EUROPÄISCHE
KOMMISSION

Brüssel, den 15.9.2022
COM(2022) 454 final

2022/0272 (COD)

Vorschlag für eine

VERORDNUNG DES EUROPÄISCHEN PARLAMENTS UND DES RATES

über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen und zur Änderung der Verordnung (EU) 2019/1020

(Text von Bedeutung für den EWR)

{SEC(2022) 321 final} - {SWD(2022) 282 final} - {SWD(2022) 283 final}

BEGRÜNDUNG

1. KONTEXT DES VORSCHLAGS

• Gründe und Ziele des Vorschlags

Hardware- und Softwareprodukte werden zunehmend zum Ziel erfolgreicher Cyberangriffe. Die dadurch entstehenden jährlichen Kosten der Cyberkriminalität werden bis zum Jahr 2021 auf 5,5 Billionen EUR geschätzt. Im Zusammenhang mit diesen Produkten gibt es zwei große Probleme, die hohe zusätzliche Kosten für die Nutzer und die Gesellschaft verursachen: 1) ein geringes Maß an Cybersicherheit, das sich in weitverbreiteten Schwachstellen und der unzureichenden und inkohärenten Bereitstellung von Sicherheitsaktualisierungen zu deren Behebung widerspiegelt, und 2) ein unzureichendes Verständnis und ein mangelnder Informationszugang der Nutzer, wodurch sie daran gehindert werden, Produkte mit angemessenen Cybersicherheitsmerkmalen auszuwählen oder sicher zu verwenden. In einem vernetzten Umfeld kann ein Cybersicherheitsvorfall bei einem Produkt eine ganze Organisation oder eine ganze Lieferkette beeinträchtigen und sich oft innerhalb von Minuten über die Grenzen des Binnenmarkts hinweg verbreiten. Dies kann zu einer schwerwiegenden Störung wirtschaftlicher und sozialer Tätigkeiten führen oder sogar lebensbedrohlich werden.

Die Cybersicherheit von Produkten mit digitalen Elementen hat eine ausgeprägte grenzüberschreitende Dimension, weil die in einem Land hergestellten Produkte häufig im gesamten Binnenmarkt verwendet werden. Darüber hinaus breiten sich Vorfälle, die ursprünglich nur eine einzige Stelle oder einen einzelnen Mitgliedstaat betreffen, oftmals innerhalb von Minuten auf den gesamten Binnenmarkt aus.

Die bestehenden Binnenmarktvorschriften gelten zwar für bestimmte Produkte mit digitalen Elementen, für die meisten Hardware- und Softwareprodukte gibt es derzeit aber keine EU-Rechtsvorschriften, die deren Cybersicherheit betreffen. Insbesondere erstreckt sich der derzeitige EU-Rechtsrahmen nicht auf die Cybersicherheit nicht eingebetteter Software, obwohl Cyberangriffe zunehmend auf Schwachstellen in diesen Produkten abzielen und erhebliche gesellschaftliche und wirtschaftliche Kosten verursachten. Es gibt zahlreiche Beispiele für bemerkenswerte Cyberangriffe, die auf eine unzureichende Produktsicherheit zurückzuführen sind, wie etwa der Ransomware-Wurm WannaCry, mit dem eine Windows-Schwachstelle ausgenutzt wurde und von dem im Jahr 2017 200 000 Computer in 150 Ländern befallen wurden, wodurch ein Schaden in Höhe von einigen Milliarden USD entstand, der Angriff auf die Lieferkette von Kaseya VSA, bei dem die Kaseya-Netzverwaltungssoftware benutzt wurde, um mehr als 1000 Unternehmen anzugreifen und eine Supermarktkette zur Schließung aller ihrer 500 Ladengeschäfte in ganz Schweden zu zwingen, oder die zahlreichen Vorfälle, bei denen Bankanwendungen gehackt werden, um ahnungslosen Verbrauchern ihr Geld zu stehlen.

Im Hinblick auf die Gewährleistung des reibungslosen Funktionierens des Binnenmarkts wurden zwei Hauptziele festgelegt: 1) die Schaffung der Bedingungen für die Entwicklung sicherer Produkte mit digitalen Elementen, damit Hardware- und Softwareprodukte mit weniger Schwachstellen in Verkehr gebracht werden und damit die Hersteller sich während des gesamten Lebenszyklus eines Produkts ernsthaft um die Sicherheit kümmern, und 2) die Schaffung von Bedingungen, die es den Nutzern ermöglichen, bei der Auswahl und Verwendung von Produkten mit digitalen Elementen die Cybersicherheit zu berücksichtigen. Es wurden vier spezifische Ziele festgelegt: i) Gewährleistung, dass die Hersteller die Sicherheit von Produkten mit digitalen Elementen schon ab der Konzeptions- und Entwicklungsphase und über den gesamten Lebenszyklus verbessern, ii) Gewährleistung eines kohärenten Cybersicherheitsrahmens, der den Hardware- und Software-Herstellern die

Einhaltung der Vorschriften erleichtert, iii) Erhöhung der Transparenz der Sicherheitseigenschaften von Produkten mit digitalen Elementen und iv) Befähigung der Unternehmen und Verbraucher, damit sie Produkte mit digitalen Elementen sicher verwenden können.

Aufgrund des ausgeprägten grenzüberschreitenden Charakters der Cybersicherheit und der zunehmenden Häufigkeit der Sicherheitsvorfälle, die sich über Grenzen, Sektoren und Produkte hinweg auswirken, können die Ziele von den Mitgliedstaaten allein nicht wirksam erreicht werden. Angesichts des globalen Charakters der Märkte für Produkte mit digitalen Elementen sehen sich verschiedene Mitgliedstaaten mit denselben Risiken bei denselben Produkten mit digitalen Elementen in ihrem Hoheitsgebiet konfrontiert. Aus einem sich abzeichnenden fragmentierten Rahmen mit möglicherweise voneinander abweichenden nationalen Vorschriften erwächst die Gefahr, dass Hindernisse für einen offenen und wettbewerbsfähigen Binnenmarkt für Produkte mit digitalen Elementen entstehen. Daher ist ein gemeinsames Vorgehen auf EU-Ebene erforderlich, um das Vertrauen der Nutzer und die Attraktivität von EU-Produkten mit digitalen Elementen zu steigern. Dies würde auch dem Binnenmarkt zugutekommen, da so Rechtssicherheit und gleiche Wettbewerbsbedingungen für Anbieter von Produkten mit digitalen Elementen geschaffen werden. Hierauf wird auch im Abschlussbericht der Konferenz zur Zukunft Europas hingewiesen, in dem die Bürgerinnen und Bürger eine stärkere Rolle der EU bei der Abwehr von Cybersicherheitsbedrohungen fordern.

- **Zusammenspiel mit den bestehenden Vorschriften in diesem Bereich**

Der bestehende EU-Rahmen umfasst mehrere horizontale Rechtsvorschriften, die bestimmte Aspekte der Cybersicherheit aus verschiedenen Blickwinkeln abdecken (Produkte, Dienstleistungen, Krisenmanagement und Straftaten). Im Jahr 2013 trat die Richtlinie über Angriffe auf Informationssysteme[1] in Kraft und bewirkte eine Harmonisierung der Straftatbestände und der Strafen für eine Reihe von Straftaten gegen Informationssysteme. Im August 2016 trat die Richtlinie (EU) 2016/1148 über die Sicherheit von Netz- und Informationssystemen (NIS-Richtlinie)[2] als erster EU-weiter Rechtsakt im Bereich der Cybersicherheit in Kraft. Mit ihrer Überarbeitung, deren Ergebnis die Richtlinie [Richtlinie XXX/XXXX (NIS2)] ist, werden noch ehrgeizigere gemeinsame Ziele auf EU-Ebene verfolgt. Im Jahr 2019 trat der EU-Rechtsakt zur Cybersicherheit[3] in Kraft, mit dem die Sicherheit von IKT-Produkten, IKT-Diensten und IKT-Prozessen durch die Einführung eines freiwilligen europäischen Rahmens für die Cybersicherheitszertifizierung[4] verbessert werden sollte.

---

1 Richtlinie 2013/40/EU des Europäischen Parlaments und des Rates vom 12. August 2013 über Angriffe auf Informationssysteme und zur Ersetzung des Rahmenbeschlusses 2005/222/JI des Rates (ABl. L 218 vom 14.8.2013, S. 8).

2 Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union (ABl. L 194 vom 19.7.2016, S. 1).

3 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).

4 Der Rechtsakt zur Cybersicherheit ermöglicht die Entwicklung spezieller Zertifizierungssysteme. Jedes System enthält Verweise auf einschlägige Normen, technische Spezifikationen oder andere Cybersicherheitsanforderungen, die in dem System definiert werden. Die Entscheidung, eine Cybersicherheitszertifizierung zu entwickeln, erfolgt risikobasiert.

Die Cybersicherheit der gesamten Lieferkette kann nur dann gewährleistet werden, wenn auch alle ihre Bestandteile cybersicher sind. Die oben genannten EU-Rechtsvorschriften weisen jedoch erhebliche Lücken in dieser Hinsicht auf, denn sie enthalten keine verbindlichen Anforderungen an die Sicherheit von Produkten mit digitalen Elementen.

Während das vorgeschlagene Cyberresilienzgesetz in Verkehr gebrachte Produkte mit digitalen Elementen erfasst, zielt die Richtlinie [Richtlinie XXX/XXX (NIS2)] darauf ab, ein hohes Maß an Cybersicherheit der Dienste wesentlicher und wichtiger Einrichtungen zu gewährleisten. Nach der Richtlinie [Richtlinie XXX/XXXX (NIS2)] müssen die Mitgliedstaaten sicherstellen, dass die erfassten wesentlichen und wichtigen Einrichtungen, wie z. B. Erbringer von Gesundheitsdienstleistungen oder Cloud-Anbieter und Einrichtungen der öffentlichen Verwaltung, geeignete und verhältnismäßige technische, betriebliche und organisatorische Cybersicherheitsmaßnahmen ergreifen. Dazu gehört unter anderem die Anforderung, Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von Netz- und Informationssystemen umzusetzen, einschließlich Management und Offenlegung von Schwachstellen. Nach der Richtlinie [Richtlinie XXX/XXXX (NIS2)] muss die Kommission Durchführungsrechtsakte zur Festlegung der technischen und methodischen Anforderungen an diese Maßnahmen für bestimmte Arten von Einrichtungen, wie z. B. Cloud-Computing-Diensteanbieter, innerhalb von 21 Monaten nach dem Inkrafttreten dieser Richtlinie erlassen. Für alle anderen Einrichtungen kann die Kommission einen Durchführungsrechtsakt erlassen, in dem sie die technischen und methodischen Anforderungen sowie sektorspezifische Anforderungen festlegt. Dieser Rahmen wird sicherstellen, dass technische Spezifikationen und Maßnahmen, die den grundlegenden Cybersicherheitsanforderungen des Cyberresilienzgesetzes gleichwertig sind, auch bei der Konzeption, Entwicklung und Behandlung von Schwachstellen in als Dienstleistung bereitgestellter Software (*Software-as-a-Service*) umgesetzt werden. So könnte ein hohes Maß an Cybersicherheit z. B. bei elektronischen Patientenakten (EHR-Systeme) gewährleistet werden, selbst wenn sie als SaaS (*Software-as-a-Service*) bereitgestellt oder innerhalb von Gesundheitseinrichtungen (intern) gemäß der vorgeschlagenen [Verordnung über den europäischen Raum für Gesundheitsdaten] entwickelt werden.

- **Zusammenspiel mit der Politik der Union in anderen Bereichen**

Wie in der Mitteilung der Kommission zur Gestaltung der digitalen Zukunft Europas[5] dargelegt wurde, ist es für die EU von entscheidender Bedeutung, dass das Potenzial des digitalen Zeitalters vollständig ausgeschöpft wird und dass die europäische Industrie und Innovationskapazität gestärkt werden, ohne bei Sicherheit und Ethik Abstriche zu machen. Die europäische Datenstrategie setzt auf vier Säulen – Datenschutz, Grundrechte, Sicherheit und Cybersicherheit – als wesentliche Voraussetzungen dafür, dass die Gesellschaft Vorteile aus der Nutzung von Daten ziehen kann.

Der derzeitige EU-Rechtsrahmen[6] für Produkte, die auch digitale Elemente enthalten können, umfasst mehrere Rechtsvorschriften, darunter EU-Rechtsvorschriften für bestimmte Produkte, die auch sicherheitsbezogene Aspekte abdecken, sowie allgemeine Rechtsvorschriften zur Produkthaftung. Der Vorschlag steht im Einklang mit dem gegenwärtigen produktbezogenen

---

5 Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen – Gestaltung der digitalen Zukunft Europas, COM(2020) 67 final vom 19. Februar 2020.

6 Hauptsächlich Rechtsvorschriften des Neuen Rechtsrahmens (NLF).

EU-Rechtsrahmen sowie mit den jüngsten Legislativvorschlägen wie dem Vorschlag der Kommission für eine Verordnung [KI-Verordnung][7].

Die vorgeschlagene Verordnung würde für alle Funkanlagen gelten, die in den Anwendungsbereich der Delegierten Verordnung (EU) 2022/30 der Kommission fallen. Darüber hinaus enthalten die in dieser Verordnung festgelegten Anforderungen alle Elemente der grundlegenden Anforderungen gemäß Artikel 3 Absatz 3 Buchstaben d, e und f der Richtlinie 2014/53/EU, einschließlich der Hauptelemente, die in dem auf der Grundlage der genannten delegierten Verordnung erlassenen [Durchführungsbeschluss XXX/2022 der Kommission über einen Normungsauftrag an die europäischen Normungsorganisationen] aufgeführt sind. Um Überschneidungen bei der Regulierung zu vermeiden, beabsichtigt die Kommission, die delegierte Verordnung in Bezug auf Funkanlagen, die unter die hier vorgeschlagene Verordnung fallen, aufzuheben oder zu ändern, sodass die vorgeschlagene Verordnung Anwendung finden würde, sobald sie anwendbar wird.

Außerdem ist im Hinblick auf die Vermeidung von Doppelarbeit vorgesehen, dass die Kommission und die europäischen Normungsorganisationen – um die Durchführung der vorliegenden Verordnung zu erleichtern – bei der Ausarbeitung und Entwicklung harmonisierter Normen die Normungsarbeiten berücksichtigen, die im Rahmen des Durchführungsbeschlusses C(2022) 5637 der Kommission über einen Normungsauftrag zur Delegierten Verordnung (EU) 2022/30 über Funkanlagen durchgeführt werden.

2. RECHTSGRUNDLAGE, SUBSIDIARITÄT UND VERHÄLTNISMÄßIGKEIT

• Rechtsgrundlage

Rechtsgrundlage für diesen Vorschlag ist Artikel 114 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV), der die Annahme von Maßnahmen für die Errichtung und das Funktionieren des Binnenmarkts vorsieht. Zweck des Vorschlags ist die Harmonisierung der Cybersicherheitsanforderungen für Produkte mit digitalen Elementen in allen Mitgliedstaaten und die Beseitigung von Hindernissen für den freien Warenverkehr.

Artikel 114 AEUV kann als Rechtsgrundlage herangezogen werden, um das Entstehen solcher Hindernisse zu verhindern, die sich aus unterschiedlichen nationalen Rechtsvorschriften und Ansätzen in Bezug darauf ergeben, wie Rechtsunsicherheiten und Lücken in den bestehenden Rechtsrahmen zu beseitigen sind[8]. Darüber hinaus hat der Gerichtshof anerkannt, dass die Anwendung heterogener technischer Anforderungen ein stichhaltiger Grund für die Heranziehung des Artikels 114 AEUV sein könnte[9].

Der derzeitige EU-Rechtsrahmen für Produkte mit digitalen Elementen beruht auf Artikel 114 AEUV und umfasst mehrere Rechtsvorschriften für bestimmte Produkte und über sicherheitsbezogene Aspekte sowie allgemeine Rechtsvorschriften zur Produkthaftung. Er deckt aber nur bestimmte Aspekte im Zusammenhang mit der Cybersicherheit materieller digitaler Produkte und gegebenenfalls der in diese Produkte eingebetteten Software ab. Auf

---

7 Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz (Gesetz über künstliche Intelligenz) und zur Änderung bestimmter Rechtsakte der Union, COM(2021) 206 final vom 21. April 2021.

8 Urteil des Gerichtshofs (Große Kammer) vom 3. Dezember 2019, Tschechische Republik gegen Europäisches Parlament und Rat der Europäischen Union, Rechtssache C-482/17, Rn. 35.

9 Urteil des Gerichtshofs (Große Kammer) vom 2. Mai 2006, Vereinigtes Königreich Großbritannien und Nordirland gegen Europäisches Parlament und Rat der Europäischen Union, Rechtssache C-217/04, Rn. 62–63.

nationaler Ebene beginnen die Mitgliedstaaten damit, nationale Maßnahmen zu ergreifen, mit denen Anbieter digitaler Produkte verpflichtet werden, ihre Cybersicherheit zu verbessern[10]. Gleichzeitig hat die Cybersicherheit digitaler Produkte eine besonders ausgeprägte grenzüberschreitende Dimension, weil die in einem Land hergestellten Produkte häufig von Organisationen und Verbrauchern im gesamten Binnenmarkt verwendet werden. Vorfälle, die ursprünglich nur eine einzige Stelle oder einen einzelnen Mitgliedstaat betreffen, breiten sich oftmals innerhalb von Minuten auf Organisationen, Sektoren und mehrere Mitgliedstaaten aus.

Die verschiedenen bisher auf EU-Ebene und auf nationaler Ebene erlassenen Vorschriften und ergriffenen Initiativen befassen sich nur teilweise mit den festgestellten Problemen und Risiken, wodurch ein legislativer Flickenteppich innerhalb des Binnenmarkts entstanden ist, der zu einer größeren Rechtsunsicherheit sowohl für die Anbieter als auch für die Nutzer solcher Produkte und zu einer größeren unnötigen Belastung der Unternehmen führt, die eine Reihe verschiedener Anforderungen in Bezug auf ähnliche Produktarten zu erfüllen haben.

Die vorgeschlagene Verordnung würde das Regulierungsumfeld der EU straffen und harmonisieren, indem Cybersicherheitsanforderungen für Produkte mit digitalen Elementen eingeführt und Überschneidungen mit Anforderungen, die sich aus verschiedenen Rechtsvorschriften ergeben, vermieden werden. Dies würde zu mehr Rechtssicherheit für Wirtschaftsakteure und Nutzer in der gesamten Union sowie zu einer besseren Harmonisierung des europäischen Binnenmarkts führen, wodurch bessere Bedingungen für Wirtschaftsakteure geschaffen würden, die in den EU-Markt eintreten wollen.

- **Subsidiarität (bei nicht ausschließlicher Zuständigkeit)**

Aufgrund des ausgeprägten grenzüberschreitenden Charakters der Cybersicherheit im Allgemeinen und der zunehmenden Zahl der Risiken und Sicherheitsvorfälle, die sich über Grenzen, Sektoren und Produkte hinweg auswirken, können die Ziele der vorliegenden Maßnahme von den Mitgliedstaaten allein nicht wirksam erreicht werden. Durch nationale Ansätze zur Lösung der Probleme und insbesondere durch Konzepte, mit denen verbindliche Anforderungen eingeführt werden, entstehen zusätzliche Rechtsunsicherheit und rechtliche Hindernisse. Unternehmen könnten so daran gehindert werden, nahtlos in andere Mitgliedstaaten zu expandieren, wodurch die Vorteile ihrer Produkte den dortigen Nutzern vorenthalten würden.

Daher ist ein gemeinsames Vorgehen auf EU-Ebene erforderlich, um bei den Nutzern Vertrauen zu schaffen und die Attraktivität von EU-Produkten mit digitalen Elementen zu steigern. Dies würde auch dem digitalen Binnenmarkt und dem Binnenmarkt im Allgemeinen zugutekommen, denn so wird Rechtssicherheit gewährleistet und es werden gleiche Wettbewerbsbedingungen für die Hersteller von Produkten mit digitalen Elementen geschaffen.

Schließlich wurde die Kommission in den Schlussfolgerungen des Rates vom 23. Mai 2022 zur Entwicklung der Cyberabwehr der Europäischen Union aufgefordert, bis Ende 2022 gemeinsame Anforderungen an die Cybersicherheit vernetzter Geräte vorzuschlagen.

---

[10] So hat Finnland im Jahr 2019 ein Kennzeichnungssystem für IoT-Geräte wie Smart TVs, Smartphones und Spielzeug auf der Grundlage der ETSI-Normen eingeführt. Deutschland hat kürzlich im Interesse des Verbraucherschutzes eine Sicherheitskennzeichnung für Breitband-Router, Smart-TVs, Kameras, Lautsprecher, Spielzeug sowie Reinigungs- und Gartenroboter eingeführt.

- **Verhältnismäßigkeit**

Was die Verhältnismäßigkeit der vorgeschlagenen Verordnung betrifft, würden die Maßnahmen der erwogenen Politikoptionen nicht über das zur Erreichung der allgemeinen und besonderen Ziele erforderliche Maß hinausgehen und keine unverhältnismäßig hohen Kosten verursachen. Konkret würde mit dem in Betracht gezogenen Eingreifen sichergestellt, dass Produkte mit digitalen Elementen während ihres gesamten Lebenszyklus und proportional zu den bestehenden Risiken abgesichert werden, und zwar durch objektive und technologieneutrale Anforderungen, die angemessen bleiben und im Allgemeinen den Interessen der beteiligten Unternehmen entsprechen.

Die grundlegenden Cybersicherheitsanforderungen in dem Vorschlag bauen auf bereits weitverbreiteten Normen auf, und das anschließende Normungsverfahren würde den technischen Besonderheiten der Produkte Rechnung tragen. Das bedeutet, dass die Sicherheitskontrollen angepasst werden, wenn dies für ein bestimmtes Risikoniveau erforderlich ist. Darüber hinaus würden die geplanten horizontalen Vorschriften für kritische Produkte ausschließlich eine Konformitätsbewertung durch Dritte vorsehen. Dies würde aber nur einen geringen Anteil des Marktes für Produkte mit digitalen Elementen betreffen. Die Auswirkungen auf KMU würden von ihrer Marktpräsenz bei diesen Produktkategorien abhängen.

Was die Verhältnismäßigkeit der Kosten der Konformitätsbewertung betrifft, würden die notifizierten Stellen, die die Bewertungen durch Dritte durchführen, bei der Festsetzung ihrer Gebühren die Unternehmensgröße berücksichtigen. Außerdem würde zur Vorbereitung der Umsetzung ein angemessener Übergangszeitraum von 24 Monaten vorgesehen, damit die betroffenen Märkte Zeit für die Vorbereitung haben und gleichzeitig eine klare Zielrichtung für FuE-Investitionen bekommen. Etwaige Befolgungskosten für die Unternehmen würden durch die Vorteile aufgewogen, die ein höheres Sicherheitsniveau der Produkte mit digitalen Elementen und letztlich ein höheres Vertrauen der Nutzer in diese Produkte mit sich bringen.

- **Wahl des Instruments**

Ein regulatorisches Eingreifen würde den Erlass einer Verordnung und nicht einer Richtlinie erforderlich machen, denn bei dieser besonderen Art von Produktvorschriften lassen sich mit einer Verordnung die festgestellten Probleme wirksamer angehen und die gesetzten Ziele effektiver erreichen, da es sich um einen Eingriff handelt, mit dem die Bedingungen für das Inverkehrbringen einer sehr breiten Kategorie von Produkten auf dem Binnenmarkt geregelt werden. Im Falle einer Richtlinie könnte der Umsetzungsprozess für ein solches Eingreifen zu viel Ermessensspielraum auf nationaler Ebene belassen, was möglicherweise zu einer mangelnden Einheitlichkeit bestimmter grundlegender Cybersicherheitsanforderungen, Rechtsunsicherheit, einer weiteren Fragmentierung oder sogar diskriminierenden grenzübergreifenden Situationen führen könnte, zumal die erfassten Produkte zu unterschiedlichen Zwecken verwendet werden könnten und die Hersteller mehrere Kategorien solcher Produkte herstellen können.

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

- **Konsultation der Interessenträger**

Die Kommission hat eine Vielzahl verschiedener Interessenträger konsultiert. Die Mitgliedstaaten und Interessenträger wurden aufgefordert, sich an der öffentlichen Konsultation sowie an den Umfragen und Workshops zu beteiligen, die im Rahmen einer Studie veranstaltet wurden, die von einem Konsortium zur Unterstützung der

Vorbereitungsarbeiten der Kommission für die Folgenabschätzung durchgeführt wurden, nämlich von Wavestone, Zentrum für Europäische Politische Studien (CEPS und ICF). Zu den konsultierten Interessenträgern gehörten nationale Marktüberwachungsbehörden, mit Cybersicherheit befasste Unionseinrichtungen, Hardware- und Software-Hersteller, Einführer und Händler von Hard- und Software, Wirtschaftsverbände, Verbraucherorganisationen und Nutzer von Produkten mit digitalen Elementen sowie Bürgerinnen und Bürger, Forscher und Hochschulen, notifizierte Stellen und Akkreditierungsstellen sowie Fachkreise der Cybersicherheitsbranche.

Die Konsultationsmaßnahmen umfassten Folgendes:

- Eine erste Studie wurde von einem Konsortium aus ICF, Wavestone, Carsa und CEPS durchgeführt und im Dezember 2021 veröffentlicht[11]. Darin wurden mehrere Arten von Marktversagen festgestellt und mögliche Regulierungsmaßnahmen untersucht.
- Es wurde eine öffentliche Konsultation durchgeführt, die sich an Bürgerinnen und Bürger, Interessenträger und Cybersicherheitsexperten richtete. Darauf gingen 176 Antworten ein. Diese trugen zur Erfassung verschiedener Meinungen und Erfahrungen aus allen Interessengruppen bei.
- Es wurden Workshops im Rahmen der Studie zur Unterstützung der Vorbereitungsarbeiten der Kommission für ein Cyberresilienzgesetz organisiert, an denen rund 100 Vertreter aus allen 27 Mitgliedstaaten teilnahmen, die eine Vielzahl von Interessenträgern vertraten.
- Es wurden Expertenbefragungen durchgeführt, um ein tieferes Verständnis der aktuellen Cybersicherheitsprobleme im Zusammenhang mit Produkten mit digitalen Elementen zu gewinnen und Politikoption für mögliche Regulierungsmaßnahmen zu erörtern.
- Es fanden bilaterale Gespräche mit nationalen Cybersicherheitsbehörden, dem Privatsektor und Verbraucherorganisationen statt.
- Wichtige KMU-Akteure wurden gezielt angesprochen.

- **Einholung und Nutzung von Expertenwissen**

Mit den Konsultationstätigkeiten sollten auf der Grundlage der EU-Leitlinien für eine bessere Rechtsetzung Beiträge zu den fünf wichtigsten Bewertungskriterien (Wirksamkeit, Effizienz, Relevanz, Kohärenz, EU-Mehrwert) sowie zu den potenziellen Auswirkungen möglicher Optionen für die Zukunft eingeholt werden. Der Auftragnehmer wandte sich nicht nur an die Interessenträger, die von der vorgeschlagenen Verordnung unmittelbar betroffen wären, sondern konsultierte darüber hinaus ein breites Spektrum von Fachleuten im Bereich der Cybersicherheit.

- **Folgenabschätzung**

Die Kommission führte eine Folgenabschätzung für diesen Vorschlag durch, die vom Ausschuss für Regulierungskontrolle (RSB) der Kommission geprüft wurde. Am 6. Juli 2022

[11] Studie über die Notwendigkeit von Cybersicherheitsanforderungen für IKT-Produkte – Nr. 2020-0715, Abschlussbericht der Studie abrufbar unter https://digital-strategy.ec.europa.eu/en/library/study-need-cybersecurity-requirements-ict-products.

fand eine Sitzung mit dem RSB statt, in deren Folge dieser eine befürwortende Stellungnahme abgab. Die Folgenabschätzung wurde angepasst, um den Empfehlungen und Anmerkungen des RSB Rechnung zu tragen.

Die Kommission prüfte verschiedene Politikoptionen zur Erreichung des allgemeinen Ziels des Vorschlags.

- Nicht zwingendes Recht und freiwillige Maßnahmen (Option 1): Bei dieser Option gäbe es keine verbindlichen Regulierungsmaßnahmen. Stattdessen würde die Kommission Mitteilungen, Leitlinien, Empfehlungen und möglicherweise Verhaltenskodizes herausgeben, um freiwillige Maßnahmen zu fördern. Um das Fehlen horizontaler EU-Vorschriften auszugleichen, würden weiterhin freiwillige oder obligatorische nationale Regelungen geschaffen.
- Ad-hoc-Regulierung der Cybersicherheit materieller Produkte mit digitalen Elementen und entsprechender eingebetteter Software (Option 2): Diese Option brächte eine produktspezifische Ad-hoc-Regulierung mit sich, die darauf beschränkt wäre, die Cybersicherheitsanforderungen in den bereits bestehenden Rechtsvorschriften zu ergänzen oder zu ändern oder neue Rechtsvorschriften einzuführen, sobald neue Risiken entstünden, gegebenenfalls auch in Bezug auf nicht eingebettete Software.

Die Optionen 3 und 4 betreffen eine horizontale Regulierung mit verschiedenen Anwendungsbereichen und sind weitgehend an den Neuen Rechtsrahmen (NLF) angelehnt. In diesem Rahmen sind grundlegende Anforderungen als Voraussetzung für das Inverkehrbringen bestimmter Produkte auf dem Binnenmarkt festgelegt. Der NLF sieht in der Regel auch eine Konformitätsbewertung vor, d. h. das vom Hersteller durchgeführte Verfahren zum Nachweis, dass bestimmte Anforderungen an ein Produkt erfüllt werden.

- Gemischter Ansatz mit verbindlichen horizontalen Vorschriften für die Cybersicherheit materieller Produkte mit digitalen Elementen und der jeweiligen eingebetteten Software und einem abgestuften Ansatz für nicht eingebettete Software (Option 3): Diese Option umfasst eine Verordnung zur Einführung horizontaler Cybersicherheitsanforderungen für alle materiellen Produkte mit digitalen Elementen und darin eingebettete Software als Voraussetzung für das Inverkehrbringen und zwei Unteroptionen mit und ohne obligatorische Konformitätsbewertung durch Dritte (3i und 3ii). Nicht eingebettete Software würde nicht reguliert werden.
- Horizontale Regulierung zur Einführung von Cybersicherheitsanforderungen für eine breite Palette materieller und immaterieller digitaler Produkte und zugehöriger Dienste, einschließlich nicht eingebetteter Software (Option 4): Abgesehen vom Anwendungsbereich ähnelt diese Option der Option 3. Bei der Option 4 würde nicht eingebettete Software (mit zwei Unteroptionen: 4a) nur mit kritischer bzw. 4b) mit aller Software) in den Anwendungsbereich einer möglichen Verordnung einbezogen werden. Für jede Unteroption würden dieselben Unteroptionen zur Konformitätsbewertung in Betracht gezogen wie bei Option 3.

Die Option 4 (mit Unteroptionen, die alle Software abdecken und eine obligatorische Konformitätsbewertung kritischer Produkte durch Dritte vorsehen) ergab sich als bevorzugte Option auf der Grundlage der Bewertung der Wirksamkeit hinsichtlich der besonderen Ziele und der Effizienz im Hinblick auf das Kosten-Nutzen-Verhältnis. Diese Option würde die Festlegung spezifischer horizontaler Cybersicherheitsanforderungen für alle auf dem Binnenmarkt in Verkehr gebrachten oder bereitgestellten Produkte mit digitalen Elementen gewährleisten und wäre die einzige Option, die die gesamte digitale Lieferkette abdeckt. Eine

solche Regulierung würde auch nicht eingebettete Software erfassen, die häufig Schwachstellen aufweist, wodurch ein kohärenter Ansatz für alle Produkte mit digitalen Elementen und eine klare Verteilung der Verantwortlichkeiten der verschiedenen Wirtschaftsakteure gewährleistet würde.

Diese Politikoption bringt noch einen zusätzlichen Vorteil, weil sie auch Aspekte der Sorgfaltspflicht und des gesamten Lebenszyklus nach dem Inverkehrbringen der Produkte mit digitalen Elementen mit abdeckt, sodass unter anderem angemessene Informationen über die Sicherheitsunterstützung und die Bereitstellung von Sicherheitsaktualisierungen gewährleistet werden. Diese Politikoption würde auch die jüngste Überprüfung des NIS-Rahmens am wirksamsten ergänzen, da sie sicherstellt, dass die Voraussetzungen für eine erhöhte Sicherheit der Lieferkette geschaffen würden.

Die bevorzugte Option würde den verschiedenen Beteiligten erhebliche Vorteile bringen. Für Unternehmen würde sie abweichende Sicherheitsvorschriften für Produkte mit digitalen Elementen verhindern und die Kosten der Einhaltung der einschlägigen Rechtsvorschriften zur Cybersicherheit senken. Sie würde dazu beitragen, die Zahl der Cybervorfälle, die Kosten der Bewältigung von Sicherheitsvorfällen und die Rufschädigung zu verringern. Schätzungen zufolge könnte die Initiative für die gesamte EU eine Senkung der den Unternehmen durch Vorfälle entstehenden Kosten um etwa 180 bis 290 Mrd. EUR pro Jahr bewirken. Sie würde auch zu höheren Umsätzen infolge einer steigenden Nachfrage nach Produkten mit digitalen Elementen führen. Dies würde zudem den weltweiten Ruf der Unternehmen verbessern und eine wachsende Nachfrage auch außerhalb der EU nach sich ziehen. Für die Nutzer würde die bevorzugte Option die Transparenz der Sicherheitseigenschaften erhöhen und die Verwendung von Produkten mit digitalen Elementen erleichtern. Außerdem kämen die Verbraucher und Bürger so in den Genuss eines besseren Schutzes ihrer Grundrechte, z. B. im Hinblick auf die Privatsphäre und den Datenschutz.

Auf die Frage nach der Einschätzung der Wirksamkeit der Maßnahmen stimmten die Teilnehmer der öffentlichen Konsultation darin überein, dass die Option 4 die wirksamste Maßnahme wäre (4,08 auf einer Skala von 1 bis 5). Dazu gehören Verbraucherorganisationen (5,00), Befragte, die sich als Nutzer bezeichnen (4,22), notifizierte Stellen (4,17), Marktüberwachungsbehörden (5,00) und Hersteller von Produkten mit digitalen Elementen (3,85), einschließlich kleiner und mittlerer Unternehmen (4,05).

- **Effizienz der Rechtsetzung und Vereinfachung**

In diesem Vorschlag werden Anforderungen festgelegt, die für die Herstellung von Software und Hardware gelten sollen. Es ist nötig, für Rechtssicherheit zu sorgen und eine weitere Fragmentierung der produktbezogenen Cybersicherheitsanforderungen im Binnenmarkt zu vermeiden, wie die breite Unterstützung verschiedener Interessenträger für ein horizontales Eingreifen verdeutlicht hat. Mit dem Vorschlag wird der Regelungsaufwand, der den Herstellern durch mehrere Rechtsakte zur Produktsicherheit entsteht, so gering wie möglich gehalten. Durch die Angleichung an den NLF wird das Funktionieren der Maßnahme und ihre Durchsetzung verbessert. Mit dem Vorschlag wird der Ablauf des Schutzklauselverfahrens gestrafft, indem Hersteller und Mitgliedstaaten eingebunden werden, bevor die Kommission unterrichtet wird. Ein Großteil der Hersteller, die in den Anwendungsbereich des Vorschlags fallen, ist bereits mit der Funktionsweise des NLF vertraut, was zu dessen Verständnis und Umsetzung beitragen wird. Der Vorschlag wird das Vertrauen der Verbraucher und Unternehmen in Produkte mit digitalen Elementen fördern.

- **Grundrechte**

Alle Politikoptionen dürften bis zu einem gewissen Grad den Schutz der Grundrechte und Grundfreiheiten wie Privatsphäre, Schutz personenbezogener Daten, unternehmerische Freiheit, Schutz des Eigentums und Schutz der persönlichen Würde und Unversehrtheit verbessern. In dieser Hinsicht am wirksamsten wäre die bevorzugte Option 4, die eine horizontale Regulierung und einen breiten Anwendungsbereich vorsieht, weil sie mit größerer Wahrscheinlichkeit dazu beitragen würde, die Zahl und Schwere von Vorfällen, einschließlich Verletzungen des Schutzes personenbezogener Daten, zu verringern. Sie würde auch die Rechtssicherheit erhöhen und gleiche Wettbewerbsbedingungen für die Wirtschaftsakteure schaffen, das Vertrauen der Nutzer stärken und die Attraktivität von EU-Produkten mit digitalen Elementen insgesamt steigern, wodurch sie das Eigentum schützt und die Bedingungen für die Geschäftstätigkeit der Wirtschaftsakteure verbessern hilft.

Die horizontalen Cybersicherheitsanforderungen würden zur Sicherheit personenbezogener Daten beitragen, indem sie die Vertraulichkeit, Integrität und Verfügbarkeit von Informationen in Produkten mit digitalen Elementen schützen. Die Einhaltung dieser Anforderungen wird die Einhaltung der Sicherheitsanforderungen der Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung, DSGVO)[12] an die Verarbeitung personenbezogener Daten erleichtern. Der Vorschlag würde die Transparenz und die Informationen für die Nutzer verbessern, auch für jene Nutzer, die geringere Cybersicherheitskompetenzen haben mögen. Die Nutzer würden auch besser über die Risiken, Fähigkeiten und Beschränkungen von Produkten mit digitalen Elementen informiert, wodurch sie besser in die Lage versetzt würden, die nötigen Präventions- und Minderungsmaßnahmen zu ergreifen, um die Restrisiken zu verringern.

4. AUSWIRKUNGEN AUF DEN HAUSHALT

Die Agentur der Europäischen Union für Cybersicherheit (ENISA) wird Personalmittel im Umfang von 4,5 VZÄ umverteilen müssen, um die ihr im Rahmen dieser Verordnung übertragenen Aufgaben zu erfüllen. Die Kommission müsste 7 VZÄ bereitstellen, um ihre Zuständigkeiten im Zusammenhang mit der Durchsetzung dieser Verordnung wahrzunehmen.

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

5. WEITERE ANGABEN

- **Durchführungspläne sowie Monitoring-, Bewertungs- und Berichterstattungsmodalitäten**

Die Kommission wird die Durchführung, Anwendung und Einhaltung dieser neuen Bestimmungen überwachen, um auch deren Wirksamkeit zu bewerten. Die Verordnung sieht eine Bewertung und Überprüfung durch die Kommission sowie die Übermittlung eines entsprechenden öffentlichen Berichts an das Europäische Parlament und den Rat vor, und zwar 36 Monate nach dem Datum des Geltungsbeginns und danach alle vier Jahre.

[12] 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).

- **Ausführliche Erläuterung einzelner Bestimmungen des Vorschlags**

Allgemeine Bestimmungen (Kapitel I)

Die vorgeschlagene Verordnung enthält a) Vorschriften für das Inverkehrbringen von Produkten mit digitalen Elementen, um die Cybersicherheit solcher Produkte zu gewährleisten; b) grundlegende Anforderungen an die Konzeption, Entwicklung und Herstellung von Produkten mit digitalen Elementen sowie Pflichten der Wirtschaftsakteure in Bezug auf diese Produkte hinsichtlich der Cybersicherheit; c) grundlegende Anforderungen an die von den Herstellern festgelegten Verfahren zur Behandlung von Schwachstellen, um die Cybersicherheit von Produkten mit digitalen Elementen während ihres gesamten Lebenszyklus zu gewährleisten, sowie Pflichten der Wirtschaftsakteure in Bezug auf diese Verfahren; d) Vorschriften für die Marktüberwachung und die Durchsetzung der oben genannten Vorschriften und Anforderungen.

Die vorgeschlagene Verordnung wird für Produkte mit digitalen Elementen gelten, deren bestimmungsgemäße und vernünftigerweise vorhersehbare Verwendung eine direkte oder indirekte logische oder physische Datenverbindung mit einem Gerät oder Netz einschließt.

Die vorgeschlagene Verordnung wird nicht für Produkte mit digitalen Elementen gelten, die in den Anwendungsbereich der Verordnung (EU) 2017/745 [Medizinprodukte für den menschlichen Gebrauch und deren Zubehör] und der Verordnung (EU) 2017/746 [In-vitro-Diagnostika für den menschlichen Gebrauch und deren Zubehör] fallen, denn beide Verordnungen enthalten Anforderungen an solche Produkte, einschließlich Software, und allgemeine Pflichten der Hersteller, die sich auf den gesamten Produktlebenszyklus und die Konformitätsbewertungsverfahren erstrecken. Die vorgeschlagene Verordnung wird weder für Produkte mit digitalen Elementen gelten, die nach der Verordnung 2018/1139 [hohes einheitliches Niveau der Flugsicherheit] zertifiziert wurden, noch für Produkte, die unter die Verordnung (EU) 2019/2144 [Typgenehmigung von Kraftfahrzeugen und Kraftfahrzeuganhängern sowie von Systemen, Bauteilen und selbstständigen technischen Einheiten für diese Fahrzeuge] fallen.

