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:

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;

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.

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.

(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.

(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;

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;

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;

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.

(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.

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;

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.

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

(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.

(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.

(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;

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

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;

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.

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,

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

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;

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;

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.

(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.

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

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;

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;

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.

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.