufgeführt ist, auf der Grundlage einer Ausnahme nicht hochriskant ist, dazu verpflichtet werden, sich und Informationen über ihr KI-System in einer von der Kommission einzurichtenden und zu verwaltenden EU-Datenbank zu registrieren. Vor der Verwendung eines KI-Systems, das in den in einem Anhang dieser Verordnung aufgeführten Anwendungsfällen mit hohem Risiko aufgeführt ist, sollten sich Betreiber von Hochrisiko-KI-Systemen, die Behörden, Einrichtungen oder sonstige Stellen sind, in dieser Datenbank registrieren und das System auswählen, dessen Verwendung sie planen. Andere Betreiber sollten berechtigt sein, dies freiwillig zu tun. Dieser Teil der EU-Datenbank sollte öffentlich und kostenlos zugänglich sein, und die Informationen sollten leicht zu navigieren, verständlich und maschinenlesbar sein. Die EU-Datenbank sollte außerdem benutzerfreundlich sein und beispielsweise die Suche, auch mit Stichwörtern, vorsehen, damit die breite Öffentlichkeit die einschlägigen Informationen finden kann, die bei der Registrierung von Hochrisiko-KI-Systemen einzureichen sind und die sich auf einen in einem Anhang dieser Verordnung aufgeführten Anwendungsfall der Hochrisiko-KI-Systeme, denen die betreffenden Hochrisiko-KI-Systeme entsprechen, beziehen. Jede wesentliche Veränderung von Hochrisiko-KI-Systemen sollte ebenfalls in der EU-Datenbank registriert werden. Bei Hochrisiko-KI-Systemen, die in den Bereichen Strafverfolgung, Migration, Asyl und Grenzkontrolle eingesetzt werden, sollten die Registrierungspflichten in einem sicheren nicht öffentlichen Teil der EU-Datenbank erfüllt werden. Der Zugang zu dem gesicherten nicht öffentlichen Teil sollte sich strikt auf die Kommission sowie auf die Marktüberwachungsbehörden und bei diesen auf ihren nationalen Teil dieser Datenbank beschränken. Hochrisiko-KI-Systeme im Bereich kritischer Infrastrukturen sollten nur auf nationaler Ebene registriert werden. Die Kommission sollte gemäß der Verordnung (EU) 2018/1725 als für die EU-Datenbank Verantwortlicher gelten. Um die volle Funktionsfähigkeit der EU-Datenbank zu gewährleisten, sollte das Verfahren für die Einrichtung der Datenbank auch die Entwicklung von funktionalen Spezifikationen durch die Kommission und einen unabhängigen Prüfbericht umfassen. Die Kommission sollte bei der Wahrnehmung ihrer Aufgaben als Verantwortliche für die EU-Datenbank die Risiken im Zusammenhang mit Cybersicherheit berücksichtigen. Um für ein Höchstmaß an Verfügbarkeit und Nutzung der EU-Datenbank durch die Öffentlichkeit zu sorgen, sollte die EU-Datenbank, einschließlich der über sie zur Verfügung gestellten Informationen, den Anforderungen der Richtlinie (EU) 2019/882 entsprechen.

(132) 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 und vorbehaltlich punktueller Ausnahmen, um den besonderen Erfordernissen der Strafverfolgung Rechnung zu tragen — 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 angemessen informierten, aufmerksamen und verständigen natürlichen Person aufgrund der Umstände und des Kontexts der Nutzung offensichtlich. Bei der Umsetzung dieser Pflicht sollten die Merkmale von natürlichen Personen, die aufgrund ihres Alters oder einer Behinderung schutzbedürftigen Gruppen angehören, berücksichtigt werden, soweit das KI-System auch mit diesen Gruppen interagieren soll. Darüber hinaus sollte natürlichen Personen mitgeteilt werden, wenn sie KI-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 etwa Geschlecht, Alter, Haarfarbe, Augenfarbe, Tätowierungen, persönliche Merkmale, ethnische Herkunft sowie persönliche Vorlieben und Interessen betreffen. Diese Informationen und Mitteilungen sollten für Menschen mit Behinderungen in entsprechend barrierefrei zugänglicher Form bereitgestellt werden.

[sn502] Anbieter

[sn503] Betreiber

(133) Eine Vielzahl von KI-Systemen kann große Mengen synthetischer Inhalte erzeugen, bei denen es für Menschen immer schwieriger wird, sie vom Menschen erzeugten und authentischen Inhalten zu unterscheiden. Die breite Verfügbarkeit und die zunehmenden Fähigkeiten dieser Systeme wirken sich erheblich auf die Integrität des Informationsökosystems und das ihm entgegengebrachte Vertrauen aus, weil neue Risiken in Bezug auf Fehlinformation und Manipulation in großem Maßstab, Betrug, Identitätsbetrug und Täuschung der Verbraucher entstehen. Angesichts dieser Auswirkungen, des raschen Tempos im Technologiebereich und der Notwendigkeit neuer Methoden und Techniken zur Rückverfolgung der Herkunft von Informationen sollten die Anbieter dieser Systeme verpflichtet werden, technische Lösungen zu integrieren, die die Kennzeichnung in einem maschinenlesbaren Format und die Feststellung ermöglichen, dass die Ausgabe von einem KI-System und nicht von einem Menschen erzeugt oder manipuliert wurde. Diese Techniken und Methoden sollten — soweit technisch möglich — hinreichend zuverlässig, interoperabel, wirksam und belastbar sein, wobei verfügbare Techniken, wie Wasserzeichen, Metadatenidentifizierungen, kryptografische Methoden zum Nachweis der Herkunft und Authentizität des Inhalts, Protokollierungsmethoden, Fingerabdrücke oder andere Techniken, oder eine Kombination solcher Techniken je nach Sachlage zu berücksichtigen sind. Bei der Umsetzung dieser Pflicht sollten die Anbieter auch die Besonderheiten und Einschränkungen der verschiedenen Arten von Inhalten und die einschlägigen technologischen Entwicklungen und Marktentwicklungen in diesem Bereich, die dem allgemein anerkannten Stand der Technik entsprechen, berücksichtigen. Solche Techniken und Methoden können auf der Ebene des KI-Systems oder der Ebene des KI-Modells, darunter KI-Modelle mit allgemeinem Verwendungszweck zur Erzeugung von Inhalten, angewandt werden, wodurch dem nachgelagerten Anbieter des KI-Systems die Erfüllung dieser Pflicht erleichtert wird. Um die Verhältnismäßigkeit zu wahren, sollte vorgesehen werden, dass diese Kennzeichnungspflicht weder für KI-Systeme, die in erster Linie eine unterstützende Funktion für die Standardbearbeitung ausführen, noch für KI-Systeme, die die vom Betreiber bereitgestellten Eingabedaten oder deren Semantik nicht wesentlich verändern, gilt.

(134) Neben den technischen Lösungen, die von den Anbietern von KI-Systemen eingesetzt werden, sollten Betreiber, die ein KI-System zum Erzeugen oder Manipulieren von Bild-, Audio- oder Videoinhalte verwenden, die wirklichen Personen, Gegenständen, Orten, Einrichtungen oder Ereignissen merklich ähneln und einer Person fälschlicherweise echt oder wahr erscheinen würden (Deepfakes), auch klar und deutlich offenlegen, dass die Inhalte künstlich erzeugt oder manipuliert wurden, indem sie die Ausgaben von KI entsprechend kennzeichnen und auf ihren künstlichen Ursprung hinweisen. Die Einhaltung dieser Transparenzpflicht sollte nicht so ausgelegt werden, dass sie darauf hindeutet, dass die Verwendung des KI-Systems oder seiner Ausgabe das Recht auf freie Meinungsäußerung und das Recht auf Freiheit der Kunst und Wissenschaft, die in der Charta garantiert sind, behindern, insbesondere wenn der Inhalt Teil eines offensichtlich kreativen, satirischen, künstlerischen, fiktionalen oder analogen Werks oder Programms ist und geeignete Schutzvorkehrungen für die Rechte und Freiheiten Dritter bestehen. In diesen Fällen beschränkt sich die in dieser Verordnung festgelegte Transparenzpflicht für Deepfakes darauf, das Vorhandenseins solcher erzeugten oder manipulierten Inhalte in geeigneter Weise offenzulegen, die die Darstellung oder den Genuss des Werks, einschließlich seiner normalen Nutzung und Verwendung, nicht beeinträchtigt und gleichzeitig den Nutzen und die Qualität des Werks aufrechterhält. Darüber hinaus ist es angezeigt, eine ähnliche Offenlegungspflicht in Bezug auf durch KI erzeugte oder manipulierte Texte anzustreben, soweit diese veröffentlicht werden, um die Öffentlichkeit über Angelegenheiten von öffentlichem Interesse zu informieren, es sei denn, die durch KI erzeugten Inhalte wurden einem Verfahren der menschlichen Überprüfung oder redaktionellen Kontrolle unterzogen und eine natürliche oder juristische Person trägt die redaktionelle Verantwortung für die Veröffentlichung der Inhalte.

(135) Unbeschadet des verbindlichen Charakters und der uneingeschränkten Anwendbarkeit der Transparenzpflichten kann die Kommission zudem die Ausarbeitung von Praxisleitfäden auf Unionsebene im Hinblick auf die Ermöglichung der wirksamen Umsetzung der Pflichten in Bezug auf die Feststellung und Kennzeichnung künstlich erzeugter oder manipulierter Inhalte erleichtern und fördern, auch um praktische Vorkehrungen zu unterstützen, mit denen gegebenenfalls die Feststellungsmechanismen zugänglich gemacht werden, die Zusammenarbeit mit anderen Akteuren entlang der Wertschöpfungskette erleichtert wird und Inhalte verbreitet oder ihre Echtheit und Herkunft überprüft werden, damit die Öffentlichkeit durch KI erzeugte Inhalte wirksam erkennen kann.

(136) Die Pflichten, die Anbietern und Betreibern bestimmter KI-Systeme mit dieser Verordnung auferlegt werden, die Feststellung und Offenlegung zu ermöglichen, dass die Ausgaben dieser Systeme künstlich erzeugt oder manipuliert werden, sind von besonderer Bedeutung für die Erleichterung der wirksamen Umsetzung der Verordnung (EU) 2022/2065. Dies gilt insbesondere für die Pflicht der Anbieter sehr großer Online-Plattformen oder sehr großer Online-Suchmaschinen, systemische Risiken zu ermitteln und zu mindern, die aus der Verbreitung von künstlich erzeugten oder manipulierten Inhalten entstehen können, insbesondere das Risiko tatsächlicher oder vorhersehbarer negativer Auswirkungen auf demokratische Prozesse, den gesellschaftlichen Diskurs und Wahlprozesse, unter anderem durch Desinformation. Die Anforderung gemäß dieser Verordnung, durch KI-Systeme erzeugte Inhalte zu kennzeichnen, berührt nicht die Pflicht in Artikel 16 Absatz 6 der Verordnung (EU) 2022/2065 für Anbieter von Hostingdiensten, gemäß Artikel 16 Absatz 1 der genannten Verordnung eingegangene Meldungen über illegale Inhalte zu bearbeiten, und sollte nicht die Beurteilung der Rechtswidrigkeit der betreffenden Inhalte und die Entscheidung darüber beeinflussen. Diese Beurteilung sollte ausschließlich anhand der Vorschriften für die Rechtmäßigkeit der Inhalte vorgenommen werden.

[sn503] Betreiber

(137) Die Einhaltung der Transparenzpflichten für die von dieser Verordnung erfassten KI-Systeme sollte nicht als Hinweis darauf ausgelegt werden, dass die Verwendung des KI-Systems oder seiner Ausgabe nach dieser Verordnung oder anderen Rechtsvorschriften der Union und der Mitgliedstaaten rechtmäßig ist, und sollte andere Transparenzpflichten für Betreiber von KI-Systemen, die im Unionsrecht oder im nationalen Recht festgelegt sind, unberührt lassen.

[sn506] KI-Reallabor

[sn504] Inverkehrbringen

(138) KI bezeichnet eine Reihe sich rasch entwickelnder Technologien, die eine Regulierungsaufsicht und einen sicheren und kontrollierten Raum für die Erprobung erfordern, wobei gleichzeitig eine verantwortungsvolle Innovation und die Integration geeigneter Schutzvorkehrungen und Risikominderungsmaßnahmen gewährleistet werden müssen. Um einen innovationsfördernden, zukunftssicheren und gegenüber Störungen widerstandsfähigen Rechtsrahmen sicherzustellen, sollten die Mitgliedstaaten sicherstellen, dass ihre zuständigen nationalen Behörden mindestens ein KI-Reallabor auf nationaler Ebene einrichten, um die Entwicklung und die Erprobung innovativer KI-Systeme vor deren Inverkehrbringen oder anderweitiger Inbetriebnahme unter strenger Regulierungsaufsicht zu erleichtern. Die Mitgliedstaaten könnten diese Pflicht auch erfüllen, indem sie sich an bereits bestehenden Reallaboren beteiligen oder ein Reallabor mit den zuständigen Behörden eines oder mehrerer Mitgliedstaaten gemeinsam einrichten, insoweit diese Beteiligung eine gleichwertige nationale Abdeckung für die teilnehmenden Mitgliedstaaten bietet. KI-Reallabore könnten in physischer, digitaler oder Hybrid-Form eingerichtet werden, und sie können physische sowie digitale Produkte umfassen. Die einrichtenden Behörden sollten ferner sicherstellen, dass die KI-Reallabore über angemessene Ressourcen für ihre Aufgaben, einschließlich finanzieller und personeller Ressourcen, verfügen.

[sn502] Anbieter

(139) Die Ziele der KI-Reallabore sollten in Folgendem 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 anderem einschlägigen Unionsrecht und dem nationalen Recht in Einklang stehen. Darüber hinaus sollten die KI-Reallabore darauf abzielen, die Rechtssicherheit für Innovatoren sowie die Aufsicht und das Verständnis der zuständigen Behörden in Bezug auf die Möglichkeiten, neu auftretenden Risiken und Auswirkungen der KI-Nutzung zu verbessern, das regulatorische Lernen für Behörden und Unternehmen zu erleichtern, unter anderem im Hinblick auf künftige Anpassungen des Rechtsrahmens, die Zusammenarbeit und den Austausch bewährter Praktiken mit den an dem KI-Reallabor beteiligten Behörden zu unterstützen und den Marktzugang zu beschleunigen, unter anderem indem Hindernisse für KMU, einschließlich Start-up-Unternehmen, abgebaut werden. KI-Reallabore sollten in der gesamten Union weithin verfügbar sein, und ein besonderes Augenmerk sollte auf ihre Zugänglichkeit für KMU, einschließlich Start-up-Unternehmen, gelegt 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 evidenzbasiertem 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. Alle erheblichen Risiken, die bei der Entwicklung und Erprobung solcher KI-Systeme festgestellt werden, sollten eine angemessene Risikominderung und, in Ermangelung dessen, die Aussetzung des Entwicklungs- und Erprobungsprozesses nach sich ziehen. Gegebenenfalls sollten die zuständigen nationalen Behörden, die KI-Reallabore einrichten, mit anderen einschlägigen Behörden zusammenarbeiten, einschließlich derjenigen, 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, Europäischer Digitaler Innovationszentren und einschlägiger Interessenträger und Organisationen der Zivilgesellschaft. Im Interesse einer unionsweit einheitlichen Umsetzung und der Erzielung von Größenvorteilen ist es angezeigt, dass gemeinsame Vorschriften für die Umsetzung von KI-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 werden, sollten anderes Recht, das die Einrichtung anderer Reallabore ermöglicht, unberührt lassen, um die Einhaltung anderen Rechts 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 am KI-Reallabor Beteiligten können Tests unter Realbedingungen auch im Rahmen des KI-Reallabors durchgeführt und beaufsichtigt werden.

(140) 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, 6 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 — ausschließlich unter bestimmten Bedingungen — personenbezogener Daten, die für andere Zwecke erhoben wurden, zur Entwicklung bestimmter KI-Systeme im öffentlichen Interesse innerhalb des KI-Reallabors durch die Anbieter und zukünftigen Anbieter im KI-Reallabor bilden. Alle anderen Pflichten von Verantwortlichen und Rechte betroffener Personen im Rahmen der Verordnungen (EU) 2016/679 und (EU) 2018/1725 und der Richtlinie (EU) 2016/680 gelten weiterhin. Insbesondere sollte diese Verordnung keine Rechtsgrundlage im Sinne des Artikels 22 Absatz 2 Buchstabe b der Verordnung (EU) 2016/679 und des Artikels 24 Absatz 2 Buchstabe b der Verordnung (EU) 2018/1725 bilden. Anbieter und zukünftige Anbieter im KI-Reallabor sollten angemessene Schutzvorkehrungen treffen und mit den zuständigen Behörden zusammenarbeiten, unter anderem indem sie deren Anleitung

folgen und zügig und nach Treu und Glauben handeln, um etwaige erhebliche Risiken für die Sicherheit, die Gesundheit und die Grundrechte, die bei der Entwicklung, bei der Erprobung und bei Versuchen in diesem Reallabor auftreten können, zu mindern.

[sn502] Anbieter

(141) Um den Prozess der Entwicklung und des Inverkehrbringens der in einem Anhang dieser Verordnung 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 Realbedingungen profitieren können, ohne sich an einem KI-Reallabor zu beteiligen. In solchen Fällen, unter Berücksichtigung der möglichen Folgen solcher Tests für Einzelpersonen, sollte jedoch sichergestellt werden, dass mit dieser Verordnung angemessene und ausreichende Garantien und Bedingungen für Anbieter oder zukünftige Anbieter eingeführt werden. Diese Garantien sollten unter anderem die Einholung der informierten Einwilligung natürlicher Personen in die Beteiligung an Tests unter Realbedingungen umfassen, mit Ausnahme der Strafverfolgung, wenn die Einholung der informierten 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 greift dieser nicht vor. Ferner ist es wichtig, die Risiken zu minimieren und die Aufsicht durch die zuständigen Behörden zu ermöglichen und daher von zukünftigen Anbietern zu verlangen, dass sie der zuständigen Marktüberwachungsbehörde einen Plan für einen Test unter Realbedingungen vorgelegt haben, die Tests — vorbehaltlich einiger begrenzter Ausnahmen — in den dafür vorgesehenen Abschnitten der EU-Datenbank zu registrieren, den Zeitraum zu begrenzen, in dem die Tests durchgeführt werden können, und zusätzliche Schutzmaßnahmen für Personen, die schutzbedürftigen Gruppen angehören, sowie eine schriftliche Einwilligung mit der Festlegung der Aufgaben und Zuständigkeiten der zukünftigen Anbieter und der Betreiber und eine wirksame Aufsicht durch zuständiges Personal, das an den Tests unter Realbedingungen beteiligt ist, zu verlangen. Darüber hinaus ist es angezeigt, zusätzliche Schutzmaßnahmen vorzusehen, um sicherzustellen, dass die Vorhersagen, Empfehlungen oder Entscheidungen des KI-Systems effektiv rückgängig gemacht und missachtet werden können, und dass personenbezogene Daten geschützt sind und gelöscht werden, wenn die Testteilnehmer ihre Einwilligung zur Teilnahme an den Tests widerrufen haben, und zwar unbeschadet ihrer Rechte als betroffene Personen nach dem Datenschutzrecht der Union. Was die Datenübermittlung betrifft, so ist es angezeigt vorzusehen, dass Daten, die zum Zweck von Tests unter Realbedingungen erhoben und verarbeitet wurden, nur dann an Drittstaaten übermittelt werden sollten, wenn angemessene und anwendbare Schutzmaßnahmen nach dem Unionsrecht umgesetzt wurden, insbesondere im Einklang mit den Grundlagen für die Übermittlung personenbezogener Daten nach dem Datenschutzrecht der Union, während für nicht personenbezogene Daten angemessene Schutzmaßnahmen im Einklang mit dem Unionsrecht, z. B. den Verordnungen (EU) 2022/868 ([42]) und (EU) 2023/2854 ([43]) des Europäischen Parlaments und des Rates eingerichtet wurden.

[sn908] EU-Datenbank

[sn503] Betreiber

(142) Um sicherzustellen, dass KI zu sozial und ökologisch vorteilhaften Ergebnissen führt, werden die Mitgliedstaaten ermutigt, Forschung und Entwicklung zu KI-Lösungen, die zu sozial und ökologisch vorteilhaften Ergebnissen beitragen, zu unterstützen und zu fördern, wie KI-gestützte Lösungen für mehr Barrierefreiheit für Personen mit Behinderungen, zur Bekämpfung sozioökonomischer Ungleichheiten oder zur Erreichung von Umweltzielen, indem ausreichend Ressourcen — einschließlich öffentlicher Mittel und Unionsmittel — bereitgestellt werden, und — soweit angebracht und sofern die Voraussetzungen und Zulassungskriterien erfüllt sind — insbesondere unter Berücksichtigung von Projekten, mit denen diese Ziele verfolgt werden. Diese Projekte sollten auf dem Grundsatz der interdisziplinären Zusammenarbeit zwischen KI-Entwicklern, Sachverständigen in den Bereichen Gleichstellung und Nichtdiskriminierung, Barrierefreiheit und Verbraucher-, Umwelt- und digitale Rechte sowie Wissenschaftlern beruhen.

(143) Um Innovationen zu fördern und zu schützen, ist es wichtig, die Interessen von KMU, einschließlich Start-up-Unternehmen, die Anbieter und Betreiber von KI-Systemen sind, besonders zu berücksichtigen. Zu diesem Zweck sollten die Mitgliedstaaten Initiativen ergreifen, die sich an diese Akteure richten, darunter auch Sensibilisierungs- und Informationsmaßnahmen. Die Mitgliedstaaten sollten KMU, einschließlich Start-up-Unternehmen, die ihren Sitz oder eine Zweigniederlassung in der Union haben, vorrangigen Zugang zu den KI-Reallaboren gewähren, soweit sie die Voraussetzungen und Zulassungskriterien erfüllen und ohne andere Anbieter und zukünftige Anbieter am Zugang zu den Reallaboren zu hindern, sofern die gleichen Voraussetzungen und Kriterien erfüllt sind. Die Mitgliedstaaten sollten bestehende Kanäle nutzen und gegebenenfalls neue Kanäle für die Kommunikation mit KMU, einschließlich Start-up-Unternehmen, Betreibern, anderen Innovatoren und gegebenenfalls Behörden einrichten, um KMU auf ihrem gesamten Entwicklungsweg zu unterstützen, indem sie ihnen Orientierungshilfe bieten und Fragen zur Durchführung dieser Verordnung beantworten. Diese Kanäle sollten gegebenenfalls zusammenarbeiten, um Synergien zu schaffen und eine Homogenität ihrer Leitlinien für KMU, einschließlich Start-up-Unternehmen, und Betreiber sicherzustellen. Darüber hinaus sollten die Mitgliedstaaten die Beteiligung von KMU und anderen einschlägigen Interessenträgern an der Entwicklung von Normen fördern. Außerdem sollten die besonderen Interessen und Bedürfnisse von Anbietern, die KMU, einschließlich

([42]) Verordnung (EU) 2022/868 des Europäischen Parlaments und des Rates vom 30. Mai 2022 über europäische Daten-Governance und zur Änderung der Verordnung (EU) 2018/1724 (Daten-Governance-Rechtsakt) (ABl. L 152 vom 3.6.2022, S. 1).

([43]) Verordnung (EU) 2023/2854 des Rates und des Europäischen Parlaments vom 13. Dezember 2023 über harmonisierte Vorschriften für einen fairen Datenzugang und eine faire Datennutzung sowie zur Änderung der Verordnung (EU) 2017/2394 und der Richtlinie (EU) 2020/1828 (Datenverordnung) (ABl. L, 2023/2854, 22.12.2023, ELI: http://data.europa.eu/eli/reg/2023/2854/oj).

[sn502] Anbieter

Start-up-Unternehmen, sind, bei der Festlegung der Gebühren für die Konformitätsbewertung durch die notifizierten Stellen berücksichtigt werden. Die Kommission sollte regelmäßig die Zertifizierungs- und Befolgungskosten für KMU, einschließlich Start-up-Unternehmen, durch transparente Konsultationen bewerten, und sie sollte mit den Mitgliedstaaten zusammenarbeiten, um diese Kosten zu senken. So können beispielsweise Übersetzungen im Zusammenhang mit der verpflichtenden Dokumentation und Kommunikation mit Behörden für Anbieter und andere Akteure, insbesondere die 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 Betreiber weitgehend verstanden wird. Um den besonderen Bedürfnissen von KMU, einschließlich Start-up-Unternehmen, gerecht zu werden, sollte die Kommission auf Ersuchen des KI-Gremiums standardisierte Vorlagen für die unter diese Verordnung fallenden Bereiche bereitstellen. Ferner sollte die Kommission die Bemühungen der Mitgliedstaaten ergänzen, indem sie eine zentrale Informationsplattform mit leicht nutzbaren Informationen über diese Verordnung für alle Anbieter und Betreiber bereitstellt, indem sie angemessene Informationskampagnen durchführt, um für die aus dieser Verordnung erwachsenden Pflichten zu sensibilisieren, und indem sie die Konvergenz bewährter Praktiken bei Vergabeverfahren im Zusammenhang mit KI-Systemen bewertet und fördert. Mittlere Unternehmen, die bis vor kurzem als kleine Unternehmen im Sinne des Anhangs der Empfehlung 2003/361/EG der Kommission ([44]) galten, sollten Zugang zu diesen Unterstützungsmaßnahmen haben, da diese neuen mittleren Unternehmen mitunter nicht über die erforderlichen rechtlichen Ressourcen und Ausbildung verfügen, um ein ordnungsgemäßes Verständnis und eine entsprechende Einhaltung dieser Verordnung zu gewährleisten.

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

(145) 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, einschließlich Start-up-Unternehmen, und notifizierten Stellen die Einhaltung ihrer Pflichten aus dieser Verordnung zu erleichtern, sollten insbesondere die Plattform für KI auf Abruf, die europäischen Zentren für digitale Innovation und die Test- und Versuchseinrichtungen, die von der Kommission und den Mitgliedstaaten auf Unionsebene bzw. auf nationaler Ebene eingerichtet werden, zur Durchführung dieser Verordnung beitragen. Die Plattform für KI auf Abruf, die europäischen Zentren für digitale Innovation und die Test- und Versuchseinrichtungen können Anbieter und notifizierte Stellen im Rahmen ihres jeweiligen Auftrags und ihrer jeweiligen Kompetenzbereiche insbesondere technisch und wissenschaftlich unterstützen.

(146) Angesichts der sehr geringen Größe einiger Akteure und um die Verhältnismäßigkeit in Bezug auf die Innovationskosten sicherzustellen, ist es darüber hinaus angezeigt, Kleinstunternehmen zu erlauben, eine der kostspieligsten Pflichten, nämlich die Einführung eines Qualitätsmanagementsystems, in vereinfachter Weise zu erfüllen, 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. Die Kommission sollte Leitlinien ausarbeiten, um die Elemente des Qualitätsmanagementsystems zu bestimmen, die von Kleinstunternehmen auf diese vereinfachte Weise zu erfüllen sind.

[sn901] Büro für Künstliche Intelligenz

(147) 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, so weit wie möglich den Zugang zu Test- und Versuchseinrichtungen erleichtert. Dies gilt insbesondere für Expertengremien, Fachlaboratorien und Referenzlaboratorien im Bereich Medizinprodukte gemäß den Verordnungen (EU) 2017/745 und (EU) 2017/746.

(148) Mit dieser Verordnung sollte ein Governance-Rahmen geschaffen werden, der sowohl die Koordinierung und Unterstützung der Anwendung dieser Verordnung auf nationaler Ebene als auch den Aufbau von Kapazitäten auf Unionsebene und die Integration von Interessenträgern im Bereich der KI ermöglicht. Für die wirksame Umsetzung und Durchsetzung dieser Verordnung ist ein Governance-Rahmen erforderlich, der es ermöglicht, zentrales Fachwissen auf Unionsebene zu koordinieren und aufzubauen. Per Kommissionbeschluss ([45]) wurde das Büro für Künstliche Intelligenz errichtet, dessen Aufgabe es ist, Fachwissen und Kapazitäten der Union im Bereich der KI zu entwickeln und zur Umsetzung des Unionsrechts im KI-Bereich beizutragen. Die Mitgliedstaaten sollten die Aufgaben des Büros für Künstliche Intelligenz erleichtern, um die Entwicklung von Fachwissen und Kapazitäten auf Unionsebene zu unterstützen und die Funktionsweise des digitalen Binnenmarkts zu stärken. Darüber hinaus sollten ein aus Vertretern der Mitgliedstaaten zusammengesetztes KI-Gremium, ein wissenschaftliches Gremium zur Integration der Wissenschaftsgemeinschaft und ein Beratungsforum für Beiträge von Interessenträgern zur

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

([45]) Beschluss C(2024) 390 der Kommission vom 24.1.2024 zur Errichtung des Europäischen Amts für künstliche Intelligenz.

[sn901] Büro für Künstliche Intelligenz

Durchführung dieser Verordnung auf Unionsebene und auf nationaler Ebene eingerichtet werden. Die Entwicklung von Fachwissen und Kapazitäten der Union sollte auch die Nutzung bestehender Ressourcen und Fachkenntnisse umfassen, insbesondere durch Synergien mit Strukturen, die im Rahmen der Durchsetzung anderen Rechts auf Unionsebene aufgebaut wurden, und Synergien mit einschlägigen Initiativen auf Unionsebene, wie dem Gemeinsamen Unternehmen EuroHPC und den KI-Test- und Versuchseinrichtungen im Rahmen des Programms „Digitales Europa".

(149) Um eine reibungslose, wirksame und harmonisierte Durchführung dieser Verordnung zu erleichtern, sollte ein KI-Gremium eingerichtet werden. Das KI-Gremium sollte die verschiedenen Interessen des KI-Ökosystems widerspiegeln und sich aus Vertretern der Mitgliedstaaten zusammensetzen. Das KI-Gremium sollte für eine Reihe von Beratungsaufgaben zuständig sein, einschließlich der Abgabe von Stellungnahmen, Empfehlungen, Ratschlägen oder Beiträgen zu Leitlinien zu Fragen im Zusammenhang mit der Durchführung dieser Verordnung — darunter zu Durchsetzungsfragen, technischen Spezifikationen oder bestehenden Normen in Bezug auf die in dieser Verordnung festgelegten Anforderungen — sowie der Beratung der Kommission und der Mitgliedstaaten und ihrer zuständigen nationalen Behörden in spezifischen Fragen im Zusammenhang mit KI. Um den Mitgliedstaaten eine gewisse Flexibilität bei der Benennung ihrer Vertreter im KI-Gremium zu geben, können diese Vertreter alle Personen sein, die öffentlichen Einrichtungen angehören, die über einschlägige Zuständigkeiten und Befugnisse verfügen sollten, um die Koordinierung auf nationaler Ebene zu erleichtern und zur Erfüllung der Aufgaben des KI-Gremiums beizutragen. Das KI-Gremium sollte zwei ständige Untergruppen einrichten, um Marktüberwachungsbehörden und notifizierenden Behörden für die Zusammenarbeit und den Austausch in Fragen, die die Marktüberwachung bzw. notifizierende Stellen 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 Artikel 33 der genannten Verordnung 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. Das KI-Gremium kann weitere ständige oder nichtständige Untergruppen einrichten, falls das für die Prüfung bestimmter Fragen zweckmäßig sein sollte. Das KI-Gremium sollte gegebenenfalls auch mit einschlägigen Einrichtungen, Sachverständigengruppen und Netzwerken der Union zusammenarbeiten, die im Zusammenhang mit dem einschlägigen Unionsrecht tätig sind, einschließlich insbesondere derjenigen, die im Rahmen des einschlägigen Unionsrechts über Daten, digitale Produkte und Dienstleistungen tätig sind.

[sn901] Büro für Künstliche Intelligenz

[sn909] Beratungsforum

(150) Im Hinblick auf die Einbeziehung von Interessenträgern in die Umsetzung und Anwendung dieser Verordnung sollte ein Beratungsforum eingerichtet werden, um das KI-Gremium und die Kommission zu beraten und ihnen technisches Fachwissen bereitzustellen. Um eine vielfältige und ausgewogene Vertretung der Interessenträger mit gewerblichen und nicht gewerblichen Interessen und — innerhalb der Kategorie mit gewerblichen Interessen — in Bezug auf KMU und andere Unternehmen zu gewährleisten, sollten in dem Beratungsforum unter anderem die Industrie, Start-up-Unternehmen, KMU, die Wissenschaft, die Zivilgesellschaft, einschließlich der Sozialpartner, sowie die Agentur für Grundrechte, die ENISA, das Europäische Komitee für Normung (CEN), das Europäische Komitee für elektrotechnische Normung (CENELEC) und das Europäische Institut für Telekommunikationsnormen (ETSI) vertreten sein.

(151) Zur Unterstützung der Umsetzung und Durchsetzung dieser Verordnung, insbesondere der Beobachtungstätigkeiten des Büros für Künstliche Intelligenz in Bezug auf KI-Modelle mit allgemeinem Verwendungszweck, sollte ein wissenschaftliches Gremium mit unabhängigen Sachverständigen eingerichtet werden. Die unabhängigen Sachverständigen, aus denen sich das wissenschaftliche Gremium zusammensetzt, sollten auf der Grundlage des aktuellen wissenschaftlichen oder technischen Fachwissens im KI-Bereich ausgewählt werden und ihre Aufgaben unparteiisch, objektiv und unter Achtung der Vertraulichkeit der bei der Durchführung ihrer Aufgaben und Tätigkeiten erhaltenen Informationen und Daten ausüben. Um eine Aufstockung der nationalen Kapazitäten, die für die wirksame Durchsetzung dieser Verordnung erforderlich sind, zu ermöglichen, sollten die Mitgliedstaaten für ihre Durchsetzungstätigkeiten Unterstützung aus dem Pool von Sachverständigen anfordern können, der das wissenschaftliche Gremium bildet.

(152) Um eine angemessene Durchsetzung in Bezug auf KI-Systeme zu unterstützen und die Kapazitäten der Mitgliedstaaten zu stärken, sollten Unionsstrukturen zur Unterstützung der Prüfung von KI eingerichtet und den Mitgliedstaaten zur Verfügung gestellt werden.

(153) Den Mitgliedstaaten kommt bei der Anwendung und Durchsetzung dieser Verordnung eine Schlüsselrolle zu. Dazu sollte jeder Mitgliedstaat mindestens eine notifizierende Behörde und mindestens eine Marktüberwachungsbehörde als zuständige nationale Behörden benennen, die die Anwendung und Durchführung dieser Verordnung beaufsichtigen. Die Mitgliedstaaten können beschließen, öffentliche Einrichtungen jeder Art zu benennen, die die Aufgaben der zuständigen nationalen Behörden im Sinne dieser Verordnung gemäß ihren spezifischen nationalen organisatorischen Merkmalen und Bedürfnissen wahrnehmen. Um die Effizienz der Organisation aufseiten der Mitgliedstaaten zu steigern und eine zentrale Anlaufstelle gegenüber der Öffentlichkeit und anderen Ansprechpartnern auf Ebene der Mitgliedstaaten und der Union einzurichten, sollte jeder Mitgliedstaat eine Marktüberwachungsbehörde als zentrale Anlaufstelle benennen.

[sn502] Anbieter

[sn507] Beobachtung nach dem Inverkehrbringen

(154) Die zuständigen nationalen Behörden sollten ihre Befugnisse unabhängig, unparteiisch und unvoreingenommen ausüben, um die Grundsätze der Objektivität ihrer Tätigkeiten und Aufgaben zu wahren und die Anwendung und Durchführung dieser Verordnung sicherzustellen. Die Mitglieder dieser Behörden sollten sich jeder Handlung enthalten, die mit ihren Aufgaben unvereinbar wäre, und sie sollten den Vertraulichkeitsvorschriften gemäß dieser Verordnung unterliegen.

(155) 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. Gegebenenfalls sollte die Beobachtung nach dem Inverkehrbringen eine Analyse der Interaktion mit anderen KI-Systemen, einschließlich anderer Geräte und Software, umfassen. Die Beobachtung nach dem Inverkehrbringen sollte nicht für sensible operative Daten von Betreibern, die Strafverfolgungsbehörden sind, gelten. Dieses System ist auch wichtig, damit den möglichen Risiken, die von KI-Systemen ausgehen, die nach dem Inverkehrbringen oder der Inbetriebnahme dazulernen, effizienter 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; damit sind Vorfälle oder Fehlfunktionen gemeint, die zum Tod oder zu schweren Gesundheitsschäden führen, schwerwiegende und irreversible Störungen der Verwaltung und des Betriebs kritischer Infrastrukturen, Verstöße gegen Verpflichtungen aus dem Unionsrecht, mit denen die Grundrechte geschützt werden sollen, oder schwere Sach- oder Umweltschäden.

(156) Zur Gewährleistung einer angemessenen und wirksamen Durchsetzung der Anforderungen und Pflichten gemäß dieser Verordnung, bei der es sich um 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 in der vorliegenden Verordnung und der Verordnung (EU) 2019/1020 festgelegten Durchsetzungsbefugnisse verfügen und ihre Befugnisse und Aufgaben unabhängig, unparteiisch und unvoreingenommen wahrnehmen. Obwohl die meisten KI-Systeme keinen spezifischen Anforderungen und Pflichten gemäß der vorliegenden 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 beaufsichtigten Einrichtungen, ihre Aufgaben unabhängig wahrzunehmen, nicht beeinträchtigen, wenn eine solche Unabhängigkeit nach dem Unionsrecht erforderlich ist.

(157) 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 Gleichbehandlungsstellen 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 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.

(158) 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 über Finanzdienstleistungen zu gewährleisten, sollten die für die Beaufsichtigung und Durchsetzung jener Rechtsvorschriften zuständigen Behörden, insbesondere die zuständigen Behörden im Sinne der Verordnung (EU) Nr. 575/2013 des Europäischen Parlaments und des Rates ([46]) und der Richtlinien 2008/48/EG ([47]), 2009/138/EG ([48]), 2013/36/EU ([49]), 2014/17/EU ([50]) und (EU) 2016/97 ([51]) des Europäischen Parlaments und des

([46]) Verordnung (EU) Nr. 575/2013 des Europäischen Parlaments und des Rates vom 26. Juni 2013 über Aufsichtsanforderungen an Kreditinstitute und Wertpapierfirmen und zur Änderung der Verordnung (EU) Nr. 648/2012 (ABl. L 176 vom 27.6.2013, S. 1).

([47]) Richtlinie 2008/48/EG des Europäischen Parlaments und des Rates vom 23. April 2008 über Verbraucherkreditverträge und zur Aufhebung der Richtlinie 87/102/EWG des Rates (ABl. L 133 vom 22.5.2008, S. 66).

([48]) Richtlinie 2009/138/EG des Europäischen Parlaments und des Rates vom 25. November 2009 betreffend die Aufnahme und Ausübung der Versicherungs- und der Rückversicherungstätigkeit (Solvabilität II) (ABl. L 335 vom 17.12.2009, S. 1).

([49]) 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).

([50]) Richtlinie 2014/17/EU des Europäischen Parlaments und des Rates vom 4. Februar 2014 über Wohnimmobilienkreditverträge für Verbraucher und zur Änderung der Richtlinien 2008/48/EG und 2013/36/EU und der Verordnung (EU) Nr. 1093/2010 (ABl. L 60 vom 28.2.2014, S. 34).

([51]) Richtlinie (EU) 2016/97 des Europäischen Parlaments und des Rates vom 20. Januar 2016 über Versicherungsvertrieb (ABl. L 26 vom 2.2.2016, S. 19).

Rates, im Rahmen ihrer jeweiligen Zuständigkeiten auch als zuständige Behörden für die Beaufsichtigung der Durchführung 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 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 des einschlägigen Unionsrechts über Finanzdienstleistungen integriert werden können. Es ist angezeigt, vorzusehen, dass die nationalen Behörden, die für die Aufsicht über unter die Richtlinie 2013/36/EU fallende Kreditinstitute zuständig sind, welche an dem mit der Verordnung (EU) Nr. 1024/2013 des Rates ([52]) 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 der vorliegenden Verordnung und den Vorschriften für Kreditinstitute, die unter die Richtlinie 2013/36/EU 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 Beobachtungspflicht der Betreiber von Hochrisiko-KI-Systemen in Betracht gezogen 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 und Versicherungsvermittler gemäß der Richtlinie (EU) 2016/97 sowie für andere Arten von Finanzinstituten gelten, die Anforderungen in Bezug auf ihre Regelungen oder Verfahren der internen Unternehmensführung unterliegen, die gemäß einschlägigem Unionsrecht der Union über Finanzdienstleistungen festgelegt wurden, um Kohärenz und Gleichbehandlung im Finanzsektor sicherzustellen.

[sn502] Anbieter

[sn503] Betreiber

(159) Jede Marktüberwachungsbehörde für Hochrisiko-KI-Systeme im Bereich der Biometrie, die in einem Anhang zu dieser Verordnung aufgeführt sind, sollte — soweit diese Systeme für die Zwecke der Strafverfolgung, von Migration, Asyl und Grenzkontrolle oder von Rechtspflege und demokratischen Prozessen eingesetzt werden — über wirksame Ermittlungs- und Korrekturbefugnisse verfügen, einschließlich mindestens der Befugnis, Zugang zu allen personenbezogenen Daten, die verarbeitet werden, und zu allen Informationen, die für die Ausübung ihrer Aufgaben erforderlich sind, zu erhalten. Die Marktüberwachungsbehörden sollten in der Lage sein, ihre Befugnisse in völliger Unabhängigkeit auszuüben. Jede Beschränkung ihres Zugangs zu sensiblen operativen Daten im Rahmen dieser Verordnung sollte die Befugnisse unberührt lassen, die ihnen mit der Richtlinie (EU) 2016/680 übertragen wurden. Kein Ausschluss der Offenlegung von Daten gegenüber nationalen Datenschutzbehörden im Rahmen dieser Verordnung sollte die derzeitigen oder künftigen Befugnisse dieser Behörden über den Geltungsbereich dieser Verordnung hinaus beeinträchtigen.

[sn901] Büro für Künstliche Intelligenz

(160) Die Marktüberwachungsbehörden und die Kommission sollten gemeinsame Tätigkeiten, einschließlich gemeinsamer Untersuchungen, vorschlagen können, die von den Marktüberwachungsbehörden oder von den Marktüberwachungsbehörden gemeinsam mit der Kommission durchgeführt werden, um Konformität zu fördern, Nichtkonformität festzustellen, zu sensibilisieren und Orientierung zu dieser Verordnung und bestimmten Kategorien von Hochrisiko-KI-Systemen bereitzustellen, bei denen festgestellt wird, dass sie in zwei oder mehr Mitgliedstaaten ein ernstes Risiko darstellen. Gemeinsame Tätigkeiten zur Förderung der Konformität sollten im Einklang mit Artikel 9 der Verordnung (EU) 2019/1020 durchgeführt werden. Das Büro für Künstliche Intelligenz sollte die Koordinierung gemeinsamer Untersuchungen unterstützen.

(161) Die Verantwortlichkeiten und Zuständigkeiten auf Unionsebene und nationaler Ebene in Bezug auf KI-Systeme, die auf KI-Modellen mit allgemeinem Verwendungszweck aufbauen, müssen präzisiert werden. Um sich überschneidende Zuständigkeiten zu vermeiden, sollte die Aufsicht für KI-Systeme, die auf KI-Modellen mit allgemeinem Verwendungszweck beruhen und bei denen das Modell und das System vom selben Anbieter bereitgestellt werden,

([52]) Verordnung (EU) Nr. 1024/2013 des Rates vom 15. Oktober 2013 zur Übertragung besonderer Aufgaben im Zusammenhang mit der Aufsicht über Kreditinstitute auf die Europäische Zentralbank (ABl. L 287 vom 29.10.2013, S. 63).

[sn901] Büro für Künstliche Intelligenz

auf der Unionsebene durch das Büro für Künstliche Intelligenz erfolgen, das für diesen Zweck über die Befugnisse einer Marktüberwachungsbehörde im Sinne der Verordnung (EU) 2019/1020 verfügen sollte. In allen anderen Fällen sollten die nationalen Marktüberwachungsbehörden weiterhin für die Aufsicht über KI-Systeme zuständig sein. Bei KI-Systemen mit allgemeinem Verwendungszweck, die von Betreibern direkt für mindestens einen Zweck verwendet werden können, der als hochriskant eingestuft wird, sollten die Marktüberwachungsbehörden jedoch mit dem Büro für Künstliche Intelligenz zusammenarbeiten, um Konformitätsbewertungen durchzuführen, und sie sollten KI-Gremium und andere Marktüberwachungsbehörden entsprechend informieren. Darüber hinaus sollten Marktüberwachungsbehörden das Büro für Künstliche Intelligenz um Unterstützung ersuchen können, wenn die Marktüberwachungsbehörde nicht in der Lage ist, eine Untersuchung zu einem Hochrisiko-KI-System abzuschließen, weil sie keinen Zugang zu bestimmten Informationen im Zusammenhang mit dem KI-Modell mit allgemeinem Verwendungszweck, auf dem das Hochrisiko-KI-System beruht, haben. In diesen Fällen sollte das Verfahren bezüglich grenzübergreifender Amtshilfe nach Kapitel VI der Verordnung (EU) 2019/1020 entsprechend Anwendung finden.

[sn502] Anbieter

(162) Um das zentralisierte Fachwissen der Union und Synergien auf Unionsebene bestmöglich zu nutzen, sollte die Kommission für die Aufsicht und die Durchsetzung der Pflichten der Anbieter von KI-Modellen mit allgemeinem Verwendungszweck zuständig sein. Das Büro für Künstliche Intelligenz sollte alle erforderlichen Maßnahmen durchführen können, um die wirksame Umsetzung dieser Verordnung im Hinblick auf KI-Modelle mit allgemeinem Verwendungszweck zu überwachen. Es sollte mögliche Verstöße gegen die Vorschriften für Anbieter von KI-Modellen mit allgemeinem Verwendungszweck sowohl auf eigene Initiative, auf der Grundlage der Ergebnisse seiner Überwachungstätigkeiten, als auch auf Anfrage von Marktüberwachungsbehörden gemäß den in dieser Verordnung festgelegten Bedingungen untersuchen können. Zur Unterstützung einer wirksamen Überwachung durch das Büro für Künstliche Intelligenz sollte die Möglichkeit vorgesehen werden, dass nachgelagerte Anbieter Beschwerden über mögliche Verstöße gegen die Vorschriften für Anbieter von KI-Modellen und -Systemen mit allgemeinem Verwendungszweck einreichen können.

(163) Um die Governance-Systeme für KI-Modelle mit allgemeinem Verwendungszweck zu ergänzen, sollte das wissenschaftliche Gremium die Überwachungstätigkeiten des Büros für Künstliche Intelligenz unterstützen; dazu kann es in bestimmten Fällen qualifizierte Warnungen an das Büro für Künstliche Intelligenz richten, die Folgemaßnahmen wie etwa Untersuchungen auslösen. Dies sollte der Fall sein, wenn das wissenschaftliche Gremium Grund zu der Annahme hat, dass ein KI-Modell mit allgemeinem Verwendungszweck ein konkretes und identifizierbares Risiko auf Unionsebene darstellt. Außerdem sollte dies der Fall sein, wenn das wissenschaftliche Gremium Grund zu der Annahme hat, dass ein KI-Modell mit allgemeinem Verwendungszweck die Kriterien erfüllt, die zu einer Einstufung als KI-Modell mit allgemeinem Verwendungszweck mit systemischem Risiko führen würde. Um dem wissenschaftlichen Gremium die Informationen zur Verfügung zu stellen, die für die Ausübung dieser Aufgaben erforderlich sind, sollte es einen Mechanismus geben, wonach das wissenschaftliche Gremium die Kommission ersuchen kann, Unterlagen oder Informationen von einem Anbieter anzufordern.

(164) Das Büro für Künstliche Intelligenz sollte die erforderlichen Maßnahmen ergreifen können, um die wirksame Umsetzung und die Einhaltung der in dieser Verordnung festgelegten Pflichten der Anbieter von KI-Modellen mit allgemeinem Verwendungszweck zu überwachen. Das Büro für Künstliche Intelligenz sollte mögliche Verstöße im Einklang mit den in dieser Verordnung vorgesehenen Befugnissen untersuchen können, unter anderem indem es Unterlagen und Informationen anfordert, Bewertungen durchführt und Maßnahmen von Anbietern von KI-Modellen mit allgemeinem Verwendungszweck verlangt. Was die Durchführung von Bewertungen betrifft, so sollte das Büro für Künstliche Intelligenz unabhängige Sachverständige mit der Durchführung der Bewertungen in seinem Namen beauftragen können, damit unabhängiges Fachwissen genutzt werden kann. Die Einhaltung der Pflichten sollte durchsetzbar sein, unter anderem durch die Aufforderung zum Ergreifen angemessener Maßnahmen, einschließlich Risikominderungsmaßnahmen im Fall von festgestellten systemischen Risiken, sowie durch die Einschränkung der Bereitstellung des Modells auf dem Markt, die Rücknahme des Modells oder den Rückruf des Modells. Als Schutzmaßnahme, die erforderlichenfalls über die in dieser Verordnung vorgesehenen Verfahrensrechte hinausgeht, sollten die Anbieter von KI-Modellen mit allgemeinem Verwendungszweck über die in Artikel 18 der Verordnung (EU) 2019/1020 vorgesehenen Verfahrensrechte verfügen, die — unbeschadet in der vorliegenden Verordnung vorgesehener spezifischerer Verfahrensrechte — entsprechend gelten sollten.

