Amtsblatt
der Europäischen Union

DE
Reihe L

2024/2847

20.11.2024

VERORDNUNG (EU) 2024/2847 DES EUROPÄISCHEN PARLAMENTS UND DES RATES

vom 23. Oktober 2024

über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen und zur Änderung der Verordnungen (EU) Nr. 168/2013 und (EU) 2019/1020 und der Richtlinie (EU) 2020/1828 (Cyberresilienz-Verordnung)

(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 Anhörung des Ausschusses der Regionen,

gemäß dem ordentlichen Gesetzgebungsverfahren [2],

in Erwägung nachstehender Gründe:

(1) Die Cybersicherheit bedeutet eine der größten Herausforderungen für die Union. Die Zahl und Vielfalt der vernetzten Geräte wird in den kommenden Jahren exponentiell zunehmen. Cyberangriffe sind ein Thema von öffentlichem Interesse, da sie sich nicht nur auf die Wirtschaft der Union, sondern auch auf die Demokratie sowie die Sicherheit und Gesundheit der Verbraucher kritisch auswirken. Es ist deshalb nötig, das Cybersicherheitskonzept der Union zu stärken, sich mit Cyberresilienz auf Unionsebene zu befassen und 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 zeigt, 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 den Verkehr gebracht werden und damit sich die Hersteller während des gesamten Lebenszyklus eines Produkts konsequent 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, beispielsweise durch mehr Transparenz in Bezug auf den Unterstützungszeitraum für auf dem Markt bereitgestellte Produkte mit digitalen Elementen.

(3) Das geltende einschlägige Unionsrecht umfasst mehrere horizontale Vorschriften, die bestimmte Aspekte der Cybersicherheit aus unterschiedlichen Blickwinkeln regeln, darunter auch Maßnahmen zur Erhöhung der Sicherheit der digitalen Lieferkette. Das bestehende Unionsrecht in Bezug auf die Cybersicherheit, wozu die Verordnung (EU) 2019/881 des Europäischen Parlaments und des Rates [3] und die Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates [4] gehören, enthält jedoch keine unmittelbar verbindlichen Anforderungen an die Sicherheit von Produkten mit digitalen Elementen.

---

[1] ABl. C 100 vom 16.3.2023, S. 101.

[2] Standpunkt des Europäischen Parlaments vom 12. März 2024 (noch nicht im Amtsblatt veröffentlicht) und Beschluss des Rates vom 10. Oktober 2024.

[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] Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS-2-Richtlinie) (ABl. L 333 vom 27.12.2022, S. 80).

(4) Das bestehenden Unionsrecht gilt 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 und Organisationen führt, die eine Reihe verschiedener Anforderungen und Pflichten in Bezug auf ähnliche Produktarten zu erfüllen haben. Die Cybersicherheit dieser Produkte hat eine besonders ausgeprägte grenzüberschreitende Dimension, weil die in einem Mitgliedstaat oder in einem Drittland hergestellten Produkte mit digitalen Elementen häufig von Organisationen und Verbrauchern im gesamten Binnenmarkt verwendet werden. Dies macht es notwendig, den Bereich auf Unionsebene zu regulieren, um für einen harmonisierten Rechtsrahmen und Rechtssicherheit für Nutzer, Organisationen und Unternehmen, einschließlich Kleinstunternehmen und kleinen und mittleren Unternehmen im Sinne des Anhangs der Empfehlung 2003/361/EG der Kommission ([5]), zu sorgen. Das Regulierungsumfeld der Union sollte durch die Einführung von horizontalen Cybersicherheitsanforderungen für Produkte mit digitalen Elementen harmonisiert werden. Überdies gilt es, in der gesamten Union Rechtssicherheit für die Wirtschaftsakteure und Nutzer und eine bessere Harmonisierung des Binnenmarkts sowie Verhältnismäßigkeit für Kleinstunternehmen sowie kleine und mittlere Unternehmen zu gewährleisten, wodurch auch bessere Bedingungen für Wirtschaftsakteure geschaffen würden, die in diesen Markt eintreten wollen.

(5) Was Kleinstunternehmen sowie kleine und mittlere Unternehmen betrifft, so sollten bei der Bestimmung der Kategorie, in die ein Unternehmen fällt, die Bestimmungen des Anhangs der Empfehlung 2003/361/EG in vollem Umfang angewandt werden. Daher sollten bei der Berechnung der Mitarbeiterzahl und der finanziellen Schwellenwerte zur Bestimmung der Unternehmenstypen auch die Bestimmungen von Artikel 6 des Anhangs der Empfehlung 2003/361/EG über die Erstellung der Daten eines Unternehmens im Hinblick auf bestimmte Arten von Unternehmen wie Partnerunternehmen oder verbundene Unternehmen angewandt werden.

(6) Die Kommission sollte Leitlinien bereitstellen, um die Wirtschaftsakteure, insbesondere Kleinstunternehmen sowie kleine und mittlere Unternehmen, bei der Anwendung dieser Verordnung zu unterstützen. Diese Leitlinien sollten unter anderem den Anwendungsbereich dieser Verordnung, insbesondere die Datenfernverarbeitung und ihre Auswirkungen auf die Entwickler freier und quelloffener Software, die Anwendung der Kriterien zur Festlegung von Unterstützungszeiträumen für Produkte mit digitalen Elementen, das Zusammenspiel dieser Verordnung und anderer Rechtsvorschriften der Union und die Frage, was den Begriff der wesentlichen Änderung darstellt, abdecken.

(7) Auf Unionsebene wurden in verschiedenen programmatischen und politischen Papieren wie der gemeinsamen Mitteilung der Kommission und des Hohen Vertreters der Union für Außen- und Sicherheitspolitik vom 16. Dezember 2020 mit dem Titel „Die Cybersicherheitsstrategie der EU für die digitale Dekade“, den Schlussfolgerungen des Rates zur Cybersicherheit vernetzter Geräte vom 2. Dezember 2020 und den Schlussfolgerungen des Rates zur Entwicklung der Cyberabwehr der Europäischen Union vom 23. Mai 2022 und der Entschließung des Europäischen Parlaments vom 10. Juni 2021 zu der Cybersicherheitsstrategie der EU für die digitale Dekade ([6]) besondere Cybersicherheitsanforderungen der Union für digitale oder vernetzte Produkte verlangt; gleichzeitig haben mehrere Drittländer Maßnahmen ergriffen, um dieses Problem auf eigene Initiative anzugehen. Im Abschlussbericht der Konferenz zur Zukunft Europas forderten die Bürgerinnen und Bürger „eine stärkere Rolle der EU bei der Abwehr von Cybersicherheitsbedrohungen“. Damit die Union international eine führende Rolle im Bereich der Cybersicherheit einnehmen kann, ist es wichtig, einen ambitionierten Rechtsrahmen zu schaffen.

(8) Um das Gesamtniveau der Cybersicherheit aller im Binnenmarkt in den Verkehr gebrachten Produkte mit digitalen Elementen zu erhöhen, müssen für diese Produkte objektive und technologieneutrale grundlegende Cybersicherheitsanforderungen eingeführt werden, die dann horizontal gelten sollen.

(9) 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 eine erste Kompromittierung eines Geräts oder Netzes erleichtern und es böswilligen Akteuren ermöglichen, sich privilegierten Zugriff auf einem System zu verschaffen oder sich systemübergreifend zu bewegen. Die Hersteller sollten daher dafür sorgen, dass alle Produkte mit digitalen Elementen im Einklang mit den in dieser Verordnung festgelegten grundlegenden Cybersicherheitsanforderungen konzipiert und entwickelt werden. Die Pflicht bezieht sich sowohl auf Produkte, die physisch über Hardware-Schnittstellen verbunden werden können, als auch auf Produkte, die logisch verbunden werden, z. B. über Netzwerksockets, Pipes, Dateien, Anwendungsprogrammierschnittstellen oder andere Arten von Software-Schnittstellen. Da sich Cyberbedrohungen 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 mit digitalen Elementen sicherstellen, die nur indirekt mit anderen Geräten oder Netzen verbunden sind.

([5]) Empfehlung der Kommission 2003/361/EG vom 6. Mai 2003 betreffend die Definition der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen (ABl. L 124 vom 20.5.2003, S. 36).

([6]) ABl. C 67 vom 8.2.2022, S. 81.

(10) Mit der Festlegung von Cybersicherheitsanforderungen für das Inverkehrbringen von Produkten mit digitalen Elementen soll die Cybersicherheit dieser Produkte sowohl für Verbraucher als auch für Unternehmen verbessert werden. Durch diese Anforderungen wird auch sichergestellt, dass die Cybersicherheit in der gesamten Lieferkette berücksichtigt wird, sodass Endprodukte mit digitalen Elementen und ihre Komponenten sicherer gemacht werden. Dies betrifft auch Anforderungen für das Inverkehrbringen von Verbraucherprodukten mit digitalen Elementen, die für schutzbedürftige Verbraucher bestimmt sind, wie z. B. Spielzeug und Babyphone-Systeme. Die Verbraucherprodukte mit digitalen Elementen, die in dieser Verordnung als wichtige Produkte mit digitalen Elementen eingestuft werden, sind mit einem höheren Cybersicherheitsrisiko behaftet, da ihre Funktionen ein erhebliches Risiko nachteiliger Auswirkungen in Bezug auf ihre Tragweite und ihre mögliche Beeinträchtigung der Gesundheit, Sicherheit oder Unversehrtheit der Nutzer solcher Produkte bergen, und sollten einem strengeren Konformitätsbewertungsverfahren unterzogen werden. Das gilt für Produkte wie intelligente Haushaltsgeräte mit Sicherheitsfunktionen, einschließlich intelligenter Türschlösser, Babyphone-Systemen und Alarmanlagen, vernetztes Spielzeug und am Körper tragbare medizinische Geräte (Wearables). Darüber hinaus werden die strengeren Konformitätsbewertungsverfahren, denen sonstige Produkte mit digitalen Elementen, die in dieser Verordnung als wichtige oder kritische Produkte mit digitalen Elementen eingestuft werden, unterzogen werden müssen, dazu beitragen, etwaige negative Auswirkungen auf die Verbraucher zu verhindern, die sich aus der Ausnutzung von Schwachstellen ergeben könnten.

(11) Mit dieser Verordnung soll ein hohes Niveau an Cybersicherheit von Produkten mit digitalen Elementen und ihren integrierten Datenfernverarbeitungslösungen sichergestellt werden. Solche Datenfernverarbeitungslösungen sollten als entfernt stattfindende Datenverarbeitung definiert werden, für die eine Software vom Hersteller des Produkts mit digitalen Elementen selbst oder unter dessen Verantwortung konzipiert und entwickelt wird und ohne die das Produkt mit digitalen Elementen eine seiner Funktionen nicht erfüllen könnte. Damit wird sichergestellt, dass solche Produkte in ihrer Gesamtheit von ihren Herstellern angemessen gesichert werden, unabhängig davon, ob die Daten lokal auf dem Gerät des Nutzers oder aus der Ferne durch den Hersteller verarbeitet oder gespeichert werden. Gleichzeitig fällt die Fernverarbeitung oder -speicherung nur insoweit in den Anwendungsbereich dieser Verordnung, als sie notwendig ist, damit ein Produkt mit digitalen Elementen seine Funktionen erfüllen kann. Eine solche Fernverarbeitung oder -speicherung liegt vor, wenn eine mobile Anwendung den Zugang zu einer Anwendungsprogrammierschnittstelle oder zu einer Datenbank erfordert, die über einen vom Hersteller entwickelten Dienst bereitgestellt wird. In diesem Fall fällt der Dienst als Datenfernverarbeitungslösung in den Anwendungsbereich dieser Verordnung. Die Anforderungen an Datenfernverarbeitungslösungen, die in den Anwendungsbereich dieser Verordnung fallen, beinhalten daher keine technischen, betrieblichen oder organisatorischen Maßnahmen zur Beherrschung der Risiken für die Sicherheit der Netz- und Informationssysteme des Herstellers insgesamt.

(12) Cloud-Lösungen gelten nur dann als Datenfernverarbeitungslösungen im Sinne dieser Verordnung, wenn sie der in dieser Verordnung festgelegten Begriffsbestimmung entsprechen. So fallen beispielsweise vom Hersteller von intelligenten Haushaltsgeräten angebotene Cloud-Funktionen, die es den Nutzern ermöglichen, das Gerät aus der Ferne zu steuern, in den Anwendungsbereich dieser Verordnung. Dagegen fallen Websites, die die Funktionalität eines Produkts mit digitalen Elementen nicht unterstützen, oder Cloud-Dienste, die außerhalb der Verantwortung eines Herstellers eines Produkts mit digitalen Elementen entworfen und entwickelt wurden, nicht in den Anwendungsbereich dieser Verordnung. Die Richtlinie (EU) 2022/2555 gilt für Cloud-Computing-Dienste und Cloud-Dienstmodelle wie SaaS (Software as a Service), PaaS (Platform as a Service) oder IaaS (Infrastructure as a Service). Die Einrichtungen, die Cloud-Computing-Dienste in der Union erbringen und die gemäß Artikel 2 des Anhangs der Empfehlung 2003/361/EG als mittlere Unternehmen gelten oder die Schwellenwerte für mittlere Unternehmen gemäß Absatz 1 jenes Artikels überschreiten, fallen in den Anwendungsbereich der genannten Richtlinie.

(13) Im Einklang mit dem Ziel dieser Verordnung, Hindernisse für den freien Verkehr von Produkten mit digitalen Elementen auszuräumen, sollten die Mitgliedstaaten in den von dieser Verordnung erfassten Aspekten nicht die Bereitstellung auf dem Markt von Produkten mit digitalen Elementen, die dieser Verordnung entsprechen, behindern. In den durch diese Verordnung harmonisierten Bereichen können die Mitgliedstaaten daher keine zusätzlichen Cybersicherheitsanforderungen für die Bereitstellung von Produkten mit digitalen Elementen auf dem Markt vorschreiben. Jede öffentliche oder private Einrichtung kann jedoch über die in dieser Verordnung festgelegten Anforderungen hinaus zusätzliche Anforderungen für die Beschaffung oder Verwendung von Produkten mit digitalen Elementen für ihre spezifischen Zwecke festlegen und sich daher für die Verwendung von Produkten mit digitalen Elementen entscheiden, die strengere oder spezifischere Cybersicherheitsanforderungen erfüllen als die, die für die Bereitstellung auf dem Markt gemäß dieser Verordnung gelten. Unbeschadet der Richtlinien 2014/24/EU ([7]) und 2014/25/EU ([8]) des Europäischen Parlaments und des Rates sollten die Mitgliedstaaten bei der Beschaffung von Produkten mit digitalen Elementen, die den in dieser Verordnung festgelegten grundlegenden Cybersicherheitsan-

([7]) Richtlinie 2014/24/EU des Europäischen Parlaments und des Rates vom 26. Februar 2014 über die öffentliche Auftragsvergabe und zur Aufhebung der Richtlinie 2004/18/EG (ABl. L 94 vom 28.3.2014, S. 65).

([8]) Richtlinie 2014/25/EU des Europäischen Parlaments und des Rates vom 26. Februar 2014 über die Vergabe von Aufträgen durch Auftraggeber im Bereich der Wasser-, Energie- und Verkehrsversorgung sowie der Postdienste und zur Aufhebung der Richtlinie 2004/17/EG (ABl. L 94 vom 28.3.2014, S. 243).

forderungen, einschließlich jener für den Umgang mit Sicherheitsrisiken, entsprechen müssen, sicherstellen, dass diese Anforderungen im Beschaffungsprozess berücksichtigt werden und auch die Fähigkeit der Hersteller zur wirksamen Anwendung von Cybersicherheitsmaßnahmen und zur Bewältigung von Cyberbedrohungen betrachtet wird. Darüber hinaus sind in der Richtlinie (EU) 2022/2555 Risikomanagementmaßnahmen im Bereich der Cybersicherheit für die wesentlichen und wichtigen Einrichtungen im Sinne von Artikel 3 der genannten Richtlinie festgelegt, die Maßnahmen zur Sicherheit der Lieferkette umfassen könnten, die erfordern, dass diese Einrichtungen Produkte mit digitalen Elementen verwenden, die strengeren als den in dieser Verordnung festgelegten Cybersicherheitsanforderungen genügen. Gemäß der Richtlinie (EU) 2022/2555 und ihrem Grundsatz der Mindestharmonisierung können die Mitgliedstaaten daher zusätzliche Cybersicherheitsanforderungen für die Verwendung von Produkten der Informations- und Kommunikationstechnologie (IKT-Produkte) durch wesentliche oder wichtige Einrichtungen gemäß der genannten Richtlinie festlegen, um für ein höheres Cybersicherheitsniveau zu sorgen, sofern diese Anforderungen mit den im Unionsrecht festgelegten Verpflichtungen der Mitgliedstaaten im Einklang stehen. Zu den von dieser Verordnung nicht erfassten Aspekten können auch nichttechnische Faktoren im Zusammenhang mit Produkten mit digitalen Elementen und deren Herstellern gehören. Die Mitgliedstaaten können daher nationale Maßnahmen festlegen, einschließlich Beschränkungen für Produkte mit digitalen Elementen oder für Anbieter solcher Produkte, die nichttechnischen Faktoren Rechnung tragen. Die nationalen Maßnahmen in Bezug auf solche Faktoren müssen mit dem Unionsrecht vereinbar sein.

(14) Diese Verordnung sollte im Einklang mit dem Unionsrecht die Verantwortung der Mitgliedstaaten für die Gewährleistung der nationalen Sicherheit unberührt lassen. Die Mitgliedstaaten sollten Produkte mit digitalen Elementen, die für Zwecke der nationalen Sicherheit oder Verteidigung beschafft oder verwendet werden, zusätzlichen Vorgaben unterwerfen können, sofern diese Vorgaben mit den im Unionsrecht festgelegten Verpflichtungen der Mitgliedstaaten im Einklang stehen.

(15) Diese Verordnung gilt für Wirtschaftsakteure nur in Bezug auf Produkte mit digitalen Elementen, die auf dem Markt bereitgestellt werden, d. h., die im Rahmen einer Geschäftstätigkeit zum Vertrieb oder zur Verwendung auf dem Unionsmarkt geliefert werden. Eine Lieferung im Zusammenhang mit einer Geschäftstätigkeit ist möglicherweise nicht nur dadurch gekennzeichnet, dass für ein Produkt mit digitalen Elementen ein Preis verlangt wird, sondern auch dadurch, dass für technische Unterstützungsleistungen ein Entgelt verlangt wird, das nicht nur der Deckung der tatsächlichen Kosten dient, dass eine Gewinnerzielungsabsicht besteht, beispielsweise durch Bereitstellung einer Softwareplattform, über die der Hersteller andere Dienste gewinnorientiert anbietet, oder dass als Bedingung für die Nutzung die Verarbeitung personenbezogener Daten zu anderen Zwecken als der alleinigen Verbesserung der Sicherheit, Kompatibilität oder Interoperabilität der Software verlangt wird oder dass Spenden angenommen werden, die die mit der Konzeption, Entwicklung und Bereitstellung eines Produkts mit digitalen Elementen verbundenen Kosten übersteigen. Die Annahme von Spenden ohne Gewinnabsicht sollte nicht als Geschäftstätigkeit gelten.

(16) Produkte mit digitalen Elementen, die im Rahmen der Erbringung einer Dienstleistung bereitgestellt werden, für die eine Gebühr ausschließlich zur Deckung der tatsächlichen Kosten erhoben wird, die in unmittelbarem Zusammenhang mit dem Betrieb dieses Dienstes stehen, wie dies bei bestimmten Produkten mit digitalen Elementen der Fall sein kann, die von Einrichtungen der öffentlichen Verwaltung bereitgestellt werden, sollten nicht allein aus diesen Gründen als Bestandteil einer Geschäftstätigkeit im Sinne dieser Verordnung angesehen werden. Darüber hinaus sollten Produkte mit digitalen Elementen, die von einer öffentlichen Verwaltungseinrichtung ausschließlich für ihren Eigenbedarf entwickelt oder geändert werden, nicht als auf dem Markt bereitgestellt im Sinne dieser Verordnung gelten.