Kritische Produkte mit digitalen Elementen unterliegen besonderen Konformitätsbewertungsverfahren und werden anhand des von ihnen ausgehenden Cybersicherheitsrisikos gemäß Anhang III in die Klassen I und II unterteilt, wobei die Klasse II ein höheres Risiko darstellt. Ein Produkt mit digitalen Elementen gilt als kritisch und wird daher unter Berücksichtigung der Auswirkungen potenzieller Cybersicherheitslücken, die in dem Produkt mit digitalen Elementen enthalten sind, in Anhang III aufgenommen. Bei der Bestimmung des Cybersicherheitsrisikos werden die Cybersicherheitsfunktion des Produkts mit digitalen Elementen und dessen bestimmungsgemäße Verwendung in sensiblen Umgebungen wie einem industriellen Umfeld berücksichtigt.

Der Kommission wird überdies die Befugnis übertragen, delegierte Rechtsakte zur Ergänzung dieser Verordnung zu erlassen, um Kategorien hochkritischer Produkte mit digitalen Elementen festzulegen, für die die Hersteller ein europäisches Cybersicherheitszertifikat im Rahmen eines europäischen Systems für die Cybersicherheitszertifizierung erlangen müssen, um die Konformität mit den grundlegenden Anforderungen in Anhang I oder Teilen davon nachzuweisen. Bei der Festlegung solcher Kategorien hochkritischer Produkte mit digitalen Elementen berücksichtigt die Kommission das mit der Kategorie der Produkte mit digitalen Elementen verbundene Cybersicherheitsrisiko im Lichte eines oder mehrerer der Kriterien, die für die Auflistung der kritischen Produkte mit digitalen Elementen in Anhang III maßgeblich sind, sowie im Hinblick auf die Bewertung, ob Produkte dieser Produktkategorie von wesentlichen Einrichtungen der in Anhang [Anhang I] der Richtlinie

[Richtlinie XXX/XXXX (NIS2)] genannten Art verwendet werden oder diese von solchen Produkten abhängen oder solche Produkte möglicherweise künftig für die Tätigkeiten dieser Einrichtungen von Bedeutung sein werden oder ob sie für die Widerstandsfähigkeit der gesamten Lieferkette von Produkten mit digitalen Elementen gegen Störungen von Bedeutung sind.

Pflichten der Wirtschaftsakteure (Kapitel II)

Der Vorschlag enthält Pflichten für Hersteller, Einführer und Händler, die auf den Referenzbestimmungen des Beschlusses Nr. 768/2008/EG beruhen. Entsprechend den grundlegenden Cybersicherheitsanforderungen und Pflichten dürfen alle Produkte mit digitalen Elementen nur dann auf dem Markt bereitgestellt werden, wenn sie bei ordnungsgemäßer Lieferung, Installation und Wartung und bei bestimmungsgemäßer oder vernünftigerweise vorhersehbarer Verwendung den grundlegenden Cybersicherheitsanforderungen dieser Verordnung genügen.

Entsprechend den grundlegenden Anforderungen und Pflichten müssen die Hersteller die Cybersicherheit bei der Konzeption, Entwicklung und Herstellung von Produkten mit digitalen Elementen durchgehend berücksichtigen, hinsichtlich der Sicherheitsaspekte bei der Konzeption und Entwicklung ihrer Produkte die gebotene Sorgfalt walten lassen, im Hinblick auf Cybersicherheitsaspekte, die den Kunden mitgeteilt werden müssen, transparent sein, die Sicherheitsunterstützung (Aktualisierungen) auf verhältnismäßige Weise gewährleisten und die Anforderungen an die Behandlung von Schwachstellen einhalten.

Die Pflichten im Zusammenhang mit dem Inverkehrbringen von Produkten mit digitalen Elementen sollen den Wirtschaftsakteuren – von Herstellern bis hin zu Händlern und Einführern – in einem angemessenen Verhältnis zu ihrer Rolle und Verantwortung in der Lieferkette auferlegt werden.

Konformität des Produkts mit digitalen Elementen (Kapitel III)

Bei Produkten mit digitalen Elementen, die mit harmonisierten Normen oder Teilen davon übereinstimmen, deren Fundstellen im *Amtsblatt der Europäischen Union* veröffentlicht worden sind, wird eine Konformität mit den grundlegenden Anforderungen dieser vorgeschlagenen Verordnung vermutet. Wenn es keine harmonisierten Normen gibt oder diese unzureichend sind oder wenn unangemessene Verzögerungen im Normungsverfahren auftreten oder der Normungsauftrag der Kommission von den europäischen Normungsorganisationen abgelehnt wird, kann die Kommission im Wege von Durchführungsrechtsakten gemeinsame Spezifikationen annehmen.

Überdies wird bei Produkten mit digitalen Elementen, die im Rahmen eines europäischen Systems für die Cybersicherheitszertifizierung gemäß der Verordnung (EU) 2019/881 zertifiziert worden sind oder für die eine EU-Konformitätserklärung oder ein EU-Zertifikat ausgestellt wurde, für welche die Kommission im Wege eines Durchführungsrechtsakts festgelegt hat, dass sie eine Konformitätsvermutung für diese Verordnung begründen können, davon ausgegangen, dass die Produkte den grundlegenden Anforderungen dieser Verordnung oder Teilen genügen, sofern die EU-Konformitätserklärung oder das Cybersicherheitszertifikat oder Teile davon diese Anforderungen abdecken.

Um einen übermäßigen Verwaltungsaufwand für die Hersteller zu vermeiden, sollte die Kommission darüber hinaus gegebenenfalls angeben, ob mit einem im Rahmen eines solchen europäischen Systems für die Cybersicherheitszertifizierung ausgestellten Cybersicherheitszertifikat die in dieser Verordnung vorgesehene Pflicht der Hersteller, für die betreffenden Anforderungen eine Konformitätsbewertung durch Dritte durchführen zu lassen, aufgehoben werden kann.

Zum Nachweis, dass die grundlegenden Anforderungen in Anhang I erfüllt sind, muss der Hersteller das Produkt mit digitalen Elementen und die von ihm festgelegten Verfahren zur Behandlung von Schwachstellen einer Konformitätsbewertung nach einem der in Anhang VI genannten Verfahren unterziehen. Hersteller kritischer Produkte der Klassen I und II müssen dazu die jeweiligen Module anwenden, die für die Konformität erforderlich sind. Hersteller kritischer Produkte der Klasse II müssen einen Dritten in ihre Konformitätsbewertung einbeziehen.

Notifizierung von Konformitätsbewertungsstellen (Kapitel IV)

Der ordnungsgemäßen Arbeitsweise der notifizierten Stellen kommt eine entscheidende Bedeutung für die Gewährleistung eines hohen Maßes an Cybersicherheit und für das Vertrauen aller interessierten Kreise in das System nach dem neuen Konzept zu. Aus diesem Grund enthält der Vorschlag in Übereinstimmung mit dem Beschluss Nr. 768/2008/EG Anforderungen an die nationalen Behörden, die für die Konformitätsbewertungsstellen (notifizierten Stellen) zuständig sind. Die endgültige Verantwortung für die Benennung und Überwachung der notifizierten Stellen verbleibt bei den Mitgliedstaaten. Die Mitgliedstaaten benennen eine notifizierende Behörde, die für die Einrichtung und Durchführung der erforderlichen Verfahren für die Bewertung und Notifizierung von Konformitätsbewertungsstellen und für die Überwachung der notifizierten Stellen zuständig ist.

Marktüberwachung und Durchsetzung (Kapitel V)

Nach der Verordnung (EU) 2019/1020 führen die nationalen Marktüberwachungsbehörden die Marktüberwachung im Hoheitsgebiet des jeweiligen Mitgliedstaats durch. Die Mitgliedstaaten können beschließen, eine bestehende oder eine neue Behörde als Marktüberwachungsbehörde zu benennen, einschließlich der in Artikel [Artikel X] der Richtlinie [Richtlinie XXX/XXXX (NIS2)] genannten zuständigen nationalen Behörden oder der in Artikel 58 der Verordnung (EU) 2019/881 genannten benannten nationalen Behörden für die Cybersicherheitszertifizierung. Die Wirtschaftsakteure sollten umfassend mit den Marktüberwachungsbehörden und anderen zuständigen Behörden zusammenarbeiten.

Übertragene Befugnisse und Ausschussverfahren (Kapitel VI)

Damit der Rechtsrahmen erforderlichenfalls angepasst werden kann, sollte der Kommission die Befugnis übertragen werden, gemäß Artikel 290 AEUV Rechtsakte zu erlassen, um die Liste kritischer Produkte der Klassen I und II zu aktualisieren und die Definitionen dieser Produkte festzulegen, um ferner festzulegen, ob eine Einschränkung oder ein Ausschluss für Produkte mit digitalen Elementen notwendig wäre, die unter andere Unionsvorschriften mit Anforderungen fallen, mit denen dasselbe Schutzniveau wie mit dieser Verordnung erreicht wird, um die Zertifizierung bestimmter hochkritischer Produkte mit digitalen Elementen auf der Grundlage der in dieser Verordnung festgelegten Kriterien vorzuschreiben, um die Mindestangaben der EU-Konformitätserklärung und die Ergänzung der in die technische Dokumentation aufzunehmenden Elemente vorzuschreiben.

Der Kommission wird die Befugnis übertragen, Durchführungsrechtsakte zu erlassen, die Folgendes betreffen: Festlegung des Formats oder der Elemente der Meldepflichten und der Software-Stückliste; Ausweisung der europäischen Systeme für die Cybersicherheitszertifizierung, die zum Nachweis der Konformität mit den grundlegenden Anforderungen dieser Verordnung oder Teilen davon verwendet werden können; Annahme gemeinsamer Spezifikationen; Festlegung technischer Spezifikationen für die Anbringung der CE-Kennzeichnung; Annahme von Korrekturmaßnahmen oder einschränkenden Maßnahmen

auf Unionsebene unter außergewöhnlichen Umständen, die ein sofortiges Eingreifen rechtfertigen, um das reibungslose Funktionieren des Binnenmarkts zu bewahren.

Vertraulichkeit und Sanktionen (Kapitel VII)

Alle Parteien, die diese Verordnung anwenden, müssen die Vertraulichkeit der Informationen und Daten wahren, von denen sie in Ausübung ihrer Aufgaben und Tätigkeiten Kenntnis erlangen.

Um die wirksame Durchsetzung der in dieser Verordnung festgelegten Pflichten zu gewährleisten, sollte jede Marktüberwachungsbehörde befugt sein, Geldbußen aufzuerlegen oder ihre Auferlegung zu beantragen. Dafür werden in dieser Verordnung Obergrenzen für Geldbußen festgelegt, die in den einzelstaatlichen Rechtsvorschriften für Verstöße gegen die in dieser Verordnung festgelegten Pflichten vorgesehen werden sollten.

Übergangs- und Schlussbestimmungen (Kapitel VIII)

Damit Hersteller, notifizierte Stelle und Mitgliedstaaten genügend Zeit haben, um sich auf die neuen Anforderungen einzustellen, soll der Geltungsbeginn der vorgeschlagenen Verordnung [24 Monate] nach ihrem Inkrafttreten liegen, mit Ausnahme der Meldepflichten der Hersteller, die schon ab dem [12 Monate] nach dem Inkrafttreten gelten würden.

2022/0272 (COD)

Vorschlag für eine

VERORDNUNG DES EUROPÄISCHEN PARLAMENTS UND DES RATES

über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen und zur Änderung der Verordnung (EU) 2019/1020

(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 Artikel 114,

auf Vorschlag der Europäischen Kommission,

nach Zuleitung des Entwurfs des Gesetzgebungsakts an die nationalen Parlamente,

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

nach Stellungnahme des Ausschusses der Regionen[2],

gemäß dem ordentlichen Gesetzgebungsverfahren,

in Erwägung nachstehender Gründe:

(1) Es ist nötig, das Funktionieren des Binnenmarkts zu verbessern und dazu einen einheitlichen Rechtsrahmen für grundlegende Cybersicherheitsanforderungen für das Inverkehrbringen von Produkten mit digitalen Elementen auf dem Unionsmarkt festzulegen. Dabei sollten zwei große Probleme angegangen werden, die hohe Kosten für die Nutzer und die Gesellschaft verursachen: ein geringes Maß an Cybersicherheit von Produkten mit digitalen Elementen, das sich in weitverbreiteten Schwachstellen und der unzureichenden und inkohärenten Bereitstellung von Sicherheitsaktualisierungen zu deren Behebung widerspiegelt, sowie ein unzureichendes Verständnis und ein mangelnder Informationszugang der Nutzer, wodurch sie daran gehindert werden, Produkte mit angemessenen Cybersicherheitsmerkmalen auszuwählen oder sicher zu verwenden.

(2) Mit dieser Verordnung sollen die Rahmenbedingungen für die Entwicklung sicherer Produkte mit digitalen Elementen geschaffen werden, damit Hardware- und Softwareprodukte mit weniger Schwachstellen in Verkehr gebracht werden und damit die Hersteller sich während des gesamten Lebenszyklus eines Produkts ernsthaft um die Sicherheit kümmern. Außerdem sollen Bedingungen geschaffen werden, die es den Nutzern ermöglichen, bei der Auswahl und Verwendung von Produkten mit digitalen Elementen die Cybersicherheit zu berücksichtigen.

(3) Das derzeit geltende einschlägige Unionsrecht umfasst mehrere horizontale Vorschriften, die bestimmte Aspekte der Cybersicherheit aus unterschiedlichen

[1] ABl. C … vom …, S. ….
[2] ABl. C … vom …, S. ….

Blickwinkeln regeln, darunter auch Maßnahmen zur Erhöhung der Sicherheit der digitalen Lieferkette. Das bestehende Unionsrecht in Bezug auf die Cybersicherheit, wozu die [Richtlinie XXX/XXXX (NIS2)] und die Verordnung (EU) 2019/881 des Europäischen Parlaments und des Rates[3], gehören, enthält jedoch keine unmittelbar verbindlichen Anforderungen an die Sicherheit von Produkten mit digitalen Elementen.

(4) Die bestehenden Rechtsvorschriften der Union gelten zwar für bestimmte Produkte mit digitalen Elementen, jedoch gibt es keinen horizontalen Rechtsrahmen der Union, der umfassende Cybersicherheitsanforderungen für alle Produkte mit digitalen Elementen festlegen würde. Die verschiedenen bisher auf Unionsebene und auf nationaler Ebene erlassenen Vorschriften und ergriffenen Initiativen befassen sich nur teilweise mit den festgestellten Problemen und Risiken im Zusammenhang mit der Cybersicherheit, wodurch ein legislativer Flickenteppich innerhalb des Binnenmarkts entstanden ist, der zu einer größeren Rechtsunsicherheit sowohl für die Hersteller als auch für die Nutzer solcher Produkte und zu einer größeren unnötigen Belastung der Unternehmen führt, die eine Reihe verschiedener Anforderungen in Bezug auf ähnliche Produktarten zu erfüllen haben. Die Cybersicherheit dieser Produkte hat eine besonders ausgeprägte grenzüberschreitende Dimension, weil die in einem Land hergestellten Produkte häufig von Organisationen und Verbrauchern im gesamten Binnenmarkt verwendet werden. Dies macht es notwendig, den Bereich auf Unionsebene zu regulieren. Das Regulierungsumfeld der Union sollte durch die Einführung von Cybersicherheitsanforderungen für Produkte mit digitalen Elementen harmonisiert werden. Überdies gilt es, Rechtssicherheit für die Akteure und Nutzer in der gesamten Union herzustellen und eine bessere Harmonisierung des Binnenmarkts zu erreichen, wodurch auch bessere Bedingungen für Wirtschaftsteilnehmer geschaffen würden, die in den Unionsmarkt eintreten wollen.

(5) Auf Unionsebene wurden in verschiedenen programmatischen und politischen Papieren wie der EU-Cybersicherheitsstrategie für die digitale Dekade[4], den Schlussfolgerungen des Rates vom 2. Dezember 2020 und 23. Mai 2022 oder der Entschließung des Europäischen Parlaments vom 10. Juni 2021[5] besondere Cybersicherheitsanforderungen der Union für digitale oder vernetzte Produkte verlangt. Gleichzeitig haben mehrere Länder weltweit Maßnahmen ergriffen, um dieses Problem auf eigene Initiative anzugehen. Im Abschlussbericht der Konferenz zur Zukunft Europas[6] forderten die Bürgerinnen und Bürger „eine stärkere Rolle der EU bei der Abwehr von Cybersicherheitsbedrohungen“.

(6) Um das Gesamtniveau der Cybersicherheit aller im Binnenmarkt in Verkehr gebrachten Produkte mit digitalen Elementen zu erhöhen, müssen für diese Produkte

---

3 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).

4 JOIN(2020) 18 final, https://eur-lex.europa.eu/legal-content/DE/ALL/?uri=JOIN:2020:18:FIN.

5 2021/2568(RSP), https://www.europarl.europa.eu/doceo/document/TA-9-2021-0286_DE.html.

6 *Konferenz zur Zukunft Europas – Bericht über das endgültige Ergebnis*, Mai 2022, Vorschlag 28 Absatz 2. Die Konferenz fand von April 2021 bis Mai 2022 statt. Dabei handelte es sich um eine einzigartige, von Bürgerinnen und Bürgern getragene Initiative der deliberativen Demokratie auf gesamteuropäischer Ebene, an der Tausende Europäerinnen und Europäer sowie politische Akteure, Sozialpartner, Vertreterinnen und Vertreter der Zivilgesellschaft und wichtige Interessenträger beteiligt waren.

objektive und technologieneutrale grundlegende Cybersicherheitsanforderungen eingeführt werden, die dann horizontal gelten sollen.

(7) Alle Produkte mit digitalen Elementen, die in ein größeres elektronisches Informationssystem integriert oder mit ihm verbunden sind, können unter bestimmten Umständen böswilligen Akteuren als Angriffsvektor dienen. Folglich kann selbst eine als weniger kritisch geltende Hardware und Software die anfängliche Kompromittierung eines Geräts oder Netzes erleichtern und es böswilligen Akteuren ermöglichen, sich privilegierten Zugang zu einem System zu verschaffen oder sich quer von System zu System zu bewegen. Die Hersteller sollten daher dafür sorgen, dass alle verbindungsfähigen Produkte mit digitalen Elementen im Einklang mit den in dieser Verordnung festgelegten grundlegenden Anforderungen konzipiert und entwickelt werden. Dazu gehören sowohl Produkte, die physisch über Hardware-Schnittstellen verbunden werden können, als auch Produkte, die logisch verbunden werden, z. B. über Netzwerksockets, Pipes, Dateien, Anwendungsprogrammierschnittstellen oder andere Arten von Software-Schnittstellen. Da sich Cybersicherheitsbedrohungen über verschiedene Produkte mit digitalen Elementen verbreiten können, ehe ein bestimmtes Ziel erreicht wird, z. B. durch Verkettung mehrerer ausnutzbarer Schwachstellen, sollten die Hersteller auch die Cybersicherheit jener Produkte gewährleisten, die nur indirekt mit anderen Geräten oder Netzen verbunden sind.

(8) Durch die Festlegung von Cybersicherheitsanforderungen für das Inverkehrbringen von Produkten mit digitalen Elementen wird die Cybersicherheit dieser Produkte gleichermaßen sowohl für Verbraucher als auch für Unternehmen verbessert. Dies betrifft auch Anforderungen für das Inverkehrbringen von Verbraucherprodukten mit digitalen Elementen, die für schutzbedürftige Verbraucher bestimmt sind, wie z. B. Spielzeug und Babymonitore.

(9) Diese Verordnung gewährleistet ein hohes Niveau der Cybersicherheit von Produkten mit digitalen Elementen. Sie enthält keine Vorschriften für Dienstleistungen wie *Software-as-a-Service* (SaaS), mit Ausnahme von Datenfernverarbeitungslösungen, die sich auf ein Produkt mit digitalen Elementen beziehen und als entfernt stattfindende Datenverarbeitung verstanden werden, für die eine Software vom Hersteller selbst oder unter dessen Verantwortung konzipiert und entwickelt wird und ohne die das Produkt mit digitalen Elementen eine seiner Funktionen nicht erfüllen könnte. Mit der [Richtlinie XXX/XXXX (NIS2)] werden Anforderungen an die Cybersicherheit und die Meldung von Sicherheitsvorfällen für wesentliche und wichtige Einrichtungen wie kritische Infrastrukturen festgelegt, um die Resilienz der von ihnen erbrachten Dienste zu erhöhen. Die [Richtlinie XXX/XXXX (NIS2)] gilt für Cloud-Computing-Dienste und Cloud-Dienstmodelle wie SaaS. In den Anwendungsbereich dieser Richtlinie fallen alle Einrichtungen, die Cloud-Computing-Dienste in der Union erbringen und den Schwellenwert für mittlere Unternehmen erreichen oder überschreiten.

(10) Um die Innovation oder die Forschung nicht zu behindern, sollte freie und quelloffene Software, die außerhalb einer Geschäftstätigkeit entwickelt oder bereitgestellt wird, nicht unter diese Verordnung fallen. Dies gilt insbesondere für offen geteilte und frei zugängliche, nutzbare, veränderbare und weiterverteilbare Software, einschließlich ihres Quellcodes und ihrer veränderten Versionen. Im Zusammenhang mit Software ist eine Geschäftstätigkeit möglicherweise nicht nur dadurch gekennzeichnet, dass für ein Produkt ein Preis verlangt wird, sondern auch dadurch, dass für technische Unterstützungsleistungen ein Entgelt verlangt wird, dass eine Softwareplattform

bereitgestellt wird, über die der Hersteller andere Dienste monetisiert, oder dass personenbezogene Daten zu anderen Zwecken als der alleinigen Verbesserung der Sicherheit, Kompatibilität oder Interoperabilität der Software verwendet werden.

(11) Ein sicheres Internet ist für das Funktionieren kritischer Infrastrukturen und für die Gesellschaft insgesamt unverzichtbar. Die [Richtlinie XXX/XXXX (NIS2)] zielt darauf ab, ein hohes Maß an Cybersicherheit der Dienste wesentlicher und wichtiger Einrichtungen zu gewährleisten, zu denen auch die Betreiber digitaler Infrastrukturen zählen, die Kernfunktionen des offenen Internets unterstützen und den Internetzugang und Internetdienste gewährleisten. Deshalb ist es wichtig, dass die Produkte mit digitalen Elementen, die erforderlich sind, damit die Betreiber digitaler Infrastrukturen das Funktionieren des Internets gewährleisten können, auf sichere Weise entwickelt werden und dass sie den etablierten Internetsicherheitsstandards entsprechen. Diese Verordnung, die für alle verbindungsfähigen Hardware- und Softwareprodukte gilt, zielt auch darauf ab, den Betreibern digitaler Infrastrukturen die Einhaltung der Anforderungen der [Richtlinie XXX/XXXX (NIS2)] an die Lieferketten zu erleichtern, indem sichergestellt wird, dass die Produkte mit digitalen Elementen, die sie für die Erbringung ihrer Dienste verwenden, auf sichere Weise entwickelt werden und dass sie rechtzeitig Sicherheitsaktualisierungen für solche Produkte erhalten.

(12) Die Verordnung (EU) 2017/745 des Europäischen Parlaments und des Rates[7] enthält Vorschriften für Medizinprodukte und die Verordnung (EU) 2017/746 des Europäischen Parlaments und des Rates[8] enthält Vorschriften für In-vitro-Diagnostika. Beide Verordnungen dienen der Bewältigung von Cybersicherheitsrisiken und folgen besonderen Ansätzen, die auch dieser Verordnung zugrunde liegen. Insbesondere enthalten die Verordnungen (EU) 2017/745 und (EU) 2017/746 grundlegende Anforderungen an Medizinprodukte, die mittels eines elektronischen Systems funktionieren oder die selbst Software sind. Bestimmte nicht eingebettete Software und der gesamte Lebenszyklusansatz werden ebenfalls von diesen Verordnungen erfasst. Nach diesen Anforderungen müssen die Hersteller bei der Entwicklung und Konstruktion ihrer Produkte Risikomanagementgrundsätze anwenden und dazu Anforderungen an IT-Sicherheitsmaßnahmen sowie entsprechende Konformitätsbewertungsverfahren festlegen. Darüber hinaus gibt es seit Dezember 2019 spezifische Leitlinien zur Cybersicherheit von Medizinprodukten, die den Herstellern von Medizinprodukten und In-vitro-Diagnostika Orientierungen für die Einhaltung aller einschlägigen grundlegenden Anforderungen in Anhang I dieser Verordnungen in Bezug auf die Cybersicherheit an die Hand geben[9]. Produkte mit digitalen Elementen, die unter eine dieser Verordnungen fallen, sollten daher nicht von der vorliegenden Verordnung erfasst werden.

---

7 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).

8 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).

9 MDCG 2019-16, gebilligt von der gemäß Artikel 103 der Verordnung (EU) 2017/745 eingesetzten Koordinierungsgruppe Medizinprodukte (MDCG).

(13) Mit der Verordnung (EU) 2019/2144 des Europäischen Parlaments und des Rates[10] sind Anforderungen an die Typgenehmigung von Kraftfahrzeugen sowie von Systemen und Bauteilen für diese Fahrzeuge festgelegt und bestimmte Cybersicherheitsanforderungen eingeführt worden, auch in Bezug auf den Betrieb eines zertifizierten Cybersicherheitsmanagementsystems, Software-Aktualisierungen, welche die Strategien und Verfahren der Organisationen für den Umgang mit Cybersicherheitsrisiken über dem gesamten Lebenszyklus von Fahrzeugen, Ausrüstungen und Diensten im Einklang mit den geltenden Regelungen der Vereinten Nationen über technische Spezifikationen und Cybersicherheit[11] umfassen und spezifische Konformitätsbewertungsverfahren vorsehen. Im Bereich der Luftfahrt besteht das Hauptziel der Verordnung (EU) 2018/1139 des Europäischen Parlaments und des Rates[12] in der Festlegung und Aufrechterhaltung eines hohen einheitlichen Niveaus der Flugsicherheit in der Union. Die Verordnung schafft einen Rahmen für grundlegende Anforderungen an die Lufttüchtigkeit luftfahrttechnischer Erzeugnisse, Teile und Ausrüstungen, einschließlich Software, die den Pflichten zum Schutz vor Bedrohungen der Informationssicherheit Rechnung tragen. Produkte mit digitalen Elementen, die unter die Verordnung (EU) 2019/2144 fallen, und Produkte, die nach der Verordnung (EU) 2018/1139 zertifiziert worden sind, unterliegen daher nicht den in der vorliegenden Verordnung festgelegten grundlegenden Anforderungen und Konformitätsbewertungsverfahren. Das Zertifizierungsverfahren nach der Verordnung (EU) 2018/1139 gewährleistet die mit der vorliegenden Verordnung angestrebte Vertrauenswürdigkeit.

(14) In dieser Verordnung werden horizontale Cybersicherheitsvorschriften festgelegt, die nicht speziell für bestimmte Sektoren oder bestimmte Produkte mit digitalen Elementen gelten sollen. Dennoch könnten sektor- oder produktspezifische Unionsvorschriften mit denen Anforderungen eingeführt werden, die sich auf alle oder einige der Risiken beziehen, die von den in dieser Verordnung festgelegten grundlegenden Anforderungen abgedeckt werden. Die Anwendung dieser Verordnung auf Produkte mit digitalen Elementen, die unter andere Unionsvorschriften mit Anforderungen in Bezug auf alle oder einige der von den grundlegenden Anforderungen in Anhang I dieser Verordnung abgedeckten Risiken fallen, kann in

---

10 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).

11 UN-Regelung Nr. 155 – Einheitliche Bedingungen für die Genehmigung von Fahrzeugen hinsichtlich der Cybersicherheit und des Cybersicherheitsmanagementsystems [2021/387].

12 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).

solchen Fällen eingeschränkt oder ausgeschlossen werden, sofern die Einschränkung oder der Ausschluss mit dem für diese Produkte geltenden allgemeinen Rechtsrahmen vereinbar ist und mit den sektorspezifischen Vorschriften dasselbe Schutzniveau erreicht wird, wie es diese Verordnung gewährleistet. Der Kommission wird die Befugnis übertragen, delegierte Rechtsakte zur Änderung dieser Verordnung im Hinblick auf die Festlegung solcher Produkte und Vorschriften zu erlassen. In Bezug auf bestehende Rechtsvorschriften der Union, für die solche Einschränkungen oder Ausschlüsse gelten sollten, enthält diese Verordnung besondere Bestimmungen, um ihr Verhältnis zu diesen Rechtsvorschriften der Union zu präzisieren.

(15) Nach der Delegierten Verordnung (EU) 2022/30 gelten die grundlegenden Anforderungen gemäß Artikel 3 Absatz 3 Buchstabe d (schädliche Auswirkungen auf das Netz und missbräuchliche Nutzung von Netzressourcen), Buchstabe e (personenbezogene Daten und Privatsphäre) und Buchstabe f (Betrug) der Richtlinie 2014/53/EU für bestimmte Funkanlagen. Der [Durchführungsbeschluss XXX/2022 der Kommission über einen Normungsauftrag an die europäischen Normungsorganisationen] enthält Anforderungen für die Entwicklung spezifischer Normen, in denen präzisiert wird, wie diese drei grundlegenden Anforderungen zu behandeln sind. Die in dieser Verordnung festgelegten grundlegenden Anforderungen umfassen alle Elemente der grundlegenden Anforderungen gemäß Artikel 3 Absatz 3 Buchstaben d, e und f der Richtlinie 2014/53/EU. Darüber hinaus stehen die in dieser Verordnung festgelegten grundlegenden Anforderungen im Einklang mit den Zielen der Anforderungen an die spezifischen Normen, die in diesem Normungsauftrag vorgesehenen sind. Sollte die Kommission die Delegierte Verordnung (EU) 2022/30 aufheben oder ändern, sodass sie für bestimmte von der vorliegenden Verordnung erfasste Produkte nicht mehr gilt, so sollten daher dann die Kommission und die europäischen Normungsorganisationen bei der Ausarbeitung und Entwicklung harmonisierter Normen die Normungsarbeiten, die im Rahmen des Durchführungsbeschlusses C(2022) 5637 der Kommission über einen Normungsauftrag zur Delegierten Verordnung (EU) 2022/30 über Funkanlagen durchgeführt werden, berücksichtigen, um die Durchführung der vorliegenden Verordnung zu erleichtern.

(16) Die Richtlinie 85/374/EWG[13] wirkt ergänzend zu dieser Verordnung. Diese Richtlinie enthält Vorschriften über die Haftung für fehlerhafte Produkte, damit geschädigte Personen Schadenersatz verlangen können, wenn durch ein fehlerhaftes Produkt ein Schaden verursacht wurde. Darin wird der Grundsatz festgelegt, dass der Hersteller eines Produkts unabhängig vom Verschulden für Schäden haftet, die durch die mangelnde Sicherheit seines Produkts verursacht werden („verschuldensunabhängige Haftung“). Besteht ein solcher Mangel an Sicherheit in fehlenden Sicherheitsaktualisierungen nach dem Inverkehrbringen des Produkts und wird dadurch ein Schaden verursacht, könnte dies die Haftung des Herstellers nach sich ziehen. In dieser Verordnung sollten Pflichten der Hersteller in Bezug auf die Bereitstellung solcher Sicherheitsaktualisierungen festgelegt werden.

[13] 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).

(17) Die vorliegende Verordnung sollte unbeschadet der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates[14] gelten, die Bestimmungen zur Einführung von Datenschutz-Zertifizierungsverfahren und von Datenschutzsiegeln und -prüfzeichen enthält, die dem Nachweis dienen, dass die für die Datenverarbeitung Verantwortlichen und die Auftragsverarbeiter bei der Verarbeitung von Daten die Bestimmungen der letzteren Verordnung einhalten. Solche Vorgänge könnten in ein Produkt mit digitalen Elementen eingebettet werden. Die Grundsätze des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen sowie die Cybersicherheit im Allgemeinen sind Schlüsselelemente der Verordnung (EU) 2016/679. Durch den Schutz von Verbrauchern und Organisationen vor Cybersicherheitsrisiken sollen die in dieser Verordnung festgelegten grundlegenden Cybersicherheitsanforderungen auch dazu beitragen, den Schutz personenbezogener Daten und den Schutz der Privatsphäre natürlicher Personen zu verbessern. Sowohl bei der Normung als auch bei der Zertifizierung von Cybersicherheitsaspekten sollten Synergien im Rahmen der Zusammenarbeit zwischen der Kommission, den europäischen Normungsorganisationen, der Agentur der Europäischen Union für Cybersicherheit (ENISA), dem durch die Verordnung (EU) 2016/679 eingesetzten Europäischen Datenschutzausschuss (EDSA) und den nationalen Datenschutzaufsichtsbehörden berücksichtigt werden. Synergien zwischen dieser Verordnung und dem Datenschutzrecht der Union sollten auch im Bereich der Marktüberwachung und Rechtsdurchsetzung angestrebt werden. Dazu sollten die nach dieser Verordnung benannten nationalen Marktüberwachungsbehörden mit den Behörden zusammenarbeiten, die die Anwendung des Datenschutzrechtes der Union beaufsichtigen. Letztere Behörden sollten auch Zugang zu Informationen haben, die für die Erfüllung ihrer Aufgaben von Bedeutung sind.

(18) Soweit ihre Produkte in den Anwendungsbereich der vorliegenden Verordnung fallen, sollten die Aussteller von Brieftaschen für die europäische digitale Identität (EUid-Brieftaschen) gemäß Artikel [Artikel 6a Absatz 2 der Verordnung (EU) Nr. 910/2014, geändert durch den Vorschlag für eine Verordnung zur Änderung der Verordnung (EU) Nr. 910/2014 im Hinblick auf die Schaffung eines Rahmens für eine europäische digitale Identität] sowohl die in der vorliegenden Verordnung festgelegten horizontalen grundlegenden Anforderungen als auch die besonderen Sicherheitsanforderungen gemäß Artikel [Artikel 6a der Verordnung (EU) Nr. 910/2014, geändert durch den Vorschlag für eine Verordnung zur Änderung der Verordnung (EU) Nr. 910/2014 im Hinblick auf die Schaffung eines Rahmens für eine europäische digitale Identität] erfüllen. Um die Einhaltung der Vorschriften zu erleichtern, sollten Aussteller von EUid-Brieftaschen die Konformität der EUid-Brieftaschen mit den in beiden Verordnungen festgelegten Anforderungen dadurch nachweisen können, dass sie ihre Produkte im Rahmen eines europäischen Systems für die Cybersicherheitszertifizierung nach der Verordnung (EU) 2019/881 zertifizieren lassen, für das die Kommission im Wege eines Durchführungsrechtsakts eine Konformitätsvermutung für die Anforderungen der vorliegenden Verordnung festgelegt hat, soweit das Zertifikat oder Teile davon diese Anforderungen abdecken.

---

[14] 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).

(19) Bestimmte in dieser Verordnung vorgesehene Aufgaben sollten von der ENISA im Einklang mit Artikel 3 Absatz 2 der Verordnung (EU) 2019/881 wahrgenommen werden. Insbesondere sollte die ENISA Meldungen von Herstellern über aktiv ausgenutzte Schwachstellen in Produkten mit digitalen Elementen sowie über Vorfälle, die sich auf die Sicherheit dieser Produkte auswirken, entgegennehmen. Die ENISA sollte diese Meldungen auch an die zuständigen Computer-Notfallteams (CSIRTs) bzw. an die gemäß Artikel [Artikel X] der Richtlinie [Richtlinie XXX/XXXX (NIS2)] benannten zentralen Anlaufstellen der Mitgliedstaaten weiterleiten und die betreffenden Marktüberwachungsbehörden von den gemeldeten Schwachstellen unterrichten. Auf der Grundlage der von ihr erfassten Informationen sollte die ENISA alle zwei Jahre einen technischen Bericht über aufkommende Trends in Bezug auf Cybersicherheitsrisiken bei Produkten mit digitalen Elementen erstellen und ihn der in der Richtlinie [Richtlinie XXX/XXXX (NIS2)] genannten Kooperationsgruppe vorlegen. Darüber hinaus sollte die ENISA angesichts ihrer Sachkenntnis und ihres Auftrags in der Lage sein, den Prozess der Durchführung dieser Verordnung zu unterstützen. Sie sollte insbesondere in der Lage sein, gemeinsame Tätigkeiten vorzuschlagen, die von Marktüberwachungsbehörden auf der Grundlage von Hinweisen oder Informationen über eine mögliche Nichtkonformität von Produkten mit digitalen Elementen mit dieser Verordnung in mehreren Mitgliedstaaten durchgeführt werden sollen, oder Produktkategorien zu ermitteln, zu denen gleichzeitige koordinierte Kontrollen organisiert werden sollten. Unter außergewöhnlichen Umständen sollte die ENISA auf Ersuchen der Kommission Bewertungen in Bezug auf bestimmte Produkte mit digitalen Elementen, die ein erhebliches Cybersicherheitsrisiko bergen, durchführen können, wenn ein sofortiges Eingreifen erforderlich ist, um das reibungslose Funktionieren des Binnenmarkts zu bewahren.

(20) Produkte mit digitalen Elementen sollten grundsätzlich mit der CE-Kennzeichnung versehen sein, aus der ihre Konformität mit dieser Verordnung hervorgeht, sodass sie frei im Binnenmarkt verkehren können. Die Mitgliedstaaten sollten für das Inverkehrbringen von Produkten mit digitalen Elementen, die den in dieser Verordnung festgelegten Anforderungen genügen und mit der CE-Kennzeichnung versehen sind, keine ungerechtfertigten Hindernisse schaffen.

(21) Damit Hersteller Software zu Testzwecken freigeben können, bevor sie ihre Produkte einer Konformitätsbewertung unterziehen, sollten die Mitgliedstaaten nicht verhindern, dass unfertige Software z. B. als Alpha-, Beta- oder Vorabversion bereitgestellt wird, sofern die Version nur so lange zur Verfügung gestellt wird, wie es für die Tests und das Sammeln von Rückmeldungen erforderlich ist. Die Hersteller sollten sicherstellen, dass unter diesen Bedingungen bereitgestellte Software erst nach einer Risikobewertung freigegeben wird und die Sicherheitsanforderungen dieser Verordnung in Bezug auf die Eigenschaften von Produkten mit digitalen Elementen so weit wie möglich erfüllt. Die Hersteller sollten auch die Anforderungen an die Behandlung von Schwachstellen so weit wie möglich umsetzen. Die Hersteller sollten die Nutzer nicht zu einer Aktualisierung auf Versionen zwingen, die nur zu Testzwecken freigegeben wurden.

(22) Damit Produkte mit digitalen Elementen beim Inverkehrbringen keine Cybersicherheitsrisiken für Personen und Organisationen darstellen, sollten für solche Produkte grundlegende Anforderungen festgelegt werden. Werden solche Produkte nachträglich physisch oder digital in einer Weise verändert, die vom Hersteller nicht vorgesehen ist und die dazu führen kann, dass sie die betreffenden grundlegenden

Anforderungen nicht mehr erfüllen, sollte die Veränderung als wesentlich betrachtet werden. Beispielsweise könnten Software-Aktualisierungen und -Reparaturen den Wartungsarbeiten gleichgestellt werden, sofern sie ein bereits in Verkehr gebrachtes Produkt nicht so verändern, dass die Konformität mit den geltenden Anforderungen beeinträchtigt oder die bestimmungsgemäße Verwendung, für die das Produkt geprüft wurde, verändert werden kann. Ebenso wie bei physischen Reparaturen oder Änderungen sollte ein Produkt mit digitalen Elementen durch eine Softwareänderung als wesentlich verändert gelten, wenn durch die Software-Aktualisierung die ursprünglich vorgesehenen Funktionen, die Art oder die Leistung des Produkts geändert werden und diese Änderungen in der ursprünglichen Risikobewertung nicht vorgesehen waren oder sich infolge der Software-Aktualisierung die Art der Gefahr verändert hat oder das Risiko gestiegen ist.

(23) Im Einklang mit dem allgemein anerkannten Begriff der wesentlichen Änderung von Produkten, für die Harmonisierungsrechtsvorschriften der Union gelten, ist es angebracht, immer dann, wenn eine wesentliche Änderung eintritt, die sich auf die Konformität eines Produkts mit dieser Verordnung auswirken könnte, oder wenn sich die Zweckbestimmung dieses Produkts ändert, die Konformität des Produkts mit digitalen Elementen zu überprüfen und es gegebenenfalls einer neuen Konformitätsbewertung zu unterziehen. Wenn der Hersteller eine Konformitätsbewertung unter Beteiligung eines Dritten durchführt, sollten Veränderungen, die zu wesentlichen Änderungen führen könnten, dem Dritten mitgeteilt werden.

(24) Die Aufbereitung, Wartung und Reparatur eines Produkts mit digitalen Elementen im Sinne der Verordnung [Ökodesign-Verordnung] führt nicht unbedingt zu einer wesentlichen Änderung des Produkts, wenn z. B. die bestimmungsgemäße Verwendung und die Funktionen nicht geändert werden und das Risikoniveau gleich bleibt. Die Aufrüstung eines Produkts durch den Hersteller könnte jedoch zu Änderungen in der Konzeption und Entwicklung des Produkts führen und sich daher auf die bestimmungsgemäße Verwendung und die Konformität des Produkts mit den Anforderungen dieser Verordnung auswirken.