(165) Die Entwicklung anderer KI-Systeme als Hochrisiko-KI-Systeme gemäß den Anforderungen dieser Verordnung kann zu einer stärkeren Verbreitung ethischer und vertrauenswürdiger KI in der Union führen. Anbieter von KI-Systemen, die kein hohes Risiko bergen, sollten angehalten werden, Verhaltenskodizes — einschließlich zugehöriger Governance-Mechanismen — zu erstellen, um eine freiwillige Anwendung einiger oder aller der für Hochrisiko-KI-Systeme geltenden Anforderungen zu fördern, die angesichts der Zweckbestimmung der Systeme und des niedrigeren Risikos angepasst werden, und unter Berücksichtigung der verfügbaren technischen Lösungen und bewährten Verfahren der Branche wie Modell- und Datenkarten. Darüber hinaus sollten die Anbieter und gegebenenfalls die Betreiber aller KI-Systeme, ob mit hohem Risiko oder nicht, und aller KI-Modelle auch ermutigt werden, freiwillig zusätzliche Anforderungen anzuwenden, z. B. in Bezug auf die Elemente der Ethikleitlinien der

[sn801] KI-Kompetenz

Union für vertrauenswürdige KI, die ökologische Nachhaltigkeit, Maßnahmen für KI-Kompetenz, die inklusive und vielfältige Gestaltung und Entwicklung von KI-Systemen, unter anderem mit Schwerpunkt auf schutzbedürftige Personen und die Barrierefreiheit für Menschen mit Behinderungen, die Beteiligung der Interessenträger, gegebenenfalls mit Einbindung einschlägiger Interessenträger wie Unternehmensverbänden und Organisationen der Zivilgesellschaft, Wissenschaft, Forschungsorganisationen, Gewerkschaften und Verbraucherschutzorganisationen an der Konzeption und Entwicklung von KI-Systemen und die Vielfalt der Entwicklungsteams, einschließlich einer ausgewogenen Vertretung der Geschlechter. Um sicherzustellen, dass die freiwilligen Verhaltenskodizes wirksam sind, sollten sie auf klaren Zielen und zentralen Leistungsindikatoren zur Messung der Verwirklichung dieser Ziele beruhen. Sie sollten außerdem in inklusiver Weise entwickelt werden, gegebenenfalls unter Einbeziehung einschlägiger Interessenträger wie Unternehmensverbände und Organisationen der Zivilgesellschaft, Wissenschaft, Forschungsorganisationen, Gewerkschaften und Verbraucherschutzorganisationen. 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.

(166) 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 für Hochrisiko-KI-Systeme erfüllen müssen, dennoch sicher sind, wenn sie in Verkehr gebracht oder in Betrieb genommen werden. Um zu diesem Ziel beizutragen, würde die Verordnung (EU) 2023/988 des Europäischen Parlaments und des Rates ([53]) als Sicherheitsnetz dienen.

(167) 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 gemäß dem Unionsrecht und dem nationalen Recht die Vertraulichkeit der im Rahmen der Wahrnehmung ihrer Aufgaben erlangten Informationen und Daten wahren. Sie sollten ihre Aufgaben und Tätigkeiten so ausüben, dass insbesondere die Rechte des geistigen Eigentums, vertrauliche Geschäftsinformationen und Geschäftsgeheimnisse, die wirksame Durchführung dieser Verordnung, die öffentlichen und nationalen Sicherheitsinteressen, die Integrität von Straf- und Verwaltungsverfahren und die Integrität von Verschlusssachen geschützt werden.

[sn502] Anbieter

(168) Die Einhaltung dieser Verordnung sollte durch die Verhängung von Sanktionen und anderen Durchsetzungsmaßnahmen durchsetzbar sein. Die Mitgliedstaaten sollten alle erforderlichen Maßnahmen ergreifen, um sicherzustellen, dass die Bestimmungen dieser Verordnung durchgeführt werden, und dazu unter anderem wirksame, verhältnismäßige und abschreckende Sanktionen für Verstöße festlegen und das Verbot der Doppelbestrafung befolgen. Um die verwaltungsrechtlichen Sanktionen für Verstöße gegen diese Verordnung zu verschärfen und zu harmonisieren, sollten Obergrenzen für die Festsetzung der Geldbußen bei bestimmten Verstößen festgelegt werden. Bei der Bemessung der Höhe der Geldbußen sollten die Mitgliedstaaten in jedem Einzelfall alle relevanten Umstände der jeweiligen Situation berücksichtigen, insbesondere die Art, die Schwere und die Dauer des Verstoßes und seiner Folgen sowie die Größe des Anbieters, vor allem wenn es sich bei diesem um ein KMU — einschließlich eines Start-up-Unternehmens — handelt. Der Europäische Datenschutzbeauftragte sollte befugt sein, gegen Organe, Einrichtungen und sonstige Stellen der Union, die in den Anwendungsbereich dieser Verordnung fallen, Geldbußen zu verhängen.

[sn503] Betreiber

(169) Die Einhaltung der mit dieser Verordnung auferlegten Pflichten für Anbieter von KI-Modellen mit allgemeinem Verwendungszweck sollte unter anderem durch Geldbußen durchgesetzt werden können. Zu diesem Zweck sollten Geldbußen in angemessener Höhe für Verstöße gegen diese Pflichten, einschließlich der Nichteinhaltung der von der Kommission gemäß dieser Verordnung verlangten Maßnahmen, festgesetzt werden, vorbehaltlich angemessener Verjährungsfristen im Einklang mit dem Grundsatz der Verhältnismäßigkeit. Alle Beschlüsse, die die Kommission auf der Grundlage dieser Verordnung fasst, unterliegen der Überprüfung durch den Gerichtshof der Europäischen Union im Einklang mit dem AEUV, einschließlich der Befugnis des Gerichtshofs zu unbeschränkter Ermessensnachprüfung hinsichtlich Zwangsmaßnahmen im Einklang mit Artikel 261 AEUV.

(170) Im Unionsrecht und im nationalen Recht sind bereits wirksame Rechtsbehelfe für natürliche und juristische Personen vorgesehen, deren Rechte und Freiheiten durch die Nutzung von KI-Systemen beeinträchtigt werden. Unbeschadet dieser Rechtsbehelfe sollte jede natürliche oder juristische Person, die Grund zu der Annahme hat, dass gegen diese Verordnung verstoßen wurde, befugt sein, bei der betreffenden Marktüberwachungsbehörde eine Beschwerde einzureichen.

(171) Betroffene Personen sollten das Recht haben, eine Erklärung zu erhalten, wenn eine Entscheidung eines Betreibers überwiegend auf den Ausgaben bestimmter Hochrisiko-KI-systeme beruht, die in den Geltungsbereich dieser Verordnung fallen, und wenn diese Entscheidung Rechtswirkungen entfaltet oder diese Personen in ähnlicher Weise

([53]) Verordnung (EU) 2023/988 des Europäischen Parlaments und des Rates vom 10. Mai 2023 über die allgemeine Produktsicherheit, zur Änderung der Verordnung (EU) Nr. 1025/2012 des Europäischen Parlaments und des Rates und der Richtlinie (EU) 2020/1828 des Europäischen Parlaments und des Rates sowie zur Aufhebung der Richtlinie 2001/95/EG des Europäischen Parlaments und des Rates und der Richtlinie 87/357/EWG des Rates (ABl. L 135 vom 23.5.2023, S. 1).

wesentlich beeinträchtigt, und zwar so, dass sie ihrer Ansicht nach negative Auswirkungen auf ihre Gesundheit, ihre Sicherheit oder ihre Grundrechte hat. Diese Erklärung sollte klar und aussagekräftig sein, und sie sollte eine Grundlage bieten, auf der die betroffenen Personen ihre Rechte ausüben können. Das Recht auf eine Erklärung sollte nicht für die Nutzung von KI-Systemen gelten, für die sich aus dem Unionsrecht oder dem nationalen Recht Ausnahmen oder Beschränkungen ergeben, und es sollte nur insoweit gelten, als es nicht bereits in anderem Unionsrecht vorgesehen ist.

(172) Personen, die als Hinweisgeber in Bezug auf die in dieser Verordnung genannten Verstöße auftreten, sollten durch das Unionsrecht geschützt werden. Für die Meldung von Verstößen gegen diese Verordnung und den Schutz von Personen, die solche Verstöße melden, sollte daher die Richtlinie (EU) 2019/1937 des Europäischen Parlaments und des Rates ([54]) gelten.

(173) Damit der Regelungsrahmen erforderlichenfalls angepasst werden kann, sollte der Kommission die Befugnis übertragen werden, gemäß Artikel 290 AEUV Rechtsakte zur Änderung der Bedingungen, unter denen ein KI-System nicht als Hochrisiko-System einzustufen ist, der Liste der Hochrisiko-KI-Systeme, der Bestimmungen über die technische Dokumentation, des Inhalts der EU-Konformitätserklärung, der Bestimmungen über die Konformitätsbewertungsverfahren, der Bestimmungen zur Festlegung der Hochrisiko-KI-Systeme, für die das Konformitätsbewertungsverfahren auf der Grundlage der Bewertung des Qualitätsmanagementsystems und der technischen Dokumentation gelten sollte, der Schwellenwerte, Benchmarks und Indikatoren — auch durch Ergänzung dieser Benchmarks und Indikatoren — in den Vorschriften für die Einstufung von KI-Modellen mit allgemeinem Verwendungszweck mit systemischem Risiko, der Kriterien für die Benennung von KI-Modellen mit allgemeinem Verwendungszweck mit systemischem Risiko, der technischen Dokumentation für Anbieter von KI-Modellen mit allgemeinem Verwendungszweck und der Transparenzinformationen für Anbieter von KI-Modellen mit allgemeinem Verwendungszweck zu erlassen. 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 ([55]) 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.

(174) Angesichts der raschen technologischen Entwicklungen und des für die wirksame Anwendung dieser Verordnung erforderlichen technischen Fachwissens sollte die Kommission diese Verordnung bis zum 2. August 2029 und danach alle vier Jahre bewerten und überprüfen und dem Europäischen Parlament und dem Rat darüber Bericht erstatten. Darüber hinaus sollte die Kommission — unter Berücksichtigung der Auswirkungen auf den Geltungsbereich dieser Verordnung — einmal jährlich beurteilen, ob es notwendig ist, die Liste der Hochrisiko-KI-Systeme und die Liste der verbotenen Praktiken zu ändern. Außerdem sollte die Kommission bis zum 2. August 2028 und danach alle vier Jahre die Notwendigkeit einer Änderung der Liste der Hochrisikobereiche im Anhang dieser Verordnung, die KI-Systeme im Geltungsbereich der Transparenzpflichten, die Wirksamkeit des Aufsichts- und Governance-Systems und die Fortschritte bei der Entwicklung von Normungsdokumenten zur energieeffizienten Entwicklung von KI-Modellen mit allgemeinem Verwendungszweck, einschließlich der Notwendigkeit weiterer Maßnahmen oder Handlungen, bewerten und dem Europäischen Parlament und dem Rat darüber Bericht erstatten. Schließlich sollte die Kommission bis zum 2. August 2028 und danach alle drei Jahre eine Bewertung der Folgen und der Wirksamkeit der freiwilligen Verhaltenskodizes durchführen, mit denen die Anwendung der für Hochrisiko-KI-Systeme vorgesehenen Anforderungen bei anderen KI-Systemen als Hochrisiko-KI-Systemen und möglicherweise auch zusätzlicher Anforderungen an solche KI-Systeme gefördert werden soll.

(175) Zur Gewährleistung einheitlicher Bedingungen für die Durchführung dieser Verordnung sollten der Kommission Durchführungsbefugnisse übertragen werden. Diese Befugnisse sollten gemäß der Verordnung (EU) Nr. 182/2011 des Europäischen Parlaments und des Rates ([56]) ausgeübt werden.

(176) Da das Ziel dieser Verordnung, nämlich die Verbesserung der Funktionsweise des Binnenmarkts und die Förderung der Einführung einer auf den Menschen ausgerichteten und vertrauenswürdigen KI bei gleichzeitiger Gewährleistung eines hohen Maßes an Schutz der Gesundheit, der Sicherheit, der in der Charta verankerten Grundrechte, einschließlich Demokratie, Rechtsstaatlichkeit und Schutz der Umwelt vor schädlichen Auswirkungen von KI-Systemen in der Union, und der Förderung von Innovation, von den Mitgliedstaaten nicht ausreichend verwirklicht werden kann, sondern vielmehr wegen des Umfangs oder der Wirkungen der Maßnahme auf

([54]) Richtlinie (EU) 2019/1937 des Europäischen Parlaments und des Rates vom 23. Oktober 2019 zum Schutz von Personen, die Verstöße gegen das Unionsrecht melden (ABl. L 305 vom 26.11.2019, S. 17).
([55]) ABl. L 123 vom 12.5.2016, S. 1.
([56]) 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).

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.

[sn503] Betreiber
[sn502] Anbieter
[sn403] 2. August 2026
[sn401] 2. Februar 2025
[sn402] 2. August 2025

(177) 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 ist angezeigt, klarzustellen, dass der Begriff der erheblichen 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. Ausnahmsweise und im Lichte der öffentlichen Rechenschaftspflicht sollten Betreiber von KI-Systemen, die Komponenten der in einem Anhang zu dieser Verordnung aufgeführten durch Rechtsakte eingerichteten IT-Großsysteme sind, und Betreiber von Hochrisiko-KI-Systemen, die von Behörden genutzt werden sollen, die erforderlichen Schritte unternehmen, um den Anforderungen dieser Verordnung bis Ende 2030 bzw. bis zum 2. August 2030 nachzukommen.

[sn910] 2. Mai 2025
[sn901] Büro für Künstliche Intelligenz

(178) Die Anbieter von Hochrisiko-KI-Systemen werden ermutigt, auf freiwilliger Basis bereits während der Übergangsphase mit der Einhaltung der einschlägigen Pflichten aus dieser Verordnung zu beginnen.

(179) Diese Verordnung sollte ab dem 2. August 2026 gelten. Angesichts des unannehmbaren Risikos, das mit der Nutzung von KI auf bestimmte Weise verbunden ist, sollten die Verbote sowie die allgemeinen Bestimmungen dieser Verordnung jedoch bereits ab dem 2. Februar 2025 gelten. Während die volle Wirkung dieser Verbote erst mit der Festlegung der Leitung und der Durchsetzung dieser Verordnung entsteht, ist die Vorwegnahme der Anwendung der Verbote wichtig, um unannehmbaren Risiken Rechnung zu tragen und Wirkung auf andere Verfahren, etwa im Zivilrecht, zu entfalten. Darüber hinaus sollte die Infrastruktur für die Leitung und das Konformitätsbewertungssystem vor dem 2. August 2026 einsatzbereit sein, weshalb die Bestimmungen über notifizierte Stellen und die Leitungsstruktur ab dem 2. August 2025 gelten sollten. Angesichts des raschen technologischen Fortschritts und der Einführung von KI-Modellen mit allgemeinem Verwendungszweck sollten die Pflichten der Anbieter von KI-Modellen mit allgemeinem Verwendungszweck ab dem 2. August 2025 gelten. Die Verhaltenskodizes sollten bis zum 2. Mai 2025 vorliegen, damit die Anbieter die Einhaltung fristgerecht nachweisen können. Das Büro für Künstliche Intelligenz sollte sicherstellen, dass die Vorschriften und Verfahren für die Einstufung jeweils dem Stand der technologischen Entwicklung entsprechen. Darüber hinaus sollten die Mitgliedstaaten die 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 2. August 2025 gelten.

(180) Der Europäische Datenschutzbeauftragte und der Europäische Datenschutzausschuss wurden gemäß Artikel 42 Absätze 1 und 2 der Verordnung (EU) 2018/1725 angehört und haben am 18. Juni 2021 ihre gemeinsame Stellungnahme abgegeben —

HABEN FOLGENDE VERORDNUNG ERLASSEN:

KAPITEL I

ALLGEMEINE BESTIMMUNGEN

Artikel 1

Gegenstand

(1) Zweck dieser Verordnung ist es, das Funktionieren des Binnenmarkts zu verbessern und die Einführung einer auf den Menschen ausgerichteten und vertrauenswürdigen künstlichen Intelligenz (KI) zu fördern und gleichzeitig ein hohes Schutzniveau in Bezug auf Gesundheit, Sicherheit und die in der Charta verankerten Grundrechte, einschließlich Demokratie, Rechtsstaatlichkeit und Umweltschutz, vor schädlichen Auswirkungen von KI-Systemen in der Union zu gewährleisten und die Innovation zu unterstützen.

(2) In dieser Verordnung wird Folgendes festgelegt:

a) harmonisierte Vorschriften für das Inverkehrbringen, die Inbetriebnahme und die Verwendung von KI-Systemen in der Union;

[sn707] Bevollmächtigter

b) Verbote bestimmter Praktiken im KI-Bereich;

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

d) harmonisierte Transparenzvorschriften für bestimmte KI-Systeme;

e) harmonisierte Vorschriften für das Inverkehrbringen von KI-Modellen mit allgemeinem Verwendungszweck;

[sn502] Anbieter

f) Vorschriften für die Marktbeobachtung sowie die Governance und Durchsetzung der Marktüberwachung;

[sn503] Betreiber

g) Maßnahmen zur Innovationsförderung mit besonderem Augenmerk auf KMU, einschließlich Start-up-Unternehmen.

Artikel 2

Anwendungsbereich

(1) Diese Verordnung gilt für

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

b) Betreiber von KI-Systemen, die ihren Sitz in der Union haben oder in der Union befinden;

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

[sn206] Strafverfolgung

d) Einführer und Händler von KI-Systemen;

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

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

g) betroffene Personen, die sich in der Union befinden.

(2) Für KI-Systeme, die als Hochrisiko-KI-Systeme gemäß Artikel 6 Absatz 1 eingestuft sind und im Zusammenhang mit Produkten stehen, die unter die in Anhang I Abschnitt B aufgeführten Harmonisierungsrechtsvorschriften der Union fallen, gelten nur Artikel 6 Absatz 1, die Artikel 102 bis 109 und Artikel 112. Artikel 57 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 nur in den unter das Unionsrecht fallenden Bereichen und berührt keinesfalls die Zuständigkeiten der Mitgliedstaaten in Bezug auf die nationale Sicherheit, unabhängig von der Art der Einrichtung, die von den Mitgliedstaaten mit der Wahrnehmung von Aufgaben im Zusammenhang mit diesen Zuständigkeiten betraut wurde.

Diese Verordnung gilt nicht für KI-Systeme, wenn und soweit sie ausschließlich für militärische Zwecke, Verteidigungszwecke oder Zwecke der nationalen Sicherheit in Verkehr gebracht, in Betrieb genommen oder, mit oder ohne Änderungen, verwendet werden, unabhängig von der Art der Einrichtung, die diese Tätigkeiten ausübt.

Diese Verordnung gilt nicht für KI-Systeme, die nicht in der Union in Verkehr gebracht oder in Betrieb genommen werden, wenn die Ausgaben in der Union ausschließlich für militärische Zwecke, Verteidigungszwecke oder Zwecke der nationalen Sicherheit verwendet werden, 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 der internationalen Zusammenarbeit oder internationaler Übereinkünfte im Bereich der Strafverfolgung und justiziellen Zusammenarbeit mit der Union oder mit einem oder mehreren Mitgliedstaaten verwenden und sofern ein solches Drittland oder eine solche internationale Organisation angemessene Garantien hinsichtlich des Schutz der Privatsphäre, der Grundrechte und der Grundfreiheiten von Personen bietet.

(5) Die Anwendung der Bestimmungen über die Haftung der Anbieter von Vermittlungsdiensten in Kapitel II der Verordnung 2022/2065 bleibt von dieser Verordnung unberührt.

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

(7) Die Rechtsvorschriften der Union zum Schutz personenbezogener Daten, der Privatsphäre und der Vertraulichkeit der Kommunikation gelten für die Verarbeitung personenbezogener Daten im Zusammenhang mit den in dieser Verordnung festgelegten Rechten und Pflichten. Diese Verordnung berührt nicht die Verordnung (EU) 2016/679 bzw. (EU) 2018/1725 oder die Richtlinie 2002/58/EG bzw. (EU) 2016/680, unbeschadet des Artikels 10 Absatz 5 und des Artikels 59 der vorliegenden Verordnung.

[sn503] Betreiber

(8) Diese Verordnung gilt nicht für Forschungs-, Test- und Entwicklungstätigkeiten zu KI-Systemen oder KI-Modellen, bevor diese in Verkehr gebracht oder in Betrieb genommen werden. Solche Tätigkeiten werden im Einklang mit dem geltenden Unionsrecht durchgeführt. Tests unter Realbedingungen fallen nicht unter diesen Ausschluss.

(9) Diese Verordnung berührt nicht die Vorschriften anderer Rechtsakte der Union zum Verbraucherschutz und zur Produktsicherheit.

(10) Diese Verordnung gilt nicht für die Pflichten von Betreibern, die natürliche Personen sind und KI-Systeme im Rahmen einer ausschließlich persönlichen und nicht beruflichen Tätigkeit verwenden.

(11) Diese Verordnung hindert die Union oder die Mitgliedstaaten nicht daran, Rechts- oder Verwaltungsvorschriften beizubehalten oder einzuführen, die für die Arbeitnehmer im Hinblick auf den Schutz ihrer Rechte bei der Verwendung von KI-Systemen durch die Arbeitgeber vorteilhafter sind, oder die Anwendung von Kollektivvereinbarungen zu fördern oder zuzulassen, die für die Arbeitnehmer vorteilhafter sind.

[sn502] Anbieter

(12) Diese Verordnung gilt nicht für KI-Systeme, die unter freien und quelloffenen Lizenzen bereitgestellt werden, es sei denn, sie werden als Hochrisiko-KI-Systeme oder als ein KI-System, das unter Artikel 5 oder 50 fällt, in Verkehr gebracht oder in Betrieb genommen.

[sn707] Bevollmächtigter

Artikel 3

Begriffsbestimmungen

Für die Zwecke dieser Verordnung bezeichnet der Ausdruck

1. „KI-System“ ein maschinengestütztes System, das für einen in unterschiedlichem Grade autonomen Betrieb ausgelegt ist und das nach seiner Betriebsaufnahme anpassungsfähig sein kann und das aus den erhaltenen Eingaben für explizite oder implizite Ziele ableitet, wie Ausgaben wie etwa Vorhersagen, Inhalte, Empfehlungen oder Entscheidungen erstellt werden, die physische oder virtuelle Umgebungen beeinflussen können;

2. „Risiko“ die Kombination aus der Wahrscheinlichkeit des Auftretens eines Schadens und der Schwere dieses Schadens;

3. „Anbieter“ eine natürliche oder juristische Person, Behörde, Einrichtung oder sonstige Stelle, die ein KI-System oder ein KI-Modell mit allgemeinem Verwendungszweck entwickelt oder entwickeln lässt und es unter ihrem eigenen Namen oder ihrer Handelsmarke in Verkehr bringt oder das KI-System unter ihrem eigenen Namen oder ihrer Handelsmarke in Betrieb nimmt, sei es entgeltlich oder unentgeltlich;

4. „Betreiber“ eine natürliche oder juristische Person, Behörde, Einrichtung oder sonstige Stelle, die ein KI-System in eigener Verantwortung verwendet, es sei denn, das KI-System wird im Rahmen einer persönlichen und nicht beruflichen Tätigkeit verwendet;

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

6. „Einführer“ eine in der Union ansässige oder niedergelassene natürliche oder juristische Person, die ein KI-System, das den Namen oder die Handelsmarke einer in einem Drittland niedergelassenen natürlichen oder juristischen Person trägt, 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“ einen Anbieter, Produkthersteller, Betreiber, Bevollmächtigten, Einführer oder Händler;

9. „Inverkehrbringen“ die erstmalige Bereitstellung eines KI-Systems oder eines KI-Modells mit allgemeinem Verwendungszweck auf dem Unionsmarkt;

10. „Bereitstellung auf dem Markt“ die entgeltliche oder unentgeltliche Abgabe eines KI-Systems oder eines KI-Modells mit allgemeinem Verwendungszweck 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 Betreiber 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 vom Anbieter bereitgestellten Informationen in den Betriebsanleitungen, 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, auch anderen KI-Systemen, ergeben kann;

[sn505] Konformitätsbewertung

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

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

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

[sn509] CE-Kennzeichnung

17. „Rücknahme eines KI-Systems“ jede Maßnahme, mit der die Bereitstellung eines in der Lieferkette befindlichen KI-Systems auf dem Markt verhindert werden soll;

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

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

20. „Konformitätsbewertung“ ein Verfahren mit dem bewertet wird, ob die in Titel III Abschnitt 2 festgelegten Anforderungen an ein Hochrisiko-KI-System erfüllt wurden;

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

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

23. „wesentliche Veränderung“ eine Veränderung eines KI-Systems nach dessen Inverkehrbringen oder Inbetriebnahme, die in der vom Anbieter durchgeführten ursprünglichen Konformitätsbewertung nicht vorgesehen oder geplant war und durch die die Konformität des KI-Systems mit den Anforderungen in Kapitel III Abschnitt 2 beeinträchtigt wird oder die zu einer Änderung der Zweckbestimmung führt, für die das KI-System bewertet wurde;

24. „CE-Kennzeichnung“ eine Kennzeichnung, durch die ein Anbieter erklärt, dass ein KI-System die Anforderungen erfüllt, die in Kapitel III Abschnitt 2 und in anderen anwendbaren Harmonisierungsrechtsvorschriften, 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“ bezeichnet eine harmonisierte 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 des Artikels 2 Nummer 4 der Verordnung (EU) Nr. 1025/2012, deren Befolgung es ermöglicht, bestimmte Anforderungen der vorliegenden Verordnung zu erfüllen;

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

30. „Validierungsdaten“ Daten, die zur Evaluation des trainierten KI-Systems und zur Einstellung seiner nicht erlernbaren Parameter und seines Lernprozesses verwendet werden, um unter anderem eine Unter- oder Überanpassung zu vermeiden;

31. „Validierungsdatensatz“ einen separaten Datensatz oder einen Teil des Trainingsdatensatzes mit fester oder variabler Aufteilung;

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

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

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

35. „biometrische Identifizierung“ die automatisierte Erkennung physischer, physiologischer, verhaltensbezogener oder psychologischer menschlicher Merkmale zum Zwecke der Feststellung der Identität einer natürlichen Person durch den Vergleich biometrischer Daten dieser Person mit biometrischen Daten von Personen, die in einer Datenbank gespeichert sind;

36. „biometrische Verifizierung“ die automatisierte Eins-zu-eins-Verifizierung, einschließlich Authentifizierung, der Identität natürlicher Personen durch den Vergleich ihrer biometrischen Daten mit zuvor bereitgestellten biometrischen Daten;

37. „besondere Kategorien personenbezogener Daten“ die in Artikel 9 Absatz 1der Verordnung (EU) 2016/679, Artikel 10 der Richtlinie (EU) 2016/680 und Artikel 10 Absatz 1 der Verordnung (EU) 2018/1725 aufgeführten Kategorien personenbezogener Daten;

38. „sensible operative Daten“ operative Daten im Zusammenhang mit Tätigkeiten zur Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten, deren Offenlegung die Integrität von Strafverfahren gefährden könnte;

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

40. „System zur biometrischen Kategorisierung“ ein KI-System, das dem Zweck dient, natürliche Personen auf der Grundlage ihrer biometrischen Daten bestimmten Kategorien zuzuordnen, sofern es sich um eine Nebenfunktion eines anderen kommerziellen Dienstes handelt und aus objektiven technischen Gründen unbedingt erforderlich ist;

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

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

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

44. „öffentlich zugänglicher Raum“ einen einer unbestimmten Anzahl natürlicher Personen zugänglichen physischen Ort in privatem oder öffentlichem Eigentum, unabhängig davon, ob bestimmte Bedingungen für den Zugang gelten, und unabhängig von möglichen Kapazitätsbeschränkungen;

45. „Strafverfolgungsbehörde“

a) eine Behörde, 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

[sn901] Büro für Künstliche Intelligenz

b) eine andere Stelle oder Einrichtung, der durch nationales Recht 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;

46. „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;

47. „Büro für Künstliche Intelligenz“ die Aufgabe der Kommission, zur Umsetzung, Beobachtung und Überwachung von KI-Systemen und KI-Modellen mit allgemeinem Verwendungszweck und zu der im Beschluss der Kommission vom 24. Januar 2024 vorgesehenen KI-Governance beizutragen; Bezugnahmen in dieser Verordnung auf das Büro für Künstliche Intelligenz gelten als Bezugnahmen auf die Kommission;

48. „zuständige nationale Behörde“ eine notifizierende Behörde oder eine Marktüberwachungsbehörde; in Bezug auf KI-Systeme, die von Organen, Einrichtungen und sonstigen Stellen der Union in Betrieb genommen oder verwendet werden, sind Bezugnahmen auf die zuständigen nationalen Behörden oder Marktüberwachungsbehörden in dieser Verordnung als Bezugnahmen auf den Europäischen Datenschutzbeauftragten auszulegen;

49. „schwerwiegender Vorfall“ einen Vorfall oder eine Fehlfunktion bezüglich eines KI-Systems, das bzw. die direkt oder indirekt eine der nachstehenden Folgen hat:

[sn506] KI-Reallabor

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

[sn801] KI-Kompetenz

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

c) die Verletzung von Pflichten aus den Unionsrechtsvorschriften zum Schutz der Grundrechte;

d) schwere Sach- oder Umweltschäden;

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

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

52. „Profiling“ das Profiling im Sinne von Artikel 4 Nummer 4 der Verordnung (EU) 2016/679;

53. „Plan für einen Test unter Realbedingungen“ ein Dokument, in dem die Ziele, die Methodik, der geografische, bevölkerungsbezogene und zeitliche Umfang, die Überwachung, die Organisation und die Durchführung eines Tests unter Realbedingungen beschrieben werden;

54. „Plan für das Reallabor“ ein zwischen dem teilnehmenden Anbieter und der zuständigen Behörde vereinbartes Dokument, in dem die Ziele, die Bedingungen, der Zeitrahmen, die Methodik und die Anforderungen für die im Reallabor durchgeführten Tätigkeiten beschrieben werden;

55. „KI-Reallabor“ einen kontrollierten Rahmen, der von einer zuständigen Behörde geschaffen wird und den Anbieter oder zukünftige Anbieter von KI-Systemen nach einem Plan für das Reallabor einen begrenzten Zeitraum und unter regulatorischer Aufsicht nutzen können, um ein innovatives KI-System zu entwickeln, zu trainieren, zu validieren und — gegebenenfalls unter Realbedingungen — zu testen.

56. „KI-Kompetenz“ die Fähigkeiten, die Kenntnisse und das Verständnis, die es Anbietern, Betreibern und Betroffenen unter Berücksichtigung ihrer jeweiligen Rechte und Pflichten im Rahmen dieser Verordnung ermöglichen, KI-Systeme sachkundig einzusetzen sowie sich der Chancen und Risiken von KI und möglicher Schäden, die sie verursachen kann, bewusst zu werden.

57. „Test unter Realbedingungen“ den befristeten Test eines KI-Systems auf seine Zweckbestimmung, der unter Realbedingungen 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 der vorliegenden Verordnung zu bewerten und zu überprüfen, wobei dieser Test nicht als Inverkehrbringen oder Inbetriebnahme des KI-Systems im Sinne dieser Verordnung gilt, sofern alle Bedingungen nach Artikel 57 oder Artikel 60 erfüllt sind;

58. „Testteilnehmer“ für die Zwecke eines Tests unter Realbedingungen eine natürliche Person, die an dem Test unter Realbedingungen teilnimmt;

59. „informierte Einwilligung“ eine aus freien Stücken erfolgende, spezifische, eindeutige und freiwillige Erklärung der Bereitschaft, an einem bestimmten Test unter Realbedingungen teilzunehmen, durch einen Testteilnehmer, nachdem dieser über alle Aspekte des Tests, die für die Entscheidungsfindung des Testteilnehmers bezüglich der Teilnahme relevant sind, aufgeklärt wurde;

60. „Deepfake“ einen durch KI erzeugten oder manipulierten Bild-, Ton- oder Videoinhalt, der wirklichen Personen, Gegenständen, Orten, Einrichtungen oder Ereignissen ähnelt und einer Person fälschlicherweise als echt oder wahrheitsgemäß erscheinen würde;

61. „weitverbreiteter Verstoß“ jede Handlung oder Unterlassung, die gegen das Unionsrecht verstößt, das die Interessen von Einzelpersonen schützt, und die

    a) die kollektiven Interessen von Einzelpersonen in mindestens zwei anderen Mitgliedstaaten als dem Mitgliedstaat schädigt oder zu schädigen droht, in dem

        i) die Handlung oder die Unterlassung ihren Ursprung hatte oder stattfand,

        ii) der betreffende Anbieter oder gegebenenfalls sein Bevollmächtigter sich befindet oder niedergelassen ist oder

        iii) der Betreiber niedergelassen ist, sofern der Verstoß vom Betreiber begangen wird,

    b) die kollektiven Interessen von Einzelpersonen geschädigt hat, schädigt oder schädigen könnte und allgemeine Merkmale aufweist, einschließlich derselben rechtswidrigen Praxis oder desselben verletzten Interesses, und gleichzeitig auftritt und von demselben Akteur in mindestens drei Mitgliedstaaten begangen wird;

62. „kritische Infrastrukturen“ kritische Infrastrukturen im Sinne von Artikel 2 Nummer 4 der Richtlinie (EU) 2022/2557;

63. „KI-Modell mit allgemeinem Verwendungszweck“ ein KI-Modell — einschließlich der Fälle, in denen ein solches KI-Modell mit einer großen Datenmenge unter umfassender Selbstüberwachung trainiert wird —, das eine erhebliche allgemeine Verwendbarkeit aufweist und in der Lage ist, unabhängig von der Art und Weise seines Inverkehrbringens ein breites Spektrum unterschiedlicher Aufgaben kompetent zu erfüllen, und das in eine Vielzahl nachgelagerter Systeme oder Anwendungen integriert werden kann, ausgenommen KI-Modelle, die vor ihrem Inverkehrbringen für Forschungs- und Entwicklungstätigkeiten oder die Konzipierung von Prototypen eingesetzt werden;

64. „Fähigkeiten mit hoher Wirkkraft“ bezeichnet Fähigkeiten, die den bei den fortschrittlichsten KI-Modellen mit allgemeinem Verwendungszweck festgestellten Fähigkeiten entsprechen oder diese übersteigen;

65. „systemisches Risiko“ ein Risiko, das für die Fähigkeiten mit hoher Wirkkraft von KI-Modellen mit allgemeinem Verwendungszweck spezifisch ist und aufgrund deren Reichweite oder aufgrund tatsächlicher oder vernünftigerweise vorhersehbarer negativer Folgen für die öffentliche Gesundheit, die Sicherheit, die öffentliche Sicherheit, die Grundrechte oder die Gesellschaft insgesamt erhebliche Auswirkungen auf den Unionsmarkt hat, die sich in großem Umfang über die gesamte Wertschöpfungskette hinweg verbreiten können;

66. „KI-System mit allgemeinem Verwendungszweck“ ein KI-System, das auf einem KI-Modell mit allgemeinem Verwendungszweck beruht und in der Lage ist, einer Vielzahl von Zwecken sowohl für die direkte Verwendung als auch für die Integration in andere KI-Systeme zu dienen;

67. „Gleitkommaoperation“ jede Rechenoperation oder jede Zuweisung mit Gleitkommazahlen, bei denen es sich um eine Teilmenge der reellen Zahlen handelt, die auf Computern typischerweise durch das Produkt aus einer ganzen Zahl mit fester Genauigkeit und einer festen Basis mit ganzzahligem Exponenten dargestellt wird;

68. „nachgelagerter Anbieter“ einen Anbieter eines KI-Systems, einschließlich eines KI-Systems mit allgemeinem Verwendungszweck, das ein KI-Modell integriert, unabhängig davon, ob das KI-Modell von ihm selbst bereitgestellt und vertikal integriert wird oder von einer anderen Einrichtung auf der Grundlage vertraglicher Beziehungen bereitgestellt wird.

[sn101] Unterschwellige Beeinflussung
[sn904] Sanktion: Verbotene Praktiken
[sn102] Ausnutzung von Schutzbedürftigkeit
[sn103] Sozialbewertung
[sn104] Prädiktive Polizeiarbeit
[sn105] Ungezieltes Gesichtsdaten-Scraping
[sn106] Emotionserkennung am Arbeitsplatz/Bildung
[sn800] Querschnittspflichten
[sn801] KI-Kompetenz
[sn502] Anbieter
[sn503] Betreiber
[sn100] Verbotene Praktiken

Artikel 4

KI-Kompetenz

Die Anbieter und Betreiber von KI-Systemen ergreifen Maßnahmen, um nach besten Kräften sicherzustellen, dass ihr Personal und andere Personen, die in ihrem Auftrag mit dem Betrieb und der Nutzung von KI-Systemen befasst sind, über ein ausreichendes Maß an KI-Kompetenz verfügen, wobei ihre technischen Kenntnisse, ihre Erfahrung, ihre Ausbildung und Schulung und der Kontext, in dem die KI-Systeme eingesetzt werden sollen, sowie die Personen oder Personengruppen, bei denen die KI-Systeme eingesetzt werden sollen, zu berücksichtigen sind.

KAPITEL II

VERBOTENE PRAKTIKEN IM KI-BEREICH

Artikel 5

Verbotene Praktiken im KI-Bereich

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

[sn904] Sanktion: Verbotene Praktiken
[sn107] Biometrische Kategorisierung

a) das Inverkehrbringen, die Inbetriebnahme oder die Verwendung eines KI-Systems, das Techniken der unterschwelligen Beeinflussung außerhalb des Bewusstseins einer Person oder absichtlich manipulative oder täuschende Techniken mit dem Ziel oder der Wirkung einsetzt, das Verhalten einer Person oder einer Gruppe von Personen wesentlich zu verändern, indem ihre Fähigkeit, eine fundierte Entscheidung zu treffen, deutlich beeinträchtigt wird, wodurch sie veranlasst wird, eine Entscheidung zu treffen, die sie andernfalls nicht getroffen hätte, und zwar in einer Weise, die dieser Person, einer anderen Person oder einer Gruppe von Personen erheblichen Schaden zufügt oder mit hinreichender Wahrscheinlichkeit zufügen wird.

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

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

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

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

d) das Inverkehrbringen, die Inbetriebnahme für diesen spezifischen Zweck oder die Verwendung eines KI-Systems zur Durchführung von Risikobewertungen in Bezug auf natürliche Personen, um das Risiko, dass eine natürliche Person eine Straftat begeht, ausschließlich auf der Grundlage des Profiling einer natürlichen Person oder der Bewertung ihrer persönlichen Merkmale und Eigenschaften zu bewerten oder vorherzusagen; dieses Verbot gilt nicht für KI-Systeme, die dazu verwendet werden, die durch Menschen durchgeführte Bewertung der Beteiligung einer Person an einer kriminellen Aktivität, die sich bereits auf objektive und überprüfbare Tatsachen stützt, die in unmittelbarem Zusammenhang mit einer kriminellen Aktivität stehen, zu unterstützen;

e) das Inverkehrbringen, die Inbetriebnahme für diesen spezifischen Zweck oder die Verwendung von KI-Systemen, die Datenbanken zur Gesichtserkennung durch das ungezielte Auslesen von Gesichtsbildern aus dem Internet oder von Überwachungsaufnahmen erstellen oder erweitern;

f) das Inverkehrbringen, die Inbetriebnahme für diesen spezifischen Zweck oder die Verwendung von KI-Systemen zur Ableitung von Emotionen einer natürlichen Person am Arbeitsplatz und in Bildungseinrichtungen, es sei denn, die Verwendung des KI-Systems soll aus medizinischen Gründen oder Sicherheitsgründen eingeführt oder auf den Markt gebracht werden;

[sn100] Verbotene Praktiken
[sn107] Biometrische Kategorisierung
[sn904] Sanktion: Verbotene Praktiken

g) das Inverkehrbringen, die Inbetriebnahme für diesen spezifischen Zweck oder die Verwendung von Systemen zur biometrischen Kategorisierung, mit denen natürliche Personen individuell auf der Grundlage ihrer biometrischen Daten kategorisiert werden, um ihre Rasse, ihre politischen Einstellungen, ihre Gewerkschaftszugehörigkeit, ihre religiösen oder weltanschaulichen Überzeugungen, ihr Sexualleben oder ihre sexuelle Ausrichtung zu erschließen oder abzuleiten; dieses Verbot gilt nicht für die Kennzeichnung oder Filterung rechtmäßig erworbener biometrischer Datensätze, wie z. B. Bilder auf der Grundlage biometrischer Daten oder die Kategorisierung biometrischer Daten im Bereich der Strafverfolgung;

h) die Verwendung biometrischer Echtzeit-Fernidentifizierungssysteme in öffentlich zugänglichen Räumen zu Strafverfolgungszwecken, außer wenn und insoweit dies im Hinblick auf eines der folgenden Ziele unbedingt erforderlich ist:

i) gezielte Suche nach bestimmten Opfern von Entführung, Menschenhandel oder sexueller Ausbeutung sowie die Suche nach vermissten Personen;

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

iii) Aufspüren oder Identifizieren einer Person, die der Begehung einer Straftat verdächtigt wird, zum Zwecke der Durchführung von strafrechtlichen Ermittlungen oder von Strafverfahren oder der Vollstreckung einer Strafe für die in Anhang II aufgeführten Straftaten, die in dem betreffenden Mitgliedstaat nach dessen Recht mit einer Freiheitsstrafe oder einer freiheitsentziehenden Maßregel der Sicherung im Höchstmaß von mindestens vier Jahren bedroht ist.

[sn100] Verbotene Praktiken
[sn904] Sanktion: Verbotene Praktiken
[sn908] EU-Datenbank

Unterabsatz 1 Buchstabe h gilt unbeschadet des Artikels 9 der Verordnung (EU) 2016/679 für die Verarbeitung biometrischer Daten zu anderen Zwecken als der Strafverfolgung.

(2) Die Verwendung biometrischer Echtzeit-Fernidentifizierungssysteme in öffentlich zugänglichen Räumen zu Strafverfolgungszwecken im Hinblick auf die in Absatz 1 Unterabsatz 1 Buchstabe h genannten Ziele darf für die in jenem Buchstaben genannten Zwecke nur zur Bestätigung der Identität der speziell betroffenen Person erfolgen, wobei folgende Elemente berücksichtigt werden:

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

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

Darüber hinaus sind bei der Verwendung biometrischer Echtzeit-Fernidentifizierungssysteme in öffentlich zugänglichen Räumen zu Strafverfolgungszwecken im Hinblick auf die in Absatz 1 Unterabsatz 1 Buchstabe h des vorliegenden Artikels genannten Ziele notwendige und verhältnismäßige Schutzvorkehrungen und Bedingungen für die Verwendung im Einklang mit nationalem Recht über die Ermächtigung ihrer Verwendung einzuhalten, insbesondere in Bezug auf die zeitlichen, geografischen und personenbezogenen Beschränkungen. Die Verwendung biometrischer Echtzeit-Fernidentifizierungssysteme in öffentlich zugänglichen Räumen ist nur dann zu gestatten, wenn die Strafverfolgungsbehörde eine Folgenabschätzung im Hinblick auf die Grundrechte gemäß Artikel 27 abgeschlossen und das System gemäß Artikel 49 in der EU-Datenbank registriert hat. In hinreichend begründeten dringenden Fällen kann jedoch mit der Verwendung solcher Systeme zunächst ohne Registrierung in der EU-Datenbank begonnen werden, sofern diese Registrierung unverzüglich erfolgt.

(3) Für die Zwecke des Absatz 1 Unterabsatz 1 Buchstabe h und des Absatzes 2 ist für jede Verwendung eines biometrischen Echtzeit-Fernidentifizierungssystems in öffentlich zugänglichen Räumen zu Strafverfolgungszwecken eine vorherige Genehmigung erforderlich, die von einer Justizbehörde oder einer unabhängigen Verwaltungsbehörde des Mitgliedstaats, in dem die Verwendung erfolgen soll, auf begründeten Antrag und gemäß den in Absatz 5 genannten detaillierten nationalen Rechtsvorschriften erteilt wird, wobei deren Entscheidung bindend ist. In hinreichend begründeten dringenden Fällen kann jedoch mit der Verwendung eines solchen Systems zunächst ohne Genehmigung begonnen werden, sofern eine solche Genehmigung unverzüglich, spätestens jedoch innerhalb von 24 Stunden beantragt wird. Wird eine solche Genehmigung abgelehnt, so wird die Verwendung mit sofortiger Wirkung eingestellt und werden alle Daten sowie die Ergebnisse und Ausgaben dieser Verwendung unverzüglich verworfen und gelöscht.

Die zuständige Justizbehörde oder eine unabhängige Verwaltungsbehörde, deren Entscheidung bindend ist, erteilt die Genehmigung nur dann, wenn sie auf der Grundlage objektiver Nachweise oder eindeutiger Hinweise, die ihr vorgelegt werden, davon überzeugt ist, dass die Verwendung des betreffenden biometrischen Echtzeit-Fernidentifizierungssystems für das Erreichen eines der in Absatz 1 Unterabsatz 1 Buchstabe h genannten Ziele — wie im Antrag angegeben — notwendig und verhältnismäßig ist und insbesondere auf das in Bezug auf den Zeitraum sowie den geografischen und persönlichen Anwendungsbereich unbedingt erforderliche Maß beschränkt bleibt. Bei ihrer Entscheidung über den Antrag berücksichtigt

diese Behörde die in Absatz 2 genannten Elemente. Eine Entscheidung, aus der sich eine nachteilige Rechtsfolge für eine Person ergibt, darf nicht ausschließlich auf der Grundlage der Ausgabe des biometrischen Echtzeit-Fernidentifizierungssystems getroffen werden.

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

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

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

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

[sn505] Konformitätsbewertung

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

KAPITEL III

HOCHRISIKO-KI-SYSTEME

ABSCHNITT 1

Einstufung von KI-Systemen als Hochrisiko-KI-Systeme

Artikel 6

Einstufungsvorschriften für Hochrisiko-KI-Systeme

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

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

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

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

[sn209] Hochrisiko-Ausnahme

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

Unterabsatz 1 gilt, wenn eine der folgenden Bedingungen erfüllt ist:

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

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

[sn502] Anbieter

c) das KI-System ist dazu bestimmt, Entscheidungsmuster oder Abweichungen von früheren Entscheidungsmustern zu erkennen, und ist nicht dazu gedacht, die zuvor abgeschlossene menschliche Bewertung ohne eine angemessene menschliche Überprüfung zu ersetzen oder zu beeinflussen; oder

d) das KI-System ist dazu bestimmt, eine vorbereitende Aufgabe für eine Bewertung durchzuführen, die für die Zwecke der in Anhang III aufgeführten Anwendungsfälle relevant ist.

Ungeachtet des Unterabsatzes 1 gilt ein in Anhang III aufgeführtes KI-System immer dann als hochriskant, wenn es ein Profiling natürlicher Personen vornimmt.

(4) Ein Anbieter, der der Auffassung ist, dass ein in Anhang III aufgeführtes KI-System nicht hochriskant ist, dokumentiert seine Bewertung, bevor dieses System in Verkehr gebracht oder in Betrieb genommen wird. Dieser Anbieter unterliegt der Registrierungspflicht gemäß Artikel 49 Absatz 2. Auf Verlangen der zuständigen nationalen Behörden legt der Anbieter die Dokumentation der Bewertung vor.

(5) Die Kommission stellt nach Konsultation des Europäischen Gremiums für Künstliche Intelligenz (im Folgenden „KI-Gremium“) spätestens bis zum 2. Februar 2026 Leitlinien zur praktischen Umsetzung dieses Artikels gemäß Artikel 96 und eine umfassende Liste praktischer Beispiele für Anwendungsfälle für KI-Systeme, die hochriskant oder nicht hochriskant sind, bereit.

(6) Die Kommission ist befugt, gemäß Artikel 97 delegierte Rechtsakte zu erlassen, um Absatz 3 Unterabsatz 2 des vorliegenden Artikels zu ändern, indem neue Bedingungen zu den darin genannten Bedingungen hinzugefügt oder diese geändert werden, wenn konkrete und zuverlässige Beweise für das Vorhandensein von KI-Systemen vorliegen, die in den Anwendungsbereich von Anhang III fallen, jedoch kein erhebliches Risiko der Beeinträchtigung in Bezug auf die Gesundheit, Sicherheit oder Grundrechte natürlicher Personen bergen.

(7) Die Kommission erlässt gemäß Artikel 97 delegierte Rechtsakte, um Absatz 3 Unterabsatz 2 des vorliegenden Artikels zu ändern, indem eine der darin festgelegten Bedingungen gestrichen wird, wenn konkrete und zuverlässige Beweise dafür vorliegen, dass dies für die Aufrechterhaltung des Schutzniveaus in Bezug auf Gesundheit, Sicherheit und die in dieser Verordnung vorgesehenen Grundrechte erforderlich ist.

(8) Eine Änderung der in Absatz 3 Unterabsatz 2 festgelegten Bedingungen, die gemäß den Absätzen 6 und 7 des vorliegenden Artikels erlassen wurde, darf das allgemeine Schutzniveau in Bezug auf Gesundheit, Sicherheit und die in dieser Verordnung vorgesehenen Grundrechte nicht senken; dabei ist die Kohärenz mit den gemäß Artikel 7 Absatz 1 erlassenen delegierten Rechtsakten sicherzustellen und die Marktentwicklungen und die technologischen Entwicklungen sind zu berücksichtigen.

Artikel 7

Änderungen des Anhangs III

(1) Die Kommission ist befugt, gemäß Artikel 97 delegierte Rechtsakte zur Änderung von Anhang III durch Hinzufügung oder Änderung von Anwendungsfällen für Hochrisiko-KI-Systeme zu erlassen, die beide der folgenden Bedingungen erfüllen:

a) Die KI-Systeme sollen in einem der in Anhang III aufgeführten Bereiche eingesetzt werden;

b) die KI-Systeme bergen ein Risiko der Schädigung in Bezug auf die Gesundheit und Sicherheit oder haben nachteilige Auswirkungen auf die Grundrechte und dieses Risiko gleicht dem Risiko der Schädigung oder den nachteiligen Auswirkungen, das bzw. die von den in Anhang III bereits genannten Hochrisiko-KI-Systemen ausgeht bzw. ausgehen, oder übersteigt diese.