(17) Software und Daten, die offen geteilt werden und die Nutzer frei abrufen, nutzen, verändern und weiter verteilen können, auch in veränderter Form, können zu Forschung und Innovation auf dem Markt beitragen. Zur Förderung der Entwicklung und des Einsatzes von freier und quelloffener Software, insbesondere durch Kleinstunternehmen sowie kleine und mittlere Unternehmen, einschließlich Start-up-Unternehmen, Einzelpersonen, gemeinnützige Organisationen und akademische Forschungseinrichtungen, sollte bei der Anwendung dieser Verordnung auf Produkte mit digitalen Elementen, die als freie und quelloffene Software eingestuft und zum Vertrieb oder zur Nutzung im Rahmen einer Geschäftstätigkeit bereitgestellt werden, die Arten der verschiedenen Entwicklungsmodelle für Software berücksichtigt werden, die im Rahmen von Lizenzen für freie und quelloffene Software vertrieben und entwickelt wird.

(18) Unter freier und quelloffener Software ist eine Software zu verstehen, deren Quellcode offen geteilt wird und in deren Lizenz alle erforderlichen Rechte vorgesehen sind, um sie frei zugänglich, nutzbar, veränderbar und weiterverteilbar zu machen. Freie und quelloffene Software wird offen entwickelt, gepflegt und verteilt, auch über Online-Plattformen. In Bezug auf Wirtschaftsakteure, die in den Anwendungsbereich dieser Verordnung fallen, sollte nur freie und quelloffene Software, die auf dem Markt bereitgestellt und somit zum Vertrieb oder zur Nutzung im Rahmen einer Geschäftstätigkeit verfügbar gemacht wird, in den Anwendungsbereich dieser Verordnung fallen. Die bloßen Umstände, unter denen das Produkt mit digitalen Elementen entwickelt wurde, oder die Art und Weise, wie die Entwicklung finanziert wurde, sollten daher bei der Bestimmung des kommerziellen oder nichtkommerziellen Charakters der entsprechenden Tätigkeit nicht berücksichtigt werden. Insbesondere sollte für die Zwecke dieser Verordnung und in Bezug auf die Wirtschaftsakteure, die in ihren Anwendungsbereich fallen, die Bereitstellung von Produkten mit digitalen Elementen, die als freie und quelloffene Software eingestuft und von ihren Herstellern nicht

zu Geld gemacht werden, nicht als Geschäftstätigkeit betrachtet werden, damit sichergestellt ist, dass klar zwischen der Entwicklungs- und der Lieferphase unterschieden wird. Darüber hinaus sollte die Lieferung von Produkten mit digitalen Elementen, die als freie und quelloffene Softwarekomponenten eingestuft werden und zur Integration durch andere Hersteller in ihre eigenen Produkte mit digitalen Elementen bestimmt sind, nur dann als Bereitstellung auf dem Markt betrachtet werden, wenn die Komponente von ihrem ursprünglichen Hersteller zu Geld gemacht wird. Beispielsweise sollte allein der Umstand, dass ein Produkt quelloffener Software mit digitalen Elementen von den Herstellern finanziell unterstützt wird oder dass Hersteller zur Entwicklung eines solchen Produkts beitragen, für sich genommen nicht ausschlaggebend für die Feststellung sein, dass die Tätigkeit kommerzieller Art ist. Fernerhin sollte das bloße Vorhandensein regelmäßiger Veröffentlichungen von Versionen für sich genommen nicht zu der Schlussfolgerung führen, dass ein Produkt mit digitalen Elementen im Rahmen einer Geschäftstätigkeit geliefert wird. Schließlich sollte für die Zwecke dieser Verordnung die Entwicklung von Produkten mit digitalen Elementen, die als freie und quelloffene Software eingestuft werden, durch gemeinnützige Organisationen nicht als kommerzielle Tätigkeit betrachtet werden, sofern die Organisation so angelegt ist, dass sichergestellt ist, dass alle Einnahmen nach Abzug der Kosten zur Verwirklichung gemeinnütziger Ziele verwendet werden. Diese Verordnung gilt nicht für natürliche oder juristische Personen, die mit Quellcode zu Produkten mit digitalen Elementen beitragen, die als freie und quelloffene Software eingestuft sind und nicht ihrer Verantwortung unterliegen.

(19) Angesichts der Bedeutung für die Cybersicherheit, die vielen Produkten mit digitalen Elementen zukommt, die als freie und quelloffene Software eingestuft sind und im Sinne dieser Verordnung veröffentlicht, aber nicht auf dem Markt bereitgestellt werden, sollten juristische Personen, die die Entwicklung solcher für kommerzielle Tätigkeiten bestimmte Produkte dauerhaft unterstützen und eine wichtige Rolle bei der Sicherstellung der Brauchbarkeit dieser Produkte spielen (Verwalter quelloffener Software), einer vereinfachten und maßgeschneiderten Regulierungsregelung unterworfen werden. Zu den Verwaltern quelloffener Software gehören bestimmte Stiftungen sowie Einrichtungen, die freie und quelloffene Software im wirtschaftlichen Kontext entwickeln und veröffentlichen, einschließlich gemeinnütziger Einrichtungen. Bei der Regulierung sollten ihre Besonderheiten und die Vereinbarkeit mit der Art der auferlegten Verpflichtungen berücksichtigt werden. Es sollten nur Produkte mit digitalen Elementen abgedeckt sein, die als freie und quelloffene Software gelten und letztlich für kommerzielle Tätigkeiten wie die Integration in kommerzielle Dienste oder kostenpflichtige Produkte mit digitalen Elementen bestimmt sind. Für die Zwecke dieser Regulierungsregelung umfasst die beabsichtigte Integration in kostenpflichtige Produkte mit digitalen Elementen Fälle, in denen die Hersteller, die eine Komponente in ihre eigenen Produkte mit digitalen Elementen integrieren, entweder regelmäßig zur Entwicklung dieser Komponente beitragen oder regelmäßige finanzielle Unterstützung leisten, um die Kontinuität eines Softwareprodukts sicherzustellen. Die dauerhafte Unterstützung der Entwicklung eines Produkts mit digitalen Elementen umfasst unter anderem das Hosting und die Verwaltung von Plattformen für die Zusammenarbeit bei der Softwareentwicklung, das Hosting von Quellcode oder Software, das Verwalten oder Administrieren von Produkten mit digitalen Elementen, die als freie und quelloffene Software eingestuft sind, sowie die Steuerung der Entwicklung solcher Produkte. Da in der vereinfachten und maßgeschneiderten Regulierungsregelung für Verwalter quelloffener Software nicht dieselben Verpflichtungen wie für Hersteller im Rahmen dieser Verordnung vorgesehen sind, sollte es ihnen nicht gestattet sein, die CE-Kennzeichnung auf Produkten mit digitalen Elementen, deren Entwicklung sie unterstützen, anzubringen.

(20) Die bloße Bereitstellung von Produkten mit digitalen Elementen in offenen Archiven, darunter über Paketverwaltung oder auf Plattformen für die Zusammenarbeit, stellt an sich noch keine Bereitstellung eines Produkts mit digitalen Elementen auf dem Markt dar. Die Anbieter solcher Dienste sollten nur dann als Händler betrachtet werden, wenn sie diese Software auf dem Markt bereitstellen und sie somit im Rahmen einer Geschäftstätigkeit zum Vertrieb oder zur Verwendung auf dem Unionsmarkt liefern.

(21) Zur Unterstützung und Erleichterung der Sorgfaltspflicht von Herstellern, die freie und quelloffene Softwarekomponenten, die nicht den in dieser Verordnung festgelegten grundlegenden Cybersicherheitsanforderungen unterliegen, in ihre Produkte mit digitalen Elementen integrieren, sollte die Kommission die Möglichkeit haben, freiwillige Sicherheitsbescheinigungsprogramme einzurichten, entweder durch einen delegierten Rechtsakt zur Ergänzung dieser Verordnung oder durch das Anfordern eines europäischen Schemas für die Cybersicherheitszertifizierung gemäß Artikel 48 der Verordnung (EU) 2019/881, das den Besonderheiten der Modelle für die Entwicklung freier und quelloffener Software Rechnung trägt. Die Sicherheitsbescheinigungsprogramme sollten so konzipiert sein, dass nicht nur natürliche oder juristische Personen, die ein Produkt mit digitalen Elementen, die als freie und quelloffene Software eingestuft sind, entwickeln oder dazu beitragen, eine Sicherheitsbescheinigung initiieren oder finanzieren können, sondern auch Dritte, wie Hersteller, die solche Produkte mit digitalen Elementen in ihre eigenen Produkte mit digitalen Elementen integrieren, sowie Nutzer oder öffentliche Verwaltungen der Union und der Mitgliedstaaten.

(22) Im Hinblick auf die Ziele dieser Verordnung im Bereich der öffentlichen Cybersicherheit und zur Verbesserung des Lagebewusstseins der Mitgliedstaaten hinsichtlich der Abhängigkeit der Union von Softwarekomponenten und insbesondere von potenziell freien und quelloffenen Softwarekomponenten sollte eine mit dieser Verordnung eingesetzte besondere Gruppe zur administrativen Zusammenarbeit (ADCO) beschließen können, gemeinsam eine Abhängigkeitsbewertung der Union durchzuführen. Die Marktüberwachungsbehörden sollten Hersteller von Produkten mit digitalen Elementen, die in die von der ADCO aufgestellten Kategorien fallen, auffordern können, die Software-Stücklisten vorzulegen, die sie gemäß dieser Verordnung erstellt haben. Um die Vertraulichkeit der Software-Stücklisten zu schützen, sollten die Marktüberwachungsbehörden der ADCO relevante Informationen über Abhängigkeiten in anonymisierter und aggregierter Form übermitteln.

(23) Die Wirksamkeit der Durchführung dieser Verordnung wird auch davon abhängen, ob angemessene Kompetenzen im Bereich der Cybersicherheit verfügbar sind. Auf Unionsebene wurde in verschiedenen programmatischen und politischen Dokumenten, darunter in der Mitteilung der Kommission vom 18. April 2023 mit dem Titel „Schließung der Fachkräftelücke im Cybersicherheitsbereich zur Förderung der Wettbewerbsfähigkeit, des Wachstums und der Resilienz in der EU“ und in den Schlussfolgerungen des Rates vom 22. Mai 2023 zur Cyberabwehrpolitik der EU, eingeräumt, dass in der Union ein Qualifikationsdefizit im Bereich der Cybersicherheit besteht und die entsprechende Problematik sowohl im öffentlichen als auch im privaten Sektor vorrangig angegangen werden muss.. Um eine wirksame Durchführung dieser Verordnung sicherzustellen, sollten die Mitgliedstaaten dafür Sorge tragen, dass ausreichende Ressourcen für eine adäquate Personalausstattung der Marktüberwachungsbehörden und Konformitätsbewertungsstellen zur Verfügung stehen, damit diese ihre in dieser Verordnung festgelegten Aufgaben erfüllen können. Im Rahmen dieser Maßnahmen sollten die Mobilität der Arbeitskräfte im Bereich der Cybersicherheit und die damit verbundenen Karrierewege verbessert werden. Die Maßnahmen sollten auch dazu beitragen, die Beschäftigten im Bereich der Cybersicherheit resilienter und inklusiver zu machen, auch im Hinblick auf die Gleichstellung der Geschlechter. Die Mitgliedstaaten sollten daher Vorkehrungen treffen, damit die entsprechenden Aufgaben von angemessen ausgebildeten Fachkräften mit den erforderlichen Cybersicherheitskompetenzen wahrgenommen werden. Ebenso sollten die Hersteller sicherstellen, dass ihr Personal über die erforderlichen Fähigkeiten verfügt, um ihren in dieser Verordnung festgelegten Verpflichtungen nachzukommen. Die Mitgliedstaaten und die Kommission sollten im Einklang mit ihren Vorrechten und Zuständigkeiten und den ihnen durch diese Verordnung übertragenen besonderen Aufgaben Maßnahmen ergreifen, um Hersteller, insbesondere Kleinstunternehmen sowie kleine und mittlere Unternehmen, einschließlich Start-up-Unternehmen, auch in Bereichen wie dem Aufbau von Kompetenzen, zu unterstützen, damit sie ihren Verpflichtungen aus dieser Verordnung nachkommen können. Da die Mitgliedstaaten gemäß der Richtlinie (EU) 2022/2555 verpflichtet sind, im Rahmen ihrer nationalen Cybersicherheitsstrategien Maßnahmen zur Förderung und Entwicklung von Schulungen im Bereich der Cybersicherheit und der Cybersicherheitskompetenzen zu ergreifen, können die Mitgliedstaaten bei der Verabschiedung solcher Strategien auch erwägen, den sich aus dieser Verordnung ergebenden Bedarf an Cybersicherheitskompetenzen zu decken, einschließlich des Bedarfs an Umschulung und Weiterqualifizierung.

(24) Ein sicheres Internet ist für das Funktionieren kritischer Infrastrukturen und für die Gesellschaft insgesamt unverzichtbar. Die Richtlinie (EU) 2022/2555 zielt darauf ab, für ein hohes Maß an Cybersicherheit der Dienste der in Artikel 3 jener Richtlinie genannten wesentlichen und wichtigen Einrichtungen, zu denen auch die Betreiber digitaler Infrastrukturen zählen, zu sorgen, die Kernfunktionen des offenen Internets unterstützen und den Internetzugang und Internetdienste sicherzustellen. Deshalb ist es wichtig, dass die Produkte mit digitalen Elementen, die erforderlich sind, damit die Betreiber digitaler Infrastrukturen das Funktionieren des Internets sicherstellen können, auf sichere Weise entwickelt werden und dass sie den etablierten Internetsicherheitsnormen 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 (EU) 2022/2555 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.

(25) Die Verordnung (EU) 2017/745 des Europäischen Parlaments und des Rates [9] enthält Vorschriften für Medizinprodukte und die Verordnung (EU) 2017/746 des Europäischen Parlaments und des Rates [10] enthält Vorschriften für In-vitro-Diagnostika. Diese 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 gemäß Anhang I dieser Verordnungen in Bezug auf die Cybersicherheit an die Hand geben. Produkte mit digitalen Elementen, die unter eine dieser Verordnungen fallen, sollten daher nicht von der vorliegenden Verordnung erfasst werden.

(26) Produkte mit digitalen Elementen, die ausschließlich für Zwecke der nationalen Sicherheit oder für Verteidigungszwecke entwickelt oder verändert werden, oder Produkte, die speziell für die Verarbeitung von Verschlusssachen konzipiert sind, fallen nicht in den Anwendungsbereich dieser Verordnung. Die Mitgliedstaaten sind aufgefordert, mit Blick auf diese Produkte für das gleiche oder ein höheres Schutzniveau als für die Produkte zu sorgen, die in den Anwendungsbereich dieser Verordnung fallen.

---

[9] 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).

[10] 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).

(27) Mit der Verordnung (EU) 2019/2144 des Europäischen Parlaments und des Rates ([11]) 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, insbesondere die UN-Regelung Nr. 155 — Einheitliche Bedingungen für die Genehmigung von Fahrzeugen hinsichtlich der Cybersicherheit und des Cybersicherheitsmanagementsystems ([12]), umfassen und spezifische Konformitätsbewertungsverfahren vorsehen. Im Bereich der Luftfahrt besteht das Hauptziel der Verordnung (EU) 2018/1139 des Europäischen Parlaments und des Rates ([13]) 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 Pflichten zum Schutz vor Bedrohungen der Informationssicherheit umfasst. Mit dem Zertifizierungsverfahren nach der Verordnung (EU) 2018/1139 wird die mit der vorliegenden Verordnung angestrebte Vertrauenswürdigkeit sichergestellt. Produkte mit digitalen Elementen, die unter die Verordnung (EU) 2019/2144 fallen, und Produkte, die nach der Verordnung (EU) 2018/1139 zertifiziert worden sind, sollten daher nicht den in der vorliegenden Verordnung festgelegten grundlegenden Cybersicherheitsanforderungen und Konformitätsbewertungsverfahren unterliegen.

(28) In dieser Verordnung werden horizontale Cybersicherheitsvorschriften festgelegt, die nicht speziell für bestimmte Branchen oder bestimmte Produkte mit digitalen Elementen gelten sollen. Dennoch könnten branchen- 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 Cybersicherheitsanforderungen 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 Cybersicherheitsanforderungen dieser Verordnung abgedeckten Risiken fallen, kann in 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 branchenspezifischen Vorschriften zumindest dasselbe Schutzniveau erreicht wird, wie es diese Verordnung gewährleistet. Der Kommission sollte die Befugnis übertragen werden, delegierte Rechtsakte zur Ergänzung dieser Verordnung im Hinblick auf die Festlegung solcher Produkte und Vorschriften zu erlassen. In Bezug auf bestehendes Unionsrecht, für das solche Einschränkungen oder Ausschlüsse gelten sollten, enthält diese Verordnung besondere Bestimmungen, um ihr Verhältnis zu diesem Unionsrecht zu präzisieren.

(29) Damit auf dem Markt bereitgestellte Produkte mit digitalen Elementen wirksam repariert werden können und ihre Lebensdauer verlängert wird, sollte eine Ausnahme für Ersatzteile vorgesehen werden. Diese Ausnahme sollte sowohl für Ersatzteile gelten, die der Reparatur von Altprodukten dienen, die vor dem Geltungsbeginn dieser Verordnung zur Verfügung gestellt wurden, als auch für Ersatzteile, die bereits ein Konformitätsbewertungsverfahren gemäß dieser Verordnung durchlaufen haben.

(30) Nach der Delegierten Verordnung (EU) 2022/30 der Kommission ([14]) gelten die grundlegenden Anforderungen gemäß Artikel 3 Absatz 3 Buchstabe d, Buchstabe e und Buchstabe f der Richtlinie 2014/53/EU des Europäischen Parlaments und des Rates ([15]), die sich auf schädliche Auswirkungen auf das Netz und missbräuchliche Nutzung von Netzressourcen, personenbezogene Daten und Privatsphäre sowie Betrug beziehen, für bestimmte Funkanlagen. Der Durchführungsbeschluss C(2022) 5637 der Kommission vom 5. August 2022 über einen Normungsauftrag an das Europäische Komitee für Normung und das Europäische Komitee für elektrotechnische Normung 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 Cybersicherheitsanforderungen umfassen alle Elemente der grundlegenden Anforderungen gemäß Artikel 3 Absatz 3 Buchstaben d,

([11]) 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).

([12]) ABl. L 82 vom 9.3.2021, S. 30.

([13]) 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).

([14]) Delegierte Verordnung (EU) 2022/30 der Kommission vom 29. Oktober 2021 zur Ergänzung der Richtlinie 2014/53/EU des Europäischen Parlaments und des Rates im Hinblick auf die Anwendung der grundlegenden Anforderungen, auf die in Artikel 3 Absatz 3 Buchstaben d, e und f der Richtlinie Bezug genommen wird (ABl. L 7 vom 12.1.2022, S. 6).

([15]) Richtlinie 2014/53/EU des Europäischen Parlaments und des Rates vom 16. April 2014 über die Harmonisierung der Rechtsvorschriften der Mitgliedstaaten über die Bereitstellung von Funkanlagen auf dem Markt und zur Aufhebung der Richtlinie 1999/5/EG (ABl. L 153 vom 22.5.2014, S. 62).

e und f der Richtlinie 2014/53/EU. Darüber hinaus stehen die in dieser Verordnung festgelegten grundlegenden Cybersicherheitsanforderungen im Einklang mit den Zielen der Anforderungen an die spezifischen Normen, die in diesem Normungsauftrag vorgesehenen sind. Wenn die Kommission die Delegierte Verordnung (EU) 2022/30 aufhebt oder ändert, 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 durchgeführt werden, berücksichtigen, um die Durchführung der vorliegenden Verordnung zu erleichtern. Während des Übergangszeitraums für die Anwendung dieser Verordnung sollte die Kommission den Herstellern, die dieser Verordnung und auch der Delegierten Verordnung (EU) 2022/30 unterliegen, Leitlinien an die Hand geben, um den Nachweis der Einhaltung beider Verordnungen zu erleichtern.