(25) Produkte mit digitalen Elementen sollten als kritisch betrachtet werden, wenn die negativen Auswirkungen der Ausnutzung potenzieller Cybersicherheitslücken in dem Produkt unter anderem aufgrund seiner Cybersicherheitsfunktion oder seiner bestimmungsgemäßen Verwendung schwerwiegend sein können. Insbesondere können Schwachstellen in Produkten mit digitalen Elementen, die eine Cybersicherheitsfunktion haben, wie z. B. Sicherheitselemente (*Secure Elements*), zu einer Ausbreitung von Sicherheitsproblemen in der gesamten Lieferkette führen. Die Schwere der Auswirkungen eines Cybersicherheitsvorfalls kann auch zunehmen, wenn die bestimmungsgemäße Verwendung des Produkts, z. B. in einem industriellen Umfeld oder im Zusammenhang mit einer wesentlichen Einrichtung der in Anhang [Anhang I] der Richtlinie [Richtlinie XXX/XXXX (NIS2)] genannten Art, oder seine Verwendung zur Wahrnehmung kritischer oder sensibler Funktionen wie der Verarbeitung personenbezogener Daten berücksichtigt wird.

(26) Kritische Produkte mit digitalen Elementen sollten strengeren Konformitätsbewertungsverfahren unterliegen, wobei ein verhältnismäßiger Ansatz gewahrt bleiben sollte. Zu diesem Zweck sollten kritische Produkte mit digitalen Elementen in zwei Klassen unterteilt werden, die das mit diesen Produktkategorien verbundene Cybersicherheitsrisiko widerspiegeln. Ein potenzieller Cybervorfall mit Produkten der Klasse II könnte größere negative Auswirkungen haben als ein Vorfall

mit Produkten der Klasse I, beispielsweise wegen der Art ihrer Cybersicherheitsfunktion oder ihrer bestimmungsgemäßen Verwendung in sensiblen Umgebungen, und daher sollten erstere Produkte einem strengeren Konformitätsbewertungsverfahren unterzogen werden.

(27) Die in Anhang III dieser Verordnung genannten Kategorien kritischer Produkte mit digitalen Elementen sollten als jene Produkte verstanden werden, deren Kernfunktionen den in Anhang III dieser Verordnung aufgeführten Arten entsprechen. So sind in Anhang III dieser Verordnung beispielsweise Produkte aufgeführt, die durch ihre Kernfunktion als Allzweck-Mikroprozessoren der Klasse II definiert sind. Folglich unterliegen Allzweck-Mikroprozessoren einer obligatorischen Konformitätsbewertung durch Dritte. Dies gilt nicht für andere, nicht ausdrücklich in Anhang III dieser Verordnung genannte Produkte, in denen ein Allzweck-Mikroprozessor enthalten sein kann. Die Kommission sollte bis zum [12 Monate nach Inkrafttreten dieser Verordnung] delegierte Rechtsakte erlassen, in denen sie die Definitionen der nach Anhang III zur Klasse I und Klasse II gehörigen Produktkategorien festlegt.

(28) Mit dieser Verordnung werden Cybersicherheitsrisiken gezielt angegangen. Produkte mit digitalen Elementen können jedoch noch andere Sicherheitsrisiken bergen, die nicht mit der Cybersicherheit zusammenhängen. Solche anderen Risiken sollten weiterhin durch andere einschlägige Produktvorschriften der Union geregelt werden. Wenn keine anderen Harmonisierungsrechtsvorschriften der Union anwendbar sind, sollten die Produkte der Verordnung [Verordnung über die allgemeine Produktsicherheit] unterliegen. Angesichts der gezielten Ausrichtung der vorliegenden Verordnung sollten daher abweichend von Artikel 2 Absatz 1 Unterabsatz 3 Buchstabe b der Verordnung [Verordnung über die allgemeine Produktsicherheit] in Bezug auf Sicherheitsrisiken, die nicht unter die vorliegende Verordnung fallen, das Kapitel III Abschnitt 1, die Kapitel V und VII sowie die Kapitel IX bis XI der Verordnung [Verordnung über die allgemeine Produktsicherheit] auch für Produkte mit digitalen Elementen gelten, wenn diese Produkte keinen besonderen Anforderungen anderer Harmonisierungsrechtsvorschriften der Union im Sinne von [Artikel 3 Nummer 25 der Verordnung über die allgemeine Produktsicherheit] unterliegen.

(29) Produkte mit digitalen Elementen, die nach Artikel 6 der Verordnung[15] [KI-Verordnung] als Hochrisiko-KI-Systeme eingestuft sind und in den Anwendungsbereich der vorliegenden Verordnung fallen, sollten den in der vorliegenden Verordnung festgelegten grundlegenden Anforderungen genügen. Genügen diese Hochrisiko-KI-Systeme den grundlegenden Anforderungen der vorliegenden Verordnung, so sollte davon ausgegangen werden, dass sie die Cybersicherheitsanforderungen gemäß Artikel [Artikel 15] der Verordnung [KI-Verordnung] erfüllen, soweit diese Anforderungen von der nach der vorliegenden Verordnung ausgestellten EU-Konformitätserklärung oder Teilen davon abgedeckt sind. Für die Konformitätsbewertungsverfahren zu den grundlegenden Cybersicherheitsanforderungen für ein Produkt mit digitalen Elementen, das unter die vorliegende Verordnung fällt und als Hochrisiko-KI-System eingestuft ist, sollten grundsätzlich anstelle der jeweiligen Bestimmungen der vorliegenden Verordnung die einschlägigen Bestimmungen des Artikels 43 der Verordnung [KI-Verordnung]

[15] Verordnung [KI-Verordnung].

Anwendung finden. Diese Regel sollte jedoch nicht dazu führen, dass die erforderliche Vertrauenswürdigkeit für unter die vorliegende Verordnung fallende kritische Produkte mit digitalen Elementen verringert wird. Deshalb sollten abweichend von dieser Regel Hochrisiko-KI-Systeme, die in den Anwendungsbereich der Verordnung [KI-Verordnung] fallen und auch als kritische Produkte mit digitalen Elementen gemäß der vorliegenden Verordnung gelten und auf die das Konformitätsbewertungsverfahren auf der Grundlage einer internen Kontrolle gemäß Anhang VI der Verordnung [KI-Verordnung] angewandt wird, den Konformitätsbewertungsbestimmungen der vorliegenden Verordnung unterliegen, soweit die grundlegenden Anforderungen der vorliegenden Verordnung betroffen sind. In diesem Fall sollten für alle anderen Aspekte, die unter die Verordnung [KI-Verordnung] fallen, die jeweiligen Bestimmungen über die Konformitätsbewertung auf der Grundlage einer internen Kontrolle gemäß Anhang VI der Verordnung [KI-Verordnung] gelten.

(30) Maschinenprodukte, die in den Anwendungsbereich der Verordnung [Vorschlag für eine Maschinenverordnung] fallen, bei denen es sich um Produkte mit digitalen Elementen im Sinne der vorliegenden Verordnung handelt und für die auf der Grundlage der vorliegenden Verordnung eine EU-Konformitätserklärung ausgestellt wurde, sollten in Bezug auf den Schutz vor Korruption und in Bezug auf die Sicherheit und Zuverlässigkeit von Steuerungssystemen als konform mit den grundlegenden Gesundheits- und Sicherheitsanforderungen in [Anhang III Abschnitte 1.1.9 und 1.2.1] der Verordnung [Vorschlag für eine Maschinenverordnung] gelten, sofern mit der nach der vorliegenden Verordnung ausgestellten EU-Konformitätserklärung die Erfüllung der genannten Anforderungen nachgewiesen wird.

(31) Die Verordnung [Vorschlag für eine Verordnung über den europäischen Raum für Gesundheitsdaten] ergänzt die in der vorliegenden Verordnung festgelegten grundlegenden Anforderungen. Die elektronischen Patientendatensysteme (im Folgenden „EHR-Systeme“), die in den Anwendungsbereich der Verordnung [Vorschlag für eine Verordnung über den europäischen Raum für Gesundheitsdaten] fallen und bei denen es sich um Produkte mit digitalen Elementen im Sinne der vorliegenden Verordnung handelt, sollten daher auch den grundlegenden Anforderungen der vorliegenden Verordnung genügen. Ihre Hersteller sollten die Konformität nach Maßgabe der Verordnung [Vorschlag für eine Verordnung über den europäischen Raum für Gesundheitsdaten] nachweisen. Zur Erleichterung der Einhaltung der Vorschriften können die Hersteller eine einzige technische Dokumentation erstellen, die die in beiden Rechtsakten vorgeschriebenen Elemente enthält. Da die vorliegende Verordnung nicht für SaaS gilt, fallen EHR-Systeme, die im Rahmen des SaaS-Lizenzierungs- und Umsetzungsmodells angeboten werden, nicht in den Anwendungsbereich dieser Verordnung. Ebenso fallen EHR-Systeme, die intern entwickelt und verwendet werden, nicht in den Anwendungsbereich dieser Verordnung, weil sie nicht in Verkehr gebracht werden.

(32) Um sicherzustellen, dass Produkte mit digitalen Elementen sowohl zum Zeitpunkt ihres Inverkehrbringens als auch während ihres gesamten Lebenszyklus sicher sind, müssen grundlegende Anforderungen für die Behandlung von Schwachstellen und grundlegende Cybersicherheitsanforderungen in Bezug auf die Eigenschaften von Produkten mit digitalen Elementen festgelegt werden. Die Hersteller sollten sowohl alle grundlegenden Anforderungen in Bezug auf die Behandlung von Schwachstellen erfüllen und sicherstellen, dass alle ihre Produkte ohne bekannte ausnutzbare

Schwachstellen abgegeben werden, als auch bestimmen, welche anderen grundlegenden Anforderungen in Bezug auf die Produkteigenschaften für die betreffende Produktart von Bedeutung sind. Zu diesem Zweck sollten die Hersteller eine Bewertung der Cybersicherheitsrisiken vornehmen, die mit einem Produkt mit digitalen Elementen verbunden sind, um einschlägige Risiken und grundlegende Anforderungen zu ermitteln und geeignete harmonisierte Normen oder gemeinsame Spezifikationen angemessen anzuwenden.

(33) Zur Erhöhung der Sicherheit von Produkten mit digitalen Elementen, die im Binnenmarkt in Verkehr gebracht werden, ist es erforderlich, grundlegende Anforderungen festzulegen. Diese grundlegenden Anforderungen sollten die EU-weit koordinierten Risikobewertungen kritischer Lieferketten gemäß [Artikel X] der Richtlinie [Richtlinie XXX/XXXX(NIS2)][16] unberührt lassen, in denen sowohl technische als gegebenenfalls auch nichttechnische Risikofaktoren wie eine unzulässige Einflussnahme eines Drittlands auf Lieferanten berücksichtigt werden. Darüber hinaus sollten hiervon die Vorrechte der Mitgliedstaaten unberührt bleiben, zusätzliche Anforderungen festzulegen, die nichttechnischen Faktoren Rechnung tragen, um ein hohes Maß an Resilienz zu gewährleisten, einschließlich derer, die in der Empfehlung (EU) 2019/534, in der unionsweit koordinierten Risikobewertung zur Cybersicherheit in 5G-Netzen und in dem EU-Instrumentarium für die 5G-Cybersicherheit, das die in der [Richtlinie XXX/XXXX (NIS2)] genannte NIS-Kooperationsgruppe vereinbart hat, definiert worden sind.

(34) Damit die nationalen CSIRTs und die nach Artikel [X] der Richtlinie [Richtlinie XX/XXXX (NIS2)] benannte zentrale Anlaufstelle die Informationen erhalten, die sie benötigen, um ihre Aufgaben wahrzunehmen und das Gesamtniveau der Cybersicherheit wesentlicher und wichtiger Einrichtungen zu erhöhen, und um das wirksame Funktionieren der Marktüberwachungsbehörden zu gewährleisten, sollten die Hersteller von Produkten mit digitalen Elementen der ENISA alle aktiv ausgenutzten Schwachstellen melden. Da die meisten Produkte mit digitalen Elementen im gesamten Binnenmarkt vermarktet werden, sollte jede ausgenutzte Schwachstelle in einem Produkt mit digitalen Elementen als Bedrohung für das Funktionieren des Binnenmarkts betrachtet werden. Überdies sollten die Hersteller in Erwägung ziehen, behobene Schwachstellen in der gemäß der Richtlinie [Richtlinie XX/XXXX (NIS2)] eingerichteten und von der ENISA verwalteten europäischen Schwachstellendatenbank oder einer anderen öffentlich zugänglichen Schwachstellendatenbank offenzulegen.

(35) Die Hersteller sollten der ENISA auch jeden Vorfall melden, der sich auf die Sicherheit eines Produkts mit digitalen Elementen auswirkt. Ungeachtet der Verpflichtung wesentlicher und wichtiger Einrichtungen zur Meldung von Sicherheitsvorfällen gemäß der Richtlinie [Richtlinie XXX/XXXX (NIS2)] ist es von entscheidender Bedeutung, dass die ENISA, die von den Mitgliedstaaten gemäß Artikel [X] der Richtlinie [Richtlinie XXX/XXXX (NIS2)] benannten zentralen Anlaufstellen und die Marktüberwachungsbehörden von den Herstellern der Produkte mit digitalen Elementen Informationen erhalten, die es ihnen ermöglichen, die Sicherheit dieser Produkte zu bewerten. Damit die Nutzer rasch auf Vorfälle reagieren können, die sich auf die Sicherheit ihrer Produkte mit digitalen Elementen auswirken,

[16] Richtlinie XXX des Europäischen Parlaments und des Rates vom [Datum] [über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union und zur Aufhebung der Richtlinie (EU) 2016/1148] (ABl. L xx vom [Datum], S. x).

sollten die Hersteller auch ihre Nutzer über solche Vorfälle und gegebenenfalls über Korrekturmaßnahmen informieren, die die Nutzer ergreifen können, um die Auswirkungen des Vorfalls zu mindern, und zwar z. B. durch Veröffentlichung einschlägiger Informationen auf ihren Websites oder, falls der Hersteller zu den Nutzern Kontakt aufnehmen kann und die Risiken dies rechtfertigen, durch direkte Kontaktaufnahme zu den Nutzern.

(36) Hersteller von Produkten mit digitalen Elementen sollten Konzepte für die koordinierte Offenlegung von Schwachstellen einführen, um das Melden von Schwachstellen durch natürliche oder juristische Personen zu erleichtern. Ein Konzept für die koordinierte Offenlegung von Schwachstellen sollte einen strukturierten Prozess vorsehen, in dem Schwachstellen dem Hersteller in einer Weise gemeldet werden, die dem Hersteller die Diagnose und Behebung solcher Schwachstellen ermöglicht, bevor detaillierte Informationen über die Schwachstelle an Dritte oder die Öffentlichkeit weitergegeben werden. Angesichts dessen, dass mit Informationen über ausnutzbare Schwachstellen in weitverbreiteten Produkten mit digitalen Elementen auf dem Schwarzmarkt hohe Preisen zu erzielen sind, sollten die Hersteller solcher Produkte in der Lage sein, im Rahmen ihrer Konzepte für die koordinierte Offenlegung von Schwachstellen Programme durchzuführen, mit denen sie Anreize für das Melden von Schwachstellen geben, indem sie dafür sorgen, dass natürliche oder juristische Personen Anerkennung und Belohnung für ihre Bemühungen erhalten (sogenannte „Bug-Bounty-Programme“).

(37) Zur Erleichterung der Schwachstellenanalyse sollten die Hersteller feststellen und dokumentieren, welche Komponenten in den Produkten mit digitalen Elementen enthalten sind, und dazu gegebenenfalls eine Software-Stückliste aufstellen. Eine Software-Stückliste kann denjenigen, die Software herstellen, kaufen und betreiben, Informationen vermitteln, die ihr Verständnis der Lieferkette verbessern, was zahlreiche Vorteile mit sich bringt und vor allem Herstellern und Nutzern hilft, bekannte neu auftretende Schwachstellen und Risiken zu verfolgen. Für die Hersteller ist es besonders wichtig, sich zu vergewissern, dass ihre Produkte keine anfälligen Komponenten enthalten, die von Dritten entwickelt wurden.

(38) Um die Bewertung der Konformität mit den in dieser Verordnung festgelegten Anforderungen zu erleichtern, sollte eine Konformitätsvermutung für Produkte mit digitalen Elementen gelten, die harmonisierten Normen entsprechen, mit denen die grundlegenden Anforderungen dieser Verordnung in detaillierte technische Spezifikationen umgesetzt werden und die gemäß der Verordnung (EU) Nr. 1025/2012 des Europäischen Parlaments und des Rates[17] angenommen wurden. Die Verordnung (EU) Nr. 1025/2012 enthält ein Verfahren für Einwände gegen harmonisierte Normen, falls diese Normen den Anforderungen der vorliegenden Verordnung nicht in vollem Umfang entsprechen.

(39) Mit der Verordnung (EU) 2019/881 ist ein freiwilliger europäischer Rahmen für die Cybersicherheitszertifizierung von IKT-Produkten, -Prozessen und -Diensten geschaffen worden. Die europäischen Systeme für die Cybersicherheitszertifizierung

[17] 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).

können Produkte mit digitalen Elementen erfassen, die unter die vorliegende Verordnung fallen. Die vorliegende Verordnung sollte Synergien mit der Verordnung (EU) 2019/881 schaffen. Um die Bewertung der Konformität mit den in der vorliegenden Verordnung festgelegten Anforderungen zu erleichtern, wird bei Produkten mit digitalen Elementen, die zertifiziert worden sind oder für die im Rahmen eines Cybersicherheitssystems gemäß der Verordnung (EU) 2019/881 eine Konformitätserklärung ausgestellt wurde und die von der Kommission in einem Durchführungsrechtsakt aufgeführt werden, davon ausgegangen, dass sie den grundlegenden Anforderungen der vorliegenden Verordnung genügen, sofern das Cybersicherheitszertifikat oder die Konformitätserklärung oder Teile davon diese Anforderungen abdecken. Die Notwendigkeit neuer europäischer Systeme für die Cybersicherheitszertifizierung von Produkten mit digitalen Elementen sollte im Lichte der vorliegenden Verordnung geprüft werden. Solche künftigen europäischen Systeme für die Cybersicherheitszertifizierung von Produkten mit digitalen Elementen sollten den in dieser Verordnung festgelegten grundlegenden Anforderungen Rechnung tragen und die Einhaltung dieser Verordnung erleichtern. Der Kommission sollte die Befugnis übertragen werden, im Wege von Durchführungsrechtsakten die europäischen Systeme für die Cybersicherheitszertifizierung auszuweisen, die zum Nachweis der Konformität mit den grundlegenden Anforderungen dieser Verordnung verwendet werden können. Um einen übermäßigen Verwaltungsaufwand für die Hersteller zu vermeiden, sollte die Kommission darüber hinaus gegebenenfalls angeben, ob mit einem im Rahmen solcher europäischen Systeme für die Cybersicherheitszertifizierung ausgestellten Cybersicherheitszertifikat die in dieser Verordnung vorgesehene Pflicht der Hersteller, für die betreffenden Anforderungen eine Konformitätsbewertung durch Dritte durchführen zu lassen, aufgehoben werden kann.

(40) Beim Inkrafttreten des Durchführungsrechtsakts [Durchführungsverordnung (EU) …/… der Kommission vom XXX über das auf gemeinsamen Kriterien beruhende europäische System für die Cybersicherheitszertifizierung] (EUCC), der unter diese Verordnung fallende Hardwareprodukte wie Hardware-Sicherheitsmodule und Mikroprozessoren betrifft, kann die Kommission im Wege eines Durchführungsrechtsakts festlegen, auf welche Weise das EUCC eine Konformitätsvermutung mit den grundlegenden Anforderungen in Anhang I dieser Verordnung oder Teilen davon begründen kann. Darüber hinaus kann in einem solchen Durchführungsrechtsakt festgelegt werden, wie mit einem im Rahmen des EUCC ausgestellten Zertifikat die Pflicht der Hersteller, für die betreffenden Anforderungen dieser Verordnung eine Bewertung durch Dritte durchführen zu lassen, aufgehoben werden kann.

(41) Wenn keine harmonisierten Normen angenommen wurden oder die grundlegenden Anforderungen dieser Verordnung in den harmonisierten Normen nicht ausreichend berücksichtigt wurden, sollte die Kommission in der Lage sein, im Wege von Durchführungsrechtsakten gemeinsame Spezifikationen festzulegen. Gründe für die Entwicklung solcher gemeinsamen Spezifikationen anstelle der Anwendung harmonisierter Normen könnten die Ablehnung des Normungsauftrags durch die europäischen Normungsorganisationen, unangemessene Verzögerungen bei der Ausarbeitung geeigneter harmonisierter Normen oder eine mangelnde Übereinstimmung entwickelter Normen mit den Anforderungen dieser Verordnung oder mit einem Normungsauftrag der Kommission sein. Um die Bewertung der Konformität mit den grundlegenden Anforderungen dieser Verordnung zu erleichtern, sollte eine Konformitätsvermutung für Produkte mit digitalen Elementen gelten, die

den gemeinsamen Spezifikationen entsprechen, die die Kommission nach dieser Verordnung angenommen hat, um ausführliche technische Spezifikationen für diese Anforderungen zu formulieren.

(42) Die Hersteller sollten eine EU-Konformitätserklärung ausstellen, aus der die nach dieser Verordnung erforderlichen Informationen über die Konformität der Produkte mit digitalen Elementen mit den Anforderungen dieser Verordnung und gegebenenfalls den sonstigen einschlägigen Harmonisierungsrechtsvorschriften der Union, denen das Produkt unterliegt, hervorgehen. Die Hersteller können ferner auch aufgrund anderer Rechtsvorschriften der Union verpflichtet sein, eine EU-Konformitätserklärung auszustellen. Um einen wirksamen Zugang zu Informationen für die Zwecke der Marktüberwachung zu gewährleisten, sollte eine einzige EU-Konformitätserklärung in Bezug die Einhaltung aller einschlägigen Rechtsvorschriften der Union ausgestellt werden. Um den Verwaltungsaufwand für die Wirtschaftsakteure zu verringern, sollte es zulässig sein, dass diese einzige EU-Konformitätserklärung aus einer Akte besteht, die sich aus den einschlägigen einzelnen Konformitätserklärungen zusammensetzt.

(43) Die CE-Kennzeichnung bringt die Konformität eines Produkts zum Ausdruck und ist das sichtbare Ergebnis eines ganzen Prozesses, der die Konformitätsbewertung im weiteren Sinne umfasst. Die allgemeinen Grundsätze für die CE-Kennzeichnung sind in der Verordnung (EG) Nr. 765/2008 des Europäischen Parlaments und des Rates[18] festgelegt. Die Vorschriften für die Anbringung der CE-Kennzeichnung auf Produkten mit digitalen Elementen sollten in der vorliegenden Verordnung festgelegt werden. Die CE-Kennzeichnung sollte die einzige Kennzeichnung sein, die die Übereinstimmung der Produkte mit digitalen Elementen mit den Anforderungen dieser Verordnung garantiert.

(44) Damit die Wirtschaftsakteure die Konformität mit den grundlegenden Anforderungen dieser Verordnung nachweisen können und die Marktüberwachungsbehörden sicherstellen können, dass Produkte mit digitalen Elementen, die auf dem Markt bereitgestellt werden, diesen Anforderungen genügen, sind Konformitätsbewertungsverfahren vorzusehen. Im Beschluss Nr. 768/2008/EG des Europäischen Parlaments und des Rates[19] sind Module für Konformitätsbewertungsverfahren festgelegt, die der Höhe des Risikos und dem geforderten Sicherheitsniveau angemessen sind. Um die sektorübergreifende Kohärenz zu gewährleisten und Ad-hoc-Varianten zu vermeiden, beruhen die Konformitätsbewertungsverfahren zur Überprüfung der Konformität von Produkten mit digitalen Elementen mit den grundlegenden Anforderungen dieser Verordnung auf diesen Modulen. In den Konformitätsbewertungsverfahren sollten sowohl produkt- als auch verfahrensbezogene Anforderungen untersucht und überprüft werden, die den gesamten Lebenszyklus von Produkten mit digitalen Elementen abdecken, einschließlich Planung, Konzeption, Entwicklung oder Herstellung, Tests und Wartung des Produkts.

---

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

19 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).

(45) In der Regel sollte die Konformitätsbewertung von Produkten mit digitalen Elementen vom Hersteller in eigener Verantwortung nach dem Verfahren auf der Grundlage von Modul A des Beschlusses Nr. 768/2008/EG durchgeführt werden. Der Hersteller sollte die Flexibilität behalten, ein strengeres Konformitätsbewertungsverfahren unter Einbeziehung eines Dritten zu wählen. Ist das Produkt als kritisches Produkt der Klasse I eingestuft, so ist eine zusätzliche Vertrauenswürdigkeitsprüfung erforderlich, um die Konformität mit den grundlegenden Anforderungen dieser Verordnung nachzuweisen. Der Hersteller sollte die von der Kommission in einem Durchführungsrechtsakt ausgewiesenen harmonisierten Normen, gemeinsamen Spezifikationen oder Systeme für die Cybersicherheitszertifizierung gemäß der Verordnung (EU) 2019/881 verwenden, wenn er die Konformitätsbewertung in eigener Verantwortung durchführen möchte (Modul A). Verwendet der Hersteller solche harmonisierten Normen, gemeinsamen Spezifikationen oder Systeme für die Cybersicherheitszertifizierung nicht, so sollte eine Konformitätsbewertung unter Beteiligung eines Dritten durchgeführt werden. Unter Berücksichtigung des Verwaltungsaufwands für die Hersteller und der Tatsache, dass die Cybersicherheit in der Konzeptions- und Entwicklungsphase materieller und immaterieller Produkte mit digitalen Elementen eine wichtige Rolle spielt, wurden Konformitätsbewertungsverfahren auf der Grundlage der Module B und C oder des Moduls H des Beschlusses Nr. 768/2008/EG als am besten geeignet ausgewählt, um die Konformität kritischer Produkte mit digitalen Elementen auf verhältnismäßige und wirksame Weise zu bewerten. Der Hersteller, der die Konformitätsbewertung durch Dritte durchführen lässt, kann das Verfahren auswählen, das seinem Konzeptions- und Herstellungsprozess am besten entspricht. Angesichts des noch größeren Cybersicherheitsrisikos, das mit der Verwendung von Produkten verbunden ist, die als kritische Produkte der Klasse II eingestuft sind, sollte an deren Konformitätsbewertung stets ein Dritter beteiligt werden.

(46) Während die Herstellung materieller Produkte mit digitalen Elementen in der Regel einen erheblichen Aufwand während der gesamten Konzeptions-, Entwicklungs- und Herstellungsphase erfordert, konzentriert sich die Herstellung von Produkten mit digitalen Elementen in Form von Software fast ausschließlich auf die Konzeption und Entwicklung, wogegen die Herstellungsphase eine untergeordnete Rolle spielt. Dennoch müssen Softwareprodukte oft noch kompiliert und zu Versionen zusammengefügt, gepackt, zum Herunterladen bereitgestellt oder auf physische Datenträger kopiert werden, bevor sie in Verkehr gebracht werden. Bei der Anwendung der einschlägigen Konformitätsbewertungsmodule zur Überprüfung der Konformität des Produkts mit den grundlegenden Anforderungen dieser Verordnung in der Konzeptions-, Entwicklungs- und Herstellungsphase sollten diese Tätigkeiten als dem Herstellungsprozess gleichkommende Tätigkeiten betrachtet werden.

(47) Damit Produkte mit digitalen Elementen einer Konformitätsbewertung durch Dritte unterzogen werden können, sollten die nationalen notifizierenden Behörden der Kommission und den anderen Mitgliedstaaten die Konformitätsbewertungsstellen notifizieren, sofern diese eine Reihe von Anforderungen erfüllen, insbesondere in Bezug auf Unabhängigkeit, Kompetenz und Nichtvorliegen von Interessenkonflikten.

(48) Um für ein einheitliches Qualitätsniveau bei der Durchführung der Konformitätsbewertungen von Produkte mit digitalen Elementen zu sorgen, müssen auch die Anforderungen an die notifizierenden Behörden und andere Stellen, die bei der Begutachtung, Notifizierung und Überwachung von notifizierten Stellen tätig sind, festgelegt werden. Das in dieser Verordnung vorgesehene System sollte durch das

Akkreditierungssystem gemäß der Verordnung (EG) Nr. 765/2008 ergänzt werden. Da die Akkreditierung ein wichtiges Mittel zur Überprüfung der Kompetenz von Konformitätsbewertungsstellen ist, sollte sie auch zu Notifizierungszwecken eingesetzt werden.

(49) Eine transparente Akkreditierung nach Maßgabe der Verordnung (EG) Nr. 765/2008, die das notwendige Maß an Vertrauen in Konformitätsbescheinigungen gewährleistet, sollte von den nationalen Behörden unionsweit als bevorzugtes Mittel zum Nachweis der fachlichen Kompetenz von Konformitätsbewertungsstellen angesehen werden. Allerdings können nationale Behörden die Auffassung vertreten, dass sie über die geeigneten Mittel verfügen, um diese Bewertung selbst vorzunehmen. Um in solchen Fällen die Glaubwürdigkeit der durch andere nationale Behörden vorgenommenen Beurteilungen zu gewährleisten, sollten sie der Kommission und den anderen Mitgliedstaaten alle erforderlichen Unterlagen übermitteln, aus denen hervorgeht, dass die beurteilten Konformitätsbewertungsstellen die entsprechenden rechtlichen Anforderungen erfüllen.

(50) Häufig vergeben Konformitätsbewertungsstellen Teile ihrer Arbeit im Zusammenhang mit der Konformitätsbewertung an Unterauftragnehmer oder übertragen sie an Zweigstellen. Zur Wahrung des für das Inverkehrbringen von Produkten mit digitalen Elementen in der Union erforderlichen Schutzniveaus müssen die Unterauftragnehmer und Zweigstellen bei der Ausführung der Konformitätsbewertungsaufgaben unbedingt denselben Anforderungen genügen wie die notifizierten Stellen.

(51) Die Notifizierung einer Konformitätsbewertungsstelle sollte der Kommission und den anderen Mitgliedstaaten von der notifizierenden Behörde über das NANDO-Informationssystem (*New Approach Notified and Designated Organisations*, Informationssystem für die nach dem neuen Konzept notifizierten und benannten Organisationen) übermittelt werden. NANDO ist das von der Kommission entwickelte und verwaltete elektronische Notifizierungsinstrument, mit dem eine Liste aller notifizierten Stellen geführt wird.

(52) Da die notifizierten Stellen ihre Dienstleistungen in der gesamten Union anbieten können, sollten die anderen Mitgliedstaaten und die Kommission die Möglichkeit erhalten, Einwände gegen eine notifizierte Stelle zu erheben. Daher ist es wichtig, dass eine Frist vorgesehen wird, innerhalb deren etwaige Zweifel oder Bedenken hinsichtlich der Kompetenz von Konformitätsbewertungsstellen geklärt werden können, bevor diese ihre Arbeit als notifizierte Stellen aufnehmen.

(53) Im Interesse der Wettbewerbsfähigkeit ist es entscheidend, dass die notifizierten Stellen die Konformitätsbewertungsverfahren anwenden, ohne unnötigen Aufwand für die Wirtschaftsakteure zu schaffen. Aus demselben Grund, und damit die Gleichbehandlung der Wirtschaftsakteure sichergestellt ist, ist für eine einheitliche technische Anwendung der Konformitätsbewertungsverfahren zu sorgen. Dies lässt sich am besten durch eine zweckmäßige Koordinierung und Zusammenarbeit zwischen den notifizierten Stellen erreichen.

(54) Die Marktüberwachung ist ein wesentliches Instrument zur Gewährleistung der korrekten und einheitlichen Anwendung der Rechtsvorschriften der Union. Daher sollte ein Rechtsrahmen geschaffen werden, innerhalb dessen die Marktüberwachung in angemessener Weise erfolgen kann. Die Vorschriften der Verordnung

(EU) 2019/1020 des Europäischen Parlaments und des Rates[20] für die Überwachung des Unionsmarktes und die Kontrolle von Produkten, die auf den Unionsmarkt gelangen, gelten auch für Produkte mit digitalen Elementen, die unter die vorliegende Verordnung fallen.

(55) Nach der Verordnung (EU) 2019/1020 führen die Marktüberwachungsbehörden die Marktüberwachung im Hoheitsgebiet des jeweiligen Mitgliedstaats durch. Die vorliegende Verordnung sollte die Mitgliedstaaten nicht daran hindern, zu entscheiden, welche Behörden für die Wahrnehmung dieser Aufgaben zuständig sind. Jeder Mitgliedstaat sollte in seinem Hoheitsgebiet eine oder mehrere Marktüberwachungsbehörden benennen. Die Mitgliedstaaten können beschließen, eine bestehende oder eine neue Behörde als Marktüberwachungsbehörde zu benennen, einschließlich der in Artikel [Artikel X] der Richtlinie [Richtlinie XXX/XXXX (NIS2)] genannten zuständigen nationalen Behörden oder der in Artikel 58 der Verordnung (EU) 2019/881 genannten benannten nationalen Behörden für die Cybersicherheitszertifizierung. Die Wirtschaftsakteure sollten umfassend mit den Marktüberwachungsbehörden und anderen zuständigen Behörden zusammenarbeiten. Jeder Mitgliedstaat sollte die Kommission und die anderen Mitgliedstaaten über seine Marktüberwachungsbehörden und deren jeweilige Zuständigkeitsbereiche unterrichten und dafür sorgen, dass diese über die erforderlichen Ressourcen und Fähigkeiten für die Durchführung der Überwachungsaufgaben im Zusammenhang mit der vorliegenden Verordnung verfügen. Nach Artikel 10 Absätze 2 und 3 der Verordnung (EU) 2019/1020 sollte jeder Mitgliedstaat eine zentrale Verbindungsstelle benennen, die unter anderem dafür zuständig sein sollte, den abgestimmten Standpunkt der Marktüberwachungsbehörden zu vertreten und die Zusammenarbeit zwischen den Marktüberwachungsbehörden in verschiedenen Mitgliedstaaten zu unterstützen.

(56) Im Hinblick auf die einheitliche Anwendung dieser Verordnung sollte gemäß Artikel 30 Absatz 2 der Verordnung (EU) 2019/1020 eine besondere Gruppe zur administrativen Zusammenarbeit (ADCO) eingesetzt werden. Diese ADCO sollte sich aus Vertretern der benannten Marktüberwachungsbehörden und gegebenenfalls Vertretern der zentralen Verbindungsstellen zusammensetzen. Die Kommission sollte die Zusammenarbeit zwischen den Marktüberwachungsbehörden über das auf der Grundlage des Artikels 29 der Verordnung (EU) 2019/1020 eingerichtete Unionsnetzwerk für Produktkonformität unterstützen und fördern, das sich aus Vertretern der einzelnen Mitgliedstaaten, einschließlich eines Vertreters jeder zentralen Verbindungsstelle nach Artikel 10 der Verordnung (EU) 2019/1020 und eines optionalen nationalen Sachverständigen, sowie den Vorsitzenden der ADCO und Vertretern der Kommission zusammensetzt. Die Kommission sollte an den Sitzungen des Netzwerks, seiner Untergruppen und dieser ADCO teilnehmen. Sie sollte diese ADCO durch ein Exekutivsekretariat unterstützen, das technische und logistische Unterstützung leistet.

(57) Damit zeitnahe, verhältnismäßige und wirksame Maßnahmen in Bezug auf Produkte mit digitalen Elementen, die ein erhebliches Cybersicherheitsrisiko bergen, getroffen werden können, sollte ein Schutzklauselverfahren der Union vorgesehen werden, in dessen Rahmen interessierte Kreise über geplante Maßnahmen in Bezug auf solche Produkte informiert werden. Auf diese Weise könnten die

[20] 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).

Marktüberwachungsbehörden in Zusammenarbeit mit den betreffenden Wirtschaftsakteuren nötigenfalls zu einem früheren Zeitpunkt einschreiten. Wenn sich die Mitgliedstaaten und die Kommission einig sind, dass eine von einem Mitgliedstaat ergriffene Maßnahme gerechtfertigt ist, sollte die Kommission nur dann weiter tätig werden müssen, wenn sich die Nichtkonformität auf Unzulänglichkeiten einer harmonisierten Norm zurückführen lässt.

(58) In bestimmten Fällen kann ein Produkt mit digitalen Elementen, das dieser Verordnung entspricht, dennoch ein erhebliches Cybersicherheitsrisiko oder ein Risiko für die Gesundheit oder Sicherheit von Personen, für die Erfüllung der Pflichten aus dem Unionsrecht oder dem nationalen Recht zum Schutz der Grundrechte, für die Verfügbarkeit, Integrität oder Vertraulichkeit von Diensten, die über ein elektronisches Informationssystem von wesentlichen Einrichtungen der in [Anhang I der Richtlinie XXX/XXXX (NIS2)] genannten Art angeboten werden, oder für andere Aspekte des Schutzes öffentlicher Interessen darstellen. Daher müssen Vorschriften festgelegt werden, die die Minderung solcher Risiken gewährleisten. Infolgedessen sollten die Marktüberwachungsbehörden Maßnahmen treffen, mit denen sie den Wirtschaftsakteur dazu verpflichten, in Abhängigkeit vom Risiko dafür zu sorgen, dass das Produkt dieses Risiko nicht mehr birgt, oder aber es zurückzurufen oder vom Markt zu nehmen. Sobald eine Marktüberwachungsbehörde den freien Verkehr eines Produkts auf diese Weise einschränkt bzw. untersagt, sollte der Mitgliedstaat die Kommission und die anderen Mitgliedstaaten unverzüglich unter Angabe von Gründen und Argumenten für die Entscheidung in Kenntnis setzen. Ergreift eine Marktüberwachungsbehörde solche Maßnahmen gegen Produkte, von denen ein Risiko ausgeht, so sollte die Kommission unverzüglich Konsultationen mit den Mitgliedstaaten und dem bzw. den betroffenen Wirtschaftsakteur(en) aufnehmen und die nationale Maßnahme bewerten. Anhand der Ergebnisse dieser Bewertung sollte die Kommission entscheiden, ob die nationale Maßnahme gerechtfertigt ist oder nicht. Die Kommission sollte ihren Beschluss an alle Mitgliedstaaten richten und ihn diesen und dem bzw. den betroffenen Wirtschaftsakteur(en) unverzüglich mitteilen. Wird die Maßnahme als gerechtfertigt erachtet, kann die Kommission auch die Annahme von Vorschlägen zur Überarbeitung der betreffenden Rechtsvorschriften der Union in Erwägung ziehen.

(59) Bei Produkten mit digitalen Elementen, die ein erhebliches Cybersicherheitsrisiko bergen und bei denen Grund zu der Annahme besteht, dass sie dieser Verordnung nicht entsprechen, oder bei Produkten, die zwar dieser Verordnung entsprechen, aber andere große Risiken bergen, wie Risiken für die Gesundheit oder Sicherheit von Personen, die Grundrechte oder die Erbringung der Dienste von wesentlichen Einrichtungen der in [Anhang I der Richtlinie XXX/XXXX (NIS2)] genannten Art, kann die Kommission die ENISA ersuchen, eine Bewertung vorzunehmen. Auf der Grundlage dieser Bewertung kann die Kommission im Wege von Durchführungsrechtsakten Korrekturmaßnahmen oder einschränkende Maßnahmen auf Unionsebene erlassen, einschließlich der Anordnung der Rücknahme des betroffenen Produkts vom Markt oder seines Rückrufs innerhalb einer der Art des Risikos angemessenen Frist. Ein solches Eingreifen der Kommission ist nur unter außergewöhnlichen Umständen geboten, die ein sofortiges Eingreifen zur Bewahrung des reibungslosen Funktionierens des Binnenmarkts rechtfertigen, und nur dann, wenn die Überwachungsbehörden keine wirksamen Maßnahmen ergriffen haben, um Abhilfe zu schaffen. Solche außergewöhnlichen Umstände können Notfälle sein, in denen beispielsweise ein nichtkonformes Produkt vom Hersteller in mehreren Mitgliedstaaten in großem Umfang auf dem Markt bereitgestellt und auch in

Schlüsselsektoren von Einrichtungen verwendet wird, die in den Anwendungsbereich der [Richtlinie XXX/XXXX (NIS2)] fallen, und es bekannte Schwachstellen aufweist, die von böswilligen Akteuren ausgenutzt werden und für die der Hersteller keine verfügbaren Patches bereitstellt. Die Kommission darf in solchen Notfällen nur während der Dauer der außergewöhnlichen Umstände und nur solange eingreifen, wie die Nichtkonformität mit dieser Verordnung oder die großen Risiken fortbestehen.

(60) In Fällen, in denen es Hinweise auf eine Nichtkonformität mit dieser Verordnung in mehreren Mitgliedstaaten gibt, sollten die Marktüberwachungsbehörden in der Lage sein, gemeinsame Tätigkeiten mit anderen Behörden durchzuführen, um die Konformität zu überprüfen und Cybersicherheitsrisiken von Produkten mit digitalen Elementen zu ermitteln.

(61) Gleichzeitige koordinierte Kontrollen („*Sweeps*“) sind besondere Durchsetzungsmaßnahmen, die von Marktüberwachungsbehörden durchgeführt werden und die Produktsicherheit weiter verbessern können. Sweeps sollten insbesondere dann durchgeführt werden, wenn Marktentwicklungen, Beschwerden von Verbrauchern oder andere Anzeichen dafür sprechen, dass bestimmte Produktkategorien häufig Cybersicherheitsrisiken aufweisen. Die ENISA sollte den Marktüberwachungsbehörden Vorschläge für Produktkategorien vorlegen, für die Sweeps organisiert werden könnten, und zwar unter anderem auf der Grundlage der bei ihr eingegangenen Meldungen über Produktschwachstellen und Vorfälle.