(2) Bei der Bewertung der Bedingung gemäß Absatz 1 Buchstabe b 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) die Art und den Umfang der vom KI-System verarbeiteten und verwendeten Daten, insbesondere die Frage, ob besondere Kategorien personenbezogener Daten verarbeitet werden;

d) das Ausmaß, in dem das KI-System autonom handelt, und die Möglichkeit, dass ein Mensch eine Entscheidung oder Empfehlungen, die zu einem potenziellen Schaden führen können, außer Kraft setzt;

[sn503] Betreiber

e) das Ausmaß, in dem durch die Verwendung eines KI-Systems schon die Gesundheit und Sicherheit geschädigt wurden, es nachteilige Auswirkungen auf die Grundrechte gab oder z. B. nach Berichten oder dokumentierten Behauptungen, die den zuständigen nationalen Behörden übermittelt werden, oder gegebenenfalls anderen Berichten Anlass zu erheblichen Bedenken hinsichtlich der Wahrscheinlichkeit eines solchen Schadens oder solcher nachteiligen Auswirkungen besteht;

f) das potenzielle Ausmaß solcher Schäden oder nachteiligen Auswirkungen, insbesondere hinsichtlich ihrer Intensität und ihrer Eignung, mehrere Personen zu beeinträchtigen oder eine bestimmte Gruppe von Personen unverhältnismäßig stark zu beeinträchtigen;

g) das Ausmaß, in dem Personen, die potenziell geschädigt oder negative Auswirkungen erleiden werden, 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;

h) das Ausmaß, in dem ein Machtungleichgewicht besteht oder in dem Personen, die potenziell geschädigt oder negative Auswirkungen erleiden werden, gegenüber dem Betreiber eines KI-Systems schutzbedürftig sind, insbesondere aufgrund von Status, Autorität, Wissen, wirtschaftlichen oder sozialen Umständen oder Alter;

i) das Ausmaß, in dem das mithilfe eines KI-Systems hervorgebrachte Ergebnis unter Berücksichtigung der verfügbaren technischen Lösungen für seine Korrektur oder Rückgängigmachung leicht zu korrigieren oder rückgängig zu machen ist, wobei Ergebnisse, die sich auf die Gesundheit, Sicherheit oder Grundrechte von Personen negativ auswirken, nicht als leicht korrigierbar oder rückgängig zu machen gelten;

[sn301] Risikomanagementsystem

j) das Ausmaß und die Wahrscheinlichkeit, dass der Einsatz des KI-Systems für Einzelpersonen, Gruppen oder die Gesellschaft im Allgemeinen, einschließlich möglicher Verbesserungen der Produktsicherheit, nützlich ist;

k) das Ausmaß, in dem bestehendes Unionsrecht Folgendes vorsieht:

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.

(3) Die Kommission ist befugt, gemäß Artikel 97 delegierte Rechtsakte zur Änderung der Liste in Anhang III zu erlassen, um Hochrisiko-KI-Systeme zu streichen, die beide der folgenden Bedingungen erfüllen:

a) Das betreffende Hochrisiko-KI-System weist unter Berücksichtigung der in Absatz 2 aufgeführten Kriterien keine erheblichen Risiken mehr für die 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.

ABSCHNITT 2

Anforderungen an Hochrisiko-KI-Systeme

Artikel 8

Einhaltung der Anforderungen

(1) Hochrisiko-KI-Systeme müssen die in diesem Abschnitt festgelegten Anforderungen erfüllen, wobei ihrer Zweckbestimmung sowie dem allgemein anerkannten Stand der Technik in Bezug auf KI und KI-bezogene Technologien Rechnung zu tragen ist. Bei der Gewährleistung der Einhaltung dieser Anforderungen wird dem in Artikel 9 genannten Risikomanagementsystem Rechnung getragen.

[sn502] Anbieter

(2) Enthält ein Produkt ein KI-System, für das die Anforderungen dieser Verordnung und die Anforderungen der in Anhang I Abschnitt A aufgeführten Harmonisierungsrechtsvorschriften der Union gelten, so sind die Anbieter dafür verantwortlich, sicherzustellen, dass ihr Produkt alle geltenden Anforderungen der geltenden Harmonisierungsrechtsvorschriften der Union vollständig erfüllt. Bei der Gewährleistung der Erfüllung der in diesem Abschnitt festgelegten Anforderungen durch die in Absatz 1 genannten Hochrisiko-KI-Systeme und im Hinblick auf die Gewährleistung der Kohärenz, der Vermeidung von Doppelarbeit und der Minimierung zusätzlicher Belastungen haben die Anbieter die Wahl, die erforderlichen Test- und Berichterstattungsverfahren, Informationen und Dokumentationen, die sie im Zusammenhang mit ihrem Produkt bereitstellen, gegebenenfalls in Dokumentationen und Verfahren zu integrieren, die bereits bestehen und gemäß den in Anhang I Abschnitt A aufgeführten Harmonisierungsrechtsvorschriften der Union vorgeschrieben sind.

[sn301] Risikomanagementsystem

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 Überprüfung und Aktualisierung erfordert. Es umfasst folgende Schritte:

a) die Ermittlung und Analyse der bekannten und vernünftigerweise vorhersehbaren Risiken, die vom Hochrisiko-KI-System für die Gesundheit, Sicherheit oder Grundrechte ausgehen können, wenn es entsprechend seiner Zweckbestimmung verwendet wird;

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

c) die Bewertung anderer möglicherweise auftretender Risiken auf der Grundlage der Auswertung der Daten aus dem in Artikel 72 genannten System zur Beobachtung nach dem Inverkehrbringen;

[sn503] Betreiber

d) die Ergreifung geeigneter und gezielter Risikomanagementmaßnahmen zur Bewältigung der gemäß Buchstabe a ermittelten Risiken.

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

(4) Bei den in Absatz 2 Buchstabe d genannten Risikomanagementmaßnahmen werden die Auswirkungen und möglichen Wechselwirkungen, die sich aus der kombinierten Anwendung der Anforderungen dieses Abschnitts ergeben, gebührend berücksichtigt, um die Risiken wirksamer zu minimieren und gleichzeitig ein angemessenes Gleichgewicht bei der Durchführung der Maßnahmen zur Erfüllung dieser Anforderungen sicherzustellen.

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

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

a) soweit technisch möglich, Beseitigung oder Verringerung der gemäß Absatz 2 ermittelten und bewerteten Risiken durch eine geeignete Konzeption und Entwicklung des Hochrisiko-KI-Systems;

b) gegebenenfalls Anwendung angemessener Minderungs- und Kontrollmaßnahmen zur Bewältigung nicht auszuschließender Risiken;

c) Bereitstellung der gemäß Artikel 13 erforderlichen Informationen und gegebenenfalls entsprechende Schulung der Betreiber.

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 Betreiber erwartet werden können, sowie der voraussichtliche Kontext, in dem das System eingesetzt werden soll, gebührend berücksichtigt.

[sn900] Governance und Durchsetzung
[sn802] DSGVO und Datenschutz

(6) Hochrisiko-KI-Systeme müssen getestet werden, um die am besten geeigneten gezielten Risikomanagemente-maßnahmen zu ermitteln. Durch das Testen wird sichergestellt, dass Hochrisiko-KI-Systeme stets im Einklang mit ihrer Zweckbestimmung funktionieren und die Anforderungen dieses Abschnitts erfüllen.

[sn301] Risikomanagementsystem
[sn502] Anbieter

(7) Die Testverfahren können einen Test unter Realbedingungen gemäß Artikel 60 umfassen.

(8) Das Testen von Hochrisiko-KI-Systemen erfolgt zu jedem geeigneten Zeitpunkt während des gesamten Entwicklungsprozesses und in jedem Fall vor ihrem Inverkehrbringen oder ihrer Inbetriebnahme. Das Testen erfolgt anhand vorab festgelegter Metriken und Wahrscheinlichkeitsschwellenwerte, die für die Zweckbestimmung des Hochrisiko-KI-Systems geeignet sind.

[sn302] Daten und Daten-Governance

(9) Bei der Umsetzung des in den Absätzen 1 bis 7 vorgesehenen Risikomanagementsystems berücksichtigen die Anbieter, ob angesichts seiner Zweckbestimmung das Hochrisiko-KI-System wahrscheinlich nachteilige Auswirkungen auf Personen unter 18 Jahren oder gegebenenfalls andere schutzbedürftige Gruppen haben wird.

(10) Bei Anbietern von Hochrisiko-KI-Systemen, die den Anforderungen an interne Risikomanagementprozesse gemäß anderen einschlägigen Bestimmungen des Unionsrechts unterliegen, können die in den Absätzen 1 bis 9 enthaltenen Aspekte Bestandteil der nach diesem Recht festgelegten Risikomanagementverfahren sein oder mit diesen Verfahren kombiniert werden.

Artikel 10

Daten und Daten-Governance

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

(2) Für Trainings-, Validierungs- und Testdatensätze gelten Daten-Governance- und Datenverwaltungsverfahren, die für die Zweckbestimmung des Hochrisiko-KI-Systems geeignet sind. Diese Verfahren betreffen insbesondere

a) die einschlägigen konzeptionellen Entscheidungen,

b) die Datenerhebungsverfahren und die Herkunft der Daten und im Falle personenbezogener Daten den ursprünglichen Zweck der Datenerhebung,

c) relevante Datenaufbereitungsvorgänge wie Annotation, Kennzeichnung, Bereinigung, Aktualisierung, Anreicherung und Aggregierung,

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

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

f) eine Untersuchung im Hinblick auf mögliche Verzerrungen (Bias), die die Gesundheit und Sicherheit von Personen beeinträchtigen, sich negativ auf die Grundrechte auswirken oder zu einer nach den Rechtsvorschriften der Union verbotenen Diskriminierung führen könnten, insbesondere wenn die Datenausgaben die Eingaben für künftige Operationen beeinflussen,

g) geeignete Maßnahmen zur Erkennung, Verhinderung und Abschwächung möglicher gemäß Buchstabe f ermittelter Verzerrungen,

h) die Ermittlung relevanter Datenlücken oder Mängel, die der Einhaltung dieser Verordnung entgegenstehen, und wie diese Lücken und Mängel behoben werden können.

(3) Die Trainings-, Validierungs- und Testdatensätze müssen im Hinblick auf die Zweckbestimmung relevant, hinreichend repräsentativ und so weit wie möglich fehlerfrei und vollständig sein. Sie müssen die geeigneten statistischen Merkmale, gegebenenfalls auch bezüglich der Personen oder Personengruppen, für die das Hochrisiko-KI-System bestimmungsgemäß verwendet werden soll, haben. Diese Merkmale der Datensätze können auf der Ebene einzelner Datensätze oder auf der Ebene einer Kombination davon erfüllt werden.

(4) Die Datensätze müssen, soweit dies für die Zweckbestimmung erforderlich ist, die entsprechenden Merkmale oder Elemente berücksichtigen, die für die besonderen geografischen, kontextuellen, verhaltensbezogenen oder funktionalen Rahmenbedingungen, unter denen das Hochrisiko-KI-System bestimmungsgemäß verwendet werden soll, typisch sind.

[sn602] GPAI Technische Dokumentation
[sn803] Nichtdiskriminierung
[sn502] Anbieter

(5) Soweit dies für die Erkennung und Korrektur von Verzerrungen im Zusammenhang mit Hochrisiko-KI-Systemen im Einklang mit Absatz 2 Buchstaben f und g dieses Artikels unbedingt erforderlich ist, dürfen die Anbieter solcher Systeme ausnahmsweise besondere Kategorien personenbezogener Daten verarbeiten, wobei sie angemessene Vorkehrungen für den Schutz der Grundrechte und Grundfreiheiten natürlicher Personen treffen müssen. Zusätzlich zu den Bestimmungen der Verordnungen (EU) 2016/679 und (EU) 2018/1725 und der Richtlinie (EU) 2016/680 müssen alle folgenden Bedingungen erfüllt sein, damit eine solche Verarbeitung stattfinden kann:

a) Die Erkennung und Korrektur von Verzerrungen kann durch die Verarbeitung anderer Daten, einschließlich synthetischer oder anonymisierter Daten, nicht effektiv durchgeführt werden;

b) die besonderen Kategorien personenbezogener Daten unterliegen technischen Beschränkungen einer Weiterverwendung der personenbezogenen Daten und modernsten Sicherheits- und Datenschutzmaßnahmen, einschließlich Pseudonymisierung;

c) die besonderen Kategorien personenbezogener Daten unterliegen Maßnahmen, mit denen sichergestellt wird, dass die verarbeiteten personenbezogenen Daten gesichert, geschützt und Gegenstand angemessener Sicherheitsvorkehrungen sind, wozu auch strenge Kontrollen des Zugriffs und seine Dokumentation gehören, um Missbrauch zu verhindern und sicherzustellen, dass nur befugte Personen Zugang zu diesen personenbezogenen Daten mit angemessenen Vertraulichkeitspflichten haben;

[sn303] Technische Dokumentation

d) die besonderen Kategorien personenbezogener Daten werden nicht an Dritte übermittelt oder übertragen, noch haben diese Dritten anderweitigen Zugang zu diesen Daten;

[sn602] GPAI Technische Dokumentation

e) die besonderen Kategorien personenbezogener Daten werden gelöscht, sobald die Verzerrung korrigiert wurde oder das Ende der Speicherfrist für die personenbezogenen Daten erreicht ist, je nachdem, was zuerst eintritt;

[sn505] Konformitätsbewertung

f) die Aufzeichnungen über Verarbeitungstätigkeiten gemäß den Verordnungen (EU) 2016/679 und (EU) 2018/1725 und der Richtlinie (EU) 2016/680 enthalten die Gründe, warum die Verarbeitung besonderer Kategorien personenbezogener Daten für die Erkennung und Korrektur von Verzerrungen unbedingt erforderlich war und warum dieses Ziel mit der Verarbeitung anderer Daten nicht erreicht werden konnte.

(6) Bei der Entwicklung von Hochrisiko-KI-Systemen, in denen keine Techniken eingesetzt werden, bei denen KI-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 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 Abschnitts erfüllt, und dass den zuständigen nationalen Behörden und den notifizierten Stellen die 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. KMU, einschließlich Start-up-Unternehmen, können die in Anhang IV aufgeführten Elemente der technischen Dokumentation in vereinfachter Weise bereitstellen. Zu diesem Zweck erstellt die Kommission ein vereinfachtes Formular für die technische Dokumentation, das auf die Bedürfnisse von kleinen Unternehmen und Kleinstunternehmen zugeschnitten ist. Entscheidet sich ein KMU, einschließlich Start-up-Unternehmen, für eine vereinfachte Bereitstellung der in Anhang IV vorgeschriebenen Angaben, so verwendet es das in diesem Absatz genannte Formular. Die notifizierten Stellen akzeptieren das Formular für die Zwecke der Konformitätsbewertung.

(2) Wird ein Hochrisiko-KI-System, das mit einem Produkt verbunden ist, das unter die in Anhang I Abschnitt A aufgeführten Harmonisierungsrechtsvorschriften der Union fällt, in Verkehr gebracht oder in Betrieb genommen, so wird eine einzige technische Dokumentation erstellt, die alle in Absatz 1 genannten Informationen sowie die nach diesen Rechtsakten erforderlichen Informationen enthält.

(3) Die Kommission ist befugt, wenn dies nötig ist, gemäß Artikel 97 delegierte Rechtsakte zur Änderung des Anhangs IV zu erlassen, 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 Abschnitts erfüllt.

[sn304] Protokollierung

Artikel 12

Aufzeichnungspflichten

(1) Die Technik der Hochrisiko-KI-Systeme muss die automatische Aufzeichnung von Ereignissen (im Folgenden „Protokollierung“) während des Lebenszyklus des Systems ermöglichen.

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

a) die Ermittlung von Situationen, die dazu führen können, dass das Hochrisiko-KI-System ein Risiko im Sinne des Artikels 79 Absatz 1 birgt oder dass es zu einer wesentlichen Änderung kommt,

[sn503] Betreiber

b) die Erleichterung der Beobachtung nach dem Inverkehrbringen gemäß Artikel 72 und

[sn502] Anbieter

c) die Überwachung des Betriebs der Hochrisiko-KI-Systeme gemäß Artikel 26 Absatz 5.

(3) Die Protokollierungsfunktionen der in Anhang III Nummer 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 Betreiber

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

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

(3) Die Betriebsanleitungen enthalten mindestens folgende Informationen:

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

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

i) seiner Zweckbestimmung,

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

iii) aller bekannten oder vorhersehbaren Umstände bezüglich der Verwendung des Hochrisiko-KI-Systems im Einklang mit seiner Zweckbestimmung oder einer vernünftigerweise vorhersehbaren Fehlanwendung, die zu den in Artikel 9 Absatz 2 genannten Risiken für die Gesundheit und Sicherheit oder die Grundrechte führen können,

iv) gegebenenfalls der technischen Fähigkeiten und Merkmale des Hochrisiko-KI-Systems, um Informationen bereitzustellen, die zur Erläuterung seiner Ausgaben relevant sind;

v) gegebenenfalls seiner Leistung in Bezug auf bestimmte Personen oder Personengruppen, auf die das System bestimmungsgemäß angewandt werden soll;

[sn505] Konformitätsbewertung

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

vii) gegebenenfalls Informationen, die es den Betreibern ermöglichen, die Ausgabe des Hochrisiko-KI-Systems zu interpretieren und es angemessen zu nutzen;

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

[sn306] Menschliche Aufsicht

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

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

f) gegebenenfalls eine Beschreibung der in das Hochrisiko-KI-System integrierten Mechanismen, die es den Betreibern ermöglicht, die Protokolle im Einklang mit Artikel 12 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 ihrer Verwendung — auch mit geeigneten Instrumenten einer Mensch-Maschine-Schnittstelle — von natürlichen Personen wirksam beaufsichtigt werden können.

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

(3) Die Aufsichtsmaßnahmen müssen den Risiken, dem Grad der Autonomie und dem Kontext der Nutzung des Hochrisiko-KI-Systems angemessen sein und werden durch eine oder beide der folgenden Arten von Vorkehrungen gewährleistet:

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

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

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

a) die einschlägigen Fähigkeiten und Grenzen des Hochrisiko-KI-Systems angemessen zu verstehen und seinen Betrieb ordnungsgemäß zu überwachen, einschließlich in Bezug auf das Erkennen und Beheben von Anomalien, Fehlfunktionen und unerwarteter Leistung;

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

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

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

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

[sn307] Genauigkeit, Robustheit und Cybersicherheit

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

Die Anforderung einer getrennten Überprüfung durch mindestens zwei natürliche Personen gilt nicht für Hochrisiko-KI-Systeme, die für Zwecke in den Bereichen Strafverfolgung, Migration, Grenzkontrolle oder Asyl verwendet werden, wenn die Anwendung dieser Anforderung nach Unionsrecht oder nationalem Recht unverhältnismäßig wäre.

Artikel 15

Genauigkeit, Robustheit und Cybersicherheit

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

(2) Um die technischen Aspekte der Art und Weise der Messung des angemessenen Maßes an Genauigkeit und Robustheit gemäß Absatz 1 und anderer einschlägiger Leistungsmetriken anzugehen, fördert die Kommission in Zusammenarbeit mit einschlägigen Interessenträgern und Organisationen wie Metrologie- und Benchmarking-Behörden gegebenenfalls die Entwicklung von Benchmarks und Messmethoden.

(3) Die Maße an Genauigkeit und die relevanten Genauigkeitsmetriken von Hochrisiko-KI-Systemen werden in den ihnen beigefügten Betriebsanleitungen angegeben.

(4) Hochrisiko-KI-Systeme müssen so widerstandsfähig wie möglich 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. In diesem Zusammenhang sind technische und organisatorische Maßnahmen zu ergreifen.

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 Ausgaben, die künftige Vorgänge beeinflussen („Rückkopplungsschleifen“), beseitigt oder so gering wie möglich gehalten wird und sichergestellt wird, dass auf solche Rückkopplungsschleifen angemessen mit geeigneten Risikominderungsmaßnahmen eingegangen wird.

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

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

Die technischen Lösungen für den Umgang mit KI-spezifischen Schwachstellen umfassen gegebenenfalls Maßnahmen, um Angriffe, mit denen versucht wird, eine Manipulation des Trainingsdatensatzes („data poisoning“) oder vortrainierter Komponenten, die beim Training verwendet werden („model poisoning“), vorzunehmen, Eingabedaten, die das KI-Modell zu Fehlern verleiten sollen („adversarial examples“ oder „model evasions“), Angriffe auf vertrauliche Daten oder Modellmängel zu verhüten, zu erkennen, darauf zu reagieren, sie zu beseitigen und zu kontrollieren.

[sn701] Anbieterpflichten

ABSCHNITT 3

Pflichten der Anbieter und Betreiber von Hochrisiko-KI-Systemen und anderer Beteiligter

Artikel 16

Pflichten der Anbieter von Hochrisiko-KI-Systemen

Anbieter von Hochrisiko-KI-Systemen müssen

[sn509] CE-Kennzeichnung

a) sicherstellen, dass ihre Hochrisiko-KI-Systeme die in Abschnitt 2 festgelegten Anforderungen erfüllen;

b) auf dem Hochrisiko-KI-System oder, falls dies nicht möglich ist, auf seiner Verpackung oder in der beigefügten Dokumentation ihren Namen, ihren eingetragenen Handelsnamen bzw. ihre eingetragene Handelsmarke und ihre Kontaktanschrift angeben;

c) über ein Qualitätsmanagementsystem verfügen, das Artikel 17 entspricht;

d) die in Artikel 18 genannte Dokumentation aufbewahren;

e) die von ihren Hochrisiko-KI-Systemen automatisch erzeugten Protokolle gemäß Artikel 19 aufbewahren, wenn diese ihrer Kontrolle unterliegen;

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

g) eine EU-Konformitätserklärung gemäß Artikel 47 ausstellen;

h) die CE-Kennzeichnung an das Hochrisiko-KI-System oder, falls dies nicht möglich ist, auf seiner Verpackung oder in der beigefügten Dokumentation anbringen, um Konformität mit dieser Verordnung gemäß Artikel 48 anzuzeigen;

i) den in Artikel 49 Absatz 1 genannten Registrierungspflichten nachkommen;

j) die erforderlichen Korrekturmaßnahmen ergreifen und die gemäß Artikel 20 erforderlichen Informationen bereitstellen;

k) auf begründete Anfrage einer zuständigen nationalen Behörde nachweisen, dass das Hochrisiko-KI-System die Anforderungen in Abschnitt 2 erfüllt;

l) sicherstellen, dass das Hochrisiko-KI-System die Barrierefreiheitsanforderungen gemäß den Richtlinien (EU) 2016/2102 und (EU) 2019/882 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 dem Hochrisiko-KI-System 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;

[sn301] Risikomanagementsystem

e) die technischen Spezifikationen und Normen, die anzuwenden sind und, falls die einschlägigen harmonisierten Normen nicht vollständig angewandt werden oder sie nicht alle relevanten Anforderungen gemäß Abschnitt 2 abdecken, die Mittel, mit denen gewährleistet werden soll, dass das Hochrisiko-KI-System diese Anforderungen erfüllt;

f) Systeme und Verfahren für das Datenmanagement, einschließlich Datengewinnung, Datenerhebung, 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) die Einrichtung, Anwendung und Aufrechterhaltung eines Systems zur Beobachtung nach dem Inverkehrbringen gemäß Artikel 72;

i) Verfahren zur Meldung eines schwerwiegenden Vorfalls gemäß Artikel 73;

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

k) Systeme und Verfahren für die Aufzeichnung sämtlicher einschlägigen Dokumentation und Informationen;

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

[sn303] Technische Dokumentation

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

(2) Die Umsetzung der in Absatz 1 genannten Aspekte erfolgt in einem angemessenen Verhältnis zur Größe der Organisation des Anbieters. Die Anbieter müssen in jedem Fall den Grad der Strenge und das Schutzniveau einhalten, die erforderlich sind, um die Übereinstimmung ihrer Hochrisiko-KI-Systeme mit dieser Verordnung sicherzustellen.

(3) Anbieter von Hochrisiko-KI-Systemen, die Pflichten in Bezug auf Qualitätsmanagementsysteme oder eine gleichwertige Funktion gemäß den sektorspezifischen Rechtsvorschriften der Union unterliegen, können die in Absatz 1 aufgeführten Aspekte als Bestandteil der nach den genannten Rechtsvorschriften festgelegten Qualitätsmanagementsysteme einbeziehen.

(4) Bei Anbietern, die Finanzinstitute sind und gemäß den Rechtsvorschriften der Union über Finanzdienstleistungen Anforderungen in Bezug auf ihre Regelungen oder Verfahren der internen Unternehmensführung unterliegen, gilt die Pflicht zur Einrichtung eines Qualitätsmanagementsystems — mit Ausnahme des Absatzes 1 Buchstaben g, h und i des vorliegenden Artikels — als erfüllt, wenn die Vorschriften über Regelungen oder Verfahren der internen Unternehmensführung gemäß dem einschlägigen Unionsrecht über Finanzdienstleistungen eingehalten werden. Zu diesem Zweck werden die in Artikel 40 genannten harmonisierten Normen berücksichtigt.

Artikel 18

Aufbewahrung der 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 Dokumentation zu dem in Artikel 17 genannten Qualitätsmanagementsystem;

c) die Dokumentation über etwaige von notifizierten Stellen genehmigte Änderungen;

d) gegebenenfalls die von den notifizierten Stellen ausgestellten Entscheidungen und sonstigen Dokumente;

e) die in Artikel 47 genannte EU-Konformitätserklärung.

(2) 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.

(3) Anbieter, die Finanzinstitute sind und gemäß dem Unionsrecht über Finanzdienstleistungen Anforderungen in Bezug auf ihre Regelungen oder Verfahren der internen Unternehmensführung unterliegen, pflegen die technische Dokumentation als Teil der gemäß dem Unionsrecht über Finanzdienstleistungen aufzubewahrenden Dokumentation.

Artikel 19

Automatisch erzeugte Protokolle

(1) Anbieter von Hochrisiko-KI-Systemen bewahren die von ihren Hochrisiko-KI-Systemen automatisch erzeugten Protokolle gemäß Artikel 12 Absatz 1 auf, soweit diese Protokolle ihrer Kontrolle unterliegen. Unbeschadet des geltenden Unionsrechts oder nationalen Rechts werden die Protokolle für einen der Zweckbestimmung des Hochrisiko-KI-Systems angemessenen Zeitraum von mindestens sechs Monaten aufbewahrt, sofern in den geltenden Rechtsvorschriften der Union, insbesondere im Unionsrecht zum Schutz personenbezogener Daten, oder im geltenden nationalen Recht nichts anderes vorgesehen ist.

(2) Anbieter, die Finanzinstitute sind und gemäß den Rechtsvorschriften der Union über 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 dem einschlägigen Unionsrecht über Finanzdienstleistungen aufzubewahrenden Dokumentation auf.

Artikel 20

Korrekturmaßnahmen und Informationspflicht

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

(2) Birgt das Hochrisiko-KI-System ein Risiko im Sinne des Artikels 79 Absatz 1 und wird sich der Anbieter des Systems dieses Risikos bewusst, so führt er unverzüglich gegebenenfalls gemeinsam mit dem meldenden Betreiber eine Untersuchung der Ursachen durch und informiert er die Marktüberwachungsbehörden, in deren Zuständigkeit das betroffene Hochrisiko-KI-System fällt, und gegebenenfalls die notifizierte Stelle, die eine Bescheinigung für dieses Hochrisiko-KI-System gemäß Artikel 44 ausgestellt hat, insbesondere über die Art der Nichtkonformität und über bereits ergriffene relevante Korrekturmaßnahmen.

Artikel 21

Zusammenarbeit mit den zuständigen Behörden

(1) Anbieter von Hochrisiko-KI-Systemen übermitteln einer zuständigen Behörde auf deren begründete Anfrage sämtliche Informationen und Dokumentation, die erforderlich sind, um die Konformität des Hochrisiko-KI-Systems mit den in Abschnitt 2 festgelegten Anforderungen nachzuweisen, und zwar in einer Sprache, die für die Behörde leicht verständlich ist und bei der es sich um eine der von dem betreffenden Mitgliedstaat angegebenen Amtssprachen der Institutionen der Union handelt.

(2) Auf begründete Anfrage einer zuständigen Behörde gewähren die Anbieter der anfragenden zuständigen Behörde gegebenenfalls auch Zugang zu den automatisch erzeugten Protokollen des Hochrisiko-KI-Systems gemäß Artikel 12 Absatz 1, soweit diese Protokolle ihrer Kontrolle unterliegen.

(3) Alle Informationen, die eine zuständige Behörde aufgrund dieses Artikels erhält, werden im Einklang mit den in Artikel 78 festgelegten Vertraulichkeitspflichten behandelt.

[sn707] Bevollmächtigter

[sn303] Technische Dokumentation

[sn703] Pflichten der Einführer

[sn509] CE-Kennzeichnung

Artikel 22

Bevollmächtigte der Anbieter von Hochrisiko-KI-Systemen

(1) Anbieter, die in Drittländern niedergelassen sind, benennen vor der Bereitstellung ihrer Hochrisiko-KI-Systeme auf dem Unionsmarkt schriftlich einen in der Union niedergelassenen Bevollmächtigten.

(2) Der Anbieter muss seinem Bevollmächtigten ermöglichen, die Aufgaben wahrzunehmen, die im vom Anbieter erhaltenen Auftrag festgelegt sind.

(3) Der Bevollmächtigte nimmt die Aufgaben wahr, die in seinem vom Anbieter erhaltenen Auftrag festgelegt sind. Er stellt den Marktüberwachungsbehörden auf Anfrage eine Kopie des Auftrags in einer von der zuständigen Behörde angegebenen Amtssprache der Institutionen der Union bereit. Für die Zwecke dieser Verordnung ermächtigt der Auftrag den Bevollmächtigten zumindest zur Wahrnehmung folgender Aufgaben:

a) Überprüfung, ob die in Artikel 47 genannte EU-Konformitätserklärung und die technische Dokumentation gemäß Artikel 11 erstellt wurden und ob der Anbieter ein angemessenes Konformitätsbewertungsverfahren durchgeführt hat;

b) 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 in Artikel 47 genannten EU-Konformitätserklärung, der technischen Dokumentation und gegebenenfalls der von der notifizierten Stelle ausgestellten Bescheinigung für die zuständigen Behörden und die in Artikel 74 Absatz 10 genannten nationalen Behörden oder Stellen;

c) Übermittlung sämtlicher — auch der unter Buchstabe b dieses Unterabsatzes genannten — Informationen und Dokumentation, die erforderlich sind, um die Konformität eines Hochrisiko-KI-Systems mit den in Abschnitt 2 festgelegten Anforderungen nachzuweisen, an eine zuständige Behörde auf deren begründete Anfrage, einschließlich der Gewährung des Zugangs zu den vom Hochrisiko-KI-System automatisch erzeugten Protokollen gemäß Artikel 12 Absatz 1, soweit diese Protokolle der Kontrolle des Anbieters unterliegen;

d) Zusammenarbeit mit den zuständigen Behörden auf deren begründete Anfrage bei allen Maßnahmen, die Letztere im Zusammenhang mit dem Hochrisiko-KI-System ergreifen, um insbesondere die von dem Hochrisiko-KI-System ausgehenden Risiken zu verringern und abzumildern;

e) gegebenenfalls die Einhaltung der Registrierungspflichten gemäß Artikel 49 Absatz 1 oder, falls die Registrierung vom Anbieter selbst vorgenommen wird, Sicherstellung der Richtigkeit der in Anhang VIII Abschnitt A Nummer 3 aufgeführten Informationen.

Mit dem Auftrag wird der Bevollmächtigte ermächtigt, neben oder anstelle des Anbieters als Ansprechpartner für die zuständigen Behörden in allen Fragen zu dienen, die die Gewährleistung der Einhaltung dieser Verordnung betreffen.

(4) Der Bevollmächtigte beendet den Auftrag, wenn er der Auffassung ist oder Grund zu der Annahme hat, dass der Anbieter gegen seine Pflichten gemäß dieser Verordnung verstößt. In diesem Fall informiert er unverzüglich die betreffende Marktüberwachungsbehörde und gegebenenfalls die betreffende notifizierte Stelle über die Beendigung des Auftrags und deren Gründe.

Artikel 23

Pflichten der Einführer

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

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

b) der Anbieter die technische Dokumentation gemäß Artikel 11 und Anhang IV erstellt hat;

c) das System mit der erforderlichen CE-Kennzeichnung versehen ist und ihm die in Artikel 47 genannte EU-Konformitätserklärung und Betriebsanleitungen beigefügt sind;

d) der Anbieter einen Bevollmächtigten gemäß Artikel 22 Absatz 1 benannt hat.

(2) Hat ein Einführer hinreichenden Grund zu der Annahme, dass ein Hochrisiko-KI-System nicht dieser Verordnung entspricht oder gefälscht ist oder diesem eine gefälschte Dokumentation beigefügt ist, so bringt er das System erst in Verkehr, nachdem dessen Konformität hergestellt wurde. Birgt das Hochrisiko-KI-System ein Risiko im Sinne des Artikels 79 Absatz 1, so informiert der Einführer den Anbieter des Systems, die Bevollmächtigten und die Marktüberwachungsbehörden darüber.

(3) Die Einführer geben ihren Namen, ihren eingetragenen Handelsnamen oder ihre eingetragene Handelsmarke und die Anschrift, unter der sie in Bezug auf das Hochrisiko-KI-System kontaktiert werden können, auf der Verpackung oder gegebenenfalls in der beigefügten Dokumentation an.

(4) Solange sich ein Hochrisiko-KI-System in ihrer Verantwortung befindet, gewährleisten Einführer, dass — soweit zutreffend — die Lagerungs- oder Transportbedingungen seine Konformität mit den in Abschnitt 2 festgelegten Anforderungen nicht beeinträchtigen.

(5) Die Einführer halten für einen Zeitraum von zehn Jahren ab dem Inverkehrbringen oder der Inbetriebnahme des Hochrisiko-KI-Systems ein Exemplar der von der notifizierten Stelle ausgestellten Bescheinigung sowie gegebenenfalls die Betriebsanleitungen und die in Artikel 47 genannte EU-Konformitätserklärung bereit.

(6) Die Einführer übermitteln den betreffenden nationalen Behörden auf deren begründete Anfrage sämtliche — auch die in Absatz 5 genannten — Informationen und Dokumentation, die erforderlich sind, um die Konformität des Hochrisiko-KI-Systems mit den in Abschnitt 2 festgelegten Anforderungen nachzuweisen, und zwar in einer Sprache, die für jene leicht verständlich ist. Zu diesem Zweck stellen sie auch sicher, dass diesen Behörden die technische Dokumentation zur Verfügung gestellt werden kann.

(7) Die Einführer arbeiten mit den betreffenden nationalen Behörden bei allen Maßnahmen zusammen, die diese Behörden im Zusammenhang mit einem von den Einführern in Verkehr gebrachten Hochrisiko-KI-System ergreifen, um insbesondere die von diesem System ausgehenden Risiken zu verringern und abzumildern.

Artikel 24

Pflichten der Händler

(1) Bevor Händler ein Hochrisiko-KI-System auf dem Markt bereitstellen, überprüfen sie, ob es mit der erforderlichen CE-Kennzeichnung versehen ist, ob ihm eine Kopie der in Artikel 47 genannten EU-Konformitätserklärung und Betriebsanleitungen beigefügt sind und ob der Anbieter und gegebenenfalls der Einführer dieses Systems ihre in Artikel 16 Buchstaben b und c sowie Artikel 23 Absatz 3 festgelegten jeweiligen Pflichten erfüllt haben.

(2) Ist ein Händler der Auffassung oder hat er aufgrund von Informationen, die ihm zur Verfügung stehen, Grund zu der Annahme, dass ein Hochrisiko-KI-System nicht den Anforderungen in Abschnitt 2 entspricht, so stellt er das Hochrisiko-KI-System erst auf dem Markt bereit, nachdem die Konformität des Systems mit den Anforderungen hergestellt wurde. Birgt das Hochrisiko-IT-System zudem ein Risiko im Sinne des Artikels 79 Absatz 1, so informiert der Händler den Anbieter bzw. den Einführer des Systems darüber.

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

(4) Ein Händler, der aufgrund von Informationen, die ihm zur Verfügung stehen, der Auffassung ist oder Grund zu der Annahme hat, dass ein von ihm auf dem Markt bereitgestelltes Hochrisiko-KI-System nicht den Anforderungen in Abschnitt 2 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 79 Absatz 1, so informiert der Händler unverzüglich den Anbieter bzw. den Einführer des Systems sowie die für das betroffene Hochrisiko-KI-System zuständigen Behörden und macht dabei ausführliche Angaben, insbesondere zur Nichtkonformität und zu bereits ergriffenen Korrekturmaßnahmen.

(5) Auf begründete Anfrage einer betreffenden zuständigen Behörde übermitteln die Händler eines Hochrisiko-KI-Systems dieser Behörde sämtliche Informationen und Dokumentation in Bezug auf ihre Maßnahmen gemäß den Absätzen 1 bis 4, die erforderlich sind, um die Konformität dieses Systems mit den in Abschnitt 2 festgelegten Anforderungen nachzuweisen.

(6) Die Händler arbeiten mit den betreffenden zuständigen Behörden bei allen Maßnahmen zusammen, die diese Behörden im Zusammenhang mit einem von den Händlern auf dem Markt bereitgestellten Hochrisiko-KI-System ergreifen, um insbesondere das von diesem System ausgehende Risiko zu verringern oder abzumildern.

Artikel 25

Verantwortlichkeiten entlang der KI-Wertschöpfungskette

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

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

b) wenn sie eine wesentliche Veränderung eines Hochrisiko-KI-Systems, das bereits in Verkehr gebracht oder in Betrieb genommen wurde, so vornehmen, dass es weiterhin ein Hochrisiko-KI-System gemäß Artikel 6 bleibt;

c) wenn sie die Zweckbestimmung eines KI-Systems, einschließlich eines KI-Systems mit allgemeinem Verwendungszweck, das nicht als hochriskant eingestuft wurde und bereits in Verkehr gebracht oder in Betrieb genommen wurde, so verändern, dass das betreffende KI-System zu einem Hochrisiko-KI-System im Sinne von Artikel 6 wird.

(2) Unter den in Absatz 1 genannten Umständen gilt der Anbieter, der das KI-System ursprünglich in Verkehr gebracht oder in Betrieb genommen hatte, nicht mehr als Anbieter dieses spezifischen KI-Systems für die Zwecke dieser Verordnung. Dieser Erstanbieter arbeitet eng mit neuen Anbietern zusammen, stellt die erforderlichen Informationen zur Verfügung und sorgt für den vernünftigerweise zu erwartenden technischen Zugang und sonstige Unterstützung, die für die Erfüllung der in dieser Verordnung festgelegten Pflichten, insbesondere in Bezug auf die Konformitätsbewertung von Hochrisiko-KI-Systemen, erforderlich sind. Dieser Absatz gilt nicht in Fällen, in denen der Erstanbieter eindeutig festgelegt hat, dass sein KI-System nicht in ein Hochrisiko-KI-System umgewandelt werden darf und daher nicht der Pflicht zur Übergabe der Dokumentation unterliegt.

[sn705] Verantwortlichkeiten in der Wertschöpfungskette

(3) Im Falle von Hochrisiko-KI-Systemen, bei denen es sich um Sicherheitsbauteile von Produkten handelt, die unter die in Anhang I Abschnitt A aufgeführten Harmonisierungsrechtsvorschriften der Union fallen, gilt der Produkthersteller als Anbieter des Hochrisiko-KI-Systems und unterliegt in den beiden nachfolgenden Fällen den Pflichten nach Artikel 16:

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

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

(4) Der Anbieter eines Hochrisiko-KI-Systems und der Dritte, der ein KI-System, Instrumente, Dienste, Komponenten oder Verfahren bereitstellt, die in einem Hochrisiko-KI-System verwendet oder integriert werden, legen in einer schriftlichen Vereinbarung die Informationen, die Fähigkeiten, den technischen Zugang und die sonstige Unterstützung nach dem allgemein anerkannten Stand der Technik fest, die erforderlich sind, damit der Anbieter des Hochrisiko-KI-Systems die in dieser Verordnung festgelegten Pflichten vollständig erfüllen kann. Dieser Absatz gilt nicht für Dritte, die Instrumente, Dienste, Verfahren oder Komponenten, bei denen es sich nicht um KI-Modelle mit allgemeinem Verwendungszweck handelt, im Rahmen einer freien und quelloffenen Lizenz öffentlich zugänglich machen.

Das Büro für Künstliche Intelligenz kann freiwillige Musterbedingungen für Verträge zwischen Anbietern von Hochrisiko-KI-Systemen und Dritten, die Instrumente, Dienste, Komponenten oder Verfahren bereitstellen, die für Hochrisiko-KI-Systeme verwendet oder in diese integriert werden, ausarbeiten und empfehlen. Bei der Ausarbeitung dieser freiwilligen Musterbedingungen berücksichtigt das Büro für Künstliche Intelligenz mögliche vertragliche Anforderungen, die in bestimmten Sektoren oder Geschäftsfällen gelten. Die freiwilligen Musterbedingungen werden veröffentlicht und sind kostenlos in einem leicht nutzbaren elektronischen Format verfügbar.

(5) Die Absätze 2 und 3 berühren nicht die Notwendigkeit, Rechte des geistigen Eigentums, vertrauliche Geschäftsinformationen und Geschäftsgeheimnisse im Einklang mit dem Unionsrecht und dem nationalen Recht zu achten und zu schützen.

Artikel 26

Pflichten der Betreiber von Hochrisiko-KI-Systemen

(1) Die Betreiber von Hochrisiko-KI-Systemen treffen geeignete technische und organisatorische Maßnahmen, um sicherzustellen, dass sie solche Systeme entsprechend der den Systemen beigefügten Betriebsanleitungen und gemäß den Absätzen 3 und 6 verwenden.

(2) Die Betreiber übertragen natürlichen Personen, die über die erforderliche Kompetenz, Ausbildung und Befugnis verfügen, die menschliche Aufsicht und lassen ihnen die erforderliche Unterstützung zukommen.

(3) Die Pflichten nach den Absätzen 1 und 2 lassen sonstige Pflichten der Betreiber nach Unionsrecht oder nationalem Recht sowie die Freiheit der Betreiber bei der Organisation ihrer eigenen Ressourcen und Tätigkeiten zur Wahrnehmung der vom Anbieter angegebenen Maßnahmen der menschlichen Aufsicht unberührt.

(4) Unbeschadet der Absätze 1 und 2 und soweit die Eingabedaten ihrer Kontrolle unterliegen, sorgen die Betreiber dafür, dass die Eingabedaten der Zweckbestimmung des Hochrisiko-KI-Systems entsprechen und ausreichend repräsentativ sind.

(5) Die Betreiber überwachen den Betrieb des Hochrisiko-KI-Systems anhand der Betriebsanleitung und informieren gegebenenfalls die Anbieter gemäß Artikel 72. Haben Betreiber Grund zu der Annahme, dass die Verwendung gemäß der Betriebsanleitung dazu führen kann, dass dieses Hochrisiko-KI-System ein Risiko im Sinne des Artikels 79 Absatz 1 birgt, so informieren sie unverzüglich den Anbieter oder Händler und die zuständige Marktüberwachungsbehörde und setzen die Verwendung dieses Systems aus. Haben die Betreiber einen schwerwiegenden Vorfall festgestellt, informieren sie auch unverzüglich zuerst den Anbieter und dann den Einführer oder Händler und die zuständigen Marktüberwachungsbehörden über diesen Vorfall. Kann der Betreiber den Anbieter nicht erreichen, so gilt Artikel 73 entsprechend. Diese Pflicht gilt nicht für sensible operative Daten von Betreibern von KI-Systemen, die Strafverfolgungsbehörden sind.

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

(6) Betreiber von Hochrisiko-KI-Systemen bewahren die von ihrem Hochrisiko-KI-System automatisch erzeugten Protokolle, soweit diese Protokolle ihrer Kontrolle unterliegen, für einen der Zweckbestimmung des Hochrisiko-KI-Systems angemessenen Zeitraum von mindestens sechs Monaten auf, sofern im geltenden Unionsrecht, insbesondere im Unionsrecht über den Schutz personenbezogener Daten, oder im geltenden nationalen Recht nichts anderes bestimmt ist.

[sn908] EU-Datenbank

Betreiber, die Finanzinstitute sind und gemäß den Rechtsvorschriften der Union über Finanzdienstleistungen Anforderungen in Bezug auf ihre Regelungen oder Verfahren der internen Unternehmensführung unterliegen, bewahren die Protokolle als Teil der gemäß einschlägigem Unionsecht über Finanzdienstleistungen aufzubewahrenden Dokumentation auf.

(7) Vor der Inbetriebnahme oder Verwendung eines Hochrisiko-KI-Systems am Arbeitsplatz informieren Betreiber, die Arbeitgeber sind, die Arbeitnehmervertreter und die betroffenen Arbeitnehmer darüber, dass sie der Verwendung des Hochrisiko-KI-Systems unterliegen werden. Diese Informationen werden gegebenenfalls im Einklang mit den Vorschriften und Gepflogenheiten auf Unionsebene und nationaler Ebene in Bezug auf die Unterrichtung der Arbeitnehmer und ihrer Vertreter bereitgestellt.

(8) Betreiber von Hochrisiko-KI-Systemen, bei denen es sich um Organe, Einrichtungen oder sonstige Stellen der Union handelt, müssen den Registrierungspflichten gemäß Artikel 49 nachkommen. Stellen diese Betreiber fest, dass das Hochrisiko-KI-System, dessen Verwendung sie planen, nicht in der in Artikel 71 genannten EU-Datenbank registriert wurde, sehen sie von der Verwendung dieses Systems ab und informieren den Anbieter oder den Händler.

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

(10) Unbeschadet der Richtlinie (EU) 2016/680 beantragt der Betreiber eines Hochrisiko-KI-Systems zur nachträglichen biometrischen Fernfernidentifizierung im Rahmen von Ermittlungen zur gezielten Suche einer Person, die der Begehung einer Straftat verdächtigt wird oder aufgrund einer solchen verurteilt wurde, vorab oder unverzüglich, spätestens jedoch binnen 48 Stunden bei einer Justizbehörde oder einer Verwaltungsbehörde, deren Entscheidung bindend ist und einer justiziellen Überprüfung unterliegt, die Genehmigung für die Nutzung dieses Systems, es sei denn, es wird zur erstmaligen Identifizierung eines potenziellen Verdächtigen auf der Grundlage objektiver und nachprüfbarer Tatsachen, die in unmittelbarem Zusammenhang mit der Straftat stehen, verwendet. Jede Verwendung ist auf das für die Ermittlung einer bestimmten Straftat unbedingt erforderliche Maß zu beschränken.

Wird die gemäß Unterabsatz 1 beantragte Genehmigung abgelehnt, so wird die Verwendung des mit dieser beantragten Genehmigung verbundenen Systems zur nachträglichen biometrischen Fernidentifizierung mit sofortiger Wirkung eingestellt und werden die personenbezogenen Daten, die im Zusammenhang mit der Verwendung des Hochrisiko-KI-Systems stehen, für die die Genehmigung beantragt wurde, gelöscht.

In keinem Fall darf ein solches Hochrisiko-KI-System zur nachträglichen biometrischen Fernidentifizierung zu Strafverfolgungszwecken in nicht zielgerichteter Weise und ohne jeglichen Zusammenhang mit einer Straftat, einem Strafverfahren, einer tatsächlichen und bestehenden oder tatsächlichen und vorhersehbaren Gefahr einer Straftat oder der Suche nach einer bestimmten vermissten Person verwendet werden. Es muss sichergestellt werden, dass die Strafverfolgungsbehörden keine ausschließlich auf der Grundlage der Ausgabe solcher Systeme zur nachträglichen biometrischen Fernidentifizierung beruhende Entscheidung, aus der sich eine nachteilige Rechtsfolge für eine Person ergibt, treffen.

[sn503] Betreiber

Dieser Absatz gilt unbeschadet des Artikels 9 der Verordnung (EU) 2016/679 und des Artikels 10 der Richtlinie (EU) 2016/680 für die Verarbeitung biometrischer Daten.

Unabhängig vom Zweck oder Betreiber wird jede Verwendung solcher Hochrisiko-KI-Systeme in der einschlägigen Polizeiakte dokumentiert und der zuständigen Marktüberwachungsbehörde und der nationalen Datenschutzbehörde auf Anfrage zur Verfügung gestellt, wovon die Offenlegung sensibler operativer Daten im Zusammenhang mit der Strafverfolgung ausgenommen ist. Dieser Unterabsatz berührt nicht die den Aufsichtsbehörden durch die Richtlinie (EU) 2016/680 übertragenen Befugnisse.

Die Betreiber legen den zuständigen Marktüberwachungsbehörden und den nationalen Datenschutzbehörden Jahresberichte über ihre Verwendung von Systemen zur nachträglichen biometrischen Fernidentifizierung vor, wovon die Offenlegung sensibler operativer Daten im Zusammenhang mit der Strafverfolgung ausgenommen ist. Die Berichte können eine Zusammenfassung sein, damit sie mehr als einen Einsatz abdecken.

[sn706] Grundrechte-Folgenabschätzung

Die Mitgliedstaaten können im Einklang mit dem Unionsrecht strengere Rechtsvorschriften für die Verwendung von Systemen zur nachträglichen biometrischen Fernidentifizierung erlassen.

[sn306] Menschliche Aufsicht

(11) Unbeschadet des Artikels 50 der vorliegenden Verordnung informieren die Betreiber der in Anhang III aufgeführten Hochrisiko-KI-Systeme, die natürliche Personen betreffende Entscheidungen treffen oder bei solchen Entscheidungen Unterstützung leisten, die natürlichen Personen darüber, dass sie der Verwendung des Hochrisiko-KI-Systems unterliegen. Für Hochrisiko-KI-Systeme, die zu Strafverfolgungszwecken verwendet werden, gilt Artikel 13 der Richtlinie (EU) 2016/680.