(31) Die Richtlinie (EU) 2024/2853 des Europäischen Parlaments und des Rates ([16]) 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.

(32) Die vorliegende Verordnung sollte unbeschadet der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates ([17]) gelten, die Bestimmungen im Zusammenhang mit der 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 und den nationalen Datenschutzaufsichtsbehörden berücksichtigt werden. Synergieeffekte zwischen dieser Verordnung und dem Datenschutzrecht der Union sollten auch im Bereich der Marktüberwachung und Rechtsdurchsetzung angestrebt werden. Hierzu 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.

(33) Soweit ihre Produkte in den Anwendungsbereich der vorliegenden Verordnung fallen, sollten die Anbieter von Brieftaschen für die europäische digitale Identität (EUid-Brieftaschen) gemäß Artikel 5a Absatz 2 der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates ([18]) sowohl die in der vorliegenden Verordnung festgelegten horizontalen grundlegenden Cybersicherheitsanforderungen als auch die besonderen Sicherheitsanforderungen gemäß Artikel 5a der Verordnung (EU) Nr. 910/2014 erfüllen. Um die Einhaltung der Vorschriften zu erleichtern, sollten Anbieter von EUid-Brieftaschen die Konformität der EUid-Brieftaschen mit den in der vorliegenden Verordnung und in der Verordnung (EU) Nr. 910/2014 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 delegierten Rechtsakts eine Konformitätsvermutung für die Anforderungen der vorliegenden Verordnung festgelegt hat, soweit das Zertifikat oder Teile davon diese Anforderungen abdecken.

(34) Wenn die Hersteller in der Entwurfs- und Entwicklungsphase von Dritten bezogene Komponenten in Produkte mit digitalen Elementen integrieren, sollten sie in Bezug auf diese Komponenten, einschließlich freier und quelloffener Softwarekomponenten, die nicht auf dem Markt bereitgestellt wurden, die gebotene Sorgfalt walten lassen, um sicherzustellen, dass die Produkte im Einklang mit den in dieser Verordnung festgelegten grundlegenden

([16]) Richtlinie (EU) 2024/2853 des Europäischen Parlaments und des Rates vom 23. Oktober 2024 über die Haftung für fehlerhafte Produkte und zur Aufhebung der Richtlinie 85/374/EWG des Rates (ABl. L, 2024/2853, 18.11.2024, ELI: http://data.europa.eu/eli/dir/2024/2853/oj).

([17]) 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).

([18]) Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG (ABl. L 257 vom 28.8.2014, S. 73).

Cybersicherheitsanforderungen konzipiert, entwickelt und hergestellt werden. Der angemessene Umfang der Sorgfaltspflicht richtet sich nach der Art und dem Ausmaß des Cybersicherheitsrisikos, das mit einer bestimmten Komponente verbunden ist; dabei sollten zu diesem Zweck eine oder mehrere der folgenden Maßnahmen Berücksichtigung finden: gegebenenfalls Überprüfung, ob der Hersteller einer Komponente die Konformität mit dieser Verordnung nachgewiesen hat, einschließlich einer Kontrolle der Frage, ob die Komponente bereits mit der CE-Kennzeichnung versehen ist; Überprüfung, ob für eine Komponente regelmäßig Sicherheitsaktualisierungen vorgenommen werden, etwa durch Kontrolle der bisherigen Sicherheitsaktualisierungen; Überprüfung, ob eine Komponente frei von den Schwachstellen ist, die in der gemäß Artikel 12 Absatz 2 der Richtlinie (EU) 2022/2555 eingerichteten europäischen Schwachstellendatenbank oder anderen öffentlich zugänglichen Schwachstellendatenbanken registriert sind, oder Durchführung zusätzlicher Sicherheitsprüfungen. Die in dieser Verordnung festgelegten Pflichten zum Umgang mit Schwachstellen, die die Hersteller beim Inverkehrbringen eines Produkts mit digitalen Elementen und während des Unterstützungszeitraums erfüllen müssen, gelten für Produkte mit digitalen Elementen in ihrer Gesamtheit, einschließlich aller integrierten Komponenten. Stellt der Hersteller des Produkts mit digitalen Elementen im Rahmen seiner Sorgfaltspflicht eine Schwachstelle in einer Komponente, auch in einer freien und quelloffenen Komponente, fest, sollte er die Person oder die Einrichtung, die die Komponente hergestellt hat bzw. wartet, informieren, die Schwachstelle beheben und der Person oder der Einrichtung gegebenenfalls den eingesetzten Sicherheits-Patch zur Verfügung stellen.

(35) Unmittelbar nach dem Übergangszeitraum für die Anwendung dieser Verordnung ist ein Hersteller eines Produkts mit digitalen Elementen, das eine oder mehrere Komponenten enthält, die von Dritten bezogen werden, die ebenfalls dieser Verordnung unterliegen, möglicherweise nicht in der Lage, im Rahmen seiner Sorgfaltspflicht zu überprüfen, ob die Hersteller dieser Komponenten die Konformität mit dieser Verordnung nachgewiesen haben, indem er beispielsweise kontrolliert, ob die Komponenten bereits die CE-Kennzeichnung tragen. Dies kann der Fall sein, wenn die Komponenten integriert wurden, bevor diese Verordnung auf die Hersteller dieser Komponente anwendbar wird. In einem solchen Fall sollte ein Hersteller, der solche Komponenten integriert, seiner Sorgfaltspflicht auf andere Weise nachkommen.

(36) Produkte mit digitalen Elementen sollten grundsätzlich mit der CE-Kennzeichnung versehen sein, aus der ihre Konformität mit dieser Verordnung gut sichtbar, lesbar und dauerhaft 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. Ferner sollten die Mitgliedstaaten nicht die Präsentation oder Verwendung eines Produkts mit digitalen Elementen, das dieser Verordnung nicht entspricht, bei Messen, Ausstellungen, Vorführungen oder ähnlichen Veranstaltungen, einschließlich Prototypen, verhindern, sofern das Produkt eine sichtbare Kennzeichnung aufweist, die deutlich darauf hinweist, dass das Produkt dieser Verordnung nicht entspricht und erst auf dem Markt bereitgestellt werden darf, wenn es dies tut.

(37) Damit Hersteller Software zu Testzwecken freigeben können, bevor sie ihre Produkte mit digitalen Elementen einer Konformitätsbewertung unterziehen, sollten die Mitgliedstaaten nicht verhindern, dass unfertige Software z. B. als Alpha-, Beta- oder Vorabversion bereitgestellt wird, sofern die unfertige Software 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.

(38) Damit Produkte mit digitalen Elementen beim Inverkehrbringen keine Cybersicherheitsrisiken für Personen und Organisationen darstellen, sollten für solche Produkte grundlegende Cybersicherheitsanforderungen festgelegt werden. Diese grundlegenden Cybersicherheitsanforderungen, einschließlich der Anforderungen an das Schwachstellenmanagement, gelten für jedes einzelne Produkt mit digitalen Elementen, wenn es in den Verkehr gebracht wird, unabhängig davon, ob das Produkt mit digitalen Elementen als Einzelstück oder in Serie hergestellt wird. So sollte beispielsweise bei einer Produktart jedes einzelne Produkt mit digitalen Elementen alle verfügbaren Sicherheits-Patches oder Aktualisierungen zur Behebung relevanter Sicherheitsprobleme erhalten haben, wenn es in den Verkehr gebracht wird. Werden solche Produkte mit digitalen Elementen nachträglich physisch oder digital in einer Weise verändert, die vom Hersteller in der ursprünglichen Risikobewertung nicht vorgesehen ist und die dazu führen kann, dass sie die einschlägigen grundlegenden Cybersicherheitsanforderungen nicht mehr erfüllen, sollte die Veränderung als wesentlich betrachtet werden. Beispielsweise könnten Reparaturen den Wartungsarbeiten gleichgestellt werden, sofern sie ein bereits in den Verkehr gebrachtes Produkt mit digitalen Elementen nicht so verändern, dass die Konformität mit den geltenden Anforderungen beeinträchtigt oder die Zweckbestimmung, für die das Produkt geprüft wurde, verändert werden kann.

(39) Wie bei physischen Reparaturen oder Änderungen sollte ein Produkt mit digitalen Elementen als durch eine Softwareänderung wesentlich geändert gelten, wenn die Softwareaktualisierung die Zweckbestimmung des Produkts ändert und diese Änderungen vom Hersteller in der ursprünglichen Risikobewertung nicht vorhergesehen wurden, oder wenn sich die Art der Gefahr geändert oder sich das Cybersicherheitsrisiko aufgrund der Softwareaktualisierung erhöht hat und die aktualisierte Version des Produkts auf dem Markt bereitgestellt wird. Wenn eine Sicherheitsaktualisierung, mit der das Cybersicherheitsrisiko eines Produkts mit digitalen Elementen verringert

werden soll, die Zweckbestimmung eines Produkts mit digitalen Elementen nicht verändert, gilt sie nicht als wesentliche Änderung. Dies schließt in der Regel Fälle ein, in denen eine Sicherheitsaktualisierung nur geringfügige Anpassungen des Quellcodes nach sich zieht. Dies könnte zum Beispiel der Fall sein, wenn mit einer Sicherheitsaktualisierung eine bekannte Schwachstelle behoben wird, auch durch Änderung der Funktionen oder der Leistung eines Produkts mit digitalen Elementen zu dem alleinigen Zweck, das Cybersicherheitsrisiko zu senken. Ebenso sollte eine geringfügige Aktualisierung der Funktionalitäten, etwa eine visuelle Verbesserung oder die Hinzufügung neuer Sprachen oder neuer Piktogramme zur Benutzeroberfläche, im Allgemeinen nicht als wesentliche Änderungen betrachtet werden. Umgekehrt sollte eine Funktionsaktualisierung die die ursprünglich beabsichtigten Funktionen oder die Art oder Leistung eines Produkts mit digitalen Elementen verändert und die oben genannten Kriterien erfüllt, als wesentliche Änderung betrachtet werden, da das Hinzufügen neuer Funktionen in der Regel zu einer größeren Angriffsfläche führt und damit das Cybersicherheitsrisiko erhöht. Dies könnte zum Beispiel der Fall sein, wenn einer Anwendung ein neues Eingabeelement hinzugefügt wird, sodass der Hersteller für eine adäquate Eingabevalidierung sorgen muss. Bei der Beurteilung, ob eine Funktionsaktualisierung als wesentliche Änderung anzusehen ist, spielt es keine Rolle, ob sie als separate Aktualisierung oder in Kombination mit einer Sicherheitsaktualisierung bereitgestellt wird. Die Kommission sollte Leitlinien zur Bestimmung dessen herausgeben, was eine wesentliche Änderung ist.

(40) In Anbetracht des der Softwareentwicklung innewohnenden Wiederholungscharakters sollten Hersteller, die aufgrund einer späteren wesentlichen Änderung an dem Produkt neue Versionen eines Softwareprodukts in den Verkehr gebracht haben, die Möglichkeit haben, während des Unterstützungszeitraums nur für die Version des Softwareprodukts, die sie zuletzt in den Verkehr gebracht haben, Sicherheitsaktualisierungen anzubieten. Dazu sollten sie nur dann berechtigt sein, wenn die Nutzer der einschlägigen früheren Produktversionen Zugang zu der zuletzt in den Verkehr gebrachten Produktversion haben und ihnen keine zusätzlichen Kosten für die Anpassung der Hardware- oder Softwareumgebung, in der sie das Produkt betreiben, entstehen. Das könnte beispielsweise der Fall sein, wenn eine Aufrüstung des Desktop-Betriebssystems keine neue Hardware erfordert, z. B. eine schnellere Zentraleinheit oder mehr Speicher. Dessen ungeachtet sollte der Hersteller während des Unterstützungszeitraums weiterhin sonstige Anforderungen an die Behandlung von Schwachstellen erfüllen und etwa über eine Strategie zur abgestimmten Offenlegung von Schwachstellen verfügen oder Vorkehrungen getroffen haben, um den Informationsaustausch über potenzielle Schwachstellen für alle nachfolgenden, wesentlich geänderten Versionen des in den Verkehr gebrachten Softwareprodukts zu erleichtern. Die Hersteller sollten die Möglichkeit haben, geringfügige Sicherheits- oder Funktionsaktualisierungen, die keine wesentliche Änderung darstellen, nur für die letzte Version oder Unterversion eines Softwareprodukts, das nicht wesentlich geändert wurde, bereitzustellen. Gleichzeitig sollte der Hersteller in Fällen, in denen ein Hardwareprodukt wie ein Smartphone nicht mit der neuesten Version des Betriebssystems kompatibel ist, mit dem es ursprünglich geliefert wurde, während des Unterstützungszeitraums zumindest für die letzte kompatible Version des Betriebssystems weiterhin Sicherheitsaktualisierungen bereitstellen.

(41) Im Einklang mit dem allgemein anerkannten Konzept der wesentlichen Änderung von Produkten, für die Harmonisierungsrechtsvorschriften der Union gelten, ist es angebracht, wenn eine wesentliche Änderung eintritt, die sich auf die Konformität eines Produkts mit digitalen Elementen 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, sollte eine Veränderung, die zu einer wesentlichen Änderung führen könnte, dem Dritten mitgeteilt werden.

(42) Wird ein Produkt mit digitalen Elementen einer „Überholung", „Wartung" und „Reparatur" im Sinne des Artikels 2 Nummern 18, 19 und 20 der Verordnung (EU) 2024/1781 des Europäischen Parlaments und des Rates ([19]) unterzogen, führt dies nicht unbedingt zu einer wesentlichen Änderung des Produkts, wenn z. B. die Zweckbestimmung und die Funktionen nicht geändert werden und das Risikoniveau gleich bleibt. Die Aufrüstung eines Produkts mit digitalen Elementen durch den Hersteller könnte jedoch zu Änderungen in der Konzeption und Entwicklung des Produkts führen und sich daher auf seine Zweckbestimmung und die Konformität mit den in dieser Verordnung festgelegten Anforderungen auswirken.

(43) Produkte mit digitalen Elementen sollten als wichtig betrachtet werden, wenn die negativen Auswirkungen der Ausnutzung potenzieller Cybersicherheitslücken in dem Produkt schwerwiegend sein können, unter anderem aufgrund seiner Cybersicherheitsfunktion oder einer Funktion, die ein beträchtliches Risiko nachteiliger Auswirkungen birgt, was ihre Tragweite und ihre Möglichkeit anbelangt, eine große Zahl anderer Produkte mit digitalen Elementen zu stören, zu kontrollieren oder zu schädigen oder die Gesundheit, die Sicherheit oder die Unversehrtheit ihrer Nutzer zu beeinträchtigen, indem sie direkt manipuliert wird, wie etwa eine zentrale Systemfunktion, einschließlich Netzverwaltung, Konfigurationskontrolle, Virtualisierung oder Verarbeitung personenbezogener Daten. Insbesondere können Schwachstellen in Produkten mit digitalen Elementen, die eine Cybersicherheitsfunktion haben, wie z. B. Bootmanager, zu einer Ausbreitung von Sicherheitsproblemen in der

([19]) Verordnung (EU) 2024/1781 des Europäischen Parlaments und des Rates vom 13. Juni 2024 zur Schaffung eines Rahmens für die Festlegung von Ökodesign-Anforderungen für nachhaltige Produkte, zur Änderung der Richtlinie (EU) 2020/1828 und der Verordnung (EU) 2023/1542 und zur Aufhebung der Richtlinie 2009/125/EG (ABl. L, 2024/1781, 28.6.2024, ELI: http://data.europa.eu/eli/reg/2024/1781/oj).

gesamten Lieferkette führen. Die Schwere der Auswirkungen eines Sicherheitsvorfalls kann auch zunehmen, wenn das Produkt in erster Linie eine zentrale Systemfunktion ausübt, einschließlich Netzverwaltung, Konfigurationskontrolle, Virtualisierung oder Verarbeitung personenbezogener Daten.

(44) Bestimmte Kategorien von Produkten mit digitalen Elementen sollten strengeren Konformitätsbewertungsverfahren unterliegen, wobei die Verhältnismäßigkeit gewahrt werden sollte. Zu diesem Zweck sollten wichtige Produkte mit digitalen Elementen in zwei Klassen unterteilt werden, die das mit diesen Produktkategorien verbundene Cybersicherheitsrisiko widerspiegeln. Ein Sicherheitsvorfall mit wichtigen Produkten mit digitalen Elementen, die in Klasse II fallen, könnte größere negative Auswirkungen haben als ein Sicherheitsvorfall mit wichtigen Produkten mit digitalen Elementen, die in Klasse I fallen, beispielsweise wegen der Art ihrer Cybersicherheitsfunktion oder der Ausübung einer anderen Funktion, die ein erhebliches Risiko nachteiliger Auswirkungen birgt. Ein Anhaltspunkt für größere negative Auswirkungen könnte es sein, dass Produkte mit digitalen Elementen, die in Klasse II fallen, entweder eine Cybersicherheitsfunktion übernehmen oder eine andere Funktion, die mit einem höheren Risiko schädlicher Auswirkungen als bei Produkten in Klasse I verbunden ist, oder beide genannten Kriterien erfüllen. Wichtige Produkte mit digitalen Elementen, die in Klasse II fallen, sollten daher einem strengeren Konformitätsbewertungsverfahren unterzogen werden.

(45) Wichtige Produkte mit digitalen Elementen, auf die in dieser Verordnung Bezug genommen wird, sollten als Produkte verstanden werden, die die Kernfunktion einer in dieser Verordnung festgelegten Kategorie wichtiger Produkte mit digitalen Elementen aufweisen. So werden in dieser Verordnung beispielsweise Kategorien wichtiger Produkte mit digitalen Elementen festgelegt, die durch ihre Kernfunktion als Firewalls oder Intrusion-Detection-Systeme oder Intrusion-Prevention-Systeme der Klasse II definiert werden. Folglich unterliegen Firewalls und Intrusion-Detection-Systeme und Intrusion-Prevention-Systeme einer obligatorischen Konformitätsbewertung durch Dritte. Dies gilt nicht für andere Produkte mit digitalen Elementen, die nicht als wichtige Produkte mit digitalen Elementen eingestuft sind und die Firewalls oder Intrusion-Detection-Systeme oder Intrusion-Prevention-Systeme enthalten können. Die Kommission sollte einen Durchführungsrechtsakt erlassen, um die technische Beschreibung der Kategorien wichtiger Produkte mit digitalen Elementen, die unter die Klassen I und II gemäß dieser Verordnung fallen, zu präzisieren.