(62) Damit der Rechtsrahmen erforderlichenfalls angepasst werden kann, sollte der Kommission die Befugnis übertragen werden, gemäß Artikel 290 AEUV Rechtsakte zu erlassen, um die Liste kritischer Produkte in Anhang III zu aktualisieren und die Definitionen dieser Produktkategorien festzulegen. Der Kommission sollte die Befugnis übertragen werden, gemäß dem genannten Artikel Rechtsakte zu erlassen, um Produkte mit digitalen Elementen festzulegen, die unter andere Unionsvorschriften fallen, mit denen dasselbe Schutzniveau wie mit dieser Verordnung erreicht wird, und um festzustellen, ob eine Einschränkung oder ein Ausschluss vom Anwendungsbereich dieser Verordnung notwendig wäre, und gegebenenfalls den Umfang dieser Einschränkung festzulegen. Der Kommission sollte auch die Befugnis übertragen werden, gemäß dem genannten Artikel Rechtsakte zu erlassen, um möglichweise die Zertifizierung bestimmter hochkritischer Produkte mit digitalen Elementen auf der Grundlage der in dieser Verordnung festgelegten Kritikalitätskriterien sowie die Mindestangaben für die EU-Konformitätserklärung und die Ergänzung der in die technische Dokumentation aufzunehmenden Elemente vorzuschreiben. 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 im Einklang stehen, die in der Interinstitutionellen Vereinbarung vom 13. April 2016 über bessere Rechtsetzung[21] 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.

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

(63) Zur Gewährleistung einheitlicher Bedingungen für die Durchführung dieser Verordnung sollten der Kommission Durchführungsbefugnisse in Bezug auf Folgendes übertragen werden: Festlegung des Formats und der Elemente der Software-Stückliste, Präzisierung der Art der Angaben, des Formats und des Verfahrens der Meldungen über aktiv ausgenutzte Schwachstellen und Sicherheitsvorfälle, die Hersteller der ENISA übermitteln, Ausweisung der nach der Verordnung (EU) 2019/881 angenommenen europäischen Systeme für die Cybersicherheitszertifizierung, die zum Nachweis der Konformität mit den grundlegenden Anforderungen in Anhang I dieser Verordnung oder Teilen davon verwendet werden können, Annahme gemeinsamer Spezifikationen für die grundlegenden Anforderungen in Anhang I, Festlegung technischer Spezifikationen für Piktogramme oder andere Kennzeichnungen in Bezug auf die Sicherheit von Produkten mit digitalen Elementen sowie Mechanismen zur Förderung ihrer Verwendung, Entscheidung über Korrekturmaßnahmen oder einschränkende Maßnahmen auf Unionsebene unter außergewöhnlichen Umständen, die ein sofortiges Eingreifen rechtfertigen, um das reibungslose Funktionieren des Binnenmarkts zu bewahren. Diese Befugnisse sollten im Einklang mit der Verordnung (EU) Nr. 182/2011 des Europäischen Parlaments und des Rates[22] ausgeübt werden.

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

(65) Um die wirksame Durchsetzung der in dieser Verordnung festgelegten Pflichten zu gewährleisten, sollte jede Marktüberwachungsbehörde befugt sein, Geldbußen aufzuerlegen oder ihre Auferlegung zu beantragen. Daher sollten auch Obergrenzen für Geldbußen festgelegt werden, die in den einzelstaatlichen Rechtsvorschriften für Verstöße gegen die in dieser Verordnung festgelegten Pflichten vorzusehen sind. Bei der Entscheidung über die Höhe der Geldbuße sollten in jedem Einzelfall alle relevanten Umstände der konkreten Situation und zumindest die in dieser Verordnung ausdrücklich festgelegten Umstände berücksichtigt werden, einschließlich der Frage, ob bereits andere Marktüberwachungsbehörden demselben Akteur für einen ähnlichen Verstoß Geldbußen auferlegt haben. Solche Umstände können entweder erschwerend wirken, falls der Verstoß desselben Akteurs im Hoheitsgebiet eines anderen Mitgliedstaats als desjenigen, in dem bereits eine Geldbuße verhängt wurde, weiter andauert, oder aber mildernd, indem sichergestellt wird, dass in anderen Mitgliedstaaten verhängte Sanktionen und deren Höhe sowie andere einschlägige konkrete Umstände berücksichtigt werden, wenn eine andere Marktüberwachungsbehörde für denselben Wirtschaftsakteur oder dieselbe Art von Verstoß eine weitere Geldbuße in Betracht zieht. Jedenfalls sollte der Gesamtbetrag der Geldbußen, die die Marktüberwachungsbehörden mehrerer Mitgliedstaaten wegen derselben Art von Verstößen gegen denselben Wirtschaftsakteur verhängen könnten, dem Grundsatz der Verhältnismäßigkeit entsprechen.

(66) Werden Geldbußen Personen auferlegt, bei denen es sich nicht um Unternehmen handelt, so sollte die zuständige Behörde bei der Bemessung der Geldbuße dem

---

[22] 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).

allgemeinen Einkommensniveau in dem betreffenden Mitgliedstaat und der wirtschaftlichen Lage der Personen Rechnung tragen. Die Mitgliedstaaten sollten bestimmen können, ob und inwieweit gegen Behörden Geldbußen verhängt werden können.

(67) In ihren Beziehungen mit Drittländern strebt die EU die Förderung des internationalen Handels mit regulierten Produkten an. Zur Erleichterung des Handels kann eine ganze Palette von Maßnahmen angewandt werden, darunter verschiedene Rechtsinstrumente wie bilaterale (zwischenstaatliche) Abkommen über die gegenseitige Anerkennung (MRA) der Konformitätsbewertung und der Kennzeichnung regulierter Produkte. Abkommen über die gegenseitige Anerkennung werden zwischen der Union und Drittländern geschlossen, die sich auf einem vergleichbaren Niveau der technischen Entwicklung befinden und deren Herangehensweise an die Konformitätsbewertung als kompatibel betrachtet wird. Diese Abkommen haben die gegenseitige Anerkennung von Bescheinigungen, Konformitätszeichen und Prüfberichten zur Grundlage, die von den Konformitätsbewertungsstellen der Vertragsparteien entsprechend den Rechtsvorschriften der jeweils anderen Partei vorgelegt werden. Solche Abkommen über die gegenseitige Anerkennung bestehen derzeit mit mehreren Ländern. Die Abkommen werden für eine Reihe bestimmter Sektoren geschlossen, die sich von Land zu Land unterscheiden können. Zur weiteren Erleichterung des Handels und im Bewusstsein dessen, dass die Lieferketten für Produkte mit digitalen Elementen global sind, kann die Union für Produkte, die unter diese Verordnung fallen, gemäß Artikel 218 AEUV Abkommen über die gegenseitige Anerkennung der Konformitätsbewertung schließen. Ebenfalls wichtig ist die Zusammenarbeit mit Partnerländern, um die weltweite Abwehrfähigkeit gegen Cyberangriffe zu stärken, da dies langfristig zu einem gestärkten Cybersicherheitsrahmen sowohl innerhalb als auch außerhalb der EU beitragen wird.

(68) Die Kommission sollte diese Verordnung regelmäßig in Abstimmung mit interessierten Kreisen überprüfen, insbesondere um festzustellen, ob sie veränderten gesellschaftlichen, politischen oder technischen Bedingungen oder veränderten Marktbedingungen anzupassen ist.

(69) Den Wirtschaftsakteuren sollte ausreichend Zeit für die Anpassung an die Anforderungen dieser Verordnung eingeräumt werden. Diese Verordnung sollte ab dem [24 Monate nach dem Datum ihres Inkrafttretens] gelten, mit Ausnahme der Meldepflichten für aktiv ausgenutzte Schwachstellen und Sicherheitsvorfälle, die ab dem [12 Monate nach dem Datum des Inkrafttretens dieser Verordnung] gelten sollten.

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

(71) Der Europäische Datenschutzbeauftragte wurde gemäß Artikel 42 Absatz 1 der Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates[23] angehört und gab am […] seine Stellungnahme ab —

HABEN FOLGENDE VERORDNUNG ERLASSEN:

KAPITEL I

ALLGEMEINE BESTIMMUNGEN

Artikel 1

Gegenstand

Mit dieser Verordnung wird Folgendes festgelegt:

a) Vorschriften für das Inverkehrbringen von Produkten mit digitalen Elementen, um die Cybersicherheit solcher Produkte zu gewährleisten;

b) grundlegende Anforderungen an die Konzeption, Entwicklung und Herstellung von Produkten mit digitalen Elementen sowie Pflichten der Wirtschaftsakteure in Bezug auf diese Produkte hinsichtlich der Cybersicherheit;

c) grundlegende Anforderungen an die von den Herstellern festgelegten Verfahren zur Behandlung von Schwachstellen, um die Cybersicherheit von Produkten mit digitalen Elementen während ihres gesamten Lebenszyklus zu gewährleisten, sowie Pflichten der Wirtschaftsakteure in Bezug auf diese Verfahren;

d) Vorschriften für die Marktüberwachung und die Durchsetzung der oben genannten Vorschriften und Anforderungen.

Artikel 2

Anwendungsbereich

(1) Diese Verordnung gilt für Produkte mit digitalen Elementen, deren bestimmungsgemäße oder vernünftigerweise vorhersehbare Verwendung eine direkte oder indirekte logische oder physische Datenverbindung mit einem Gerät oder Netz einschließt.

(2) Diese Verordnung gilt nicht für Produkte mit digitalen Elementen, auf die folgende Rechtsakte der Union Anwendung finden:

a) Verordnung (EU) 2017/745,

b) Verordnung (EU) 2017/746,

c) Verordnung (EU) 2019/2144.

(3) Diese Verordnung gilt nicht für Produkte mit digitalen Elementen, die nach der Verordnung (EU) 2018/1139 zertifiziert worden sind.

---

[23] 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).

(4) Die Anwendung dieser Verordnung auf Produkte mit digitalen Elementen, die unter andere Rechtsvorschriften der Union mit Anforderungen für alle oder einige der von den grundlegenden Anforderungen in Anhang I abgedeckten Risiken fallen, kann eingeschränkt oder ausgeschlossen werden, wenn

a) eine solche Einschränkung oder ein solcher Ausschluss mit dem für diese Produkte geltenden allgemeinen Rechtsrahmen vereinbar ist und

b) mit den sektorspezifischen Vorschriften dasselbe Schutzniveau erreicht wird, wie es diese Verordnung gewährleistet.

Der Kommission wird die Befugnis übertragen, gemäß Artikel 50 zur Änderung dieser Verordnung delegierte Rechtsakte zu erlassen, in denen sie die Notwendigkeit einer solchen Einschränkung oder eines solchen Ausschlusses feststellt und gegebenenfalls die betreffenden Produkte und Vorschriften sowie den Umfang der Einschränkung festlegt.

(5) Diese Verordnung gilt nicht für Produkte mit digitalen Elementen, die ausschließlich für Zwecke der nationalen Sicherheit oder für militärische Zwecke entwickelt wurden, und auch nicht für Produkte, die speziell für die Verarbeitung von Verschlusssachen konzipiert sind.

Artikel 3

Begriffsbestimmungen

Für die Zwecke dieser Verordnung bezeichnet der Ausdruck

1. „Produkt mit digitalen Elementen“ ein Software- oder Hardwareprodukt und dessen Datenfernverarbeitungslösungen, einschließlich Software- oder Hardwarekomponenten, die getrennt in Verkehr gebracht werden sollen;

2. „Datenfernverarbeitung“ jede entfernt stattfindende Datenverarbeitung, für die eine Software vom Hersteller selbst oder unter dessen Verantwortung konzipiert und entwickelt wird und ohne die das Produkt mit digitalen Elementen eine seiner Funktionen nicht erfüllen könnte;

3. „kritisches Produkt mit digitalen Elementen“ ein Produkt mit digitalen Elementen, das nach den in Artikel 6 Absatz 2 festgelegten Kriterien ein Cybersicherheitsrisiko birgt und dessen Kernfunktionen in Anhang III aufgeführt sind;

4. „hochkritisches Produkt mit digitalen Elementen“ ein Produkt mit digitalen Elementen, das nach den in Artikel 6 Absatz 5 festgelegten Kriterien ein Cybersicherheitsrisiko birgt;

5. „operative Technik“ programmierbare digitale Systeme oder Geräte, die mit der physischen Umgebung interagieren oder Geräte verwalten, die mit der physischen Umgebung interagieren;

6. „Software“ den Teil eines elektronischen Informationssystems, der aus Computercode besteht;

7. „Hardware“ ein physisches elektronisches Informationssystem, das digitale Daten verarbeiten, speichern oder übertragen kann, oder Teile eines solchen Systems;

8. „Komponente“ Software oder Hardware, die für die Integration in ein elektronisches Informationssystem bestimmt ist;

9. „elektronisches Informationssystem“ ein System, einschließlich elektrischer oder elektronischer Ausrüstung, das digitale Daten verarbeiten, speichern oder übertragen kann;

10. „logische Verbindung“ eine virtuelle Darstellung einer Datenverbindung, die über eine Softwareschnittstelle hergestellt wird;

11. „physische Verbindung“ eine Verbindung zwischen elektronischen Informationssystemen oder Komponenten, die mit physikalischen Mitteln wie elektrischen oder mechanischen Schnittstellen, Drähten oder Funkwellen hergestellt wird;

12. „indirekte Verbindung“ eine Verbindung zu einem Gerät oder Netz, die nicht direkt erfolgt, sondern als Teil eines größeren Systems, das seinerseits direkt mit diesem Gerät oder Netz verbunden werden kann;

13. „Privileg“ ein Zugangsrecht, das bestimmten Nutzern oder Programmen zur Durchführung sicherheitsrelevanter Vorgänge in einem elektronischen Informationssystem gewährt wird;

14. „erhöhtes Privileg“ ein Zugangsrecht, das bestimmten Nutzern oder Programmen zur Durchführung einer erweiterten Reihe sicherheitsrelevanter Vorgänge in einem elektronischen Informationssystem gewährt wird und im Falle des Missbrauchs oder der Kompromittierung einem böswilligen Akteur einen breiteren Zugang zu den Ressourcen eines Systems oder einer Organisation ermöglichen könnte;

15. „Endpunkt“ ein Gerät, das an ein Netz angeschlossen ist und als Zugangspunkt zu diesem Netz dient;

16. „Netz- oder Rechenressourcen“ Daten oder Hardware- oder Softwarefunktionen, die entweder lokal oder über ein Netz oder ein anderes verbundenes Gerät zugänglich sind;

17. „Wirtschaftsakteur“ den Hersteller, den Bevollmächtigten, den Einführer, den Händler oder jede andere natürliche oder juristische Person, die den in dieser Verordnung festgelegten Pflichten unterliegt;

18. „Hersteller“ eine natürliche oder juristische Person, die Produkte mit digitalen Elementen entwickelt oder herstellt oder die Produkte mit digitalen Elementen konzipieren, entwickeln oder herstellen lässt und sie unter eigenen Namen oder eigener Marke vermarktet, sei es entgeltlich oder unentgeltlich;

19. „Bevollmächtigter“ eine in der Union ansässige oder niedergelassene natürliche oder juristische Person, die von einem Hersteller schriftlich beauftragt wurde, in seinem Namen bestimmte Aufgaben wahrzunehmen;

20. „Einführer“ eine in der Union ansässige oder niedergelassene natürliche oder juristische Person, die ein Produkt mit digitalen Elementen unter dem Namen oder der Marke einer außerhalb der Union ansässigen oder niedergelassenen natürlichen oder juristischen Person in der Union in Verkehr bringt;

21. „Händler“ eine natürliche oder juristische Person in der Lieferkette, die ein Produkt mit digitalen Elementen ohne Änderung seiner Eigenschaften auf dem Unionsmarkt bereitstellt, mit Ausnahme des Herstellers oder des Einführers;

22. „Inverkehrbringen“ die erstmalige Bereitstellung eines Produkts mit digitalen Elementen auf dem Unionsmarkt;

23. „Bereitstellung auf dem Markt“ jede entgeltliche oder unentgeltliche Abgabe eines Produkts mit digitalen Elementen zum Vertrieb oder zur Verwendung auf dem Unionsmarkt im Rahmen einer Geschäftstätigkeit;

24. „Zweckbestimmung“ die Verwendung, für die ein Produkt mit digitalen Elementen laut Hersteller bestimmt ist, einschließlich der besonderen Nutzungsumstände und Nutzungsbedingungen entsprechend den Angaben des Herstellers in der Gebrauchsanleitung, im Werbe- oder Verkaufsmaterial und in diesbezüglichen Erklärungen sowie in der technischen Dokumentation;

25. „vernünftigerweise vorhersehbare Verwendung“ eine Verwendung, die nicht unbedingt der vom Hersteller in der Gebrauchsanleitung, im Werbe- oder Verkaufsmaterial und in Erklärungen und der technischen Dokumentation angegebenen Zweckbestimmung entspricht, die sich aber aus einem vernünftigerweise vorhersehbaren menschlichen Verhalten oder aus technischen Vorgängen oder Wechselwirkungen wahrscheinlich ergibt;

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

27. „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;

28. „Konformitätsbewertung“ das Verfahren, mit dem überprüft wird, ob die grundlegenden Anforderungen in Anhang I erfüllt werden;

29. „Konformitätsbewertungsstelle“ eine Stelle gemäß der Begriffsbestimmung in Artikel 2 Nummer 13 der Verordnung (EG) Nr. 765/2008;

30. „notifizierte Stelle“ eine Konformitätsbewertungsstelle, die nach Artikel 33 dieser Verordnung und anderen einschlägigen Harmonisierungsrechtsvorschriften der Union benannt wurde;

31. „wesentliche Änderung“ eine Änderung des Produkts mit digitalen Elementen nach dessen Inverkehrbringen, die sich auf die Konformität des Produkts mit den grundlegenden Anforderungen in Anhang I Abschnitt 1 auswirkt oder zu einer Änderung der bestimmungsgemäßen Verwendung, für die das Produkt geprüft wurde, führt;

32. „CE-Kennzeichnung“ eine Kennzeichnung, durch die ein Hersteller erklärt, dass ein Produkt mit digitalen Elementen und die vom Hersteller festgelegten Verfahren den grundlegenden Anforderungen in Anhang I und anderen geltenden Rechtsvorschriften der Union zur Harmonisierung der Bedingungen für die Vermarktung von Produkten (im Folgenden „Harmonisierungsrechtsvorschriften der Union“) über ihre Anbringung genügen;

33. „Marktüberwachungsbehörde“ die Behörde gemäß der Begriffsbestimmung in Artikel 3 Nummer 4 der Verordnung (EU) 2019/1020;

34. „harmonisierte Norm“ eine Norm gemäß der Begriffsbestimmung in Artikel 2 Nummer 1 Buchstabe c der Verordnung (EU) Nr. 1025/2012;

35. „Cybersicherheitsrisiko“ das Risiko gemäß der Begriffsbestimmung in Artikel [Artikel X] der Richtlinie [Richtlinie XXX/XXXX (NIS2)];

36. „erhebliches Cybersicherheitsrisiko“ ein Cybersicherheitsrisiko, bei dem aufgrund seiner technischen Merkmale davon auszugehen ist, dass es mit hoher Wahrscheinlichkeit zu einem Sicherheitsvorfall führen wird, der schwerwiegende negative Auswirkungen haben und erhebliche materielle oder immaterielle Verluste oder Störungen verursachen könnte;

37. „Software-Stückliste“ eine formale Aufzeichnung der Einzelheiten und Lieferkettenbeziehungen der Komponenten, die in den Softwareelementen eines Produkts mit digitalen Elementen enthalten sind;

38. „Schwachstelle“ eine Sicherheitslücke gemäß der Begriffsbestimmung in Artikel [Artikel X] der Richtlinie [Richtlinie XXX/XXXX (NIS2)];

39. „aktiv ausgenutzte Schwachstelle“ eine Schwachstelle zu der verlässliche Nachweise dafür vorliegen, dass ein Akteur ohne Zustimmung des Systemeigners schädlichen Programmcode in einem System ausgeführt hat;

40. „personenbezogene Daten“ Daten gemäß der Begriffsbestimmung in Artikel 4 Nummer 1 der Verordnung (EU) 2016/679.

Artikel 4

Freier Verkehr

(1) Die Mitgliedstaaten behindern in den von dieser Verordnung erfassten Aspekten nicht die Bereitstellung auf dem Markt von Produkten mit digitalen Elementen, die dieser Verordnung entsprechen.

(2) Die Mitgliedstaaten verhindern nicht die Präsentation und Verwendung eines Produkts mit digitalen Elementen, das dieser Verordnung nicht entspricht, bei Messen, Ausstellungen und Vorführungen oder ähnlichen Veranstaltungen.

(3) Die Mitgliedstaaten verhindern nicht die Bereitstellung unfertiger Software, die dieser Verordnung nicht entspricht, sofern die Software nur für einen begrenzten Zeitraum zur Verfügung gestellt wird, der für Testzwecke erforderlich ist, und eine sichtbare Kennzeichnung deutlich darauf hinweist, dass sie dieser Verordnung nicht entspricht und außer zu Testzwecken nicht auf dem Markt bereitgestellt wird.

Artikel 5

Anforderungen an Produkte mit digitalen Elementen

Produkte mit digitalen Elementen werden nur dann auf dem Markt bereitgestellt, wenn

1. sie den grundlegenden Anforderungen in Anhang I Abschnitt 1 genügen und unter der Bedingung, dass sie ordnungsgemäß installiert, gewartet und bestimmungsgemäß oder unter vernünftigerweise vorhersehbaren Umständen verwendet sowie gegebenenfalls aktualisiert werden, und

2. die vom Hersteller festgelegten Verfahren den grundlegenden Anforderungen in Anhang I Abschnitt 2 entsprechen.

Artikel 6

Kritische Produkte mit digitalen Elementen

(1) Produkte mit digitalen Elementen, die zu einer in Anhang III aufgeführten Kategorie gehören, gelten als kritische Produkte mit digitalen Elementen. Produkte, die die Kernfunktionen einer in Anhang III dieser Verordnung aufgeführten Kategorie aufweisen, gelten als Produkte, die unter diese Kategorie fallen. Die Kategorien kritischer Produkte mit digitalen Elementen werden gemäß Anhang III unter Berücksichtigung des mit diesen Produkten verbundenen Cybersicherheitsrisikos in die Klassen I und II unterteilt.

(2) Der Kommission wird die Befugnis übertragen, gemäß Artikel 50 delegierte Rechtsakte zur Änderung des Anhangs III zu erlassen, um eine neue Kategorie in die Liste der Kategorien kritischer Produkte mit digitalen Elementen aufzunehmen oder eine bestehende Kategorie von dieser Liste zu streichen. Bei der Bewertung der Notwendigkeit einer Änderung der Liste in Anhang III berücksichtigt die Kommission die Höhe des Cybersicherheitsrisikos, das mit der Kategorie von Produkten mit digitalen Elementen verbunden ist. Die Bestimmung der Höhe des Cybersicherheitsrisikos erfolgt anhand eines oder mehrerer der folgenden Kriterien:

a) die Cybersicherheitsfunktion des Produkts mit digitalen Elementen und ob das Produkt mit digitalen Elementen mindestens eines der folgenden Merkmale aufweist:

   i) Es ist für den Betrieb mit erhöhten Privilegien oder für die Verwaltung von Privilegien konzipiert;

   ii) es hat direkten oder privilegierten Zugang zu Netz- oder Rechenressourcen;

   iii) es ist für die Kontrolle des Zugangs zu Daten oder zu operativer Technik bestimmt;

   iv) es erfüllt eine Funktion, die für das Vertrauen von entscheidender Bedeutung ist, insbesondere eine Sicherheitsfunktion wie Netzsteuerung, Endpunktsicherheit und Schutz des Netzes;

b) die bestimmungsgemäße Verwendung in sensiblen Umgebungen, auch in industriellen Umfeldern oder durch wesentliche Einrichtungen der im Anhang [Anhang I] der Richtlinie [Richtlinie XXX/XXXX (NIS2)] genannten Art;

c) die bestimmungsgemäße Verwendung kritischer oder sensibler Funktionen, wie der Verarbeitung personenbezogener Daten;

d) das potenzielle Ausmaß nachteiliger Auswirkungen, insbesondere hinsichtlich ihrer Intensität und ihrer Eignung, eine Vielzahl von Personen zu beeinträchtigen;

e) das Ausmaß, in dem die Verwendung von Produkten mit digitalen Elementen bereits zu materiellen oder immateriellen Verlusten oder Störungen geführt hat oder Anlass zu erheblichen Bedenken hinsichtlich des Eintretens nachteiliger Auswirkungen gegeben hat.

(3) Der Kommission wird die Befugnis übertragen, gemäß Artikel 50 einen delegierten Rechtsakt zur Ergänzung dieser Verordnung zu erlassen, in dem sie die Definitionen der nach Anhang III zur Klasse I und Klasse II gehörigen Produktkategorien festlegt.

Der delegierte Rechtsakt wird bis zum [12 Monate nach Inkrafttreten dieser Verordnung] erlassen.

(4) Kritische Produkte mit digitalen Elementen unterliegen den Konformitätsbewertungsverfahren nach Artikel 24 Absätze 2 und 3.

(5) Der Kommission wird die Befugnis übertragen, gemäß Artikel 50 delegierte Rechtsakte zur Ergänzung dieser Verordnung zu erlassen, um Kategorien hochkritischer Produkte mit digitalen Elementen festzulegen, für die die Hersteller ein europäisches Cybersicherheitszertifikat im Rahmen eines europäischen Systems für die Cybersicherheitszertifizierung gemäß der Verordnung (EU) 2019/881 erlangen müssen, um die Konformität mit den grundlegenden Anforderungen in Anhang I oder Teilen davon nachzuweisen. Bei der Festlegung solcher Kategorien hochkritischer Produkte mit digitalen Elementen berücksichtigt die Kommission das mit der Kategorie der Produkte mit digitalen Elementen verbundene Cybersicherheitsrisiko im Lichte eines oder mehrerer der in Absatz 2 aufgeführten Kriterien sowie im Hinblick auf die Bewertung, ob Produkte dieser Produktkategorie

a) von wesentlichen Einrichtungen der in Anhang [Anhang I] der Richtlinie [Richtlinie XXX/XXXX (NIS2)] genannten Art verwendet werden oder diese von solchen Produkten abhängen oder solche Produkte möglicherweise künftig für die Tätigkeiten dieser Einrichtungen von Bedeutung sein werden oder

b) für die Widerstandsfähigkeit der gesamten Lieferkette von Produkten mit digitalen Elementen gegen Störungen von Bedeutung sind.

Artikel 7

Allgemeine Produktsicherheit

Abweichend von Artikel 2 Absatz 1 Unterabsatz 3 Buchstabe b der Verordnung [Verordnung über die allgemeine Produktsicherheit] gilt: Wenn Produkte mit digitalen Elementen keinen besonderen Anforderungen unterliegen, die in anderen Harmonisierungsrechtsvorschriften der Union im Sinne des [Artikels 3 Nummer 25 der Verordnung über die allgemeine Produktsicherheit] festgelegt sind, so finden in Bezug auf nicht von der vorliegenden Verordnung erfasste Sicherheitsrisiken auf diese Produkte das Kapitel III Abschnitt 1, die Kapitel V und VII sowie die Kapitel IX bis XI der Verordnung [Verordnung über die allgemeine Produktsicherheit] Anwendung.

Artikel 8

Hochrisiko-KI-Systeme

(1) Produkte mit digitalen Elementen, die nach Artikel [Artikel 6] der Verordnung [KI-Verordnung] als Hochrisiko-KI-Systeme eingestuft sind, in den Anwendungsbereich der vorliegenden Verordnung fallen und die grundlegenden Anforderungen in Anhang I Abschnitt 1 der vorliegenden Verordnung erfüllen, gelten – sofern die vom Hersteller festgelegten Verfahren die grundlegenden Anforderungen in Anhang I Abschnitt 2 erfüllen – unbeschadet der anderen in dem genannten Artikel aufgeführten Anforderungen in Bezug auf Genauigkeit und Robustheit als mit den Cybersicherheitsanforderungen gemäß Artikel [Artikel 15] der Verordnung [KI-Verordnung] konform, soweit das Erreichen des nach diesen Anforderungen erforderlichen Schutzniveaus durch die nach der vorliegenden Verordnung ausgestellte EU-Konformitätserklärung nachgewiesen wird.

(2) Für die in Absatz 1 genannten Produkte und Cybersicherheitsanforderungen gilt das einschlägige Konformitätsbewertungsverfahren gemäß Artikel [Artikel 43] der Verordnung [KI-Verordnung]. Für die Zwecke dieser Bewertung sind die notifizierten Stellen, die gemäß der Verordnung [KI-Verordnung] berechtigt sind, die Konformität der Hochrisiko-KI-Systeme zu kontrollieren, auch berechtigt, im Rahmen der vorliegenden Verordnung die Konformität der Hochrisiko-KI-Systeme mit den Anforderungen in Anhang I der vorliegenden Verordnung zu kontrollieren, sofern in dem nach der Verordnung [KI-Verordnung] durchgeführten Notifizierungsverfahren geprüft wurde, ob diese notifizierten Stellen die in Artikel 29 der vorliegenden Verordnung festgelegten Anforderungen erfüllen.

(3) Abweichend von Absatz 2 unterliegen die in Anhang III der vorliegenden Verordnung aufgeführten kritischen Produkte mit digitalen Elementen, die den Konformitätsbewertungsverfahren gemäß Artikel 24 Absatz 2 Buchstabe a, Artikel 24 Absatz 2 Buchstabe b, Artikel 24 Absatz 3 Buchstabe a und Artikel 24 Absatz 3 Buchstabe b der vorliegenden Verordnung unterliegen und auch nach Artikel [Artikel 6] der Verordnung [KI-Verordnung] als Hochrisiko-KI-Systeme eingestuft sind und für die das Konformitätsbewertungsverfahren auf der Grundlage einer internen Kontrolle gemäß Anhang [Anhang VI] der Verordnung [KI-Verordnung] gilt, den Konformitätsbewertungsverfahren gemäß der vorliegenden Verordnung, soweit dies die grundlegenden Anforderungen der vorliegenden Verordnung betrifft.

Artikel 9

Maschinenprodukte

Maschinenprodukte, die in den Anwendungsbereich der Verordnung [Vorschlag für eine Maschinenverordnung] fallen, bei denen es sich um Produkte mit digitalen Elementen im Sinne der vorliegenden Verordnung handelt und für die auf der Grundlage der vorliegenden Verordnung eine EU-Konformitätserklärung ausgestellt wurde, gelten in Bezug auf den Schutz vor Korruption und die Sicherheit und Zuverlässigkeit von Steuerungssystemen als konform mit den grundlegenden Gesundheits- und Sicherheitsanforderungen in Anhang [Anhang III Abschnitte 1.1.9 und 1.2.1] der Verordnung [Vorschlag für eine Maschinenverordnung], sofern das Erreichen des nach diesen Anforderungen erforderlichen Schutzniveaus mit der nach der vorliegenden Verordnung ausgestellten EU-Konformitätserklärung nachgewiesen wird.

KAPITEL II

PFLICHTEN DER WIRTSCHAFTSAKTEURE

Artikel 10

Pflichten der Hersteller

(1) Wenn sie ein Produkt mit digitalen Elementen in Verkehr bringen, gewährleisten die Hersteller, dass das Produkt gemäß den grundlegenden Anforderungen in Anhang I Abschnitt 1 konzipiert, entwickelt und hergestellt worden ist.

(2) Für die Zwecke der Erfüllung der in Absatz 1 festgelegten Pflicht führen die Hersteller eine Bewertung der Cybersicherheitsrisiken durch, die ein Produkt mit digitalen Elementen birgt, und berücksichtigen das Ergebnis dieser Bewertung in der

Planungs-, Konzeptions-, Entwicklungs-, Herstellungs-, Liefer- und Wartungsphase des Produkts mit digitalen Elementen, um die Cybersicherheitsrisiken zu minimieren, Sicherheitsvorfälle zu verhindern und die Auswirkungen solcher Vorfälle, auch in Bezug auf die Gesundheit und Sicherheit der Nutzer, so gering wie möglich zu halten.

(3) Wenn er ein Produkt mit digitalen Elementen in Verkehr bringt, nimmt der Hersteller in die technische Dokumentation gemäß Artikel 23 und Anhang V eine Bewertung der Cybersicherheitsrisiken auf. Bei Produkten mit digitalen Elementen gemäß Artikel 8 und Artikel 24 Absatz 4, die auch anderen Unionsvorschriften unterliegen, kann die Bewertung der Cybersicherheitsrisiken auch Teil der in den betreffenden Unionsvorschriften geforderten Risikobewertungen sein. Sind bestimmte grundlegende Anforderungen nicht auf das in Verkehr gebrachte Produkt mit digitalen Elementen anwendbar, so nimmt der Hersteller eine klare Begründung hierfür in diese Dokumentation auf.

(4) Für die Zwecke der Erfüllung der in Absatz 1 festgelegten Pflicht lassen die Hersteller die gebotene Sorgfalt walten, wenn sie von Dritten bezogene Komponenten in ihre Produkte mit digitalen Elementen integrieren. Sie stellen sicher, dass solche Komponenten die Sicherheit des Produkts mit digitalen Elementen nicht beeinträchtigen.

(5) Der Hersteller dokumentiert systematisch und in einer der Art der Cybersicherheitsrisiken angemessenen Weise alle relevante Cybersicherheitsaspekte des Produkts mit digitalen Elementen, einschließlich der Schwachstellen, von denen er Kenntnis erlangt, und aller von Dritten bereitgestellten einschlägigen Informationen und aktualisiert gegebenenfalls die Risikobewertung des Produkts.

(6) Wenn sie ein Produkt mit digitalen Elementen in Verkehr bringen und während der erwarteten Produktlebensdauer oder während eines Zeitraums von fünf Jahren ab dem Inverkehrbringen des Produkts, je nachdem, welcher Zeitraum kürzer ist, stellen die Hersteller sicher, dass Schwachstellen dieses Produkts wirksam und im Einklang mit den grundlegenden Anforderungen in Anhang I Abschnitt 2 behandelt werden.

Die Hersteller haben geeignete Strategien und Verfahren, darunter Konzepte für die koordinierte Offenlegung der in Anhang I Abschnitt 2 Nummer 5 genannten Schwachstellen, um potenzielle Schwachstellen in dem Produkt mit digitalen Elementen, die von internen oder externen Quellen gemeldet werden, zu bearbeiten und zu beheben.

(7) Bevor sie ein Produkt mit digitalen Elementen in Verkehr bringen, erstellen die Hersteller die in Artikel 23 genannte technische Dokumentation.

Sie führen die gewählten Konformitätsbewertungsverfahren gemäß Artikel 24 durch oder lassen sie durchführen.

Ist mit diesem Konformitätsbewertungsverfahren nachgewiesen worden, dass das Produkt mit digitalen Elementen den grundlegenden Anforderungen in Anhang I Abschnitt 1 genügt und die vom Hersteller festgelegten Verfahren den grundlegenden Anforderungen in Anhang I Abschnitt 2 genügen, so stellen die Hersteller die EU-Konformitätserklärung gemäß Artikel 20 aus und bringen die CE-Kennzeichnung gemäß Artikel 22 an.

(8) Die Hersteller bewahren die technische Dokumentation und gegebenenfalls die EU-Konformitätserklärung nach dem Inverkehrbringen des Produkts mit digitalen Elementen zehn Jahre lang für die Marktüberwachungsbehörden auf.

(9) Die Hersteller gewährleisten durch geeignete Verfahren, dass die Konformität von Produkten mit digitalen Elementen bei einer Serienherstellung sichergestellt bleibt. Der Hersteller berücksichtigt in angemessener Weise etwaige Änderungen am Entwicklungs- und Herstellungsverfahren oder an der Konzeption oder den Merkmalen des Produkts mit digitalen Elementen sowie Änderungen der harmonisierten Normen, der europäischen Systeme für die Cybersicherheitszertifizierung oder der in Artikel 19 genannten gemeinsamen Spezifikationen, die bei der Erklärung der Konformität des Produkts mit digitalen Elementen zugrunde gelegt oder bei der Überprüfung seiner Konformität angewandt wurden.

(10) Die Hersteller gewährleisten, dass den Produkten mit digitalen Elementen die in Anhang II genannten Informationen und Anleitungen in elektronischer Form oder in Papierform beigefügt sind. Diese Informationen und Anleitungen müssen in einer Sprache abgefasst sein, die von den Nutzern leicht verstanden werden kann. Sie müssen klar, verständlich, deutlich und lesbar sein. Sie müssen eine sichere Installation, einen sicheren Betrieb und eine sichere Verwendung der Produkte mit digitalen Elementen ermöglichen.

(11) Die Hersteller fügen die EU-Konformitätserklärung entweder dem Produkt mit digitalen Elementen bei oder geben in den Anleitungen und Informationen gemäß Anhang II die Internetadresse an, unter der die EU-Konformitätserklärung eingesehen werden kann.

(12) Ab dem Inverkehrbringen und während der erwarteten Produktlebensdauer oder während eines Zeitraums von fünf Jahren ab dem Inverkehrbringen eines Produkts mit digitalen Elementen, je nachdem, welcher Zeitraum kürzer ist, ergreifen die Hersteller, denen bekannt ist oder die Grund zu der Annahme haben, dass das Produkt mit digitalen Elementen oder die vom Hersteller festgelegten Verfahren den grundlegenden Anforderungen in Anhang I nicht genügen, unverzüglich die erforderlichen Korrekturmaßnahmen, um die Konformität dieses Produkts mit digitalen Elementen oder der Prozesse des Herstellers herzustellen oder um gegebenenfalls das Produkt vom Markt zu nehmen oder zurückzurufen.

(13) Die Hersteller übermitteln der Marktüberwachungsbehörde auf deren begründetes Verlangen in Papierform oder in elektronischer Form in einer für die Behörde leicht verständlichen Sprache alle Informationen und Unterlagen, die für den Nachweis der Konformität des Produkts mit digitalen Elementen und der vom Hersteller festgelegten Verfahren mit den grundlegenden Anforderungen in Anhang I erforderlich sind. Sie arbeiten mit dieser Behörde auf deren Verlangen bei allen Maßnahmen zur Abwendung der Cybersicherheitsrisiken zusammen, die mit dem von ihnen in Verkehr gebrachten Produkt mit digitalen Elementen verbunden sind.

(14) Ein Hersteller, der seine Betriebstätigkeit einstellt und infolgedessen nicht in der Lage ist, die in dieser Verordnung festgelegten Pflichten zu erfüllen, unterrichtet hiervon vor dem Wirksamwerden der Betriebseinstellung die zuständigen Marktüberwachungsbehörden sowie – mit allen verfügbaren Mitteln und soweit möglich – die Nutzer der betroffenen in Verkehr gebrachten Produkte mit digitalen Elementen.

(15) Die Kommission kann im Wege von Durchführungsrechtsakten das Format und die Elemente der Software-Stückliste gemäß Anhang I Abschnitt 2 Nummer 1 festlegen. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 51 Absatz 2 genannten Prüfverfahren erlassen.

Artikel 11

Meldepflichten der Hersteller

(1) Der Hersteller meldet der ENISA unverzüglich, jedenfalls aber innerhalb von 24 Stunden, nachdem er davon Kenntnis erlangt hat, jede aktiv ausgenutzte Schwachstelle, die in dem Produkt mit digitalen Elementen enthalten ist. Die Meldung enthält Einzelheiten zu dieser Schwachstelle und zu den gegebenenfalls ergriffenen Korrektur- oder Minderungsmaßnahmen. Die ENISA leitet die Meldung nach dem Eingang unverzüglich an das für die Zwecke der koordinierten Offenlegung von Schwachstellen gemäß Artikel [Artikel X] der Richtlinie [Richtlinie XXX/XXXX (NIS2)] benannte CSIRT der betroffenen Mitgliedstaaten weiter und unterrichtet die Marktüberwachungsbehörde von der gemeldeten Schwachstelle, sofern dem keine berechtigten Gründe in Bezug auf das Cybersicherheitsrisiko entgegenstehen.

(2) Der Hersteller meldet der ENISA unverzüglich, jedenfalls aber innerhalb von 24 Stunden, nachdem er davon Kenntnis erlangt hat, jeden Vorfall, der sich auf die Sicherheit des Produkts mit digitalen Elementen auswirkt. Die ENISA leitet die Meldungen unverzüglich an die gemäß Artikel [Artikel X] der Richtlinie [Richtlinie XXX/XXXX (NIS2)] benannte zentrale Anlaufstelle der betroffenen Mitgliedstaaten weiter und unterrichtet die Marktüberwachungsbehörde von den gemeldeten Vorfällen, sofern dem keine berechtigten Gründe in Bezug auf das Cybersicherheitsrisiko entgegenstehen. Die Meldung eines Vorfalls enthält Informationen über die Schwere und die Auswirkungen des Vorfalls und gegebenenfalls Angaben dazu, ob der Hersteller den Verdacht hat, dass der Vorfall durch rechtswidrige oder böswillige Handlungen verursacht wurde, oder ob er davon ausgeht, dass der Vorfall grenzüberschreitende Auswirkungen hat.

(3) Die ENISA übermittelt dem Europäischen Netzwerk der Verbindungsorganisationen für Cyberkrisen (EU-CyCLONe), das durch Artikel [Artikel X] der Richtlinie [Richtlinie XXX/XXXX (NIS2)] eingerichtet wurde, die gemäß den Absätzen 1 und 2 gemeldeten Informationen, sofern diese Informationen für das koordinierte Management massiver Cybersicherheitsvorfälle und -krisen auf operativer Ebene von Bedeutung sind.