(12) Die Betreiber arbeiten mit den zuständigen Behörden bei allen Maßnahmen zusammen, die diese Behörden im Zusammenhang mit dem Hochrisiko-KI-System zur Umsetzung dieser Verordnung ergreifen.

[sn502] Anbieter

Artikel 27

Grundrechte-Folgenabschätzung für Hochrisiko-KI-Systeme

(1) Vor der Inbetriebnahme eines Hochrisiko-KI-Systems gemäß Artikel 6 Absatz 2 — mit Ausnahme von Hochrisiko-KI-Systemen, die in dem in Anhang III Nummer 2 aufgeführten Bereich verwendet werden sollen — führen Betreiber, bei denen es sich um Einrichtungen des öffentlichen Rechts oder private Einrichtungen, die öffentliche Dienste erbringen, handelt, und Betreiber von Hochrisiko-KI-Systemen gemäß Anhang III Nummer 5 Buchstaben b und c eine Abschätzung der Auswirkungen, die die Verwendung eines solchen Systems auf die Grundrechte haben kann, durch. Zu diesem Zweck führen die Betreiber eine Abschätzung durch, die Folgendes umfasst:

a) eine Beschreibung der Verfahren des Betreibers, bei denen das Hochrisiko-KI-System im Einklang mit seiner Zweckbestimmung verwendet wird;

b) eine Beschreibung des Zeitraums und der Häufigkeit, innerhalb dessen bzw. mit der jedes Hochrisiko-KI-System verwendet werden soll;

c) die Kategorien der natürlichen Personen und Personengruppen, die von seiner Verwendung im spezifischen Kontext betroffen sein könnten;

d) die spezifischen Schadensrisiken, die sich auf die gemäß Buchstabe c dieses Absatzes ermittelten Kategorien natürlicher Personen oder Personengruppen auswirken könnten, unter Berücksichtigung der vom Anbieter gemäß Artikel 13 bereitgestellten Informationen;

e) eine Beschreibung der Umsetzung von Maßnahmen der menschlichen Aufsicht entsprechend den Betriebsanleitungen;

f) die Maßnahmen, die im Falle des Eintretens dieser Risiken zu ergreifen sind, einschließlich der Regelungen für die interne Unternehmensführung und Beschwerdemechanismen.

[sn503] Betreiber

[sn706] Grundrechte-Folgenabschätzung

[sn901] Büro für Künstliche Intelligenz

(2) Die in Absatz 1 festgelegte Pflicht gilt für die erste Verwendung eines Hochrisiko-KI-Systems. Der Betreiber kann sich in ähnlichen Fällen auf zuvor durchgeführte Grundrechte-Folgenabschätzungen oder bereits vorhandene Folgenabschätzungen, die vom Anbieter durchgeführt wurden, stützen. Gelangt der Betreiber während der Verwendung des Hochrisiko-KI-Systems zur Auffassung, dass sich eines der in Absatz 1 aufgeführten Elemente geändert hat oder nicht mehr auf dem neuesten Stand ist, so unternimmt der Betreiber die erforderlichen Schritte, um die Informationen zu aktualisieren.

(3) Sobald die Abschätzung gemäß Absatz 1 des vorliegenden Artikels durchgeführt wurde, teilt der Betreiber der Marktüberwachungsbehörde ihre Ergebnisse mit, indem er das ausgefüllte, in Absatz 5 des vorliegenden Artikels genannte Muster als Teil der Mitteilung übermittelt. In dem in Artikel 46 Absatz 1 genannten Fall können die Betreiber von der Mitteilungspflicht befreit werden.

(4) Wird eine der in diesem Artikel festgelegten Pflichten bereits infolge einer gemäß Artikel 35 der Verordnung (EU) 2016/679 oder Artikel 27 der Richtlinie (EU) 2016/680 durchgeführten Datenschutz-Folgenabschätzung erfüllt, so ergänzt die Grundrechte-Folgenabschätzung gemäß Absatz 1 des vorliegenden Artikels diese Datenschutz-Folgenabschätzung.

(5) Das Büro für Künstliche Intelligenz arbeitet ein Muster für einen Fragebogen — auch mithilfe eines automatisierten Instruments — aus, um die Betreiber in die Lage zu versetzen, ihren Pflichten gemäß diesem Artikel in vereinfachter Weise nachzukommen.

ABSCHNITT 4

Notifizierende Behörden und notifizierte Stellen

Artikel 28

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. Diese Verfahren werden in Zusammenarbeit zwischen den notifizierenden Behörden aller Mitgliedstaaten entwickelt.

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

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

(4) Notifizierende Behörden werden so organisiert, 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 gemäß Artikel 78 die Vertraulichkeit der von ihnen erlangten Informationen.

(7) Notifizierende Behörden verfügen über eine angemessene Anzahl kompetenter Mitarbeiter, sodass sie ihre Aufgaben ordnungsgemäß wahrnehmen können. Die kompetenten Mitarbeiter verfügen — wo erforderlich — über das für ihre Funktion erforderliche Fachwissen in Bereichen wie Informationstechnologie sowie KI und Recht, einschließlich der Überwachung der Grundrechte.

Artikel 29

Antrag einer Konformitätsbewertungsstelle auf Notifizierung

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

(2) Dem Antrag auf Notifizierung legen sie eine Beschreibung der Konformitätsbewertungstätigkeiten, des bzw. der Konformitätsbewertungsmodule und der Art 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 31 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 betreffende 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 31 erfüllt.

(4) 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 den Absätzen 2 und 3 des vorliegenden Artikels genannte Dokumentation immer dann, wenn sich relevante Änderungen ergeben, damit die für notifizierte Stellen zuständige Behörde überwachen und überprüfen kann, ob die Anforderungen des Artikels 31 kontinuierlich erfüllt sind.

Artikel 30

Notifizierungsverfahren

(1) Die notifizierenden Behörden dürfen nur Konformitätsbewertungsstellen notifizieren, die die Anforderungen des Artikels 31 erfüllen.

(2) Die notifizierenden Behörden unterrichten die Kommission und die übrigen Mitgliedstaaten mithilfe des elektronischen Notifizierungsinstruments, das von der Kommission entwickelt und verwaltet wird, über jede Konformitätsbewertungsstelle gemäß Absatz 1.

(3) Die Notifizierung gemäß Absatz 2 des vorliegenden Artikels enthält vollständige Angaben zu den Konformitätsbewertungstätigkeiten, dem betreffenden Konformitätsbewertungsmodul oder den betreffenden Konformitätsbewertungsmodulen, den betreffenden Arten der KI-Systeme und der einschlägigen Bestätigung der Kompetenz. Beruht eine Notifizierung nicht auf einer Akkreditierungsurkunde gemäß Artikel 29 Absatz 2, so legt die notifizierende Behörde der Kommission und den anderen Mitgliedstaaten die Unterlagen vor, die die Kompetenz der Konformitätsbewertungsstelle und die Vereinbarungen nachweisen, die getroffen wurden, um sicherzustellen, dass die Stelle regelmäßig überwacht wird und weiterhin die Anforderungen des Artikels 31 erfüllt.

(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, falls eine Akkreditierungsurkunde gemäß Artikel 29 Absatz 2 vorgelegt wird, oder innerhalb von zwei Monaten nach einer Notifizierung durch eine notifizierende Behörde, falls als Nachweis Unterlagen gemäß Artikel 29 Absatz 3 vorgelegt werden, Einwände erhoben haben.

(5) Werden Einwände erhoben, konsultiert die Kommission unverzüglich die betreffenden Mitgliedstaaten und die Konformitätsbewertungsstelle. Im Hinblick darauf entscheidet die Kommission, ob die Genehmigung gerechtfertigt ist. Die Kommission richtet ihren Beschluss an die betroffenen Mitgliedstaaten und an die zuständige Konformitätsbewertungsstelle.

Artikel 31

Anforderungen an notifizierte Stellen

(1) Eine notifizierte Stelle wird nach dem nationalen Recht eines Mitgliedstaats gegründet und muss mit Rechtspersönlichkeit ausgestattet sein.

(2) Die notifizierten Stellen müssen die zur Wahrnehmung ihrer Aufgaben erforderlichen Anforderungen an die Organisation, das Qualitätsmanagement, die Ressourcenausstattung und die Verfahren sowie angemessene Cybersicherheitsanforderungen erfüllen.

(3) Die Organisationsstruktur, die Zuweisung der Zuständigkeiten, die Berichtslinien und die Funktionsweise der notifizierten Stellen müssen das Vertrauen in ihre Leistung und in die Ergebnisse der von ihnen durchgeführten Konformitätsbewertungstätigkeiten gewährleisten.

(4) Die notifizierten Stellen müssen von dem Anbieter eines Hochrisiko-KI-Systems, zu dem sie Konformitätsbewertungstätigkeiten durchführen, unabhängig sein. Außerdem müssen die notifizierten Stellen von allen anderen Akteuren, die ein wirtschaftliches Interesse an den bewerteten Hochrisiko-KI-Systemen haben, und von allen Wettbewerbern des Anbieters unabhängig sein. Dies schließt die Verwendung von bewerteten Hochrisiko-KI-Systemen, die für die Tätigkeit der Konformitätsbewertungsstelle nötig sind, oder die Verwendung solcher Hochrisiko-KI-Systeme zum persönlichen Gebrauch nicht aus.

(5) Weder die Konformitätsbewertungsstelle, ihre oberste Leitungsebene noch die für die Erfüllung ihrer Konformitätsbewertungsaufgaben zuständigen Mitarbeiter dürfen direkt an Entwurf, Entwicklung, Vermarktung oder Verwendung von Hochrisiko-KI-Systemen beteiligt sein oder die an diesen Tätigkeiten beteiligten Parteien vertreten. Sie dürfen sich nicht mit Tätigkeiten befassen, die ihre Unabhängigkeit bei der Beurteilung oder ihre Integrität im Zusammenhang mit den Konformitätsbewertungstätigkeiten, für die sie notifiziert sind, beeinträchtigen könnten. Dies gilt besonders für Beratungsdienstleistungen.

(6) Notifizierte Stellen werden so organisiert und geführt, 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, von allen Mitarbeitern und bei allen Bewertungstätigkeiten gefördert und angewandt werden.

(7) Die notifizierten Stellen gewährleisten durch dokumentierte Verfahren, dass ihre Mitarbeiter, Ausschüsse, Zweigstellen, Unterauftragnehmer sowie alle zugeordneten Stellen oder Mitarbeiter externer Einrichtungen die Vertraulichkeit der Informationen, die bei der Durchführung der Konformitätsbewertungstätigkeiten in ihren Besitz gelangen, im Einklang mit Artikel 78 wahren, außer wenn ihre 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.

(8) Die notifizierten Stellen verfügen über Verfahren zur Durchführung ihrer Tätigkeiten unter gebührender Berücksichtigung der Größe eines Betreibers, des Sektors, in dem er tätig ist, seiner Struktur sowie der Komplexität des betreffenden KI-Systems.

(9) 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 niedergelassen sind, gedeckt oder dieser Mitgliedstaat ist selbst unmittelbar für die Konformitätsbewertung zuständig.

(10) Die notifizierten Stellen müssen in der Lage sein, ihre Aufgaben gemäß dieser Verordnung 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 durchgeführt werden.

(11) Die notifizierten Stellen müssen über ausreichende interne Kompetenzen verfügen, um die von externen Stellen in ihrem Namen wahrgenommen Aufgaben wirksam beurteilen zu können. Die notifizierten Stellen müssen ständig über ausreichendes administratives, technisches, juristisches und wissenschaftliches Personal verfügen, das Erfahrungen und Kenntnisse in Bezug auf einschlägige Arten der KI-Systeme, Daten und Datenverarbeitung sowie die in Abschnitt 2 festgelegten Anforderungen besitzt.

(12) 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.

Artikel 32

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, so wird davon ausgegangen, dass sie die Anforderungen des Artikels 31, soweit diese von den geltenden harmonisierten Normen erfasst werden, erfüllt.

Artikel 33

Zweigstellen notifizierter Stellen und Vergabe von Unteraufträgen

[sn502] Anbieter

(1) Vergibt eine 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 31 erfüllt, und informiert die notifizierende Behörde darüber.

(2) Die notifizierten Stellen tragen die volle Verantwortung für Arbeiten, die von jedweden Unterauftragnehmern oder Zweigstellen ausgeführt werden.

(3) Tätigkeiten dürfen nur mit Zustimmung des Anbieters an einen Unterauftragnehmer vergeben oder einer Zweigstelle übertragen werden. Die notifizierten Stellen veröffentlichen ein Verzeichnis ihrer Zweigstellen.

(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 Unterauftragsvergabe für die notifizierende Behörde bereitgehalten.

Artikel 34

Operative Pflichten der notifizierten Stellen

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

(2) Die notifizierten Stellen vermeiden bei der Durchführung ihrer Tätigkeiten unnötige Belastungen für die Anbieter und berücksichtigen gebührend die Größe des Anbieters, den Sektor, in dem er tätig ist, seine Struktur sowie die Komplexität des betreffenden Hochrisiko-KI-Systems, um insbesondere den Verwaltungsaufwand und die Befolgungskosten für Kleinstunternehmen und kleine Unternehmen im Sinne der Empfehlung 2003/361/EG zu minimieren. Die notifizierte Stelle muss jedoch den Grad der Strenge und das Schutzniveau einhalten, die für die Konformität des Hochrisiko-KI-Systems mit den Anforderungen dieser Verordnung erforderlich sind.

(3) Die notifizierten Stellen machen der in Artikel 28 genannten notifizierenden Behörde sämtliche einschlägige Dokumentation, einschließlich der Dokumentation des Anbieters, zugänglich bzw. übermitteln diese auf Anfrage, damit diese Behörde ihre Bewertungs-, Benennungs-, Notifizierungs- und Überwachungstätigkeiten durchführen kann und die Bewertung gemäß diesem Abschnitt erleichtert wird.

Artikel 35

Identifizierungsnummern und Verzeichnisse notifizierter Stellen

(1) Die Kommission weist jeder notifizierten Stelle eine einzige Identifizierungsnummer zu, selbst wenn eine Stelle nach mehr als einem Rechtsakt der Union notifiziert wurde.

(2) Die Kommission veröffentlicht das Verzeichnis der nach dieser Verordnung notifizierten Stellen samt ihren Identifizierungsnummern und den Tätigkeiten, für die sie notifiziert wurden. Die Kommission stellt sicher, dass das Verzeichnis auf dem neuesten Stand gehalten wird.

Artikel 36

Änderungen der Notifizierungen

(1) Die notifizierende Behörde unterrichtet die Kommission und die anderen Mitgliedstaaten mithilfe des in Artikel 30 Absatz 2 genannten elektronischen Notifizierungsinstruments über alle relevanten Änderungen der Notifizierung einer notifizierten Stelle.

(2) Für Erweiterungen des Anwendungsbereichs der Notifizierung gelten die in den Artikeln 29 und 30 festgelegten Verfahren.

Für andere Änderungen der Notifizierung als Erweiterungen ihres Anwendungsbereichs gelten die in den Absätzen 3 bis 9 dargelegten Verfahren.

[sn502] Anbieter

(3) Beschließt eine notifizierte Stelle die Einstellung ihrer Konformitätsbewertungstätigkeiten, so informiert sie die betreffende notifizierende Behörde und die betreffenden Anbieter so bald wie möglich und im Falle einer geplanten Einstellung ihrer Tätigkeiten mindestens ein Jahr vor deren Einstellung darüber. Die Bescheinigungen der notifizierten Stelle können für einen 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 Hochrisiko-KI-Systeme übernimmt. Die letztgenannte notifizierte Stelle führt vor Ablauf dieser Frist von neun Monaten eine vollständige Bewertung der betroffenen Hochrisiko-KI-Systeme durch, bevor sie für diese neue Bescheinigungen ausstellt. Stellt die notifizierte Stelle ihre Tätigkeit ein, so widerruft die notifizierende Behörde die Benennung.

(4) Hat eine notifizierende Behörde hinreichenden Grund zu der Annahme, dass eine notifizierte Stelle die in Artikel 31 festgelegten Anforderungen nicht mehr erfüllt oder dass sie ihren Pflichten nicht nachkommt, so untersucht die notifizierende Behörde den Sachverhalt unverzüglich und mit äußerster Sorgfalt. In diesem Zusammenhang teilt sie der betreffenden notifizierten Stelle die erhobenen Einwände mit und gibt ihr die Möglichkeit, dazu Stellung zu nehmen. Kommt die notifizierende Behörde zu dem Schluss, dass die notifizierte Stelle die in Artikel 31 festgelegten Anforderungen nicht mehr erfüllt oder dass sie ihren Pflichten nicht nachkommt, schränkt sie die Benennung gegebenenfalls ein, setzt sie aus oder widerruft sie, je nach Schwere der Nichterfüllung dieser Anforderungen oder Pflichtverletzung. Sie informiert die Kommission und die anderen Mitgliedstaaten unverzüglich darüber.

(5) Wird die Benennung einer notifizierten Stelle ausgesetzt, eingeschränkt oder vollständig oder teilweise widerrufen, so informiert die notifizierte Stelle die betreffenden Anbieter innerhalb von zehn Tagen darüber.

(6) Wird eine Benennung 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.

(7) Wird eine Benennung eingeschränkt, ausgesetzt 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 Notifizierung der Änderungen der Benennung einen Bericht über ihre diesbezüglichen Ergebnisse vor;

c) sie weist die notifizierte Stelle zur Gewährleistung der fortlaufenden Konformität der im Verkehr befindlichen Hochrisiko-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 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; diese Behörde ergreift erforderlichenfalls geeignete Maßnahmen, um ein mögliches Risiko für Gesundheit, Sicherheit oder Grundrechte zu verhindern.

(8) Abgesehen von den Fällen, in denen Bescheinigungen nicht ordnungsgemäß ausgestellt wurden und in denen eine Benennung ausgesetzt oder eingeschränkt wurde, bleiben die Bescheinigungen unter einem der folgenden Umstände 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 für Maßnahmen zur Aufhebung der Aussetzung oder Einschränkung genannt 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 notifizierende Behörde feststellt, dass die notifizierte Stelle nicht in der Lage ist, bestehende ausgestellte Bescheinigungen weiterzuführen, so bestätigt der Anbieter des von der Bescheinigung abgedeckten Systems den zuständigen nationalen Behörden des Mitgliedstaats, in dem er 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 Bescheinigung übernimmt und dass sie während der Dauer der Aussetzung oder Einschränkung für die Bescheinigung verantwortlich bleibt.

(9) 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 Hochrisiko-KI-Systems seine eingetragene Niederlassung hat, hat bestätigt, dass im Zusammenhang mit den betreffenden Hochrisiko-KI-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 KI-Systeme übernehmen und deren Bewertung innerhalb von 12 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 zusätzliche Zeiträume von je drei Monaten, jedoch nicht um insgesamt mehr als 12 Monate, verlängern.

Die zuständige nationale Behörde oder die notifizierte Stelle, die die Aufgaben der von der Benennungsänderung betroffenen notifizierten Stelle übernimmt, informiert unverzüglich die Kommission, die anderen Mitgliedstaaten und die anderen notifizierten Stellen darüber.

Artikel 37

Anfechtungen der Kompetenz notifizierter Stellen

(1) Die Kommission untersucht erforderlichenfalls alle Fälle, in denen begründete Zweifel an der Kompetenz einer notifizierten Stelle oder daran bestehen, dass eine notifizierte Stelle die in Artikel 31 festgelegten Anforderungen und ihre geltenden Pflichten weiterhin erfüllt.

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

(3) Die Kommission stellt sicher, dass alle im Verlauf ihrer Untersuchungen gemäß diesem Artikel erlangten sensiblen Informationen gemäß Artikel 78 vertraulich behandelt werden.

(4) Stellt die Kommission fest, dass eine notifizierte Stelle die Anforderungen für ihre Notifizierung nicht oder nicht mehr erfüllt, so informiert sie den notifizierenden Mitgliedstaat entsprechend und fordert ihn auf, die erforderlichen Abhilfemaßnahmen zu treffen, einschließlich einer Aussetzung oder eines Widerrufs der Notifizierung, sofern dies nötig ist. Versäumt es ein Mitgliedstaat, die erforderlichen Abhilfemaßnahmen zu ergreifen, kann die Kommission die Benennung im Wege eines Durchführungsrechtsakts aussetzen, einschränken oder widerrufen. Dieser Durchführungsrechtsakt wird gemäß dem in Artikel 98 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) Jede notifizierende Behörde sorgt dafür, dass sich die von ihr notifizierten Stellen direkt oder über benannte Vertreter an der Arbeit der in Absatz 1 genannten Gruppe beteiligen.

(3) Die Kommission sorgt für den Austausch von Wissen und bewährten Verfahren zwischen den notifizierenden Behörden.

Artikel 39

Konformitätsbewertungsstellen in Drittländern

Konformitätsbewertungsstellen, die nach dem Recht eines Drittlands errichtet wurden, mit dem die Union ein Abkommen geschlossen hat, können ermächtigt werden, die Tätigkeiten notifizierter Stellen gemäß dieser Verordnung durchzuführen, sofern sie die Anforderungen gemäß Artikel 31 erfüllen oder das gleiche Maß an Konformität gewährleisten.

ABSCHNITT 5

Normen, Konformitätsbewertung, Bescheinigungen, Registrierung

Artikel 40

[sn909] Beratungsforum

Harmonisierte Normen und Normungsdokumente

(1) Bei Hochrisiko-KI-Systemen oder KI-Modellen mit allgemeinem Verwendungszweck, die mit harmonisierten Normen oder Teilen davon, deren Fundstellen gemäß der Verordnung (EU) Nr. 1025/2012 im *Amtsblatt der Europäischen Union* veröffentlicht wurden, übereinstimmen, wird eine Konformität mit den Anforderungen gemäß Abschnitt 2 des vorliegenden Kapitels oder gegebenenfalls mit den Pflichten gemäß Kapitel V Abschnitte 2 und 3 der vorliegenden Verordnung vermutet, soweit diese Anforderungen oder Verpflichtungen von den Normen abgedeckt sind.

(2) Gemäß Artikel 10 der Verordnung (EU) Nr. 1025/2012 erteilt die Kommission unverzüglich Normungsaufträge, die alle Anforderungen gemäß Abschnitt 2 des vorliegenden Kapitels abdecken und gegebenenfalls Normungsaufträge, die Pflichten gemäß Kapitel V Abschnitte 2 und 3 der vorliegenden Verordnung abdecken. In dem Normungsauftrag werden auch Dokumente zu den Berichterstattungs- und Dokumentationsverfahren im Hinblick auf die Verbesserung der Ressourcenleistung von KI-Systemen z. B. durch die Verringerung des Energie- und sonstigen Ressourcenverbrauchs des Hochrisiko-KI-Systems während seines gesamten Lebenszyklus und zu der energieeffizienten Entwicklung von KI-Modellen mit allgemeinem Verwendungszweck verlangt. Bei der Ausarbeitung des Normungsauftrags konsultiert die Kommission das KI-Gremium und die einschlägigen Interessenträger, darunter das Beratungsforum.

Bei der Erteilung eines Normungsauftrags an die europäischen Normungsorganisationen gibt die Kommission an, dass die Normen klar und — u. a. mit den Normen, die in den verschiedenen Sektoren für Produkte entwickelt wurden, die unter die in Anhang I aufgeführten geltenden Harmonisierungsrechtsvorschriften der Union fallen — konsistent sein müssen und sicherstellen sollen, dass die in der Union in Verkehr gebrachten oder in Betrieb genommenen Hochrisiko-KI-Systeme oder KI-Modelle mit allgemeinem Verwendungszweck die in dieser Verordnung festgelegten einschlägigen Anforderungen oder Pflichten erfüllen.

Die Kommission fordert die europäischen Normungsorganisationen auf, Nachweise dafür vorzulegen, dass sie sich nach besten Kräften bemühen, die in den Unterabsätzen 1 und 2 dieses Absatzes genannten Ziele im Einklang mit Artikel 24 der Verordnung (EU) Nr. 1025/2012 zu erreichen.

(3) Die am Normungsprozess Beteiligten bemühen sich, Investitionen und Innovationen im Bereich der KI, u. a. durch Erhöhung der Rechtssicherheit, sowie der Wettbewerbsfähigkeit und des Wachstums des Unionsmarktes zu fördern und zur Stärkung der weltweiten Zusammenarbeit bei der Normung und zur Berücksichtigung bestehender internationaler Normen im Bereich der KI, die mit den Werten, Grundrechten und Interessen der Union im Einklang stehen, beizutragen und die Multi-Stakeholder-Governance zu verbessern, indem eine ausgewogene Vertretung der Interessen und eine wirksame Beteiligung aller relevanten Interessenträger gemäß den Artikeln 5, 6 und 7 der Verordnung (EU) Nr. 1025/2012 sichergestellt werden.

Artikel 41

Gemeinsame Spezifikationen

(1) Die Kommission kann Durchführungsrechtsakte zur Festlegung gemeinsamer Spezifikationen für die Anforderungen gemäß Abschnitt 2 dieses Kapitels oder gegebenenfalls die Pflichten gemäß Kapitel V Abschnitte 2 und 3 erlassen, wenn die folgenden Bedingungen erfüllt sind:

a) 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 in Abschnitt 2 dieses Kapitels festgelegten Anforderungen oder gegebenenfalls für die in Kapitel V Abschnitte 2 und 3 festgelegten Pflichten zu erarbeiten, und

   i) der Auftrag wurde von keiner der europäischen Normungsorganisationen angenommen oder

ii) die harmonisierten Normen, die Gegenstand dieses Auftrags sind, werden nicht innerhalb der gemäß Artikel 10 Absatz 1 der Verordnung (EU) Nr. 1025/2012 festgelegten Frist erarbeitet oder

iii) die einschlägigen harmonisierten Normen tragen den Bedenken im Bereich der Grundrechte nicht ausreichend Rechnung oder

[sn909] Beratungsforum

iv) die harmonisierten Normen entsprechen nicht dem Auftrag und

b) im *Amtsblatt der Europäischen Union* sind keine Fundstellen zu harmonisierten Normen gemäß der Verordnung (EU) Nr. 1025/2012 veröffentlicht, die den in Abschnitt 2 dieses Kapitels aufgeführten Anforderungen oder gegebenenfalls den in Kapitel V Abschnitte 2 und 3 aufgeführten Pflichten genügen, und es ist nicht zu erwarten, dass eine solche Fundstelle innerhalb eines angemessenen Zeitraums veröffentlicht wird.

Bei der Verfassung der gemeinsamen Spezifikationen konsultiert die Kommission das in Artikel 67 genannte Beratungsforum.

Die in Unterabsatz 1 des vorliegenden Absatzes genannten Durchführungsrechtsakte werden gemäß dem in Artikel 98 Absatz 2 genannten Prüfverfahren erlassen.

[sn502] Anbieter

(2) Vor der Ausarbeitung eines Entwurfs eines Durchführungsrechtsakts informiert die Kommission den in Artikel 22 der Verordnung (EU) Nr. 1025/2012 genannten Ausschuss darüber, dass sie die in Absatz 1 des vorliegenden Artikels festgelegten Bedingungen als erfüllt erachtet.

(3) Bei Hochrisiko-KI-Systemen oder KI-Modellen mit allgemeinem Verwendungszweck, die mit den in Absatz 1 genannten gemeinsamen Spezifikationen oder Teilen dieser Spezifikationen übereinstimmen, wird eine Konformität mit den Anforderungen in Abschnitt 2 dieses Kapitels oder gegebenenfalls die Einhaltung der in Kapitel V Abschnitte 2 und 3 genannten Pflichten vermutet, soweit diese Anforderungen oder diese Pflichten von den gemeinsamen Spezifikationen abgedeckt sind.

(4) Wird eine harmonisierte Norm von einer europäischen Normungsorganisation angenommen und der Kommission zur Veröffentlichung ihrer Fundstelle im *Amtsblatt der Europäischen Union* vorgeschlagen, so bewertet die Kommission die harmonisierte Norm gemäß der Verordnung (EU) Nr. 1025/2012. Wird die Fundstelle zu einer harmonisierten Norm im *Amtsblatt der Europäischen Union* veröffentlicht, so werden die in Absatz 1 genannten Durchführungsrechtsakte, die dieselben Anforderungen gemäß Abschnitt 2 dieses Kapitels oder gegebenenfalls dieselben Pflichten gemäß Kapitel V Abschnitte 2 und 3 erfassen, von der Kommission ganz oder teilweise aufgehoben.

(5) Wenn Anbieter von Hochrisiko-KI-Systemen oder KI-Modellen mit allgemeinem Verwendungszweck die in Absatz 1 genannten gemeinsamen Spezifikationen nicht befolgen, müssen sie hinreichend nachweisen, dass sie technische Lösungen verwenden, die die in Abschnitt 2 dieses Kapitels aufgeführten Anforderungen oder gegebenenfalls die Pflichten gemäß Kapitel V Abschnitte 2 und 3 zumindest in gleichem Maße erfüllen;

(6) Ist ein Mitgliedstaat der Auffassung, dass eine gemeinsame Spezifikation den Anforderungen gemäß Abschnitt 2 nicht vollständig entspricht oder gegebenenfalls die Pflichten gemäß Kapitel V Abschnitte 2 und 3 nicht vollständig erfüllt, so setzt er die Kommission im Rahmen einer ausführlichen Erläuterung davon in Kenntnis. Die Kommission bewertet die betreffende Information und ändert gegebenenfalls den Durchführungsrechtsakt, durch den die betreffende gemeinsame Spezifikation festgelegt wurde.

Artikel 42

Vermutung der Konformität mit bestimmten Anforderungen

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

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

[sn505] Konformitätsbewertung

[sn502] Anbieter

Artikel 43

Konformitätsbewertung

(1) Hat ein Anbieter zum Nachweis, dass ein in Anhang III Nummer 1 aufgeführtes Hochrisiko-KI-System die in Abschnitt 2 festgelegten Anforderungen erfüllt, harmonisierte Normen gemäß Artikel 40 oder gegebenenfalls gemeinsame Spezifikationen gemäß Artikel 41 angewandt, so entscheidet er sich für eines der folgenden Konformitätsbewertungsverfahren auf der Grundlage

a) der internen Kontrolle gemäß Anhang VI oder

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

Zum Nachweis, dass sein Hochrisiko-KI-System die in Abschnitt 2 festgelegten Anforderungen erfüllt, befolgt der Anbieter das Konformitätsbewertungsverfahren gemäß Anhang VII, wenn

a) es harmonisierte Normen gemäß Artikel 40 nicht gibt und keine gemeinsamen Spezifikationen gemäß Artikel 41 vorliegen,

b) der Anbieter die harmonisierte Norm nicht oder nur teilweise angewandt hat;

c) die unter Buchstabe a genannten gemeinsamen Spezifikationen zwar vorliegen, der Anbieter sie jedoch nicht angewandt hat;

d) eine oder mehrere der unter Buchstabe a genannten harmonisierten Normen mit einer Einschränkung und nur für den eingeschränkten Teil der Norm veröffentlicht wurden.

Für die Zwecke des Konformitätsbewertungsverfahrens gemäß Anhang VII kann der Anbieter eine der notifizierten Stellen auswählen. Soll das Hochrisiko-KI-System jedoch von Strafverfolgungs-, Einwanderungs- oder Asylbehörden oder von Organen, Einrichtungen oder sonstigen Stellen der Union in Betrieb genommen werden, so übernimmt die in Artikel 74 Absatz 8 bzw. 9 genannte Marktüberwachungsbehörde die Funktion der notifizierten Stelle.

[sn503] Betreiber

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

(3) Bei den Hochrisiko-KI-Systemen, die unter die in Anhang I Abschnitt A aufgeführten Harmonisierungsrechtsakte der Union fallen, befolgt der Anbieter die einschlägigen Konformitätsbewertungsverfahren, die nach diesen Rechtsakten erforderlich sind. Die in Abschnitt 2 dieses Kapitels festgelegten Anforderungen gelten für diese Hochrisiko-KI-Systeme und werden in diese Bewertung einbezogen. Anhang VII Nummern 4.3, 4.4 und 4.5 sowie Nummer 4.6 Absatz 5 finden ebenfalls Anwendung.

Für die Zwecke dieser Bewertung sind die notifizierten Stellen, die gemäß diesen Rechtsakten notifiziert wurden, berechtigt, die Konformität der Hochrisiko-KI-Systeme mit den in Abschnitt 2 festgelegten Anforderungen zu kontrollieren, sofern im Rahmen des gemäß diesen Rechtsakten durchgeführten Notifizierungsverfahrens geprüft wurde, dass diese notifizierten Stellen die in Artikel 31 Absätze 4, 5, 10 und 11 festgelegten Anforderungen erfüllen.

Wenn ein in Anhang I Abschnitt A aufgeführter Rechtsakte es dem Hersteller des Produkts ermöglicht, 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 alle in Abschnitt 2 dieses Kapitels festgelegten Anforderungen abdecken, angewandt hat.

(4) Hochrisiko-KI-Systeme, die bereits Gegenstand eines Konformitätsbewertungsverfahren gewesen sind, werden im Falle einer wesentlichen Änderung einem neuen Konformitätsbewertungsverfahren unterzogen, unabhängig davon, ob das geänderte System noch weiter in Verkehr gebracht oder vom derzeitigen Betreiber weitergenutzt werden soll.

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

(5) Die Kommission ist befugt, gemäß Artikel 97 delegierte Rechtsakte zu erlassen, um die Anhänge VI und VII zu ändern, indem sie sie angesichts des technischen Fortschritts aktualisiert.

(6) Die Kommission ist befugt, gemäß Artikel 97 delegierte Rechtsakte zur Änderung der Absätze 1 und 2 des vorliegenden Artikels 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.

[sn502] Anbieter

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 für unter Anhang I fallende KI-Systeme und maximal vier Jahre für unter Anhang III fallende KI-Systeme 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 für unter Anhang I fallende KI-Systeme und höchstens vier Jahre für unter Anhang III fallende KI-Systeme verlängert werden. Eine Ergänzung zu einer Bescheinigung bleibt gültig, sofern die Bescheinigung, zu der sie gehört, gültig ist.

(3) Stellt eine notifizierte Stelle fest, dass ein KI-System die in Abschnitt 2 festgelegten Anforderungen nicht mehr erfüllt, so setzt sie die ausgestellte Bescheinigung aus, widerruft sie 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.

Es muss ein Einspruchsverfahren gegen die Entscheidungen der notifizierten Stellen, auch solche über ausgestellte Konformitätsbescheinigungen, vorgesehen sein.

Artikel 45

Informationspflichten der notifizierten Stellen

(1) Die notifizierten Stellen informieren die notifizierende Behörde über

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 informiert 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 Bescheinigungen der Union 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 Arten der KI-Systeme nachgehen, einschlägige Informationen über negative und auf Anfrage über positive Konformitätsbewertungsergebnisse.

(4) Notifizierende Behörden gewährleisten gemäß Artikel 78 die Vertraulichkeit der von ihnen erlangten Informationen.

Artikel 46

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 oder des Schutzes wichtiger Industrie- und Infrastrukturanlagen genehmigen. Diese Genehmigung wird auf die Dauer der erforderlichen Konformitätsbewertungsverfahren befristet, wobei den außergewöhnlichen Gründen für die Ausnahme Rechnung getragen wird. Der Abschluss dieser Verfahren erfolgt unverzüglich.

(2) 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 die Genehmigung gemäß Absatz 1 abgelehnt wird, wird Verwendung des Hochrisiko-KI-Systems mit sofortiger Wirkung eingestellt und sämtliche Ergebnisse und Ausgaben dieser Verwendung werden unverzüglich verworfen.

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

[sn502] Anbieter

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

(5) Erhebt innerhalb von 15 Kalendertagen nach Erhalt der in Absatz 3 genannten Mitteilung ein Mitgliedstaat Einwände gegen eine von einer Marktüberwachungsbehörde eines anderen Mitgliedstaats erteilte Genehmigung oder ist die Kommission der Auffassung, dass die Genehmigung mit dem Unionsrecht unvereinbar ist oder dass die Schlussfolgerung der Mitgliedstaaten in Bezug auf die Konformität des in Absatz 3 genannten Systems unbegründet ist, so nimmt die Kommission unverzüglich Konsultationen mit dem betreffenden Mitgliedstaat auf. Die betroffenen Akteure werden konsultiert und erhalten Gelegenheit, dazu Stellung zu nehmen. In Anbetracht dessen entscheidet die Kommission, ob die Genehmigung gerechtfertigt ist. Die Kommission richtet ihren Beschluss an den betroffenen Mitgliedstaat und an die betroffenen Akteure.

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

(7) Für Hochrisiko-KI-Systeme im Zusammenhang mit Produkten, die unter die in Anhang I Abschnitt A aufgeführten Harmonisierungsrechtsvorschriften der Union fallen, gelten nur die in diesen Harmonisierungsrechtsvorschriften der Union festgelegten Ausnahmen von den Konformitätsbewertungsverfahren.

Artikel 47

EU-Konformitätserklärung

(1) Der Anbieter stellt für jedes Hochrisiko-KI-System eine schriftliche maschinenlesbare, physische oder elektronisch unterzeichnete EU-Konformitätserklärung aus und hält sie für einen Zeitraum von 10 Jahren ab dem Inverkehrbringen oder der Inbetriebnahme des Hochrisiko-KI-Systems für die zuständigen nationalen Behörden bereit. Aus der EU-Konformitätserklärung geht hervor, für welches Hochrisiko-KI-System sie ausgestellt wurde. Eine Kopie der EU-Konformitätserklärung wird den zuständigen nationalen Behörden auf Anfrage übermittelt.

(2) Die EU-Konformitätserklärung muss feststellen, dass das betreffende Hochrisiko-KI-System die in Abschnitt 2 festgelegten Anforderungen erfüllt. Die EU-Konformitätserklärung enthält die in Anhang V festgelegten Informationen und wird in eine Sprache übersetzt, die für die zuständigen nationalen Behörden der Mitgliedstaaten, in denen das Hochrisiko-KI-System in Verkehr gebracht oder bereitgestellt wird, leicht verständlich ist.

[sn502] Anbieter

(3) Unterliegen Hochrisiko-KI-Systeme 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 Informationen zur Feststellung der Harmonisierungsrechtsvorschriften der Union, auf die sich die Erklärung bezieht.

[sn509] CE-Kennzeichnung

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

(5) Der Kommission ist befugt, gemäß Artikel 97 delegierte Rechtsakte zur Aktualisierung des in Anhang V festgelegten Inhalts der EU-Konformitätserklärung zu erlassen, um den genannten Anhang durch die Einführung von Elementen zu ändern, die angesichts des technischen Fortschritts erforderlich werden.

Artikel 48

CE-Kennzeichnung

(1) Für die CE-Kennzeichnung gelten die in Artikel 30 der Verordnung (EG) Nr. 765/2008 festgelegten allgemeinen Grundsätze.

(2) Bei digital bereitgestellten Hochrisiko-KI-Systemen wird eine digitale CE-Kennzeichnung nur dann verwendet, wenn sie über die Schnittstelle, von der aus auf dieses System zugegriffen wird, oder über einen leicht zugänglichen maschinenlesbaren Code oder andere elektronische Mittel leicht zugänglich ist.

[sn707] Bevollmächtigter

[sn908] EU-Datenbank

(3) 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 bzw. der beigefügten Dokumentation angebracht.

[sn503] Betreiber

(4) Gegebenenfalls wird der CE-Kennzeichnung die Identifizierungsnummer der für die in Artikel 43 festgelegten Konformitätsbewertungsverfahren zuständigen notifizierten Stelle hinzugefügt. Die Identifizierungsnummer der notifizierten Stelle ist entweder von der Stelle selbst oder nach ihren Anweisungen durch den Anbieter oder den Bevollmächtigten des Anbieters anzubringen. Diese Identifizierungsnummer wird auch auf jeglichem Werbematerial angegeben, in dem darauf hingewiesen wird, dass das Hochrisiko-KI-System die Anforderungen für die CE-Kennzeichnung erfüllt.

(5) Falls Hochrisiko-KI-Systeme ferner unter andere Rechtsvorschriften der Union fallen, in denen die CE-Kennzeichnung auch vorgesehen ist, bedeutet die CE-Kennzeichnung, dass das Hochrisiko-KI-System auch die Anforderungen dieser anderen Rechtsvorschriften erfüllt.

Artikel 49

Registrierung

(1) Vor dem Inverkehrbringen oder der Inbetriebnahme eines in Anhang III aufgeführten Hochrisiko-KI-Systems — mit Ausnahme der in Anhang III Nummer 2 genannten Hochrisiko-KI-Systeme — registriert der Anbieter oder gegebenenfalls sein Bevollmächtigter sich und sein System in der in Artikel 71 genannten EU-Datenbank.

(2) Vor dem Inverkehrbringen oder der Inbetriebnahme eines Hochrisiko-KI-Systems, bei dem der Anbieter zu dem Schluss gelangt ist, dass es nicht hochriskant gemäß Artikel 6 Absatz 3 ist, registriert dieser Anbieter oder gegebenenfalls sein Bevollmächtigter sich und dieses System in der in Artikel 71 genannten EU-Datenbank.

(3) Vor der Inbetriebnahme oder Verwendung eines in Anhang III aufgeführten Hochrisiko-KI-Systems — mit Ausnahme der in Anhang III Nummer 2 aufgeführten Hochrisiko-KI-Systeme — registrieren sich Betreiber, bei denen es sich um Behörden oder Organe, Einrichtungen oder sonstige Stellen der Union oder in ihrem Namen handelnde Personen handelt, in der in Artikel 71 genannten EU-Datenbank, wählen das System aus und registrieren es dort.

[sn550] Pflichten bei begrenztem Risiko
[sn551] Offenlegung menschlicher Interaktion
[sn552] Kennzeichnung synthetischer Inhalte
[sn553] Emotions-/Biometrie-Offenlegung
[sn554] Deep-Fake-Offenlegung
[sn908] EU-Datenbank
[sn503] Betreiber

(4) Bei den in Anhang III Nummern 1, 6 und 7 genannten Hochrisiko-KI-Systemen erfolgt in den Bereichen Strafverfolgung, Migration, Asyl und Grenzkontrolle die Registrierung gemäß den Absätzen 1, 2 und 3 des vorliegenden Artikels in einem sicheren nicht öffentlichen Teil der in Artikel 71 genannten EU-Datenbank und enthält, soweit zutreffend, lediglich die Informationen gemäß

a) Anhang VIII Abschnitt A Nummern 1 bis 10 mit Ausnahme der Nummern 6, 8 und 9,

b) Anhang VIII Abschnitt B Nummern 1 bis 5 sowie Nummern 8 und 9,

c) Anhang VIII Abschnitt C Nummern 1 bis 3,

d) Anhang IX Nummern 1, 2, 3 und Nummer 5.

Nur die Kommission und die in Artikel 74 Absatz 8 genannten nationalen Behörden haben Zugang zu den jeweiligen beschränkten Teilen der EU-Datenbank gemäß Unterabsatz 1 dieses Absatzes.

(5) Die in Anhang III Nummer 2 genannten Hochrisiko-KI-Systeme werden auf nationaler Ebene registriert.

KAPITEL IV

TRANSPARENZPFLICHTEN FÜR ANBIETER UND BETREIBER BESTIMMTER KI-SYSTEME

Artikel 50

Transparenzpflichten für Anbieter und Betreiber bestimmter KI-Systeme

(1) Die Anbieter stellen sicher, dass KI-Systeme, die für die direkte Interaktion mit natürlichen Personen bestimmt sind, so konzipiert und entwickelt werden, dass die betreffenden natürlichen Personen informiert werden, dass sie mit einem KI-System interagieren, es sei denn, dies ist aus Sicht einer angemessen informierten, aufmerksamen und verständigen natürlichen Person aufgrund der Umstände und des Kontexts der Nutzung offensichtlich. Diese Pflicht gilt nicht für gesetzlich zur Aufdeckung, Verhütung, Ermittlung oder 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) Anbieter von KI-Systemen, einschließlich KI-Systemen mit allgemeinem Verwendungszweck, die synthetische Audio-, Bild-, Video- oder Textinhalte erzeugen, stellen sicher, dass die Ausgaben des KI-Systems in einem maschinenlesbaren Format gekennzeichnet und als künstlich erzeugt oder manipuliert erkennbar sind. Die Anbieter sorgen dafür, dass — soweit technisch möglich — ihre technischen Lösungen wirksam, interoperabel, belastbar und zuverlässig sind und berücksichtigen dabei die Besonderheiten und Beschränkungen der verschiedenen Arten von Inhalten, die Umsetzungskosten und den allgemein anerkannten Stand der Technik, wie er in den einschlägigen technischen Normen zum Ausdruck kommen kann. Diese Pflicht gilt nicht, soweit die KI-Systeme eine unterstützende Funktion für die Standardbearbeitung ausführen oder die vom Betreiber bereitgestellten Eingabedaten oder deren Semantik nicht wesentlich verändern oder wenn sie zur Aufdeckung, Verhütung, Ermittlung oder Verfolgung von Straftaten gesetzlich zugelassen sind.

(3) Die Betreiber eines Emotionserkennungssystems oder eines Systems zur biometrischen Kategorisierung informieren die davon betroffenen natürlichen Personen über den Betrieb des Systems und verarbeiten personenbezogene Daten gemäß den Verordnungen (EU) 2016/679 und (EU) 2018/1725 und der Richtlinie (EU) 2016/680. Diese Pflicht gilt nicht für gesetzlich zur Aufdeckung, Verhütung oder Ermittlung von Straftaten zugelassene KI-Systeme, die zur biometrischen Kategorisierung und Emotionserkennung im Einklang mit dem Unionsrecht verwendet werden, sofern geeignete Schutzvorkehrungen für die Rechte und Freiheiten Dritter bestehen.

(4) Betreiber eines KI-Systems, das Bild-, Ton- oder Videoinhalte erzeugt oder manipuliert, die ein Deepfake sind, müssen offenlegen, dass die Inhalte künstlich erzeugt oder manipuliert wurden. Diese Pflicht gilt nicht, wenn die Verwendung zur Aufdeckung, Verhütung, Ermittlung oder Verfolgung von Straftaten gesetzlich zugelassen ist. Ist der Inhalt Teil eines offensichtlich künstlerischen, kreativen, satirischen, fiktionalen oder analogen Werks oder Programms, so beschränken sich die in diesem Absatz festgelegten Transparenzpflichten darauf, das Vorhandensein solcher erzeugten oder manipulierten Inhalte in geeigneter Weise offenzulegen, die die Darstellung oder den Genuss des Werks nicht beeinträchtigt.

Betreiber eines KI-Systems, das Text erzeugt oder manipuliert, der veröffentlicht wird, um die Öffentlichkeit über Angelegenheiten von öffentlichem Interesse zu informieren, müssen offenlegen, dass der Text künstlich erzeugt oder manipuliert wurde. Diese Pflicht gilt nicht, wenn die Verwendung zur Aufdeckung, Verhütung, Ermittlung oder Verfolgung von Straftaten gesetzlich zugelassen ist oder wenn die durch KI erzeugten Inhalte einem Verfahren der menschlichen Überprüfung oder redaktionellen Kontrolle unterzogen wurden und wenn eine natürliche oder juristische Person die redaktionelle Verantwortung für die Veröffentlichung der Inhalte trägt.

[sn601] Klassifizierung systemischer Risiken

[sn901] Büro für Künstliche Intelligenz

[sn600] KI-Modelle mit allgemeinem Verwendungszweck

(5) Die in den Absätzen 1 bis 4 genannten Informationen werden den betreffenden natürlichen Personen spätestens zum Zeitpunkt der ersten Interaktion oder Aussetzung in klarer und eindeutiger Weise bereitgestellt. Die Informationen müssen den geltenden Barrierefreiheitsanforderungen entsprechen.

(6) Die Absätze 1 bis 4 lassen die in Kapitel III festgelegten Anforderungen und Pflichten unberührt und berühren nicht andere Transparenzpflichten, die im Unionsrecht oder dem nationalen Recht für Betreiber von KI-Systemen festgelegt sind.

(7) Das Büro für Künstliche Intelligenz fördert und erleichtert die Ausarbeitung von Praxisleitfäden auf Unionsebene, um die wirksame Umsetzung der Pflichten in Bezug auf die Feststellung und Kennzeichnung künstlich erzeugter oder manipulierter Inhalte zu erleichtern. Die Kommission kann Durchführungsrechtsakte zur Genehmigung dieser Praxisleitfäden nach dem in Artikel 56 Absatz 6 festgelegten Verfahren erlassen. Hält sie einen Kodex für nicht angemessen, so kann die Kommission einen Durchführungsrechtsakt gemäß dem in Artikel 98 Absatz 2 genannten Prüfverfahren erlassen, in dem gemeinsame Vorschriften für die Umsetzung dieser Pflichten festgelegt werden.

KAPITEL V

KI-MODELLE MIT ALLGEMEINEM VERWENDUNGSZWECK

ABSCHNITT 1

Einstufungsvorschriften

Artikel 51

Einstufung von KI-Modellen mit allgemeinem Verwendungszweck als KI-Modelle mit allgemeinem Verwendungszweck mit systemischem Risiko

[sn502] Anbieter

(1) Ein KI-Modell mit allgemeinem Verwendungszweck wird als KI-Modell mit allgemeinem Verwendungszweck mit systemischem Risiko eingestuft, wenn eine der folgenden Bedingungen erfüllt ist:

a) Es verfügt über Fähigkeiten mit hohem Wirkungsgrad, die mithilfe geeigneter technischer Instrumente und Methoden, einschließlich Indikatoren und Benchmarks, bewertet werden;

b) einem unter Berücksichtigung der in Anhang XIII festgelegten Kriterien von der Kommission von Amts wegen oder aufgrund einer qualifizierten Warnung des wissenschaftlichen Gremiums getroffenen Entscheidung zufolge verfügt es über Fähigkeiten oder eine Wirkung, die denen gemäß Buchstabe a entsprechen.