(46) Die in dieser Verordnung festgelegten Kategorien kritischer Produkte mit digitalen Elementen sind mit einer Cybersicherheitsfunktion verbunden und werden für eine Funktion verwendet, die ein beträchtliches Risiko nachteiliger Auswirkungen birgt, was ihre Tragweite und ihre Möglichkeit anbelangt, eine große Zahl anderer Produkte mit digitalen Elementen zu stören, zu kontrollieren oder zu schädigen, indem sie direkt manipuliert wird. Darüber hinaus gelten diese Kategorien von Produkten mit digitalen Elementen als kritische Abhängigkeiten für die in Artikel 3 Absatz 1 der Richtlinie (EU) 2022/2555 genannten wesentlichen Einrichtungen. Die Kategorien kritischer Produkte mit digitalen Elementen, die aufgrund ihrer Kritikalität in einem Anhang dieser Verordnung aufgeführt sind, nutzen bereits häufig verschiedene Formen der Zertifizierung und fallen auch unter das auf gemeinsamen Kriterien beruhende europäische System für die Cybersicherheitszertifizierung (EUCC), das in der Durchführungsverordnung (EU) 2024/482 ([20]) festgelegt ist. Um einen gemeinsamen angemessenen Schutz der Cybersicherheit kritischer Produkte mit digitalen Elementen in der Union sicherzustellen, könnte es daher angemessen und verhältnismäßig sein, solche Produktkategorien im Wege eines delegierten Rechtsakts der obligatorischen europäischen Cybersicherheitszertifizierung zu unterwerfen, wenn bereits ein einschlägiges europäisches Schema für die Cybersicherheitszertifizierung für diese Produkte besteht und die Kommission eine Bewertung der potenziellen Auswirkungen der geplanten obligatorischen Zertifizierung auf den Markt vorgenommen hat. Bei dieser Bewertung sollten sowohl die Angebots- als auch die Nachfrageseite berücksichtigt werden, einschließlich der Frage, ob eine ausreichende Nachfrage nach den betreffenden Produkten mit digitalen Elementen sowohl bei den Mitgliedstaaten als auch bei den Nutzern besteht, sodass eine europäische Cybersicherheitszertifizierung erforderlich ist, sowie die Zwecke, für die die Produkte mit digitalen Elementen verwendet werden sollen, einschließlich der kritischen Abhängigkeiten davon seitens der in Artikel 3 Absatz 1 der Richtlinie (EU) 2022/2555 genannten wesentlichen Einrichtungen. Bei der Bewertung sollten auch die potenziellen Auswirkungen der obligatorischen Zertifizierung auf die Verfügbarkeit dieser Produkte auf dem Binnenmarkt sowie die Fähigkeiten und die Bereitschaft der Mitgliedstaaten mit Blick auf die Umsetzung der einschlägigen europäischen Schemata für die Cybersicherheitszertifizierung analysiert werden.

(47) In delegierten Rechtsakten, mit denen eine verpflichtende europäische Cybersicherheitszertifizierung vorgeschrieben wird, sollten die Produkte mit digitalen Elementen bestimmt werden, die die Kernfunktionen einer in dieser Verordnung festgelegten Kategorie kritischer Produkte mit digitalen Elementen, die einer obligatorischen Zertifizierung unterworfen werden sollen, sowie die erforderliche Vertrauenswürdigkeitsstufe, die mindestens „mittel“ sein sollte, aufweisen. Die erforderliche Vertrauenswürdigkeitsstufe sollte in einem angemessenen Verhältnis zum Niveau des Cybersicherheitsrisikos stehen, das mit dem Produkt mit digitalen Elementen verbunden ist. Wenn beispielsweise das Produkt mit digitalen Elementen die Kernfunktion einer in dieser Verordnung festgelegten Kategorie kritischer Produkte mit digitalen Elementen aufweist und für die Verwendung in einer empfindlichen oder

([20]) Durchführungsverordnung (EU) 2024/482 der Kommission vom 31. Januar 2024 mit Durchführungsbestimmungen zur Verordnung (EU) 2019/881 des Europäischen Parlaments und des Rates hinsichtlich der Annahme des auf den Gemeinsamen Kriterien beruhenden europäischen Systems für die Cybersicherheitszertifizierung (EUCC) (ABl. L, 2024/482, 7.2.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/482/oj).

kritischen Umgebung vorgesehen ist, wie Produkte, die für die Verwendung durch die in Artikel 3 Absatz 1 der Richtlinie (EU) 2022/2555 genannten wesentlichen Einrichtungen bestimmt sind, ist unter Umständen die höchste Vertrauenswürdigkeitsstufe erforderlich.

(48) Um für einen gemeinsamen, angemessenen Schutz der Cybersicherheit von Produkten mit digitalen Elementen in der Union zu sorgen, die die Kernfunktion einer in dieser Verordnung festgelegten Kategorie kritischer Produkte mit digitalen Elementen aufweisen, sollte der Kommission auch die Befugnis übertragen werden, delegierte Rechtsakte zur Änderung dieser Verordnung zu erlassen, indem Kategorien kritischer Produkte mit digitalen Elementen hinzugefügt oder gestrichen werden, für die von den Herstellern verlangt werden könnte, im Rahmen eines europäischen Schemas für die Cybersicherheitszertifizierung gemäß der Verordnung (EU) 2019/881 ein europäisches Cybersicherheitszertifikat einzuholen, um die Konformität mit der vorliegenden Verordnung nachzuweisen. Eine neue Kategorie kritischer Produkte mit digitalen Elementen kann zu diesen Kategorien hinzugefügt werden, wenn eine kritische Abhängigkeit der in Artikel 3 Absatz 1 der Richtlinie (EU) 2022/2555 genannten wesentlichen Einrichtungen von diesen Produkten besteht oder wenn sie von Sicherheitsvorfällen betroffen sind oder ausgenutzte Schwachstellen enthalten und dies zu Unterbrechungen kritischer Lieferketten führen könnte. Bei der Bewertung der Frage, ob es notwendig ist, mittels eines delegierten Rechtsakts Kategorien kritischer Produkte mit digitalen Bestandteilen hinzuzufügen oder zu streichen, sollte die Kommission berücksichtigen können, ob die Mitgliedstaaten auf nationaler Ebene Produkte mit digitalen Elementen ermittelt haben, die für die Resilienz wesentlicher Einrichtungen im Sinne von Artikel 3 Absatz 1 der Richtlinie (EU) 2022/2555 von maßgeblicher Bedeutung sind und die zunehmend mit Cyberangriffen auf die Lieferkette zu kämpfen haben, was schwerwiegende Beeinträchtigungen zur Folge haben könnte. Darüber hinaus sollte die Kommission die Möglichkeit haben, das Ergebnis der koordinierten Risikobewertungen in Bezug auf die Sicherheit kritischer Lieferketten auf Ebene der Union, die gemäß Artikel 22 der Richtlinie (EU) 2022/2555 durchgeführt werden, zu berücksichtigen.

(49) Die Kommission sollte sicherstellen, dass bei der Ausarbeitung von Maßnahmen zur Durchführung dieser Verordnung ein breites Spektrum einschlägiger Interessengruppen in strukturierter und regelmäßiger Weise konsultiert wird. Dies sollte insbesondere dann der Fall sein, wenn die Kommission prüft, ob die Listen der Kategorien wichtiger oder kritischer Produkte mit digitalen Elementen möglicherweise aktualisiert werden müssen, wobei die einschlägigen Hersteller konsultiert und ihre Ansichten berücksichtigt werden sollten, um die Cybersicherheitsrisiken und das Kosten-Nutzen-Verhältnis zu analysieren, die mit der Einstufung solcher Produktkategorien als wichtig oder kritisch verbunden sind.

(50) Mit dieser Verordnung werden Cybersicherheitsrisiken gezielt angegangen. Produkte mit digitalen Elementen können jedoch noch andere Sicherheitsrisiken bergen, die nicht immer mit der Cybersicherheit zusammenhängen, sich aber aus einer Sicherheitsverletzung ergeben können. Diese Risiken sollten weiterhin durch andere einschlägige Harmonisierungsrechtsvorschriften der Union als diese Verordnung geregelt werden. Wenn keine anderen Harmonisierungsrechtsvorschriften der Union als diese Verordnung anwendbar sind, sollten sie der Verordnung (EU) 2023/988 des Europäischen Parlaments und des Rates ([21]) unterliegen. Angesichts der gezielten Ausrichtung der vorliegenden Verordnung sollten daher abweichend von Artikel 2 Absatz 1 Unterabsatz 3 Buchstabe b der Verordnung (EU) 2023/988 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 (EU) 2023/988 auch für Produkte mit digitalen Elementen gelten, wenn diese Produkte keinen besonderen Anforderungen anderer Harmonisierungsrechtsvorschriften der Union als dieser Verordnung im Sinne von Artikel 3 Nummer 27 der Verordnung (EU) 2023/988 unterliegen.

(51) Produkte mit digitalen Elementen, die nach Artikel 6 der Verordnung (EU) 2024/1689 des Europäischen Parlaments und des Rates ([22]) als Hochrisiko-KI-Systeme eingestuft sind und in den Anwendungsbereich der vorliegenden Verordnung fallen, sollten den in der vorliegenden Verordnung festgelegten grundlegenden Cybersicherheitsanforderungen genügen. Genügen diese Hochrisiko-KI-Systeme den in der vorliegenden Verordnung festgelegten grundlegenden Cybersicherheitsanforderungen, so gelten sie als die Cybersicherheitsanforderungen gemäß Artikel 15 der Verordnung (EU) 2024/1689 erfüllend, soweit diese Anforderungen von der nach der vorliegenden Verordnung ausgestellten EU-Konformitätserklärung oder Teilen davon abgedeckt sind. Zu diesem Zweck sollten bei der Bewertung der mit einem Produkt mit digitalen Elementen, das als KI-System mit hohem Risiko gemäß der VO (EU) 2024/1689 eingestuft wird, verbundenen Cybersicherheitsrisiken, die während der Planungs-, Entwurfs-, Entwicklungs-, Produktions-, Liefer- und Wartungsphasen eines solchen Produkts zu berücksichtigen ist, wie in dieser Verordnung vorgeschrieben, die Risiken für die Cyberresilienz eines KI-Systems berücksichtigt werden in Bezug auf Versuche unbefugter Dritter, die Nutzung, das Verhalten oder die Leistung des Systems zu verändern, einschließlich KI-spezifischer Schwachstellen wie Data Poisoning oder adversarial attack, sowie gegebenenfalls

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

([22]) Verordnung (EU) 2024/1689 des Europäischen Parlaments und des Rates vom 13. Juni 2024 zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz (und zur Änderung der Verordnungen (EG) Nr. 300/2008, (EU) Nr. 167/2013, (EU) Nr. 168/2013, (EU) 2018/858, (EU) 2018/1139 und (EU) 2019/2144 sowie der Richtlinien 2014/90/EU, (EU) 2016/797 und (EU) 2020/1828 (Gesetz über künstliche Intelligenz) (ABl. L, 2024/1689, 12.7.2024, ELI: http://data.europa.eu/eli/reg/2024/1689/oj).

Risiken für die Grundrechte, gemäß der Verordnung (EU) 2024/1689. Für die Konformitätsbewertungsverfahren zu den grundlegenden Cybersicherheitsanforderungen an ein Produkt mit digitalen Elementen, das in den Anwendungsbereich der vorliegenden Verordnung fällt und als Hochrisiko-KI-System eingestuft ist, sollte grundsätzlich anstelle der einschlägigen Bestimmungen der vorliegenden Verordnung Artikels 43 der Verordnung (EU) 2024/1689 Anwendung finden. Diese Regel sollte jedoch nicht dazu führen, dass die erforderliche Vertrauenswürdigkeit für die in der vorliegenden Verordnung genannten wichtigen oder kritischen Produkte mit digitalen Elementen verringert wird. Deshalb sollten abweichend von dieser Regel Hochrisiko-KI-Systeme, die in den Anwendungsbereich der Verordnung (EU) 2024/1689 fallen und auch wichtige oder kritische Produkte mit digitalen Elementen, wie in der vorliegenden Verordnung genannt, sind und auf die das Konformitätsbewertungsverfahren auf der Grundlage einer internen Kontrolle gemäß Anhang VI der Verordnung (EU) 2024/1689 angewandt wird, den Konformitätsbewertungsverfahren der vorliegenden Verordnung unterliegen, soweit die in der vorliegenden Verordnung festgelegten grundlegenden Cybersicherheitsanforderungen betroffen sind. In diesem Fall sollten für alle anderen Aspekte, die unter die Verordnung (EU) 2024/1689 fallen, die einschlägigen Bestimmungen über die Konformitätsbewertung auf der Grundlage einer internen Kontrolle gemäß Anhang VI der genannten Verordnung gelten.

(52) Zur Erhöhung der Sicherheit von Produkten mit digitalen Elementen, die im Binnenmarkt in den Verkehr gebracht werden, ist es erforderlich, grundlegende Cybersicherheitsanforderungen festzulegen, die für solche Produkte gelten. Diese grundlegenden Cybersicherheitsanforderungen sollten die koordinierten Risikobewertungen in Bezug auf die Sicherheit kritischer Lieferketten auf Ebene der Union, die in Artikel 22 der der Richtlinie (EU) 2022/2555 vorgesehen sind, unberührt lassen, in denen sowohl technische als gegebenenfalls auch nichttechnische Risikofaktoren wie eine unzulässige Einflussnahme eines Drittlands auf Lieferanten berücksichtigt werden. Darüber hinaus sollten sie die Vorrechte der Mitgliedstaaten unberührt lassen, zusätzliche Anforderungen festzulegen, die nichttechnischen Faktoren Rechnung tragen, um ein hohes Maß an Resilienz sicherzustellen, einschließlich derer, die in der Empfehlung (EU) 2019/534 der Kommission ([23]), in der EU-weit koordinierten Risikobewertung zur Cybersicherheit der 5G-Netze und in dem EU-Instrumentarium für die 5G-Cybersicherheit definiert worden sind, das die gemäß Artikel 14 der Richtlinie (EU) 2022/2555 eingerichtete NIS-Kooperationsgruppe beschlossen hat.

(53) Die Hersteller von Produkten, die in den Anwendungsbereich der Verordnung (EU) 2023/1230 des Europäischen Parlaments und des Rates ([24]) fallen und bei deren Produkten es sich auch um Produkte mit digitalen Elementen im Sinne der vorliegenden Verordnung handelt, sollten sowohl die grundlegenden Cybersicherheitsanforderungen der vorliegenden Verordnung als auch die grundlegenden Sicherheits- und Gesundheitsschutzanforderungen gemäß der Verordnung (EU) 2023/1230 erfüllen. Die in dieser Verordnung festgelegten grundlegenden Cybersicherheitsanforderungen und bestimmte grundlegende Anforderungen der Verordnung (EU) 2023/1230 betreffen unter Umstände ähnliche Cybersicherheitsrisiken. Daher könnte die Einhaltung der in der vorliegenden Verordnung festgelegten grundlegenden Cybersicherheitsanforderungen die Einhaltung der grundlegenden Anforderungen erleichtern, die auch bestimmte Cybersicherheitsrisiken gemäß der Verordnung (EU) 2023/1230 abdecken, insbesondere die Anforderungen in Bezug auf den Schutz gegen Korrumpierung sowie die Sicherheit und Zuverlässigkeit von Steuerungen gemäß Anhang III Abschnitte 1.1.9 und 1.2.1 der genannten Verordnung. Solche Synergieeffekte müssen vom Hersteller nachgewiesen werden, beispielsweise durch die Anwendung harmonisierter Normen oder anderer technischer Spezifikationen, die die einschlägigen grundlegenden Cybersicherheitsanforderungen abdecken, nachdem eine Risikobewertung für die entsprechenden Cybersicherheitsrisiken durchgeführt wurde. Der Hersteller sollte auch die geltenden Konformitätsbewertungsverfahren gemäß dieser Verordnung und der Verordnung (EU) 2023/1230 befolgen. Die Kommission und die europäischen Normungsorganisationen sollten bei den vorbereitenden Arbeiten zur Unterstützung der Umsetzung dieser Verordnung und der Verordnung (EU) 2023/1230 und der damit verbundenen Normungsverfahren die Kohärenz fördern, was die Bewertung der Cybersicherheitsrisiken und die Art und Weise betrifft, wie diese Risiken durch harmonisierte Normen im Hinblick auf die einschlägigen grundlegenden Anforderungen abgedeckt werden sollen. Insbesondere sollten die Kommission und die europäischen Normungsorganisationen diese Verordnung bei der Ausarbeitung und Entwicklung harmonisierter Normen berücksichtigen, um die Durchführung der Verordnung (EU) 2023/1230 insbesondere in Bezug auf die Cybersicherheitsaspekte im Zusammenhang mit dem Schutz gegen Korrumpierung sowie der Sicherheit und Zuverlässigkeit von Steuerungen, die in Anhang III Abschnitte 1.1.9 und 1.2.1 der genannten Verordnung aufgeführt sind, zu erleichtern. Die Kommission sollte Leitlinien bereitstellen, um Hersteller, die dieser Verordnung und auch der Verordnung (EU) 2023/1230 unterliegen, zu unterstützen, um insbesondere den Nachweis der Einhaltung der einschlägigen grundlegenden Anforderungen der vorliegenden Verordnung und der Verordnung (EU) 2023/1230 zu erleichtern.

(54) Um sicherzustellen, dass Produkte mit digitalen Elementen sowohl zum Zeitpunkt ihres Inverkehrbringens als auch während der voraussichtlichen Nutzungsdauer des Produkts mit digitalen Elementen sicher sind, müssen grundlegende Cybersicherheitsanforderungen für die Behandlung von Schwachstellen und grundlegende Cybersicherheitsanforderungen in Bezug auf die Eigenschaften von Produkten mit digitalen Elementen festgelegt

([23]) Empfehlung (EU) 2019/534 der Kommission vom 26. März 2019 mit dem Titel „Cybersicherheit der 5G-Netze“ (ABl. L 88 vom 29.3.2019, S. 42).

([24]) Verordnung (EU) 2023/1230 des Europäischen Parlaments und des Rates vom 14. Juni 2023 über Maschinen und zur Aufhebung der Richtlinie 2006/42/EG des Europäischen Parlaments und des Rates und der Richtlinie 73/361/EWG des Rates (ABl. L 165 vom 29.6.2023, S. 1).

werden. Die Hersteller sollten sowohl alle grundlegenden Cybersicherheitsanforderungen in Bezug auf die Behandlung von Schwachstellen während des gesamten Unterstützungszeitraums erfüllen, als auch bestimmen, welche anderen grundlegenden Cybersicherheitsanforderungen in Bezug auf die Produkteigenschaften für die betreffende Art von Produkten mit digitalen Elementen 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 Cybersicherheitsanforderungen zu ermitteln, sodass sie ihre Produkte mit digitalen Elementen ohne bekannte ausnutzbare Schwachstellen bereitstellen, die sich auf die Sicherheit dieser Produkte auswirken könnten, und um geeignete harmonisierte Normen, gemeinsame Spezifikationen oder europäische oder internationale Normen angemessen anzuwenden.

(55) Sind bestimmte grundlegende Cybersicherheitsanforderungen auf ein Produkt mit digitalen Elementen nicht anwendbar, sollte der Hersteller dies in der Risikobewertung für die Cybersicherheit eindeutig begründen, die der technischen Dokumentation beigefügt ist. Dies könnte der Fall sein, wenn eine grundlegende Cybersicherheitsanforderung mit der Art eines Produkts mit digitalen Elementen unvereinbar ist. So kann es beispielsweise aufgrund der Zweckbestimmung eines Produkts mit digitalen Elementen erforderlich sein, dass der Hersteller weithin anerkannte Interoperabilitätsnormen befolgt, selbst wenn seine Sicherheitsmerkmale nicht mehr dem Stand der Technik entsprechen. Auch andere Rechtsvorschriften der Union verlangen, dass die Hersteller spezifischen Interoperabilitätsanforderungen genügen. Wenn eine grundlegende Cybersicherheitsanforderungen nicht für ein Produkt mit digitalen Elementen anwendbar ist, der Hersteller jedoch Cybersicherheitsrisiken im Zusammenhang mit dieser grundlegenden Cybersicherheitsanforderung ermittelt hat, sollte er Maßnahmen ergreifen, um diesen Risiken mit anderen Mitteln zu begegnen, beispielsweise indem er die Zweckbestimmung des Produkts auf vertrauenswürdige Umgebungen beschränkt oder die Nutzer über diese Risiken informiert.