(4) Der Hersteller informiert die Nutzer des Produkts mit digitalen Elementen unverzüglich, nachdem er Kenntnis davon erlangt hat, über den Vorfall und erforderlichenfalls über Korrekturmaßnahmen, die der Nutzer ergreifen kann, um die Auswirkungen des Vorfalls zu mindern.

(5) Die Kommission kann im Wege von Durchführungsrechtsakten die Art der Angaben sowie das Format und Verfahren für die nach den Absätzen 1 und 2 übermittelten Meldungen präzisieren. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 51 Absatz 2 genannten Prüfverfahren erlassen.

(6) Die ENISA erstellt auf der Grundlage der nach den Absätzen 1 und 2 eingegangenen Meldungen alle zwei Jahre einen technischen Bericht über aufkommende Trends der Cybersicherheitsrisiken bei Produkten mit digitalen Elementen und legt ihn der in Artikel [X] der Richtlinie [Richtlinie XXX/XXXX (NIS2)] genannten Kooperationsgruppe vor. Der erste solche Bericht wird innerhalb von 24 Monaten nach Beginn der Geltung der in den Absätzen 1 und 2 festgelegten Pflichten vorgelegt.

(7) Sobald der Hersteller eine Schwachstelle in einer in das Produkt mit digitalen Elementen integrierten Komponente, einschließlich einer Open-Source-Komponente, feststellt, meldet er die Schwachstelle der Person oder Einrichtung, die diese Komponente wartet.

Artikel 12

Bevollmächtigte

(1) Ein Hersteller kann schriftlich einen Bevollmächtigten benennen.

(2) Die in Artikel 10 Absätze 1 bis 7 erster Spiegelstrich und Absatz 9 festgelegten Pflichten sind nicht Teil des Auftrags des Bevollmächtigten.

(3) Ein Bevollmächtigter nimmt die Aufgaben wahr, die in dem vom Hersteller erteilten Auftrag festgelegt sind. Der Auftrag muss es dem Bevollmächtigten ermöglichen, mindestens folgende Aufgaben wahrzunehmen:

a) Bereithaltung der in Artikel 20 genannten EU-Konformitätserklärung und der in Artikel 23 genannten technischen Dokumentation für die Marktüberwachungsbehörden zehn Jahre lang ab dem Inverkehrbringen des Produkts mit digitalen Elementen;

b) Übermittlung aller zum Nachweis der Konformität des Produkts mit digitalen Elementen erforderlichen Informationen und Unterlagen an eine Marktüberwachungsbehörde auf deren begründetes Verlangen;

c) Zusammenarbeit mit den Marktüberwachungsbehörden auf deren Verlangen bei allen Maßnahmen zur Abwendung der Risiken, die von einem Produkt mit digitalen Elementen ausgehen, das zum Aufgabenbereich des Bevollmächtigten gehört.

Artikel 13

Pflichten der Einführer

(1) Die Einführer bringen nur Produkte mit digitalen Elementen in Verkehr, die den grundlegenden Anforderungen in Anhang I Abschnitt 1 genügen und bei denen die vom Hersteller festgelegten Verfahren den grundlegenden Anforderungen in Anhang I Abschnitt 2 genügen.

(2) Bevor sie ein Produkt mit digitalen Elementen in Verkehr bringen, stellen die Einführer sicher, dass

a) der Hersteller die geeigneten Konformitätsbewertungsverfahren nach Artikel 24 durchgeführt hat;

b) der Hersteller die technische Dokumentation erstellt hat;

c) das Produkt mit digitalen Elementen mit der in Artikel 22 genannten CE-Kennzeichnung versehen ist und ihm die Informationen und Gebrauchsanleitungen gemäß Anhang II beigefügt sind.

(3) Ist ein Einführer der Auffassung oder hat er Grund zu der Annahme, dass ein Produkt mit digitalen Elementen oder die vom Hersteller festgelegten Verfahren den grundlegenden Anforderungen in Anhang I nicht genügen, bringt er das Produkt erst dann in Verkehr, wenn die Konformität dieses Produkts und der vom Hersteller festgelegten Verfahren mit den grundlegenden Anforderungen in Anhang I

hergestellt ist. Wenn das Produkt mit digitalen Elementen ein erhebliches Cybersicherheitsrisiko birgt, unterrichtet der Einführer zudem den Hersteller und die Marktüberwachungsbehörden hiervon.

(4) Die Einführer geben ihren Namen, ihren eingetragenen Handelsnamen oder ihre eingetragene Handelsmarke, ihre Postanschrift und ihre E-Mail-Adresse, unter der sie zu erreichen sind, entweder auf dem Produkt mit digitalen Elementen selbst oder, wenn dies nicht möglich ist, auf der Verpackung oder in den dem Produkt mit digitalen Elementen beigefügten Unterlagen an. Die Kontaktangaben sind in einer Sprache abzufassen, die von den Nutzern und den Marktüberwachungsbehörden leicht verstanden werden kann.

(5) Die Einführer stellen sicher, dass dem Produkt mit digitalen Elementen die Anleitungen und Informationen gemäß Anhang II in einer Sprache, die von den Nutzern leicht verstanden werden kann, beigefügt sind.

(6) Einführer, denen bekannt ist oder die Grund zu der Annahme haben, dass ein Produkt mit digitalen Elementen, das sie in Verkehr gebracht haben, oder die von dessen Hersteller festgelegten Verfahren den grundlegenden Anforderungen in Anhang I nicht genügen, ergreifen unverzüglich die erforderlichen Korrekturmaßnahmen, um die Konformität dieses Produkts mit digitalen Elementen und der vom Hersteller festgelegten Verfahren mit den grundlegenden Anforderungen in Anhang I herzustellen oder um gegebenenfalls das Produkt vom Markt zu nehmen oder zurückzurufen.

Bei Feststellung einer Schwachstelle in dem Produkt mit digitalen Elementen informieren die Einführer den Hersteller unverzüglich über diese Schwachstelle. Wenn das Produkt mit digitalen Elementen ein erhebliches Cybersicherheitsrisiko birgt, unterrichten die Einführer zudem unverzüglich die Marktüberwachungsbehörden der Mitgliedstaaten, in denen sie das Produkt mit digitalen Elementen auf dem Markt bereitgestellt haben, und machen dabei genaue Angaben insbesondere über die Nichtkonformität und ergriffene Korrekturmaßnahmen.

(7) Die Einführer halten ab dem Inverkehrbringen des Produkts mit digitalen Elementen zehn Jahre lang ein Exemplar der EU-Konformitätserklärung für die Marktüberwachungsbehörden bereit und sorgen dafür, dass sie diesen die technische Dokumentation auf Verlangen vorlegen können.

(8) Die Einführer übermitteln der Marktüberwachungsbehörde auf deren begründetes Verlangen in Papierform oder in elektronischer Form in einer Sprache, die von der Behörde leicht verstanden werden kann, alle Informationen und Unterlagen, die für den Nachweis der Konformität des Produkts mit digitalen Elementen mit den grundlegenden Anforderungen in Anhang I Abschnitt 1 und der vom Hersteller festgelegten Verfahren mit den grundlegenden Anforderungen in Anhang I Abschnitt 2 erforderlich sind. Sie arbeiten mit dieser Behörde auf deren Verlangen bei allen Maßnahmen zur Abwendung der Cybersicherheitsrisiken zusammen, die mit einem von ihnen in Verkehr gebrachten Produkt mit digitalen Elementen verbunden sind.

(9) Wird dem Einführer eines Produkts mit digitalen Elementen bekannt, dass der Hersteller dieses Produkts seine Betriebstätigkeit eingestellt hat und infolgedessen nicht in der Lage ist, die in dieser Verordnung festgelegten Pflichten zu erfüllen, unterrichtet er hiervon die zuständigen Marktüberwachungsbehörden sowie – mit

allen verfügbaren Mitteln und soweit möglich – die Nutzer der in Verkehr gebrachten Produkte mit digitalen Elementen.

Artikel 14

Pflichten der Händler

(1) Wenn sie ein Produkt mit digitalen Elementen auf dem Markt bereitstellen, befolgen die Händler die Vorschriften dieser Verordnung mit der gebührenden Sorgfalt.

(2) Bevor sie ein Produkt mit digitalen Elementen auf dem Markt bereitstellen, überprüfen die Händler, ob

a) das Produkt mit digitalen Elementen mit der CE-Kennzeichnung versehen ist;

b) der Hersteller und der Einführer die Anforderungen nach Artikel 10 Absatz 10, Artikel 10 Absatz 11 bzw. Artikel 13 Absatz 4 erfüllt haben.

(3) Ist ein Händler der Auffassung oder hat er Grund zu der Annahme, dass ein Produkt mit digitalen Elementen oder die vom Hersteller festgelegten Verfahren den grundlegenden Anforderungen in Anhang I nicht genügen, stellt er das Produkt mit digitalen Elementen erst dann auf dem Markt bereit, wenn die Konformität dieses Produkts und der vom Hersteller festgelegten Verfahren hergestellt ist. Wenn das Produkt mit digitalen Elementen ein erhebliches Cybersicherheitsrisiko birgt, unterrichtet der Händler zudem den Hersteller und die Marktüberwachungsbehörden hiervon.

(4) Händler, denen bekannt ist oder die Grund zu der Annahme haben, dass ein Produkt mit digitalen Elementen, das sie auf dem Markt bereitgestellt haben, oder die von dessen Hersteller festgelegten Verfahren den grundlegenden Anforderungen in Anhang I nicht genügen, sorgt dafür, dass unverzüglich die erforderlichen Korrekturmaßnahmen ergriffen werden, um die Konformität dieses Produkts mit digitalen Elementen und der vom Hersteller festgelegten Verfahren herzustellen oder um gegebenenfalls das Produkt vom Markt zu nehmen oder zurückzurufen.

Bei Feststellung einer Schwachstelle in dem Produkt mit digitalen Elementen informieren die Händler den Hersteller unverzüglich über diese Schwachstelle. Wenn das Produkt mit digitalen Elementen ein erhebliches Cybersicherheitsrisiko birgt, unterrichten die Händler zudem unverzüglich die Marktüberwachungsbehörden der Mitgliedstaaten, in denen sie das Produkt mit digitalen Elementen auf dem Markt bereitgestellt haben, und machen dabei genaue Angaben insbesondere über die Nichtkonformität und ergriffene Korrekturmaßnahmen.

(5) Die Händler übermitteln der Marktüberwachungsbehörde auf deren begründetes Verlangen in Papierform oder in elektronischer Form in einer Sprache, die von der Behörde leicht verstanden werden kann, alle Informationen und Unterlagen, die für den Nachweis der Konformität des Produkts mit digitalen Elementen und der vom Hersteller festgelegten Verfahren mit den grundlegenden Anforderungen in Anhang I erforderlich sind. Sie arbeiten mit dieser Behörde auf deren Verlangen bei allen Maßnahmen zur Abwendung der Cybersicherheitsrisiken zusammen, die mit einem von ihnen auf dem Markt bereitgestellten Produkt mit digitalen Elementen verbunden sind.

(6) Wird dem Händler eines Produkts mit digitalen Elementen bekannt, dass der Hersteller dieses Produkts seine Betriebstätigkeit eingestellt hat und infolgedessen nicht in der Lage ist, die in dieser Verordnung festgelegten Pflichten zu erfüllen,

unterrichtet er hiervon die zuständigen Marktüberwachungsbehörden sowie – mit allen verfügbaren Mitteln und soweit möglich – die Nutzer der in Verkehr gebrachten Produkte mit digitalen Elementen.

Artikel 15

Fälle, in denen die Pflichten der Hersteller auch für Einführer und Händler gelten

Ein Einführer oder Händler gilt für die Zwecke dieser Verordnung als Hersteller und unterliegt den in Artikel 10 und Artikel 11 Absätze 1, 2, 4 und 7 genannten Pflichten des Herstellers, wenn dieser Einführer oder Händler ein Produkt mit digitalen Elementen unter seinem eigenen Namen oder seiner eigenen Marke in Verkehr bringt oder eine wesentliche Änderung an einem bereits in Verkehr gebrachten Produkt mit digitalen Elementen vornimmt.

Artikel 16

Sonstige Fälle, in denen die Pflichten der Hersteller gelten

Eine natürliche oder juristische Person, bei der es sich nicht um den Hersteller, Einführer oder Händler handelt und die eine wesentliche Änderung an dem Produkt mit digitalen Elementen vornimmt, gilt für die Zwecke dieser Verordnung als Hersteller.

Diese Person unterliegt den Pflichten des Herstellers gemäß Artikel 10 und Artikel 11 Absätze 1, 2, 4 und 7 für den Teil des Produkts, der von der wesentlichen Änderung betroffen ist, oder, wenn sich die wesentliche Änderung auf die Cybersicherheit des Produkts mit digitalen Elementen insgesamt auswirkt, für das gesamte Produkt.

Artikel 17

Identifizierung der Wirtschaftsakteure

(1) Die Wirtschaftsakteure übermitteln den Marktüberwachungsbehörden auf Anfrage folgende Informationen, sofern diese verfügbar sind:

a) Name und Anschrift aller Wirtschaftsakteure, von denen sie Produkte mit digitalen Elementen bezogen haben,

b) Name und Anschrift aller Wirtschaftsakteure, an die sie Produkte mit digitalen Elementen abgegeben haben.

(2) Die Wirtschaftsakteure müssen diese in Absatz 1 genannten Informationen zehn Jahre nach dem Bezug des Produkts mit digitalen Elementen sowie zehn Jahre nach der Abgabe des Produkts mit digitalen Elementen vorlegen können.

KAPITEL III

Konformität des Produkts mit digitalen Elementen

Artikel 18

Konformitätsvermutung

(1) Bei Produkten mit digitalen Elementen und vom Hersteller festgelegten Verfahren, die mit harmonisierten Normen oder Teilen davon übereinstimmen, deren Fundstellen im *Amtsblatt der Europäischen Union* veröffentlicht worden sind, wird eine Konformität mit den grundlegenden Anforderungen in Anhang I vermutet,

soweit diese Anforderungen von den betreffenden Normen oder Teilen davon abgedeckt sind.

(2) Bei Produkten mit digitalen Elementen und vom Hersteller festgelegten Verfahren, die mit den in Artikel 19 genannten gemeinsamen Spezifikationen übereinstimmen, wird eine Konformität mit den Anforderungen in Anhang I vermutet, soweit die gemeinsamen Spezifikationen diese Anforderungen abdecken.

(3) Bei Produkten mit digitalen Elementen und vom Hersteller festgelegten Verfahren, für die eine EU-Konformitätserklärung oder ein Cybersicherheitszertifikat im Rahmen eines gemäß der Verordnung (EU) 2019/881 angenommenen und gemäß Absatz 4 ausgewiesenen europäischen Systems für die Cybersicherheitszertifizierung ausgestellt wurde, wird eine Konformität mit den grundlegenden Anforderungen in Anhang I vermutet, sofern die EU-Konformitätserklärung oder das Cybersicherheitszertifikat oder Teile davon diese Anforderungen abdecken.

(4) Der Kommission wird die Befugnis übertragen, im Wege von Durchführungsrechtsakten die gemäß der Verordnung (EU) 2019/881 angenommenen europäischen Systeme für die Cybersicherheitszertifizierung auszuweisen, die zum Nachweis der Konformität mit den grundlegenden Anforderungen in Anhang I oder Teilen davon verwendet werden können. Darüber hinaus gibt die Kommission gegebenenfalls an, ob mit einem im Rahmen eines solchen Systems ausgestellten Cybersicherheitszertifikat die in Artikel 24 Absatz 2 Buchstaben a und b und Artikel 24 Absatz 3 Buchstaben a und b vorgesehene Pflicht des Herstellers, für die betreffenden Anforderungen eine Konformitätsbewertung durch Dritte durchführen zu lassen, aufgehoben werden kann. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 51 Absatz 2 genannten Prüfverfahren erlassen.

Artikel 19

Gemeinsame Spezifikationen

Gibt es keine harmonisierten Normen gemäß Artikel 18 oder ist die Kommission der Auffassung, dass die einschlägigen harmonisierten Normen nicht ausreichen, um die Anforderungen dieser Verordnung zu erfüllen oder dem Normungsauftrag der Kommission gerecht zu werden, oder treten unangemessene Verzögerungen im Normungsverfahren auf oder wird der Auftrag der Kommission zur Ausarbeitung harmonisierter Normen von den europäischen Normungsorganisationen nicht angenommen, so wird der Kommission die Befugnis übertragen, im Wege von Durchführungsrechtsakten gemeinsame Spezifikationen für die grundlegenden Anforderungen in Anhang I anzunehmen. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 51 Absatz 2 genannten Prüfverfahren erlassen.

Artikel 20

EU-Konformitätserklärung

(1) Die EU-Konformitätserklärung wird vom Hersteller gemäß Artikel 10 Absatz 7 ausgestellt und besagt, dass die Erfüllung der grundlegenden Anforderungen in Anhang I nachgewiesen worden ist.

(2) Die EU-Konformitätserklärung entspricht in ihrem Aufbau dem Muster in Anhang IV und enthält die in den einschlägigen Konformitätsbewertungsverfahren

gemäß Anhang VI angegebenen Elemente. Eine solche Erklärung wird laufend aktualisiert. Sie wird in der Sprache bzw. den Sprachen abgefasst, die der Mitgliedstaat vorschreibt, in dem das Produkt mit digitalen Elementen in Verkehr gebracht oder auf dem Markt bereitgestellt wird.

(3) Unterliegt ein Produkt mit digitalen Elementen mehreren Rechtsvorschriften der Europäischen Union, in denen jeweils eine EU-Konformitätserklärung vorgeschrieben ist, so wird eine einzige EU-Konformitätserklärung für sämtliche Unionsvorschriften ausgestellt. In dieser Erklärung werden die betreffenden Rechtsvorschriften der Union samt ihren Fundstellen im Amtsblatt angegeben.

(4) Mit der Ausstellung der EU-Konformitätserklärung übernimmt der Hersteller die Verantwortung für die Konformität des Produkts.

(5) Der Kommission wird die Befugnis übertragen, gemäß Artikel 50 delegierte Rechtsakte zur Ergänzung dieser Verordnung zu erlassen, um angesichts der technischen Entwicklungen zu den in Anhang IV aufgeführten Mindestangaben für die EU-Konformitätserklärung neue Elemente hinzuzufügen.

Artikel 21

Allgemeine Grundsätze der CE-Kennzeichnung

Für die CE-Kennzeichnung im Sinne des Artikels 3 Nummer 32 gelten die allgemeinen Grundsätze gemäß Artikel 30 der Verordnung (EG) Nr. 765/2008.

Artikel 22

Vorschriften und Bedingungen für die Anbringung der CE-Kennzeichnung

(1) Die CE-Kennzeichnung ist gut sichtbar, leserlich und dauerhaft auf dem Produkt mit digitalen Elementen anzubringen. Falls die Art des Produkts mit digitalen Elementen dies nicht zulässt oder nicht rechtfertigt, wird die CE-Kennzeichnung auf der Verpackung und der dem Produkt mit digitalen Elementen beigefügten EU-Konformitätserklärung gemäß Artikel 20 angebracht. Bei Produkten mit digitalen Elementen in Form von Software wird die CE-Kennzeichnung entweder auf der EU-Konformitätserklärung gemäß Artikel 20 oder auf der das Softwareprodukt begleitenden Website angebracht.

(2) Aufgrund der Art des Produkts mit digitalen Elementen kann die Höhe des daran angebrachten CE-Kennzeichens kleiner als 5 mm sein, sofern es weiterhin sichtbar und lesbar ist.

(3) Die CE-Kennzeichnung wird vor dem Inverkehrbringen des Produkts mit digitalen Elementen angebracht. Ihr kann ein Piktogramm oder ein anderes Zeichen folgen, das auf ein besonderes Risiko oder eine besondere Verwendung hinweist, die in Durchführungsrechtsakten gemäß Absatz 6 festgelegt werden.

(4) Auf die CE-Kennzeichnung folgt die Kennnummer der notifizierten Stelle, sofern diese an dem Konformitätsbewertungsverfahren auf der Grundlage einer umfassenden Qualitätssicherung (auf der Grundlage von Modul H) gemäß Artikel 24 beteiligt ist.

Die Kennnummer der notifizierten Stelle wird entweder von der Stelle selbst oder nach ihren Anweisungen vom Hersteller oder seinem Bevollmächtigten angebracht.

(5) Die Mitgliedstaaten bauen auf bestehenden Mechanismen auf, um eine ordnungsgemäße Durchführung des Systems der CE-Kennzeichnung sicherzustellen, und leiten im Fall einer missbräuchlichen Verwendung dieser Kennzeichnung angemessene Maßnahmen ein. Falls das Produkt mit digitalen Elementen auch unter andere Rechtsvorschriften der Union fällt, in denen die CE-Kennzeichnung ebenfalls vorgesehen ist, bedeutet die CE-Kennzeichnung, dass das Produkt auch die Anforderungen dieser anderen Rechtsvorschriften erfüllt.

(6) Die Kommission kann im Wege von Durchführungsrechtsakten technische Spezifikationen für Piktogramme oder andere Kennzeichen in Bezug auf die Sicherheit von Produkten mit digitalen Elementen sowie Mechanismen zur Förderung ihrer Verwendung festlegen. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 51 Absatz 2 genannten Prüfverfahren erlassen.

Artikel 23

Technische Dokumentation

(1) Die technische Dokumentation enthält alle einschlägigen Daten oder Einzelheiten darüber, wie der Hersteller sicherstellt, dass das Produkt mit digitalen Elementen und die vom Hersteller festgelegten Verfahren den grundlegenden Anforderungen in Anhang I genügen. Sie enthält zumindest die in Anhang V genannten Angaben.

(2) Die technische Dokumentation wird vor dem Inverkehrbringen des Produkts mit digitalen Elementen erstellt und gegebenenfalls während der erwarteten Produktlebensdauer oder während eines Zeitraums von fünf Jahren ab dem Inverkehrbringen des Produkts mit digitalen Elementen, je nachdem, welcher Zeitraum kürzer ist, laufend aktualisiert.

(3) Bei Produkten mit digitalen Elementen gemäß Artikel 8 und Artikel 24 Absatz 4, die auch anderen Unionsvorschriften unterliegen, wird eine einzige technische Dokumentation erstellt, die die in Anhang V dieser Verordnung genannten Informationen sowie die nach den anderen Unionsvorschriften erforderlichen Informationen enthält.

(4) Die technische Dokumentation und die Korrespondenz im Zusammenhang mit den Konformitätsbewertungsverfahren werden in einer Amtssprache des Mitgliedstaats, in dem die notifizierte Stelle ansässig ist, oder in einer von dieser Stelle zugelassenen Sprache abgefasst.

(5) Der Kommission wird die Befugnis übertragen, gemäß Artikel 50 delegierte Rechtsakte zu erlassen, mit denen diese Verordnung um die Elemente ergänzt wird, die in die technische Dokumentation gemäß Anhang V aufzunehmen sind, um den technischen Entwicklungen und den Entwicklungen bei der Durchführung dieser Verordnung Rechnung zu tragen.

Artikel 24

Konformitätsbewertungsverfahren für Produkte mit digitalen Elementen

(1) Der Hersteller führt eine Konformitätsbewertung des Produkts mit digitalen Elementen und der vom Hersteller festgelegten Verfahren durch, um festzustellen, ob die grundlegenden Anforderungen in Anhang I erfüllt sind. Der Hersteller oder sein Bevollmächtigter erbringt den Nachweis der Konformität mit den grundlegenden Anforderungen anhand eines der folgenden Verfahren:

a) internes Kontrollverfahren (auf der Grundlage von Modul A) gemäß Anhang VI oder

b) EU-Baumusterprüfverfahren (auf der Grundlage von Modul B) gemäß Anhang VI und anschließende Konformität mit dem EU-Baumuster auf der Grundlage der internen Fertigungskontrolle (auf der Grundlage von Modul C) gemäß Anhang VI oder

c) Konformitätsbewertung auf der Grundlage einer umfassenden Qualitätssicherung (auf der Grundlage von Modul H) gemäß Anhang VI.

(2) Hat der Hersteller oder sein Bevollmächtigter bei der Bewertung der Konformität eines kritischen Produkts mit digitalen Elementen der Klasse I gemäß Anhang III und der von dessen Hersteller festgelegten Verfahren mit den grundlegenden Anforderungen in Anhang I harmonisierte Normen, gemeinsame Spezifikationen oder europäische Systeme für die Cybersicherheitszertifizierung gemäß Artikel 18 nicht oder nur zum Teil angewandt oder sind solche harmonisierten Normen, gemeinsamen Spezifikationen oder europäischen Systeme für die Cybersicherheitszertifizierung nicht vorhanden, so sind die Produkte mit digitalen Elementen und die vom Hersteller festgelegten Verfahren im Hinblick auf die grundlegenden Anforderungen einem der folgenden Verfahren zu unterziehen:

a) EU-Baumusterprüfverfahren (auf der Grundlage von Modul B) gemäß Anhang VI und anschließend Konformität mit dem EU-Baumuster auf der Grundlage der internen Fertigungskontrolle (auf der Grundlage von Modul C) gemäß Anhang VI oder

b) Konformitätsbewertung auf der Grundlage einer umfassenden Qualitätssicherung (auf der Grundlage von Modul H) gemäß Anhang VI.

(3) Handelt es sich bei dem Produkt um ein kritisches Produkt mit digitalen Elementen der Klasse II gemäß Anhang III, so erbringt der Hersteller oder sein Bevollmächtigter den Nachweis der Konformität mit den grundlegenden Anforderungen in Anhang I anhand eines der folgenden Verfahren:

a) EU-Baumusterprüfverfahren (auf der Grundlage von Modul B) gemäß Anhang VI und anschließende Konformität mit dem EU-Baumuster auf der Grundlage der internen Fertigungskontrolle (auf der Grundlage von Modul C) gemäß Anhang VI oder

b) Konformitätsbewertung auf der Grundlage einer umfassenden Qualitätssicherung (auf der Grundlage von Modul H) gemäß Anhang VI.

(4) Hersteller von Produkten mit digitalen Elementen, die als EHR-Systeme gemäß der Verordnung [Verordnung über den europäischen Raum für Gesundheitsdaten] eingestuft sind, erbringen den Nachweis der Konformität mit den grundlegenden Anforderungen in Anhang I der vorliegenden Verordnung anhand des einschlägigen Konformitätsbewertungsverfahrens gemäß der Verordnung [Kapitel III der Verordnung über den europäischen Raum für Gesundheitsdaten].

(5) Die notifizierten Stellen berücksichtigen bei der Festsetzung der Gebühren für die Konformitätsbewertung die besonderen Interessen und Bedürfnisse kleiner und mittlerer Unternehmen (KMU) und senken diese Gebühren proportional zu deren besonderen Interessen und Bedürfnissen.

KAPITEL IV

NOTIFIZIERUNG VON KONFORMITÄTSBEWERTUNGSSTELLEN

Artikel 25

Notifizierung

Die Mitgliedstaaten notifizieren der Kommission und den anderen Mitgliedstaaten die Konformitätsbewertungsstellen, die befugt sind, Konformitätsbewertungen gemäß dieser Verordnung durchzuführen.

Artikel 26

Notifizierende Behörden

(1) Die Mitgliedstaaten benennen eine notifizierende Behörde, die für die Einrichtung und Durchführung der erforderlichen Verfahren für die Bewertung und Notifizierung von Konformitätsbewertungsstellen und für die Überwachung der notifizierten Stellen, einschließlich der Einhaltung des Artikels 31, zuständig ist.

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

Artikel 27

Anforderungen an notifizierende Behörden

(1) Notifizierende Behörden werden so eingerichtet, dass es zu keinerlei Interessenkonflikt mit den Konformitätsbewertungsstellen kommt.

(2) Notifizierende Behörden gewährleisten durch ihre Organisation und Arbeitsweise, dass bei der Ausübung ihrer Tätigkeit Objektivität und Unparteilichkeit gewahrt sind.

(3) Notifizierende Behörden werden so strukturiert, dass jede Entscheidung über die Notifizierung einer Konformitätsbewertungsstelle von kompetenten Personen getroffen wird, die nicht mit den Personen identisch sind, welche die Bewertung durchgeführt haben.

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

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

(6) Einer notifizierenden Behörde stehen kompetente Mitarbeiter in ausreichender Zahl zur Verfügung, sodass sie ihre Aufgaben ordnungsgemäß wahrnehmen kann.

Artikel 28

Informationspflichten der notifizierenden Behörden

(1) Die Mitgliedstaaten unterrichten die Kommission über ihre Verfahren zur Bewertung und Notifizierung von Konformitätsbewertungsstellen und zur Überwachung notifizierter Stellen sowie über diesbezügliche Änderungen.

(2) Die Kommission macht diese Information der Öffentlichkeit zugänglich.

Artikel 29

Anforderungen an notifizierte Stellen

(1) Konformitätsbewertungsstellen erfüllen für die Zwecke der Notifizierung die Anforderungen der Absätze 2 bis 12.

(2) Eine Konformitätsbewertungsstelle ist nach nationalem Recht gegründet und ist mit Rechtspersönlichkeit ausgestattet.

(3) Bei einer Konformitätsbewertungsstelle handelt es sich um einen unabhängigen Dritten, der von der Organisation oder dem Produkt, die bzw. das bewertet wird, unabhängig ist.

Eine Stelle, die einem Wirtschaftsverband oder einem Fachverband angehört und Produkte mit digitalen Elementen bewertet, an deren Konzeption, Entwicklung, Herstellung, Bereitstellung, Montage, Verwendung oder Wartung Unternehmen beteiligt sind, die von diesem Verband vertreten werden, kann als solche Stelle gelten, sofern ihre Unabhängigkeit sowie das Fehlen jedweder Interessenskonflikte nachgewiesen sind.

(4) Eine Konformitätsbewertungsstelle, ihre oberste Leitungsebene und die für die Erfüllung der Konformitätsbewertungsaufgaben zuständigen Mitarbeiter dürfen nicht Konstrukteur, Entwickler, Hersteller, Lieferant, Installateur, Käufer, Eigentümer, Verwender oder Wartungsbetrieb der zu bewertenden Produkte mit digitalen Elementen oder Bevollmächtigte einer dieser Parteien sein. Dies schließt die Verwendung von bereits einer Konformitätsbewertung unterzogenen Produkten, die für die Tätigkeit der Konformitätsbewertungsstelle erforderlich sind, oder die Verwendung solcher Produkte zum persönlichen Gebrauch nicht aus.

Eine Konformitätsbewertungsstelle, ihre oberste Leitungsebene und die für die Erfüllung der Konformitätsbewertungsaufgaben zuständigen Mitarbeiter dürfen weder direkt an Konzeption, Entwicklung, Herstellung, Vermarktung, Installation, Verwendung oder Wartung dieser Produkte beteiligt sein, noch 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.

Die Konformitätsbewertungsstellen gewährleisten, dass Tätigkeiten ihrer Zweigstellen oder Unterauftragnehmer die Vertraulichkeit, Objektivität oder Unparteilichkeit ihrer Konformitätsbewertungstätigkeiten nicht beeinträchtigen.

(5) Die Konformitätsbewertungsstellen und ihre Mitarbeiter führen die Konformitätsbewertungstätigkeiten mit der größtmöglichen Professionalität und der erforderlichen fachlichen Kompetenz in dem betreffenden Bereich durch; sie dürfen keinerlei Einflussnahme, insbesondere finanzieller Art, ausgesetzt sein, die sich auf ihre Beurteilung oder die Ergebnisse ihrer Konformitätsbewertungsarbeit auswirken könnte; dies gilt speziell für Einflussnahmen durch Personen oder Personengruppen, die ein Interesse am Ergebnis dieser Tätigkeiten haben.

(6) Eine Konformitätsbewertungsstelle ist in der Lage, alle Konformitätsbewertungsaufgaben zu bewältigen, die ihr nach Anhang VI zufallen

und für die sie notifiziert wurde, gleichgültig, ob diese Aufgaben von der Stelle selbst, in ihrem Auftrag oder unter ihrer Verantwortung ausgeführt werden.

Eine Konformitätsbewertungsstelle verfügt jederzeit, für jedes Konformitätsbewertungsverfahren und für jede Art und Kategorie von Produkten mit digitalen Elementen, für die sie notifiziert wurde, über

a) die erforderlichen Mitarbeiter mit Fachkenntnis und ausreichender einschlägiger Erfahrung, um die bei der Konformitätsbewertung anfallenden Aufgaben zu erfüllen;

b) Beschreibungen von Verfahren, nach denen die Konformitätsbewertung durchgeführt wird, um die Transparenz und die Wiederholbarkeit dieser Verfahren sicherzustellen. Sie verfügt über angemessene Vorgaben und geeignete Verfahren, bei denen zwischen den Aufgaben, die sie als notifizierte Stelle wahrnimmt, und anderen Tätigkeiten unterschieden wird;

c) Verfahren zur Durchführung von Tätigkeiten unter gebührender Berücksichtigung der Größe eines Unternehmens, der Branche, in der es tätig ist, seiner Struktur, des Grads der Komplexität der jeweiligen Produkttechnologie und des Massenfertigungs- oder Seriencharakters des Fertigungsprozesses.

Sie verfügt über die erforderlichen Mittel zur angemessenen Erledigung der technischen und administrativen Aufgaben, die mit den Konformitätsbewertungstätigkeiten verbunden sind, und sie hat Zugang zu allen benötigten Ausrüstungen oder Einrichtungen.

(7) Die Mitarbeiter, die für die Durchführung der Konformitätsbewertungstätigkeiten zuständig sind, müssen über Folgendes verfügen:

a) eine solide Fach- und Berufsausbildung, die alle Konformitätsbewertungstätigkeiten in dem Bereich umfasst, für den die Konformitätsbewertungsstelle notifiziert wurde;

b) eine ausreichende Kenntnis der Anforderungen, die mit den durchzuführenden Bewertungen verbunden sind, und die entsprechende Befugnis, solche Bewertungen durchzuführen;

c) angemessene Kenntnisse und Verständnis der wesentlichen Anforderungen, der geltenden harmonisierten Normen und der einschlägigen Harmonisierungsrechtsvorschriften der Union sowie ihrer Durchführungsvorschriften;

d) die Fähigkeit zur Erstellung von Bescheinigungen, Protokollen und Berichten als Nachweis für durchgeführte Bewertungen.

(8) Die Unparteilichkeit der Konformitätsbewertungsstellen, ihrer obersten Leitungsebene und ihres bewertenden Personals muss garantiert sein.

Die Entlohnung der obersten Leitungsebene und des bewertenden Personals der Konformitätsbewertungsstelle darf sich nicht nach der Anzahl der durchgeführten Bewertungen oder deren Ergebnissen richten.

(9) Die Konformitätsbewertungsstellen schließen eine Haftpflichtversicherung ab, sofern die Haftpflicht nicht aufgrund der nationalen Rechtsvorschriften vom Staat übernommen wird oder der Mitgliedstaat selbst unmittelbar für die Konformitätsbewertung verantwortlich ist.

(10) Informationen, welche die Mitarbeiter einer Konformitätsbewertungsstelle bei der Durchführung ihrer Aufgaben gemäß Anhang VI oder einer der einschlägigen nationalen Durchführungsvorschriften erhalten, fallen unter die berufliche Schweigepflicht, außer gegenüber den Marktüberwachungsbehörden des Mitgliedstaats, in dem sie ihre Tätigkeiten ausüben. Eigentumsrechte werden geschützt. Die Konformitätsbewertungsstelle verfügt über dokumentierte Verfahren, mit denen die Einhaltung dieses Absatzes sichergestellt wird.

(11) Die Konformitätsbewertungsstellen wirken an den einschlägigen Normungstätigkeiten und den Tätigkeiten der gemäß Artikel 40 eingerichteten Koordinierungsgruppe notifizierter Stellen mit bzw. sorgen dafür, dass ihr bewertendes Personal darüber informiert ist, und wenden die von dieser Gruppe erarbeiteten Verwaltungsentscheidungen und Dokumente als allgemeine Leitlinie an.

(12) Konformitätsbewertungsstellen üben ihre Tätigkeiten im Einklang mit einer Reihe kohärenter, gerechter und angemessener Geschäftsbedingungen aus, wobei sie insbesondere in Bezug auf Gebühren die Interessen der KMU berücksichtigen.

Artikel 30

Konformitätsvermutung bei notifizierten Stellen

Weist eine Konformitätsbewertungsstelle nach, dass sie die Kriterien der einschlägigen harmonisierten Normen, deren Fundstellen im *Amtsblatt der Europäischen Union* veröffentlicht wurden, oder von Teilen davon erfüllt, so wird davon ausgegangen, dass sie die Anforderungen nach Artikel 29 erfüllt, soweit die geltenden Normen diese Anforderungen abdecken.

Artikel 31

Zweigstellen notifizierter Stellen und Vergabe von Unteraufträgen durch notifizierte Stellen

(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 29 erfüllt, und unterrichtet die notifizierende Behörde hierüber.

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

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

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

Artikel 32

Antrag auf Notifizierung

(1) Eine Konformitätsbewertungsstelle beantragt ihre Notifizierung bei der notifizierenden Behörde des Mitgliedstaats, in dem sie niedergelassen ist.

(2) Dem Antrag wird eine Beschreibung der Konformitätsbewertungstätigkeiten, des bzw. der Konformitätsbewertungsverfahren und des Produkts oder der Produkte, für die diese Stelle Kompetenz beansprucht, sowie, falls vorhanden, eine Akkreditierungsurkunde beigelegt, die von einer nationalen Akkreditierungsstelle ausgestellt wurde und in der diese bescheinigt, dass die Konformitätsbewertungsstelle die Anforderungen des Artikels 29 erfüllt.

(3) Kann die Konformitätsbewertungsstelle keine Akkreditierungsurkunde vorweisen, 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 29 erfüllt.

Artikel 33

Notifizierungsverfahren

(1) Die notifizierenden Behörden dürfen nur Konformitätsbewertungsstellen notifizieren, die die Anforderungen des Artikels 29 erfüllen.

(2) Die notifizierende Behörde unterrichtet die Kommission und die anderen Mitgliedstaaten mittels des von der Kommission entwickelten und verwalteten NANDO-Informationssystems (*New Approach Notified and Designated Organisations*, Informationssystem für die nach dem neuen Konzept notifizierten und benannten Organisationen).

(3) Die Notifizierung enthält vollständige Angaben zu den Konformitätsbewertungstätigkeiten, dem bzw. den betreffenden Konformitätsbewertungsmodulen und Produkten sowie die betreffende Bestätigung der Kompetenz.

(4) Beruht eine Notifizierung nicht auf einer Akkreditierungsurkunde gemäß Artikel 32 Absatz 2, legt die notifizierende Behörde der Kommission und den anderen Mitgliedstaaten Unterlagen vor, mit denen die Kompetenz der Konformitätsbewertungsstelle nachgewiesen wird, sowie die Vereinbarungen, die getroffen wurden, um sicherzustellen, dass die Stelle regelmäßig überwacht wird und stets den Anforderungen des Artikels 29 genügt.

(5) Die betreffende Stelle darf die Aufgaben einer notifizierten Stelle nur dann wahrnehmen, wenn weder die Kommission noch die anderen Mitgliedstaaten innerhalb von zwei Wochen nach der Notifizierung, falls eine Akkreditierungsurkunde vorliegt, oder innerhalb von zwei Monaten nach der Notifizierung, falls keine Akkreditierung vorliegt, Einwände erhoben haben.

Nur eine solche Stelle gilt für die Zwecke dieser Verordnung als notifizierte Stelle.

(6) Die Kommission und die anderen Mitgliedstaaten werden über alle späteren wesentlichen Änderung der Notifizierung informiert.

Artikel 34

Kennnummern und Verzeichnisse notifizierter Stellen

(1) Die Kommission weist jeder notifizierten Stelle eine Kennnummer zu.

Selbst wenn eine Stelle nach mehreren Rechtsvorschriften der Union notifiziert ist, erhält sie nur eine einzige Kennnummer.

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

Die Kommission sorgt dafür, dass dieses Verzeichnis stets auf dem neuesten Stand gehalten wird.

Artikel 35

Änderungen der Notifizierungen

(1) Falls eine notifizierende Behörde feststellt oder davon unterrichtet wird, dass eine notifizierte Stelle die Anforderungen des Artikels 29 nicht mehr erfüllt oder dass sie ihren Verpflichtungen nicht nachkommt, schränkt sie die Notifizierung gegebenenfalls ein, setzt sie aus oder widerruft sie, wobei sie das Ausmaß berücksichtigt, in dem diesen Anforderungen nicht genügt oder diesen Verpflichtungen nicht nachgekommen wurde. Sie setzt die Kommission und die anderen Mitgliedstaaten unverzüglich davon in Kenntnis.

(2) Bei Einschränkung, Aussetzung oder Widerruf der Notifizierung oder wenn die notifizierte Stelle ihre Tätigkeit einstellt, ergreift der notifizierende Mitgliedstaat die geeigneten Maßnahmen, um zu gewährleisten, dass die Akten dieser Stelle von einer anderen notifizierten Stelle weiter bearbeitet bzw. für die zuständigen notifizierenden Behörden und Marktüberwachungsbehörden auf deren Verlangen bereitgehalten werden.