(2) Bei einem KI-Modell mit allgemeinem Verwendungszweck wird angenommen, dass es über Fähigkeiten mit hohem Wirkungsgrad gemäß Absatz 1 Buchstabe a verfügt, wenn die kumulierte Menge der für sein Training verwendeten Berechnungen, gemessen in Gleitkommaoperationen, mehr als 10^{25} beträgt.

(3) Die Kommission erlässt gemäß Artikel 97 delegierte Rechtsakte zur Änderung der in den Absätzen 1 und 2 des vorliegenden Artikels aufgeführten Schwellenwerte sowie zur Ergänzung von Benchmarks und Indikatoren vor dem Hintergrund sich wandelnder technologischer Entwicklungen, wie z. B. algorithmische Verbesserungen oder erhöhte Hardwareeffizienz, wenn dies erforderlich ist, damit diese Schwellenwerte dem Stand der Technik entsprechen.

Artikel 52

Verfahren

(1) Erfüllt ein KI-Modell mit allgemeinem Verwendungszweck die Bedingung gemäß Artikel 51 Absatz 1 Buchstabe a, so teilt der betreffende Anbieter dies der Kommission unverzüglich, in jedem Fall jedoch innerhalb von zwei Wochen, nachdem diese Bedingung erfüllt ist oder bekannt wird, dass sie erfüllt wird, mit. Diese Mitteilung muss die Informationen enthalten, die erforderlich sind, um nachzuweisen, dass die betreffende Bedingung erfüllt ist. Erlangt die Kommission Kenntnis von einem KI-Modell mit allgemeinem Verwendungszweck, das systemische Risiken birgt, die ihr nicht mitgeteilt wurden, so kann sie entscheiden, es als Modell mit systemischen Risiken auszuweisen.

(2) Der Anbieter eines KI-Modells mit allgemeinem Verwendungszweck, das die in Artikel 51 Absatz 1 Buchstabe a genannte Bedingung erfüllt, kann in seiner Mitteilung hinreichend begründete Argumente vorbringen, um nachzuweisen, dass das KI-Modell mit allgemeinem Verwendungszweck, obwohl es diese Bedingung erfüllt, aufgrund seiner besonderen Merkmale außerordentlicherweise keine systemischen Risiken birgt und daher nicht als KI-Modell mit allgemeinem Verwendungszweck mit systemischem Risiko eingestuft werden sollte.

[sn603] Informationen für nachgelagerte Anbieter
[sn604] Urheberrechtskonformität
[sn502] Anbieter

(3) Gelangt die Kommission zu dem Schluss, dass die gemäß Absatz 2 vorgebrachten Argumente nicht hinreichend begründet sind, und konnte der betreffende Anbieter nicht nachweisen, dass das KI-Modell mit allgemeinem Verwendungszweck aufgrund seiner besonderen Merkmale keine systemischen Risiken aufweist, weist sie diese Argumente zurück, und das KI-Modell mit allgemeinem Verwendungszweck gilt als KI-Modell mit allgemeiner Zweckbestimmung mit systemischem Risiko.

(4) Die Kommission kann ein KI-Modell mit allgemeinem Verwendungszweck von Amts wegen oder aufgrund einer qualifizierten Warnung des wissenschaftlichen Gremiums gemäß Artikel 90 Absatz 1 Buchstabe a auf der Grundlage der in Anhang XIII festgelegten Kriterien als KI-Modell mit systemischen Risiken ausweisen.

Die Kommission ist befugt, gemäß Artikel 97 delegierte Rechtsakte zu erlassen, um Anhang XIII zu ändern, indem die in dem genannten Anhang genannten Indikatoren präzisiert und aktualisiert werden.

(5) Stellt der Anbieter, dessen Modell gemäß Absatz 4 als KI-Modell mit allgemeinem Verwendungszweck mit systemischem Risiko ausgewiesen wurde, einen entsprechenden Antrag, berücksichtigt die Kommission den Antrag und kann entscheiden, erneut zu prüfen, ob beim KI-Modell mit allgemeinem Verwendungszweck auf der Grundlage der in Anhang XIII festgelegten Kriterien immer noch davon ausgegangen werden kann, dass es systemische Risiken aufweist. Dieser Antrag muss objektive, detaillierte und neue Gründe enthalten, die sich seit der Entscheidung zur Ausweisung ergeben haben. Die Anbieter können frühestens sechs Monate nach der Entscheidung zur Ausweisung eine Neubewertung beantragen. Entscheidet die Kommission nach ihrer Neubewertung, die Ausweisung als KI-Modell mit allgemeiner Zweckbestimmung mit systemischem Risiko beizubehalten, können die Anbieter frühestens sechs Monate nach dieser Entscheidung eine Neubewertung beantragen.

[sn901] Büro für Künstliche Intelligenz

(6) Die Kommission stellt sicher, dass eine Liste von KI-Modellen mit allgemeinem Verwendungszweck mit systemischem Risiko veröffentlicht wird, und hält diese Liste unbeschadet der Notwendigkeit, Rechte des geistigen Eigentums und vertrauliche Geschäftsinformationen oder Geschäftsgeheimnisse im Einklang mit dem Unionsrecht und dem nationalen Recht zu achten und zu schützen, auf dem neuesten Stand.

ABSCHNITT 2

Pflichten für Anbieter von KI-Modellen mit allgemeinem Verwendungszweck

Artikel 53

Pflichten für Anbieter von KI-Modellen mit allgemeinem Verwendungszweck

(1) Anbieter von KI-Modellen mit allgemeinem Verwendungszweck

a) erstellen und aktualisieren die technische Dokumentation des Modells, einschließlich seines Trainings- und Testverfahrens und der Ergebnisse seiner Bewertung, die mindestens die in Anhang XI aufgeführten Informationen enthält, damit sie dem Büro für Künstliche Intelligenz und den zuständigen nationalen Behörden auf Anfrage zur Verfügung gestellt werden kann;

b) erstellen und aktualisieren Informationen und die Dokumentation und stellen sie Anbietern von KI-Systemen zur Verfügung, die beabsichtigen, das KI-Modell mit allgemeinem Verwendungszweck in ihre KI-Systeme zu integrieren. Unbeschadet der Notwendigkeit, die Rechte des geistigen Eigentums und vertrauliche Geschäftsinformationen oder Geschäftsgeheimnisse im Einklang mit dem Unionsrecht und dem nationalen Recht zu achten und zu schützen, müssen die Informationen und die Dokumentation

   i) die Anbieter von KI-Systemen in die Lage versetzen, die Fähigkeiten und Grenzen des KI-Modells mit allgemeinem Verwendungszweck gut zu verstehen und ihren Pflichten gemäß dieser Verordnung nachzukommen, und

   ii) zumindest die in Anhang XII genannten Elemente enthalten;

c) bringen eine Strategie zur Einhaltung des Urheberrechts der Union und damit zusammenhängender Rechte und insbesondere zur Ermittlung und Einhaltung eines gemäß Artikel 4 Absatz 3 der Richtlinie (EU) 2019/790 geltend gemachten Rechtsvorbehalts, auch durch modernste Technologien, auf den Weg;

d) erstellen und veröffentlichen eine hinreichend detaillierte Zusammenfassung der für das Training des KI-Modells mit allgemeinem Verwendungszweck verwendeten Inhalte nach einer vom Büro für Künstliche Intelligenz bereitgestellten Vorlage.

[sn502] Anbieter
[sn707] Bevollmächtigter
[sn607] Open-Source-Ausnahme

(2) Die Pflichten gemäß Absatz 1 Buchstaben a und b gelten nicht für Anbieter von KI-Modellen, die im Rahmen einer freien und quelloffenen Lizenz bereitgestellt werden, die den Zugang, die Nutzung, die Änderung und die Verbreitung des Modells ermöglicht und deren Parameter, einschließlich Gewichte, Informationen über die Modellarchitektur und Informationen über die Modellnutzung, öffentlich zugänglich gemacht werden. Diese Ausnahme gilt nicht für KI-Modellen mit allgemeinem Verwendungszweck mit systemischen Risiken.

(3) Anbieter von KI-Modellen mit allgemeinem Verwendungszweck arbeiten bei der Ausübung ihrer Zuständigkeiten und Befugnisse gemäß dieser Verordnung erforderlichenfalls mit der Kommission und den zuständigen nationalen Behörden zusammen.

(4) Anbieter von KI-Modellen mit allgemeinem Verwendungszweck können sich bis zur Veröffentlichung einer harmonisierten Norm auf Praxisleitfäden im Sinne des Artikels 56 stützen, um die Einhaltung der in Absatz 1 des vorliegenden Artikels genannten Pflichten nachzuweisen. Die Einhaltung der harmonisierten europäischen Norm begründet für die Anbieter die Vermutung der Konformität, insoweit diese Normen diese Verpflichtungen abdecken. Anbieter von KI-Modellen mit allgemeinem Verwendungszweck, die keinen genehmigten Praxisleitfaden befolgen oder eine harmonisierte europäische Norm nicht einhalten, müssen geeignete alternative Verfahren der Einhaltung aufzeigen, die von der Kommission zu bewerten sind.

(5) Um die Einhaltung von Anhang XI, insbesondere Nummer 2 Buchstaben d und e, zu erleichtern, ist die Kommission befugt, gemäß Artikel 97 delegierte Rechtsakte zu erlassen, um die Mess- und Berechnungsmethoden im Einzelnen festzulegen, damit eine vergleichbare und überprüfbare Dokumentation ermöglicht wird.

[sn707] Bevollmächtigter
[sn901] Büro für Künstliche Intelligenz

(6) Die Kommission ist befugt, gemäß Artikel 97 Absatz 2 delegierte Rechtsakte zu erlassen, um die Anhänge XI und XII vor dem Hintergrund sich wandelnder technologischer Entwicklungen zu ändern.

(7) Jegliche Informationen oder Dokumentation, die gemäß diesem Artikel erlangt werden, einschließlich Geschäftsgeheimnisse, werden im Einklang mit den in Artikel 78 festgelegten Vertraulichkeitspflichten behandelt.

Artikel 54

Bevollmächtigte der Anbieter von KI-Modellen mit allgemeinem Verwendungszweck

(1) Anbieter, die in Drittländern niedergelassen sind, benennen vor dem Inverkehrbringen eines KI-Modells mit allgemeinem Verwendungszweck auf dem Unionsmarkt schriftlich einen in der Union niedergelassenen Bevollmächtigten.

(2) Der Anbieter muss seinem Bevollmächtigten ermöglichen, die Aufgaben wahrzunehmen, die im vom Anbieter erhaltenen Auftrag festgelegt sind.

(3) Der Bevollmächtigte nimmt die Aufgaben wahr, die in seinem vom Anbieter erhaltenen Auftrag festgelegt sind. Er stellt dem Büro für Künstliche Intelligenz auf Anfrage eine Kopie des Auftrags in einer der Amtssprachen der Institutionen der Union bereit. Für die Zwecke dieser Verordnung ermächtigt der Auftrag den Bevollmächtigten zumindest zur Wahrnehmung folgender Aufgaben:

a) Überprüfung, ob die technische Dokumentation gemäß Anhang XI erstellt wurde und alle Pflichten gemäß Artikel 53 und gegebenenfalls gemäß Artikel 55 vom Anbieter erfüllt wurden;

b) Bereithaltung einer Kopie der technischen Dokumentation gemäß Anhang XI für das Büro für Künstliche Intelligenz und die zuständigen nationalen Behörden für einen Zeitraum von zehn Jahren nach dem Inverkehrbringen des KI-Modells mit allgemeinem Verwendungszweck und der Kontaktdaten des Anbieters, der den Bevollmächtigten benannt hat;

c) Bereitstellung sämtlicher zum Nachweis der Einhaltung der Pflichten gemäß diesem Kapitel erforderlichen Informationen und Dokumentation, einschließlich der unter Buchstabe b genannten Informationen und Dokumentation, an das Büro für Künstliche Intelligenz auf begründeten Antrag;

d) Zusammenarbeit mit dem Büro für Künstliche Intelligenz und den zuständigen Behörden auf begründeten Antrag bei allen Maßnahmen, die sie im Zusammenhang mit einem KI-Modell mit allgemeinem Verwendungszweck ergreifen, auch wenn das Modell in KI-Systeme integriert ist, die in der Union in Verkehr gebracht oder in Betrieb genommen werden.

(4) Mit dem Auftrag wird der Bevollmächtigte ermächtigt, neben oder anstelle des Anbieters als Ansprechpartner für das Büro für Künstliche Intelligenz oder die zuständigen Behörden in allen Fragen zu dienen, die die Gewährleistung der Einhaltung dieser Verordnung betreffen.

(5) Der Bevollmächtigte beendet den Auftrag, wenn er der Auffassung ist oder Grund zu der Annahme hat, dass der Anbieter gegen seine Pflichten gemäß dieser Verordnung verstößt. In einem solchen Fall informiert er auch das Büro für Künstliche Intelligenz unverzüglich über die Beendigung des Auftrags und die Gründe dafür.

(6) Die Pflicht gemäß diesem Artikel gilt nicht für Anbieter von KI-Modellen, die im Rahmen einer freien und quelloffenen Lizenz bereitgestellt werden, die den Zugang, die Nutzung, die Änderung und die Verbreitung des Modells ermöglicht und deren Parameter, einschließlich Gewichte, Informationen über die Modellarchitektur und Informationen über die Modellnutzung, öffentlich zugänglich gemacht werden, es sei denn, die KI-Modelle mit allgemeinem Verwendungszweck bergen systemische Risiken.

ABSCHNITT 3

Pflichten der Anbieter von KI-Modellen mit allgemeinem Verwendungszweck mit systemischem Risiko

Artikel 55

Pflichten der Anbieter von KI-Modellen mit allgemeinem Verwendungszweck mit systemischem Risiko

(1) Zusätzlich zu den in den Artikeln 53 und 54 aufgeführten Pflichten müssen Anbieter von KI-Modellen mit allgemeinem Verwendungszweck mit systemischem Risiko

a) eine Modellbewertung mit standardisierten Protokollen und Instrumenten, die dem Stand der Technik entsprechen, durchführen, wozu auch die Durchführung und Dokumentation von Angriffstests beim Modell gehören, um systemische Risiken zu ermitteln und zu mindern,

b) mögliche systemische Risiken auf Unionsebene — einschließlich ihrer Ursachen —, die sich aus der Entwicklung, dem Inverkehrbringen oder der Verwendung von KI-Modellen mit allgemeinem Verwendungszweck mit systemischem Risiko ergeben können, bewerten und mindern,

c) einschlägige Informationen über schwerwiegende Vorfälle und mögliche Abhilfemaßnahmen erfassen und dokumentieren und das Büro für Künstliche Intelligenz und gegebenenfalls die zuständigen nationalen Behörden unverzüglich darüber unterrichten,

d) ein angemessenes Maß an Cybersicherheit für die KI-Modelle mit allgemeinem Verwendungszweck mit systemischem Risiko und die physische Infrastruktur des Modells gewährleisten.

(2) Anbieter von KI-Modellen mit allgemeinem Verwendungszweck mit systemischem Risiko können sich bis zur Veröffentlichung einer harmonisierten Norm auf Praxisleitfäden im Sinne des Artikels 56 stützen, um die Einhaltung der in Absatz 1 des vorliegenden Artikels genannten Pflichten nachzuweisen. Die Einhaltung der harmonisierten europäischen Norm begründet für die Anbieter die Vermutung der Konformität, insoweit diese Normen diese Verpflichtungen abdecken. Anbieter von KI-Modellen mit allgemeinem Verwendungszweck mit systemischem Risiko, die einen genehmigten Praxisleitfaden nicht befolgen oder eine harmonisierte europäische Norm nicht einhalten, müssen geeignete alternative Verfahren der Einhaltung aufzeigen, die von der Kommission zu bewerten sind.

(3) Jegliche Informationen oder Dokumentation, die gemäß diesem Artikel erlangt werden, werden im Einklang mit den in Artikel 78 festgelegten Vertraulichkeitspflichten behandelt.

ABSCHNITT 4

Praxisleitfäden

Artikel 56

Praxisleitfäden

(1) Das Büro für Künstliche Intelligenz fördert und erleichtert die Ausarbeitung von Praxisleitfäden auf Unionsebene, um unter Berücksichtigung internationaler Ansätze zur ordnungsgemäßen Anwendung dieser Verordnung beizutragen.

(2) Das Büro für Künstliche Intelligenz und das KI-Gremium streben an, sicherzustellen, dass die Praxisleitfäden mindestens die in den Artikeln 53 und 55 vorgesehenen Pflichten abdecken, einschließlich der folgenden Aspekte:

a) Mittel, mit denen sichergestellt wird, dass die in Artikel 53 Absatz 1 Buchstaben a und b genannten Informationen vor dem Hintergrund der Marktentwicklungen und technologischen Entwicklungen auf dem neuesten Stand gehalten werden;

b) die angemessene Detailgenauigkeit bei der Zusammenfassung der für das Training verwendeten Inhalte;

[sn901] Büro für Künstliche Intelligenz

[sn606] Praxisleitfäden

c) die Ermittlung von Art und Wesen der systemischen Risiken auf Unionsebene, gegebenenfalls einschließlich ihrer Ursachen;

d) die Maßnahmen, Verfahren und Modalitäten für die Bewertung und das Management der systemischen Risiken auf Unionsebene, einschließlich ihrer Dokumentation, die in einem angemessenen Verhältnis zu den Risiken stehen, ihrer Schwere und Wahrscheinlichkeit Rechnung tragen und die spezifischen Herausforderungen bei der Bewältigung dieser Risiken vor dem Hintergrund der möglichen Arten der Entstehung und des Eintretens solcher Risiken entlang der KI-Wertschöpfungskette berücksichtigen.

(3) Das Büro für Künstliche Intelligenz kann alle Anbieter von KI-Modellen mit allgemeinem Verwendungszweck sowie die einschlägigen zuständigen nationalen Behörden ersuchen, sich an der Ausarbeitung von Praxisleitfäden zu beteiligen. Organisationen der Zivilgesellschaft, die Industrie, die Wissenschaft und andere einschlägige Interessenträger wie nachgelagerte Anbieter und unabhängige Sachverständige können den Prozess unterstützen.

(4) Das Büro für Künstliche Intelligenz und das KI-Gremium streben an, sicherzustellen, dass in den Praxisleitfäden ihre spezifischen Ziele eindeutig festgelegt sind und Verpflichtungen oder Maßnahmen, gegebenenfalls einschließlich wesentlicher Leistungsindikatoren, enthalten, um die Verwirklichung dieser Ziele gewährleisten, und dass sie den Bedürfnissen und Interessen aller interessierten Kreise, einschließlich betroffener Personen, auf Unionsebene gebührend Rechnung tragen.

(5) Das Büro für Künstliche Intelligenz strebt an, sicherzustellen, dass die an Praxisleitfäden Beteiligten dem Büro für Künstliche Intelligenz regelmäßig über die Umsetzung der Verpflichtungen, die ergriffenen Maßnahmen und deren Ergebnisse, die gegebenenfalls auch anhand der wesentlichen Leistungsindikatoren gemessen werden, Bericht erstatten. Bei den wesentlichen Leistungsindikatoren und den Berichtspflichten wird den Größen- und Kapazitätsunterschieden zwischen den verschiedenen Beteiligten Rechnung getragen.

[sn910] 2. Mai 2025

[sn402] 2. August 2025

(6) Das Büro für Künstliche Intelligenz und KI-Gremium überwachen und bewerten regelmäßig die Verwirklichung der Ziele der Praxisleitfäden durch die Beteiligten und deren Beitrag zur ordnungsgemäßen Anwendung dieser Verordnung. Das Büro für Künstliche Intelligenz und das KI-Gremium bewerten, ob die Praxisleitfäden die in den Artikeln 53 und 55 vorgesehenen Pflichten abdecken, und überwachen und bewerten regelmäßig die Verwirklichung von deren Zielen. Sie veröffentlichen ihre Bewertung der Angemessenheit der Praxisleitfäden.

Die Kommission kann im Wege eines Durchführungsrechtsakts einen Praxisleitfaden genehmigen und ihm in der Union allgemeine Gültigkeit verleihen. Dieser Durchführungsrechtsakt wird gemäß dem in Artikel 98 Absatz 2 genannten Prüfverfahren erlassen.

(7) Das Büro für Künstliche Intelligenz kann alle Anbieter von KI-Modellen mit allgemeinem Verwendungszweck ersuchen, die Praxisleitfäden zu befolgen. Für Anbieter von KI-Modellen mit allgemeinem Verwendungszweck, die keine systemischen Risiken bergen, kann diese Befolgung auf die in Artikel 53 vorgesehenen Pflichten beschränkt werden, es sei denn, sie erklären ausdrücklich ihr Interesse, sich dem ganzen Kodex anzuschließen.

(8) Das Büro für Künstliche Intelligenz fördert und erleichtert gegebenenfalls auch die Überprüfung und Anpassung der Praxisleitfäden, insbesondere vor dem Hintergrund neuer Normen. Das Büro für Künstliche Intelligenz unterstützt bei der Bewertung der verfügbaren Normen.

(9) Praxisleitfäden müssen spätestens am 2. Mai 2025 vorliegen. Das Büro für Künstliche Intelligenz unternimmt die erforderlichen Schritte, einschließlich des Ersuchens von Anbietern gemäß Absatz 7.

Kann bis zum 2. August 2025 ein Verhaltenskodex nicht fertiggestellt werden oder erachtet das Büro für Künstliche Intelligenz dies nach seiner Bewertung gemäß Absatz 6 des vorliegenden Artikels für nicht angemessen, kann die Kommission im Wege von Durchführungsrechtsakten gemeinsame Vorschriften für die Umsetzung der in den Artikeln 53 und 55 vorgesehenen Pflichten, einschließlich der in Absatz 2 des vorliegenden Artikels genannten Aspekte, festlegen. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 98 Absatz 2 genannten Prüfverfahren erlassen.

KAPITEL VI

[sn506] KI-Reallabor

MASSNAHMEN ZUR INNOVATIONSFÖRDERUNG

[sn403] 2. August 2026

Artikel 57

KI-Reallabore

(1) Die Mitgliedstaaten sorgen dafür, dass ihre zuständigen Behörden mindestens ein KI-Reallabor auf nationaler Ebene einrichten, das bis zum 2. August 2026 einsatzbereit sein muss. Dieses Reallabor kann auch gemeinsam mit den zuständigen Behörden anderer Mitgliedstaaten eingerichtet werden. Die Kommission kann technische Unterstützung, Beratung und Instrumente für die Einrichtung und den Betrieb von KI-Reallaboren bereitstellen.

Die Verpflichtung nach Unterabsatz 1 kann auch durch Beteiligung an einem bestehenden Reallabor erfüllt werden, sofern eine solche Beteiligung die nationale Abdeckung der teilnehmenden Mitgliedstaaten in gleichwertigem Maße gewährleistet.

(2) Es können auch zusätzliche KI-Reallabore auf regionaler oder lokaler Ebene oder gemeinsam mit den zuständigen Behörden anderer Mitgliedstaaten eingerichtet werden;

[sn502] Anbieter

(3) Der Europäische Datenschutzbeauftragte kann auch ein KI-Reallabor für Organe, Einrichtungen und sonstige Stellen der Union einrichten und die Rollen und Aufgaben der zuständigen nationalen Behörden im Einklang mit diesem Kapitel wahrnehmen.

(4) Die Mitgliedstaaten stellen sicher, dass die in den Absätzen 1 und 2 genannten zuständigen Behörden ausreichende Mittel bereitstellen, um diesem Artikel wirksam und zeitnah nachzukommen. Gegebenenfalls arbeiten die zuständigen nationalen Behörden mit anderen einschlägigen Behörden zusammen und können die Einbeziehung anderer Akteure des KI-Ökosystems gestatten. Andere Reallabore, die im Rahmen des Unionsrechts oder des nationalen Rechts eingerichtet wurden, bleiben von diesem Artikel unberührt. Die Mitgliedstaaten sorgen dafür, dass die diese anderen Reallabore beaufsichtigenden Behörden und die zuständigen nationalen Behörden angemessen zusammenarbeiten.

(5) Die nach Absatz 1 eingerichteten KI-Reallabore bieten eine kontrollierte Umgebung, um Innovation zu fördern und die Entwicklung, das Training, das Testen und die Validierung innovativer KI-Systeme für einen begrenzten Zeitraum vor ihrem Inverkehrbringen oder ihrer Inbetriebnahme nach einem bestimmten zwischen den Anbietern oder zukünftigen Anbietern und der zuständigen Behörde vereinbarten Reallabor-Plan zu erleichtern. In diesen Reallaboren können auch darin beaufsichtigte Tests unter Realbedingungen durchgeführt werden.

(6) Die zuständigen Behörden stellen innerhalb der KI-Reallabore gegebenenfalls Anleitung, Aufsicht und Unterstützung bereit, um Risiken, insbesondere im Hinblick auf Grundrechte, Gesundheit und Sicherheit, Tests und Risikominderungsmaßnahmen sowie deren Wirksamkeit hinsichtlich der Pflichten und Anforderungen dieser Verordnung und gegebenenfalls anderem Unionsrecht und nationalem Recht, deren Einhaltung innerhalb des Reallabors beaufsichtigt wird, zu ermitteln.

(7) Die zuständigen Behörden stellen den Anbietern und zukünftigen Anbietern, die am KI-Reallabor teilnehmen, Leitfäden zu regulatorischen Erwartungen und zur Erfüllung der in dieser Verordnung festgelegten Anforderungen und Pflichten zur Verfügung.

Die zuständige Behörde legt dem Anbieter oder zukünftigen Anbieter des KI-Systems auf dessen Anfrage einen schriftlichen Nachweis für die im Reallabor erfolgreich durchgeführten Tätigkeiten vor. Außerdem legt die zuständige Behörde einen Abschlussbericht vor, in dem sie die im Reallabor durchgeführten Tätigkeiten, deren Ergebnisse und die gewonnenen Erkenntnisse im Einzelnen darlegt. Die Anbieter können diese Unterlagen nutzen, um im Rahmen des Konformitätsbewertungsverfahrens oder einschlägiger Marktüberwachungstätigkeiten nachzuweisen, dass sie dieser Verordnung nachkommen. In diesem Zusammenhang werden die Abschlussberichte und die von der zuständigen nationalen Behörde vorgelegten schriftlichen Nachweise von den Marktüberwachungsbehörden und den notifizierten Stellen im Hinblick auf eine Beschleunigung der Konformitätsbewertungsverfahren in angemessenem Maße positiv gewertet.

(8) Vorbehaltlich der in Artikel 78 enthaltenen Bestimmungen über die Vertraulichkeit und im Einvernehmen mit den Anbietern oder zukünftigen Anbietern, sind die Kommission und das KI-Gremium befugt, die Abschlussberichte einzusehen und tragen diesen gegebenenfalls bei der Wahrnehmung ihrer Aufgaben gemäß dieser Verordnung Rechnung. Wenn der Anbieter oder der zukünftige Anbieter und die zuständige nationale Behörde ihr ausdrückliches Einverständnis erklären, kann der Abschlussbericht über die in diesem Artikel genannte zentrale Informationsplattform veröffentlicht werden.

(9) Die Einrichtung von KI-Reallaboren soll zu den folgenden Zielen beitragen:

a) Verbesserung der Rechtssicherheit, um für die Einhaltung der Regulierungsvorschriften dieser Verordnung oder, gegebenenfalls, anderem geltenden Unionsrecht und nationalem Recht zu sorgen;

b) Förderung des Austauschs bewährter Verfahren durch Zusammenarbeit mit den am KI-Reallabor beteiligten Behörden;

c) Förderung von Innovation und Wettbewerbsfähigkeit sowie Erleichterung der Entwicklung eines KI-Ökosystems;

d) Leisten eines Beitrags zum evidenzbasierten regulatorischen Lernen;

e) Erleichterung und Beschleunigung des Zugangs von KI-Systemen zum Unionsmarkt, insbesondere wenn sie von KMU — einschließlich Start-up-Unternehmen — angeboten werden.

[sn901] Büro für Künstliche Intelligenz

(10) Soweit die innovativen KI-Systeme personenbezogene Daten verarbeiten oder anderweitig der Aufsicht anderer nationaler Behörden oder zuständiger Behörden unterstehen, die den Zugang zu personenbezogenen Daten gewähren oder unterstützen, sorgen die zuständigen nationalen Behörden dafür, dass die nationalen Datenschutzbehörden oder diese anderen nationalen oder zuständigen Behörden in den Betrieb des KI-Reallabors sowie in die Überwachung dieser Aspekte im vollen Umfang ihrer entsprechenden Aufgaben und Befugnisse einbezogen werden.

(11) Die KI-Reallabore lassen die Aufsichts- oder Abhilfebefugnisse der die Reallabore beaufsichtigenden zuständigen Behörden, einschließlich auf regionaler oder lokaler Ebene, unberührt. Alle erheblichen Risiken für die Gesundheit und Sicherheit und die Grundrechte, die bei der Entwicklung und Erprobung solcher KI-Systeme festgestellt werden, führen zur sofortigen und angemessenen Risikominderung. Die zuständigen nationalen Behörden sind befugt, das Testverfahren oder die Beteiligung am Reallabor vorübergehend oder dauerhaft auszusetzen, wenn keine wirksame Risikominderung möglich ist, und unterrichten das Büro für Künstliche Intelligenz über diese Entscheidung. Um Innovationen im Bereich KI in der Union zu fördern, üben die zuständigen nationalen Behörden ihre Aufsichtsbefugnisse im Rahmen des geltenden Rechts aus, indem sie bei der Anwendung der Rechtsvorschriften auf ein bestimmtes KI-Reallabor ihren Ermessensspielraum nutzen.

(12) Die am KI-Reallabor beteiligten Anbieter und zukünftigen Anbieter bleiben nach geltendem Recht der Union und nationalem Haftungsrecht für Schäden haftbar, die Dritten infolge der Erprobung im Reallabor entstehen. Sofern die zukünftigen Anbieter den spezifischen Plan und die Bedingungen für ihre Beteiligung beachten und der Anleitung durch die zuständigen nationalen Behörden in gutem Glauben folgen, werden jedoch von den Behörden keine Geldbußen für Verstöße gegen diese Verordnung verhängt. In Fällen, in denen andere zuständige Behörden, die für anderes Unionsrecht und nationales Recht zuständig sind, aktiv an der Beaufsichtigung des KI-Systems im Reallabor beteiligt waren und Anleitung für die Einhaltung gegeben haben, werden im Hinblick auf dieses Recht keine Geldbußen verhängt.

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

(14) Die zuständigen nationalen Behörden koordinieren ihre Tätigkeiten und arbeiten im Rahmen des KI-Gremiums zusammen.

(15) Die zuständigen nationalen Behörden unterrichten das Büro für Künstliche Intelligenz und das KI-Gremium über die Einrichtung eines Reallabors und können sie um Unterstützung und Anleitung bitten. Das Büro für Künstliche Intelligenz veröffentlicht eine Liste der geplanten und bestehenden Reallabore und hält sie auf dem neuesten Stand, um eine stärkere Interaktion in den KI-Reallaboren und die grenzüberschreitende Zusammenarbeit zu fördern.

(16) Die zuständigen nationalen Behörden übermitteln dem Büro für Künstliche Intelligenz und dem KI-Gremium jährliche Berichte, und zwar ab einem Jahr nach der Einrichtung des Reallabors und dann jedes Jahr bis zu dessen Beendigung, sowie einen Abschlussbericht. Diese Berichte informieren über den Fortschritt und die Ergebnisse der Umsetzung dieser Reallabore, einschließlich bewährter Verfahren, Vorfällen, gewonnener Erkenntnisse und Empfehlungen zu deren Aufbau, sowie gegebenenfalls über die Anwendung und mögliche Überarbeitung dieser Verordnung, einschließlich ihrer delegierten Rechtsakte und Durchführungsrechtsakte, sowie über die Anwendung anderen Unionsrechts, deren Einhaltung von den zuständigen Behörden innerhalb des Reallabors beaufsichtigt wird. Die zuständigen nationalen Behörden stellen diese jährlichen Berichte oder Zusammenfassungen davon der Öffentlichkeit online zur Verfügung. Die Kommission trägt den jährlichen Berichten gegebenenfalls bei der Wahrnehmung ihrer Aufgaben gemäß dieser Verordnung Rechnung.

(17) Die Kommission richtet eine eigene Schnittstelle ein, die alle relevanten Informationen zu den KI-Reallaboren enthält, um es den Interessenträgern zu ermöglichen, mit den KI-Reallaboren zu interagieren und Anfragen an die zuständigen Behörden zu richten und unverbindliche Beratung zur Konformität von innovativen Produkten, Dienstleistungen und Geschäftsmodellen mit integrierter KI-Technologie im Einklang mit Artikel 62 Absatz 1 Buchstabe c einzuholen. Die Kommission stimmt sich gegebenenfalls proaktiv mit den zuständigen nationalen Behörden ab.

Artikel 58

Detaillierte Regelungen für KI-Reallabore und deren Funktionsweise

(1) Um eine Zersplitterung in der Union zu vermeiden, erlässt die Kommission Durchführungsrechtsakte, in denen detaillierte Regelungen für die Einrichtung, Entwicklung, Umsetzung, den Betrieb und die Beaufsichtigung der KI-Reallabore enthalten sind. In den Durchführungsrechtsakten sind gemeinsame Grundsätze zu den folgenden Aspekten festgelegt:

a) Voraussetzungen und Auswahlkriterien 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.

Diese Durchführungsrechtsakte werden gemäß dem in Artikel 98 Absatz 2 genannten Prüfverfahren erlassen.

(2) Die in Absatz 1 genannten Durchführungsrechtsakte gewährleisten,

a) dass KI-Reallabore allen Anbietern oder zukünftigen Anbietern eines KI-Systems, die einen Antrag stellen und die Voraussetzungen und Auswahlkriterien erfüllen, offen stehen; diese Voraussetzungen und Kriterien sind transparent und fair und die zuständigen nationalen Behörden informieren die Antragsteller innerhalb von drei Monaten nach Antragstellung über ihre Entscheidung;

b) dass die KI-Reallabore einen breiten und gleichberechtigten Zugang ermöglichen und mit der Nachfrage nach Beteiligung Schritt halten; die Anbieter und zukünftigen Anbieter auch Anträge zusammen mit Betreibern oder einschlägigen Dritten, die ihre Partner sind, stellen können;

c) dass die detaillierten Regelungen und Bedingungen für KI-Reallabore so gut wie möglich die Flexibilität der zuständigen nationalen Behörden bei der Einrichtung und dem Betrieb ihrer KI-Reallabore unterstützen;

d) dass der Zugang zu KI-Reallaboren für KMU, einschließlich Start-up-Unternehmen, kostenlos ist, unbeschadet außergewöhnlicher Kosten, die die zuständigen nationalen Behörden in einer fairen und verhältnismäßigen Weise einfordern können;

e) dass den Anbietern und zukünftigen Anbietern die Einhaltung der Verpflichtungen zur Konformitätsbewertung nach dieser Verordnung oder die freiwillige Anwendung der in Artikel 95 genannten Verhaltenskodizes mittels der gewonnenen Erkenntnisse der KI-Reallabore erleichtert wird;

f) dass KI-Reallabore die Einbeziehung anderer einschlägiger Akteure innerhalb des KI-Ökosystems, wie etwa notifizierte Stellen und Normungsorganisationen, KMU, einschließlich Start-up-Unternehmen, Unternehmen, Innovatoren, Test- und Versuchseinrichtungen, Forschungs- und Versuchslabore, europäische digitale Innovationszentren, Kompetenzzentren und einzelne Forscher begünstigen, um die Zusammenarbeit mit dem öffentlichen und dem privaten Sektor zu ermöglichen und zu erleichtern;

g) dass die Verfahren, Prozesse und administrativen Anforderungen für die Antragstellung, die Auswahl, die Beteiligung und den Ausstieg aus dem KI-Reallabor einfach, leicht verständlich und klar kommuniziert sind, um die Beteiligung von KMU, einschließlich Start-up-Unternehmen, mit begrenzten rechtlichen und administrativen Kapazitäten zu erleichtern, sowie unionsweit gestrafft sind, um eine Zersplitterung zu vermeiden, und dass die Beteiligung an einem von einem Mitgliedstaat oder dem Europäischen Datenschutzbeauftragten eingerichteten KI-Reallabor gegenseitig und einheitlich anerkannt wird und in der gesamten Union die gleiche Rechtswirkung hat;

h) dass die Beteiligung an dem KI-Reallabor auf einen der Komplexität und dem Umfang des Projekts entsprechenden Zeitraum beschränkt ist, der von der zuständigen nationalen Behörde verlängert werden kann;

i) dass die KI-Reallabore die Entwicklung von Instrumenten und Infrastruktur für das Testen, das Benchmarking, die Bewertung und die Erklärung der Dimensionen von KI-Systemen erleichtern, die für das regulatorische Lernen Bedeutung sind, wie etwa Genauigkeit, Robustheit und Cybersicherheit, sowie Maßnahmen zur Risikominderung im Hinblick auf die Grundrechte und die Gesellschaft als Ganzes fördern.

(3) Zukünftige Anbieter in den KI-Reallaboren, insbesondere KMU und Start-up-Unternehmen, werden gegebenenfalls vor der Einrichtung an Dienste verwiesen, die beispielsweise eine Anleitung zur Umsetzung dieser Verordnung oder andere Mehrwertdienste wie Hilfe bei Normungsdokumenten bereitstellen, sowie an Zertifizierungs-, Test- und Versuchseinrichtungen, europäische digitale Innovationszentren und Exzellenzzentren.

(4) Wenn zuständige nationale Behörden in Betracht ziehen, Tests unter Realbedingungen zu genehmigen, die im Rahmen eines KI-Reallabors beaufsichtigt werden, welches nach diesem Artikel einzurichten ist, vereinbaren sie mit den Beteiligten ausdrücklich die Anforderungen und Bedingungen für diese Tests und insbesondere geeignete Schutzvorkehrungen für Grundrechte, Gesundheit und Sicherheit. Gegebenenfalls arbeiten sie mit anderen zuständigen nationalen Behörden zusammen, um für unionsweit einheitliche Verfahren zu sorgen.

Artikel 59

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 ausschließlich für die Zwecke der Entwicklung, des Trainings und des Testens bestimmter KI-Systeme im Reallabor verarbeitet werden, wenn alle der folgenden Bedingungen erfüllt sind:

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

   i) öffentliche Sicherheit und öffentliche Gesundheit, einschließlich Erkennung, Diagnose, Verhütung, Bekämpfung und Behandlung von Krankheiten sowie Verbesserung von Gesundheitsversorgungssystemen;

[sn502] Anbieter

[sn303] Technische Dokumentation

   ii) hohes Umweltschutzniveau und Verbesserung der Umweltqualität, Schutz der biologischen Vielfalt, Schutz gegen Umweltverschmutzung, Maßnahmen für den grünen Wandel sowie Klimaschutz und Anpassung an den Klimawandel;

   iii) nachhaltige Energie;

   iv) Sicherheit und Widerstandsfähigkeit von Verkehrssystemen und Mobilität, kritischen Infrastrukturen und Netzen;

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

b) die verarbeiteten Daten sind für die Erfüllung einer oder mehrerer der in Kapitel III Abschnitt 2 genannten Anforderungen erforderlich, sofern 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 betroffener 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 des zukünftigen Anbieters, und nur befugte Personen haben Zugriff auf diese Daten;

e) Anbieter dürfen die ursprünglich erhobenen Daten nur im Einklang mit dem Datenschutzrecht der Union weitergeben; personenbezogene Daten, die im Reallabor erstellt wurden, dürfen nicht außerhalb des Reallabors weitergegeben werden;

f) eine Verarbeitung personenbezogener Daten im Rahmen des Reallabors führt zu keinen Maßnahmen oder Entscheidungen, die Auswirkungen auf die betroffenen Personen haben, und berührt nicht die Anwendung ihrer Rechte, die in den Rechtsvorschriften der Union über den Schutz personenbezogener Daten festgelegt sind;

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 nationalen 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 Reallabor entwickelten KI-Projekts, seiner Ziele und der 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.

(2) Für die Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstrekkung — 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 in KI-Reallaboren auf der Grundlage eines spezifischen Unionsrechts oder nationalen Rechts und unterliegt den kumulativen Bedingungen des Absatzes 1.

(3) Das Unionsrecht oder nationale Recht, das die Verarbeitung personenbezogener Daten für andere Zwecke als die ausdrücklich in jenem Recht genannten ausschließt, sowie Unionsrecht oder nationales Recht, in dem die Grundlagen für eine für die Zwecke der Entwicklung, des Testens oder 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.

[sn502] Anbieter

Artikel 60

Tests von Hochrisiko-KI-Systemen unter Realbedingungen außerhalb von KI-Reallaboren

[sn503] Betreiber

(1) Tests von Hochrisiko-KI-Systemen unter Realbedingungen können von Anbietern oder zukünftigen Anbietern von in Anhang III aufgeführten Hochrisiko-KI-Systemen außerhalb von KI-Reallaboren gemäß diesem Artikel und — unbeschadet der Bestimmungen unter Artikel 5 — dem in diesem Artikel genannten Plan für einen Test unter Realbedingungen durchgeführt werden.

Die Kommission legt die einzelnen Elemente des Plans für einen Test unter Realbedingungen im Wege von Durchführungsrechtsakten fest. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 98 Absatz 2 genannten Prüfverfahren erlassen.

Das Unionsrecht oder nationale Recht für das Testen von Hochrisiko-KI-Systemen unter Realbedingungen im Zusammenhang mit Produkten, die unter die in Anhang I aufgeführten Harmonisierungsrechtsvorschriften der Union fallen, bleibt von dieser Bestimmung unberührt.

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

[sn908] EU-Datenbank

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

(4) Tests unter Realbedingungen 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 einen Test unter Realbedingungen erstellt und diesen bei der Marktüberwachungsbehörde in dem Mitgliedstaat eingereicht, in dem der Test unter Realbedingungen stattfinden soll;

b) die Marktüberwachungsbehörde in dem Mitgliedstaat, in dem der Test unter Realbedingungen stattfinden soll, hat den Test unter Realbedingungen und den Plan für einen Test unter Realbedingungen genehmigt; hat die Marktüberwachungsbehörde innerhalb von 30 Tagen keine Antwort gegeben, so gelten der Test unter Realbedingungen und der Plan für einen Test unter Realbedingungen als genehmigt; ist im nationalen Recht keine stillschweigende Genehmigung vorgesehen, so bleibt der Test unter Realbedingungen genehmigungspflichtig;

c) der Anbieter oder zukünftige Anbieter, mit Ausnahme der in Anhang III Nummern 1, 6 und 7 genannten Anbieter oder zukünftigen Anbieter von Hochrisiko-KI-Systemen in den Bereichen Strafverfolgung, Migration, Asyl und Grenzkontrolle und der in Anhang III Nummer 2 genannten Hochrisiko-KI-Systeme, hat den Test unter Realbedingungen unter Angabe einer unionsweit einmaligen Identifizierungsnummer und der in Anhang IX festgelegten Informationen gemäß Artikel 71 Absatz 4 registriert; der Anbieter oder zukünftige Anbieter von Hochrisiko-KI-Systemen gemäß Anhang III Nummern 1, 6 und 7 in den Bereichen Strafverfolgung, Migration, Asyl und Grenzkontrollmanagement hat die Tests unter Realbedingungen im sicheren nicht öffentlichen Teil der EU-Datenbank gemäß Artikel 49 Absatz 4 Buchstabe d mit einer unionsweit einmaligen Identifizierungsnummer und den darin festgelegten Informationen registriert; der Anbieter oder zukünftige Anbieter von Hochrisiko-KI-Systemen gemäß Anhang III Nummer 2 hat die Tests unter Realbedingungen gemäß Artikel 49 Absatz 5 registriert;

d) der Anbieter oder der zukünftige Anbieter, der den Test unter Realbedingungen durchführt, ist in der Union niedergelassen oder hat einen in der Union niedergelassenen gesetzlichen Vertreter bestellt;

e) die für die Zwecke des Tests unter Realbedingungen erhobenen und verarbeiteten Daten werden nur dann an Drittländer übermittelt, wenn gemäß Unionsrecht geeignete und anwendbare Schutzvorkehrungen greifen;

[sn503] Betreiber

f) der Test unter Realbedingungen dauert nicht länger als zur Erfüllung seiner Zielsetzungen nötig und in keinem Fall länger als sechs Monate; dieser Zeitraum kann um weitere sechs Monate verlängert werden, sofern der Anbieter oder der zukünftige Anbieter die Marktüberwachungsbehörde davon vorab in Kenntnis setzt und erläutert, warum eine solche Verlängerung erforderlich ist;

g) Testteilnehmer im Rahmen von Tests unter Realbedingungen, die aufgrund ihres Alters oder einer Behinderung schutzbedürftigen Gruppen angehören, sind angemessen geschützt;

h) wenn ein Anbieter oder zukünftiger Anbieter den Test unter Realbedingungen in Zusammenarbeit mit einem oder mehreren Betreibern oder zukünftigen Betreibern organisiert, werden Letztere vorab über alle für ihre Teilnahmeentscheidung relevanten Aspekte des Tests informiert und erhalten die einschlägigen in Artikel 13 genannten Betriebsanleitungen für das KI-System; der Anbieter oder zukünftige Anbieter und der Betreiber oder zukünftige Betreiber schließen eine Vereinbarung, in der ihre Aufgaben und Zuständigkeiten festgelegt sind, um für die Einhaltung der nach dieser Verordnung und anderem Unionsrecht und nationalem Recht für Tests unter Realbedingungen geltenden Bestimmungen zu sorgen;

i) die Testteilnehmer im Rahmen von Tests unter Realbedingungen erteilen ihre informierte Einwilligung gemäß Artikel 61, oder, wenn im Fall der Strafverfolgung die Einholung einer informierten Einwilligung den Test des KI-Systems verhindern würde, dürfen sich der Test und die Ergebnisse des Tests unter Realbedingungen nicht negativ auf die Testteilnehmer auswirken und ihre personenbezogenen Daten werden nach Durchführung des Tests gelöscht;

j) der Anbieter oder zukünftige Anbieter und die Betreiber und zukünftigen Betreiber lassen den Test unter Realbedingungen von Personen wirksam überwachen, die auf dem betreffenden Gebiet angemessen qualifiziert sind und über die Fähigkeit, Ausbildung und Befugnis verfügen, die für die Wahrnehmung ihrer Aufgaben erforderlich sind;

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

(5) Jeder Testteilnehmer bezüglich des Tests unter Realbedingungen oder gegebenenfalls dessen gesetzlicher Vertreter kann seine Teilnahme an dem Test jederzeit durch Widerruf seiner informierten Einwilligung beenden und die unverzügliche und dauerhafte Löschung seiner personenbezogenen Daten verlangen, ohne dass ihm daraus Nachteile entstehen und er dies in irgendeiner Weise begründen müsste. Der Widerruf der informierten Einwilligung wirkt sich nicht auf bereits durchgeführte Tätigkeiten aus.

(6) Im Einklang mit Artikel 75 übertragen die Mitgliedstaaten ihren Marktüberwachungsbehörden die Befugnis, Anbieter und zukünftige Anbieter zur Bereitstellung von Informationen zu verpflichten, unangekündigte Ferninspektionen oder Vor-Ort-Inspektionen durchzuführen und die Durchführung der Tests unter Realbedingungen und damit zusammenhängende Hochrisiko-KI-Systeme zu prüfen. Die Marktüberwachungsbehörden nutzen diese Befugnisse, um für die sichere Entwicklung von Tests unter Realbedingungen zu sorgen.

(7) Jegliche schwerwiegenden Vorfälle im Verlauf des Tests unter Realbedingungen sind den nationalen Marktüberwachungsbehörden gemäß Artikel 73 zu melden. Der Anbieter oder zukünftige Anbieter trifft Sofortmaßnahmen zur Schadensbegrenzung; andernfalls setzt er den Test unter Realbedingungen so lange aus, bis eine Schadensbegrenzung stattgefunden hat, oder bricht ihn ab. Im Fall eines solchen Abbruchs des Tests unter Realbedingungen richtet der Anbieter oder zukünftige Anbieter ein Verfahren für den sofortigen Rückruf des KI-Systems ein.

(8) Anbieter oder zukünftige Anbieter setzen die nationalen Marktüberwachungsbehörde in dem Mitgliedstaat, in dem der Test unter Realbedingungen stattfindet, über die Aussetzung oder den Abbruch des Tests unter Realbedingungen und die Endergebnisse in Kenntnis.

(9) Anbieter oder zukünftige Anbieter sind nach geltendem Recht der Union und geltendem nationalen Recht für Schäden haftbar, die während ihrer Tests unter Realbedingungen entstehen.

[sn506] KI-Reallabor

Artikel 61

Informierte Einwilligung zur Teilnahme an einem Test unter Realbedingungen außerhalb von KI-Reallaboren

(1) Für die Zwecke von Tests unter Realbedingungen gemäß Artikel 60 ist von den Testteilnehmern eine freiwillig erteilte informierte Einwilligung einzuholen, bevor sie an dem Test teilnehmen und nachdem sie mit präzisen, klaren, relevanten und verständlichen Informationen über Folgendes ordnungsgemäß informiert wurden:

a) die Art und die Zielsetzungen des Tests unter Realbedingungen und etwaige mit ihrer Teilnahme verbundene Unannehmlichkeiten;

[sn502] Anbieter

b) die Bedingungen, unter denen der Test unter Realbedingungen erfolgen soll, einschließlich der voraussichtlichen Dauer der Teilnahme des Testteilnehmers oder der Testteilnehmer;

c) ihre Rechte und Garantien, die ihnen bezüglich ihrer Teilnahme zustehen, insbesondere ihr Recht, die Teilnahme an dem Test unter Realbedingungen zu verweigern oder diese Teilnahme jederzeit zu beenden, ohne dass ihnen daraus Nachteile entstehen und sie dies in irgendeiner Weise begründen müssten;

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

e) die unionsweit einmalige Identifizierungsnummer des Tests unter Realbedingungen gemäß Artikel 60 Absatz 4 Buchstabe c und die Kontaktdaten des Anbieters oder seines gesetzlichen Vertreters, bei dem weitere Informationen eingeholt werden können.