(56) Eine der wichtigsten Maßnahmen, die die Nutzer ergreifen müssen, um ihre Produkte mit digitalen Elementen vor Cyberangriffen zu schützen, ist die schnellstmögliche Installation der neuesten verfügbaren Sicherheitsaktualisierungen. Die Hersteller sollten daher ihre Produkte so gestalten und Verfahren einrichten, dass Produkte mit digitalen Elementen automatische Funktionen mit Blick auf die Benachrichtigung, die Verteilung, das Herunterladen und die Installation von Sicherheitsaktualisierungen enthalten, insbesondere im Falle von Verbraucherprodukten. Sie sollten auch die Möglichkeit bieten, als letzte Etappe das Herunterladen und die Installation der Sicherheitsaktualisierungen zu genehmigen. Die Nutzer sollten weiterhin die Möglichkeit haben, automatische Aktualisierungen zu deaktivieren, und zwar mit einem klaren und einfach zu bedienenden Vorgang, der durch eindeutige Erläuterungen dazu ergänzt wird, wie die Nutzer auf Aktualisierungen verzichten können. Die in einem Anhang dieser Verordnung festgelegten Anforderungen an automatische Aktualisierungen gelten nicht für Produkte mit digitalen Elementen, die in erster Linie dazu bestimmt sind, als Komponenten in andere Produkte integriert zu werden. Sie gelten auch nicht für Produkte mit digitalen Elementen, bei denen die Nutzer normalerweise keine automatischen Aktualisierungen erwarten würden, einschließlich Produkten mit digitalen Elementen, die für den Einsatz in professionellen IKT-Netzen und insbesondere in kritischen und industriellen Umgebungen bestimmt sind, in denen eine automatische Aktualisierung zu Störungen des Betriebs führen könnte. Unabhängig davon, ob ein Produkt mit digitalen Elementen für den Empfang automatischer Aktualisierungen konzipiert ist oder nicht, sollte sein Hersteller die Nutzer über Schwachstellen informieren und Sicherheitsaktualisierungen unverzüglich zur Verfügung stellen. Verfügt ein Produkt mit digitalen Elementen über eine Benutzerschnittstelle oder ähnliche technische Mittel, die eine direkte Interaktion mit seinen Nutzern ermöglichen, so sollte der Hersteller diese Funktionen nutzen, um die Nutzer darüber zu informieren, dass ihr Produkt mit digitalen Elementen das Ende des Unterstützungszeitraums erreicht hat. Die Meldungen sollten sich auf das Maß beschränken, das erforderlich ist, um den tatsächlichen Empfang dieser Informationen sicherzustellen, und sie sollten sich nicht negativ auf das Nutzererlebnis des Produkts mit digitalen Elementen auswirken.

(57) Um die Verfahren zur Behandlung von Schwachstellen transparenter zu machen und um sicherzustellen, dass die Nutzer nicht gezwungen sind, neue Funktionsaktualisierungen zu installieren, nur um die neuesten Sicherheitsaktualisierungen zu erhalten, sollten die Hersteller dafür Sorge tragen, dass neue Sicherheitsaktualisierungen, soweit technisch machbar, getrennt von Funktionsaktualisierungen bereitgestellt werden.

(58) In der gemeinsamen Mitteilung der Kommission und des Hohen Vertreters der Union für Außen- und Sicherheitspolitik vom 20. Juni 2023 über eine „Europäische Strategie für wirtschaftliche Sicherheit“ heißt es, dass die Union durch einen gemeinsamen strategischen Rahmen für die wirtschaftliche Sicherheit der Union die Vorteile ihrer wirtschaftlichen Offenheit maximieren und gleichzeitig die Risiken aus wirtschaftlichen Abhängigkeiten von Anbietern mit hohem Risiko minimieren muss. Abhängigkeiten von risikoreichen Anbietern von Produkten mit digitalen Elementen können ein strategisches Risiko darstellen, das auf Unionsebene angegangen werden muss, insbesondere wenn die Produkte mit digitalen Elementen für die Verwendung durch die in Artikel 3 Absatz 1 der Richtlinie (EU) 2022/2555 genannten wesentlichen Einrichtungen bestimmt sind. Diese Risiken können unter anderem mit der für den Hersteller geltenden Gerichtsbarkeit, den Merkmalen seines Unternehmenseigentums und den von Kontrolle bestimmten Beziehungen zu der Regierung eines Drittlands, in dem er niedergelassen ist, zusammenhängen, insbesondere wenn das Drittland Wirtschaftsspionage betreibt oder unverantwortliches staatliches Verhalten im Cyberspace an den Tag legt und seine Gesetze einen willkürlichen Zugang zu Geschäftsvorgängen oder Unternehmensdaten jeglicher Art, einschließlich wirtschaftlich sensibler Daten, ermöglichen und unter Umständen nachrichtendienstliche Verpflichtungen auferlegen, ohne dass es demokratische Schutzmechanismen, Kontrollmechanismen, ordnungsgemäße Verfahren oder das Recht auf Anrufung eines unabhängigen Gerichts gibt. Bei der Bestimmung der Erheblichkeit eines Cybersicherheitsrisikos im Sinne dieser Verordnung sollten die Kommission und die Marktüberwachungsbehörden im Rahmen ihrer in dieser Verordnung

festgelegten Zuständigkeiten auch nichttechnische Risikofaktoren berücksichtigen, insbesondere solche, die als Ergebnis von koordinierten Risikobewertungen in Bezug auf die Sicherheit der Lieferketten auf Ebene der Union, die gemäß Artikel 22 der Richtlinie (EU) 2022/2555 durchgeführt werden, ermittelt wurden.

(59) Um für die Sicherheit von Produkten mit digitalen Elementen nach ihrem Inverkehrbringen zu sorgen, sollten die Hersteller den Unterstützungszeitraum festlegen, der der voraussichtlichen Nutzungsdauer des Produkts mit digitalen Elementen Rechnung tragen sollte. Bei der Festlegung eines Unterstützungszeitraums sollte ein Hersteller insbesondere die berechtigten Erwartungen der Nutzer, die Art des Produkts sowie das einschlägige Unionsrecht zur Festlegung der Lebensdauer von Produkten mit digitalen Elementen berücksichtigen. Die Hersteller sollten auch andere relevante Faktoren berücksichtigen können. Die Kriterien sollten so angewandt werden, dass die Verhältnismäßigkeit bei der Festlegung der Unterstützungszeiträume gegeben ist. Auf Anfrage sollte ein Hersteller den Marktüberwachungsbehörden die Informationen zur Verfügung stellen, die bei der Festlegung des Unterstützungszeitraums eines Produkts mit digitalen Elementen berücksichtigt wurden.

(60) Der Unterstützungszeitraum, für den der Hersteller die wirksame Behandlung von Schwachstellen gewährleistet, sollte mindestens fünf Jahre betragen, es sei denn, die Lebensdauer des Produkts mit digitalen Elementen beträgt weniger als fünf Jahre; in diesem Fall sollte der Hersteller die Behandlung von Schwachstellen für die entsprechende Lebensdauer sicherstellen. Wenn nach vernünftigem Ermessen davon auszugehen ist, dass das Produkt mit digitalen Elementen länger als fünf Jahre verwendet wird, wie dies häufig bei Hardwarekomponenten wie Hauptplatinen oder Mikroprozessoren, bei Netzwerkgeräten wie Routern, Modems oder Switches sowie bei Software wie Betriebssystemen oder Videobearbeitungstools der Fall ist, sollten die Hersteller dementsprechend längere Unterstützungszeiträume sicherstellen. Insbesondere Produkte mit digitalen Elementen, die für die Verwendung in industriellen Umgebungen bestimmt sind, wie etwa industrielle Steuerungssysteme, werden häufig über deutlich längere Zeiträume hinweg verwendet. Ein Hersteller sollte nur dann einen Unterstützungszeitraum von weniger als fünf Jahren festlegen können, wenn dies durch das Wesen des betreffenden Produkts mit digitalen Elementen gerechtfertigt ist und das Produkt voraussichtlich weniger als fünf Jahre in Verwendung sein wird; in diesem Fall sollte der Unterstützungszeitraum der erwarteten Nutzungsdauer entsprechen. Beispielsweise könnte die Lebensdauer einer Kontaktnachverfolgungs-App, die für die Nutzung während einer Pandemie bestimmt ist, auf die Dauer der Pandemie begrenzt werden. Darüber hinaus können einige Software-Anwendungen naturgemäß nur auf der Grundlage eines Abonnements zur Verfügung gestellt werden, insbesondere wenn die Anwendung nach Ablauf des Abonnements für den Nutzer nicht mehr zur Verfügung steht und folglich nicht mehr genutzt wird.

(61) Wenn bei Produkten mit digitalen Elementen das Ende des jeweiligen Unterstützungszeitraums erreicht ist, sollten die Hersteller in Erwägung ziehen, den Quellcode dieser Produkte mit digitalen Elementen entweder gegenüber anderen Unternehmen, die sich zu einer verlängerten Bereitstellung von Diensten zur Behandlung von Schwachstellen verpflichten, oder für die Öffentlichkeit freizugeben, damit Schwachstellen auch nach Ablauf des Unterstützungszeitraums behandelt werden können. Wenn Hersteller den Quellcode an andere Unternehmen weitergeben, sollten sie in der Lage sein, das Eigentumsrecht an dem Produkt mit digitalen Elementen zu schützen und die Weitergabe des Quellcodes an die Öffentlichkeit zu verhindern, etwa im Wege vertraglicher Vereinbarungen.

(62) Um sicherzustellen, dass die Hersteller in der gesamten Union vergleichbare Unterstützungszeiträume für vergleichbare Produkte mit digitalen Elementen festlegen, sollte die ADCO Statistiken über die von den Herstellern für Kategorien von Produkten mit digitalen Elementen festgelegten durchschnittlichen Unterstützungszeiträume veröffentlichen und Leitlinien herausgeben, in denen angemessene Unterstützungszeiträume für diese Kategorien angegeben sind. Darüber hinaus sollte die Kommission im Hinblick auf die Gewährleistung eines über den gesamten Binnenmarkt hinweg harmonisierten Ansatzes delegierte Rechtsakte erlassen können, um Mindestunterstützungszeiträume für bestimmte Produktkategorien festzulegen, wenn die von den Marktüberwachungsbehörden bereitgestellten Daten entweder darauf hindeuten, dass die von den Herstellern festgelegten Unterstützungszeiträume systematisch nicht den in dieser Verordnung festgelegten Kriterien für die Festlegung der Unterstützungszeiträume entsprechen, oder darauf hindeuten, dass Hersteller aus verschiedenen Mitgliedstaaten ungerechtfertigt unterschiedliche Unterstützungszeiträume festlegen.

(63) Die Hersteller sollten eine zentrale Anlaufstelle einrichten, die es den Nutzern ermöglicht, mühelos mit ihnen zu kommunizieren, etwa um Schwachstellen des Produkts mit digitalen Elementen zu melden und Informationen zu diesen Schwachstellen zu erhalten. Sie sollten die zentrale Anlaufstelle für die Nutzer leicht zugänglich und klare Angaben zu ihrer Erreichbarkeit machen und diese Informationen auf dem neuesten Stand halten. Wenn Hersteller sich dafür entscheiden, automatisierte Instrumente wie etwa Chatboxen anzubieten, sollten sie auch eine Telefonnummer oder andere digitale Kontaktmöglichkeiten wie eine E-Mail-Adresse oder ein Kontaktformular anbieten. Die zentrale Anlaufstelle sollte nicht ausschließlich auf automatisierten Instrumenten beruhen.

(64) Die Hersteller sollten ihre Produkte mit digitalen Elementen mit einer sicheren Standardkonfiguration auf dem Markt bereitstellen und den Nutzern kostenlos Sicherheitsaktualisierungen zur Verfügung stellen. Die Hersteller sollten von den grundlegenden Cybersicherheitsanforderungen nur abweichen können, wenn es sich um maßgeschneiderte Produkte handelt, die für einen bestimmten gewerblichen Nutzer auf einen bestimmten Zweck zugeschnitten sind und bei denen sowohl der Hersteller als auch der Nutzer ausdrücklich anderen Vertragsbedingungen zugestimmt haben.

(65) Aktiv ausgenutzte Schwachstellen in Produkten mit digitalen Elementen sowie schwerwiegende Sicherheitsvorfälle, die sich auf die Sicherheit dieser Produkte auswirken, sollten die Hersteller über die einheitliche Meldeplattform gleichzeitig sowohl dem als Koordinator benannten Computer Security Incident Response Team (CSIRT) als auch der ENISA melden. Die Meldungen sollten über den Endpunkt für die elektronische Meldung eines als Koordinator benannten CSIRT übermittelt werden und gleichzeitig der ENISA zugänglich sein.

(66) Die Hersteller sollten aktiv ausgenutzte Schwachstellen melden, um dafür zu sorgen, dass die als Koordinatoren benannten CSIRTs und die ENISA einen angemessenen Überblick über diese Schwachstellen haben und die Informationen erhalten, die sie benötigen, um ihre Aufgaben gemäß der Richtlinie (EU) 2022/2555 wahrzunehmen und das Gesamtniveau der Cybersicherheit wesentlicher und wichtiger Einrichtungen gemäß Artikel 3 der genannten Richtlinie zu erhöhen, und um das wirksame Funktionieren der Marktüberwachungsbehörden zu gewährleisten. 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. Im Einvernehmen mit dem Hersteller sollte die ENISA behobene Schwachstellen in der gemäß Artikel 12 Absatz 2 der Richtlinie (EU) 2022/2555 eingerichteten europäischen Schwachstellendatenbank offenlegen. Die europäische Schwachstellendatenbank wird die Hersteller dabei unterstützen, bekannte ausnutzbare Schwachstellen in ihren Produkten zu ermitteln, um sicherzustellen, dass auf dem Markt sichere Produkte bereitgestellt werden.

(67) Die Hersteller sollten dem als Koordinator benannten CSIRT und der ENISA auch jeden schwerwiegenden Sicherheitsvorfall melden, der sich auf die Sicherheit eines Produkts mit digitalen Elementen auswirkt. Damit die Nutzer rasch auf schwerwiegende Sicherheitsvorfälle reagieren können, die sich auf die Sicherheit ihrer Produkte mit digitalen Elementen auswirken, sollten die Hersteller auch ihre Nutzer über solche Sicherheitsvorfälle und gegebenenfalls über Korrekturmaßnahmen informieren, die die Nutzer ergreifen können, um die Auswirkungen des Sicherheitsvorfalls 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 Cybersicherheitsrisiken dies rechtfertigen, durch direkte Kontaktaufnahme zu den Nutzern.

(68) Bei aktiv ausgenutzten Schwachstellen handelt es sich um Fälle, in denen ein Hersteller feststellt, dass eine Sicherheitsverletzung, die sich auf seine Nutzer oder andere natürliche oder juristische Personen auswirkt, darauf zurückzuführen ist, dass ein böswilliger Akteur einen Fehler in einem der Produkte mit digitalen Elementen nutzt, die vom Hersteller auf dem Markt bereitgestellt werden. Bei solchen Schwachstellen kann es sich beispielsweise um Schwächen in den Identifizierungs- und Authentifizierungsfunktionen eines Produkts handeln. Schwachstellen, die ohne böswillige Absicht bei in gutem Glauben ausgeführten Tests, Untersuchungen, Korrekturen oder Offenlegungen, die auf die Sicherheit und den Schutz des Systemeigners und seiner Nutzer abzielen, festgestellt werden, sollten nicht meldepflichtig sein. Schwerwiegende Sicherheitsvorfälle, die sich auf die Sicherheit des Produkts mit digitalen Elementen auswirken, beziehen sich hingegen auf Situationen, in denen ein Cybersicherheitsvorfall die Entwicklungs-, Herstellungs- oder Wartungsprozesse des Herstellers so beeinträchtigt, dass er zu einem erhöhten Cybersicherheitsrisiko für die Nutzer oder andere Personen führen könnte. Zu diesen schwerwiegenden Sicherheitsvorfällen gehört beispielsweise der Fall, dass ein Angreifer erfolgreich ein Schadprogramm in den Freigabekanal eingeschleust hat, über den der Hersteller Sicherheitsaktualisierungen für die Nutzer freigibt.

(69) Damit Meldungen rasch an alle einschlägigen als Koordinatoren benannten CSIRTs weitergeleitet werden können und die Hersteller in jeder Phase des Meldeverfahrens die Möglichkeit einer Einzelnotifizierung haben, sollte die ENISA eine einheitliche Meldeplattform mit nationalen Endpunkten für die elektronische Meldung einrichten. Der laufende Betrieb der einheitlichen Meldeplattform sollte von der ENISA gesteuert und aufrechterhalten werden. Die als Koordinatoren benannten CSIRTs sollten ihre jeweiligen Marktüberwachungsbehörden über gemeldete Schwachstellen oder Sicherheitsvorfälle unterrichten. Die einheitliche Meldeplattform sollte so gestaltet sein, dass die Vertraulichkeit der Meldungen gewahrt bleibt, wobei dies insbesondere für Schwachstellen gilt, für die noch keine Sicherheitsaktualisierung verfügbar ist. Darüber hinaus sollte die ENISA Verfahrensweisen für den sicheren und vertraulichen Umgang mit Informationen festlegen. Auf der Grundlage der von ihr erfassten Informationen sollte die ENISA alle zwei Jahre einen technischen Bericht über sich abzeichnende Trends in Bezug auf Cybersicherheitsrisiken bei Produkten mit digitalen Elementen erstellen und ihn der gemäß Artikel 14 der Richtlinie (EU) 2022/2555 eingesetzten Kooperationsgruppe vorlegen.

(70) Unter außergewöhnlichen Umständen und insbesondere auf Ersuchen des Herstellers sollte das als Koordinator benannte CSIRT, bei dem die Meldung zunächst eingeht, beschließen können, die Übermittlung über die einheitliche Meldeplattform an die anderen einschlägigen als Koordinatoren benannten CSIRTs aufzuschieben, wenn dies aus Gründen der Cybersicherheit und für einen unbedingt erforderlichen Zeitraum gerechtfertigt werden kann. Das als Koordinator benannte CSIRT sollte die ENISA unverzüglich über die Entscheidung zur Aufschiebung und die Gründe dafür sowie darüber informieren, wann es eine Weiterverbreitung beabsichtigt. Die Kommission sollte im Wege eines delegierten Rechtsakts technische Einzelheiten zu den Bedingungen ausarbeiten, unter denen Gründe der Cybersicherheit geltend gemacht werden könnten, und bei der Ausarbeitung des Entwurfs eines delegierten Rechtsakts mit dem gemäß Artikel 15 der Richtlinie (EU) 2022/2555 errichteten CSIRTs-Netzwerk und der ENISA zusammenarbeiten. Bei Gründen der Cybersicherheit kann es sich etwa um ein laufendes Verfahren zur koordinierten Offenlegung von Schwachstellen oder um Situationen handeln, in denen erwartet wird, dass ein Hersteller in Kürze eine Minderungsmaßnahme ergreift und die mit einer unmittelbaren Weiterleitung über die einheitliche Meldeplattform verbundenen Cybersicherheitsrisiken die mit dieser Weiterleitung einhergehenden

Vorteile überwiegen. Auf Ersuchen des als Koordinator benannten CSIRT sollte die ENISA in der Lage sein, das CSIRT bei der Geltendmachung von Gründen der Cybersicherheit im Zusammenhang mit der Aufschiebung der Weiterleitung der Meldung auf der Grundlage der Informationen zu unterstützen, die die ENISA von diesem CSIRT in Bezug auf die Entscheidung erhalten hat, eine Meldung aus diesen cybersicherheitsbezogenen Gründen zurückzuhalten. Darüber hinaus sollte die ENISA unter besonders außergewöhnlichen Umständen nicht alle Einzelheiten einer Meldung über eine aktiv ausgenutzte Schwachstelle gleichzeitig erhalten. Dies wäre der Fall, wenn der Hersteller in seiner Meldung angibt, dass die gemeldete Schwachstelle von einem böswilligen Akteur aktiv ausgenutzt wurde und dass sie nach den verfügbaren Informationen in keinem anderen Mitgliedstaat als dem des als Koordinator benannten CSIRT, dem der Hersteller die Schwachstelle gemeldet hat, ausgenutzt wurde, wenn eine unverzügliche Weiterverbreitung der Meldung über die Schwachstelle voraussichtlich zu einer Zuleitung von Informationen führen würde, deren Offenlegung den wesentlichen Interessen dieses Mitgliedstaats zuwiderliefe, oder wenn die gemeldete Schwachstelle aufgrund der Weiterverbreitung ein unmittelbares hohes Cybersicherheitsrisiko darstellen würde. In solchen Fällen erhält die ENISA nur gleichzeitigen Zugang zu der Information, dass der Hersteller eine Meldung getätigt hat, zu allgemeinen Informationen über das betreffende Produkt mit digitalen Elementen, zu den Informationen über die allgemeine Art der Ausnutzung und zu Informationen darüber, dass diese Sicherheitsgründe vom Hersteller geltend gemacht wurden und der vollständige Inhalt der Meldung daher zurückgehalten wird. Die vollständige Meldung sollte der ENISA und anderen einschlägigen als Koordinatoren benannten CSIRTs dann zur Verfügung gestellt werden, wenn das als Koordinator benannte CSIRT, das die Meldung ursprünglich erhält, feststellt, dass diese Sicherheitsgründe, die besonders außergewöhnliche Umstände im Sinne dieser Verordnung widerspiegeln, nicht mehr bestehen. Ist die ENISA auf der Grundlage der verfügbaren Informationen der Auffassung, dass ein Systemrisiko für die Sicherheit des Binnenmarkts besteht, sollte sie dem CSIRT, bei dem die Meldung eingegangen ist, empfehlen, die vollständige Meldung an die anderen als Koordinatoren benannten CSIRTs und an die ENISA selbst weiterzuleiten.