Artikel 36

Anfechtung der Kompetenz notifizierter Stellen

(1) Die Kommission untersucht alle Fälle, in denen sie die Kompetenz einer notifizierten Stelle oder die dauerhafte Erfüllung der für die Stelle geltenden Anforderungen und Pflichten durch eine notifizierte Stelle anzweifelt oder ihr Zweifel daran zur Kenntnis gebracht werden.

(2) Der notifizierende Mitgliedstaat erteilt der Kommission auf Verlangen sämtliche Auskünfte über die Grundlage der Notifizierung oder die Erhaltung der Kompetenz der betreffenden Stelle.

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

(4) Stellt die Kommission fest, dass eine notifizierte Stelle die Voraussetzungen für ihre Notifizierung nicht oder nicht mehr erfüllt, setzt sie den notifizierenden Mitgliedstaat davon in Kenntnis und fordert ihn auf, die erforderlichen Korrekturmaßnahmen zu treffen, einschließlich eines Widerrufs der Notifizierung, sofern dies nötig ist.

Artikel 37

Operative Pflichten der notifizierten Stellen

(1) Die notifizierten Stellen führen die Konformitätsbewertungen im Einklang mit den Konformitätsbewertungsverfahren gemäß Artikel 24 und Anhang VI durch.

(2) Die Konformitätsbewertungen werden unter Wahrung der Verhältnismäßigkeit durchgeführt, wobei unnötige Belastungen der Wirtschaftsakteure vermieden

werden. Die Konformitätsbewertungsstellen üben ihre Tätigkeiten unter gebührender Berücksichtigung der Größe eines Unternehmens, der Branche, in der es tätig ist, seiner Struktur, des Grads der Komplexität der betroffenen Produkttechnologie und des Massenfertigungs- oder Seriencharakters des Fertigungsprozesses aus.

(3) Die notifizierten Stellen gehen hierbei jedoch so streng vor und halten ein solches Schutzniveau ein, wie dies für die Konformität des Produkts mit den Bestimmungen dieser Verordnung erforderlich ist.

(4) Stellt eine notifizierte Stelle fest, dass ein Hersteller die in Anhang I oder in den entsprechenden harmonisierten Normen oder gemeinsamen Spezifikationen gemäß Artikel 19 festgelegten Anforderungen nicht erfüllt hat, fordert sie den Hersteller auf, angemessene Korrekturmaßnahmen zu ergreifen, und stellt keine Konformitätsbescheinigung aus.

(5) Hat eine notifizierte Stelle bereits eine Bescheinigung ausgestellt und stellt im Rahmen der Überwachung der Konformität fest, dass das Produkt die in dieser Verordnung festgelegten Anforderungen nicht mehr erfüllt, fordert sie den Hersteller auf, angemessene Korrekturmaßnahmen zu ergreifen, und setzt die Bescheinigung falls nötig aus oder widerruft sie.

(6) Werden keine Korrekturmaßnahmen ergriffen oder zeigen sie nicht die nötige Wirkung, so schränkt die notifizierte Stelle die Bescheinigungen ein, setzt sie aus bzw. widerruft sie, je nachdem, was angemessen ist.

Artikel 38

Meldepflichten der notifizierten Stellen

(1) Die notifizierten Stellen melden der notifizierenden Behörde

a) alle Verweigerungen, Einschränkungen, Aussetzungen und Widerrufe einer Bescheinigung,

b) alle Umstände mit Auswirkungen auf den Geltungsbereich und die Bedingungen der Notifizierung,

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

d) auf Anfrage, die Konformitätsbewertungstätigkeiten, denen sie im Geltungsbereich ihrer Notifizierung nachgegangen sind, und sonstige Tätigkeiten, einschließlich grenzüberschreitender Tätigkeiten und Vergabe von Unteraufträgen, die sie ausgeführt haben.

(2) Die notifizierten Stellen übermitteln den übrigen Stellen, die nach dieser Verordnung notifiziert sind und ähnlichen Konformitätsbewertungstätigkeiten für dieselben Produkte nachgehen, einschlägige Informationen über negative und auf Verlangen auch über positive Ergebnisse von Konformitätsbewertungen.

Artikel 39

Erfahrungsaustausch

Die Kommission organisiert den Erfahrungsaustausch zwischen den für die Notifizierungspolitik zuständigen nationalen Behörden der Mitgliedstaaten.

Artikel 40

Koordinierung der notifizierten Stellen

(1) Die Kommission sorgt dafür, dass eine angemessene Koordinierung und Zusammenarbeit zwischen notifizierten Stellen in Form einer sektorübergreifenden Gruppe notifizierter Stellen eingerichtet und ordnungsgemäß weitergeführt wird.

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

KAPITEL V

MARKTÜBERWACHUNG UND DURCHSETZUNG

Artikel 41

Marktüberwachung und Kontrolle von Produkten mit digitalen Elementen auf dem Unionsmarkt

(1) Die Verordnung (EU) 2019/1020 gilt für die Produkte mit digitalen Elementen, die in den Anwendungsbereich der vorliegenden Verordnung fallen.

(2) Jeder Mitgliedstaat benennt für die Zwecke der Gewährleistung der wirksamen Durchführung der vorliegenden Verordnung eine oder mehrere Marktüberwachungsbehörden. Die Mitgliedstaaten können eine bestehende oder eine neue Behörde benennen, die im Rahmen der vorliegenden Verordnung als Marktüberwachungsbehörde tätig wird.

(3) Die Marktüberwachungsbehörden arbeiten gegebenenfalls mit den nach Artikel 58 der Verordnung (EU) 2019/881 benannten nationalen Behörden für die Cybersicherheitszertifizierung zusammen und tauschen regelmäßig Informationen mit ihnen aus. Bei der Beaufsichtigung der Umsetzung der Meldepflichten nach Artikel 11 der vorliegenden Verordnung arbeiten die benannten Marktüberwachungsbehörden mit der ENISA zusammen.

(4) Die Marktüberwachungsbehörden arbeiten gegebenenfalls mit anderen Marktüberwachungsbehörden zusammen, die auf der Grundlage anderer Harmonisierungsrechtsvorschriften der Union für andere Produkte benannt wurden, und tauschen regelmäßig Informationen mit ihnen aus.

(5) Die Marktüberwachungsbehörden arbeiten gegebenenfalls mit den Behörden zusammen, die die Anwendung des Datenschutzrechts der Union beaufsichtigen. Diese Zusammenarbeit umfasst die Unterrichtung dieser Behörden über alle Erkenntnisse, die für die Wahrnehmung ihrer Zuständigkeiten von Bedeutung sind, auch bezüglich der Herausgabe von Leitlinien und der Beratung nach Absatz 8 dieses Artikels, soweit solche Leitlinien und Ratschläge die Verarbeitung personenbezogener Daten betreffen.

Die Behörden, die die Anwendung des Datenschutzrechts der Union beaufsichtigen, sind befugt, alle im Rahmen dieser Verordnung erstellten oder geführten Unterlagen anzufordern und darauf zuzugreifen, soweit der Zugang zu diesen Unterlagen für die Erfüllung ihrer Aufgaben erforderlich ist. Sie unterrichten die benannten Marktüberwachungsbehörden des betreffenden Mitgliedstaats über jedes solches Ersuchen.

(6) Die Mitgliedstaaten sorgen dafür, dass die benannten Marktüberwachungsbehörden mit angemessenen finanziellen und personellen Ressourcen ausgestattet werden, damit sie ihre Aufgaben im Rahmen dieser Verordnung wahrnehmen können.

(7) Die Kommission fördert den Erfahrungsaustausch zwischen den benannten Marktüberwachungsbehörden.

(8) Die Marktüberwachungsbehörden können den Wirtschaftsakteuren mit Unterstützung der Kommission Leitlinien und Ratschläge für die Durchführung dieser Verordnung geben.

(9) Die Marktüberwachungsbehörden erstatten der Kommission jährlich über die Ergebnisse ihrer jeweiligen Marktüberwachungstätigkeiten Bericht. Die benannten Marktüberwachungsbehörden melden der Kommission und den einschlägigen nationalen Wettbewerbsbehörden unverzüglich alle Informationen, die sie im Verlauf ihrer Marktüberwachungstätigkeiten erlangt haben und die für die Anwendung des Wettbewerbsrechts der Union von Interesse sein könnten.

(10) Bei Produkten mit digitalen Elementen, die in den Anwendungsbereich der vorliegenden Verordnung fallen und gemäß Artikel [Artikel 6] der Verordnung [KI-Verordnung] als Hochrisiko-KI-Systeme eingestuft sind, sind die für die Zwecke der Verordnung [KI-Verordnung] benannten Marktüberwachungsbehörden auch für die nach der vorliegenden Verordnung erforderlichen Marktüberwachungstätigkeiten zuständig. Die nach der Verordnung [KI-Verordnung] benannten Marktüberwachungsbehörden arbeiten gegebenenfalls mit den nach der vorliegenden Verordnung benannten Marktüberwachungsbehörden und – bezüglich der Aufsicht über die Umsetzung der Meldepflichten nach Artikel 11 – mit der ENISA zusammen. Die nach der Verordnung [KI-Verordnung] benannten Marktüberwachungsbehörden unterrichten insbesondere die nach der vorliegenden Verordnung benannten Marktüberwachungsbehörden über alle Erkenntnisse, die für die Wahrnehmung ihrer Aufgaben im Zusammenhang mit der Durchführung der vorliegenden Verordnung von Bedeutung sind.

(11) Im Hinblick auf die einheitliche Anwendung dieser Verordnung wird gemäß Artikel 30 Absatz 2 der Verordnung (EU) 2019/1020 eine besondere Gruppe zur administrativen Zusammenarbeit (ADCO) eingesetzt. Die ADCO setzt sich aus Vertretern der benannten Marktüberwachungsbehörden und gegebenenfalls Vertretern der zentralen Verbindungsstellen zusammen.

Artikel 42

Zugang zu Daten und zur Dokumentation

Soweit dies für die Bewertung der Konformität von Produkten mit digitalen Elementen und der von deren Herstellern festgelegten Verfahren mit den grundlegenden Anforderungen in Anhang I erforderlich ist, erhalten die Marktüberwachungsbehörden auf begründeten Antrag Zugang zu den Daten, die für die Bewertung der Konzeption, Entwicklung, Herstellung und die Behandlung von Schwachstellen solcher Produkte erforderlich sind, einschließlich der betreffenden internen Unterlagen des jeweiligen Wirtschaftsakteurs.

Artikel 43

Nationale Verfahren für Produkte mit digitalen Elementen, die ein erhebliches Cybersicherheitsrisiko bergen

(1) Hat die Marktüberwachungsbehörde eines Mitgliedstaats hinreichende Gründe zu der Annahme, dass ein Produkt mit digitalen Elementen, einschließlich der Behandlung von Schwachstellen, ein erhebliches Cybersicherheitsrisiko birgt, so prüft sie das betreffende Produkt mit digitalen Elementen auf die Erfüllung aller in dieser Verordnung festgelegten Anforderungen. Die betroffenen Wirtschaftsakteure arbeiten im erforderlichen Umfang mit der Marktüberwachungsbehörde zusammen.

Gelangt die Marktüberwachungsbehörde im Verlauf dieser Prüfung zu dem Ergebnis, dass das Produkt mit digitalen Elementen die Anforderungen dieser Verordnung nicht erfüllt, so fordert sie den betroffenen Wirtschaftsakteur unverzüglich dazu auf, innerhalb einer von der Behörde vorgeschriebenen, der Art der Gefahr angemessenen Frist alle geeigneten Korrekturmaßnahmen zu ergreifen, um die Konformität des Produkts mit diesen Anforderungen herzustellen oder um das Produkt vom Markt zu nehmen oder es zurückzurufen.

Die Marktüberwachungsbehörde unterrichtet die betreffende notifizierte Stelle hierüber. Artikel 18 der Verordnung (EU) 2019/1020 gilt für die geeigneten Korrekturmaßnahmen.

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

(3) Der Hersteller sorgt dafür, dass alle geeigneten Korrekturmaßnahmen in Bezug auf sämtliche betroffenen Produkte mit digitalen Elementen, die er in der Union auf dem Markt bereitgestellt hat, ergriffen werden.

(4) Ergreift der Hersteller eines Produkts mit digitalen Elementen innerhalb der in Absatz 1 Unterabsatz 2 genannten Frist keine angemessenen Korrekturmaßnahmen, so treffen die Marktüberwachungsbehörden alle geeigneten vorläufigen Maßnahmen, um die Bereitstellung des Produkts auf ihrem nationalen Markt zu untersagen oder einzuschränken, das Produkt vom Markt zu nehmen oder es zurückzurufen.

Diese Behörde unterrichtet die Kommission und die anderen Mitgliedstaaten unverzüglich über diese Maßnahmen.

(5) Die in Absatz 4 genannten Informationen enthalten alle verfügbaren Einzelheiten, insbesondere die notwendigen Daten für die Identifizierung des nichtkonformen Produkts mit digitalen Elementen, die Herkunft des Produkts mit digitalen Elementen, die Art der behaupteten Nichtkonformität und das damit verbundene Risiko sowie die Art und Dauer der getroffenen nationalen Maßnahmen und die Argumente des betreffenden Wirtschaftsakteurs. Die Marktüberwachungsbehörde gibt insbesondere an, ob die Nichtkonformität eine oder mehrere der folgenden Ursachen hat:

a) Das Produkt oder die vom Hersteller festgelegten Verfahren erfüllen nicht die grundlegenden Anforderungen in Anhang I;

b) Mängel in den harmonisierten Normen, den Systemen für die Cybersicherheitszertifizierung oder den gemeinsamen Spezifikationen gemäß Artikel 18.

(6) Die Marktüberwachungsbehörden der Mitgliedstaaten, außer derjenigen, die das Verfahren eingeleitet hat, unterrichten unverzüglich die Kommission und die anderen Mitgliedstaaten von jeglichen Maßnahmen und ihnen vorliegenden zusätzlichen Erkenntnissen über die Nichtkonformität des betreffenden Produkts sowie über ihre Einwände, falls sie die ihnen mitgeteilte nationale Maßnahme ablehnen.

(7) Erhebt weder ein Mitgliedstaat noch die Kommission innerhalb von drei Monaten nach Erhalt der in Absatz 4 genannten Informationen einen Einwand gegen eine vorläufige Maßnahme eines Mitgliedstaats, so gilt diese Maßnahme als gerechtfertigt. Die Verfahrensrechte des betreffenden Akteurs nach Artikel 18 der Verordnung (EU) 2019/1020 bleiben hiervon unberührt.

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

Artikel 44

Schutzklauselverfahren der Union

(1) Erhebt ein Mitgliedstaat innerhalb von drei Monaten nach Eingang der in Artikel 43 Absatz 4 genannten Unterrichtung Einwände gegen eine von einem anderen Mitgliedstaat getroffene Maßnahme oder ist die Kommission der Ansicht, dass die Maßnahme mit dem Unionsrecht unvereinbar ist, so nimmt die Kommission unverzüglich Konsultationen mit dem betreffenden Mitgliedstaat oder Wirtschaftsakteur auf und prüft die nationale Maßnahme. Anhand der Ergebnisse dieser Prüfung entscheidet die Kommission innerhalb von neun Monaten nach Eingang der in Artikel 43 Absatz 4 genannten Unterrichtung, ob die nationale Maßnahme gerechtfertigt ist oder nicht und teilt dem betreffenden Mitgliedstaat ihre Entscheidung mit.

(2) Hält sie die nationale Maßnahme für gerechtfertigt, so ergreifen alle Mitgliedstaaten die erforderlichen Maßnahmen, um zu gewährleisten, dass das nichtkonforme Produkt mit digitalen Elementen von ihrem Markt genommen wird, und unterrichten die Kommission darüber. Hält sie die nationale Maßnahme nicht für gerechtfertigt, so nimmt der betreffende Mitgliedstaat die Maßnahme zurück.

(3) Wird die nationale Maßnahme als gerechtfertigt erachtet und wird die Nichtkonformität des Produkts mit digitalen Elementen auf Mängel in den harmonisierten Normen zurückgeführt, so leitet die Kommission das Verfahren nach Artikel 10 der Verordnung (EU) Nr. 1025/2012 ein.

(4) Wird die nationale Maßnahme als gerechtfertigt erachtet und wird die Nichtkonformität des Produkts mit digitalen Elementen auf Mängel in einem europäischen System für die Cybersicherheitszertifizierung gemäß Artikel 18 zurückgeführt, so prüft die Kommission, ob der Durchführungsrechtsakt gemäß Artikel 18 Absatz 4, in dem die Konformitätsvermutung in Bezug auf dieses Zertifizierungssystem festgelegt worden ist, zu ändern oder aufzuheben ist.

(5) Wird die nationale Maßnahme als gerechtfertigt erachtet und wird die Nichtkonformität des Produkts mit digitalen Elementen auf Mängel in gemeinsamen Spezifikationen gemäß Artikel 19 zurückgeführt, so prüft die Kommission, ob der Durchführungsrechtsakt gemäß Artikel 19, in dem die gemeinsamen Spezifikationen festgelegt worden sind, zu ändern oder aufzuheben ist.

Artikel 45

EU-Verfahren für Produkte mit digitalen Elementen, die ein erhebliches Cybersicherheitsrisiko bergen

(1) Hat die Kommission – auch aufgrund von Informationen der ENISA – hinreichende Gründe zu der Annahme, dass ein Produkt mit digitalen Elementen, das ein erhebliches Cybersicherheitsrisiko birgt, den Anforderungen dieser Verordnung nicht genügt, so kann sie die zuständigen Marktüberwachungsbehörden auffordern, eine Konformitätsbewertung durchzuführen und die in Artikel 43 genannten Verfahren anzuwenden.

(2) Unter außergewöhnlichen Umständen, die ein sofortiges Eingreifen rechtfertigen, um das reibungslose Funktionieren des Binnenmarkts zu bewahren, und wenn die Kommission hinreichende Gründe zu der Annahme hat, dass das in Absatz 1 genannte Produkt weiterhin den Anforderungen dieser Verordnung nicht genügt und die zuständigen Marktüberwachungsbehörden keine wirksamen Maßnahmen ergriffen haben, kann die Kommission die ENISA ersuchen, eine Bewertung der Konformität vorzunehmen. Die Kommission unterrichtet die betreffenden Marktüberwachungsbehörden hierüber. Die betroffenen Wirtschaftsakteure arbeiten im erforderlichen Umfang mit der ENISA zusammen.

(3) Auf der Grundlage der Bewertung der ENISA kann die Kommission beschließen, dass eine Korrekturmaßnahme oder eine einschränkende Maßnahme auf Unionsebene erforderlich ist. Zu diesem Zweck konsultiert sie unverzüglich die betroffenen Mitgliedstaaten und den bzw. die betroffenen Wirtschaftsakteure.

(4) Auf der Grundlage der in Absatz 3 genannten Konsultation kann die Kommission Durchführungsrechtsakte über Korrekturmaßnahmen oder einschränkende Maßnahmen auf Unionsebene erlassen, einschließlich der Anordnung der Rücknahme vom Markt oder des Rückrufs innerhalb einer der Art des Risikos angemessenen Frist. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 51 Absatz 2 genannten Prüfverfahren erlassen.

(5) Die Kommission unterrichtet den bzw. die betroffenen Wirtschaftsakteure unverzüglich über den in Absatz 4 genannten Beschluss. Die Mitgliedstaaten führen die Durchführungsrechtsakte nach Absatz 4 unverzüglich durch und unterrichten die Kommission hierüber.

(6) Die Absätze 2 bis 5 gelten für die Dauer der außergewöhnlichen Umstände, die das Eingreifen der Kommission gerechtfertigt haben, und solange die Konformität des betreffenden Produkts mit dieser Verordnung nicht hergestellt worden ist.

Artikel 46

Konforme Produkte mit digitalen Elementen, die ein erhebliches Cybersicherheitsrisiko bergen

(1) Stellt die Marktüberwachungsbehörde eines Mitgliedstaats nach einer Bewertung gemäß Artikel 43 fest, dass ein Produkt mit digitalen Elementen und die vom Hersteller festgelegten Verfahren, obwohl sie dieser Verordnung entsprechen, ein erhebliches Cybersicherheitsrisiko bergen und darüber hinaus ein Risiko für die Gesundheit oder Sicherheit von Personen, für die Erfüllung der Pflichten aus dem Unionsrecht oder dem nationalen Recht zum Schutz der Grundrechte, für die Verfügbarkeit, Integrität oder Vertraulichkeit von Diensten, die über ein

elektronisches Informationssystem von wesentlichen Einrichtungen der in [Anhang I der Richtlinie XXX/XXXX (NIS2)] genannten Art angeboten werden, oder für andere Aspekte des Schutzes öffentlicher Interessen darstellen, so fordert sie den betroffenen Akteur auf, alle geeigneten Maßnahmen zu treffen, damit das Produkt mit digitalen Elementen und die vom betreffenden Hersteller festgelegten Verfahren bei seinem Inverkehrbringen dieses Risiko nicht mehr bergen, oder um das Produkt mit digitalen Elementen innerhalb einer der Art des Risikos angemessenen Frist vom Markt zu nehmen oder zurückzurufen.

(2) Der Hersteller oder andere einschlägige Akteure sorgen dafür, dass in Bezug auf alle betroffenen Produkte mit digitalen Elementen, die sie in der Union auf dem Markt bereitgestellt haben, innerhalb der von der Marktüberwachungsbehörde des in Absatz 1 genannten Mitgliedstaats gesetzten Frist Korrekturmaßnahmen ergriffen werden.

(3) Der Mitgliedstaat unterrichtet die Kommission und die anderen Mitgliedstaaten unverzüglich über alle gemäß Absatz 1 ergriffenen Maßnahmen. Aus diesen Informationen gehen alle verfügbaren Einzelheiten hervor, insbesondere die Daten zur Identifizierung des betroffenen Produkts mit digitalen Elementen, dessen Herkunft und Lieferkette, die Art des damit verbundenen Risikos sowie die Art und Dauer der ergriffenen nationalen Maßnahmen.

(4) Die Kommission konsultiert unverzüglich die Mitgliedstaaten und den betroffenen Wirtschaftsakteur und nimmt eine Prüfung der ergriffenen nationalen Maßnahmen vor. Anhand der Ergebnisse dieser Prüfung beschließt die Kommission, ob die Maßnahme gerechtfertigt ist oder nicht, und schlägt, falls erforderlich, geeignete Maßnahmen vor.

(5) Die Kommission richtet diesen Beschluss an die Mitgliedstaaten.

(6) Hat die Kommission – auch aufgrund von Informationen der ENISA – hinreichende Gründe zu der Annahme, dass ein Produkt mit digitalen Elementen, obwohl es dieser Verordnung entspricht, die in Absatz 1 genannten Risiken birgt, so kann sie die betreffende(n) Marktüberwachungsbehörde(n) auffordern, eine Konformitätsbewertung durchzuführen und die in Artikel 43 und in den Absätzen 1, 2 und 3 dieses Artikels genannten Verfahren anzuwenden.

(7) Unter außergewöhnlichen Umständen, die ein sofortiges Eingreifen rechtfertigen, um das reibungslose Funktionieren des Binnenmarkts zu bewahren, und wenn die Kommission hinreichende Gründe zu der Annahme hat, dass das in Absatz 6 genannte Produkt weiterhin die in Absatz 1 genannten Risiken birgt und die zuständigen Marktüberwachungsbehörden keine wirksamen Maßnahmen ergriffen haben, kann die Kommission die ENISA ersuchen, eine Bewertung der Risiken, die dieses Produkt birgt, vorzunehmen, und unterrichtet die betreffenden Marktüberwachungsbehörden hierüber. Die betroffenen Wirtschaftsakteure arbeiten im erforderlichen Umfang mit der ENISA zusammen.

(8) Auf der Grundlage der Bewertung der ENISA nach Absatz 7 kann die Kommission feststellen, dass eine Korrekturmaßnahme oder eine einschränkende Maßnahme auf Unionsebene erforderlich ist. Zu diesem Zweck konsultiert sie unverzüglich die betroffenen Mitgliedstaaten und den bzw. die betroffenen Akteur(e).

(9) Auf der Grundlage der in Absatz 8 genannten Konsultation kann die Kommission Durchführungsrechtsakte über Korrekturmaßnahmen oder einschränkende Maßnahmen auf Unionsebene erlassen, einschließlich der Anordnung der

Rücknahme vom Markt oder des Rückrufs innerhalb einer der Art des Risikos angemessenen Frist. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 51 Absatz 2 genannten Prüfverfahren erlassen.

(10) Die Kommission unterrichtet den bzw. die betroffenen Akteur(e) unverzüglich über den in Absatz 9 genannten Beschluss. Die Mitgliedstaaten führen diese Durchführungsrechtsakte unverzüglich durch und unterrichten die Kommission hierüber.

(11) Die Absätze 6 bis 10 gelten für die Dauer der außergewöhnlichen Umstände, die das Eingreifen der Kommission gerechtfertigt haben, und solange das betroffene Produkt weiterhin die in Absatz 1 genannten Risiken birgt.

Artikel 47

Formale Nichtkonformität

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

a) die Konformitätskennzeichnung wurde unter Nichteinhaltung der Artikel 21 und 22 angebracht;

b) die Konformitätskennzeichnung wurde nicht angebracht;

c) die EU-Konformitätserklärung wurde nicht ausgestellt;

d) die EU-Konformitätserklärung wurde nicht ordnungsgemäß ausgestellt;

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

f) die technische Dokumentation ist entweder nicht verfügbar oder nicht vollständig.

(2) Besteht die in Absatz 1 genannte Nichtkonformität weiter, so ergreift der betreffende Mitgliedstaat alle geeigneten Maßnahmen, um die Bereitstellung des Produkts mit digitalen Elementen auf dem Markt einzuschränken oder zu untersagen oder um dafür zu sorgen, dass es zurückgerufen oder vom Markt genommen wird.

Artikel 48

Gemeinsame Tätigkeiten der Marktüberwachungsbehörden

(1) Die Marktüberwachungsbehörden können mit anderen einschlägigen Behörden die Durchführung gemeinsamer Tätigkeiten zur Gewährleistung der Cybersicherheit und des Verbraucherschutzes in Bezug auf bestimmte in Verkehr gebrachte oder auf dem Markt bereitgestellte Produkte mit digitalen Elementen vereinbaren, insbesondere in Bezug auf Produkte, bei denen häufig Cybersicherheitsrisiken festgestellt werden.

(2) Die Kommission oder die ENISA können gemeinsame Tätigkeiten zur Überprüfung der Einhaltung dieser Verordnung vorschlagen, die von Marktüberwachungsbehörden auf der Grundlage von Hinweisen oder Informationen, wonach Produkte, die in den Anwendungsbereich dieser Verordnung fallen, möglicherweise in mehreren Mitgliedstaaten den Anforderungen dieser Verordnung nicht entsprechen, durchgeführt werden sollen.

(3) Die Marktüberwachungsbehörden und die Kommission tragen dafür Sorge, dass die Vereinbarung über gemeinsame Tätigkeiten weder einen unfairen Wettbewerb zwischen Wirtschaftsakteuren nach sich zieht noch die Objektivität, Unabhängigkeit oder Unparteilichkeit der Parteien der Vereinbarung beeinträchtigt.

(4) Eine Marktüberwachungsbehörde kann alle Informationen verwenden, die sie im Rahmen gemeinsamer Tätigkeiten, die Teil einer von ihr durchgeführten Untersuchung waren, erlangt hat.

(5) Die betreffende Marktüberwachungsbehörde und die Kommission machen die Vereinbarung über gemeinsame Tätigkeiten einschließlich der Namen der Beteiligten der Öffentlichkeit zugänglich.

Artikel 49

Koordinierte Kontrollen (Sweeps)

(1) Die Marktüberwachungsbehörden können zur Prüfung der Einhaltung dieser Verordnung oder zur Feststellung von Verstößen gegen diese Verordnung beschließen, gleichzeitige koordinierte Kontrollen („*Sweeps*“) zu bestimmten Produkten mit digitalen Elementen durchzuführen.

(2) Sofern die betreffenden Marktüberwachungsbehörden nichts anderes vereinbaren, werden solche Sweeps von der Kommission koordiniert. Der Koordinator des Sweeps kann die aggregierten Ergebnisse gegebenenfalls veröffentlichen.

(3) Die ENISA kann in Wahrnehmung ihrer Aufgaben, auch aufgrund der gemäß Artikel 11 Absätze 1 und 2 eingegangenen Meldungen, Produktkategorien bestimmen, zu denen Sweeps organisiert werden können. Der Vorschlag für Sweeps wird dem in Absatz 2 genannten potenziellen Koordinator zur Prüfung durch die Marktüberwachungsbehörden vorgelegt.

(4) Bei der Durchführung von Sweeps können die beteiligten Marktüberwachungsbehörden die Ermittlungsbefugnisse nach den Artikeln 41 bis 47 und weitere Befugnisse, die ihnen nach nationalem Recht übertragen wurden, nutzen.

(5) Die Marktüberwachungsbehörden können Kommissionsbeamte und weitere von der Kommission autorisierte Begleitpersonen zur Teilnahme an Sweeps einladen.

KAPITEL VI

ÜBERTRAGENE BEFUGNISSE UND AUSSCHUSSVERFAHREN

Artikel 50

Ausübung der Befugnisübertragung

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

(2) Die Befugnis zum Erlass delegierter Rechtsakte gemäß Artikel 2 Absatz 4, Artikel 6 Absatz 2, Artikel 6 Absatz 3, Artikel 6 Absatz 5, Artikel 20 Absatz 5 und Artikel 23 Absatz 5 wird der Kommission übertragen.

(3) Die Befugnisübertragung gemäß Artikel 2 Absatz 4, Artikel 6 Absatz 2, Artikel 6 Absatz 3, Artikel 6 Absatz 5, Artikel 20 Absatz 5 und Artikel 23 Absatz 5 kann vom Europäischen Parlament oder vom Rat jederzeit widerrufen werden. Der Beschluss

über den Widerruf beendet die Übertragung der in diesem Beschluss angegebenen Befugnis. Er wird am Tag nach seiner Veröffentlichung im *Amtsblatt der Europäischen Union* oder zu einem im Beschluss über den Widerruf 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 enthaltenen Grundsätzen.

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

(6) Ein delegierter Rechtsakt, der gemäß Artikel 2 Absatz 4, Artikel 6 Absatz 2, Artikel 6 Absatz 3, Artikel 6 Absatz 5, Artikel 20 Absatz 5 und Artikel 23 Absatz 5 erlassen wurde, tritt nur in Kraft, wenn weder das Europäische Parlament noch der Rat innerhalb einer Frist von zwei Monaten nach Übermittlung dieses Rechtsakts an das Europäische Parlament und den Rat Einwände erhoben haben oder wenn vor Ablauf dieser Frist das Europäische Parlament und der Rat beide der Kommission mitgeteilt haben, dass sie keine Einwände erheben werden. Auf Initiative des Europäischen Parlaments oder des Rates wird diese Frist um zwei Monate verlängert.

Artikel 51

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.

(3) Wird die Stellungnahme des Ausschusses im schriftlichen Verfahren eingeholt, so wird das Verfahren ohne Ergebnis abgeschlossen, wenn der Vorsitz des Ausschusses dies innerhalb der Frist zur Abgabe der Stellungnahme beschließt oder ein Ausschussmitglied dies verlangt.

KAPITEL VII

VERTRAULICHKEIT UND SANKTIONEN

Artikel 52

Vertraulichkeit

(1) Alle an der Anwendung dieser Verordnung beteiligten Parteien wahren die Vertraulichkeit der Informationen und Daten, von denen sie in Ausübung ihrer Aufgaben und Tätigkeiten Kenntnis erlangen, und schützen dabei insbesondere Folgendes:

a) Rechte des geistigen Eigentums, vertrauliche Geschäftsinformationen oder Geschäftsgeheimnisse natürlicher oder juristischer Personen, auch Quellcode,

mit Ausnahme der in Artikel 5 der Richtlinie 2016/943 des Europäischen Parlaments und des Rates[24] genannten Fälle,

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

c) öffentliche und nationale Sicherheitsinteressen,

d) die Integrität von Straf- oder Verwaltungsverfahren.

(2) Unbeschadet des Absatzes 1 werden die Informationen, die die Marktüberwachungsbehörden auf vertraulicher Basis untereinander oder mit der Kommission ausgetauscht haben, nicht ohne die vorherige Zustimmung der Marktüberwachungsbehörde, von der die Informationen stammen, weitergegeben.

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

(4) Die Kommission und die Mitgliedstaaten können mit einschlägigen Behörden von Drittstaaten, mit denen sie bilaterale oder multilaterale Vertraulichkeitsvereinbarungen getroffen haben und die ein angemessenes Schutzniveau gewährleisten, erforderlichenfalls sensible Informationen austauschen.

Artikel 53

Sanktionen

(1) Die Mitgliedstaaten erlassen Vorschriften über Sanktionen, die bei Verstößen der Wirtschaftsakteure gegen diese Verordnung zu verhängen sind, und treffen alle für die Durchsetzung der Sanktionen erforderlichen Maßnahmen. Die vorgesehenen Sanktionen müssen wirksam, verhältnismäßig und abschreckend sein.

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

(3) Bei Nichteinhaltung der grundlegenden Anforderungen in Anhang I oder Verstößen gegen die in den Artikeln 10 und 11 festgelegten Pflichten, werden Geldbußen von bis zu 15 000 000 EUR oder – im Falle von Unternehmen – von bis zu 2,5 % des gesamten weltweiten Jahresumsatzes des vorangegangenen Geschäftsjahres verhängt, je nachdem, welcher Betrag höher ist.

(4) Bei Verstößen gegen andere Pflichten aus dieser Verordnung werden Geldbußen von bis zu 10 000 000 EUR oder – im Falle von Unternehmen – von bis zu 2 % des gesamten weltweiten Jahresumsatzes des vorangegangenen Geschäftsjahres verhängt, je nachdem, welcher Betrag höher ist.

(5) Werden gegenüber notifizierten Stellen und Marktüberwachungsbehörden auf deren Auskunftsverlangen hin falsche, unvollständige oder irreführende Angaben gemacht, so werden Geldbußen von bis zu 5 000 000 EUR oder – im Falle von Unternehmen –

[24] 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).

von bis zu 1 % des gesamten weltweiten Jahresumsatzes des vorangegangenen Geschäftsjahres verhängt, je nachdem, welcher Betrag höher ist.

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

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

b) ob bereits andere Marktüberwachungsbehörden demselben Akteur für einen ähnlichen Verstoß Geldbußen auferlegt haben,

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

(7) Marktüberwachungsbehörden, die Geldbußen verhängen, teilen dies den Marktüberwachungsbehörden der anderen Mitgliedstaaten über das in Artikel 34 der Verordnung (EU) 2019/1020 genannte Informations- und Kommunikationssystem mit.

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

(9) In Abhängigkeit vom Rechtssystem des betreffenden Mitgliedstaats können die Vorschriften über Geldbußen je nach den dort geltenden Regeln so angewandt werden, dass die Geldbußen entsprechend der auf nationaler Ebene in den Mitgliedstaaten festgelegten Verteilung der Zuständigkeiten von zuständigen nationalen Gerichten oder von anderen Stellen verhängt werden. Die Anwendung dieser Vorschriften in diesen Mitgliedstaaten muss eine gleichwertige Wirkung haben.

(10) Geldbußen können je nach den Umständen des Einzelfalls zusätzlich zu anderen Korrekturmaßnahmen oder einschränkenden Maßnahmen, die Marktüberwachungsbehörden für denselben Verstoß auferlegen, verhängt werden.

KAPITEL VIII

ÜBERGANGS- UND SCHLUSSBESTIMMUNGEN

Artikel 54

Änderung der Verordnung (EU) 2019/1020

In Anhang I der Verordnung (EU) 2019/1020 wird folgende Nummer angefügt:

„71. [Verordnung XXX][Cyberresilienzgesetz]“.

Artikel 55

Übergangsbestimmungen

(1) EU-Baumusterprüfbescheinigungen und Zulassungen, die in Bezug auf Cybersicherheitsanforderungen für Produkte mit digitalen Elementen erteilt wurden, die anderen Harmonisierungsrechtsvorschriften der Union unterliegen, bleiben bis zum [42 Monate nach dem Inkrafttreten dieser Verordnung] gültig, sofern sie nicht vor diesem Zeitpunkt ablaufen oder sofern in anderen Rechtsvorschriften der Union nichts anderes festgelegt ist; in letzterem Fall bleiben sie gemäß den letztgenannten Rechtsvorschriften der Union gültig.

(2) Produkte mit digitalen Elementen, die vor dem [Datum des Geltungsbeginns dieser Verordnung gemäß Artikel 57] in Verkehr gebracht wurden, unterliegen den Anforderungen dieser Verordnung nur dann, wenn nach diesem Zeitpunkt die Konzeption oder Zweckbestimmung dieser Produkte wesentlich geändert wurde.

(3) Abweichend von Absatz 2 gelten die in Artikel 11 festgelegten Pflichten für alle Produkte mit digitalen Elementen, die in den Anwendungsbereich dieser Verordnung fallen und vor dem [Datum des Geltungsbeginns dieser Verordnung gemäß Artikel 57] in Verkehr gebracht wurden.

Artikel 56

Bewertung und Überprüfung

Bis zum [36 Monate nach dem Datum des Geltungsbeginns dieser Verordnung] und danach alle vier Jahre legt die Kommission dem Europäischen Parlament und dem Rat einen Bericht über die Bewertung und Überprüfung dieser Verordnung vor. Die Berichte werden veröffentlicht.

Artikel 57

Inkrafttreten und Geltungsbeginn

Diese Verordnung tritt am zwanzigsten Tag nach ihrer Veröffentlichung im *Amtsblatt der Europäischen Union* in Kraft.

Sie gilt ab dem [24 Monate nach dem Datum des Inkrafttretens dieser Verordnung]. Artikel 11 gilt jedoch ab dem [12 Monate nach dem Datum des Inkrafttretens dieser Verordnung].

Diese Verordnung ist in allen ihren Teilen verbindlich und gilt unmittelbar in jedem Mitgliedstaat.

Geschehen zu Brüssel am […]

Im Namen des Europäischen Parlaments	*Im Namen des Rates*
Der Präsident /// Die Präsidentin	*Der Präsident /// Die Präsidentin*

FINANZBOGEN ZU RECHTSAKTEN

1. RAHMEN DES VORSCHLAGS/DER INITIATIVE

1.1. Bezeichnung des Vorschlags/der Initiative

1.2. Politikbereich(e)

1.3. Der Vorschlag/Die Initiative betrifft

1.4. Ziel(e)

1.4.1. Allgemeine(s) Ziel(e)

1.4.2. Einzelziel(e)

1.4.3. Erwartete Ergebnisse und Auswirkungen

1.4.4. Leistungsindikatoren

1.5. Begründung des Vorschlags/der Initiative

1.5.1. Kurz- oder langfristig zu deckender Bedarf, einschließlich einer detaillierten Zeitleiste für die Durchführung der Initiative

1.5.2. Mehrwert aufgrund des Tätigwerdens der Union (kann sich aus unterschiedlichen Faktoren ergeben, z. B. Vorteile durch Koordinierung, Rechtssicherheit, größerer Wirksamkeit oder Komplementarität). Für die Zwecke dieser Nummer bezeichnet der Ausdruck „Mehrwert aufgrund des Tätigwerdens der Union“ den Wert, der sich aus dem Tätigwerden der Union ergibt und den Wert ergänzt, der andernfalls allein von den Mitgliedstaaten geschaffen worden wäre.

1.5.3. Aus früheren ähnlichen Maßnahmen gewonnene Erkenntnisse

1.5.4. Vereinbarkeit mit dem Mehrjährigen Finanzrahmen sowie mögliche Synergieeffekte mit anderen geeigneten Instrumenten

1.5.5. Bewertung der verschiedenen verfügbaren Finanzierungsoptionen, einschließlich der Möglichkeiten für eine Umschichtung

1.6. Laufzeit und finanzielle Auswirkungen des Vorschlags/der Initiative

1.7. Vorgeschlagene Methode(n) der Mittelverwaltung

2. VERWALTUNGSMAßNAHMEN

2.1. Überwachung und Berichterstattung

2.2. Verwaltungs- und Kontrollsystem(e)

2.2.1. Begründung der Methode(n) der Mittelverwaltung, des Durchführungsmechanismus/der Durchführungsmechanismen für die Finanzierung, der Zahlungsmodalitäten und der Kontrollstrategie, wie vorgeschlagen

2.2.2. Angaben zu den ermittelten Risiken und dem/den zu deren Eindämmung eingerichteten System(en) der internen Kontrolle

2.2.3. Schätzung und Begründung der Kosteneffizienz der Kontrollen (Verhältnis zwischen den Kontrollkosten und dem Wert der betreffenden verwalteten Mittel) sowie Bewertung des erwarteten Ausmaßes des Fehlerrisikos (bei Zahlung und beim Abschluss)

2.3. Prävention von Betrug und Unregelmäßigkeiten

3. GESCHÄTZTE FINANZIELLE AUSWIRKUNGEN DES VORSCHLAGS/DER INITIATIVE

3.1. Betroffene Rubrik(en) des Mehrjährigen Finanzrahmens und Ausgabenlinie(n) im Haushaltsplan

3.2. Geschätzte finanzielle Auswirkungen des Vorschlags auf die Mittel

3.2.1. Übersicht über die geschätzten Auswirkungen auf die operativen Mittel

3.2.2. Geschätzte Ergebnisse, die mit operativen Mitteln finanziert werden

3.2.3. Übersicht über die geschätzten Auswirkungen auf die Verwaltungsmittel

3.2.4. Vereinbarkeit mit dem Mehrjährigen Finanzrahmen

3.2.5. Finanzierungsbeteiligung Dritter

3.3. Geschätzte Auswirkungen auf die Einnahmen

FINANZBOGEN ZU RECHTSAKTEN

1. RAHMEN DES VORSCHLAGS/DER INITIATIVE

1.1. Bezeichnung des Vorschlags/der Initiative

Vorschlag für eine Verordnung über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen (Cyberresilienzgesetz)

1.2. Politikbereich(e)

Kommunikationsnetze, Inhalte und Technologien

1.3. Der Vorschlag/Die Initiative betrifft

× **eine neue Maßnahme**

☐ **eine neue Maßnahme im Anschluss an ein Pilotprojekt/eine vorbereitende Maßnahme**[37]

☐ **die Verlängerung einer bestehenden Maßnahme**

☐ **die Zusammenführung mehrerer Maßnahmen oder die Neuausrichtung mindestens einer Maßnahme**

1.4. Ziel(e)

1.4.1. Allgemeine(s) Ziel(e)

Der Vorschlag hat zwei Hauptziele im Hinblick auf die Gewährleistung des reibungslosen Funktionierens des Binnenmarkts: 1) **die Schaffung der Bedingungen für die Entwicklung sicherer Produkte mit digitalen Elementen**, damit Hardware- und Softwareprodukte mit weniger Schwachstellen in Verkehr gebracht werden und damit die Hersteller sich während des gesamten Lebenszyklus eines Produkts ernsthaft um die Sicherheit kümmern; und 2) **die Schaffung von Bedingungen, die es den Nutzern ermöglichen, bei der Auswahl und Verwendung von Produkten mit digitalen Elementen die Cybersicherheit zu berücksichtigen**.