(2) Die informierte Einwilligung ist zu datieren und zu dokumentieren, und eine Kopie wird den Testteilnehmern oder ihren gesetzlichen Vertretern ausgehändigt.

[sn901] Büro für Künstliche Intelligenz

Artikel 62

Maßnahmen für Anbieter und Betreiber, insbesondere KMU, einschließlich Start-up-Unternehmen

(1) Die Mitgliedstaaten ergreifen die folgenden Maßnahmen:

a) Sie gewähren KMU — einschließlich Start-up-Unternehmen —, die ihren Sitz oder eine Zweigniederlassung in der Union haben, soweit sie die Voraussetzungen und Auswahlkriterien erfüllen, vorrangigen Zugang zu den KI-Reallaboren; der vorrangige Zugang schließt nicht aus, dass andere als die in diesem Absatz genannten KMU, einschließlich Start-up-Unternehmen, Zugang zum KI-Reallabor erhalten, sofern sie ebenfalls die Zulassungsvoraussetzungen und Auswahlkriterien erfüllen;

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

c) sie nutzen entsprechende bestehende Kanäle und richten gegebenenfalls neue Kanäle für die Kommunikation mit KMU, einschließlich Start-up-Unternehmen, Betreibern, anderen Innovatoren sowie gegebenenfalls lokalen Behörden ein, um Ratschläge zu geben und Fragen zur Durchführung dieser Verordnung, auch bezüglich der Beteiligung an KI-Reallaboren, zu beantworten;

d) sie fördern die Beteiligung von KMU und anderen einschlägigen Interessenträgern an der Entwicklung von Normen.

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

(3) Das Büro für Künstliche Intelligenz ergreift die folgenden Maßnahmen:

a) es stellt standardisierte Muster für die unter diese Verordnung fallenden Bereiche bereit, wie vom KI-Gremium in seinem Antrag festgelegt;

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

[sn902] Europäisches KI-Gremium

c) es führt geeignete Informationskampagnen durch, um für die aus dieser Verordnung erwachsenden Pflichten zu sensibilisieren;

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

Artikel 63

Ausnahmen für bestimmte Akteure

(1) Kleinstunternehmen im Sinne der Empfehlung 2003/361/EG können bestimmte Elemente des in Artikel 17 dieser Verordnung vorgeschriebenen Qualitätsmanagementsystems in vereinfachter Weise einhalten, sofern sie keine Partnerunternehmen oder verbundenen Unternehmen im Sinne dieser Empfehlung haben. Zu diesem Zweck arbeitet die Kommission Leitlinien zu den Elementen des Qualitätsmanagementsystems aus, die unter Berücksichtigung der Bedürfnisse von Kleinstunternehmen in vereinfachter Weise eingehalten werden können, ohne das Schutzniveau oder die Notwendigkeit zur Einhaltung der Anforderungen in Bezug auf Hochrisiko-KI-Systeme zu beeinträchtigen.

[sn501] Künstliche Intelligenz

[sn901] Büro für Künstliche Intelligenz

(2) Absatz 1 dieses Artikels ist nicht dahin gehend auszulegen, dass diese Akteure auch von anderen in dieser Verordnung festgelegten Anforderungen oder Pflichten, einschließlich der nach den Artikeln 9, 10, 11, 12, 13, 14, 15, 72 und 73 geltenden, befreit sind.

KAPITEL VII

GOVERNANCE

ABSCHNITT 1

Governance auf Unionsebene

Artikel 64

Büro für Künstliche Intelligenz

(1) Die Kommission entwickelt über das Büro für Künstliche Intelligenz die Sachkenntnis und Fähigkeiten der Union auf dem Gebiet der KI.

(2) Die Mitgliedstaaten erleichtern dem Büro für Künstliche Intelligenz die ihm gemäß dieser Verordnung übertragenen Aufgaben.

Artikel 65

Einrichtung und Struktur des Europäischen Gremiums für Künstliche Intelligenz

(1) Ein Europäisches Gremium für Künstliche Intelligenz (im Folgenden „KI-Gremium“) wird hiermit eingerichtet.

(2) Das KI-Gremium setzt sich aus einem Vertreter je Mitgliedstaat zusammen. Der Europäische Datenschutzbeauftragte nimmt als Beobachter teil. Das Büro für Künstliche Intelligenz nimmt ebenfalls an den Sitzungen des KI-Gremiums teil, ohne sich jedoch an den Abstimmungen zu beteiligen. Andere Behörden oder Stellen der Mitgliedstaaten und der Union oder Sachverständige können im Einzelfall zu den Sitzungen des KI-Gremiums eingeladen werden, wenn die erörterten Fragen für sie von Belang sind.

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

(4) Die Mitgliedstaaten sorgen dafür, dass ihre Vertreter im KI-Gremium

a) in ihrem Mitgliedstaat über die einschlägigen Kompetenzen und Befugnisse verfügen, sodass sie aktiv zur Bewältigung der in Artikel 66 genannten Aufgaben des KI-Gremiums beitragen können;

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

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

(5) Die benannten Vertreter der Mitgliedstaaten nehmen die Geschäftsordnung des KI-Gremiums 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 Abstimmungsregelungen und die Organisation der Tätigkeiten des KI-Gremiums und seiner Untergruppen festgelegt.

[sn909] Beratungsforum

(6) Das KI-Gremium richtet zwei ständige Untergruppen ein, um Marktüberwachungsbehörden eine Plattform für die Zusammenarbeit und den Austausch zu bieten und Behörden über Angelegenheiten, die jeweils die Marktüberwachung und notifizierte Stellen betreffen, zu unterrichten.

[sn901] Büro für Künstliche Intelligenz

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.

Das KI-Gremium kann weitere ständige oder nichtständige Untergruppen einrichten, falls das für die Prüfung bestimmter Fragen zweckmäßig sein sollte. Gegebenenfalls können Vertreter des in Artikel 67 genannten Beratungsforums als Beobachter zu diesen Untergruppen oder zu bestimmten Sitzungen dieser Untergruppen eingeladen werden.

(7) Das KI-Gremium wird so organisiert und geführt, dass bei seinen Tätigkeiten Objektivität und Unparteilichkeit gewahrt sind.

(8) Den Vorsitz im KI-Gremium führt einer der Vertreter der Mitgliedstaaten. Die Sekretariatsgeschäfte des KI-Gremiums werden vom Büro für Künstliche Intelligenz geführt; dieses beruft auf Anfrage des Vorsitzes die Sitzungen ein und erstellt die Tagesordnung im Einklang mit den Aufgaben des KI-Gremiums gemäß dieser Verordnung und seiner Geschäftsordnung.

Artikel 66

Aufgaben des KI-Gremiums

[sn908] EU-Datenbank

Das KI-Gremium berät und unterstützt die Kommission und die Mitgliedstaaten, um die einheitliche und wirksame Anwendung dieser Verordnung zu erleichtern. Für diese Zwecke kann das KI-Gremium insbesondere

a) zur Koordinierung zwischen den für die Anwendung dieser Verordnung zuständigen nationalen Behörden beitragen und in Zusammenarbeit mit den betreffenden Marktüberwachungsbehörden und vorbehaltlich ihrer Zustimmung gemeinsame Tätigkeiten der Marktüberwachungsbehörden gemäß Artikel 74 Absatz 11 unterstützen;

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

c) zur Durchführung dieser Verordnung Beratung anbieten, insbesondere im Hinblick auf die Durchsetzung der Vorschriften zu KI-Modellen mit allgemeinem Verwendungszweck;

d) zur Harmonisierung der Verwaltungspraxis in den Mitgliedstaaten beitragen, auch bezüglich der Ausnahme vom Konformitätsbewertungsverfahren gemäß Artikel 46 und der Funktionsweise von KI-Reallaboren und Tests unter Realbedingungen gemäß den Artikeln 57, 59 und 60;

e) auf Anfrage der Kommission oder in Eigeninitiative Empfehlungen und schriftliche Stellungnahmen zu einschlägigen Fragen der Durchführung dieser Verordnung und ihrer einheitlichen und wirksamen Anwendung abgeben, einschließlich

   i) zur Entwicklung und Anwendung von Verhaltenskodizes und Praxisleitfäden gemäß dieser Verordnung sowie der Leitlinien der Kommission;

   ii) zur Bewertung und Überprüfung dieser Verordnung gemäß Artikel 112, auch in Bezug auf die Meldung schwerwiegender Vorfälle gemäß Artikel 73 und das Funktionieren der EU-Datenbank gemäß Artikel 71, die Ausarbeitung der delegierten Rechtsakte oder Durchführungsrechtsakte sowie im Hinblick auf mögliche Anpassungen dieser Verordnung an die in Anhang I aufgeführten Harmonisierungsrechtsvorschriften der Union;

   iii) zu technischen Spezifikationen oder geltenden Normen in Bezug auf die in Kapitel III Abschnitt 2 festgelegten Anforderungen;

iv) zur Anwendung der in den Artikeln 40 und 41 genannten harmonisierten Normen oder gemeinsamen Spezifikationen;

v) zu Tendenzen, etwa im Bereich der globalen Wettbewerbsfähigkeit Europas auf dem Gebiet der KI, bei der Verbreitung von KI in der Union und bei der Entwicklung digitaler Fähigkeiten;

vi) zu Tendenzen im Bereich der sich ständig weiterentwickelnden Typologie der KI-Wertschöpfungsketten insbesondere hinsichtlich der sich daraus ergebenden Auswirkungen auf die Rechenschaftspflicht;

vii) zur möglicherweise notwendigen Änderung des Anhangs III im Einklang mit Artikel 7 und zur möglicherweise notwendigen Überarbeitung des Artikels 5 gemäß Artikel 112 unter Berücksichtigung der einschlägigen verfügbaren Erkenntnisse und der neuesten technologischen Entwicklungen;

f) die Kommission bei der Förderung der KI-Kompetenz, der Sensibilisierung und Aufklärung der Öffentlichkeit in Bezug auf die Vorteile, Risiken, Schutzmaßnahmen, Rechte und Pflichten im Zusammenhang mit der Nutzung von KI-Systemen unterstützen;

g) die Entwicklung gemeinsamer Kriterien und eines gemeinsamen Verständnisses der Marktteilnehmer und der zuständigen Behörden in Bezug auf die in dieser Verordnung vorgesehenen einschlägigen Konzepte erleichtern, auch durch einen Beitrag zur Entwicklung von Benchmarks;

h) gegebenenfalls mit anderen Organen, Einrichtungen und sonstigen Stellen der EU, einschlägigen Sachverständigengruppen und Netzwerken der EU insbesondere in den Bereichen Produktsicherheit, Cybersicherheit, Wettbewerb, digitale und Mediendienste, Finanzdienstleistungen, Verbraucherschutz, Datenschutz und Schutz der Grundrechte zusammenarbeiten;

i) zur wirksamen Zusammenarbeit mit den zuständigen Behörden von Drittstaaten und mit internationalen Organisationen beitragen;

[sn909] Beratungsforum

j) die zuständigen nationalen Behörden und die Kommission beim Aufbau des für die Durchführung dieser Verordnung erforderlichen organisatorischen und technischen Fachwissens beraten, unter anderem durch einen Beitrag zur Einschätzung des Schulungsbedarfs des Personals der Mitgliedstaaten, das an der Durchführung dieser Verordnung beteiligt ist;

k) dem Büro für Künstliche Intelligenz helfen, die zuständigen nationalen Behörden bei der Einrichtung und Entwicklung von KI-Reallaboren zu unterstützen, und die Zusammenarbeit und den Informationsaustausch zwischen KI-Reallaboren erleichtern;

l) zur Entwicklung von Leitfäden beitragen und diesbezüglich entsprechend beraten;

m) die Kommission zu internationalen Angelegenheiten im Bereich der KI beraten;

n) der Kommission Stellungnahmen zu qualifizierten Warnungen in Bezug auf KI-Modelle mit allgemeinem Verwendungszweck vorlegen;

o) Stellungnahmen der Mitgliedstaaten zu qualifizierten Warnungen in Bezug auf KI-Modelle mit allgemeinem Verwendungszweck entgegennehmen sowie zu nationalen Erfahrungen und Praktiken bei der Überwachung und Durchsetzung von KI-Systemen, insbesondere von Systemen, die KI-Modelle mit allgemeinem Verwendungszweck integrieren.

Artikel 67

Beratungsforum

(1) Es wird ein Beratungsforum eingerichtet, das technisches Fachwissen bereitstellt, das KI-Gremium und die Kommission berät und zu deren Aufgaben im Rahmen dieser Verordnung beiträgt.

(2) Die Mitglieder des Beratungsforums vertreten eine ausgewogene Auswahl von Interessenträgern, darunter die Industrie, Start-up-Unternehmen, KMU, die Zivilgesellschaft und die Wissenschaft. Bei der Zusammensetzung des Beratungsforums wird auf ein ausgewogenes Verhältnis zwischen wirtschaftlichen und nicht-wirtschaftlichen Interessen und innerhalb der Kategorie der wirtschaftlichen Interessen zwischen KMU und anderen Unternehmen geachtet.

(3) Die Kommission ernennt die Mitglieder des Beratungsforums gemäß den in Absatz 2 genannten Kriterien aus dem Kreis der Interessenträger mit anerkanntem Fachwissen auf dem Gebiet der KI.

(4) Die Amtszeit der Mitglieder des Beratungsforums beträgt zwei Jahre; sie kann bis zu höchstens vier Jahre verlängert werden.

(5) Die Agentur der Europäischen Union für Grundrechte, ENISA, das Europäische Komitee für Normung (CEN), das Europäische Komitee für elektrotechnische Normung (CENELEC) und das Europäische Institut für Telekommunikationsnormen (ETSI) sind ständige Mitglieder des Beratungsforums.

(6) Das Beratungsforum gibt sich eine Geschäftsordnung. Es wählt gemäß den in Absatz 2 festgelegten Kriterien zwei Ko-Vorsitzende unter seinen Mitgliedern. Die Amtszeit der Ko-Vorsitzenden beträgt zwei Jahre und kann einmal verlängert werden.

(7) Das Beratungsforum hält mindestens zweimal pro Jahr Sitzungen ab. Das Beratungsforum kann Sachverständige und andere Interessenträger zu seinen Sitzungen einladen.

(8) Das Beratungsforum kann auf Ersuchen des KI-Gremiums oder der Kommission Stellungnahmen, Empfehlungen und schriftliche Beiträge ausarbeiten.

(9) Das Beratungsforum kann gegebenenfalls ständige oder zeitweilige Untergruppen einsetzen, um spezifische Fragen im Zusammenhang mit den Zielen dieser Verordnung zu prüfen.

(10) Das Beratungsforum erstellt jährlich einen Bericht über seine Tätigkeit. Dieser Bericht wird veröffentlicht.

[sn901] Büro für Künstliche Intelligenz

Artikel 68

Wissenschaftliches Gremium unabhängiger Sachverständiger

(1) Die Kommission erlässt im Wege eines Durchführungsrechtsakts Bestimmungen über die Einrichtung eines wissenschaftlichen Gremiums unabhängiger Sachverständiger („wissenschaftliches Gremium"), das die Durchsetzungstätigkeiten im Rahmen dieser Verordnung unterstützen soll. Dieser Durchführungsrechtsakt wird gemäß dem in Artikel 98 Absatz 2 genannten Prüfverfahren erlassen.

(2) Das wissenschaftliche Gremium setzt sich aus Sachverständigen zusammen, die von der Kommission auf der Grundlage aktueller wissenschaftlicher oder technischer Fachkenntnisse auf dem Gebiet der KI, die zur Erfüllung der in Absatz 3 genannten Aufgaben erforderlich sind, ausgewählt werden, und muss nachweisen können, dass es alle folgenden Bedingungen erfüllt:

a) es verfügt über besondere Fachkenntnisse und Kompetenzen sowie über wissenschaftliches oder technisches Fachwissen auf dem Gebiet der KI;

b) es ist von Anbietern von KI-Systemen oder KI-Modellen mit allgemeinem Verwendungszweck unabhängig;

c) es ist in der Lage, Tätigkeiten sorgfältig, präzise und objektiv auszuführen.

Die Kommission legt in Absprache mit dem KI-Gremium die Anzahl der Sachverständigen des Gremiums nach Maßgabe der jeweiligen Erfordernisse fest und sorgt für eine ausgewogene Vertretung der Geschlechter und eine gerechte geografische Verteilung.

(3) Das wissenschaftliche Gremium berät und unterstützt das Büro für Künstliche Intelligenz, insbesondere in Bezug auf folgende Aufgaben:

a) Unterstützung bei der Durchführung und Durchsetzung dieser Verordnung in Bezug auf KI-Modelle und -Systeme mit allgemeinem Verwendungszweck, insbesondere indem es

   i) das Büro für Künstliche Intelligenz im Einklang mit Artikel 90 vor möglichen systemischen Risiken von KI-Modellen mit allgemeinem Verwendungszweck auf Unionsebene warnt;

   ii) einen Beitrag zur Entwicklung von Instrumenten und Methoden für die Bewertung der Fähigkeiten von KI-Modellen und -Systemen mit allgemeinem Verwendungszweck, auch durch Benchmarks, leistet;

   iii) Beratung über die Einstufung von KI-Modellen mit allgemeinem Verwendungszweck mit systemischem Risiko anbietet;

   iv) Beratung über die Einstufung verschiedener KI-Modelle und -Systeme mit allgemeinem Verwendungszweck anbietet;

v) einen Beitrag zur Entwicklung von Instrumenten und Mustern leistet;

b) Unterstützung der Arbeit der Marktüberwachungsbehörden auf deren Ersuchen;

c) Unterstützung grenzüberschreitender Marktüberwachungstätigkeiten gemäß Artikel 74 Absatz 11, ohne dass die Befugnisse der Marktüberwachungsbehörden berührt werden;

[sn901] Büro für Künstliche Intelligenz

d) Unterstützung des Büros für Künstliche Intelligenz bei der Wahrnehmung seiner Aufgaben im Rahmen des Schutzklauselverfahrens der Union gemäß Artikel 81.

(4) Die Sachverständigen des wissenschaftlichen Gremiums 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. Sie dürfen bei der Wahrnehmung ihrer Aufgaben nach Absatz 3 weder Weisungen anfordern noch entgegennehmen. Jeder Sachverständige gibt eine Interessenerklärung ab, die öffentlich zugänglich gemacht wird. Das Büro für Künstliche Intelligenz richtet Systeme und Verfahren ein, mit denen mögliche Interessenkonflikte aktiv bewältigt und verhindert werden können.

(5) Der in Absatz 1 genannte Durchführungsrechtsakt enthält Bestimmungen über die Bedingungen, Verfahren und detaillierten Regelungen nach denen das wissenschaftliche Gremium und seine Mitglieder Warnungen ausgeben und das Büro für Künstliche Intelligenz um Unterstützung bei der Wahrnehmung der Aufgaben des wissenschaftlichen Gremiums ersuchen können.

Artikel 69

Zugang zum Pool von Sachverständigen durch die Mitgliedstaaten

(1) Die Mitgliedstaaten können Sachverständige des wissenschaftlichen Gremiums hinzuziehen, um ihre Durchsetzungstätigkeiten im Rahmen dieser Verordnung zu unterstützen.

(2) Die Mitgliedstaaten können verpflichtet werden, für die Beratung und Unterstützung durch die Sachverständigen Gebühren zu entrichten. Struktur und Höhe der Gebühren sowie Umfang und Struktur erstattungsfähiger Kosten werden in dem in Artikel 68 Absatz 1 genannten Durchführungsrechtsakt festgelegt, wobei die Zielsetzung berücksichtigt wird, für die angemessene Durchführung dieser Verordnung, für Kosteneffizienz sowie dafür zu sorgen, dass alle Mitgliedstaaten effektiven Zugang zu Sachverständigen haben müssen.

[sn402] 2. August 2025

(3) Die Kommission ermöglicht den Mitgliedstaaten bei Bedarf einen rechtzeitigen Zugang zu den Sachverständigen und sorgt dafür, dass die Kombination aus unterstützenden Tätigkeiten durch die Union zur Prüfung von KI gemäß Artikel 84 und durch die Sachverständigen gemäß dem vorliegenden Artikel effizient organisiert ist und den bestmöglichen zusätzlichen Nutzen bringt.

ABSCHNITT 2

Zuständige nationale Behörden

Artikel 70

Benennung von zuständigen nationalen Behörden und zentrale Anlaufstelle

(1) Jeder Mitgliedstaat muss für die Zwecke dieser Verordnung mindestens eine notifizierende Behörde und mindestens eine Marktüberwachungsbehörde als zuständige nationale Behörden einrichten oder benennen. Diese zuständigen nationalen Behörden üben ihre Befugnisse unabhängig, unparteiisch und unvoreingenommen aus, um die Objektivität ihrer Tätigkeiten und Aufgaben zu gewährleisten und die Anwendung und Durchführung dieser Verordnung sicherzustellen. Die Mitglieder dieser Behörden haben jede Handlung zu unterlassen, die mit ihren Aufgaben unvereinbar ist. Sofern diese Grundsätze gewahrt werden, können die betreffenden Tätigkeiten und Aufgaben gemäß den organisatorischen Erfordernissen des Mitgliedstaats von einer oder mehreren benannten Behörden wahrgenommen werden.

(2) Die Mitgliedstaaten teilen der Kommission die Namen der notifizierenden Behörden und der Marktüberwachungsbehörden und die Aufgaben dieser Behörden sowie alle späteren Änderungen mit. Die Mitgliedstaaten machen Informationen darüber, wie die zuständigen Behörden und zentralen Anlaufstellen bis zum 2. August 2025 auf elektronischem Wege kontaktiert werden können, öffentlich zugänglich. Die Mitgliedstaaten benennen eine Marktüberwachungsbehörde, die als zentrale Anlaufstelle für diese Verordnung fungiert, und teilen der Kommission den Namen der zentralen Anlaufstelle mit. Die Kommission erstellt eine öffentlich verfügbare Liste der zentralen Anlaufstellen.

(3) Die Mitgliedstaaten sorgen dafür, dass ihre zuständigen nationalen Behörden mit angemessenen technischen und finanziellen Mitteln sowie geeignetem Personal und Infrastrukturen ausgestattet werden, damit sie ihre Aufgaben im Rahmen dieser Verordnung wirksam erfüllen können. Insbesondere müssen die zuständigen nationalen Behörden zu jeder Zeit über eine ausreichende Zahl von Mitarbeitern verfügen, zu deren Kompetenzen und Fachwissen ein tiefes Verständnis der KI-Technologien, der Daten und Datenverarbeitung, des Schutzes personenbezogener Daten, der Cybersicherheit, der Grundrechte, der Gesundheits- und Sicherheitsrisiken sowie Kenntnis der bestehenden Normen und rechtlichen Anforderungen gehört. Die Mitgliedstaaten bewerten und aktualisieren, falls erforderlich, jährlich die in diesem Absatz genannten Erfordernisse bezüglich Kompetenzen und Ressourcen.

[sn402] 2. August 2025

(4) Die zuständigen nationalen Behörden ergreifen geeignete Maßnahmen zur Sicherstellung eines angemessenen Maßes an Cybersicherheit.

(5) Bei der Erfüllung ihrer Aufgaben halten sich die zuständigen nationalen Behörden an die in Artikel 78 festgelegten Vertraulichkeitspflichten.

(6) Bis zum 2. August 2025 und anschließend alle zwei Jahre erstatten die Mitgliedstaaten der Kommission Bericht über den Sachstand bezüglich der finanziellen Mittel und des Personals der zuständigen nationalen Behörden und geben eine Einschätzung über deren Angemessenheit ab. Die Kommission leitet diese Informationen zur Erörterung und etwaigen Abgabe von Empfehlungen an das KI-Gremium weiter.

[sn908] EU-Datenbank

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

(8) Die zuständigen nationalen Behörden können gegebenenfalls insbesondere KMU, einschließlich Start-up-Unternehmen, unter Berücksichtigung der Anleitung und Beratung durch das KI-Gremium oder der Kommission mit Anleitung und Beratung bei der Durchführung dieser Verordnung zur Seite stehen. Wenn zuständige nationale Behörden beabsichtigen, Anleitung und Beratung in Bezug auf ein KI-System in Bereichen anzubieten, die unter das Unionrecht fallen, so sind gegebenenfalls die nach jenen Unionsrecht zuständigen nationalen Behörden zu konsultieren.

[sn502] Anbieter

(9) 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.

[sn503] Betreiber

KAPITEL VIII

EU-DATENBANK FÜR HOCHRISIKO-KI-SYSTEME

Artikel 71

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 den Absätzen 2 und 3 dieses Artikels genannten Informationen über Hochrisiko-KI-Systeme nach Artikel 6 Absatz 2, die gemäß den Artikeln 49 und 60 registriert werden und über KI-Systeme, die nicht als Hochrisiko-KI-Systeme gemäß Artikel 6 Absatz 3 gelten und gemäß Artikel 6 Absatz 4 und Artikel 49 registriert werden. Bei der Festlegung der Funktionsspezifikationen dieser Datenbank konsultiert die Kommission die einschlägigen Sachverständigen und bei der Aktualisierung der Funktionsspezifikationen dieser Datenbank konsultiert sie das KI-Gremium.

(2) Die in Anhang VIII Abschnitte A und B aufgeführten Daten werden vom Anbieter oder gegebenenfalls vom Bevollmächtigten in die EU-Datenbank eingegeben.

(3) Die in Anhang VIII Abschnitt C aufgeführten Daten werden vom Betreiber, der eine Behörde, Einrichtung oder sonstige Stelle ist oder in deren Namen handelt, gemäß Artikel 49 Absätze 3 und 4 in die EU-Datenbank eingegeben.

(4) Mit Ausnahme des in Artikel 49 Absatz 4 und Artikel 60 Absatz 4 Buchstabe c genannten Abschnitts müssen die gemäß Artikel 49 in der Datenbank registrierten und dort enthaltenen Informationen auf benutzerfreundliche Weise zugänglich und öffentlich verfügbar sein. Die Informationen sollten leicht handhabbar und maschinenlesbar sein. Auf die gemäß Artikel 60 registrierten Informationen können nur Marktüberwachungsbehörden und die Kommission zugreifen, es sei denn, der zukünftige Anbieter oder der Anbieter hat seine Zustimmung dafür erteilt, dass die Informationen auch öffentlich zugänglich sind.

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

[sn502] Anbieter
[sn908] EU-Datenbank
[sn503] Betreiber

(6) Die Kommission gilt als für die EU-Datenbank Verantwortlicher. Sie stellt Anbietern, zukünftigen Anbietern und Betreibern angemessene technische und administrative Unterstützung bereit. Die EU-Datenbank muss den geltenden Barrierefreiheitsanforderungen entsprechen.

KAPITEL IX

BEOBACHTUNG NACH DEM INVERKEHRBRINGEN, INFORMATIONSAUSTAUSCH UND MARKTÜBERWACHUNG

ABSCHNITT 1

Beobachtung nach dem Inverkehrbringen

Artikel 72

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 zur Art der KI-Technik und zu den Risiken des Hochrisiko-KI-Systems steht, einrichten und dokumentieren.

(2) Mit dem System zur Beobachtung nach dem Inverkehrbringen müssen sich die einschlägigen Daten zur Leistung der Hochrisiko-KI-Systeme, die von den Anbietern oder den Betreibern bereitgestellt oder aus anderen Quellen erhoben werden können, über ihre gesamte Lebensdauer hinweg aktiv und systematisch erheben, dokumentieren und analysieren lassen, und der Anbieter muss damit die fortdauernde Einhaltung der in Kapitel III Abschnitt 2 genannten Anforderungen an die KI-Systeme bewerten können. Gegebenenfalls umfasst die Beobachtung nach dem Inverkehrbringen eine Analyse der Interaktion mit anderen KI-Systemen. Diese Pflicht gilt nicht für sensible operative Daten von Betreibern, die Strafverfolgungsbehörden sind.

[sn508] Meldung schwerwiegender Vorfälle

(3) Das System zur Beobachtung nach dem Inverkehrbringen muss auf einem Plan für die Beobachtung nach dem Inverkehrbringen 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 detaillierte Bestimmungen für die Erstellung eines Musters des Plans für die Beobachtung nach dem Inverkehrbringen sowie die Liste der in den Plan aufzunehmenden Elemente bis zum 2. Februar 2026 detailliert festlegt. Dieser Durchführungsrechtsakt wird gemäß dem in Artikel 98 Absatz 2 genannten Prüfverfahren erlassen.

(4) Bei Hochrisiko-KI-Systemen, die unter die in Anhang I Abschnitt A aufgeführten Harmonisierungsrechtsvorschriften der Union fallen, und für die auf der Grundlage dieser Rechtvorschriften bereits ein System zur Beobachtung nach dem Inverkehrbringen sowie ein entsprechender Plan festgelegt wurden, haben die Anbieter zur Gewährleistung der Kohärenz, zur Vermeidung von Doppelarbeit und zur Minimierung zusätzlicher Belastungen die Möglichkeit, unter Verwendung des Musters nach Absatz 3, gegebenenfalls die in den Absätzen 1, 2 und 3 genannten erforderlichen Elemente in die im Rahmen dieser Vorschriften bereits vorhandenen Systeme und Pläne zu integrieren, sofern ein gleichwertiges Schutzniveau erreicht wird.

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

ABSCHNITT 2

Austausch von Informationen über schwerwiegende Vorfälle

Artikel 73

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.

[sn502] Anbieter

[sn503] Betreiber

(2) Die Meldung nach Absatz 1 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 oder gegebenenfalls der Betreiber Kenntnis von diesem schwerwiegenden Vorfall erlangt hat.

Bezüglich des in Unterabsatz 1 genannten Meldezeitraums wird der Schwere des schwerwiegenden Vorfalls Rechnung getragen.

(3) Ungeachtet des Absatzes 2 dieses Artikels erfolgt die in Absatz 1 dieses Artikels genannte Meldung im Falle eines weitverbreiteten Verstoßes oder eines schwerwiegenden Vorfalls im Sinne des Artikels 3 Nummer 49 Buchstabe b unverzüglich, spätestens jedoch zwei Tage nachdem der Anbieter oder gegebenenfalls der Betreiber von diesem Vorfall Kenntnis erlangt hat.

(4) Ungeachtet des Absatzes 2 erfolgt die Meldung im Falle des Todes einer Person unverzüglich nachdem der Anbieter oder der Betreiber einen kausalen Zusammenhang zwischen dem Hochrisiko-KI-System und dem schwerwiegenden Vorfall festgestellt hat, oder einen solchen vermutet, spätestens jedoch zehn Tage nach dem Datum, an dem der Anbieter oder gegebenenfalls der Betreiber von dem schwerwiegenden Vorfall Kenntnis erlangt hat.

[sn402] 2. August 2025

(5) Wenn es zur Gewährleistung der rechtzeitigen Meldung erforderlich ist, kann der Anbieter oder gegebenenfalls der Betreiber einen unvollständigen Erstbericht vorlegen, dem ein vollständiger Bericht folgt.

(6) Im Anschluss an die Meldung eines schwerwiegenden Vorfalls gemäß Absatz 1 führt der Anbieter unverzüglich die erforderlichen Untersuchungen im Zusammenhang mit dem schwerwiegenden Vorfall und dem betroffenen KI-System durch. Dies umfasst eine Risikobewertung des Vorfalls sowie Korrekturmaßnahmen.

Der Anbieter arbeitet bei den Untersuchungen gemäß Unterabsatz 1 mit den zuständigen Behörden und gegebenenfalls mit der betroffenen notifizierten Stelle zusammen und nimmt keine Untersuchung vor, die zu einer Veränderung des betroffenen KI-Systems in einer Weise führt, die möglicherweise Auswirkungen auf eine spätere Bewertung der Ursachen des Vorfalls hat, bevor er die zuständigen Behörden über eine solche Maßnahme nicht unterrichtet hat.

(7) Sobald die zuständige Marktüberwachungsbehörde eine Meldung über einen in Artikel 3 Nummer 49 Buchstabe c genannten schwerwiegenden Vorfall erhält, informiert sie die in Artikel 77 Absatz 1 genannten nationalen Behörden oder öffentlichen Stellen. Zur leichteren Einhaltung der Pflichten nach Absatz 1 dieses Artikels arbeitet die Kommission entsprechende Leitlinien aus. Diese Leitlinien werden bis zum 2. August 2025 veröffentlicht und regelmäßig bewertet.

(8) Die Marktüberwachungsbehörde ergreift innerhalb von sieben Tagen nach Eingang der in Absatz 1 dieses Artikels genannten Meldung geeignete Maßnahmen gemäß Artikel 19 der Verordnung (EU) 2019/1020 und befolgt die in der genannten Verordnung vorgesehenen Meldeverfahren.

(9) Bei Hochrisiko-KI-Systemen nach Anhang III, die von Anbietern in Verkehr gebracht oder in Betrieb genommen wurden, die Rechtsinstrumenten der Union mit gleichwertigen Meldepflichten wie jenen in dieser Verordnung festgesetzten unterliegen, müssen nur jene schwerwiegenden Vorfälle gemeldet werden, die in Artikel 3 Nummer 49 Buchstabe c genannt werden.

(10) Bei Hochrisiko-KI-Systemen, bei denen es sich um Sicherheitsbauteile von Produkten handelt, die unter die Verordnungen (EU) 2017/745 und (EU) 2017/746 fallen, oder die selbst solche Produkte sind, müssen nur die in Artikel 3 Nummer 49 Buchstabe c dieser Verordnung genannten schwerwiegenden Vorfälle gemeldet werden, und zwar der zuständigen nationalen Behörde, die für diesen Zweck von den Mitgliedstaaten, in denen der Vorfall stattgefunden hat, ausgewählt wurde.

(11) Die zuständigen nationalen Behörden melden der Kommission unverzüglich jeden schwerwiegenden Vorfall gemäß Artikel 20 der Verordnung (EU) 2019/1020, unabhängig davon, ob sie diesbezüglich Maßnahmen ergriffen haben.

ABSCHNITT 3

Durchsetzung

Artikel 74

Marktüberwachung und Kontrolle von KI-Systemen auf dem Unionsmarkt

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

a) Jede Bezugnahme auf einen Wirtschaftsakteur nach der Verordnung (EU) 2019/1020 gilt auch als Bezugnahme auf alle Akteure, die in Artikel 2 Absatz 1 der vorliegenden Verordnung genannt werden;

b) jede Bezugnahme auf ein Produkt nach der Verordnung (EU) 2019/1020 gilt auch als Bezugnahme auf alle KI-Systeme, die in den Anwendungsbereich der vorliegenden Verordnung fallen.

(2) Im Rahmen ihrer Berichtspflichten gemäß Artikel 34 Absatz 4 der Verordnung (EU) 2019/1020 melden die Marktüberwachungsbehörden der Kommission und den einschlägigen nationalen Wettbewerbsbehörden jährlich alle Informationen, die sie im Verlauf ihrer Marktüberwachungstätigkeiten erlangt haben und die für die Anwendung von Unionsrecht im Bereich der Wettbewerbsregeln von Interesse sein könnten. Ferner erstatten sie der Kommission jährlich Bericht über die Anwendung verbotener Praktiken in dem betreffenden Jahr und über die ergriffenen Maßnahmen.

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

Abweichend von Unterabsatz 1 und unter geeigneten Umständen können die Mitgliedstaaten eine andere einschlägige Behörde benennen, die die Funktion der Marktüberwachungsbehörde übernimmt, sofern sie die Koordinierung mit den einschlägigen sektorspezifischen Marktüberwachungsbehörden, die für die Durchsetzung der in Anhang I aufgeführten Harmonisierungsrechtsvorschriften der Union zuständig sind, sicherstellen.

(4) Die Verfahren gemäß den Artikeln 79 bis 83 der vorliegenden Verordnung gelten nicht für KI-Systeme, die im Zusammenhang mit Produkten stehen, auf die die in Anhang I Abschnitt A aufgeführten Harmonisierungsrechtsvorschriften der Union Anwendung finden, wenn in diesen Rechtsakten bereits Verfahren, die ein gleichwertiges Schutzniveau sicherstellen und dasselbe Ziel haben, vorgesehen sind. In diesen Fällen kommen stattdessen die einschlägigen sektorspezifischen Verfahren zur Anwendung.

(5) Unbeschadet der Befugnisse der Marktüberwachungsbehörden gemäß Artikel 14 der Verordnung (EU) 2019/1020 können die Marktüberwachungsbehörden für die Zwecke der Sicherstellung der wirksamen Durchsetzung der vorliegenden Verordnung die in Artikel 14 Absatz 4 Buchstaben d und j der genannten Verordnung genannten Befugnisse gegebenenfalls aus der Ferne ausüben.

(6) Bei Hochrisiko-KI-Systemen, die von auf der Grundlage des Unionsrechts im Bereich der Finanzdienstleistungen 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.

(7) Abweichend von Absatz 6 kann der Mitgliedstaat — unter geeigneten Umständen und wenn für Abstimmung gesorgt ist — eine andere einschlägige Behörde als Marktüberwachungsbehörde für die Zwecke dieser Verordnung benennen.

Nationale Marktüberwachungsbehörden, die unter die Richtlinie 2013/36/EU fallende Kreditinstitute, welche an dem mit der Verordnung (EU) Nr. 1024/2013 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.

(8) Für die in Anhang III Nummer 1 der vorliegenden Verordnung genannten Hochrisiko-KI-Systeme, sofern diese Systeme für Strafverfolgungszwecke, Grenzmanagement und Justiz und Demokratie eingesetzt werden, und für die in Anhang III Nummern 6, 7 und 8 genannten Hochrisiko-KI-Systeme benennen die Mitgliedstaaten für die Zwecke dieser Verordnung als Marktüberwachungsbehörden entweder die nach der Verordnung (EU) 2016/679 oder der Richtlinie (EU) 2016/680 für den Datenschutz zuständigen Aufsichtsbehörden oder jede andere gemäß denselben Bedingungen wie den in den Artikeln 41 bis 44 der Richtlinie (EU) 2016/680 festgelegten benannte Behörde. Marktüberwachungstätigkeiten dürfen in keiner Weise die Unabhängigkeit von Justizbehörden beeinträchtigen oder deren Handlungen im Rahmen ihrer justiziellen Tätigkeit anderweitig beeinflussen.

(9) 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 — ausgenommen für den Gerichtshof der Europäischen Union im Rahmen seiner Rechtsprechungstätigkeit.

(10) 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 I aufgeführten Harmonisierungsrechtsvorschriften der Union oder sonstigen Unionsrechts überwachen, das für die in Anhang III genannten Hochrisiko-KI-Systeme relevant sein könnte.

[sn901] Büro für Künstliche Intelligenz

[sn502] Anbieter

(11) Die Marktüberwachungsbehörden und die Kommission können gemeinsame Tätigkeiten, einschließlich gemeinsamer Untersuchungen, vorschlagen, die von den Marktüberwachungsbehörden oder von den Marktüberwachungsbehörden gemeinsam mit der Kommission durchgeführt werden, um Konformität zu fördern, Nichtkonformität festzustellen, zu sensibilisieren oder Orientierung zu dieser Verordnung und bestimmten Kategorien von Hochrisiko-KI-Systemen, bei denen festgestellt wird, dass sie in zwei oder mehr Mitgliedstaaten gemäß Artikel 9 der Verordnung (EU) 2019/1020 ein ernstes Risiko darstellen, zu geben. Das Büro für Künstliche Intelligenz unterstützt die Koordinierung der gemeinsamen Untersuchungen.

(12) Die Anbieter gewähren 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 von Hochrisiko-KI-Systemen verwendeten Trainings-, Validierungs- und Testdatensätzen, gegebenenfalls und unter Einhaltung von Sicherheitsvorkehrungen auch über die Anwendungsprogrammierschnittstellen (im Folgenden „API“) oder andere einschlägige technische Mittel und Instrumente, die den Fernzugriff ermöglichen.

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

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

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

(14) Jegliche Informationen oder Dokumentation, in deren Besitz die Marktüberwachungsbehörden gelangen, werden im Einklang mit den in Artikel 78 festgelegten Vertraulichkeitspflichten behandelt.

Artikel 75

Amtshilfe, Marktüberwachung und Kontrolle von KI-Systemen mit allgemeinem Verwendungszweck

(1) Beruht ein KI-System auf einem KI-Modell mit allgemeinem Verwendungszweck und werden das Modell und das System vom selben Anbieter entwickelt, so ist das Büro für Künstliche Intelligenz befugt, die Konformität des KI-Systems mit den Pflichten aus dieser Verordnung zu überwachen und beaufsichtigen. Zur Wahrnehmung seiner Beobachtungs- und Überwachungsaufgaben hat das Büro für Künstliche Intelligenz alle in diesem Abschnitt und in der Verordnung (EU) 2019/1020 vorgesehenen Befugnisse einer Marktüberwachungsbehörde.

(2) Haben die zuständigen Marktüberwachungsbehörden hinreichenden Grund für die Auffassung, dass KI-Systeme mit allgemeinem Verwendungszweck, die von Betreibern direkt für mindestens einen Zweck, der gemäß dieser Verordnung als hochriskant eingestuft ist, verwendet werden können, nicht mit den in dieser Verordnung festgelegten Anforderungen konform sind, so arbeiten sie bei der Durchführung von Konformitätsbewertungen mit dem Büro für Künstliche Intelligenz zusammen und unterrichten das KI-Gremium und andere Marktüberwachungsbehörden entsprechend.

(3) Ist eine Marktüberwachungsbehörde wegen der Unzugänglichkeit bestimmter Informationen im Zusammenhang mit dem KI-Modell mit allgemeinem Verwendungszweck nicht in der Lage, ihre Ermittlungen zu dem Hochrisiko-KI-System abzuschließen, obwohl sie alle angemessenen Anstrengungen unternommen hat, diese Informationen zu erhalten, kann sie ein begründetes Ersuchen an das Büro für Künstliche Intelligenz richten, durch das der Zugang zu den Informationen durchgesetzt werden kann. In diesem Fall übermittelt das Büro für Künstliche Intelligenz der ersuchenden Behörde unverzüglich, spätestens aber innerhalb von 30 Tagen, alle Informationen, die das Büro für Künstliche Intelligenz für die Feststellung, ob ein Hochrisiko-KI-System nicht konform ist, für erforderlich erachtet. Die Marktüberwachungsbehörden gewährleisten gemäß Artikel 78 der vorliegenden Verordnung die Vertraulichkeit der von ihnen erlangten Informationen. Das Verfahren nach Kapitel VI der Verordnung (EU) 2019/1020 gilt entsprechend.

Artikel 76

Beaufsichtigung von Tests unter Realbedingungen durch Marktüberwachungsbehörden

(1) Marktüberwachungsbehörden müssen über die Kompetenzen und Befugnisse verfügen, um sicherzustellen, dass Tests unter Realbedingungen gemäß dieser Verordnung erfolgen.

(2) Wenn ein Test unter Realbedingungen für KI-Systeme durchgeführt wird, die in einem KI-Reallabor gemäß Artikel 58 beaufsichtigt werden, überprüfen die Marktüberwachungsbehörden im Rahmen ihrer Aufsichtsaufgaben für das KI-Reallabor die Einhaltung des Artikels 60. Die Behörden können gegebenenfalls gestatten, dass der Anbieter oder zukünftige Anbieter den Test unter Realbedingungen in Abweichung von den in Artikel 60 Absatz 4 Buchstaben f und g festgelegten Bedingungen durchführt.

[sn503] Betreiber

(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 60 und 61 festgelegten Bedingungen nicht erfüllt sind, kann sie — je nachdem, was angemessen ist — in ihrem Hoheitsgebiet gegebenenfalls entscheiden, entweder

a) den Test unter Realbedingungen auszusetzen oder abzubrechen oder

b) den Anbieter oder zukünftigen Anbieter und die Betreiber oder zukünftigen Betreiber zur Änderung eines beliebigen Aspekts des Tests unter Realbedingungen zu verpflichten.

(4) Wenn eine Marktüberwachungsbehörde eine Entscheidung nach Absatz 3 des vorliegenden Artikels getroffen oder Einwände im Sinne des Artikels 60 Absatz 4 Buchstabe b erhoben hat, sind im Rahmen der Entscheidung oder der Einwände die Gründe dafür zu nennen sowie anzugeben, wie der Anbieter oder zukünftige Anbieter die Entscheidung oder die Einwände anfechten kann.

(5) Wenn eine Marktüberwachungsbehörde eine Entscheidung nach Absatz 3 getroffen hat, teilt sie ihre Gründe dafür gegebenenfalls den Marktüberwachungsbehörden anderer Mitgliedstaaten mit, in denen das KI-System gemäß dem Plan für den Test getestet wurde.

Artikel 77

Befugnisse der für den Schutz der Grundrechte zuständigen Behörden

(1) 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 genannten Hochrisiko-KI-Systeme beaufsichtigen oder durchsetzen, sind befugt, sämtliche auf der Grundlage dieser Verordnung in zugänglicher Sprache und Format erstellte oder geführte Dokumentation anzufordern und einzusehen, sofern der Zugang zu dieser Dokumentation für die wirksame Ausübung ihrer Aufträge im Rahmen ihrer Befugnisse innerhalb der Grenzen ihrer Hoheitsgewalt notwendig ist. Die jeweilige Behörde oder öffentliche Stelle informiert die Marktüberwachungsbehörde des betreffenden Mitgliedstaats von jeder diesbezüglichen Anfrage.

(2) Bis 2. November 2024 muss jeder Mitgliedstaat die in Absatz 1 genannten Behörden oder öffentlichen Stellen benennen und in einer öffentlichen Liste verfügbar machen. Die Mitgliedstaaten übermitteln die Liste der Kommission und den anderen Mitgliedstaaten und halten die Liste auf dem neuesten Stand.

(3) Sollte die in Absatz 1 genannte Dokumentation nicht ausreichen, um feststellen zu können, ob ein Verstoß gegen das Unionsrecht zum Schutz der Grundrechte vorliegt, so kann die in Absatz 1 genannte Behörde oder öffentliche Stelle bei der Marktüberwachungsbehörde einen begründeten Antrag auf Durchführung eines technischen 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.

(4) Jegliche Informationen oder Dokumentation, in deren Besitz die in Absatz 1 des vorliegenden Artikels genannten nationalen Behörden oder öffentlichen Stellen auf der Grundlage des vorliegenden Artikels gelangen, werden im Einklang mit den in Artikel 78 festgelegten Vertraulichkeitspflichten behandelt.

Artikel 78

Vertraulichkeit

(1) Die Kommission, die Marktüberwachungsbehörden und die notifizierten Stellen sowie alle anderen natürlichen oder juristischen Personen, die an der Anwendung dieser Verordnung beteiligt sind, wahren gemäß dem Unionsrecht oder dem nationalen Recht die Vertraulichkeit der Informationen und Daten, in deren Besitz sie bei der Ausführung ihrer Aufgaben und Tätigkeiten gelangen, sodass insbesondere Folgendes geschützt ist:

a) die Rechte des geistigen Eigentums sowie vertrauliche Geschäftsinformationen oder Geschäftsgeheimnisse natürlicher oder juristischer Personen, einschließlich Quellcodes, mit Ausnahme der in Artikel 5 der Richtlinie (EU) 2016/943 des Europäischen Parlaments und des Rates ([57]);

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

c) öffentliche und nationale Sicherheitsinteressen;

d) die Durchführung von Straf- oder Verwaltungsverfahren;

e) gemäß dem Unionsrecht oder dem nationalen Recht als Verschlusssache eingestufte Informationen.

(2) Die gemäß Absatz 1 an der Anwendung dieser Verordnung beteiligten Behörden fragen nur Daten an, die für die Bewertung des von KI-Systemen ausgehenden Risikos und für die Ausübung ihrer Befugnisse in Übereinstimmung mit dieser Verordnung und mit der Verordnung (EU) 2019/1020 unbedingt erforderlich sind. Sie ergreifen angemessene und wirksame Cybersicherheitsmaßnahmen zum Schutz der Sicherheit und Vertraulichkeit der erlangten Informationen und Daten und löschen im Einklang mit dem geltenden Unionsrecht oder nationalen Recht die erhobenen Daten, sobald sie für den Zweck, für den sie erlangt wurden, nicht mehr benötigt werden.

(3) Unbeschadet der Absätze 1 und 2 darf der Austausch vertraulicher Informationen zwischen den zuständigen nationalen Behörden untereinander oder zwischen den zuständigen nationalen Behörden und der Kommission nicht ohne vorherige Rücksprache mit der zuständigen nationalen Behörde, von der die Informationen stammen, und dem Betreiber offengelegt werden, sofern die in Anhang III Nummer 1, 6 oder 7 genannten Hochrisiko-KI-Systeme von Strafverfolgungs-, Grenzschutz-, Einwanderungs- oder Asylbehörden verwendet werden und eine solche Offenlegung die öffentlichen und nationalen Sicherheitsinteressen gefährden könnte. Dieser Informationsaustausch erstreckt sich nicht auf sensible operative Daten zu den Tätigkeiten von Strafverfolgungs-, Grenzschutz-, Einwanderungs- oder Asylbehörden.

Handeln Strafverfolgungs-, Einwanderungs- oder Asylbehörden als Anbieter von in Anhang III Nummer 1, 6 oder 7 genannten Hochrisiko-KI-Systemen, so verbleibt die technische Dokumentation nach Anhang IV in den Räumlichkeiten dieser Behörden. Diese Behörden sorgen dafür, dass die in Artikel 74 Absätze 8 und 9 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.

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

(5) Die Kommission und die Mitgliedstaaten können erforderlichenfalls und im Einklang mit den einschlägigen Bestimmungen internationaler Übereinkommen und Handelsabkommen mit Regulierungsbehörden von Drittstaaten, mit denen sie bilaterale oder multilaterale Vertraulichkeitsvereinbarungen getroffen haben und die ein angemessenes Niveau an Vertraulichkeit gewährleisten, vertrauliche Informationen austauschen.