(71) Wenn Hersteller eine aktiv ausgenutzte Schwachstelle oder einen schwerwiegenden Sicherheitsvorfall melden, die bzw. der sich auf die Sicherheit des Produkts mit digitalen Elementen auswirkt, sollten sie angeben, für wie sensibel sie die gemeldeten Informationen halten. Das als Koordinator benannte CSIRT, das die Meldung ursprünglich erhält, sollte diese Informationen bei der Prüfung, ob die Meldung außergewöhnliche Umstände nahelegt, die eine Aufschiebung der Weiterleitung der Meldung an die anderen einschlägigen als Koordinatoren benannten CSIRTs aus berechtigten Gründen der Cybersicherheit rechtfertigen, berücksichtigen. Zudem sollte es diese Informationen bei der Beurteilung der Frage berücksichtigen, ob die Meldung über eine aktiv ausgenutzte Schwachstelle besonders außergewöhnliche Umstände nahelegt, die es rechtfertigen, dass die vollständige Meldung nicht gleichzeitig der ENISA zur Verfügung gestellt wird. Darüber hinaus sollten die als Koordinatoren benannten CSIRTs in der Lage sein, diese Informationen bei der Festlegung geeigneter Maßnahmen zur Minderung der Risiken, die sich aus den entsprechenden Schwachstellen und Sicherheitsvorfällen ergeben, zu berücksichtigen.

(72) Um die im Rahmen dieser Verordnung vorgeschriebene Meldung von Informationen unter Berücksichtigung anderer ergänzender Meldepflichten, die im Unionsrecht etwa in der Verordnung (EU) 2016/679, der Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates ([25]), der Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates ([26]) und der Richtlinie (EU) 2022/2555 festgelegt sind, zu vereinfachen und den Verwaltungsaufwand für Einrichtungen zu verringern, wird den Mitgliedstaaten nahegelegt, die Einrichtung zentraler Anlaufstellen für solche Meldepflichten auf nationaler Ebene in Erwägung zu ziehen. Die Nutzung solcher nationalen zentralen Anlaufstellen für die Meldung von Sicherheitsvorfällen gemäß der Verordnung (EU) 2016/679 und der Richtlinie 2002/58/EG sollte die Anwendung der Bestimmungen der Verordnung (EU) 2016/679 und der Richtlinie 2002/58/EG, insbesondere der Bestimmungen über die Unabhängigkeit der darin genannten Behörden, unberührt lassen. Bei der Einrichtung der in dieser Verordnung genannten einheitlichen Meldeplattform sollte die ENISA der Möglichkeit Rechnung tragen, dass die in dieser Verordnung genannten nationalen Endpunkte für die elektronische Meldung in nationale zentrale Anlaufstellen integriert werden können, die auch andere nach dem Unionsrecht erforderliche Meldungen umfassen können.

(73) Um sich Erfahrungen aus der Vergangenheit zunutze zu machen, sollte die ENISA bei der Einrichtung der in dieser Verordnung genannten einheitlichen Meldeplattform andere Organe oder Agenturen der Union konsultieren, die Plattformen oder Datenbanken verwalten, die strengen Sicherheitsanforderungen unterliegen, wie etwa die Agentur der Europäischen Union für das Betriebsmanagement von IT-Großsystemen im Raum der Freiheit, der Sicherheit und des Rechts (eu-LISA). Außerdem sollte die ENISA mögliche Komplementaritäten mit der gemäß Artikel 12 Absatz 2 der Richtlinie (EU) 2022/2555 eingerichteten europäischen Schwachstellendatenbank prüfen.

(74) Hersteller und andere natürliche und juristische Personen sollten in der Lage sein, einem als Koordinator benannten CSIRT oder der ENISA auf freiwilliger Basis jedwede in einem Produkt mit digitalen Elementen enthaltene

([25]) Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über die digitale operationale Resilienz im Finanzsektor und zur Änderung der Verordnungen (EG) Nr. 1060/2009, (EU) Nr. 648/2012, (EU) Nr. 600/2014, (EU) Nr. 909/2014 und (EU) 2016/1011 (ABl. L 333 vom 27.12.2022, S. 1).

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

Schwachstelle, Cyberbedrohungen, die sich auf das Risikoprofil eines Produkts mit digitalen Elementen auswirken könnten, jedweden Sicherheitsvorfall, der sich auf die Sicherheit des Produkts mit digitalen Elementen auswirkt, sowie Beinahe-Vorfälle, die zu einem solchen Sicherheitsvorfall hätten führen können, zu melden.

(75) Die Mitgliedstaaten sollten im Einklang mit den nationalen Rechtsvorschriften so weit wie möglich die Herausforderungen angehen, mit denen Forscher, die sich mit Schwachstellen befassen, konfrontiert sind, wobei hierzu auch deren potenzielle strafrechtliche Haftung gehört. Da natürliche und juristische Personen, die Schwachstellen erforschen, in einigen Mitgliedstaaten der strafrechtlichen und zivilrechtlichen Haftung unterliegen könnten, werden die Mitgliedstaaten aufgefordert, Leitlinien für die Nichtverfolgung von Forschern im Bereich der Informationssicherheit zu verabschieden und eine Ausnahme von der zivilrechtlichen Haftung für ihre Tätigkeiten zu erlassen.

(76) Die 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 entweder direkt an den Hersteller oder indirekt und auf Wunsch anonym über die CSIRTs zu erleichtern, die gemäß Artikel 12 Absatz 1 der Richtlinie (EU) 2022/2555 als Koordinatoren für die Zwecke der koordinierten Offenlegung von Schwachstellen benannt werden. Das Konzept der Hersteller 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. Darüber hinaus sollten die Hersteller auch in Erwägung ziehen, ihre Sicherheitskonzepte in maschinenlesbarem Format zu veröffentlichen. 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 schaffen, indem sie dafür sorgen, dass natürliche oder juristische Personen Anerkennung und Belohnung für ihre Bemühungen erhalten. Hierbei handelt es sich um sogenannte „Bug-Bounty-Programme“.

(77) 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. Über eine Software-Stückliste können denjenigen, die Software herstellen, kaufen und betreiben, Informationen bereitgestellt werden, die ihnen helfen, die Lieferkette besser zu verstehen, was zahlreiche Vorteile mit sich bringt und insbesondere Herstellern und Nutzern hilft, bekannte neu aufgetretene Schwachstellen und Cybersicherheitsrisiken zu verfolgen. Besonders wichtig ist es, dass die Hersteller sicherstellen, dass ihre Produkte mit digitalen Elementen keine anfälligen Komponenten enthalten, die von Dritten entwickelt wurden. Die Hersteller sollten nicht verpflichtet sein, die Software-Stückliste zu veröffentlichen.

(78) Im Rahmen der neuen komplexen Geschäftsmodelle im Zusammenhang mit Online-Verkäufen kann ein online tätiges Unternehmen eine Vielzahl von Dienstleistungen anbieten. Je nach Art der in Bezug auf ein bestimmtes Produkt mit digitalen Elementen erbrachten Dienstleistungen kann ein und dasselbe Unternehmen in verschiedene Kategorien von Geschäftsmodellen oder Wirtschaftsakteuren fallen. Erbringt ein Unternehmen ausschließlich Online-Vermittlungsdienste für ein bestimmtes Produkt mit digitalen Elementen und handelt es sich bei diesem Unternehmen lediglich um einen Anbieter eines Online-Marktplatzes im Sinne von Artikel 3 Nummer 14 der Verordnung (EU) 2023/988, so fällt es nicht in eine der Kategorien von Wirtschaftsakteuren im Sinne dieser Verordnung. Handelt es sich bei einem Unternehmen um einen Anbieter eines Online-Marktplatzes, der beim Verkauf bestimmter Produkte mit digitalen Elementen zudem als Wirtschaftsakteur im Sinne dieser Verordnung fungiert, so sollte es den für diese Art von Wirtschaftsakteur in dieser Verordnung festgelegten Verpflichtungen unterliegen. Vertreibt beispielsweise der Anbieter eines Online-Marktplatzes auch ein Produkt mit digitalen Elementen, so wird er in Bezug auf den Verkauf dieses Produkts als Händler betrachtet. Ebenso würde das betreffende Unternehmen, wenn es seine eigenen Markenprodukte mit digitalen Elementen verkauft, als Hersteller gelten und müsste somit die für Hersteller geltenden Anforderungen erfüllen. Darüber hinaus können einige Unternehmen als Fulfilment-Dienstleister im Sinne von Artikel 3 Nummer 11 der Verordnung (EU) 2019/1020 des Europäischen Parlaments und des Rates ([27]) gelten, wenn sie die entsprechenden Dienstleistungen anbieten. Die betreffenden Fälle müssten im Einzelfall bewertet werden. Angesichts der herausragenden Rolle, die Online-Marktplätze bei der Ermöglichung des elektronischen Geschäftsverkehrs spielen, sollten diese bestrebt sein, mit den Marktüberwachungsbehörden der Mitgliedstaaten zusammenzuarbeiten, um dazu beizutragen, dass über Online-Marktplätze erworbene Produkte mit digitalen Elementen die in dieser Verordnung festgelegten Cybersicherheitsanforderungen erfüllen.

(79) 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 in dieser Verordnung festgelegten grundlegenden Cybersicherheitsanforderungen in detaillierte technische Spezifikationen umgesetzt werden und die gemäß der Verordnung (EU) Nr. 1025/2012 des Europäischen

([27]) 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).

Parlaments und des Rates ([28]) angenommen wurden. Die genannte Verordnung enthält ein Verfahren für Einwände gegen harmonisierte Normen für den Fall, dass diese Normen den in der vorliegenden Verordnung festgelegten Anforderungen nicht in vollem Umfang entsprechen. Im Rahmen des Normierungsprozesses sollte eine ausgewogene Interessenvertretung und eine wirksame Einbeziehung von Interessenträgern der Zivilgesellschaft, darunter von Verbraucherorganisationen, sichergestellt werden. Internationale Normen, die mit dem Cybersicherheitsschutzniveau, das mit den in dieser Verordnung festgelegten grundlegenden Cybersicherheitsanforderungen angestrebt wird, im Einklang stehen, sollten ebenfalls berücksichtigt werden, um die Entwicklung harmonisierter Normen und die Durchführung dieser Verordnung zu unterstützen und Unternehmen, insbesondere Kleinstunternehmen, kleinen und mittleren Unternehmen sowie weltweit tätigen Unternehmen, die Konformität zu erleichtern.

(80) Die rechtzeitige Entwicklung harmonisierter Normen während des Übergangszeitraums für die Anwendung dieser Verordnung und ihre Verfügbarkeit vor dem Geltungsbeginn dieser Verordnung werden für ihre wirksame Umsetzung besonders wichtig sein. Insbesondere ist dies bei wichtigen Produkten mit digitalen Elementen der Klasse I der Fall. Die Verfügbarkeit harmonisierter Normen wird es den Herstellern der entsprechenden Produkte ermöglichen, die Konformitätsbewertungen im Wege des internen Kontrollverfahrens durchzuführen, und kann so dazu beitragen, Engpässe und Verzögerungen bei den Tätigkeiten von Konformitätsbewertungsstellen zu umgehen.

(81) Mit der Verordnung (EU) 2019/881 ist ein freiwilliger europäischer Rahmen für die Cybersicherheitszertifizierung von IKT-Produkten, -Prozessen und -Diensten geschaffen worden. Die europäischen Schemata für die Cybersicherheitszertifizierung schaffen einen gemeinsamen Rahmen für das Vertrauen der Nutzer in die Verwendung von Produkten mit digitalen Elementen, die in den Anwendungsbereich der vorliegenden Verordnung fallen. Die vorliegende Verordnung sollte folglich Synergieeffekte 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 im Rahmen eines von der Kommission in einem Durchführungsrechtsakt festgelegten europäischen Cybersicherheitsschemas gemäß der Verordnung (EU) 2019/881 zertifiziert worden sind oder für die im Rahmen eines solchen Schemas eine Konformitätserklärung ausgestellt wurde, davon ausgegangen, dass sie den in der vorliegenden Verordnung festgelegten grundlegenden Cybersicherheitsanforderungen genügen, sofern das europäische Cybersicherheitszertifikat oder die Konformitätserklärung oder Teile davon diese Anforderungen abdecken. Die Notwendigkeit neuer europäischer Schemata für die Cybersicherheitszertifizierung von Produkten mit digitalen Elementen sollte im Lichte der vorliegenden Verordnung geprüft werden, auch bei der Ausarbeitung des fortlaufenden Arbeitsprogramms der Union gemäß der Verordnung (EU) 2019/881. Wenn ein neues Schema für Produkte mit digitalen Elementen erforderlich ist, um etwa die Einhaltung dieser Verordnung zu erleichtern, kann die Kommission die ENISA gemäß Artikel 48 der Verordnung (EU) 2019/881 ersuchen, mögliche Schemata auszuarbeiten. Solche künftigen europäischen Schemata für die Cybersicherheitszertifizierung von Produkten mit digitalen Elementen sollten den in dieser Verordnung festgelegten grundlegenden Cybersicherheitsanforderungen und Konformitätsbewertungsverfahren Rechnung tragen und die Einhaltung dieser Verordnung erleichtern. Für europäische Schemata für die Cybersicherheitszertifizierung, die vor dem Inkrafttreten dieser Verordnung in Kraft treten, können weitere Spezifikationen zu detaillierten Aspekten bezüglich der Anwendung einer Konformitätsvermutung erforderlich sein. Der Kommission sollte die Befugnis übertragen werden, im Wege von delegierten Rechtsakten festzulegen, unter welchen Bedingungen die europäischen Schemata für die Cybersicherheitszertifizierung zum Nachweis der Konformität mit den in dieser Verordnung festgelegten grundlegenden Cybersicherheitsanforderungen verwendet werden können. Um einen übermäßigen Verwaltungsaufwand zu vermeiden, sollten die Hersteller darüber hinaus nicht verpflichtet sein, für die betreffenden Anforderungen eine Konformitätsbewertung durch Dritte, wie in dieser Verordnung vorgesehen, durchzuführen zu lassen, wenn im Rahmen solcher europäischen Schemata für die Cybersicherheitszertifizierung ein europäisches Cybersicherheitszertifikat mindestens für die Stufe „mittel“ ausgestellt wurde.

(82) Beim Inkrafttreten der Durchführungsverordnung (EU) 2024/482, die in den Anwendungsbereich dieser Verordnung fallende Produkte wie Hardware-Sicherheitsmodule und Mikroprozessoren betrifft, sollte die Kommission im Wege eines delegierten Rechtsakts festlegen können, auf welche Weise das EUCC eine Vermutung der Konformität mit den in dieser Verordnung festgelegten grundlegenden Cybersicherheitsanforderungen oder Teilen davon begründen kann. Darüber hinaus kann in einem solchen delegierten Rechtsakt festgelegt werden, wie mit einem im Rahmen des EUCC ausgestellten Zertifikat die in dieser Verordnung vorgesehene Pflicht der Hersteller, eine Bewertung durch Dritte durchführen zu lassen, für die betreffenden Anforderungen aufgehoben werden kann.

(83) Der bestehende europäische Normungsrahmen, dem die Grundsätze der neuen Konzeption gemäß der Entschließung des Rates vom 7. Mai 1985 über eine neue Konzeption auf dem Gebiet der technischen Harmonisierung und der Normung und die Verordnung (EU) Nr. 1025/2012 zugrunde liegen, bildet den Standardrahmen für die Ausarbeitung von Normen, die eine Konformitätsvermutung mit den in dieser Verordnung festgelegten einschlägigen grundlegenden Cybersicherheitsanforderungen vorsehen. Europäische Normen sollten marktorientiert sein, dem öffentlichen Interesse sowie den politischen Zielen Rechnung tragen, die im Auftrag der Kommission an eine oder mehrere europäische Normungsorganisationen, innerhalb einer bestimmten Frist harmonisierte Normen auszuarbeiten, präzise dargelegt sind, und auf Konsens beruhen. In Ermangelung

([28]) 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).

einschlägiger Verweise auf harmonisierte Normen sollte die Kommission jedoch die Möglichkeit haben, in Ausnahmefällen als Ausweichlösung und unter gebührender Achtung der Rolle und der Aufgaben der europäischen Normungsorganisationen Durchführungsrechtsakte zu erlassen, in denen gemeinsame Spezifikationen für die in dieser Verordnung festgelegten grundlegenden Cybersicherheitsanforderungen festgelegt werden, um es dem Hersteller zu erleichtern, seiner Pflicht zur Einhaltung dieser grundlegenden Cybersicherheitsanforderungen nachzukommen, wenn das Normungsverfahren blockiert ist oder wenn es bei der Ausarbeitung angemessener harmonisierter Normen zu Verzögerungen kommt. Ist eine solche Verzögerung auf die technische Komplexität der betreffenden Norm zurückzuführen, so sollte die Kommission dies berücksichtigen, bevor sie die Festlegung gemeinsamer Spezifikationen in Erwägung zieht.

(84) Um bei der Festlegung gemeinsamer Spezifikationen, die die in dieser Verordnung genannten grundlegenden Cybersicherheitsanforderungen abdecken, möglichst effizient vorzugehen, sollte die Kommission einschlägige Interessenträger in den Prozess einbeziehen.

(85) Unter einer angemessenen Frist ist in Bezug auf die Veröffentlichung der Fundstelle harmonisierter Normen im *Amtsblatt der Europäischen Union* gemäß der Verordnung (EU) Nr. 1025/2012 ein Zeitraum zu verstehen, in dem die Fundstelle der Norm, ihre Berichtigung oder ihre Änderung voraussichtlich im *Amtsblatt der Europäischen Union* veröffentlicht wird und der ein Jahr nach Ablauf der Frist für die Erstellung des Entwurfs einer europäischen Norm gemäß der Verordnung (EU) Nr. 1025/2012 nicht überschreiten sollte.

(86) Um die Bewertung der Konformität mit den in dieser Verordnung festgelegten grundlegenden Cybersicherheitsanforderungen zu erleichtern, sollte eine Konformitätsvermutung für Produkte mit digitalen Elementen gelten, die den gemeinsamen Spezifikationen entsprechen, die die Kommission gemäß dieser Verordnung angenommen hat, um ausführliche technische Spezifikationen für diese Anforderungen zu formulieren.