1.4.2. Einzelziel(e)

In dem Vorschlag wurden **vier spezifische Ziele** festgelegt: i) Gewährleistung, dass die Hersteller die Sicherheit von Produkten mit digitalen Elementen schon ab der Konzeptions- und Entwicklungsphase und über den gesamten Lebenszyklus verbessern; ii) Gewährleistung eines kohärenten Cybersicherheitsrahmens, der den Hardware- und Software-Herstellern die Einhaltung der Vorschriften erleichtert; iii) Erhöhung der Transparenz der Sicherheitseigenschaften von Produkten mit digitalen Elementen und iv) Befähigung der Unternehmen und Verbraucher, damit die Produkte mit digitalen Elementen sicher verwenden.

Erwartete Ergebnisse und Auswirkungen

Bitte geben Sie an, wie sich der Vorschlag/die Initiative auf die Begünstigten/Zielgruppen auswirken dürfte.

[37] Im Sinne des Artikels 58 Absatz 2 Buchstabe a oder b der Haushaltsordnung.

Die vorgeschlagene Verordnung würde den verschiedenen Beteiligten erhebliche Vorteile bringen. Für Unternehmen würde sie abweichende Sicherheitsvorschriften für Produkte mit digitalen Elementen verhindern und die Kosten der Einhaltung der einschlägigen Rechtsvorschriften zur Cybersicherheit senken. Sie würde dazu beitragen, die Zahl der Cybervorfälle, die Kosten der Bewältigung von Sicherheitsvorfällen und die Rufschädigung zu verringern. Schätzungen zufolge könnte die Initiative für die gesamte EU eine Senkung der den Unternehmen durch Vorfälle entstehenden Kosten um ungefähr 180 Mrd. EUR bis 290 Mrd. EUR pro Jahr bewirken[38]. Sie würde auch zu höheren Umsätzen infolge einer steigenden Nachfrage nach Produkten mit digitalen Elementen führen. Dies würde zudem den weltweiten Ruf der Unternehmen verbessern und eine wachsende Nachfrage auch außerhalb der EU nach sich ziehen. Für die Nutzer würde die bevorzugte Option die Transparenz der Sicherheitseigenschaften erhöhen und die Verwendung von Produkten mit digitalen Elementen erleichtern. Außerdem kämen die Verbraucher und Bürger so in den Genuss eines besseren Schutzes ihrer Grundrechte, z. B. im Hinblick auf die Privatsphäre und den Datenschutz.

Gleichzeitig würde der Vorschlag die Befolgungs- und Durchsetzungskosten für Unternehmen, notifizierte Stellen und Behörden, auch die Akkreditierungsstellen und Marktüberwachungsbehörden, erhöhen. Für Softwareentwickler und Hardwarehersteller werden dadurch zusätzliche direkte Befolgungskosten aufgrund neuer Sicherheitsanforderungen, Konformitätsbewertungs-, Dokumentations- und Meldepflichten anfallen, was zu aggregierten Befolgungskosten von bis zu 29 Mrd. EUR bei einem geschätzten Marktwert von 1485 Mrd. EUR führen wird[39]. Auf Seiten der Nutzer können sich für gewerbliche Nutzer, Verbraucher und die Bürgerinnen und Bürger höhere Preise für Produkte mit digitalen Elementen ergeben. Diese Preise sollten jedoch vor dem Hintergrund der oben beschriebenen erheblichen Vorteile betrachtet werden.

1.4.3. Leistungsindikatoren

Bitte geben Sie an, anhand welcher Indikatoren sich die Fortschritte und Ergebnisse verfolgen lassen.

Zur Überprüfung, ob die Hersteller die Sicherheit ihrer Produkte mit digitalen Elementen ab der Konzeptions- und Entwicklungsphase und während des gesamten Lebenszyklus dieser Produkte verbessern, könnten mehrere Indikatoren herangezogen werden. Solche Indikatoren wären z. B. die Zahl der durch Schwachstellen verursachten erheblichen Sicherheitsvorfälle in der Union, der Anteil der Hardware- und Software-Hersteller, die einen systematisch gesicherten Entwicklungszyklus befolgen, eine qualitative Analyse der Sicherheit von Produkten mit digitalen Elementen, eine quantitative und qualitative Bewertung von Schwachstellendatenbanken, die Häufigkeit der von Herstellern bereitgestellten Sicherheits-Patches oder die durchschnittliche Zahl der Tage zwischen der Aufdeckung einer Schwachstelle und der Bereitstellung von Sicherheits-Patches.

Ein Indikator für einen kohärenten Cybersicherheitsrahmen könnte das Fehlen gezielter produktspezifischer nationaler Cybersicherheitsvorschriften sein.

---

38 Siehe [Arbeitsunterlage der Kommissionsdienststellen über den Folgenabschätzungsbericht zur Verordnung über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen].

39 Siehe [Arbeitsunterlage der Kommissionsdienststellen über den Folgenabschätzungsbericht zur Verordnung über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen].

Ein Indikator für eine erhöhte Transparenz in Bezug auf die Sicherheitseigenschaften von Produkten mit digitalen Elementen könnte der Anteil der Produkte mit digitalen Elementen sein, die mit Informationen über Sicherheitseigenschaften ausgeliefert werden. Darüber hinaus könnte der Anteil der Produkte mit digitalen Elementen, die mit einer Gebrauchsanleitung für eine sichere Verwendung ausgeliefert werden, als Indikator dafür dienen, ob Organisationen und Verbraucher in die Lage versetzt werden, die Produkte mit digitalen Elementen sicher zu verwenden.

Zur Überwachung der Auswirkungen der Verordnung würden bestimmte Indikatoren in Betracht gezogen, die von der Kommission, gegebenenfalls mit Unterstützung der ENISA, geprüft werden müssten. In Abhängigkeit von dem zu erreichenden operativen Ziel wären einige der Überwachungsindikatoren, auf deren Grundlage der Erfolg der horizontalen Cybersicherheitsanforderungen bewertet würde, folgendermaßen zu bewerten sein:

Für die Bewertung eines hohen Niveaus der Cybersicherheit von Produkten mit digitalen Elementen:

– Statistiken und qualitative Analysen zu Vorfällen, die Produkte mit digitalen Elementen und die Art und Weise des Umgangs mit ihnen betreffen. Diese könnten von der Kommission mit Unterstützung der ENISA erfasst und bewertet werden.

– Aufzeichnungen über bekannte Schwachstellen und Analysen dazu, wie diese behandelt wurden. Eine solche Analyse könnte anhand der europäischen Schwachstellendatenbank, die auf der Grundlage der [Richtlinie XXX/XXXX (NIS2)] eingerichtet wurde, von der ENISA durchgeführt werden.

– Umfragen bei Hardware- und Software-Herstellern zur Verfolgung der Fortschritte.

Für die Bewertung des Umfangs der Informationen über Sicherheitsmerkmale, Sicherheitsunterstützung, Ende der Lebensdauer und Sorgfaltspflicht: Ergebnisse von Umfragen, die von der Kommission mit Unterstützung der ENISA sowohl bei Nutzern als bei Unternehmen durchgeführt werden müssten.

Für die Bewertung der Umsetzung möchte die Kommission sicherstellen, dass die Konformitätsbewertungen effektiv durchgeführt werden. Zu diesem Zweck wird ein Normungsauftrag erteilt, dessen Durchführung verfolgt wird. Die Kommission wird auch die Kapazitäten der notifizierten Stellen und gegebenenfalls der Zertifizierungsstellen überprüfen.

Bezüglich der Anwendung wird die Kommission anhand der Berichte der Mitgliedstaaten überprüfen, dass nationale Initiativen keine Aspekte betreffen, die unter diese Verordnung fallen.

1.5. Begründung des Vorschlags/der Initiative

1.5.1. Kurz- oder langfristig zu deckender Bedarf, einschließlich einer detaillierten Zeitleiste für die Durchführung der Initiative

Die Verordnung sollte 24 Monate nach ihrem Inkrafttreten uneingeschränkt anwendbar sein. Die Elemente der Leitungsstruktur sollten jedoch bereits vor diesem Zeitpunkt eingerichtet sein. Insbesondere müssen die Mitgliedstaaten bereits bestehende Behörden benannt und/oder neue Behörden eingerichtet haben, die die in den Rechtsvorschriften festgelegten Aufgaben wahrnehmen.

1.5.2. Mehrwert aufgrund des Tätigwerdens der Union (kann sich aus unterschiedlichen Faktoren ergeben, z. B. Vorteile durch Koordinierung, Rechtssicherheit, größerer

Wirksamkeit oder Komplementarität). Für die Zwecke dieser Nummer bezeichnet der Ausdruck „Mehrwert aufgrund des Tätigwerdens der Union“ den Wert, der sich aus dem Tätigwerden der Union ergibt und den Wert ergänzt, der andernfalls allein von den Mitgliedstaaten geschaffen worden wäre.

Aufgrund des ausgeprägten grenzüberschreitenden Charakters der Cybersicherheit und der zunehmenden Häufigkeit der Sicherheitsvorfälle, die sich über Grenzen, Sektoren und Produkte hinweg auswirken, können die Ziele von den Mitgliedstaaten allein nicht wirksam erreicht werden. Angesichts des globalen Charakters der Märkte für Produkte mit digitalen Elementen sehen sich die Mitgliedstaaten mit denselben Risiken bei denselben Produkten mit digitalen Elementen in ihrem Hoheitsgebiet konfrontiert. Aus einem sich abzeichnenden fragmentierten Rahmen mit möglicherweise voneinander abweichenden nationalen Vorschriften erwächst auch die Gefahr, dass Hindernisse für einen offenen und wettbewerbsfähigen Binnenmarkt für Produkte mit digitalen Elementen entstehen. Daher ist ein gemeinsames Vorgehen auf EU-Ebene erforderlich, um das Vertrauen der Nutzer und die Attraktivität von EU-Produkten mit digitalen Elementen zu steigern. Dies würde auch dem Binnenmarkt zugutekommen, denn so wird Rechtssicherheit gewährleistet und es werden gleiche Wettbewerbsbedingungen für die Anbieter von Produkten mit digitalen Elementen geschaffen.

1.5.3. Aus früheren ähnlichen Maßnahmen gewonnene Erkenntnisse

Das Cyberresilienzgesetz ist die erste Verordnung ihrer Art, mit der Cybersicherheitsanforderungen für das Inverkehrbringen von Produkten mit digitalen Elementen eingeführt werden. Die Verordnung beruht jedoch auf der Festlegung des Neuen Rechtsrahmens (NLF) und den Erkenntnissen, die bei der Durchführung bestehender Harmonisierungsrechtsvorschriften der Union für eine Vielzahl von Produkten gewonnen wurden, insbesondere im Hinblick auf die Vorbereitung der Durchführung mit Aspekten wie der Ausarbeitung harmonisierter Normen.

1.5.4. Vereinbarkeit mit dem Mehrjährigen Finanzrahmen sowie mögliche Synergieeffekte mit anderen geeigneten Instrumenten

In der Verordnung über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen werden neue Cybersicherheitsanforderungen für alle in der EU in Verkehr gebrachten Produkte mit digitalen Elementen festgelegt, die über die Anforderungen der bereits bestehenden Rechtsvorschriften hinausgehen. Gleichzeitig baut der Vorschlag auf dem bestehenden Rahmen der Rechtsvorschriften des Neuen Rechtsrahmens (NLF) auf. Die vorgeschlagene Verordnung würde daher auf bestehenden Strukturen und Verfahren des NLF aufbauen, wie etwa der Zusammenarbeit der notifizierten Stellen und der Marktüberwachung, den Konformitätsbewertungsmodulen und der Ausarbeitung harmonisierter Normen. Der neue Vorschlag würde sich auch auf einige Strukturen stützen, die im Rahmen anderer Rechtsvorschriften zur Cybersicherheit geschaffen wurden, wie der Richtlinie 2016/1148 (NIS-Richtlinie), der [Richtlinie XXX/XXXX (NIS2)] oder der Verordnung (EU) 2019/881 (Rechtsakt zur Cybersicherheit).

1.5.5. Bewertung der verschiedenen verfügbaren Finanzierungsoptionen, einschließlich der Möglichkeiten für eine Umschichtung

Das Management der Handlungsbereiche, die der ENISA zugewiesen werden, passt zu ihrem bestehenden Mandat und gehört zu ihren bestehenden allgemeinen Aufgaben. Diese Handlungsbereiche machen möglicherweise spezifische Profile

oder neue Aufgabenstellungen erforderlich, die jedoch nicht ins Gewicht fallen und sich mit den vorhandenen Ressourcen der ENISA durch Neuzuweisungen oder Verknüpfungen verschiedener Aufgaben abdecken lassen. Einer der Haupthandlungsbereiche, die der ENISA zugewiesen werden, betrifft beispielsweise das Erfassen und Bearbeiten von Meldungen der Hersteller über ausgenutzte Schwachstellen in den Produkten. So hat die ENISA aufgrund der [Richtlinie XXX/XXXX (NIS2)] bereits den Auftrag, eine europäische Schwachstellendatenbank einzurichten, in der öffentlich bekannte Schwachstellen auf freiwilliger Basis offengelegt und registriert werden können, damit die Nutzer geeignete Abhilfemaßnahmen ergreifen können. Die dafür zugewiesenen Mittel könnten auch für die oben genannten neuen Aufträge im Zusammenhang mit der Meldung von Produktschwachstellen verwendet werden. Dies würde eine wirksame Verwendung der vorhandenen Ressourcen sicherstellen und auch die notwendigen Synergien zwischen solchen Aufgaben schaffen, damit die ENISA über eine bessere Grundlage für ihre Analysen der Cybersicherheitsrisiken und -bedrohungen verfügt.

1.6. Laufzeit und finanzielle Auswirkungen des Vorschlags/der Initiative

☐ **befristete Laufzeit**

– ☐ Laufzeit: [TT.MM.]JJJJ bis [TT.MM.]JJJJ

– ☐ Finanzielle Auswirkungen auf die Mittel für Verpflichtungen von JJJJ bis JJJJ und auf die Mittel für Zahlungen von JJJJ bis JJJJ.

× **unbefristete Laufzeit**

– Anlaufphase ab 2025,

– anschließend reguläre Umsetzung.

1.7. Vorgeschlagene Methode(n) der Mittelverwaltung[40]

☐ **Direkte Mittelverwaltung** durch die Kommission

– × durch ihre Dienststellen, einschließlich ihres Personals in den Delegationen der Union

– ☐ durch Exekutivagenturen

☐ **Geteilte Mittelverwaltung** mit Mitgliedstaaten

☐ **Indirekte Mittelverwaltung** durch Übertragung von Haushaltsvollzugsaufgaben an:

– ☐ Drittländer oder die von ihnen benannten Einrichtungen

– ☐ internationale Einrichtungen und deren Agenturen (bitte angeben)

– ☐ die EIB und den Europäischen Investitionsfonds

– ☐ Einrichtungen im Sinne der Artikel 70 und 71 der Haushaltsordnung

– ☐ öffentlich-rechtliche Körperschaften

– ☐ privatrechtliche Einrichtungen, die im öffentlichen Auftrag tätig werden, sofern ihnen ausreichende finanzielle Garantien bereitgestellt werden

[40] Erläuterungen zu den Methoden der Mittelverwaltung und Verweise auf die Haushaltsordnung enthält die Website BudgWeb (in französischer und englischer Sprache): https://myintracomm.ec.europa.eu/budgweb/EN/man/budgmanag/Pages/budgmanag.aspx.

– ☐ privatrechtliche Einrichtungen eines Mitgliedstaats, die mit der Einrichtung einer öffentlich-privaten Partnerschaft betraut werden und denen ausreichende finanzielle Garantien bereitgestellt werden

– ☐ Personen, die mit der Durchführung bestimmter Maßnahmen im Bereich der GASP im Rahmen des Titels V EUV betraut und in dem maßgeblichen Basisrechtsakt benannt sind

– *Falls mehrere Methoden der Mittelverwaltung angegeben werden, ist dies unter „Bemerkungen" näher zu erläutern.*

Bemerkungen

In dieser Verordnung werden der ENISA bestimmte Maßnahmen übertragen; diese stehen im Einklang mit ihrem bestehenden Mandat und insbesondere mit Artikel 3 Absatz 2 der Verordnung (EU) 2019/881, wonach die ENISA die ihr durch Rechtsakte der Union zugewiesenen Aufgaben wahrnimmt, mit denen die Rechts- und Verwaltungsvorschriften der Mitgliedstaaten auf dem Gebiet der Cybersicherheit angeglichen werden sollen. Insbesondere wird die ENISA beauftragt, Meldungen von Herstellern über aktiv ausgenutzte Schwachstellen in Produkten mit digitalen Elementen sowie über Vorfälle, die sich auf die Sicherheit dieser Produkte auswirken, entgegennehmen. Die ENISA sollte diese Meldungen auch an die zuständigen CSIRTs bzw. an die gemäß Artikel [Artikel X] der Richtlinie [Richtlinie XXX/XXXX (NIS2)] benannten zentralen Anlaufstellen der Mitgliedstaaten weiterleiten und die Marktüberwachungsbehörden unterrichten. Auf der Grundlage der von ihr erfassten Informationen sollte die ENISA alle zwei Jahre einen technischen Bericht über aufkommende Trends der Cybersicherheitsrisiken bei Produkten mit digitalen Elementen erstellen und ihn der NIS-Kooperationsgruppe vorlegen. Darüber hinaus kann die ENISA angesichts ihrer Sachkenntnis, ihrer gesammelten Informationen und ihrer Bedrohungsanalysen den Prozess der Durchführung dieser Verordnung unterstützen und dazu gemeinsame Tätigkeiten vorschlagen, die von nationalen Marktüberwachungsbehörden auf der Grundlage von Hinweisen oder Informationen über eine mögliche Nichtkonformität von Produkten mit digitalen Elementen mit dieser Verordnung in mehreren Mitgliedstaaten durchgeführt werden sollen, oder Produktkategorien ermitteln, zu denen gleichzeitige koordinierte Kontrollen organisiert werden sollten. Die ENISA kann von der Kommission unter außergewöhnlichen Umständen beauftragt werden, Bewertungen in Bezug auf bestimmte Produkte mit digitalen Elementen durchzuführen, die ein erhebliches Cybersicherheitsrisiko bergen, wenn ein sofortiges Eingreifen erforderlich ist, um das reibungslose Funktionieren des Binnenmarkts zu bewahren.

Der Umfang aller dieser Aufträge wird auf etwa 4,5 VZÄ geschätzt, die aus den bestehenden Ressourcen der ENISA bereitzustellen sind, wobei auf vorhandenes Fachwissen und vorbereitende Arbeiten zurückgegriffen wird, die von der ENISA bereits durchgeführt werden, unter anderem zur Unterstützung der bevorstehenden Umsetzung der [Richtlinie XXX/XXXX (NIS2)], wofür die ENISA-Ressourcen aufgestockt wurden.

2. VERWALTUNGSMAßNAHMEN

2.1. Überwachung und Berichterstattung

Bitte geben Sie an, wie oft und unter welchen Bedingungen diese Tätigkeiten erfolgen.

Bis spätestens 36 Monate nach dem Datum des Geltungsbeginns dieser Verordnung und danach alle vier Jahre wird die Kommission dem Europäischen Parlament und dem Rat einen Bericht über ihre Bewertung und Überprüfung vorlegen. Die Berichte werden veröffentlicht.

2.2. Verwaltungs- und Kontrollsystem(e)

2.2.1. Begründung der Methode(n) der Mittelverwaltung, des Durchführungsmechanismus/der Durchführungsmechanismen für die Finanzierung, der Zahlungsmodalitäten und der Kontrollstrategie, wie vorgeschlagen

Mit dieser Verordnung wird ein neuer Politikansatz in Bezug auf harmonisierte Cybersicherheitsanforderungen festgelegt, die für Produkte mit digitalen Elementen, die im Binnenmarkt in Verkehr gebracht werden, über deren gesamten Lebenszyklus gelten sollen. Im Anschluss an den Erlass der Verordnung wird die Kommission den europäischen Normungsgremien Aufträge zur Ausarbeitung von Normen erteilen.

Um diesen neuen Aufgaben gerecht zu werden, müssen die Dienststellen der Kommission angemessen mit Ressourcen ausgestattet werden. Für die Durchsetzung der neuen Verordnung werden schätzungsweise 7 VZÄ (davon ein ANS) benötigt, um folgende Aufgaben wahrzunehmen:

– Ausarbeitung des Normungsauftrags und/oder gemeinsamer Spezifikationen, die ohne erfolgreiches Normungsverfahren im Wege von Durchführungsrechtsakte angenommen werden;

– Ausarbeitung eines delegierten Rechtsakts [innerhalb von 12 Monaten nach Inkrafttreten der Verordnung], in dem die Definitionen der kritischen Produkte mit digitalen Elementen festgelegt werden;

– mögliche Ausarbeitung delegierter Rechtsakte zur Aktualisierung der Liste kritischer Produkte der Klassen I und II, um festzulegen, ob eine Einschränkung oder ein Ausschluss für Produkte mit digitalen Elementen notwendig wäre, die unter andere Unionsvorschriften mit Anforderungen fallen, mit denen dasselbe Schutzniveau wie mit dieser Verordnung erreicht wird, um die Zertifizierung bestimmter hochkritischer Produkte mit digitalen Elementen auf der Grundlage der in dieser Verordnung festgelegten Kriterien vorzuschreiben, um die Mindestangaben der EU-Konformitätserklärung und die Ergänzung der in die technische Dokumentation aufzunehmenden Elemente vorzuschreiben;

– mögliche Ausarbeitung von Durchführungsrechtsakten in Bezug auf Format oder Elemente der Meldepflichten, der Software-Stückliste, gemeinsame Spezifikationen oder die Anbringung der CE-Kennzeichnung;

– mögliche Vorbereitung eines sofortigen Eingreifens zur Verhängung von Korrekturmaßnahmen oder einschränkenden Maßnahmen unter außergewöhnlichen Umständen, um das reibungslose Funktionieren des Binnenmarkts zu bewahren, einschließlich der Ausarbeitung eines Durchführungsrechtsakts;

– Organisation und Koordinierung der Notifizierungen notifizierter Stellen durch die Mitgliedstaaten und Koordinierung der benannten Stellen; – Unterstützung der Koordinierung der Marktüberwachungsbehörden der Mitgliedstaaten.

2.2.2. Angaben zu den ermittelten Risiken und dem/den zu deren Eindämmung eingerichteten System(en) der internen Kontrolle

Um sicherzustellen, dass die notifizierten Stellen und die Marktüberwachungsbehörden Informationen austauschen und gut zusammenarbeiten, übernimmt die Kommission ihre Koordinierung. Für die Nutzung technischen und marktbezogenen Fachwissens soll eine Expertengruppe eingesetzt werden.

2.2.3. Schätzung und Begründung der Kosteneffizienz der Kontrollen (Verhältnis zwischen den Kontrollkosten und dem Wert der betreffenden verwalteten Mittel) sowie Bewertung des erwarteten Ausmaßes des Fehlerrisikos (bei Zahlung und beim Abschluss)

2.3. Für die Sitzungskosten erscheinen angesichts des geringen Werts pro Transaktion (z. B. Erstattung der Reisekosten eines Delegierten für eine Sitzung) die üblichen Kontrollverfahren ausreichend. Prävention von Betrug und Unregelmäßigkeiten

Bitte geben Sie an, welche Präventions- und Schutzmaßnahmen, z. B. im Rahmen der Betrugsbekämpfungsstrategie, bereits bestehen oder angedacht sind.

Die für die Kommission geltenden Betrugsbekämpfungsmaßnahmen gelten auch für die zusätzlichen Mittel, die für diese Verordnung erforderlich werden.

3. GESCHÄTZTE FINANZIELLE AUSWIRKUNGEN DES VORSCHLAGS/DER INITIATIVE

3.1. Betroffene Rubrik(en) des Mehrjährigen Finanzrahmens und Ausgabenlinie(n) im Haushaltsplan

- Bestehende Haushaltslinien

Schema

- Neu zu schaffende Haushaltslinien

Nicht zutreffend

3.2. Geschätzte finanzielle Auswirkungen des Vorschlags auf die Mittel

3.2.1. Übersicht über die geschätzten Auswirkungen auf die operativen Mittel

– ☑ Für den Vorschlag/die Initiative werden keine operativen Mittel benötigt.

– ☐ Für den Vorschlag/die Initiative werden die folgenden operativen Mittel benötigt:

in Mio. EUR (3 Dezimalstellen)

Rubrik des Mehrjährigen Finanzrahmens	Nummer	

GD: <…….>			Jahr **N**[41]	Jahr **N+1**	Jahr **N+2**	Jahr **N+3**	Bei länger andauernden Auswirkungen (siehe 1.6.) bitte weitere Spalten einfügen.			**INSGESAMT**
•Operative Mittel										
Haushaltslinie[42]	Verpflichtungen	(1a)								
	Zahlungen	(2a)								
Haushaltslinie	Verpflichtungen	(1b)								
	Zahlungen	(2b)								
Aus der Dotation bestimmter spezifischer Programme finanzierte Verwaltungsausgaben[43]										
Haushaltslinie		(3)								
Mittel INSGESAMT für GD <…….>	Verpflichtungen	=1a+1b +3								
	Zahlungen	=2a+2b +3								

41 Das Jahr N ist das Jahr, in dem mit der Umsetzung des Vorschlags/der Initiative begonnen wird. Bitte ersetzen Sie „N“ durch das voraussichtlich erste Jahr der Umsetzung (z. B. 2021). Dasselbe gilt für die folgenden Jahre.

42 Gemäß dem offiziellen Eingliederungsplan.

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

• Operative Mittel INSGESAMT	Verpflichtungen	(4)								
	Zahlungen	(5)								
• Aus der Dotation bestimmter spezifischer Programme finanzierte Verwaltungsausgaben INSGESAMT		(6)								
Mittel INSGESAMT unter der Rubrik <….> des Mehrjährigen Finanzrahmens	Verpflichtungen	=4+6								
	Zahlungen	=5+6								

Wenn der Vorschlag/die Initiative mehrere operative Rubriken betrifft, ist der vorstehende Abschnitt zu wiederholen:

• Operative Mittel INSGESAMT (alle operativen Rubriken)	Verpflichtungen	(4)								
	Zahlungen	(5)								
Aus der Dotation bestimmter spezifischer Programme finanzierte Verwaltungsausgaben INSGESAMT (alle operativen Rubriken)		(6)								
Mittel INSGESAMT unter den Rubriken 1 bis 6 des Mehrjährigen Finanzrahmens (Referenzbetrag)	Verpflichtungen	=4+6								
	Zahlungen	=5+6								

Rubrik des Mehrjährigen Finanzrahmens	7	Verwaltungsausgaben

Zum Ausfüllen dieses Teils ist die „Tabelle für Verwaltungsausgaben“ zu verwenden, die zuerst in den Anhang des Finanzbogens zu Rechtsakten (Anhang V der Internen Vorschriften), der für die dienststellenübergreifende Konsultation in DECIDE hochgeladen wird, aufgenommen wird.

in Mio. EUR (3 Dezimalstellen)

		Jahr **2024**	Jahr **2025**	Jahr **2026**	Jahr **2027**	**INSGESAMT**
GD: CNECT						
• Personal		1,030	1,030	1,030	1,030	**4,120**
• Sonstige Verwaltungsausgaben		**0,222**	**0,222**	**0,222**	**0,222**	**0,888**
GD CNECT INSGESAMT	Mittel	**1,252**	**1,252**	**1,252**	**1,252**	**5,008**

Mittel INSGESAMT unter der Rubrik 7 des Mehrjährigen Finanzrahmens	(Verpflichtungen insges. = Zahlungen insges.)	**1,252**	**1,252**	**1,252**	**1,252**	**5,008**

in Mio. EUR (3 Dezimalstellen)

		Jahr **2024**	Jahr **2025**	Jahr **2026**	Jahr **2027**	**INSGESAMT**
Mittel INSGESAMT unter den Rubriken 1 bis 7 des Mehrjährigen Finanzrahmens	Verpflichtungen	**1,252**	**1,252**	**1,252**	**1,252**	**5,008**
	Zahlungen	**1,252**	**1,252**	**1,252**	**1,252**	**5,008**

3.2.2. Geschätzte Ergebnisse, die mit operativen Mitteln finanziert werden

Mittel für Verpflichtungen, in Mio. EUR (3 Dezimalstellen)

Ziele und Ergebnisse angeben ⇩			Jahr **N**		Jahr **N+1**		Jahr **N+2**		Jahr **N+3**		Bei länger andauernden Auswirkungen (siehe 1.6.) bitte weitere Spalten einfügen.						**INSGESAMT**	
	ERGEBNISSE																	
	Art[44]	Durch-schnitts-kosten	Anzahl	Kosten	Anzahl	Kosten	Anzahl	Kosten	Anzahl	Kosten	Anzahl	Kosten	Anzahl	Kosten	Anzahl	Kosten	Gesamt-zahl	Gesamt-kosten
EINZELZIEL Nr. 1[45] …																		
- Ergebnis																		
- Ergebnis																		
- Ergebnis																		
Zwischensumme für Einzelziel Nr. 1																		
EINZELZIEL Nr. 2 …																		
- Ergebnis																		
Zwischensumme für Einzelziel Nr. 2																		
INSGESAMT																		

[44] Ergebnisse sind Produkte, die geliefert, und Dienstleistungen, die erbracht werden (z. B.: Zahl der Austauschstudenten, gebaute Straßenkilometer…).

[45] Wie unter 1.4.2. („Einzelziele…“) beschrieben.

3.2.3. Übersicht über die geschätzten Auswirkungen auf die Verwaltungsmittel

– ☐ Für den Vorschlag/die Initiative werden keine Verwaltungsmittel benötigt.

– ☑ Für den Vorschlag/die Initiative werden die folgenden Verwaltungsmittel benötigt:

in Mio. EUR (3 Dezimalstellen)

	Jahr **2024**	Jahr **2025**	Jahr **2026**	Jahr **2027**	
RUBRIK 7 des Mehrjährigen Finanzrahmens					
Personal	1,030	1,030	1,030	1,030	**4,120**
Sonstige Verwaltungsausgaben	0,222	0,222	0,222	0,222	**0,888**
Zwischensummer der Rubrik 7 des Mehrjährigen Finanzrahmens	1,252	1,252	1,252	1,252	**5,008**
Außerhalb der Rubrik 7[46] des Mehrjährigen Finanzrahmens					
Personal					
Sonstige Verwaltungsausgaben					
Zwischensumme außerhalb der Rubrik 7 des Mehrjährigen Finanzrahmens					
INSGESAMT	1,252	1,252	1,252	1,252	**5,008**

Der Mittelbedarf für Personal- und sonstige Verwaltungsausgaben wird durch der Verwaltung der Maßnahme zugeordnete Mittel der GD oder GD-interne Personalumschichtung gedeckt. Hinzu kommen etwaige zusätzliche Mittel, die der für die Verwaltung der Maßnahme zuständigen GD nach Maßgabe der verfügbaren Mittel im Rahmen der jährlichen Mittelzuweisung zugeteilt werden.

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

3.2.3.1. Geschätzter Personalbedarf

– ☐ Für den Vorschlag/die Initiative wird kein Personal benötigt.

– ☑ Für den Vorschlag/die Initiative wird folgendes Personal benötigt:

Schätzung in Vollzeitäquivalenten

		Jahr **2024**	Jahr **2025**	Jahr **2026**	Jahr **2027**
20 01 02 01 (am Sitz und in den Vertretungen der Kommission)		6	6	6	6
20 01 02 03 (in den Delegationen)					
01 01 01 01 (indirekte Forschung)					
01 01 01 11 (direkte Forschung)					
Sonstige Haushaltslinien (bitte angeben)					
• Externes Personal (in Vollzeitäquivalenten – VZÄ)[47]					
20 02 01 (VB, ANS und LAK der Globaldotation)		1	1	1	1
20 02 03 (VB, ÖB, ANS, LAK und JFD in den Delegationen)					
XX 01 xx **yy zz**[48]	- am Sitz				
	- in den Delegationen				
01 01 01 02 (VB, ANS und LAK der indirekten Forschung)					
01 01 01 12 (VB, ANS und LAK der direkten Forschung)					
Sonstige Haushaltslinien (bitte angeben)					
INSGESAMT		**7**	**7**	**7**	**7**

XX steht für den jeweiligen Politikbereich bzw. Haushaltstitel.

Der Personalbedarf wird durch der Verwaltung der Maßnahme zugeordnetes Personal der GD oder GD-interne Personalumschichtung gedeckt. Hinzu kommen etwaige zusätzliche Mittel, die der für die Verwaltung der Maßnahme zuständigen GD nach Maßgabe der verfügbaren Mittel im Rahmen der jährlichen Mittelzuweisung zugeteilt werden.

Beschreibung der auszuführenden Aufgaben:

Beamte und Zeitbedienstete 6 VZÄ x 157 000 EUR/Jahr = 942 000 EUR	Wie unter 2.2.1. – Ausarbeitung des Normungsauftrags und/oder gemeinsamer Spezifikationen, die ohne erfolgreiches Normungsverfahren im Wege von Durchführungsrechtsakte angenommen werden; – Ausarbeitung eines delegierten Rechtsakts [innerhalb von 12 Monaten nach Inkrafttreten der Verordnung], in dem die Definitionen der kritischen Produkte mit digitalen Elementen festgelegt werden; – mögliche Ausarbeitung delegierter Rechtsakte zur Aktualisierung der Liste kritischer Produkte der Klassen I und II, um festzulegen, ob eine Einschränkung oder ein Ausschluss für Produkte mit digitalen Elementen notwendig wäre, die unter andere Unionsvorschriften mit Anforderungen fallen, mit denen dasselbe Schutzniveau wie mit dieser Verordnung erreicht wird, um die Zertifizierung bestimmter hochkritischer Produkte mit digitalen Elementen auf der Grundlage der in dieser Verordnung festgelegten Kriterien vorzuschreiben, um die Mindestangaben der EU-Konformitätserklärung und die Ergänzung der in die technische Dokumentation aufzunehmenden Elemente vorzuschreiben; – mögliche Ausarbeitung von Durchführungsrechtsakten in Bezug auf Format oder Elemente der Meldepflichten, der Software-Stückliste, gemeinsame

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

[48] Teilobergrenze für aus operativen Mitteln finanziertes externes Personal (vormalige BA-Linien).

	Spezifikationen oder die Anbringung der CE-Kennzeichnung; – mögliche Vorbereitung eines sofortigen Eingreifens zur Verhängung von Korrekturmaßnahmen oder einschränkenden Maßnahmen unter außergewöhnlichen Umständen, um das reibungslose Funktionieren des Binnenmarkts zu bewahren, einschließlich der Ausarbeitung eines Durchführungsrechtsakts; – Organisation und Koordinierung der Notifizierungen notifizierter Stellen durch die Mitgliedstaaten und Koordinierung der benannten Stellen; – Unterstützung der Koordinierung der Marktüberwachungsbehörden der Mitgliedstaaten.
Externes Personal 1 ANS x 88 000 EUR/Jahr	Wie unter 2.2.1. – Ausarbeitung des Normungsauftrags und/oder gemeinsamer Spezifikationen, die ohne erfolgreiches Normungsverfahren im Wege von Durchführungsrechtsakte angenommen werden; – Ausarbeitung eines delegierten Rechtsakts [innerhalb von 12 Monaten nach Inkrafttreten der Verordnung], in dem die Definitionen der kritischen Produkte mit digitalen Elementen festgelegt werden; – mögliche Ausarbeitung delegierter Rechtsakte zur Aktualisierung der Liste kritischer Produkte der Klassen I und II, um festzulegen, ob eine Einschränkung oder ein Ausschluss für Produkte mit digitalen Elementen notwendig wäre, die unter andere Unionsvorschriften mit Anforderungen fallen, mit denen dasselbe Schutzniveau wie mit dieser Verordnung erreicht wird, um die Zertifizierung bestimmter hochkritischer Produkte mit digitalen Elementen auf der Grundlage der in dieser Verordnung festgelegten Kriterien vorzuschreiben, um die Mindestangaben der EU-Konformitätserklärung und die Ergänzung der in die technische Dokumentation aufzunehmenden Elemente vorzuschreiben; – mögliche Ausarbeitung von Durchführungsrechtsakten in Bezug auf Format oder Elemente der Meldepflichten, der Software-Stückliste, gemeinsame Spezifikationen oder die Anbringung der CE-Kennzeichnung; – mögliche Vorbereitung eines sofortigen Eingreifens zur Verhängung von Korrekturmaßnahmen oder einschränkenden Maßnahmen unter außergewöhnlichen Umständen, um das reibungslose Funktionieren des Binnenmarkts zu bewahren, einschließlich der Ausarbeitung eines Durchführungsrechtsakts; – Organisation und Koordinierung der Notifizierungen notifizierter Stellen durch die Mitgliedstaaten und Koordinierung der benannten Stellen; – Unterstützung der Koordinierung der Marktüberwachungsbehörden der Mitgliedstaaten.

3.2.4. Vereinbarkeit mit dem Mehrjährigen Finanzrahmen

Der Vorschlag/Die Initiative

– x kann durch Umschichtungen innerhalb der entsprechenden Rubrik des Mehrjährigen Finanzrahmens (MFR) in voller Höhe finanziert werden.

Keine Anpassung erforderlich.

– ☐ erfordert die Inanspruchnahme des verbleibenden Spielraums unter der einschlägigen Rubrik des MFR und/oder den Einsatz der besonderen Instrumente im Sinne der MFR-Verordnung.

-

– ☐ erfordert eine Revision des MFR.

-

3.2.5. Finanzierungsbeteiligung Dritter

Der Vorschlag/Die Initiative

– x sieht keine Kofinanzierung durch Dritte vor.

– ☐ sieht folgende Kofinanzierung durch Dritte vor:

Mittel in Mio. EUR (3 Dezimalstellen)

	Jahr **N**[49]	Jahr **N+1**	Jahr **N+2**	Jahr **N+3**	Bei länger andauernden Auswirkungen (siehe 1.6.) bitte weitere Spalten einfügen.			Insgesamt
Kofinanzierende Einrichtung								
Kofinanzierung INSGESAMT								

[49] Das Jahr N ist das Jahr, in dem mit der Umsetzung des Vorschlags/der Initiative begonnen wird. Bitte ersetzen Sie „N“ durch das voraussichtlich erste Jahr der Umsetzung (z. B. 2021). Dasselbe gilt für die folgenden Jahre.

3.3. Geschätzte Auswirkungen auf die Einnahmen

– ☐ Der Vorschlag/Die Initiative wirkt sich nicht auf die Einnahmen aus.

– ☐ Der Vorschlag/Die Initiative wirkt sich auf die Einnahmen aus, und zwar

  – ☐ auf die Eigenmittel

  – ☐ auf die übrigen Einnahmen

  – Bitte geben Sie an, ob die Einnahmen bestimmten Ausgabenlinien zugewiesen sind. ☐

in Mio. EUR (3 Dezimalstellen)

Einnahmenlinie:	Für das laufende Haushaltsjahr zur Verfügung stehende Mittel	Auswirkungen des Vorschlags/der Initiative[50]						
		Jahr **N**	Jahr **N+1**	Jahr **N+2**	Jahr **N+3**	Bei länger andauernden Auswirkungen (siehe 1.6.) bitte weitere Spalten einfügen.		
Artikel ….								

Bitte geben Sie für die sonstigen zweckgebundenen Einnahmen die betreffende(n) Ausgabenlinie(n) im Haushaltsplan an.

Sonstige Anmerkungen (bei der Ermittlung der Auswirkungen auf die Einnahmen verwendete Methode/Formel oder weitere Informationen).