Artikel 79

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

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

(2) Hat die Marktüberwachungsbehörde eines Mitgliedstaats hinreichend Grund zu der Annahme, dass ein KI-System ein Risiko nach Absatz 1 des vorliegenden Artikels birgt, so prüft sie das betreffende KI-System im Hinblick auf die Erfüllung aller in der vorliegenden Verordnung festgelegten Anforderungen und Pflichten. Besondere Aufmerksamkeit gilt KI-Systemen, die für schutzbedürftige Gruppen ein Risiko bergen. Wenn Risiken für die Grundrechte festgestellt werden, informiert die Marktüberwachungsbehörde auch die in Artikel 77 Absatz 1 genannten einschlägigen nationalen Behörden oder öffentlichen Stellen und arbeitet uneingeschränkt mit ihnen zusammen. Die betreffenden Akteure arbeiten erforderlichenfalls mit der Marktüberwachungsbehörde und den in Artikel 77 Absatz 1 genannten anderen Behörden oder öffentlichen Stellen zusammen.

([57]) Richtlinie (EU) 2016/943 des Europäischen Parlaments und des Rates vom 8. Juni 2016 über den Schutz vertraulichen Know-hows und vertraulicher Geschäftsinformationen (Geschäftsgeheimnisse) vor rechtswidrigem Erwerb sowie rechtswidriger Nutzung und Offenlegung (ABl. L 157 vom 15.6.2016, S. 1).

Stellt die Marktüberwachungsbehörde oder gegebenenfalls die Marktüberwachungsbehörde in Zusammenarbeit mit der in Artikel 77 Absatz 1 genannten nationalen Behörde im Verlauf dieser Prüfung fest, dass das KI-System die in dieser Verordnung festgelegten Anforderungen und Pflichten nicht erfüllt, fordert sie den jeweiligen Akteur unverzüglich auf, alle Korrekturmaßnahmen zu ergreifen, die geeignet sind, die Konformität des KI-Systems herzustellen, das KI-System vom Markt zu nehmen oder es innerhalb einer Frist, die die Marktüberwachungsbehörde vorgeben kann, in jedem Fall innerhalb von weniger als 15 Arbeitstagen, oder gemäß den einschlägigen Harmonisierungsrechtsvorschriften der Union zurückzurufen.

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

(3) Gelangt die Marktüberwachungsbehörde zu der Auffassung, dass die Nichtkonformität nicht auf ihr nationales Hoheitsgebiet beschränkt ist, so informiert 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 alle betreffenden KI-Systeme, die er auf dem Unionsmarkt bereitgestellt 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 oder Inbetriebnahme des KI-Systems auf ihrem nationalen Markt zu verbieten oder einzuschränken, das Produkt oder das eigenständige KI-System von diesem Markt zu nehmen oder es zurückzurufen. Diese Behörde notifiziert unverzüglich die Kommission und die anderen Mitgliedstaaten 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 und die Lieferkette, die Art der vermuteten Nichtkonformität und das sich daraus ergebende Risiko, die Art und Dauer der ergriffenen nationalen Maßnahmen und die von dem betreffenden Akteur vorgebrachten Argumente. Die 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;

b) Nichterfüllung der in Kapitel III Abschnitt 2 festgelegten Anforderungen durch ein Hochrisiko-KI-System;

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

d) Nichteinhaltung des Artikels 50.

(7) Die anderen Marktüberwachungsbehörden — mit Ausnahme der Marktüberwachungsbehörde des Mitgliedstaats, der das Verfahren eingeleitet hat — informieren unverzüglich die Kommission und die anderen Mitgliedstaaten über jegliche Maßnahmen und ihnen vorliegende zusätzlichen Informationen zur Nichtkonformität des betreffenden KI-Systems sowie — falls sie die ihnen mitgeteilte nationale Maßnahme ablehnen — über ihre Einwände.

(8) Erhebt weder eine Marktüberwachungsbehörde eines Mitgliedstaats noch die Kommission innerhalb von drei Monaten nach Eingang der in Absatz 5 des vorliegenden Artikels genannten Notifizierung Einwände gegen eine von einer Marktüberwachungsbehörde eines anderen Mitgliedstaats 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 Frist von drei Monaten gemäß dem vorliegenden Absatz wird bei Nichteinhaltung des Verbots der in Artikel 5 der vorliegenden Verordnung genannten KI-Praktiken auf 30 Tage verkürzt.

(9) Die Marktüberwachungsbehörden tragen dafür Sorge, dass geeignete einschränkende Maßnahmen in Bezug auf das betreffende Produkt oder KI-System ergriffen werden, beispielsweise die unverzügliche Rücknahme des Produkts oder KI-Systems von ihrem Markt.

Artikel 80

Verfahren für den Umgang mit KI-Systemen, die vom Anbieter gemäß Anhang III als nicht hochriskant eingestuft werden

(1) Hat eine Marktüberwachungsbehörde hinreichend Grund zu der Annahme, dass ein vom Anbieter als nicht hochriskant gemäß Artikel 6 Absatz 3 eingestuftes KI-System tatsächlich hochriskant ist, so prüft die Marktüberwachungsbehörde das betreffende KI-System im Hinblick auf seine Einstufung als Hochrisiko-KI-System auf der Grundlage der in Artikel 6 Absatz 3 festgelegten Bedingungen und den Leitlinien der Kommission.

[sn502] Anbieter

(2) Stellt die Marktüberwachungsbehörde im Verlauf dieser Prüfung fest, dass das betreffende KI-System hochriskant ist, fordert sie den jeweiligen Anbieter unverzüglich auf, alle erforderlichen Maßnahmen zu ergreifen, um die Konformität des KI-Systems mit den in dieser Verordnung festgelegten Anforderungen und Pflichten herzustellen, sowie innerhalb einer Frist, die die Marktüberwachungsbehörde vorgeben kann, geeignete Korrekturmaßnahmen zu ergreifen.

(3) Gelangt die Marktüberwachungsbehörde zu der Auffassung, dass die Verwendung des betreffenden KI-Systems nicht auf ihr nationales Hoheitsgebiet beschränkt ist, so informiert sie die Kommission und die anderen Mitgliedstaaten unverzüglich über die Ergebnisse der Prüfung und über die Maßnahmen, zu denen sie den Anbieter aufgefordert hat.

(4) Der Anbieter sorgt dafür, dass alle erforderlichen Maßnahmen ergriffen werden, um die Konformität des KI-Systems mit den in dieser Verordnung festgelegten Anforderungen und Pflichten herzustellen. Stellt der Anbieter eines betroffenen KI-Systems die Konformität des KI-Systems mit diesen Anforderungen und Pflichten nicht innerhalb der in Absatz 2 des vorliegenden Artikels genannten Frist her, so werden gegen den Anbieter Geldbußen gemäß Artikel 99 verhängt.

(5) Der Anbieter sorgt dafür, dass alle geeigneten Korrekturmaßnahmen in Bezug auf alle betreffenden KI-Systeme, die er auf dem Unionsmarkt bereitgestellt hat, getroffen werden.

[sn908] EU-Datenbank

(6) Ergreift der Anbieter des betreffenden KI-Systems innerhalb der in Absatz 2 des vorliegenden Artikels genannten Frist keine angemessenen Korrekturmaßnahmen, so findet Artikel 79 Absätze 5 bis 9 Anwendung.

(7) Stellt die Marktüberwachungsbehörde im Verlauf der Prüfung gemäß Absatz 1 des vorliegenden Artikels fest, dass das KI-System vom Anbieter fälschlich als nicht hochriskant eingestuft wurde, um die Geltung der Anforderungen von Kapitel III Abschnitt 2 zu umgehen, so werden gegen den Anbieter Geldbußen gemäß Artikel 99 verhängt.

[se004] gilt für

(8) Bei der Ausübung ihrer Befugnis zur Überwachung der Anwendung dieses Artikels können die Marktüberwachungsbehörden im Einklang mit Artikel 11 der Verordnung (EU) 2019/1020 geeignete Überprüfungen durchführen, wobei sie insbesondere Informationen berücksichtigen, die in der EU-Datenbank gemäß Artikel 71 der vorliegenden Verordnung gespeichert sind.

Artikel 81

Schutzklauselverfahren der Union

(1) Erhebt eine Marktüberwachungsbehörde eines Mitgliedstaats innerhalb von drei Monaten nach Eingang der in Artikel 79 Absatz 5 genannten Notifizierung — oder bei Nichteinhaltung des Verbots der in Artikel 5 genannten KI-Praktiken innerhalb von 30 Tagen — Einwände gegen eine von der Marktüberwachungsbehörde eines anderen Mitgliedstaats getroffene Maßnahme oder ist die Kommission der Ansicht, dass die Maßnahme mit dem Unionsrecht unvereinbar ist, so nimmt die Kommission unverzüglich Konsultationen mit der Marktüberwachungsbehörde des betreffenden Mitgliedstaats und dem Akteur bzw. den Akteuren auf und prüft die nationale Maßnahme. Anhand der Ergebnisse dieser Prüfung entscheidet die Kommission innerhalb von sechs Monaten — oder bei Nichteinhaltung des Verbots der in Artikel 5 genannten KI-Praktiken innerhalb von 60 Tagen — ab dem Eingang der in Artikel 79 Absatz 5 genannten Notifizierung, ob die nationale Maßnahme gerechtfertigt ist, und teilt der Marktüberwachungsbehörde des betreffenden Mitgliedstaats ihre Entscheidung mit. Die Kommission unterrichtet auch alle übrigen Marktüberwachungsbehörden über ihre Entscheidung.

(2) Ist die Kommission der Ansicht, dass die von dem betreffenden Mitgliedstaat ergriffene Maßnahme gerechtfertigt ist, so tragen alle Mitgliedstaaten dafür Sorge, dass sie geeignete einschränkende Maßnahmen in Bezug auf das betreffende KI-System ergreifen, etwa die Anordnung der unverzüglichen Rücknahme des KI-Systems von ihrem Markt, und informiert die Kommission darüber. Erachtet die Kommission die nationale Maßnahme als nicht gerechtfertigt, nimmt der betreffende Mitgliedstaat die Maßnahme zurück und informiert die Kommission darüber.

(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 82

Konforme KI-Systeme, die ein Risiko bergen

(1) Stellt die Marktüberwachungsbehörde eines Mitgliedstaats — nach einer Konsultation der in Artikel 77 Absatz 1 genannten betreffenden nationalen Behörde — nach der gemäß Artikel 79 durchgeführten Prüfung fest, dass ein Hochrisiko-KI-System zwar dieser Verordnung entspricht, aber dennoch ein Risiko für die Gesundheit oder Sicherheit von Personen, für die Grundrechte oder für andere Aspekte des Schutzes öffentlicher Interessen darstellt, so fordert sie unverzüglich 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, und zwar innerhalb einer Frist, die sie vorgeben kann.

(2) Der Anbieter oder der andere einschlägige Akteur sorgt dafür, dass in Bezug auf alle betroffenen KI-Systeme, die er auf dem Unionsmarkt bereitgestellt hat, innerhalb der Frist, die von der in Absatz 1 genannten Marktüberwachungsbehörde des Mitgliedstaats vorgegeben wurde, Korrekturmaßnahmen ergriffen werden.

(3) Die Mitgliedstaaten unterrichten unverzüglich die Kommission und die anderen Mitgliedstaaten über Feststellungen gemäß Absatz 1. 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.

[sn509] CE-Kennzeichnung

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

[sn908] EU-Datenbank

[sn707] Bevollmächtigter

[sn303] Technische Dokumentation

(5) Die Kommission teilt ihren Beschluss unverzüglich den betroffenen Mitgliedstaaten und den jeweiligen Akteuren mit. Sie unterrichtet auch die übrigen Mitgliedstaaten.

Artikel 83

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 vorgeben kann, zu beheben:

a) die CE-Kennzeichnung wurde unter Verstoß gegen Artikel 48 angebracht;

b) es wurde keine CE-Kennzeichnung angebracht;

c) es wurde keine EU-Konformitätserklärung gemäß Artikel 47 ausgestellt;

d) es wurde keine EU-Konformitätserklärung gemäß Artikel 47 ordnungsgemäß ausgestellt;

e) es wurde keine Registrierung in der EU-Datenbank gemäß Artikel 71 vorgenommen;

f) es wurde kein Bevollmächtigter — sofern erforderlich — ernannt;

g) es ist keine technische Dokumentation verfügbar.

(2) Besteht die Nichtkonformität nach Absatz 1 weiter, so ergreift die Marktüberwachungsbehörde des betreffenden Mitgliedstaats geeignete und verhältnismäßige Maßnahmen, um die Bereitstellung des Hochrisiko-KI-Systems auf dem Markt zu beschränken oder zu verbieten oder um dafür zu sorgen, dass es unverzüglich zurückgerufen oder vom Markt genommen wird.

Artikel 84

Unionsstrukturen zur Unterstützung der Prüfung von KI

(1) Die Kommission benennt eine oder mehrere Unionsstrukturen zur Unterstützung der Prüfung von KI, die die Aufgaben gemäß Artikel 21 Absatz 6 der Verordnung (EU) 2019/1020 im KI-Bereich wahrnehmen.

(2) Unbeschadet der in Absatz 1 genannten Aufgaben leisten die Unionsstrukturen zur Unterstützung der Prüfung von KI auf Anfrage des KI-Gremiums, der Kommission oder der Marktüberwachungsbehörden auch unabhängige technische oder wissenschaftliche Beratung.

[sn805] Recht auf Erklärung

[sn806] Hinweisgeberschutz

[sn807] Beschwerderecht

ABSCHNITT 4

Rechtsbehelfe

Artikel 85

Recht auf Beschwerde bei einer Marktüberwachungsbehörde

[sn503] Betreiber

Unbeschadet anderer verwaltungsrechtlicher oder gerichtlicher Rechtsbehelfe kann jede natürliche oder juristische Person, die Grund zu der Annahme hat, dass gegen die Bestimmungen dieser Verordnung verstoßen wurde, bei der betreffenden Marktüberwachungsbehörde Beschwerden einreichen.

Gemäß der Verordnung (EU) 2019/1020 werden solche Beschwerden für die Zwecke der Durchführung von Marktüberwachungstätigkeiten berücksichtigt und nach den einschlägigen von den Marktüberwachungsbehörden dafür eingerichteten Verfahren behandelt.

Artikel 86

Recht auf Erläuterung der Entscheidungsfindung im Einzelfall

(1) Personen, die von einer Entscheidung betroffen sind, die der Betreiber auf der Grundlage der Ausgaben eines in Anhang III aufgeführten Hochrisiko-KI-Systems, mit Ausnahme der in Nummer 2 des genannten Anhangs aufgeführten Systeme, getroffen hat und die rechtliche Auswirkungen hat oder sie in ähnlicher Art erheblich auf eine Weise beeinträchtigt, die ihrer Ansicht nach ihre Gesundheit, ihre Sicherheit oder ihre Grundrechte beeinträchtigt, haben das Recht, vom Betreiber eine klare und aussagekräftige Erläuterung zur Rolle des KI-Systems im Entscheidungsprozess und zu den wichtigsten Elementen der getroffenen Entscheidung zu erhalten.

[sn901] Büro für Künstliche Intelligenz

(2) Absatz 1 gilt nicht für die Verwendung von KI-Systemen, bei denen sich Ausnahmen von oder Beschränkungen der Pflicht nach dem genannten Absatz aus dem Unionsrecht oder dem nationalen Recht im Einklang mit dem Unionsrecht ergeben.

(3) Dieser Artikel gilt nur insoweit, als das Recht gemäß Absatz 1 nicht anderweitig im Unionsrecht festgelegt ist.

Artikel 87

Meldung von Verstößen und Schutz von Hinweisgebern

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

ABSCHNITT 5

Aufsicht, Ermittlung, Durchsetzung und Überwachung in Bezug auf Anbieter von KI-Modellen mit allgemeinem Verwendungszweck

Artikel 88

Durchsetzung der Pflichten der Anbieter von KI-Modellen mit allgemeinem Verwendungszweck

(1) Die Kommission verfügt unter Berücksichtigung der Verfahrensgarantien nach Artikel 94 über ausschließliche Befugnisse zur Beaufsichtigung und Durchsetzung von Kapitel V. Unbeschadet der Organisationsbefugnisse der Kommission und der Aufteilung der Zuständigkeiten zwischen den Mitgliedstaaten und der Union auf der Grundlage der Verträge überträgt die Kommission dem Büro für Künstliche Intelligenz die Durchführung dieser Aufgaben.

(2) Unbeschadet des Artikels 75 Absatz 3 können die Marktüberwachungsbehörden die Kommission ersuchen, die in diesem Abschnitt festgelegten Befugnisse auszuüben, wenn es erforderlich und verhältnismäßig ist, um die Wahrnehmung ihrer Aufgaben gemäß dieser Verordnung zu unterstützen.

[sn901] Büro für Künstliche Intelligenz
[sn502] Anbieter

Artikel 89

Überwachungsmaßnahmen

(1) Zur Wahrnehmung der ihr in diesem Abschnitt übertragenen Aufgaben kann das Büro für Künstliche Intelligenz die erforderlichen Maßnahmen ergreifen, um die wirksame Umsetzung und Einhaltung dieser Verordnung durch Anbieter von KI-Modellen mit allgemeinem Verwendungszweck, einschließlich der Einhaltung genehmigter Praxisleitfäden, zu überwachen.

(2) Nachgelagerte Anbieter haben das Recht, eine Beschwerde wegen eines Verstoßes gegen diese Verordnung einzureichen. Eine Beschwerde ist hinreichend zu begründen und enthält mindestens Folgendes:

a) die Kontaktstelle des Anbieters des betreffenden KI-Modells mit allgemeinem Verwendungszweck;

b) eine Beschreibung der einschlägigen Fakten, die betreffenden Bestimmungen dieser Verordnung und die Begründung, warum der nachgelagerte Anbieter der Auffassung ist, dass der Anbieter des KI-Modells mit allgemeinem Verwendungszweck gegen diese Verordnung verstoßen hat;

c) alle sonstigen Informationen, die der nachgelagerte Anbieter, der die Anfrage übermittelt hat, für relevant hält, gegebenenfalls einschließlich Informationen, die er auf eigene Initiative hin zusammengetragen hat.

Artikel 90

Warnungen des wissenschaftlichen Gremiums vor systemischen Risiken

(1) Das wissenschaftliche Gremium kann dem Büro für Künstliche Intelligenz eine qualifizierte Warnung übermitteln, wenn es Grund zu der Annahme hat, dass

a) ein KI-Modell mit allgemeinem Verwendungszweck ein konkretes, identifizierbares Risiko auf Unionsebene birgt oder

b) ein KI-Modell mit allgemeinem Verwendungszweck die Bedingungen gemäß Artikel 51 erfüllt.

(2) Aufgrund einer solchen qualifizierten Warnung kann die Kommission über das Büro für Künstliche Intelligenz und nach Unterrichtung des KI-Gremiums die in diesem Abschnitt festgelegten Befugnisse zur Beurteilung der Angelegenheit ausüben. Das Büro für Künstliche Intelligenz unterrichtet das KI-Gremium über jede Maßnahme gemäß den Artikeln 91 bis 94.

(3) Eine qualifizierte Warnung ist hinreichend zu begründen und enthält mindestens Folgendes:

a) die Kontaktstelle des Anbieters des betreffenden KI-Modells mit allgemeinem Verwendungszweck mit systemischem Risiko;

b) eine Beschreibung der einschlägigen Fakten und der Gründe für die Warnung durch das wissenschaftliche Gremium;

c) alle sonstigen Informationen, die das wissenschaftliche Gremium für relevant hält, gegebenenfalls einschließlich Informationen, die es auf eigene Initiative hin zusammengetragen hat.

Artikel 91

Befugnis zur Anforderung von Dokumentation und Informationen

(1) Die Kommission kann den Anbieter des betreffenden KI-Modells mit allgemeinem Verwendungszweck auffordern, die vom Anbieter gemäß den Artikeln 53 und 55 erstellte Dokumentation oder alle zusätzlichen Informationen vorzulegen, die erforderlich sind, um die Einhaltung dieser Verordnung durch den Anbieter zu beurteilen.

(2) Vor der Übermittlung des Informationsersuchens kann das Büro für Künstliche Intelligenz einen strukturierten Dialog mit dem Anbieter des KI-Modells mit allgemeinem Verwendungszweck einleiten.

(3) Auf hinreichend begründeten Antrag des wissenschaftlichen Gremiums kann die Kommission ein Informationsersuchen an einen Anbieter eines KI-Modells mit allgemeinem Verwendungszweck richten, wenn der Zugang zu Informationen für die Wahrnehmung der Aufgaben des wissenschaftlichen Gremiums gemäß Artikel 68 Absatz 2 erforderlich und verhältnismäßig ist.

[sn502] Anbieter

(4) In dem Auskunftsersuchen sind die Rechtsgrundlage und der Zweck des Ersuchens zu nennen, anzugeben, welche Informationen benötigt werden, eine Frist für die Übermittlung der Informationen zu setzen, und die Geldbußen für die Erteilung unrichtiger, unvollständiger oder irreführender Informationen gemäß Artikel 101 anzugeben.

(5) Der Anbieter des betreffenden KI-Modells mit allgemeinem Verwendungszweck oder sein Vertreter stellt die angeforderten Informationen bereit. Im Falle juristischer Personen, Gesellschaften oder — wenn der Anbieter keine Rechtspersönlichkeit besitzt — die Personen, die nach Gesetz oder Satzung zur Vertretung dieser Personen befugt sind, stellen die angeforderten Informationen im Namen des Anbieters des betreffenden KI-Modells mit allgemeinem Verwendungszweck zur Verfügung. Ordnungsgemäß bevollmächtigte Rechtsanwälte können Informationen im Namen ihrer Mandanten erteilen. Die Mandanten bleiben jedoch in vollem Umfang dafür verantwortlich, dass die erteilten Auskünfte vollständig, sachlich richtig oder nicht irreführend sind.

[sn901] Büro für Künstliche Intelligenz

Artikel 92

Befugnis zur Durchführung von Bewertungen

(1) Das Büro für Künstliche Intelligenz kann nach Konsultation des KI-Gremiums Bewertungen des betreffenden KI-Modells mit allgemeinem Verwendungszweck durchführen, um

a) die Einhaltung der Pflichten aus dieser Verordnung durch den Anbieter zu beurteilen, wenn die gemäß Artikel 91 eingeholten Informationen unzureichend sind, oder

b) systemische Risiken auf Unionsebene von KI-Modellen mit allgemeinem Verwendungszweck mit systemischem Risiko zu ermitteln, insbesondere im Anschluss an eine qualifizierte Warnung des wissenschaftlichen Gremiums gemäß Artikel 90 Absatz 1 Buchstabe a.

(2) Die Kommission kann beschließen, unabhängige Sachverständige zu benennen, die in ihrem Namen Bewertungen durchführen, einschließlich aus dem gemäß Artikel 68 eingesetzten wissenschaftlichen Gremium. Die für diese Aufgabe benannten unabhängigen Sachverständigen erfüllen die in Artikel 68 Absatz 2 umrissenen Kriterien.

(3) Für die Zwecke des Absatzes 1 kann die Kommission über API oder weitere geeignete technische Mittel und Instrumente, einschließlich Quellcode, Zugang zu dem betreffenden KI-Modell mit allgemeinem Verwendungszweck anfordern.

(4) In der Anforderung des Zugangs sind die Rechtsgrundlage, der Zweck und die Gründe für die Anforderung zu nennen und die Frist für die Bereitstellung des Zugangs zu setzen und die Geldbußen gemäß Artikel 101 für den Fall, dass der Zugang nicht bereitgestellt wird, anzugeben.

(5) Die Anbieter des betreffenden KI-Modells mit allgemeinem Verwendungszweck oder seine Vertreter stellen die angeforderten Informationen zur Verfügung. Im Falle juristischer Personen, Gesellschaften oder — wenn der Anbieter keine Rechtspersönlichkeit besitzt — die Personen, die nach Gesetz oder ihrer Satzung zur Vertretung dieser Personen befugt sind, stellen den angeforderten Zugang im Namen des Anbieters des betreffenden KI-Modells mit allgemeinem Verwendungszweck zur Verfügung.

(6) Die Kommission erlässt Durchführungsrechtsakte, in denen die detaillierten Regelungen und Voraussetzungen für die Bewertungen, einschließlich der detaillierten Regelungen für die Einbeziehung unabhängiger Sachverständiger, und das Verfahren für deren Auswahl festgelegt werden. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 98 Absatz 2 genannten Prüfverfahren erlassen.

(7) Bevor es den Zugang zu dem betreffenden KI-Modell mit allgemeinem Verwendungszweck anfordert, kann das Büro für Künstliche Intelligenz einen strukturierten Dialog mit dem Anbieter des KI-Modells mit allgemeinem Verwendungszweck einleiten, um mehr Informationen über die interne Erprobung des Modells, interne Vorkehrungen zur Vermeidung systemischer Risiken und andere interne Verfahren und Maßnahmen, die der Anbieter zur Minderung dieser Risiken ergriffen hat, einzuholen.

Artikel 93

Befugnis zur Aufforderung zu Maßnahmen

(1) Soweit erforderlich und angemessen, kann die Kommission die Anbieter auffordern,

a) geeignete Maßnahmen zu ergreifen, um die Verpflichtungen gemäß den Artikeln 53 und 54 einzuhalten;

[sn804] Freiwillige Verhaltenskodizes

[sn901] Büro für Künstliche Intelligenz

[sn502] Anbieter

b) Risikominderungsmaßnahmen durchzuführen, wenn die gemäß Artikel 92 durchgeführte Bewertung zu ernsthaften und begründeten Bedenken hinsichtlich eines systemischen Risikos auf Unionsebene geführt hat;

c) die Bereitstellung des Modells auf dem Markt einzuschränken, es zurückzunehmen oder zurückzurufen.

(2) Vor der Aufforderung zu einer Maßnahme kann das Büro für Künstliche Intelligenz einen strukturierten Dialog mit dem Anbieter des KI-Modells mit allgemeinem Verwendungszweck einleiten.

(3) Wenn der Anbieter des KI-Modells mit allgemeinem Verwendungszweck im Rahmen des strukturierten Dialogs gemäß Absatz 2 Verpflichtungszusagen zur Durchführung von Risikominderungsmaßnahmen, um einem systemischen Risiko auf Unionsebene zu begegnen, anbietet, kann die Kommission diese Verpflichtungszusagen durch einen Beschluss für bindend erklären und feststellen, dass es keinen weiteren Anlass zum Handeln gibt.

Artikel 94

Verfahrensrechte der Wirtschaftsakteure des KI-Modells mit allgemeinem Verwendungszweck

Unbeschadet der in dieser Verordnung enthaltenen spezifischeren Verfahrensrechte gilt für die Anbieter des KI-Modells mit allgemeinem Verwendungszweck Artikel 18 der Verordnung (EU) 2019/1020 sinngemäß.

KAPITEL X

VERHALTENSKODIZES UND LEITLINIEN

Artikel 95

Verhaltenskodizes für die freiwillige Anwendung bestimmter Anforderungen

(1) Das Büro für Künstliche Intelligenz und die Mitgliedstaaten fördern und erleichtern die Aufstellung von Verhaltenskodizes, einschließlich damit zusammenhängender Governance-Mechanismen, mit denen die freiwillige Anwendung einiger oder aller der in Kapitel III Abschnitt 2 genannten Anforderungen auf KI-Systeme, die kein hohes Risiko bergen, gefördert werden soll, wobei den verfügbaren technischen Lösungen und bewährten Verfahren der Branche, die die Anwendung dieser Anforderungen ermöglichen, Rechnung zu tragen ist.

(2) Das Büro für Künstliche Intelligenz und die Mitgliedstaaten erleichtern die Aufstellung von Verhaltenskodizes in Bezug auf die freiwillige Anwendung spezifischer Anforderungen auf alle KI-Systeme, einschließlich durch Betreiber, auf der Grundlage klarer Zielsetzungen sowie wesentlicher Leistungsindikatoren zur Messung der Erfüllung dieser Zielsetzungen, einschließlich unter anderem folgender Elemente:

a) in den Ethik-Leitlinien der Union für eine vertrauenswürdige KI enthaltene anwendbare Elemente;

b) Beurteilung und Minimierung der Auswirkungen von KI-Systemen auf die ökologische Nachhaltigkeit, einschließlich im Hinblick auf energieeffizientes Programmieren, und Techniken, um KI effizient zu gestalten, zu trainieren und zu nutzen;

c) Förderung der KI-Kompetenz, insbesondere der von Personen, die mit der Entwicklung, dem Betrieb und der Nutzung von KI befasst sind;

d) Erleichterung einer inklusiven und vielfältigen Gestaltung von KI-Systemen, unter anderem durch die Einsetzung inklusiver und vielfältiger Entwicklungsteams und die Förderung der Beteiligung der Interessenträger an diesem Prozess;

e) Bewertung und Verhinderung der negativen Auswirkungen von KI-Systemen auf schutzbedürftige Personen oder Gruppen schutzbedürftiger Personen, einschließlich im Hinblick auf die Barrierefreiheit für Personen mit Behinderungen, sowie auf die Gleichstellung der Geschlechter.

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

(4) Das Büro für Künstliche Intelligenz und die Mitgliedstaaten berücksichtigen die besonderen Interessen und Bedürfnisse von KMU, einschließlich Startups, bei der Förderung und Erleichterung der Aufstellung von Verhaltenskodizes.

Artikel 96

Leitlinien der Kommission zur Durchführung dieser Verordnung

(1) Die Kommission erarbeitet Leitlinien für die praktische Umsetzung dieser Verordnung, die sich insbesondere auf Folgendes beziehen:

a) die Anwendung der in den Artikeln 8 bis 15 und in Artikel 25 genannten Anforderungen und Pflichten;

b) die in Artikel 5 genannten verbotenen Praktiken;

c) die praktische Durchführung der Bestimmungen über wesentliche Veränderungen;

d) die praktische Umsetzung der Transparenzpflichten gemäß Artikel 50;

e) detaillierte Informationen über das Verhältnis dieser Verordnung zu den in Anhang I aufgeführten Harmonisierungsrechtsvorschriften der Union sowie zu anderen einschlägigen Rechtsvorschriften der Union, auch in Bezug auf deren kohärente Durchsetzung;

f) die Anwendung der Definition eines KI-Systems gemäß Artikel 3 Nummer 1.

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

Die Leitlinien gemäß Unterabsatz 1 dieses Absatzes tragen dem allgemein anerkannten Stand der Technik im Bereich KI sowie den einschlägigen harmonisierten Normen und gemeinsamen Spezifikationen, auf die in den Artikeln 40 und 41 Bezug genommen wird, oder den harmonisierten Normen oder technischen Spezifikationen, die gemäß den Harmonisierungsrechtsvorschriften der Union festgelegt wurden, gebührend Rechnung.

(2) Auf Ersuchen der Mitgliedstaaten oder des Büros für Künstliche Intelligenz oder von sich aus aktualisiert die Kommission früher verabschiedete Leitlinien, wenn es als notwendig erachtet wird.

KAPITEL XI

BEFUGNISÜBERTRAGUNG UND AUSSCHUSSVERFAHREN

Artikel 97

Ausübung der Befugnisübertragung

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

(2) Die in Artikel 6 Absätze 6 und 7, Artikel 7 Absätze 1 und 3, Artikel 11 Absatz 3, Artikel 43 Absätze 5 und 6, Artikel 47 Absatz 5, Artikel 51 Absatz 3, Artikel 52 Absatz 4 sowie Artikel 53 Absätze 5 und 6 genannte Befugnis zum Erlass delegierter Rechtsakte wird der Kommission für einen Zeitraum von fünf Jahren ab 1. August 2024 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 Befugnisübertragung gemäß Artikel 6 Absätze 6 und 7, Artikel 7 Absätze 1 und 3, Artikel 11 Absatz 3, Artikel 43 Absätze 5 und 6, Artikel 47 Absatz 5, Artikel 51 Absatz 3, Artikel 52 Absatz 4 sowie Artikel 53 Absätze 5 und 6 kann vom Europäischen Parlament oder vom Rat jederzeit widerrufen werden. Der Beschluss über den Widerruf beendet die Übertragung der in jenem 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) Vor dem Erlass eines delegierten Rechtsakts konsultiert die Kommission die von den einzelnen Mitgliedstaaten benannten Sachverständigen im Einklang mit den in der Interinstitutionellen Vereinbarung vom 13. April 2016 über bessere Rechtsetzung niedergelegten Grundsätzen.

[sn905] Sanktion: Betreiberpflichten

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

(6) Ein delegierter Rechtsakt, der nach Artikel 6 Absatz 6 oder 7, Artikel 7 Absatz 1 oder 3, Artikel 11 Absatz 3, Artikel 43 Absatz 5 oder 6, Artikel 47 Absatz 5, Artikel 51 Absatz 3, Artikel 52 Absatz 4 sowie Artikel 53 Absatz 5 oder 6 erlassen wurde, tritt nur in Kraft, wenn weder das Europäische Parlament noch der Rat innerhalb einer Frist von drei Monaten nach Übermittlung jenes 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 98

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, so gilt Artikel 5 der Verordnung (EU) Nr. 182/2011.

KAPITEL XII

SANKTIONEN

[sn502] Anbieter

Artikel 99

Sanktionen

[sn503] Betreiber

(1) Entsprechend den Vorgaben dieser Verordnung erlassen die Mitgliedstaaten Vorschriften für Sanktionen und andere Durchsetzungsmaßnahmen, zu denen auch Verwarnungen und nichtmonetäre Maßnahmen gehören können, die bei Verstößen gegen diese Verordnung durch Akteure Anwendung finden, und ergreifen alle Maßnahmen, die für deren ordnungsgemäße und wirksame Durchsetzung notwendig sind, wobei die von der Kommission gemäß Artikel 96 erteilten Leitlinien zu berücksichtigen sind. Die vorgesehenen Sanktionen müssen wirksam, verhältnismäßig und abschreckend sein. Sie berücksichtigen die Interessen von KMU, einschließlich Start-up-Unternehmen, sowie deren wirtschaftliches Überleben.

(2) Die Mitgliedstaaten teilen der Kommission die Vorschriften für Sanktionen und andere Durchsetzungsmaßnahmen gemäß Absatz 1 unverzüglich und spätestens zum Zeitpunkt ihres Inkrafttretens mit und melden ihr unverzüglich etwaige spätere Änderungen.

(3) Bei Missachtung des Verbots der in Artikel 5 genannten KI-Praktiken werden Geldbußen von bis zu 35 000 000 EUR oder — im Falle von Unternehmen — von bis zu 7 % des gesamten weltweiten Jahresumsatzes des vorangegangenen Geschäftsjahres verhängt, je nachdem, welcher Betrag höher ist.

(4) Für Verstöße gegen folgende für Akteure oder notifizierte Stellen geltende Bestimmungen, mit Ausnahme der in Artikel 5 genannten, werden Geldbußen von bis zu 15 000 000 EUR oder — im Falle von Unternehmen — von bis zu 3 % des gesamten weltweiten Jahresumsatzes des vorangegangenen Geschäftsjahres verhängt, je nachdem, welcher Betrag höher ist:

a) Pflichten der Anbieter gemäß Artikel 16;

b) Pflichten der Bevollmächtigten gemäß Artikel 22;

c) Pflichten der Einführer gemäß Artikel 23;

d) Pflichten der Händler gemäß Artikel 24;

e) Pflichten der Betreiber gemäß Artikel 26;

f) für notifizierte Stellen geltende Anforderungen und Pflichten gemäß Artikel 31, Artikel 33 Absätze 1, 3 und 4 bzw. Artikel 34;

g) Transparenzpflichten für Anbieter und Betreiber gemäß Artikel 50.

(5) Werden notifizierten Stellen oder zuständigen nationalen Behörden auf deren Auskunftsersuchen hin falsche, unvollständige oder irreführende Informationen bereitgestellt, so werden Geldbußen von bis zu 7 500 000 EUR oder — im Falle von Unternehmen — von bis zu 1 % des gesamten weltweiten Jahresumsatzes des vorangegangenen Geschäftsjahres verhängt, je nachdem, welcher Betrag höher ist.

(6) Im Falle von KMU, einschließlich Start-up-Unternehmen, gilt für jede in diesem Artikel genannte Geldbuße der jeweils niedrigere Betrag aus den in den Absätzen 3, 4 und 5 genannten Prozentsätzen oder Summen.

(7) Bei der Entscheidung, ob eine Geldbuße verhängt wird, und bei der Festsetzung der Höhe der Geldbuße werden in jedem Einzelfall alle relevanten Umstände der konkreten Situation sowie gegebenenfalls Folgendes berücksichtigt:

a) Art, Schwere und Dauer des Verstoßes und seiner Folgen, unter Berücksichtigung des Zwecks des KI-Systems sowie gegebenenfalls der Zahl der betroffenen Personen und des Ausmaßes des von ihnen erlittenen Schadens;

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

c) 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 diese Verordnung darstellt;

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

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

f) Grad der Zusammenarbeit mit den zuständigen nationalen Behörden, um den Verstoß abzustellen und die möglichen nachteiligen Auswirkungen des Verstoßes abzumildern;

g) Grad an Verantwortung des Akteurs unter Berücksichtigung der von ihm ergriffenen technischen und organisatorischen Maßnahmen;

h) Art und Weise, wie der Verstoß den zuständigen nationalen Behörden bekannt wurde, insbesondere ob und gegebenenfalls in welchem Umfang der Akteur den Verstoß gemeldet hat;

i) Vorsätzlichkeit oder Fahrlässigkeit des Verstoßes;

j) alle Maßnahmen, die der Akteur ergriffen hat, um den Schaden, der den betroffenen Personen zugefügt wird, zu mindern.

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

(9) In Abhängigkeit vom Rechtssystem der Mitgliedstaaten 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.

(10) Die Ausübung der Befugnisse gemäß diesem Artikel muss angemessenen Verfahrensgarantien gemäß dem Unionsrecht und dem nationalen Recht, einschließlich wirksamer gerichtlicher Rechtsbehelfe und ordnungsgemäßer Verfahren, unterliegen.

(11) Die Mitgliedstaaten erstatten der Kommission jährlich Bericht über die Geldbußen, die sie in dem betreffenden Jahr gemäß diesem Artikel verhängt haben, und über damit zusammenhängende Rechtsstreitigkeiten oder Gerichtsverfahren.

Artikel 100

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 Höhe der Geldbuße werden in jedem Einzelfall alle relevanten Umstände der konkreten Situation sowie Folgendes gebührend berücksichtigt:

[sn907] GPAI-Modell-Geldbußen

a) Art, Schwere und Dauer des Verstoßes und dessen Folgen, unter Berücksichtigung des Zwecks des betreffenden KI-Systems sowie gegebenenfalls der Zahl der betroffenen Personen und des Ausmaßes des von ihnen erlittenen Schadens;

b) Grad der Verantwortung des Organs, der Einrichtung oder der sonstigen Stelle der Union unter Berücksichtigung der von diesem bzw. dieser ergriffenen technischen und organisatorischen Maßnahmen;

c) alle Maßnahmen, die das Organ, die Einrichtung oder die sonstige Stelle der Union zur Minderung des von den betroffenen Personen erlittenen Schadens ergriffen hat;

d) das Maß der 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;

e) ähnliche frühere Verstöße des Organs, der Einrichtung oder der sonstigen Stelle der Union;

f) Art und Weise, wie der Verstoß dem Europäischen Datenschutzbeauftragten bekannt wurde, insbesondere ob und gegebenenfalls in welchem Umfang das Organ, die Einrichtung oder die sonstige Stelle der Union den Verstoß gemeldet hat;

g) der Jahreshaushalt 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 1 500 000 EUR verhängt.

[sn502] Anbieter

(3) Bei Nichtkonformität des KI-Systems mit in dieser Verordnung festgelegten Anforderungen oder Pflichten, mit Ausnahme der in Artikel 5 festgelegten, werden Geldbußen von bis zu 750 000 EUR verhängt.

(4) Bevor der Europäische Datenschutzbeauftragte Entscheidungen nach dem vorliegenden Artikel trifft, gibt er dem Organ, der Einrichtung oder der sonstigen Stelle der Union, gegen das bzw. 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 die betroffenen Parteien Anspruch auf Einsicht in die Unterlagen des Europäischen Datenschutzbeauftragten.

(6) Das Aufkommen aus den nach diesem Artikel verhängten Geldbußen trägt zum Gesamthaushalt der Union bei. Die Geldbußen dürfen nicht den wirksamen Betrieb des Organs, der Einrichtung oder der sonstigen Stelle der Union beeinträchtigen, dem bzw. der die Geldbuße auferlegt wurde.

(7) Der Europäische Datenschutzbeauftragte macht der Kommission jährlich Mitteilung über die Geldbußen, die er nach Maßgabe dieses Artikels verhängt hat, und über die von ihm eingeleiteten Rechtsstreitigkeiten oder Gerichtsverfahren.

Artikel 101

Geldbußen für Anbieter von KI-Modellen mit allgemeinem Verwendungszweck

(1) Die Kommission kann gegen Anbieter von KI-Modellen mit allgemeinem Verwendungszweck Geldbußen von bis zu 3 % ihres gesamten weltweiten Jahresumsatzes im vorangegangenen Geschäftsjahr oder 15 000 000 EUR verhängen, je nachdem, welcher Betrag höher ist, wenn sie feststellt, dass der Anbieter vorsätzlich oder fahrlässig

a) gegen die einschlägigen Bestimmungen dieser Verordnung verstoßen hat;

b) der Anforderung eines Dokuments oder von Informationen gemäß Artikel 91 nicht nachgekommen ist oder falsche, unvollständige oder irreführende Informationen bereitgestellt hat;

c) einer gemäß Artikel 93 geforderten Maßnahme nicht nachgekommen ist;

d) der Kommission keinen Zugang zu dem KI-Modell mit allgemeinem Verwendungszweck oder dem KI-Modell mit allgemeinem Verwendungszweck mit systemischem Risiko gewährt hat, um eine Bewertung gemäß Artikel 92 durchzuführen.

Bei der Festsetzung der Höhe der Geldbuße oder des Zwangsgelds wird der Art, der Schwere und der Dauer des Verstoßes sowie den Grundsätzen der Verhältnismäßigkeit und der Angemessenheit gebührend Rechnung getragen. Die Kommission berücksichtigt außerdem Verpflichtungen, die gemäß Artikel 93 Absatz 3 oder in den einschlägigen Praxisleitfäden nach Artikel 56 gemacht wurden.

(2) Vor der Annahme einer Entscheidung nach Absatz 1 teilt die Kommission dem Anbieter des KI-Modells mit allgemeinem Verwendungszweck ihre vorläufige Beurteilung mit und gibt ihm Gelegenheit, Stellung zu nehmen.

(3) Die gemäß diesem Artikel verhängten Geldbußen müssen wirksam, verhältnismäßig und abschreckend sein.

(4) Informationen über gemäß diesem Artikel verhängte Geldbußen werden gegebenenfalls dem KI-Gremium mitgeteilt.

(5) Der Gerichtshof der Europäischen Union hat die unbeschränkte Befugnis zur Überprüfung der Entscheidungen der Kommission über die Festsetzung einer Geldbuße gemäß diesem Artikel. Er kann die verhängte Geldbuße aufheben, herabsetzen oder erhöhen.

(6) Die Kommission erlässt Durchführungsrechtsakte mit detaillierten Regelungen und Verfahrensgarantien für die Verfahren im Hinblick auf den möglichen Erlass von Beschlüssen gemäß Absatz 1 dieses Artikels. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 98 Absatz 2 genannten Prüfverfahren erlassen.

KAPITEL XIII

SCHLUSSBESTIMMUNGEN

Artikel 102

Änderung der Verordnung (EG) 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) 2024/1689 des Europäischen Parlaments und des Rates (*) zum Einsatz kommen, werden die in Kapitel III Abschnitt 2 jener Verordnung festgelegten Anforderungen berücksichtigt.

(*) Verordnung (EU) 2024/1689 des Europäischen Parlaments und des Rates vom 13. Juni 2024 zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz und zur Änderung der Verordnungen (EG) Nr. 300/2008, (EU) Nr. 167/2013, (EU) Nr. 168/2013, (EU) 2018/858, (EU) 2018/1139 und (EU) 2019/2144 sowie der Richtlinien 2014/90/EU, (EU) 2016/797 und (EU) 2020/1828 (Verordnung über künstliche Intelligenz) (ABl. L, 2024/1689, 12.7.2024, ELI: http://data.europa.eu/eli/reg/2024/1689/oj).“

Artikel 103

Änderung der Verordnung (EU) Nr. 167/2013

In Artikel 17 Absatz 5 der Verordnung (EU) 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 Sicherheitsbauteile im Sinne der Verordnung (EU) 2024/1689 des Europäischen Parlaments und des Rates (*) handelt, werden die in Kapitel III Abschnitt 2 jener Verordnung festgelegten Anforderungen berücksichtigt.

(*) Verordnung (EU) 2024/1689 des Europäischen Parlaments und des Rates vom 13. Juni 2024 zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz und zur Änderung der Verordnungen (EG) Nr. 300/2008, (EU) Nr. 167/2013, (EU) Nr. 168/2013, (EU) 2018/858, (EU) 2018/1139 und (EU) 2019/2144 sowie der Richtlinien 2014/90/EU, (EU) 2016/797 und (EU) 2020/1828 (Verordnung über künstliche Intelligenz) (ABl. L, 2024/1689, 12.7.2024, ELI: http://data.europa.eu/eli/reg/2024/1689/oj).“

Artikel 104

Änderung der Verordnung (EU) Nr. 168/2013

In Artikel 22 Absatz 5 der Verordnung (EU) 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 Sicherheitsbauteile im Sinne der Verordnung (EU) 2024/1689 des Europäischen Parlaments und des Rates (*) handelt, werden die in Kapitel III Abschnitt 2 jener Verordnung festgelegten Anforderungen berücksichtigt.

(*) Verordnung (EU) 2024/1689 des Europäischen Parlaments und des Rates vom 13. Juni 2024 zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz und zur Änderung der Verordnungen (EG) Nr. 300/2008, (EU) Nr. 167/2013, (EU) Nr. 168/2013, (EU) 2018/858, (EU) 2018/1139 und (EU) 2019/2144 sowie der Richtlinien 2014/90/EU, (EU) 2016/797 und (EU) 2020/1828 (Verordnung über künstliche Intelligenz) (ABl. L, 2024/1689, 12.7.2024, ELI: http://data.europa.eu/eli/reg/2024/1689/oj).“

Artikel 105

Änderung der Richtlinie 2014/90/EU

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

„(5) Bei Systemen der künstlichen Intelligenz, bei denen es sich um Sicherheitsbauteile im Sinne der Verordnung (EU) 2024/1689 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 Kapitel III Abschnitt 2 jener Verordnung festgelegten Anforderungen.

(*) Verordnung (EU) 2024/1689 des Europäischen Parlaments und des Rates vom 13. Juni 2024 zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz und zur Änderung der Verordnungen (EG) Nr. 300/2008, (EU) Nr. 167/2013, (EU) Nr. 168/2013, (EU) 2018/858, (EU) 2018/1139 und (EU) 2019/2144 sowie der Richtlinien 2014/90/EU, (EU) 2016/797 und (EU) 2020/1828 (Verordnung über künstliche Intelligenz) (ABl. L, 2024/1689, 12.7.2024, ELI: http://data.europa.eu/eli/reg/2024/1689/oj).“

Artikel 106

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 Absatz 1 und von Durchführungsrechtsakten nach Absatz 11, die sich auf Systeme der künstlichen Intelligenz beziehen, bei denen es sich um Sicherheitsbauteile im Sinne der Verordnung (EU) 2024/1689 des Europäischen Parlaments und des Rates (*) handelt, werden die in Kapitel III Abschnitt 2 jener Verordnung festgelegten Anforderungen berücksichtigt.

(*) Verordnung (EU) 2024/1689 des Europäischen Parlaments und des Rates vom 13. Juni 2024 zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz und zur Änderung der Verordnungen (EG) Nr. 300/2008, (EU) Nr. 167/2013, (EU) Nr. 168/2013, (EU) 2018/858, (EU) 2018/1139 und (EU) 2019/2144 sowie der Richtlinien 2014/90/EU, (EU) 2016/797 und (EU) 2020/1828 (Verordnung über künstliche Intelligenz) (ABl. L, 2024/1689, 12.7.2024, ELI: http://data.europa.eu/eli/reg/2024/1689/oj).“

Artikel 107

Änderung der Verordnung (EU) 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 Sicherheitsbauteile im Sinne der Verordnung (EU) 2024/1689 des Europäischen Parlaments und des Rates (*) handelt, werden die in Kapitel III Abschnitt 2 jener Verordnung festgelegten Anforderungen berücksichtigt.

(*) Verordnung (EU) 2024/1689 des Europäischen Parlaments und des Rates vom 13. Juni 2024 zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz und zur Änderung der Verordnungen (EG) Nr. 300/2008, (EU) Nr. 167/2013, (EU) Nr. 168/2013, (EU) 2018/858, (EU) 2018/1139 und (EU) 2019/2144 sowie der Richtlinien 2014/90/EU, (EU) 2016/797 und (EU) 2020/1828 (Verordnung über künstliche Intelligenz) (ABl. L, 2024/1689, 12.7.2024, ELI: http://data.europa.eu/eli/reg/2024/1689/oj).“

Artikel 108

Änderungen der Verordnung (EU) 2018/1139

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

1. In Artikel 17 wird folgender Absatz angefügt:

„(3) Unbeschadet des Absatzes 2 werden beim Erlass von Durchführungsrechtsakten nach Absatz 1, die sich auf Systeme der künstlichen Intelligenz beziehen, bei denen es sich um Sicherheitsbauteile im Sinne der Verordnung (EU) 2024/1689 des Europäischen Parlaments und des Rates (*) handelt, die in Kapitel III Abschnitt 2 jener Verordnung festgelegten Anforderungen berücksichtigt.