(87) Die Anwendung harmonisierter Normen, gemeinsamer Spezifikationen oder europäischer Schemata für die Cybersicherheitszertifizierung, die gemäß der Verordnung (EU) 2019/881 angenommen wurden und bei denen eine Konformitätsvermutung in Bezug auf die grundlegenden Cybersicherheitsanforderungen an Produkte mit digitalen Elementen besteht, wird die Konformitätsbewertung durch die Hersteller erleichtern. Entscheidet sich der Hersteller gegen die Verwendung dieser Mittel für bestimmte Anforderungen, so muss er in seinen technischen Unterlagen angeben, wie die Konformität auf andere Weise erreicht wird. Darüber hinaus würde die Anwendung harmonisierter Normen, gemeinsamer Spezifikationen oder europäischer Schemata für die Cybersicherheitszertifizierung, die gemäß der Verordnung (EU) 2019/881 angenommen wurden, durch die Begründung einer Konformitätsvermutung für die Hersteller die Überprüfung der Konformität von Produkten mit digitalen Elementen durch die Marktüberwachungsbehörden erleichtern. Daher werden die Hersteller von Produkten mit digitalen Elementen angehalten, diese harmonisierten Normen, gemeinsamen Spezifikationen oder europäischen Schemata für die Cybersicherheitszertifizierung anzuwenden.

(88) 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 in dieser Verordnung festgelegten grundlegenden Cybersicherheitsanforderungen und gegebenenfalls den sonstigen einschlägigen Harmonisierungsrechtsvorschriften der Union, denen das Produkt mit digitalen Elementen unterliegt, hervorgehen. Die Hersteller können ferner auch aufgrund anderer Rechtsakte 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 auf die Einhaltung aller einschlägigen Rechtsakte 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.

(89) 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 ([29]) 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 in dieser Verordnung festgelegten Anforderungen garantiert.

(90) Damit die Wirtschaftsakteure die Konformität mit den in dieser Verordnung festgelegten grundlegenden Cybersicherheitsanforderungen 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 ([30]) sind Module für Konformitätsbewertungsverfahren festgelegt, die der Höhe des Risikos und dem geforderten Sicherheitsniveau angemessen sind. Um die sektorübergreifende Kohärenz zu gewährleisten und

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

([30]) 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).

Ad-hoc-Varianten zu vermeiden, sollten die Konformitätsbewertungsverfahren zur Überprüfung der Konformität von Produkten mit digitalen Elementen mit den in dieser Verordnung festgelegten grundlegenden Cybersicherheitsanforderungen auf diesen Modulen beruhen. 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 mit digitalen Elementen.

(91) Die Konformitätsbewertung von Produkten mit digitalen Elementen, die in dieser Verordnung nicht als wichtige oder kritische Produkte mit digitalen Elementen aufgeführt sind, kann vom Hersteller in eigener Verantwortung nach dem internen Kontrollverfahren auf der Grundlage von Modul A des Beschlusses Nr. 768/2008/EG gemäß dieser Verordnung durchgeführt werden. Dies gilt auch für Fälle, in denen ein Hersteller beschließt, eine geltende harmonisierte Norm, eine gemeinsame Spezifikation oder ein europäisches Schema für die Cybersicherheitszertifizierung ganz oder teilweise nicht anzuwenden. Dem Hersteller bleibt freigestellt, ein strengeres Konformitätsbewertungsverfahren unter Einbeziehung eines Dritten zu wählen. Im Rahmen der nach dem internen Kontrollverfahren durchgeführten Konformitätsbewertung stellt der Hersteller sicher und erklärt er auf eigene Verantwortung, dass das Produkt mit digitalen Elementen und die Prozesse des Herstellers die in dieser Verordnung festgelegten geltenden grundlegenden Cybersicherheitsanforderungen erfüllen. Fällt ein wichtiges Produkt mit digitalen Elementen in die Klasse I, so ist eine zusätzliche Vertrauenswürdigkeitsprüfung erforderlich, um die Konformität mit den in dieser Verordnung festgelegten grundlegenden Cybersicherheitsanforderungen nachzuweisen. Der Hersteller sollte harmonisierte Normen, gemeinsame Spezifikationen oder europäische Schemata für die Cybersicherheitszertifizierung, die gemäß der Verordnung (EU) 2019/881 angenommen wurden und von der Kommission in einem Durchführungsrechtsakt ermittelt wurden, verwenden, wenn er die Konformitätsbewertung in eigener Verantwortung durchführen möchte (Modul A). Verwendet der Hersteller solche harmonisierten Normen, gemeinsamen Spezifikationen oder europäischen Schemata für die Cybersicherheitszertifizierung nicht, so sollte eine Konformitätsbewertung unter Beteiligung eines Dritten durchgeführt werden (basierend auf den Modulen B und C oder H). 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 wichtiger 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 wichtiger Produkte mit digitalen Elementen verbunden ist, die in die Klasse II fallen, sollte an deren Konformitätsbewertung stets ein Dritter beteiligt werden, auch wenn das Produkt vollständig oder teilweise harmonisierten Normen, gemeinsamen Spezifikationen oder europäischen Schemata für die Cybersicherheitszertifizierung entspricht. Hersteller wichtiger Produkte mit digitalen Elementen, die als freie und quelloffene Software gelten, sollten das interne Kontrollverfahren auf der Grundlage von Modul A anwenden können, sofern sie die technische Dokumentation der Öffentlichkeit zugänglich machen.

(92) 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 den Verkehr gebracht werden. Bei der Anwendung der einschlägigen Konformitätsbewertungsmodule zur Überprüfung der Konformität des Produkts mit den in dieser Verordnung festgelegten grundlegenden Cybersicherheitsanforderungen in der Konzeptions-, Entwicklungs- und Herstellungsphase sollten diese Tätigkeiten als dem Herstellungsprozess gleichkommende Tätigkeiten betrachtet werden.

(93) In Bezug auf Kleinstunternehmen und kleine Unternehmen ist es zur Sicherstellung von Verhältnismäßigkeit angezeigt, die Verwaltungskosten zu senken, ohne das Maß an Cybersicherheit von Produkten mit digitalen Elementen, die in den Anwendungsbereich dieser Verordnung fallen, oder das Vorliegen gleicher Wettbewerbsbedingungen zwischen den Herstellern zu beeinträchtigen. Daher sollte die Kommission ein vereinfachtes Formular für die technische Dokumentation erstellen, das auf die Bedürfnisse von Kleinst- und Kleinunternehmen zugeschnitten ist. Das von der Kommission angenommene vereinfachte Formular für die technische Dokumentation sollte alle anwendbaren Elemente im Zusammenhang mit der technischen Dokumentation gemäß dieser Verordnung abdecken und angeben, wie ein Kleinstunternehmen oder kleines Unternehmen die angeforderten Elemente in knapper Form bereitstellen kann, beispielsweise die Beschreibung der Gestaltung, Entwicklung und Herstellung des Produkts mit digitalen Elementen. Auf diese Weise würde das Formular dazu beitragen, die Verwaltungslast für die Einhaltung der Vorschriften zu verringern, indem den betroffenen Unternehmen Rechtssicherheit hinsichtlich des Umfangs und der Einzelheiten der bereitzustellenden Informationen geboten wird. Kleinstunternehmen und kleine Unternehmen sollten die Option haben, die anwendbaren Elemente im Zusammenhang mit der technischen Dokumentation in umfassender Form vorzulegen und das ihnen zur Verfügung stehende vereinfachte technische Formular nicht zu verwenden.

(94) Um Innovationen zu fördern und zu schützen, ist es wichtig, dass die Interessen von Herstellern, bei denen es sich um Kleinstunternehmen oder um kleine oder mittlere Unternehmen handelt, insbesondere von Kleinstunternehmen und Kleinunternehmen, einschließlich Start-up-Unternehmen, besondere Berücksichtigung finden. Zu diesem Zweck könnten die Mitgliedstaaten Initiativen entwickeln, die sich an Hersteller richten, bei denen es sich um Kleinstunternehmen oder kleine Unternehmen handelt, unter anderem in den Bereichen Schulung, Sensibilisierung, Kommunikation von Informationen, Tests, Konformitätsbewertung durch Dritte sowie Einrichtung von Reallaboren. Übersetzungskosten im Zusammenhang mit der verpflichtenden Dokumentation, beispielsweise der technischen Dokumentation, und den gemäß dieser Verordnung erforderlichen Informationen und Anweisungen für die Nutzer sowie mit der Kommunikation mit den Behörden können erhebliche Ausgaben für die Hersteller, insbesondere für Kleinhersteller, mit sich bringen. Daher sollten die Mitgliedstaaten auch prüfen können, ob eine der Sprachen, die sie für die einschlägige Dokumentation der Hersteller und für die Kommunikation mit den Herstellern bestimmen und akzeptieren, eine Sprache ist, die von der größtmöglichen Zahl von Nutzern weitgehend verstanden wird.

(95) Um für eine reibungslose Anwendung dieser Verordnung zu sorgen, sollten die Mitgliedstaaten vor dem Beginn der Anwendung dieser Verordnung möglichst sicherstellen, dass es eine ausreichende Zahl notifizierter Stellen gibt, die Konformitätsbewertungen durch Dritte durchführen können. Die Kommission sollte die Mitgliedstaaten und andere einschlägige Parteien bei diesem Unterfangen möglichst unterstützen, um Engpässe und Hindernisse beim Marktzugang von Herstellern zu verhindern. Gezielte Schulungsmaßnahmen unter der Leitung der Mitgliedstaaten, gegebenenfalls auch mit Unterstützung der Kommission, können zur Verfügbarkeit qualifizierter Fachkräfte und auch zur Unterstützung der Tätigkeiten notifizierter Stellen im Sinne dieser Verordnung beitragen. Darüber hinaus sollten angesichts der Kosten, die eine Konformitätsbewertung durch Dritte mit sich bringen kann, Finanzierungsinitiativen auf Unionsebene und auf nationaler Ebene in Betracht gezogen werden, die darauf abzielen, diese Kosten für Kleinstunternehmen und kleine Unternehmen zu verringern.

(96) Um die Verhältnismäßigkeit sicherzustellen, sollten die Konformitätsbewertungsstellen bei der Festlegung der Gebühren für die Verfahren der Konformitätsbewertung den besonderen Interessen und Bedürfnissen von Kleinstunternehmen sowie von kleinen und mittleren Unternehmen, einschließlich Start-up-Unternehmen, Rechnung tragen. Insbesondere sollten die Konformitätsbewertungsstellen die in dieser Verordnung vorgesehenen einschlägigen Prüfverfahren und Tests nur dann anwenden, wenn dies angemessen ist und ein risikobasierter Ansatz verfolgt wird.

(97) Die Ziele von Reallaboren sollten darin bestehen, Innovation und Wettbewerbsfähigkeit für Unternehmen zu fördern, indem vor dem Inverkehrbringen von Produkten mit digitalen Elementen kontrollierte Testumgebungen geschaffen werden. Reallabore sollten dazu beitragen, die Rechtssicherheit für alle Akteure, die in den Anwendungsbereich dieser Verordnung fallen, zu verbessern und den Zugang von Produkten mit digitalen Elementen zum Unionsmarkt zu erleichtern und zu beschleunigen, insbesondere wenn sie von Kleinstunternehmen und kleinen Unternehmen, einschließlich Start-up-Unternehmen, bereitgestellt werden.

(98) 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.

(99) Um für ein einheitliches Qualitätsniveau bei der Durchführung der Konformitätsbewertungen von Produkten 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.

(100) Konformitätsbewertungsstellen, die nach Unionsrecht akkreditiert und notifiziert wurden, in denen ähnliche Anforderungen wie in dieser Verordnung festgelegt sind, wie z. B. eine Konformitätsbewertungsstelle, die für ein gemäß der Verordnung (EU) 2019/881 angenommenes europäisches Schema für die Cybersicherheitszertifizierung oder gemäß der Delegierten Verordnung (EU) 2022/30 notifiziert wurde, sollten im Rahmen dieser Verordnung neu bewertet und notifiziert werden. Allerdings können die einschlägigen Behörden Synergien in Bezug auf sich überschneidende Anforderungen definieren, um unnötigen finanziellen und administrativen Aufwand zu vermeiden und ein reibungsloses und zeitnahes Notifizierungsverfahren sicherzustellen.

(101) 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 einschlägigen rechtlichen Anforderungen erfüllen.

(102) 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.

(103) 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. Das NANDO-Informationssystem ist das von der Kommission entwickelte und verwaltete elektronische Notifizierungsinstrument, mit dem eine Liste aller notifizierten Stellen geführt wird.

(104) 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.

(105) 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.

(106) Die Marktüberwachung ist ein wesentliches Instrument zur Gewährleistung der korrekten und einheitlichen Anwendung des Unionsrechts. Daher sollte ein Rechtsrahmen geschaffen werden, innerhalb dessen die Marktüberwachung in angemessener Weise erfolgen kann. Die Vorschriften der Verordnung (EU) 2019/1020 für die Überwachung des Unionsmarktes und die Kontrolle von Produkten, die auf den Unionsmarkt gelangen, gelten auch für Produkte mit digitalen Elementen, die in den Anwendungsbereich der vorliegenden Verordnung fallen.

(107) Nach der Verordnung (EU) 2019/1020 führt eine Marktüberwachungsbehörde die Marktüberwachung im Hoheitsgebiet des Mitgliedstaats, der sie benennt, durch. Diese Verordnung sollte die Mitgliedstaaten nicht daran hindern, zu entscheiden, welche Behörden für die Wahrnehmung der Marktüberwachungsaufgaben zuständig sind. Jeder Mitgliedstaat sollte in seinem Hoheitsgebiet eine oder mehrere Marktüberwachungsbehörden benennen. Die Mitgliedstaaten sollten beschließen können, eine bestehende oder eine neue Behörde als Marktüberwachungsbehörde zu benennen, einschließlich der gemäß Artikel 8 der Richtlinie (EU) 2022/2555 benannten oder eingesetzten zuständigen Behörden, der gemäß Artikel 58 der Verordnung (EU) 2019/881 benannten nationalen Behörden für die Cybersicherheitszertifizierung oder der im Sinne der Richtlinie 2014/53/EU benannten Marktüberwachungsbehörden. 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 Marktüberwachungsaufgaben im Zusammenhang mit der vorliegenden Verordnung verfügen. Gemäß 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.

(108) Im Hinblick auf die einheitliche Anwendung dieser Verordnung sollte gemäß Artikel 30 Absatz 2 der Verordnung (EU) 2019/1020 eine ADCO für die Cyberresilienz von Produkten mit digitalen Elementen eingesetzt werden. Die 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 gemäß Artikel 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 genannten Verordnung und eines optionalen nationalen Sachverständigen, sowie den Vorsitzenden der ADCO und Vertretern der Kommission zusammensetzt. Die Kommission sollte an den Sitzungen des Netzwerks der Union für Produktkonformität, seiner Untergruppen und der ADCO teilnehmen. Sie sollte die ADCO durch ein Exekutivsekretariat unterstützen, das technische und logistische Unterstützung leistet. Die ADCO kann auch unabhängige Sachverständige zur Teilnahme einladen und sich mit anderen ADCOs, beispielsweise derjenigen, die im Rahmen der Richtlinie 2014/53/EU eingerichtet wurde, in Verbindung setzen.

(109) Die Marktüberwachungsbehörden sollten über die im Rahmen dieser Verordnung eingerichtete ADCO eng zusammenarbeiten und in der Lage sein, Leitliniendokumente zu entwickeln, um die Marktüberwachungstätigkeiten auf nationaler Ebene zu erleichtern, beispielsweise durch die Entwicklung bewährter Verfahren und Indikatoren zur wirksamen Überprüfung der Konformität von Produkten mit digitalen Elementen mit dieser Verordnung.

(110) 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 bereitgestellt werden, in dessen Rahmen interessierte Kreise über geplante Maßnahmen in Bezug auf solche Produkte informiert werden. Auf diese Weise könnten die 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.

(111) 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, Authentizität, Integrität oder Vertraulichkeit von Diensten, die über ein elektronisches Informationssystem von wesentlichen Einrichtungen im Sinne von Artikel 3 Absatz 1 der Richtlinie (EU) 2022/2555 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 mit digitalen Elementen 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 mit digitalen Elementen, 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, sollte die Kommission auch Vorschläge zur Überarbeitung des einschlägigen Unionsrechts in Erwägung ziehen können.

(112) 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, für die Erfüllung der Pflichten aus dem Unionsrecht oder dem nationalen Recht zum Schutz der Grundrechte oder für die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit von Diensten, die über ein elektronisches Informationssystem von wesentlichen Einrichtungen im Sinne von Artikel 3 Absatz 1 der Richtlinie (EU) 2022/2555 angeboten werden, sollte die Kommission die ENISA ersuchen können, eine Bewertung vorzunehmen. Auf der Grundlage dieser Bewertung sollte die Kommission im Wege von Durchführungsrechtsakten Korrekturmaßnahmen oder einschränkende Maßnahmen auf Unionsebene erlassen können, einschließlich der Anordnung der Rücknahme der betroffenen Produkte mit digitalen Elementen vom Markt oder ihres Rückrufs innerhalb einer der Art des Risikos angemessenen Frist. Ein solches Eingreifen der Kommission sollte nur unter außergewöhnlichen Umständen möglich sein, die ein sofortiges Eingreifen zur Bewahrung des reibungslosen Funktionierens des Binnenmarkts rechtfertigen, und nur dann, wenn die Marktüberwachungsbehörden keine wirksamen Maßnahmen ergriffen haben, um Abhilfe zu schaffen. Solche außergewöhnlichen Umstände können Notfälle sein, in denen beispielsweise ein nichtkonformes Produkt mit digitalen Elementen 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 (EU) 2022/2555 fallen, und es bekannte Schwachstellen aufweist, die von böswilligen Akteuren ausgenutzt werden und für die der Hersteller keine verfügbaren Patches bereitstellt. Die Kommission sollte in solchen Notfällen nur während der Dauer der außergewöhnlichen Umstände und nur solange eingreifen können, wie die Nichtkonformität mit dieser Verordnung oder die großen Risiken fortbestehen.

(113) Gibt es Hinweise auf eine Nichtkonformität mit dieser Verordnung in mehreren Mitgliedstaaten, so 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.

(114) 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 Kategorien von Produkten mit digitalen Elementen häufig Cybersicherheitsrisiken aufweisen. Darüber hinaus sollten die Marktüberwachungsbehörden bei der Festlegung der Produktkategorien, die Sweeps zu unterziehen sind, auch die Umstände im Zusammenhang mit nichttechnischen Risikofaktoren berücksichtigen. Zu diesem Zweck sollten die Marktüberwachungsbehörden in der Lage sein, die Ergebnisse der gemäß Artikel 22 der Richtlinie (EU) 2022/2555 koordinierten Risikobewertungen in Bezug auf die Sicherheit kritischer Lieferketten auf Ebene der Union, darunter die Umstände in Bezug auf nichttechnische Risikofaktoren, zu berücksichtigen. Die ENISA sollte den Marktüberwachungsbehörden Vorschläge für Kategorien von Produkten mit digitalen Elementen vorlegen, für die Sweeps organisiert werden könnten, und zwar unter anderem auf der Grundlage der bei ihr eingegangenen Meldungen über Schwachstellen und Sicherheitsvorfälle.

(115) Angesichts ihrer Sachkenntnis und ihres Auftrags sollte die ENISA in der Lage sein, den Prozess der Durchführung dieser Verordnung zu unterstützen. Die ENISA 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 Sweeps 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.