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

EUROPÄISCHE
KOMMISSION

Brüssel, den 15.9.2022
COM(2022) 454 final

ANNEXES 1 to 6

ANHÄNGE

des

VORSCHLAGS FÜR EINE VERORDNUNG DES EUROPÄISCHEN PARLAMENTS UND DES RATES

über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen und zur Änderung der Verordnung (EU) 2019/1020

{SEC(2022) 321 final} - {SWD(2022) 282 final} - {SWD(2022) 283 final}

ANHANG I

GRUNDLEGENDE CYBERSICHERHEITSANFORDERUNGEN

1. SICHERHEITSANFORDERUNGEN IN BEZUG AUF DIE EIGENSCHAFTEN VON PRODUKTEN MIT DIGITALEN ELEMENTEN

(1) Produkte mit digitalen Elementen werden so konzipiert, entwickelt und hergestellt, dass sie angesichts der Risiken ein angemessenes Cybersicherheitsniveau gewährleisten;

(2) Produkte mit digitalen Elementen werden ohne bekannte ausnutzbare Schwachstellen ausgeliefert;

(3) Auf der Grundlage der Risikobewertung gemäß Artikel 10 Absatz 2 müssen Produkte mit digitalen Elementen, soweit zutreffend,

a) mit einer sicheren Standardkonfiguration ausgeliefert werden und die Möglichkeit bieten, das Produkt in seinen ursprünglichen Zustand zurückzusetzen,

b) durch geeignete Kontrollmechanismen Schutz vor unbefugtem Zugriff bieten, darunter u. a. zumindest Authentifizierungs-, Identitäts- oder Zugangsverwaltungssysteme,

c) die Vertraulichkeit gespeicherter, übermittelter oder anderweitig verarbeiteter personenbezogener oder sonstiger Daten schützen, z. B. durch Verschlüsselung relevanter Daten, die gespeichert sind oder gerade verwendet oder übermittelt werden, durch modernste Mechanismen,

d) die Integrität gespeicherter, übermittelter oder anderweitig verarbeiteter Daten, ob personenbezogener oder sonstiger Daten, Befehle, Programme und Konfigurationen vor einer vom Nutzer nicht genehmigten Manipulation oder Veränderung schützen sowie deren Beschädigung melden,

e) die Verarbeitung personenbezogener oder sonstiger Daten auf solche, die angemessen und relevant sind, und auf das für die bestimmungsgemäße Verwendung des Produkts erforderliche Maß beschränken („Datenminimierung“),

f) die Verfügbarkeit wesentlicher Funktionen, einschließlich der Abwehrfähigkeit gegen Überlastungsangriffe auf Server (Denial-of-Service-Angriffe) und deren Eindämmung gewährleisten,

g) ihre eigenen negativen Auswirkungen auf die Verfügbarkeit der von anderen Geräten oder Netzen bereitgestellten Dienste minimieren,

h) so konzipiert, entwickelt und hergestellt werden, dass sie – auch bei externen Schnittstellen – möglichst geringe Angriffsflächen bieten,

i) so konzipiert, entwickelt und hergestellt werden, dass die Auswirkungen eines Vorfalls durch geeignete Mechanismen und Techniken zur Minderung der möglichen Ausnutzung verringert werden,

j) sicherheitsbezogene Informationen durch Aufzeichnung und/oder Überwachung einschlägiger interner Vorgänge wie Zugang zu Daten, Diensten oder Funktionen und Änderungen daran bereitstellen,

k) sicherstellen, dass Schwachstellen durch Sicherheitsaktualisierungen behoben werden können, gegebenenfalls auch durch automatische Aktualisierungen und die Benachrichtigung der Nutzer über verfügbare Aktualisierungen.

2. ANFORDERUNGEN AN DIE BEHANDLUNG VON SCHWACHSTELLEN

Die Hersteller der Produkte mit digitalen Elementen müssen

(1) Schwachstellen und Komponenten des Produkts ermitteln und dokumentieren, u. a. durch Erstellung einer Software-Stückliste in einem gängigen maschinenlesbaren Format, aus der zumindest die obersten Abhängigkeiten des Produkts hervorgehen;

(2) im Hinblick auf die Risiken im Zusammenhang mit den Produkten mit digitalen Elementen unverzüglich Schwachstellen behandeln und beheben, unter anderem durch Bereitstellung von Sicherheitsaktualisierungen;

(3) die Sicherheit des Produkts mit digitalen Elementen regelmäßig und wirksam testen und überprüfen;

(4) sobald eine Sicherheitsaktualisierung bereitgestellt worden ist, Informationen über beseitigte Schwachstellen veröffentlichen, einschließlich einer Beschreibung der Schwachstellen mit Angaben, anhand deren die Nutzer das betroffene Produkt mit digitalen Elementen, die Auswirkungen der Schwachstellen und ihre Schwere erkennen können, sowie Informationen, die den Nutzern helfen, die Schwachstellen zu beheben;

(5) eine Strategie für die koordinierte Offenlegung von Schwachstellen aufstellen und umsetzen;

(6) Maßnahmen ergreifen, um den Austausch von Informationen über mögliche Schwachstellen in ihrem Produkt mit digitalen Elementen und darin enthaltenen Komponenten Dritter zu erleichtern, und dazu u. a. eine Kontaktadresse für die Meldung der in dem Produkt mit digitalen Elementen entdeckten Schwachstellen angeben;

(7) Mechanismen für die sichere Verbreitung von Aktualisierungen für Produkte mit digitalen Elementen bereitstellen, damit ausnutzbare Schwachstellen rechtzeitig behoben oder eingedämmt werden;

(8) dafür sorgen, dass Sicherheits-Patches oder -Aktualisierungen, die zur Bewältigung festgestellter Sicherheitsprobleme zur Verfügung stehen, unverzüglich und kostenlos verbreitet werden, zusammen mit Hinweisen und einschlägigen Informationen, auch über zu treffende mögliche Maßnahmen.

ANHANG II

INFORMATIONEN UND ANLEITUNGEN FÜR DEN NUTZER

Dem Produkt mit digitalen Elementen muss mindestens Folgendes beigefügt sein:

1. Name, eingetragener Handelsname oder eingetragene Handelsmarke, Postanschrift und E-Mail-Adresse, unter denen der Hersteller erreichbar ist, entweder auf dem Produkt selbst oder, wenn dies nicht möglich ist, auf der Verpackung oder in den dem Produkt beigefügten Unterlagen;
2. die Kontaktstelle, bei der Informationen über Cybersicherheitslücken des Produkts gemeldet werden können und entgegengenommen werden;
3. korrekte Angaben zu Typ, Chargen-, Versions- oder Seriennummer oder anderen Elementen, die eine Identifizierung des Produkts ermöglichen, sowie die entsprechenden Anleitungen und Informationen für die Nutzer;
4. die bestimmungsgemäße Verwendung, einschließlich des vom Hersteller bereitgestellten Sicherheitsumfelds, sowie die Hauptfunktionen des Produkts und Informationen über die Sicherheitseigenschaften;
5. alle bekannten oder vorhersehbaren Umstände im Zusammenhang mit der bestimmungsgemäßen Verwendung des Produkts mit digitalen Elementen oder dessen vernünftigerweise vorhersehbaren Fehlanwendung, die zu erheblichen Cybersicherheitsrisiken führen können;
6. ob und gegebenenfalls wo die Software-Stückliste abrufbar ist;
7. gegebenenfalls die Internetadresse, unter der die EU-Konformitätserklärung abrufbar ist;
8. die Art der vom Hersteller angebotenen technischen Sicherheitsunterstützung, bis wann sie zur Verfügung steht und zumindest bis wann die Nutzer Sicherheitsaktualisierungen erwarten können;
9. ausführliche Anleitungen oder eine Internetadresse, unter der auf solche ausführlichen Anleitungen und Informationen verwiesen wird, dazu,
   a) welche Maßnahmen bei der ersten Inbetriebnahme und während der gesamten Lebensdauer des Produkts getroffen werden müssen, um dessen sichere Verwendung zu gewährleisten,
   b) wie sich Änderungen am Produkt auf die Datensicherheit auswirken können,
   c) wie sicherheitsrelevante Aktualisierungen installiert werden können,
   d) wie eine sichere Außerbetriebnahme des Produkts erfolgt und wie Nutzerdaten sicher entfernt werden können.

ANHANG III

KRITISCHE PRODUKTE MIT DIGITALEN ELEMENTEN

Klasse I

1. Software für Identitätsmanagementsysteme und Software für die Verwaltung des privilegierten Zugangs;
2. eigenständige und eingebettete Browser;
3. Passwort-Manager;
4. Software für die Suche, Entfernung und Quarantäne von Schadsoftware;
5. Produkte mit digitalen Elementen mit der Funktion eines virtuellen privaten Netzes (VPN);
6. Netzmanagementsysteme;
7. Instrumente für die Netzkonfigurationsverwaltung;
8. Systeme für die Überwachung des Netzverkehrs;
9. Verwaltung der Netzressourcen;
10. Systeme für die Verwaltung von Sicherheitsinformationen und -ereignissen (SIEM);
11. Aktualisierungs- und Patchverwaltung, einschließlich Bootmanager;
12. Systeme für die Anwendungskonfigurationsverwaltung;
13. Software für Fernzugriff und gemeinsame Datennutzung;
14. Software für die Mobilgeräteverwaltung;
15. physische Netzschnittstellen;
16. Betriebssysteme, die nicht zur Klasse II gehören;
17. Firewalls, Angriffserkennungs- und/oder -präventionssysteme, die nicht zur Klasse II gehören;
18. Router, Modems für die Internetanbindung und Switches, die nicht zur Klasse II gehören;
19. Mikroprozessoren, die nicht zur Klasse II gehören;
20. Mikrocontroller;
21. anwendungsspezifische integrierte Schaltungen (ASIC) und FPGAs (*Field Programmable Gate Array*), die zur Verwendung durch wesentliche Einrichtungen der in [Anhang I der Richtlinie XXX/XXXX (NIS2)] genannten Art bestimmt sind;
22. industrielle Automatisierungs- und Steuerungssysteme (IACS), die nicht zur Klasse II gehören, wie z. B. speicherprogrammierbare Steuerungen (PLC), verteilte Steuerungssysteme (DCS), computergestützte numerische Steuerungen für Werkzeugmaschinen (CNC) und Prozesssteuerungs- und Datenerfassungssysteme (SCADA);
23. industrielles Internet der Dinge (IIoT), das nicht zur Klasse II gehört.

Klasse II

1. Betriebssysteme für Server, Desktops und Mobilgeräte;
2. Hypervisoren und Container-Runtime-Systeme, die eine virtualisierte Ausführung von Betriebssystemen und ähnlichen Umgebungen unterstützen;
3. Public-Key-Infrastrukturen und Aussteller digitaler Zertifikate;
4. Firewalls, Angriffserkennungs- und/oder -präventionssysteme für den industriellen Einsatz;
5. Allzweck-Mikroprozessoren;
6. Mikroprozessoren, die für die Integration in speicherprogrammierbare Steuerungen (PLC) und Sicherheitselemente bestimmt sind;
7. Router, Modems für die Internetanbindung und Switches für den industriellen Einsatz;
8. Sicherheitselemente;
9. Hardware-Sicherheitsmodule (HSM);
10. sichere Kryptoprozessoren;
11. Chipkarten, Chipkartenleser und Token;
12. industrielle Automatisierungs- und Steuerungssysteme (IACS), die zur Verwendung durch wesentliche Einrichtungen der in [Anhang I der Richtlinie XXX/XXXX (NIS2)] genannten Art bestimmt sind, wie z. B. speicherprogrammierbare Steuerungen (PLC), verteilte Steuerungssysteme (DCS), computergestützte numerische Steuerungen für Werkzeugmaschinen (CNC) und Prozesssteuerungs- und Datenerfassungssysteme (SCADA);
13. Geräte für das industrielle Internet der Dinge (IIoT), die zur Verwendung durch wesentliche Einrichtungen der in [Anhang I der Richtlinie XXX/XXXX (NIS2)] genannten Art bestimmt sind;
14. Sensor- und Aktuatorkomponenten von Robotern und Robotersteuerungen;
15. intelligente Zähler.

ANHANG IV

EU-KONFORMITÄTSERKLÄRUNG

Die EU-Konformitätserklärung gemäß Artikel 20 enthält alle folgenden Angaben:

1. den Namen und den Typ sowie alle zusätzlichen Informationen, die eine eindeutige Identifizierung des Produkts mit digitalen Elementen ermöglichen;
2. den Namen und die Anschrift des Herstellers oder seines Bevollmächtigten;
3. eine Erklärung darüber, dass der Anbieter die alleinige Verantwortung für die Ausstellung der EU-Konformitätserklärung trägt;
4. den Gegenstand der Erklärung (Bezeichnung des Produkts zwecks Rückverfolgbarkeit, gegebenenfalls mit Foto);
5. eine Erklärung, dass der oben beschriebene Gegenstand der Erklärung den einschlägigen Harmonisierungsrechtsvorschriften der Union entspricht;
6. Verweise auf die verwendeten einschlägigen harmonisierten Normen oder sonstigen gemeinsamen Spezifikationen oder die Cybersicherheitszertifizierung, für die die Konformität erklärt wird;
7. gegebenenfalls den Namen und die Kennnummer der notifizierten Stelle, eine Beschreibung des durchgeführten Konformitätsbewertungsverfahrens und die Kennnummer der ausgestellten Bescheinigung;
8. weitere Angaben:

Unterzeichnet für und im Namen von: ……

(Ort und Datum der Ausstellung)

(Name, Funktion) (Unterschrift)

ANHANG V

INHALT DER TECHNISCHEN DOKUMENTATION

Die in Artikel 23 genannte technische Dokumentation muss mindestens die folgenden Informationen enthalten, soweit sie für das betreffende Produkt mit digitalen Elementen von Belang sind:

1. eine allgemeine Beschreibung des Produkts mit digitalen Elementen, einschließlich
   a) seiner Zweckbestimmung,
   b) Softwareversionen, die sich auf die Erfüllung der grundlegenden Anforderungen auswirken,
   c) wenn es sich bei dem Produkt mit digitalen Elementen um ein Hardwareprodukt handelt: Fotografien oder Abbildungen, aus denen äußere Merkmale, Kennzeichnungen und innerer Aufbau hervorgehen;
   d) Informationen und Anleitungen für die Nutzer gemäß Anhang II;
2. eine Beschreibung der Konzeption, Entwicklung und Herstellung des Produkts und der Verfahren zur Behandlung von Schwachstellen, einschließlich
   a) vollständiger Informationen über die Konzeption und Entwicklung des Produkts mit digitalen Elementen, gegebenenfalls mit Zeichnungen und Schemata und/oder einer Beschreibung der Systemarchitektur, aus der hervorgeht, wie Softwarekomponenten aufeinander aufbauen, miteinander zusammenwirken und sich in die Gesamtverarbeitung integrieren;
   b) vollständiger Informationen und Spezifikationen bezüglich der vom Hersteller festgelegten Verfahren zur Behandlung von Schwachstellen, einschließlich der Software-Stückliste, des Konzepts für die koordinierte Offenlegung von Schwachstellen, des Nachweises der Bereitstellung einer Kontaktadresse für die Meldung der Schwachstellen und einer Beschreibung der gewählten technischen Lösungen für die sichere Verbreitung von Aktualisierungen;
   c) vollständiger Informationen und Spezifikationen bezüglich der Herstellungs- und Überwachungsprozesse des Produkts mit digitalen Elementen und der Validierung dieser Prozesse;
3. eine Bewertung der Cybersicherheitsrisiken, die bei der Konzeption, Entwicklung, Herstellung, Lieferung und Wartung des Produkts mit digitalen Elementen nach Artikel 10 dieser Verordnung berücksichtigt werden;
4. eine Aufstellung der vollständig oder teilweise angewandten harmonisierten Normen, deren Fundstellen im *Amtsblatt der Europäischen Union* veröffentlicht wurden, der in Artikel 19 dieser Verordnung genannten gemeinsamen Spezifikationen oder der in Artikel 18 Absatz 3 genannten Systeme für die Cybersicherheitszertifizierung gemäß der Verordnung (EU) 2019/881 und, falls keine solchen harmonisierten Normen, gemeinsamen Spezifikationen und Systeme für die Cybersicherheitszertifizierung angewandt werden, Beschreibungen der Lösungen, mit denen die grundlegenden Anforderungen in Anhang I Abschnitte 1 und 2 erfüllt werden, mit einer Aufstellung sonstiger angewandter einschlägiger technischer Spezifikationen. Bei einer teilweisen Anwendung harmonisierter Normen, gemeinsamer Spezifikationen oder

Cybersicherheitszertifizierungen ist in der technischen Dokumentation anzugeben, welche Teile angewandt wurden;

5. Berichte über die Tests und Prüfungen, die durchgeführt wurden, um die Konformität des Produkts und der Verfahren zur Behandlung von Schwachstellen mit den geltenden grundlegenden Anforderungen in Anhang I Abschnitte 1 und 2 zu überprüfen;

6. ein Exemplar der EU-Konformitätserklärung;

7. gegebenenfalls auf begründetes Verlangen der Marktüberwachungsbehörde die Software-Stückliste gemäß Artikel 3 Nummer 36, sofern dies erforderlich ist, damit diese Behörde die Einhaltung der grundlegenden Anforderungen in Anhang I überprüfen kann.

ANHANG VI

KONFORMITÄTSBEWERTUNGSVERFAHREN

Konformitätsbewertungsverfahren auf der Grundlage einer internen Kontrolle (auf der Grundlage von Modul A)

1. Bei der internen Kontrolle handelt es sich um das Konformitätsbewertungsverfahren, mit dem der Hersteller die in den Nummern 2, 3 und 4 genannten Pflichten erfüllt sowie gewährleistet und auf eigene Verantwortung erklärt, dass die Produkte mit digitalen Elementen allen grundlegenden Anforderungen in Anhang I Abschnitt 1 genügen und dass der Hersteller die grundlegenden Anforderungen in Anhang I Abschnitt 2 erfüllt.

2. Der Hersteller erstellt die technische Dokumentation gemäß Anhang V.

3. Konzeption, Entwicklung, Herstellung und Behandlung von Schwachstellen bei Produkten mit digitalen Elementen

   Der Hersteller trifft alle erforderlichen Maßnahmen, damit die Verfahren der Konzeption, Entwicklung, Herstellung und Schwachstellenbehandlung und deren Überwachung die Konformität der hergestellten oder entwickelten Produkte mit digitalen Elementen und der vom Hersteller festgelegten Verfahren mit den grundlegenden Anforderungen in Anhang I Abschnitte 1 und 2 gewährleisten.

4. Konformitätskennzeichnung und Konformitätserklärung

4.1. Der Hersteller bringt die CE-Kennzeichnung an jedem einzelnen Produkt mit digitalen Elementen an, das den geltenden Anforderungen dieser Verordnung genügt.

4.2. Der Hersteller stellt für jedes Produkt mit digitalen Elementen eine schriftliche EU-Konformitätserklärung gemäß Artikel 20 aus und hält sie zusammen mit der technischen Dokumentation für einen Zeitraum von zehn Jahren ab dem Inverkehrbringen des Produkts mit digitalen Elementen für die nationalen Behörden bereit. Aus der EU-Konformitätserklärung muss hervorgehen, für welches Produkt mit digitalen Elementen sie ausgestellt wurde. Ein Exemplar der EU-Konformitätserklärung wird den zuständigen Behörden auf Verlangen zur Verfügung gestellt.

5. Bevollmächtigte

   Die unter Nummer 4 genannten Pflichten des Herstellers können von seinem Bevollmächtigten in seinem Auftrag und unter seiner Verantwortung erfüllt werden, falls sie im Auftrag festgelegt sind.

EU-Baumusterprüfung (auf der Grundlage von Modul B)

1. Bei der EU-Baumusterprüfung handelt es sich um den Teil eines Konformitätsbewertungsverfahrens, bei dem eine notifizierte Stelle die technische Konzeption und Entwicklung eines Produkts und die vom Hersteller festgelegten Verfahren zur Behandlung von Schwachstellen untersucht und prüft und sodann bescheinigt, dass ein Produkt mit digitalen Elementen den grundlegenden Anforderungen in Anhang I Abschnitt 1 genügt und dass der Hersteller die grundlegenden Anforderungen in Anhang I Abschnitt 2 erfüllt.

– Die EU-Baumusterprüfung erfolgt als Bewertung der Eignung der technischen Konzeption und Entwicklung des Produkts anhand der Prüfung der in Nummer 3 genannten technischen Dokumentation und zusätzlichen Nachweise sowie der Prüfung von Mustern eines oder mehrerer wichtiger Teile des Produkts (Kombination aus Bau- und Konzeptionsmuster).

2. Der Antrag auf EU-Baumusterprüfung wird vom Hersteller bei einer einzigen benannten Stelle seiner Wahl eingereicht.

Der Antrag enthält

– den Namen und die Anschrift des Herstellers sowie, wenn der Antrag vom Bevollmächtigten eingereicht wird, auch dessen Namen und Anschrift;

– eine schriftliche Erklärung, dass derselbe Antrag bei keiner anderen notifizierten Stelle eingereicht worden ist;

– die technische Dokumentation, anhand deren bewertet werden kann, ob das Produkt den geltenden grundlegenden Anforderungen in Anhang I Abschnitt 1 und die Verfahren des Herstellers zur Behandlung von Schwachstellen den Anforderungen in Anhang I Abschnitt 2 genügen; sie muss auch eine angemessene Risikoanalyse und -bewertung enthalten. In der technischen Dokumentation sind die geltenden Anforderungen aufzuführen und die Konzeption, die Herstellung und die Arbeitsweise des Produkts zu erfassen, soweit sie für die Bewertung von Belang sind. Die technische Dokumentation enthält gegebenenfalls zumindest die in Anhang V aufgeführten Elemente;

– zusätzliche Nachweise für die Eignung der Lösungen für die technische Konzeption und Entwicklung und der Verfahren zur Behandlung von Schwachstellen. In diesen zusätzlichen Nachweisen müssen alle Unterlagen vermerkt sein, nach denen vorgegangen wurde, insbesondere wenn die einschlägigen harmonisierten Normen und/oder technischen Spezifikationen nicht in vollem Umfang angewandt worden sind. Die Nachweise umfassen erforderlichenfalls die Ergebnisse von Prüfungen, die von einem geeigneten Labor des Herstellers oder von einem anderen Prüflabor in seinem Auftrag und unter seiner Verantwortung durchgeführt wurden.

3. Die notifizierte Stelle

3.1. prüft die technische Dokumentation und die zusätzlichen Nachweise, um die Übereinstimmung der technischen Konzeption und Entwicklung des Produkts mit den grundlegenden Anforderungen in Anhang I Abschnitt 1 und der vom Hersteller festgelegten Verfahren zur Behandlung von Schwachstellen mit den grundlegenden Anforderungen in Anhang I Abschnitt 2 zu bewerten;

3.2. überprüft, ob das/die Muster in Übereinstimmung mit der technischen Dokumentation entwickelt oder hergestellt wurde/n, welche Elemente nach den geltenden Vorschriften der einschlägigen harmonisierten Normen und/oder technischen Spezifikationen konzipiert und entwickelt wurden und welche Elemente ohne Anwendung der einschlägigen Vorschriften dieser Normen konzipiert und entwickelt wurden;

3.3. führt geeignete Untersuchungen und Prüfungen durch bzw. veranlasst diese, um festzustellen, ob die Lösungen aus den einschlägigen harmonisierten Normen und/oder technischen Spezifikationen im Hinblick auf die Anforderungen in

Anhang I korrekt angewandt worden sind, sofern sich der Hersteller für ihre Anwendung entschieden hat;

3.4. führt geeignete Untersuchungen und Prüfungen durch bzw. veranlasst diese, um festzustellen, ob die vom Hersteller gewählten Lösungen die entsprechenden grundlegenden Anforderungen erfüllen, falls der Hersteller die Lösungen aus den einschlägigen harmonisierten Normen und/oder den technischen Spezifikationen für die Anforderungen in Anhang I nicht angewandt hat;

3.5. vereinbart mit dem Hersteller, wo die Untersuchungen und Prüfungen durchgeführt werden.

4. Die notifizierte Stelle erstellt einen Bericht über die Beurteilung der nach Nummer 4 ausgeführten Tätigkeiten und deren Ergebnisse. Unbeschadet ihrer Pflichten gegenüber den notifizierenden Behörden veröffentlicht die notifizierte Stelle den Inhalt dieses Berichts oder Teile davon nur mit Zustimmung des Herstellers.

5. Entsprechen das Baumuster und die Verfahren zur Behandlung von Schwachstellen den grundlegenden Anforderungen in Anhang I, so stellt die notifizierte Stelle dem Hersteller eine EU-Baumusterprüfbescheinigung aus. Die Bescheinigung enthält den Namen und die Anschrift des Herstellers, die Ergebnisse der Prüfung, etwaige Bedingungen für ihre Gültigkeit und die erforderlichen Daten für die Identifizierung des zugelassenen Baumusters und des Verfahrens zur Behandlung von Schwachstellen. Der Bescheinigung können ein oder mehrere Anhänge beigefügt werden.

   Die Bescheinigung und ihre Anhänge enthalten alle zweckdienlichen Angaben, anhand deren sich die Konformität der hergestellten oder entwickelten Produkte mit dem geprüften Baumuster und die Konformität der Verfahren zur Behandlung von Schwachstellen beurteilen und gegebenenfalls eine Kontrolle nach ihrer Inbetriebnahme durchführen lassen.

   Entsprechen das Baumuster und die Verfahren zur Behandlung von Schwachstellen nicht den anwendbaren grundlegenden Anforderungen in Anhang I, so verweigert die notifizierte Stelle die Ausstellung einer EU-Baumusterprüfbescheinigung und unterrichtet den Antragsteller darüber, wobei sie ihre Weigerung ausführlich begründet.

6. Die notifizierte Stelle hält sich über alle Änderungen des allgemein anerkannten Stands der Technik auf dem Laufenden; deuten diese darauf hin, dass das zugelassene Baumuster und die Verfahren zur Behandlung von Schwachstellen nicht mehr den geltenden grundlegenden Anforderungen in Anhang I dieser Verordnung entsprechen, so entscheidet sie, ob derartige Änderungen weitere Untersuchungen nötig machen. Ist dies der Fall, so setzt die notifizierte Stelle den Hersteller davon in Kenntnis.

   Der Hersteller unterrichtet die notifizierte Stelle, der die technische Dokumentation zur EU-Baumusterprüfbescheinigung vorliegt, über alle Änderungen an dem zugelassenen Baumuster und dem Verfahren zur Behandlung von Schwachstellen, die die Übereinstimmung mit den grundlegenden Anforderungen in Anhang I oder mit den Bedingungen für die Gültigkeit der Bescheinigung beeinträchtigen könnten. Derartige Änderungen erfordern eine Zusatzgenehmigung in Form einer Ergänzung der ursprünglichen EU-Baumusterprüfbescheinigung.

7. Jede notifizierte Stelle unterrichtet ihre notifizierenden Behörden über die EU-Baumusterprüfbescheinigungen und/oder etwaige Ergänzungen dazu, die sie

ausgestellt oder zurückgenommen hat, und übermittelt ihren notifizierenden Behörden in regelmäßigen Abständen oder auf Verlangen eine Aufstellung aller Bescheinigungen und/oder Ergänzungen dazu, die sie verweigert, ausgesetzt oder auf andere Art eingeschränkt hat.

Jede notifizierte Stelle unterrichtet die übrigen notifizierten Stellen über die EU-Baumusterprüfbescheinigungen und/oder etwaige Ergänzungen dazu, die sie verweigert, zurückgenommen, ausgesetzt oder auf andere Weise eingeschränkt hat, und auf Verlangen über die Bescheinigungen und/oder Ergänzungen dazu, die sie ausgestellt hat.

Auf Verlangen erhalten die Kommission, die Mitgliedstaaten und die anderen notifizierten Stellen ein Exemplar der EU-Baumusterprüfbescheinigungen und/oder ihrer Ergänzungen. Die Kommission und die Mitgliedstaaten erhalten auf Verlangen ein Exemplar der technischen Dokumentation und der Ergebnisse der durch die notifizierte Stelle vorgenommenen Prüfungen. Die notifizierte Stelle bewahrt ein Exemplar der EU-Baumusterprüfbescheinigung samt Anhängen und Ergänzungen sowie des technischen Dossiers einschließlich der vom Hersteller eingereichten Unterlagen so lange auf, bis die Gültigkeitsdauer der Bescheinigung endet.

8. Der Hersteller hält ein Exemplar der EU-Baumusterprüfbescheinigung samt Anhängen und Ergänzungen zusammen mit der technischen Dokumentation zehn Jahre lang nach dem Inverkehrbringen des Erzeugnisses für die nationalen Behörden bereit.

9. Der Bevollmächtigte des Herstellers kann den in Nummer 3 genannten Antrag einreichen und die in den Nummern 7 und 9 genannten Pflichten erfüllen, falls sie in dem Auftrag festgelegt sind.

Konformität mit dem Baumuster auf der Grundlage einer internen Fertigungskontrolle (auf der Grundlage von Modul C)

1. Bei der Konformität mit dem Baumuster auf der Grundlage einer internen Fertigungskontrolle handelt es sich um den Teil eines Konformitätsbewertungsverfahrens, bei dem der Hersteller die in den Nummern 2 und 3 genannten Pflichten erfüllt sowie gewährleistet und erklärt, dass die betreffenden Produkte dem in der EU-Baumusterprüfbescheinigung beschriebenen Baumuster entsprechen und den grundlegenden Anforderungen in Anhang I Abschnitt 1 genügen.

2. Herstellung

2.1. Der Hersteller trifft alle erforderlichen Maßnahmen, damit die Konformität der hergestellten Produkte mit dem in der EU-Baumusterprüfbescheinigung beschriebenen zugelassenen Baumuster und den grundlegenden Anforderungen in Anhang I Abschnitt 1 durch die Herstellung und ihre Überwachung gewährleistet ist.

3. Konformitätskennzeichnung und Konformitätserklärung

3.1. Der Hersteller bringt an jedem einzelnen Produkt, das mit dem in der EU-Baumusterprüfbescheinigung beschriebenen Baumuster übereinstimmt und die geltenden Anforderungen der Rechtsvorschrift erfüllt, die CE-Kennzeichnung an.

3.2. Der Hersteller stellt für ein Produktmodell eine schriftliche Konformitätserklärung aus und hält sie zehn Jahre lang nach dem Inverkehrbringen des Produkts für die

nationalen Behörden bereit. Aus der Konformitätserklärung muss hervorgehen, für welches Produktmodell sie ausgestellt wurde. Ein Exemplar der Konformitätserklärung wird den zuständigen Behörden auf Verlangen zur Verfügung gestellt.

4. Bevollmächtigter

Die in Nummer 3 genannten Pflichten des Herstellers können von seinem Bevollmächtigten in seinem Auftrag und unter seiner Verantwortung erfüllt werden, falls sie im Auftrag festgelegt sind.

Konformität auf der Grundlage einer umfassenden Qualitätssicherung (auf der Grundlage von Modul H)

1. Bei der Konformität auf der Grundlage einer umfassenden Qualitätssicherung handelt es sich um das Konformitätsbewertungsverfahren, mit dem der Hersteller die in den Nummern 2 und 5 genannten Pflichten erfüllt sowie gewährleistet und auf eigene Verantwortung erklärt, dass die betreffenden Produkte (oder Produktkategorien) den grundlegenden Anforderungen in Anhang I Abschnitt 1 und die vom Hersteller festgelegten Verfahren zur Behandlung von Schwachstellen den grundlegenden Anforderungen in Anhang I Abschnitt 2 genügen.

2. Konzeption, Entwicklung, Herstellung und Behandlung von Schwachstellen bei Produkten mit digitalen Elementen

Der Hersteller betreibt ein zugelassenes Qualitätssicherungssystem nach Nummer 3 für die Konzeption, Entwicklung und Herstellung der betreffenden Produkte und für die Behandlung von Schwachstellen, erhält dessen Wirksamkeit während des gesamten Lebenszyklus der betreffenden Produkte und unterliegt der Überwachung nach Nummer 4.

3. Qualitätssicherungssystem

3.1. Der Hersteller beantragt bei einer notifizierten Stelle seiner Wahl die Bewertung seines Qualitätssicherungssystems für die betreffenden Produkte.

Der Antrag enthält

– den Namen und die Anschrift des Herstellers sowie, wenn der Antrag vom Bevollmächtigten eingereicht wird, auch dessen Namen und Anschrift;

– die technische Dokumentation jeweils für ein Modell jeder herzustellenden oder zu entwickelnden Produktkategorie; die technische Dokumentation enthält gegebenenfalls zumindest die in Anhang V aufgeführten Elemente;

– die Dokumentation zum Qualitätssicherungssystem;

– eine schriftliche Erklärung, dass derselbe Antrag bei keiner anderen notifizierten Stelle eingereicht worden ist.

3.2. Das Qualitätssicherungssystem gewährleistet die Konformität des Produkts mit den grundlegenden Anforderungen in Anhang I Abschnitt 1 und die Konformität der vom Hersteller festgelegten Verfahren zur Behandlung von Schwachstellen mit den grundlegenden Anforderungen in Anhang I Abschnitt 2.

Alle vom Hersteller berücksichtigten Grundlagen, Anforderungen und Vorschriften sind systematisch und ordnungsgemäß in Form schriftlicher Grundsätze, Verfahren und Anweisungen zusammenzustellen. Diese Unterlagen über das

Qualitätssicherungssystem gewährleisen, dass die Qualitätssicherungsprogramme, -pläne, -handbücher und qualitätsbezogene Aufzeichnungen einheitlich ausgelegt werden.

Sie enthalten insbesondere eine angemessene Beschreibung folgender Punkte:

– Qualitätsziele sowie organisatorischer Aufbau, Zuständigkeiten und Befugnisse des Managements in Bezug auf Konzeption, Entwicklung, Produktqualität und Behandlung von Schwachstellen;

– technische Spezifikationen für die Konzeption und Entwicklung, einschließlich der angewandten Normen, sowie bei nicht vollständiger Anwendung der einschlägigen harmonisierten Normen bzw. technischen Spezifikationen die Mittel, mit denen gewährleistet werden soll, dass die für die Produkte geltenden grundlegenden Anforderungen in Anhang I Abschnitt 1 erfüllt werden;

– verfahrenstechnische Spezifikationen, einschließlich der angewandten Normen, sowie bei nicht vollständiger Anwendung der einschlägigen harmonisierten Normen bzw. technischen Spezifikationen die Mittel, mit denen gewährleistet werden soll, dass die für die Verfahren geltenden grundlegenden Anforderungen in Anhang I Abschnitt 2 erfüllt werden;

– Techniken zur Steuerung der Konzeption und Entwicklung sowie Techniken zur Überprüfung der Konzeptions- und Entwicklungsergebnisse, Verfahren und systematische Maßnahmen, die bei der Konzeption und Entwicklung der zur betreffenden Produktkategorie gehörenden Produkte angewandt werden;

– entsprechende angewandte Techniken, Verfahren und systematische Maßnahmen für die Herstellung, Qualitätskontrolle und Qualitätssicherung;

– Prüfungen und Erprobungen, die vor, während und nach der Herstellung durchgeführt werden, sowie deren Häufigkeit;

– qualitätsbezogene Aufzeichnungen wie Kontrollberichte, Prüf- und Kalibrierungsdaten, Berichte über die Qualifikation der in diesem Bereich beschäftigten Mitarbeiter usw.;

– Mittel, mit denen die Verwirklichung der angestrebten Konzeptions- und Produktqualität und die wirksame Arbeitsweise des Qualitätssicherungssystems überwacht werden können.

3.3. Die notifizierte Stelle bewertet das Qualitätssicherungssystem, um festzustellen, ob es den Anforderungen nach Nummer 3.2 genügt.

Bei den Bestandteilen des Qualitätssicherungssystems, die den entsprechenden Spezifikationen der nationalen Norm zur Umsetzung der einschlägigen harmonisierten Norm und/oder einschlägigen technischen Spezifikationen entsprechen, geht sie von einer Konformität mit diesen Anforderungen aus.

Zusätzlich zur Erfahrung mit Qualitätsmanagementsystemen verfügt mindestens ein Mitglied des Auditteams über Erfahrungen mit der Bewertung in dem einschlägigen Bereich und der betreffenden Technologie des Produkts sowie über Kenntnisse der geltenden Anforderungen dieser Verordnung. Das Audit umfasst auch einen Kontrollbesuch in den Räumlichkeiten des Herstellers, falls es solche gibt. Das Auditteam überprüft die in Nummer 3.1 zweiter Gedankenstrich genannte technische

Dokumentation, um sich zu vergewissern, dass der Hersteller in der Lage ist, die anwendbaren Anforderungen dieser Verordnung zu erkennen und die erforderlichen Prüfungen durchzuführen, damit die Übereinstimmung des Produkts mit diesen Anforderungen gewährleistet ist.

Die Entscheidung wird dem Hersteller oder seinem Bevollmächtigten mitgeteilt.

Die Mitteilung enthält die Ergebnisse des Audits und die Begründung der Bewertungsentscheidung.

3.4. Der Hersteller verpflichtet sich, die mit dem zugelassenen Qualitätssicherungssystem verbundenen Pflichten zu erfüllen und dafür zu sorgen, dass das System stets sachgemäß und effizient angewandt wird.

3.5. Der Hersteller unterrichtet die notifizierte Stelle, die das Qualitätssicherungssystem zugelassen hat, über alle geplanten Änderungen des Qualitätssicherungssystems.

Die notifizierte Stelle prüft die geplanten Änderungen und entscheidet, ob das geänderte Qualitätssicherungssystem noch den in Nummer 3.2 genannten Anforderungen entspricht oder ob eine erneute Bewertung erforderlich ist.

Sie gibt dem Hersteller ihre Entscheidung bekannt. Die Mitteilung enthält die Ergebnisse der Prüfung und die Begründung der Bewertungsentscheidung.

4. Überwachung unter der Verantwortung der notifizierten Stelle

4.1. Die Überwachung soll gewährleisten, dass der Hersteller die mit dem zugelassenen Qualitätssicherungssystem verbundenen Pflichten vorschriftsmäßig erfüllt.

4.2. Der Hersteller gewährt der notifizierten Stelle zu Bewertungszwecken Zugang zu den Konzeptions-, Herstellungs-, Abnahme-, Prüf- und Lagereinrichtungen und stellt ihr alle erforderlichen Unterlagen zur Verfügung, insbesondere

– die Unterlagen über das Qualitätssicherungssystem,

– die im Qualitätssicherungssystem für den Konzeptionsteil vorgesehenen Qualitätsberichte wie Ergebnisse von Analysen, Berechnungen, Prüfungen usw.,

– die im Qualitätssicherungssystem für den Fertigungsbereich vorgesehenen qualitätsbezogenen Aufzeichnungen wie Inspektionsberichte, Testdaten, Eichdaten, Berichte über die Qualifikation der in diesem Bereich beschäftigten Mitarbeiter usw.

4.3. Die notifizierte Stelle führt regelmäßig Audits durch, um sicherzustellen, dass der Hersteller das Qualitätssicherungssystem aufrechterhält und anwendet, und übergibt ihm einen entsprechenden Prüfbericht.

5. Konformitätskennzeichnung und Konformitätserklärung

5.1. Der Hersteller bringt an jedem einzelnen Produkt, das den Anforderungen in Anhang I Abschnitt 1 dieser Verordnung genügt, die CE-Kennzeichnung und unter der Verantwortung der in Absatz 3.1 genannten notifizierten Stelle deren Kennnummer an.

5.2. Der Hersteller stellt für jedes Produktmodell eine schriftliche Konformitätserklärung aus und hält sie zehn Jahre lang nach dem Inverkehrbringen des Produkts für die nationalen Behörden bereit. Aus der Konformitätserklärung muss hervorgehen, für welches Produktmodell sie ausgestellt wurde.

Ein Exemplar der Konformitätserklärung wird den zuständigen Behörden auf Verlangen zur Verfügung gestellt.

6. Der Hersteller hält für einen Zeitraum von mindestens zehn Jahren nach dem Inverkehrbringen des Produkts folgende Unterlagen für die nationalen Behörden bereit:

   – die technische Dokumentation nach Nummer 3.1,

   – die Unterlagen über das Qualitätssicherungssystem nach Nummer 3.1,

   – die Änderung nach Nummer 3.5 in ihrer genehmigten Form,

   – die Entscheidungen und Berichte der notifizierten Stelle nach den Nummern 3.5, 4.3 und 4.4.

7. Jede notifizierte Stelle unterrichtet ihre notifizierenden Behörden über Zulassungen von Qualitätssicherungssystemen, die sie ausgestellt oder zurückgenommen hat, und übermittelt ihnen in regelmäßigen Abständen oder auf Verlangen eine Aufstellung aller Zulassungen von Qualitätssicherungssystemen, die sie verweigert, ausgesetzt oder auf andere Art eingeschränkt hat.

   Jede notifizierte Stelle unterrichtet die anderen notifizierten Stellen über Zulassungen von Qualitätssicherungssystemen, die sie verweigert, ausgesetzt oder zurückgenommen hat, und auf Verlangen über Zulassungen von Qualitätssicherungssystemen, die sie erteilt hat.

8. Bevollmächtigter

   Die unter den Nummern 3.1, 3.5, 5 und 6 genannten Pflichten des Herstellers können von seinem Bevollmächtigten in seinem Auftrag und unter seiner Verantwortung erfüllt werden, falls sie im Auftrag festgelegt sind.