(*) Verordnung (EU) 2024/1689 des Europäischen Parlaments und des Rates vom 13. Juni 2024 zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz und zur Änderung der Verordnungen (EG) Nr. 300/2008, (EU) Nr. 167/2013, (EU) Nr. 168/2013, (EU) 2018/858, (EU) 2018/1139 und (EU) 2019/2144 sowie der Richtlinien 2014/90/EU, (EU) 2016/797 und (EU) 2020/1828 (Verordnung über künstliche Intelligenz) (ABl. L, 2024/1689, 12.7.2024, ELI: http://data.europa.eu/eli/reg/2024/1689/oj).“

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 Sicherheitsbauteile im Sinne der Verordnung (EU) 2024/1689 handelt, werden die in Kapitel III Abschnitt 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 Sicherheitsbauteile im Sinne der Verordnung (EU) 2024/1689 handelt, werden die in Kapitel III Abschnitt 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 Sicherheitsbauteile im Sinne der Verordnung (EU) 2024/1689 handelt, werden die in Kapitel III Abschnitt 2 jener Verordnung festgelegten Anforderungen berücksichtigt.“

5. In Artikel 57 wird folgender Unterabsatz angefügt:

„Beim Erlass solcher Durchführungsrechtsakte, die sich auf Systeme der künstlichen Intelligenz beziehen, bei denen es sich um Sicherheitsbauteile im Sinne der Verordnung (EU) 2024/1689 handelt, werden die in Kapitel III Abschnitt 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 Sicherheitsbauteile im Sinne der Verordnung (EU) 2024/1689 handelt, werden die in Kapitel III Abschnitt 2 jener Verordnung festgelegten Anforderungen berücksichtigt."

Artikel 109

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 Sicherheitsbauteile im Sinne der Verordnung (EU) 2024/1689 des Europäischen Parlaments und des Rates (*) handelt, werden die in Kapitel III Abschnitt 2 jener Verordnung festgelegten Anforderungen berücksichtigt.

(*) Verordnung (EU) 2024/1689 des Europäischen Parlaments und des Rates vom 13. Juni 2024 zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz und zur Änderung der Verordnungen (EG) Nr. 300/2008, (EU) Nr. 167/2013, (EU) Nr. 168/2013, (EU) 2018/858, (EU) 2018/1139 und (EU) 2019/2144 sowie der Richtlinien 2014/90/EU, (EU) 2016/797 und (EU) 2020/1828 (Verordnung über künstliche Intelligenz) (ABl. L, 2024/1689, 12.7.2024, ELI: http://data.europa.eu/eli/reg/2024/1689/oj)."

[sn404] 2. August 2027

Artikel 110

Änderung der Richtlinie (EU) 2020/1828

[sn503] Betreiber

In Anhang I der Richtlinie (EU) 2020/1828 des Europäischen Parlaments und des Rates ([58]) wird die folgende Nummer angefügt:

[sn403] 2. August 2026

[sn502] Anbieter

[sn402] 2. August 2025

„68. Verordnung (EU) 2024/1689 des Europäischen Parlaments und des Rates vom 13. Juni 2024 zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz und zur Änderung der Verordnungen (EG) Nr. 300/2008, (EU) Nr. 167/2013, (EU) Nr. 168/2013, (EU) 2018/858, (EU) 2018/1139 und (EU) 2019/2144 sowie der Richtlinien 2014/90/EU, (EU) 2016/797 und (EU) 2020/1828 (Verordnung über künstliche Intelligenz) (ABl. L, 2024/1689, 12.7.2024, ELI: http://data.europa.eu/eli/reg/2024/1689/oj)."

Artikel 111

Bereits in Verkehr gebrachte oder in Betrieb genommene KI-Systeme und bereits in Verkehr gebrachte KI-Modelle mit allgemeinem Verwendungszweck

(1) Unbeschadet der Anwendung des Artikels 5 gemäß Artikel 113 Absatz 3 Buchstabe a werden KI-Systeme, bei denen es sich um Komponenten von IT-Großsystemen handelt, die mit den in Anhang X aufgeführten Rechtsakten eingerichtet wurden und vor dem 2. August 2027 in Verkehr gebracht oder in Betrieb genommen wurden, bis zum 31. Dezember 2030 mit dieser Verordnung in Einklang gebracht.

Die in dieser Verordnung festgelegten Anforderungen werden bei der Bewertung jedes IT-Großsystems, das mit den in Anhang X aufgeführten Rechtsakten eingerichtet wurde, berücksichtigt, wobei die Bewertung entsprechend den Vorgaben der jeweiligen Rechtsakte und bei Ersetzung oder Änderung dieser Rechtsakte erfolgt.

(2) Unbeschadet der Anwendung des Artikels 5 gemäß Artikel 113 Absatz 3 Buchstabe a gilt diese Verordnung für Betreiber von Hochrisiko-KI-Systemen — mit Ausnahme der in Absatz 1 des vorliegenden Artikels genannten Systeme —, die vor dem 2. August 2026 in Verkehr gebracht oder in Betrieb genommen wurden, nur dann, wenn diese Systeme danach in ihrer Konzeption erheblich verändert wurden. In jedem Fall treffen die Anbieter und Betreiber von Hochrisiko-KI-Systemen, die bestimmungsgemäß von Behörden verwendet werden sollen, die erforderlichen Maßnahmen für die Erfüllung der Anforderungen und Pflichten dieser Verordnung bis zum 2. August 2030.

(3) Anbieter von KI-Modellen mit allgemeinem Verwendungszweck, die vor dem 2. August 2025 in Verkehr gebracht wurden, treffen die erforderlichen Maßnahmen für die Erfüllung der in dieser Verordnung festgelegten Pflichten bis zum 2. August 2027.

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

Artikel 112

Bewertung und Überprüfung

(1) Die Kommission prüft nach Inkrafttreten dieser Verordnung und bis zum Ende der Befugnisübertragung gemäß Artikel 97 einmal jährlich, ob eine Änderung der Liste in Anhang III und der Liste der verbotenen Praktiken im KI-Bereich gemäß Artikel 5 erforderlich ist. Die Kommission übermittelt die Ergebnisse dieser Bewertung dem Europäischen Parlament und dem Rat.

(2) Bis zum 2. August 2028 und danach alle vier Jahre bewertet die Kommission Folgendes und erstattet dem Europäischen Parlament und dem Rat Bericht darüber:

a) Notwendigkeit von Änderungen zur Erweiterung bestehender Bereiche oder zur Aufnahme neuer Bereiche in Anhang III:

b) Änderungen der Liste der KI-Systeme, die zusätzliche Transparenzmaßnahmen erfordern, in Artikel 50;

c) Änderungen zur Verbesserung der Wirksamkeit des Überwachungs- und Governance-Systems.

(3) Bis zum 2. August 2029 und danach alle vier Jahre legt die Kommission dem Europäischen Parlament und dem Rat einen Bericht über die Bewertung und Überprüfung dieser Verordnung vor. Der Bericht enthält eine Beurteilung hinsichtlich der Durchsetzungsstruktur und der etwaigen Notwendigkeit einer Agentur der Union zur Lösung der festgestellten Mängel. Auf der Grundlage der Ergebnisse wird diesem Bericht gegebenenfalls ein Vorschlag zur Änderung dieser Verordnung beigefügt. Die Berichte werden veröffentlicht.

[sn901] Büro für Künstliche Intelligenz

(4) In den in Absatz 2 genannten Berichten wird insbesondere auf folgende Aspekte eingegangen:

a) Sachstand bezüglich der finanziellen, technischen und personellen Ressourcen der zuständigen nationalen Behörden im Hinblick auf deren Fähigkeit, die ihnen auf der Grundlage dieser Verordnung übertragenen Aufgaben wirksam zu erfüllen;

b) Stand der Sanktionen, insbesondere der Bußgelder nach Artikel 99 Absatz 1, die Mitgliedstaaten bei Verstößen gegen diese Verordnung verhängt haben;

c) angenommene harmonisierte Normen und gemeinsame Spezifikationen, die zur Unterstützung dieser Verordnung erarbeitet wurden;

d) Zahl der Unternehmen, die nach Inkrafttreten dieser Verordnung in den Markt eintreten, und wie viele davon KMU sind.

(5) Bis zum 2. August 2028 bewertet die Kommission die Arbeitsweise des Büros für Künstliche Intelligenz und prüft, ob das Büro für Künstliche Intelligenz mit ausreichenden Befugnissen und Zuständigkeiten zur Erfüllung seiner Aufgaben ausgestattet wurde, und ob es für die ordnungsgemäße Durchführung und Durchsetzung dieser Verordnung zweckmäßig und erforderlich wäre, das Büro für Künstliche Intelligenz und seine Durchsetzungskompetenzen zu erweitern und seine Ressourcen aufzustocken. Die Kommission übermittelt dem Europäischen Parlament und dem Rat einen Bericht über ihre Bewertung.

(6) Bis zum 2. August 2028 und danach alle vier Jahre legt die Kommission einen Bericht über die Überprüfung der Fortschritte bei der Entwicklung von Normungsdokumenten zur energieeffizienten Entwicklung von KI-Modellen mit allgemeinem Verwendungszweck vor und beurteilt die Notwendigkeit weiterer Maßnahmen oder Handlungen, einschließlich verbindlicher Maßnahmen oder Handlungen. Dieser Bericht wird dem Europäischen Parlament und dem Rat vorgelegt und veröffentlicht.

(7) Bis zum 2. August 2028 und danach alle drei Jahre führt die Kommission eine Bewertung der Folgen und der Wirksamkeit der freiwilligen Verhaltenskodizes durch, mit denen die Anwendung der in Kapitel III Abschnitt 2 festgelegten Anforderungen an andere KI-Systeme als Hochrisiko-KI-Systeme und möglicherweise auch zusätzlicher Anforderungen an andere KI-Systeme als Hochrisiko-KI-Systeme, auch in Bezug auf deren ökologische Nachhaltigkeit, gefördert werden soll.

(8) Für die Zwecke der Absätze 1 bis 7 übermitteln das KI-Gremium, die Mitgliedstaaten und die zuständigen nationalen Behörden der Kommission auf Anfrage unverzüglich die gewünschten Informationen.

(9) Bei den in den Absätzen 1 bis 7 genannten Bewertungen und Überprüfungen berücksichtigt die Kommission die Standpunkte und Feststellungen des KI-Gremiums, des Europäischen Parlaments, des Rates und anderer einschlägiger Stellen oder Quellen.

[sn400] Durchsetzungszeitplan

[sn901] Büro für Künstliche Intelligenz

(10) Die Kommission legt erforderlichenfalls geeignete Vorschläge zur Änderung dieser Verordnung vor und berücksichtigt dabei insbesondere technologische Entwicklungen, die Auswirkungen von KI-Systemen auf die Gesundheit und Sicherheit und auf die Grundrechte und die Fortschritte in der Informationsgesellschaft.

(11) Als Orientierung für die in den Absätzen 1 bis 7 genannten Bewertungen und Überprüfungen entwickelt das Büro für Künstliche Intelligenz ein Ziel und eine partizipative Methode für die Bewertung der Risikoniveaus anhand der in den jeweiligen Artikeln genannten Kriterien und für die Einbeziehung neuer Systeme in

a) die Liste gemäß Anhang III, einschließlich der Erweiterung bestehender Bereiche oder der Aufnahme neuer Bereiche in diesen Anhang;

b) die Liste der verbotenen Praktiken gemäß Artikel 5; und

[sn403] 2. August 2026

c) die Liste der KI-Systeme, die zusätzliche Transparenzmaßnahmen erfordern, in Artikel 50.

[sn401] 2. Februar 2025

(12) Eine Änderung dieser Verordnung im Sinne des Absatzes 10 oder entsprechende delegierte Rechtsakte oder Durchführungsrechtsakte, die sektorspezifische Rechtsvorschriften für eine unionsweite Harmonisierung gemäß Anhang I Abschnitt B betreffen, berücksichtigen die regulatorischen Besonderheiten des jeweiligen Sektors und die in der Verordnung festgelegten bestehenden Governance-, Konformitätsbewertungs- und Durchsetzungsmechanismen und -behörden.

[sn402] 2. August 2025

[sn404] 2. August 2027

(13) Bis zum 2. August 2031 nimmt die Kommission unter Berücksichtigung der ersten Jahre der Anwendung der Verordnung eine Bewertung der Durchsetzung dieser Verordnung vor und erstattet dem Europäischen Parlament, dem Rat und dem Europäischen Wirtschafts- und Sozialausschuss darüber Bericht. Auf Grundlage der Ergebnisse wird dem Bericht gegebenenfalls ein Vorschlag zur Änderung dieser Verordnung beigefügt, der die Struktur der Durchsetzung und die Notwendigkeit einer Agentur der Union für die Lösung festgestellter Mängel betrifft.

Artikel 113

Inkrafttreten und Geltungsbeginn

Diese Verordnung tritt am zwanzigsten Tag nach ihrer Veröffentlichung im *Amtsblatt der Europäischen Union* in Kraft.

Sie gilt ab dem 2. August 2026.

Jedoch:

a) Die Kapitel I und II gelten ab dem 2. Februar 2025;

b) Kapitel III Abschnitt 4, Kapitel V, Kapitel VII und Kapitel XII sowie Artikel 78 gelten ab dem 2. August 2025, mit Ausnahme des Artikels 101;

c) Artikel 6 Absatz 1 und die entsprechenden Pflichten gemäß dieser Verordnung gelten ab dem 2. August 2027.

Diese Verordnung ist in allen ihren Teilen verbindlich und gilt unmittelbar in jedem Mitgliedstaat.

Geschehen zu Brüssel am 13. Juni 2024.

Im Namen des Europäischen Parlaments	*Im Namen des Rates*
Die Präsidentin	*Der Präsident*
R. METSOLA	M. MICHEL

ANHANG I

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)

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 anderer Harmonisierungsrechtsvorschriften der Union

13. 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)

14. 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)

15. 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)

16. 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)

17. 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)

18. 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)

19. 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)

20. 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 II

Liste der Straftaten gemäß Artikel 5 Absatz 1 Unterabsatz 1 Buchstabe h Ziffer iii

Straftaten gemäß Artikel 5 Absatz 1 Unterabsatz 1 Buchstabe h Ziffer iii:

— Terrorismus,

— Menschenhandel,

— sexuelle Ausbeutung von Kindern und Kinderpornografie,

— illegaler Handel mit Drogen oder psychotropen Stoffen,

— illegaler Handel mit Waffen, Munition oder Sprengstoffen,

— Mord, schwere Körperverletzung,

— illegaler Handel mit menschlichen Organen oder menschlichem Gewebe,

— illegaler Handel mit nuklearen oder radioaktiven Substanzen,

— Entführung, Freiheitsberaubung oder Geiselnahme,

— Verbrechen, die in die Zuständigkeit des Internationalen Strafgerichtshofs fallen,

— Flugzeug- oder Schiffsentführung,

— Vergewaltigung,

— Umweltkriminalität,

— organisierter oder bewaffneter Raub,

— Sabotage,

— Beteiligung an einer kriminellen Vereinigung, die an einer oder mehreren der oben genannten Straftaten beteiligt ist.

[sn203] Bildung und Berufsausbildung
[sn204] Beschäftigung und Arbeitskräfteverwaltung
[sn205] Wesentliche Dienste
[sn201] Biometrie
[sn202] Kritische Infrastruktur

ANHANG III

Hochrisiko-KI-Systeme gemäß Artikel 6 Absatz 2

Als Hochrisiko-KI-Systeme gemäß Artikel 6 Absatz 2 gelten die in folgenden Bereichen aufgeführten KI-Systeme:

1. Biometrie, soweit ihr Einsatz nach einschlägigem Unionsrecht oder nationalem Recht zugelassen ist:

   a) biometrische Fernidentifizierungssysteme.

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

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

   c) KI-Systeme, die bestimmungsgemäß zur Emotionserkennung verwendet werden sollen.

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

3. Allgemeine und berufliche Bildung

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

   b) KI-Systeme, die bestimmungsgemäß für die Bewertung von Lernergebnissen verwendet werden sollen, einschließlich des Falles, dass diese Ergebnisse dazu dienen, den Lernprozess natürlicher Personen in Einrichtungen oder Programmen aller Ebenen der allgemeinen und beruflichen Bildung zu steuern;

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

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

4. Beschäftigung, Personalmanagement und Zugang zur Selbstständigkeit

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

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

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

   a) KI-Systeme, die bestimmungsgemäß von Behörden oder im Namen von Behörden verwendet werden sollen, um zu beurteilen, ob natürliche Personen Anspruch auf grundlegende öffentliche Unterstützungsleistungen und -dienste, einschließlich Gesundheitsdiensten, haben und ob solche Leistungen und Dienste zu gewähren, einzuschränken, zu widerrufen oder zurückzufordern sind;

   b) KI-Systeme, die bestimmungsgemäß für die Kreditwürdigkeitsprüfung und Bonitätsbewertung natürlicher Personen verwendet werden sollen, mit Ausnahme von KI-Systemen, die zur Aufdeckung von Finanzbetrug verwendet werden;

   c) KI-Systeme, die bestimmungsgemäß für die Risikobewertung und Preisbildung in Bezug auf natürliche Personen im Fall von Lebens- und Krankenversicherungen verwendet werden sollen;

[sn206] Strafverfolgung

d) KI-Systeme, die bestimmungsgemäß zur Bewertung und Klassifizierung von Notrufen von natürlichen Personen oder für die Entsendung oder Priorisierung des Einsatzes von Not- und Rettungsdiensten, einschließlich Polizei, Feuerwehr und medizinischer Nothilfe, sowie für Systeme für die Triage von Patienten bei der Notfallversorgung verwendet werden sollen.

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

a) KI-Systeme, die bestimmungsgemäß von Strafverfolgungsbehörden oder in deren Namen oder von Organen, Einrichtungen und sonstigen Stellen der Union zur Unterstützung von Strafverfolgungsbehörden oder in deren Namen zur Bewertung des Risikos einer natürlichen Person, zum Opfer von Straftaten zu werden, verwendet werden sollen;

b) KI-Systeme, die bestimmungsgemäß von Strafverfolgungsbehörden oder in deren Namen oder von Organen, Einrichtungen und sonstigen Stellen der Union zur Unterstützung von Strafverfolgungsbehörden als Lügendetektoren oder ähnliche Instrumente verwendet werden sollen;

c) KI-Systeme, die bestimmungsgemäß von Strafverfolgungsbehörden oder in deren Namen oder von Organen, Einrichtungen und sonstigen Stellen der Union zur Unterstützung von Strafverfolgungsbehörden zur Bewertung der Verlässlichkeit von Beweismitteln im Zuge der Ermittlung oder Verfolgung von Straftaten verwendet werden sollen;

[sn207] Migration, Asyl und Grenzkontrolle

d) KI-Systeme, die bestimmungsgemäß von Strafverfolgungsbehörden oder in deren Namen oder von Organen, Einrichtungen und sonstigen Stellen der Union zur Unterstützung von Strafverfolgungsbehörden zur Bewertung des Risikos, dass eine natürliche Person eine Straftat begeht oder erneut begeht, nicht nur auf der Grundlage der Erstellung von Profilen natürlicher Personen gemäß Artikel 3 Absatz 4 der Richtlinie (EU) 2016/680 oder zur Bewertung persönlicher Merkmale und Eigenschaften oder vergangenen kriminellen Verhaltens von natürlichen Personen oder Gruppen verwendet werden sollen;

e) KI-Systeme, die bestimmungsgemäß von Strafverfolgungsbehörden oder in deren Namen oder von Organen, Einrichtungen und sonstigen Stellen der Union zur Unterstützung von Strafverfolgungsbehörden zur Erstellung von Profilen natürlicher Personen gemäß Artikel 3 Absatz 4 der Richtlinie (EU) 2016/680 im Zuge der Aufdeckung, Ermittlung oder Verfolgung von Straftaten verwendet werden sollen.

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

a) KI-Systeme, die bestimmungsgemäß von zuständigen Behörden oder in deren Namen oder Organen, Einrichtungen und sonstigen Stellen der Union als Lügendetektoren verwendet werden sollen oder ähnliche Instrumente;

b) KI-Systeme, die bestimmungsgemäß von zuständigen Behörden oder in deren Namen oder von Organen, Einrichtungen und sonstigen Stellen der Union zur Bewertung eines Risikos verwendet werden sollen, einschließlich eines Sicherheitsrisikos, eines Risikos der irregulären Einwanderung oder eines Gesundheitsrisikos, das von einer natürlichen Person ausgeht, die in das Hoheitsgebiet eines Mitgliedstaats einzureisen beabsichtigt oder eingereist ist;

c) KI-Systeme, die bestimmungsgemäß von zuständigen Behörden oder in deren Namen oder von Organen, Einrichtungen und sonstigen Stellen der Union verwendet werden sollen, um zuständige Behörden bei der Prüfung von Asyl- und Visumanträgen sowie Aufenthaltstiteln und damit verbundenen Beschwerden im Hinblick auf die Feststellung der Berechtigung der den Antrag stellenden natürlichen Personen, einschließlich damit zusammenhängender Bewertungen der Verlässlichkeit von Beweismitteln, zu unterstützen;

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

8. Rechtspflege und demokratische Prozesse

a) KI-Systeme, die bestimmungsgemäß von einer oder im Namen einer Justizbehörde verwendet werden sollen, um eine Justizbehörde bei der Ermittlung und Auslegung von Sachverhalten und Rechtsvorschriften und bei der Anwendung des Rechts auf konkrete Sachverhalte zu unterstützen, oder die auf ähnliche Weise für die alternative Streitbeilegung genutzt werden sollen;

b) KI-Systeme, die bestimmungsgemäß verwendet werden sollen, um das Ergebnis einer Wahl oder eines Referendums oder das Wahlverhalten natürlicher Personen bei der Ausübung ihres Wahlrechts bei einer Wahl oder einem Referendum zu beeinflussen. Dazu gehören nicht KI-Systeme, deren Ausgaben natürliche Personen nicht direkt ausgesetzt sind, wie Instrumente zur Organisation, Optimierung oder Strukturierung politischer Kampagnen in administrativer oder logistischer Hinsicht.

[sn301] Risikomanagementsystem

[sn303] Technische Dokumentation

[sn502] Anbieter

[sn503] Betreiber

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, darunter

   a) Zweckbestimmung, Name des Anbieters und Version des Systems mit Angaben dazu, in welcher Beziehung sie zu vorherigen Versionen steht;

   b) gegebenenfalls Interaktion oder Verwendung des KI-Systems mit Hardware oder Software, einschließlich anderer KI-Systeme, die nicht Teil des KI-Systems selbst sind;

   c) Versionen der betreffenden Software oder Firmware und etwaige Anforderungen in Bezug auf Aktualisierungen der Versionen;

   d) Beschreibung aller Formen, in denen das KI-System in Verkehr gebracht oder in Betrieb genommen wird, zum Beispiel in Hardware eingebettete Softwarepakete, Herunterladen oder 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, die Kennzeichnungen und den inneren Aufbau dieser Produkte zeigen;

   g) eine grundlegende Beschreibung der Benutzerschnittstelle, die dem Betreiber zur Verfügung gestellt wird;

   h) Betriebsanleitungen für den Betreiber und gegebenenfalls eine grundlegende Beschreibung der dem Betreiber zur Verfügung gestellten Benutzerschnittstelle;

2. Detaillierte Beschreibung der Bestandteile des KI-Systems und seines Entwicklungsprozesses, darunter

   a) Methoden und Schritte zur Entwicklung des KI-Systems, gegebenenfalls einschließlich des Einsatzes von durch Dritte bereitgestellten vortrainierten Systemen oder Instrumenten, und wie diese vom Anbieter verwendet, integriert oder verändert wurden;

   b) Entwurfsspezifikationen des Systems, insbesondere die allgemeine Logik des KI-Systems und der Algorithmen; die wichtigsten Entwurfsentscheidungen mit den Gründen und getroffenen Annahmen, einschließlich in Bezug auf Personen oder Personengruppen, bezüglich deren das System angewandt werden soll; hauptsächliche Einstufungsentscheidungen; was das System optimieren soll und welche Bedeutung den verschiedenen Parametern dabei zukommt; Beschreibung der erwarteten Ausgabe des Systems und der erwarteten Qualität dieser Ausgabe; die über mögliche Kompromisse in Bezug auf die technischen Lösungen, mit denen die in Kapitel III Abschnitt 2 festgelegten Anforderungen erfüllt werden sollen, getroffenen Entscheidungen;

   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 Informationen zu deren Herkunft, Umfang und Hauptmerkmalen; Angaben zur Beschaffung und Auswahl der Daten; Kennzeichnungsverfahren (zum Beispiel für überwachtes Lernen) und Datenbereinigungsmethoden (zum Beispiel Erkennung von Ausreißern);

   e) Bewertung der nach Artikel 14 erforderlichen Maßnahmen der menschlichen Aufsicht, mit einer Bewertung der technischen Maßnahmen, die erforderlich sind, um den Betreibern gemäß Artikel 13 Absatz 3 Buchstabe d die Interpretation der Ausgaben von KI-Systemen zu erleichtern;

   f) gegebenenfalls detaillierte Beschreibung der vorab bestimmten Änderungen an dem KI-System und seiner Leistung mit allen einschlägigen Informationen zu den technischen Lösungen, mit denen sichergestellt wird, dass das KI-System die einschlägigen in Kapitel III Abschnitt 2 festgelegten Anforderungen weiterhin dauerhaft erfüllt;

   g) verwendete Validierungs- und Testverfahren, mit Informationen zu den verwendeten Validierungs- und Testdaten und deren Hauptmerkmalen; Parameter, die zur Messung der Genauigkeit, Robustheit und der Erfüllung anderer einschlägiger Anforderungen nach Kapitel III Abschnitt 2 sowie potenziell diskriminierender Auswirkungen verwendet werden; Testprotokolle und alle von den verantwortlichen Personen datierten und unterzeichneten Testberichte, auch in Bezug auf die unter Buchstabe f genannten vorab bestimmten Änderungen;

h) ergriffene Cybersicherheitsmaßnahmen;

3. Detaillierte Informationen über die Überwachung, Funktionsweise und Kontrolle des KI-Systems, insbesondere in Bezug auf Folgendes: die Fähigkeiten und Leistungsgrenzen des Systems, einschließlich der Genauigkeitsgrade bei bestimmten Personen oder Personengruppen, auf die es bestimmungsgemäß angewandt werden soll, sowie des in Bezug auf seine Zweckbestimmung insgesamt erwarteten Maßes an Genauigkeit; angesichts der Zweckbestimmung des KI-Systems vorhersehbare unbeabsichtigte Ergebnisse und Quellen von Risiken in Bezug auf Gesundheit und Sicherheit sowie Grundrechte und Diskriminierung; die nach Artikel 14 erforderlichen Maßnahmen der menschlichen Aufsicht, einschließlich der technischen Maßnahmen, die getroffen wurden, um den Betreibern die Interpretation der Ausgaben von KI-Systemen zu erleichtern; gegebenenfalls Spezifikationen zu Eingabedaten;

4. Darlegungen zur Eignung der Leistungskennzahlen für das spezifische KI-System;

5. Detaillierte Beschreibung des Risikomanagementsystems gemäß Artikel 9;

6. Beschreibung einschlägiger Änderungen, die der Anbieter während des Lebenszyklus an dem System vorgenommen hat;

7. Aufstellung der vollständig oder teilweise angewandten harmonisierten Normen, deren Fundstellen im *Amtsblatt der Europäischen Union* veröffentlicht wurden; falls keine solchen harmonisierten Normen angewandt wurden, eine detaillierte Beschreibung der Lösungen, mit denen die in Kapitel III Abschnitt 2 festgelegten Anforderungen erfüllt werden sollen, mit einer Aufstellung anderer angewandter einschlägiger Normen und technischer Spezifikationen;

8. Kopie der EU-Konformitätserklärung gemäß Artikel 47;

9. Detaillierte Beschreibung des Systems zur Bewertung der Leistung des KI-Systems in der Phase nach dem Inverkehrbringen gemäß Artikel 72, einschließlich des in Artikel 72 Absatz 3 genannten Plans für die Beobachtung nach dem Inverkehrbringen

[sn707] Bevollmächtigter

[sn502] Anbieter

ANHANG V

EU-Konformitätserklärung

Die EU-Konformitätserklärung gemäß Artikel 47 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 gemäß Artikel 47 trägt;
4. Versicherung, dass das betreffende KI-System der vorliegenden Verordnung sowie gegebenenfalls weiteren einschlägigen Rechtsvorschriften der Union, in denen die Ausstellung der EU-Konformitätserklärung gemäß Artikel 47 vorgesehen ist, entspricht;
5. wenn ein KI-System die Verarbeitung personenbezogener Daten erfordert, eine Erklärung darüber, dass das KI-System den Verordnungen (EU) 2016/679 und (EU) 2018/1725 sowie der Richtlinie (EU) 2016/680 entspricht;
6. Verweise auf die verwendeten einschlägigen harmonisierten Normen oder sonstigen gemeinsamen Spezifikationen, für die die Konformität erklärt wird;
7. gegebenenfalls Name und Identifizierungsnummer der notifizierten Stelle, Beschreibung des durchgeführten Konformitätsbewertungsverfahrens und Identifizierungsnummer der ausgestellten Bescheinigung;
8. Ort und Datum der Ausstellung der Erklärung, den Namen und die Funktion des Unterzeichners sowie Angabe, für wen oder in wessen Namen diese Person unterzeichnet hat, eine Unterschrift.

[sn303] Technische Dokumentation
[sn502] Anbieter

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, 3 und 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 Kapitel III Abschnitt 2 entspricht.
4. Der Anbieter überprüft ferner, ob der Entwurfs- und Entwicklungsprozess des KI-Systems und seine Beobachtung nach dem Inverkehrbringen gemäß Artikel 72 mit der technischen Dokumentation im Einklang stehen.

[sn707] Bevollmächtigter

ANHANG VII

Konformität auf der Grundlage einer Bewertung des Qualitätsmanagementsystems und einer Bewertung der technischen Dokumentation

[sn502] Anbieter

1. Einleitung

Die Konformität auf der Grundlage einer Bewertung des Qualitätsmanagementsystems und einer Bewertung der technischen Dokumentation entspricht dem Konformitätsbewertungsverfahren gemäß den Nummern 2 bis 5.

[sn303] Technische Dokumentation

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) Name und Anschrift des Anbieters sowie, wenn der Antrag von einem 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 angemessen und wirksam bleibt;

f) eine schriftliche Erklärung, dass derselbe Antrag bei keiner anderen notifizierten Stelle eingereicht wurde.

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 angemessen 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 unter 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 unter 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 unter Nummer 3 genannte Qualitätsmanagementsystem fällt.

4.2. Der Antrag enthält Folgendes:

a) den Namen und die Anschrift des Anbieters;

b) eine schriftliche Erklärung, dass derselbe Antrag bei keiner anderen notifizierten Stelle eingereicht wurde;

c) die in Anhang IV genannte technische Dokumentation.

[sn303] Technische Dokumentation

[sn502] Anbieter

4.3. Die technische Dokumentation wird von der notifizierten Stelle geprüft. Sofern es relevant ist und beschränkt auf das zur Wahrnehmung ihrer Aufgaben erforderliche Maß erhält die notifizierte Stelle uneingeschränkten Zugang zu den verwendeten Trainings-, Validierungs- und Testdatensätzen, gegebenenfalls und unter Einhaltung von Sicherheitsvorkehrungen auch über API oder sonstige einschlägige technische Mittel und Instrumente, die den Fernzugriff ermöglichen.

4.4. Bei der Prüfung der technischen Dokumentation kann die notifizierte Stelle vom Anbieter weitere Nachweise oder die Durchführung weiterer Tests verlangen, um eine ordnungsgemäße Bewertung der Konformität des KI-Systems mit den in Kapitel III Abschnitt 2 festgelegten Anforderungen zu ermöglichen. Ist die notifizierte Stelle mit den vom Anbieter durchgeführten Tests nicht zufrieden, so führt sie gegebenenfalls unmittelbar selbst angemessene Tests durch.

4.5. Sofern es für die Bewertung der Konformität des Hochrisiko-KI-Systems mit den in Kapitel III Abschnitt 2 festgelegten Anforderungen notwendig ist, und nachdem alle anderen sinnvollen Möglichkeiten zur Überprüfung der Konformität ausgeschöpft sind oder sich als unzureichend erwiesen haben, wird der notifizierten Stelle auf begründeten Antrag Zugang zu den Trainingsmodellen und trainierten Modellen des KI-Systems, einschließlich seiner relevanten Parameter, gewährt. Ein solcher Zugang unterliegt dem bestehenden EU-Recht zum Schutz von geistigem Eigentum und Geschäftsgeheimnissen.

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

[sn505] Konformitätsbewertung

Erfüllt das KI-System die Anforderungen in Kapitel III Abschnitt 2, so stellt die notifizierte Stelle eine Unionsbescheinigung 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 Informationen für die Beurteilung der Konformität des KI-Systems und gegebenenfalls für die Kontrolle des KI-Systems während seiner Verwendung.

Erfüllt das KI-System die in Kapitel III Abschnitt 2 festgelegten Anforderungen nicht, so verweigert die notifizierte Stelle die Ausstellung einer Unionsbescheinigung über die Bewertung der technischen Dokumentation und informiert den Antragsteller darüber, wobei sie ihre Verweigerung ausführlich begründet.

Erfüllt das KI-System nicht die Anforderung in Bezug auf die 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 Unionsbescheinigung 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 Bewertung durch die notifizierte Stelle, die die Unionsbescheinigung über die Bewertung der technischen Dokumentation ausgestellt hat. Der Anbieter informiert die notifizierte Stelle über seine Absicht, eine der 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 Unionsbescheinigung über die Bewertung der technischen Dokumentation ausgestellt werden könnte. In letzterem Fall bewertet die notifizierte Stelle die Änderungen, teilt dem Anbieter ihre Entscheidung mit und stellt ihm, sofern die Änderungen genehmigt wurden, einen Nachtrag zu der Unionsbescheinigung über die Bewertung der technischen Dokumentation aus.

5. Überwachung des genehmigten Qualitätsmanagementsystems

5.1. Mit der unter Nummer 3 genannten Überwachung durch die notifizierte Stelle soll sichergestellt werden, dass der Anbieter sich ordnungsgemäß an die Anforderungen und Bedingungen des genehmigten Qualitätsmanagementsystems hält.

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 Prüfbericht. Im Rahmen dieser Audits kann die notifizierte Stelle die KI-Systeme, für die eine Unionsbescheinigung über die Bewertung der technischen Dokumentation ausgestellt wurde, zusätzlichen Tests unterziehen.

[sn707] Bevollmächtigter
[sn908] EU-Datenbank
[sn502] Anbieter

ANHANG VIII

Bei der Registrierung des Hochrisiko-KI-Systems gemäß Artikel 49 bereitzustellende Informationen

Abschnitt A — Von Anbietern von Hochrisiko-KI-Systemen gemäß Artikel 49 Absatz 1 bereitzustellende Informationen

Für Hochrisiko-KI-Systeme, die gemäß Artikel 49 Absatz 1 zu registrieren sind, werden folgende Informationen bereitgestellt und danach auf dem neuesten Stand gehalten:

1. der Name, die Anschrift und die Kontaktdaten des Anbieters;

2. bei Vorlage von Informationen durch eine andere Person im Namen des Anbieters: der Name, die Anschrift und die Kontaktdaten dieser Person;

3. gegebenenfalls der Name, die Anschrift und die Kontaktdaten des Bevollmächtigten;

[sn206] Strafverfolgung

4. der Handelsname des KI-Systems und etwaige zusätzliche eindeutige Angaben, die die Identifizierung und Rückverfolgbarkeit des KI-Systems ermöglichen;

5. eine Beschreibung der Zweckbestimmung des KI-Systems und der durch dieses KI-System unterstützten Komponenten und Funktionen;

6. eine grundlegende und knappe Beschreibung der vom System verwendeten Informationen (Daten, Eingaben) und seiner Betriebslogik;

7. der Status des KI-Systems (in Verkehr/in Betrieb; nicht mehr in Verkehr/in Betrieb, zurückgerufen);

8. die Art, die Nummer und das Ablaufdatum der von der notifizierten Stelle ausgestellten Bescheinigung und gegebenenfalls Name oder Identifizierungsnummer dieser notifizierten Stelle;

9. gegebenenfalls eine gescannte Kopie der in Nummer 8 genannten Bescheinigung;

10. alle Mitgliedstaaten, in denen das KI-System in Verkehr gebracht, in Betrieb genommen oder in der Union bereitgestellt wurde;

11. eine Kopie der in Artikel 47 genannten EU-Konformitätserklärung;

12. elektronische Betriebsanleitungen; dies gilt nicht für Hochrisiko-KI-Systeme in den Bereichen Strafverfolgung oder Migration, Asyl und Grenzkontrolle gemäß Anhang III Nummern 1, 6 und 7;

13. Eine URL-Adresse für zusätzliche Informationen (fakultativ).

Abschnitt B — Von Anbietern von Hochrisiko-KI-Systemen gemäß Artikel 49 Absatz 2 bereitzustellende Informationen

Für KI-Systeme, die gemäß Artikel 49 Absatz 2 zu registrieren sind, werden folgende Informationen bereitgestellt und danach auf dem neuesten Stand gehalten:

1. der Name, die Anschrift und die Kontaktdaten des Anbieters;

2. bei Vorlage von Informationen durch eine andere Person im Namen des Anbieters: Name, Anschrift und Kontaktdaten dieser Person;

3. gegebenenfalls der Name, die Anschrift und die Kontaktdaten des Bevollmächtigten;

4. der Handelsname des KI-Systems und etwaige zusätzliche eindeutige Angaben, die die Identifizierung und Rückverfolgbarkeit des KI-Systems ermöglichen;

5. eine Beschreibung der Zweckbestimmung des KI-Systems;

6. die Bedingung oder Bedingungen gemäß Artikel 6 Absatz 3, aufgrund derer das KI-System nicht als Hoch-Risiko-System eingestuft wird;

7. eine kurze Zusammenfassung der Gründe, aus denen das KI-System in Anwendung des Verfahrens gemäß Artikel 6 Absatz 3 nicht als Hoch-Risiko-System eingestuft wird;

8. der Status des KI-Systems (in Verkehr/in Betrieb; nicht mehr in Verkehr/in Betrieb, zurückgerufen)

9. alle Mitgliedstaaten, in denen das KI-System in der Union in Verkehr gebracht, in Betrieb genommen oder bereitgestellt wurde.

[sn503] Betreiber

[sn908] EU-Datenbank

[sn706] Grundrechte-Folgenabschätzung

Abschnitt C — Von Betreibern von Hochrisiko-KI-Systemen gemäß Artikel 49 Absatz 3 bereitzustellende Informationen

Für Hochrisiko-KI-Systeme, die gemäß Artikel 49 Absatz 3 zu registrieren sind, werden folgende Informationen bereitgestellt und danach auf dem neuesten Stand gehalten:

1. der Name, die Anschrift und die Kontaktdaten des Betreibers;
2. der Name, die Anschrift und die Kontaktdaten der Person, die im Namen des Betreibers Informationen übermittelt;
3. die URL des Eintrags des KI-Systems in der EU-Datenbank durch seinen Anbieter;
4. eine Zusammenfassung der Ergebnisse der gemäß Artikel 27 durchgeführten Grundrechte-Folgenabschätzung;
5. gegebenenfalls eine Zusammenfassung der im Einklang mit Artikel 35 der Verordnung (EU) 2016/679 oder Artikel 27 der Richtlinie (EU) 2016/680 gemäß Artikel 26 Absatz 8 der vorliegenden Verordnung durchgeführten Datenschutz-Folgenabschätzung.

[sn502] Anbieter

[sn503] Betreiber

ANHANG IX

Bezüglich Tests unter Realbedingungen gemäß Artikel 60 bei der Registrierung von in Anhang III aufgeführten Hochrisiko-KI-Systemen bereitzustellende Informationen

Bezüglich Tests unter Realbedingungen, die gemäß Artikel 60 zu registrieren sind, werden folgende Informationen bereitgestellt und danach auf dem aktuellen Stand gehalten:

1. eine unionsweit einmalige Identifizierungsnummer des Tests unter Realbedingungen;
2. der Name und die Kontaktdaten des Anbieters oder zukünftigen Anbieters und der Betreiber, die an dem Test unter Realbedingungen teilgenommen haben;
3. eine kurze Beschreibung des KI-Systems, seine Zweckbestimmung und sonstige zu seiner Identifizierung erforderliche Informationen;
4. eine Übersicht über die Hauptmerkmale des Plans für den Test unter Realbedingungen;
5. Informationen über die Aussetzung oder den Abbruch des Tests unter Realbedingungen.

ANHANG X

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) Verordnung (EU) 2021/1133 des Europäischen Parlaments und des Rates vom 7. Juli 2021 zur Änderung der Verordnungen (EU) Nr. 603/2013, (EU) 2016/794, (EU) 2018/1862, (EU) 2019/816 und (EU) 2019/818 hinsichtlich der Festlegung der Voraussetzungen für den Zugang zu anderen Informationssystemen der EU für Zwecke des Visa-Informationssystems (ABl. L 248 vom 13.7.2021, S. 1)

b) Verordnung (EU) 2021/1134 des Europäischen Parlaments und des Rates vom 7. Juli 2021 zur Änderung der Verordnungen (EG) Nr. 767/2008, (EG) Nr. 810/2009, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1860, (EU) 2018/1861, (EU) 2019/817 und (EU) 2019/1896 des Europäischen Parlaments und des Rates und zur Aufhebung der Entscheidung 2004/512/EG und des Beschlusses 2008/633/JI des Rates zum Zwecke der Reform des Visa-Informationssystems (ABl. L 248 vom 13.7.2021, S. 11)

3. Eurodac

Verordnung (EU) 2024/1358 des Europäischen Parlaments und des Rates vom 14. Mai 2024 über die Einrichtung von Eurodac für den Abgleich biometrischer Daten zum Zwecke der effektiven Anwendung der Verordnungen (EU) 2024/1315 und (EU) 2024/1350 des Europäischen Parlaments und des Rates und der Richtlinie 2001/55/EG des Rates und zur Feststellung der Identität illegal aufhältiger Drittstaatsangehöriger und 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 des Europäischen Parlaments und des Rates und zur Aufhebung der Verordnung (EU) Nr. 603/2013 des Europäischen Parlaments und des Rates (ABl. L, 2024/1358, 22.5.2024, ELI: http://data.europa.eu/eli/reg/2024/1358/oj)

4. Einreise-/Ausreisesystem

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

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

7. Interoperabilität

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

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

[se009] regelt

[sn502] Anbieter

ANHANG XI

Technische Dokumentation gemäß Artikel 53 Absatz 1 Buchstabe a — technische Dokumentation für Anbieter von KI-Modellen mit allgemeinem Verwendungszweck

Abschnitt 1

Von allen Anbietern von KI-Modellen mit allgemeinem Verwendungszweck bereitzustellende Informationen

Die in Artikel 53 Absatz 1 Buchstabe a genannte technische Dokumentation muss mindestens die folgenden Informationen enthalten, soweit es anhand der Größe und des Risikoprofils des betreffenden Modells angemessen ist:

1. Eine allgemeine Beschreibung des KI-Modells einschließlich

   a) der Aufgaben, die das Modell erfüllen soll, sowie der Art und des Wesens der KI-Systeme, in die es integriert werden kann;

   b) die anwendbaren Regelungen der akzeptablen Nutzung;

   c) das Datum der Freigabe und die Vertriebsmethoden;

   d) die Architektur und die Anzahl der Parameter;

   e) die Modalität (zum Beispiel Text, Bild) und das Format der Ein- und Ausgaben;

   f) die Lizenz.

2. Eine ausführliche Beschreibung der Elemente des Modells gemäß Nummer 1 und relevante Informationen zum Entwicklungsverfahren, einschließlich der folgenden Elemente:

   a) die technischen Mittel (zum Beispiel Betriebsanleitungen, Infrastruktur, Instrumente), die für die Integration des KI-Modells mit allgemeinem Verwendungszweck in KI-Systeme erforderlich sind;

   b) die Entwurfsspezifikationen des Modells und des Trainingsverfahrens einschließlich Trainingsmethoden und -techniken, die wichtigsten Entwurfsentscheidungen mit den Gründen und getroffenen Annahmen; gegebenenfalls, was das Modell optimieren soll und welche Bedeutung den verschiedenen Parametern dabei zukommt;

   c) gegebenenfalls Informationen über die für das Trainieren, Testen und Validieren verwendeten Daten, einschließlich der Art und Herkunft der Daten und der Aufbereitungsmethoden (zum Beispiel Bereinigung, Filterung usw.), der Zahl der Datenpunkte, ihres Umfangs und ihrer Hauptmerkmale; gegebenenfalls die Art und Weise, wie die Daten erlangt und ausgewählt wurden, sowie alle anderen Maßnahmen zur Feststellung, ob Datenquellen ungeeignet sind, und Methoden zur Erkennung ermittelbarer Verzerrungen;

   d) die für das Trainieren des Modells verwendeten Rechenressourcen (zum Beispiel Anzahl der Gleitkommaoperationen), die Trainingszeit und andere relevante Einzelheiten im Zusammenhang mit dem Trainieren;

   e) bekannter oder geschätzter Energieverbrauch des Modells.

   Wenn der Energieverbrauch des Modells nicht bekannt ist, kann für Buchstabe e der Energieverbrauch auf Informationen über die eingesetzten Rechenressourcen gestützt werden.

Abschnitt 2

Zusätzliche von Anbietern von KI-Modellen mit allgemeinem Verwendungszweck mit systemischem Risiko bereitzustellende Informationen

1. Eine ausführliche Beschreibung der Prüfstrategien, einschließlich der Prüfungsergebnisse, auf der Grundlage öffentlich verfügbarer Prüfprotokolle und -instrumente oder anderer Prüfmethoden. Die Prüfstrategien umfassen Prüfkriterien und -metrik sowie die Methodik zur Ermittlung von Einschränkungen.

2. Gegebenenfalls eine ausführliche Beschreibung der Maßnahmen, die ergriffen wurden, um interne und/oder externe Angriffstests durchzuführen (zum Beispiel Red Teaming), Modellanpassungen, einschließlich Ausrichtung und Feinabstimmung.

3. Gegebenenfalls eine ausführliche Beschreibung der Systemarchitektur, aus der hervorgeht, wie Softwarekomponenten aufeinander aufbauen oder einander zuarbeiten und in die Gesamtverarbeitung integriert sind.

[sn502] Anbieter

ANHANG XII

Transparenzinformationen gemäß Artikel 53 Absatz 1 Buchstabe b — technische Dokumentation für Anbieter von KI-Modellen mit allgemeinem Verwendungszweck für nachgelagerte Anbieter, die das Modell in ihr KI-System integrieren

Die in Artikel 53 Absatz 1 Buchstabe b genannten Informationen enthalten mindestens Folgendes:

1. eine allgemeine Beschreibung des KI-Modells einschließlich

   a) der Aufgaben, die das Modell erfüllen soll, sowie der Art und des Wesens der KI-Systeme, in die es integriert werden kann;

   b) die anwendbaren Regelungen der akzeptablen Nutzung;

   c) das Datum der Freigabe und die Vertriebsmethoden;

   d) gegebenenfalls wie das Modell mit Hardware oder Software interagiert, die nicht Teil des Modells selbst ist, oder wie es zu einer solchen Interaktion verwendet werden kann;

   e) gegebenenfalls die Versionen der einschlägigen Software im Zusammenhang mit der Verwendung des KI-Modells mit allgemeinem Verwendungszweck;

   f) die Architektur und die Anzahl der Parameter;

   g) die Modalität (zum Beispiel Text, Bild) und das Format der Ein- und Ausgaben;

   h) die Lizenz für das Modell.

2. Eine Beschreibung der Bestandteile des Modells und seines Entwicklungsprozesses, einschließlich

   a) die technischen Mittel (zum Beispiel Betriebsanleitungen, Infrastruktur, Instrumente), die für die Integration des KI-Modells mit allgemeinem Verwendungszweck in KI-Systeme erforderlich sind;

   b) Modalität (zum Beispiel Text, Bild usw.) und Format der Ein- und Ausgaben und deren maximale Größe (zum Beispiel Länge des Kontextfensters usw.);

   c) gegebenenfalls Informationen über die für das Trainieren, Testen und Validieren verwendeten Daten, einschließlich der Art und Herkunft der Daten und der Aufbereitungsmethoden.

ANHANG XIII

Kriterien für die Benennung von KI-Modellen mit allgemeinem Verwendungszweck mit systemischem Risiko gemäß Artikel 51

Um festzustellen, ob ein KI-Modell mit allgemeinem Verwendungszweck über Fähigkeiten oder eine Wirkung verfügt, die den in Artikel 51 Absatz 1 Buchstabe a genannten gleichwertig sind, berücksichtigt die Kommission folgende Kriterien:

a) die Anzahl der Parameter des Modells;

b) die Qualität oder Größe des Datensatzes, zum Beispiel durch Tokens gemessen;

c) die Menge der für das Trainieren des Modells verwendeten Berechnungen, gemessen in Gleitkommaoperationen oder anhand einer Kombination anderer Variablen, wie geschätzte Trainingskosten, geschätzter Zeitaufwand für das Trainieren oder geschätzter Energieverbrauch für das Trainieren;

d) die Ein- und Ausgabemodalitäten des Modells, wie Text-Text (Große Sprachmodelle), Text-Bild, Multimodalität, Schwellenwerte auf dem Stand der Technik für die Bestimmung der Fähigkeiten mit hoher Wirkkraft für jede Modalität und die spezifische Art der Ein- und Ausgaben (zum Beispiel biologische Sequenzen);

e) die Benchmarks und Beurteilungen der Fähigkeiten des Modells, einschließlich unter Berücksichtigung der Zahl der Aufgaben ohne zusätzliches Training, der Anpassungsfähigkeit zum Erlernen neuer, unterschiedlicher Aufgaben, des Grades an Autonomie und Skalierbarkeit sowie der Instrumente, zu denen es Zugang hat;

f) ob es aufgrund seiner Reichweite große Auswirkungen auf den Binnenmarkt hat — davon wird ausgegangen, wenn es mindestens 10 000 in der Union niedergelassenen registrierten gewerblichen Nutzern zur Verfügung gestellt wurde;

g) die Zahl der registrierten Endnutzer.