(116) Mit dieser Verordnung werden der ENISA bestimmte Aufgaben übertragen, die angemessene Ressourcen sowohl in Bezug auf Sachkenntnis als auch auf Humanressourcen erfordern, damit die ENISA in die Lage versetzt wird, diese Aufgaben wirksam wahrzunehmen. Bei der Ausarbeitung des Entwurfs des Gesamthaushaltsplans der Union wird die Kommission gemäß dem in Artikel 29 der Verordnung (EU) 2019/881 festgelegten Verfahren die erforderlichen Haushaltsmittel für den Stellenplan der ENISA vorschlagen. Während dieses Prozesses wird die Kommission die Gesamtressourcen der ENISA berücksichtigen, um sie in die Lage zu versetzen, ihre Aufgaben wahrzunehmen, auch diejenigen, die ihr gemäß dieser Verordnung übertragen wurden.

(117) Damit der Rechtsrahmen erforderlichenfalls angepasst werden kann, sollte der Kommission die Befugnis übertragen werden, gemäß Artikel 290 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV) Rechtsakte hinsichtlich der Aktualisierung der Liste wichtiger Produkte mit digitalen Elementen und deren Aufnahme in den Anhang der vorliegenden Verordnung zu erlassen. 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 von in einem Anhang der vorliegenden Verordnung dargelegten kritischen Produkten mit digitalen Elementen im Rahmen eines europäischen Schemas für die Cybersicherheitszertifizierung vorzuschreiben, um die Liste kritischer Produkte mit digitalen Elementen auf der Grundlage der in dieser Verordnung festgelegten Kritikalitätskriterien zu aktualisieren und um die gemäß der Verordnung (EU) 2019/881 erlassenen europäischen Systeme für die Cybersicherheitszertifizierung festzulegen, die zum Nachweis der Konformität mit den grundlegenden Cybersicherheitsanforderungen oder Teilen davon gemäß einem Anhang der vorliegenden Verordnung verwendet werden können. Der Kommission sollte auch die Befugnis übertragen werden, Rechtsakte zu erlassen, um für bestimmte Produktkategorien den Mindestzeitraum für die Unterstützung zu bestimmen, wenn die Marktüberwachungsdaten auf unzureichende Unterstützungszeiträume hindeuten, und um die Geschäftsbedingungen für die Anwendung der Gründe in Bezug auf das Cybersicherheitsrisiko festzulegen, wenn Meldungen über aktiv ausgenutzte Schwachstellen nur verzögert weitergegeben werden. Darüber hinaus sollte der Kommission die Befugnis übertragen werden, Rechtsakte zu erlassen, um freiwillige Programme zur Bescheinigung der Sicherheit zwecks Bewertung der Konformität von Produkten mit digitalen Elementen, die als freie und quelloffene Software gelten, mit allen oder bestimmten grundlegenden Cybersicherheitsanforderungen oder anderweitigen in dieser Verordnung aufgeführten Pflichten festzulegen sowie um die Mindestangaben für die EU-Konformitätserklärung vorzuschreiben und die in die technische Dokumentation aufzunehmenden Elemente zu ergänzen. Es ist von besonderer Bedeutung, dass die Kommission im Zuge ihrer Vorbereitungsarbeit angemessene Konsultationen, auch auf der Ebene von Sachverständigen, durchführt, die mit den Grundsätzen in Einklang stehen, die in der Interinstitutionellen Vereinbarung vom 13. April 2016 über bessere Rechtsetzung ([31]) festgelegt 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. Die Befugnis zum Erlass delegierter Rechtsakte gemäß dieser Verordnung wird der Kommission für einen Zeitraum von fünf Jahren ab dem 10. Dezember 2024 übertragen. Die Kommission sollte spätestens neun Monate vor Ablauf des Zeitraums von fünf Jahren einen Bericht über die Befugnisübertragung erstellen. Die Befugnisübertragung sollte sich stillschweigend um Zeiträume gleicher Länge verlängern, es sei denn, das Europäische Parlament oder der Rat widersprechen einer solchen Verlängerung spätestens drei Monate vor Ablauf des jeweiligen Zeitraums.

(118) Zur Gewährleistung einheitlicher Bedingungen für die Durchführung dieser Verordnung sollten der Kommission Durchführungsbefugnisse in Bezug auf Folgendes übertragen werden: Festlegung der technischen Beschreibung der in einem Anhang dieser Verordnung aufgeführten Kategorien wichtiger Produkte mit digitalen Elementen, Festlegung des Formats und der Elemente der Software-Stückliste, Präzisierung des Formats und des Verfahrens der Meldungen über aktiv ausgenutzte Schwachstellen und schwerwiegende Sicherheitsvorfälle, die sich auf die Sicherheit von Produkten mit digitalen Elementen, wie sie von den Herstellern übermittelt wurde, auswirken, Festlegung gemeinsamer Spezifikationen für technische Anforderungen, mit deren Hilfe den grundlegenden Cybersicherheitsanforderungen in einem Anhang dieser Verordnung genügt wird, Festlegung technischer Spezifikationen für Etiketten, Piktogramme oder andere Kennzeichnungen in Bezug auf die Sicherheit von Produkten mit digitalen Elementen und deren Unterstützungszeitraum sowie Mechanismen zur Förderung ihrer Verwendung und zur

([31]) ABl. L 123 vom 12.5.2016, S. 1.

Sensibilisierung der Öffentlichkeit für die Sicherheit von Produkten mit digitalen Elementen, Festlegung des vereinfachten Formulars für die Dokumentation, das auf die Bedürfnisse von Kleinstunternehmen und kleinen Unternehmen zugeschnitten ist, sowie 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 ([32]) ausgeübt werden.

(119) 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.

(120) 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 im einzelstaatlichen Recht 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 es sich bei dem Hersteller um ein Kleinstunternehmen oder um ein kleines oder mittleres Unternehmen, einschließlich eines Start-up-Unternehmens, handelt und ob bereits dieselbe Marktüberwachungsbehörde oder andere Marktüberwachungsbehörden demselben Wirtschaftsakteur für einen ähnlichen Verstoß Geldbußen auferlegt haben. Solche Umstände könnten entweder erschwerend wirken, falls der Verstoß desselben Wirtschaftsakteurs 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. Da Geldbußen weder gegen Kleinstunternehmen oder kleine Unternehmen wegen einer Nichteinhaltung der 24-Stunden-Frist für die Frühmeldung bei aktiv ausgenutzten Schwachstellen oder schwerwiegenden Sicherheitsvorfällen, die sich auf die Sicherheit des Produkts mit digitalen Elementen auswirken, noch gegen Verwalter quelloffener Software bei Verstößen gegen diese Verordnung verhängt werden und vorbehaltlich des Grundsatzes, dass Sanktionen wirksam, verhältnismäßig und abschreckend sein sollten, sollten die Mitgliedstaaten gegen diese Einrichtungen keine anderweitigen finanziellen Sanktionen verhängen.

(121) Werden Geldbußen einer Person auferlegt, bei der es sich nicht um ein Unternehmen handelt, so sollte die zuständige Behörde bei der Bemessung der Geldbuße dem 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.

(122) Die Mitgliedstaaten sollten unter Berücksichtigung der nationalen Gegebenheiten prüfen, ob die Einnahmen aus den in dieser Verordnung vorgesehenen Sanktionen oder entsprechende gleichwertige Einnahmen verwendet werden können, um Cybersicherheitsstrategien zu unterstützen und das Maß an Cybersicherheit in der Union zu verbessern, indem unter anderem die Anzahl der qualifizierten Cybersicherheitsfachkräfte erhöht, der Kapazitätsaufbau für Kleinstunternehmen sowie kleine und mittlere Unternehmen gestärkt und die Öffentlichkeit für Cyberbedrohungen sensibilisiert wird.

(123) In ihren Beziehungen mit Drittländern strebt die Union 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 Drittländern. Diese Abkommen werden für eine Reihe bestimmter Sektoren geschlossen, die sich von einem Drittland zum anderen 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 Union beitragen wird.

([32]) 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, ELI: http://data.europa.eu/eli/reg/2011/182/oj).

(124) Verbraucher sollten ihre Rechte im Zusammenhang mit den gemäß dieser Verordnung für Wirtschaftsakteure geltenden Pflichten im Wege von Verbandsklagen gemäß der Richtlinie (EU) 2020/1828 des Europäischen Parlaments und des Rates ([33]) durchsetzen können. Zu diesem Zweck sollte in dieser Verordnung vorgesehen werden, dass die Richtlinie (EU) 2020/1828 auf Verbandsklagen wegen Verstößen gegen diese Verordnung Anwendung findet, die den Kollektivinteressen der Verbraucher schaden oder schaden können. Folglich sollte Anhang I der genannten Richtlinie entsprechend geändert werden. Es obliegt den Mitgliedstaaten, dafür zu sorgen, dass sich diese Änderungen in den Umsetzungsmaßnahmen, die sie gemäß der genannten Richtlinie erlassen, niederschlagen, wenngleich der Erlass diesbezüglicher nationaler Umsetzungsmaßnahmen keine Voraussetzung dafür ist, dass die Richtlinie auf diese Verbandsklagen Anwendung findet. Die genannte Richtlinie sollte ab dem 11. Dezember 2027 auf Verbandsklagen anwendbar sein, die wegen von Wirtschaftsakteuren begangenen Verstößen gegen Bestimmungen dieser Verordnung, die den Kollektivinteressen der Verbraucher schaden oder schaden können, eingereicht wurden.

(125) Die Kommission sollte diese Verordnung regelmäßig in Abstimmung mit einschlägigen Interessenträgern bewerten und überprüfen, insbesondere um festzustellen, ob sie veränderten gesellschaftlichen, politischen oder technischen Bedingungen oder veränderten Marktbedingungen anzupassen ist. Mit dieser Verordnung wird die Einhaltung der Verpflichtungen zur Sicherheit der Lieferkette durch Einrichtungen erleichtert, die in den Anwendungsbereich der Verordnung (EU) 2022/2554 und der Richtlinie (EU) 2022/2555 fallen und Produkte mit digitalen Elementen verwenden. Die Kommission sollte im Rahmen dieser regelmäßigen Überprüfung die kombinierten Auswirkungen des Cybersicherheitsrahmens der Union bewerten.

(126) Den Wirtschaftsakteuren sollte ausreichend Zeit für die Anpassung an die in dieser Verordnung festgelegten Anforderungen eingeräumt werden. Diese Verordnung sollte ab dem 11. Dezember 2027 gelten, mit Ausnahme der Meldepflichten für aktiv ausgenutzte Schwachstellen und schwerwiegende Sicherheitsvorfälle mit Auswirkungen auf die Sicherheit von Produkten mit digitalen Elementen, die ab dem 11. September 2026 gelten sollten, sowie der Bestimmungen über die Notifizierung von Konformitätsbewertungsstellen, die ab dem 11. Juni 2026 gelten sollten.

(127) Es ist wichtig, Kleinstunternehmen sowie kleine und mittlere Unternehmen, einschließlich Start-up-Unternehmen, bei der Durchführung dieser Verordnung zu unterstützen und die Risiken für die Durchführung, die sich aus mangelndem Wissen und fehlender Sachkenntnis auf dem Markt ergeben, zu minimieren und den Herstellern die Einhaltung ihrer in dieser Verordnung festgelegten Pflichten zu erleichtern. Im Rahmen des Programms „Digitales Europa“ und anderer einschlägiger Unionsprogramme wird finanzielle und technische Unterstützung geboten, durch die es diesen Unternehmen ermöglicht wird, zum Wachstum der Wirtschaft der Union und zur Stärkung des gemeinsamen Cybersicherheitsniveaus in der Union beizutragen. Das Europäische Kompetenzzentrum für Cybersicherheitsforschung und die nationalen Koordinierungszentren sowie die von der Kommission und den Mitgliedstaaten auf Unionsebene oder nationaler Ebene eingerichteten europäischen digitalen Innovationszentren könnten ebenfalls Unternehmen und Einrichtungen des öffentlichen Sektors unterstützen und zur Durchführung dieser Verordnung beitragen. Im Rahmen ihrer jeweiligen Aufgaben und Zuständigkeitsbereiche könnten sie Kleinstunternehmen sowie kleinen und mittleren Unternehmen technische und wissenschaftliche Unterstützung leisten, z. B. bei Testtätigkeiten und Konformitätsbewertungen durch Dritte. Sie könnten auch den Einsatz von Instrumenten zur Erleichterung der Durchführung dieser Verordnung fördern.

(128) Außerdem sollten die Mitgliedstaaten prüfen, ob sie ergänzende Maßnahmen ergreifen, die darauf abzielen, für Kleinstunternehmen sowie kleine und mittlere Unternehmen Orientierungshilfen und Unterstützung bereitzustellen, unter anderem durch die Einrichtung von Reallaboren und gezielter Kanäle für die Kommunikation. Um das Maß an Cybersicherheit in der Union zu stärken, können die Mitgliedstaaten auch in Erwägung ziehen, die Entwicklung von Kapazitäten und Kompetenzen im Zusammenhang mit der Cybersicherheit von Produkten mit digitalen Elementen zu unterstützen, die Abwehrfähigkeit von Wirtschaftsakteuren gegen Cyberangriffe, insbesondere wenn es um Kleinstunternehmen sowie um kleine und mittlere Unternehmen geht, zu verbessern und die Öffentlichkeit für die Cybersicherheit von Produkten mit digitalen Elementen zu sensibilisieren.

(129) 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.

(130) Der Europäische Datenschutzbeauftragte wurde gemäß Artikel 42 Absatz 1 der Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates ([34]) angehört und hat am 9. November 2022 ([35]) eine Stellungnahme abgegeben.

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

([34]) 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).

([35]) ABl. C 452 vom 29.11.2022, S. 23.

HABEN FOLGENDE VERORDNUNG ERLASSEN:

KAPITEL I

ALLGEMEINE BESTIMMUNGEN

Artikel 1

Gegenstand

Mit dieser Verordnung wird Folgendes festgelegt:

a) Vorschriften für die Bereitstellung auf dem Markt von Produkten mit digitalen Elementen, um die Cybersicherheit solcher Produkte zu gewährleisten;

b) grundlegende Cybersicherheitsanforderungen 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 Cybersicherheitsanforderungen an die von den Herstellern festgelegten Verfahren zur Behandlung von Schwachstellen, um die Cybersicherheit von Produkten mit digitalen Elementen während der erwarteten Nutzungsdauer der Produkte zu gewährleisten, sowie Pflichten der Wirtschaftsakteure in Bezug auf diese Verfahren;

d) Vorschriften für die Marktüberwachung, einschließlich Überwachung, und die Durchsetzung der in diesem Artikel genannten Vorschriften und Anforderungen.

Artikel 2

Anwendungsbereich

(1) Diese Verordnung gilt für auf dem Markt bereitgestellte Produkte mit digitalen Elementen, deren bestimmungsgemäßer Zweck 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.

(4) Diese Verordnung gilt nicht für Geräte, die in den Anwendungsbereich der Richtlinie 2014/90/EU des Europäischen Parlaments und des Rates ([36]) fallen.

(5) 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 Cybersicherheitsanforderungen 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, oder ein höheres.

Der Kommission wird die Befugnis übertragen, gemäß Artikel 61 zur Ergänzung 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.

([36]) Richtlinie 2014/90/EU des Europäischen Parlaments und des Rates vom 23. Juli 2014 über Schiffsausrüstung und zur Aufhebung der Richtlinie 96/98/EG des Rates (ABl. L 257 vom 28.8.2014, S. 146).

(6) Diese Verordnung gilt nicht für Ersatzteile, die auf dem Markt bereitgestellt werden, um identische Komponenten in Produkten mit digitalen Elementen zu ersetzen, und die nach denselben Spezifikationen hergestellt werden wie die Bauteile, die sie ersetzen sollen.

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

(8) Die in dieser Verordnung festgelegten Verpflichtungen umfassen nicht die Bereitstellung von Informationen, deren Offenlegung wesentlichen Interessen der Mitgliedstaaten im Bereich der nationalen Sicherheit, der öffentlichen Sicherheit oder der Verteidigung zuwiderlaufen würde.

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 den Verkehr gebracht werden;

2. „Datenfernverarbeitung“ 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. „Cybersicherheit“ Cybersicherheit im Sinne des Artikels 2 Nummer 1 der Verordnung (EU) 2019/881;

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

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

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

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

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

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

10. „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;

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

12. „Wirtschaftsakteur“ den Hersteller, den Bevollmächtigten, den Einführer, den Händler oder jede andere natürliche oder juristische Person, die Verpflichtungen im Zusammenhang mit der Herstellung von Produkten mit digitalen Elementen oder der Bereitstellung auf dem Markt von Produkten mit digitalen Elementen im Einklang mit dieser Verordnung unterliegt;

13. „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 ihrem Namen oder ihrer Marke vermarktet, sei es gegen Bezahlung, zur Monetarisierung oder unentgeltlich;

14. „Verwalter quelloffener Software“ eine juristische Person, bei der es sich nicht um einen Hersteller handelt, die den Zweck oder das Ziel hat, die Entwicklung spezifischer Produkte mit digitalen Elementen, die als freie und quelloffene Software gelten und für kommerzielle Tätigkeiten bestimmt sind, systematisch und nachhaltig zu unterstützen, und die die Brauchbarkeit dieser Produkte sicherstellt;

15. „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;

16. „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 den Verkehr bringt;

17. „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;

18. „Verbraucher“ eine natürliche Person, die zu Zwecken handelt, die nicht ihrer gewerblichen, geschäftlichen, handwerklichen oder beruflichen Tätigkeit zugerechnet werden können;

19. „Kleinstunternehmen“, „kleine Unternehmen“ und „mittlere Unternehmen“ Kleinstunternehmen, kleine Unternehmen bzw. mittlere Unternehmen im Sinne des Anhangs der Empfehlung 2003/361/EG;

20. „Unterstützungszeitraum“ den Zeitraum, in dem der Hersteller sicherstellen muss, dass die Schwachstellen des Produkts mit digitalen Elementen wirksam und im Einklang mit den grundlegenden Cybersicherheitsanforderungen in Anhang I Teil II behandelt werden;

21. „Inverkehrbringen“ bzw. „in den Verkehr bringen“ die erstmalige Bereitstellung eines Produkts mit digitalen Elementen auf dem Unionsmarkt;

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

23. „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 Erklärungen sowie in der technischen Dokumentation;

24. „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;

25. „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;

26. „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;

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

28. „Konformitätsbewertungsstelle“ eine Konformitätsbewertungsstelle im Sinne von Artikel 2 Nummer 13 der Verordnung (EG) Nr. 765/2008.

29. „notifizierte Stelle“ eine Konformitätsbewertungsstelle, die nach Artikel 43 dieser Verordnung und anderen einschlägigen Harmonisierungsrechtsvorschriften der Union benannt wurde;

30. „wesentliche Änderung“ eine Änderung des Produkts mit digitalen Elementen nach dessen Inverkehrbringen, die sich auf die Konformität des Produkts mit den grundlegenden Cybersicherheitsanforderungen in Anhang I Teil I auswirkt oder zu einer Änderung des bestimmungsgemäßen Zwecks, für den das Produkt geprüft wurde, führt;

31. „CE-Kennzeichnung“ eine Kennzeichnung, durch die ein Hersteller erklärt, dass ein Produkt mit digitalen Elementen und die vom Hersteller festgelegten Verfahren den grundlegenden Cybersicherheitsanforderungen in Anhang I und anderen geltenden Harmonisierungsrechtsvorschriften der Union über ihre Anbringung genügen;

32. „Harmonisierungsrechtsvorschriften der Union“ die in Anhang I der Verordnung (EU) 2019/1020 aufgeführten Rechtsvorschriften der Union sowie alle sonstigen Rechtsvorschriften der Union zur Harmonisierung der Bedingungen für die Vermarktung von Produkten, auf welche die genannte Verordnung Anwendung findet;

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

34. „internationale Norm“ eine internationale Norm gemäß der Begriffsbestimmung in Artikel 2 Absatz 1 Buchstabe a der Verordnung (EU) Nr. 1025/2012;

35. „europäische Norm“ eine europäische Norm gemäß der Begriffsbestimmung in Artikel 2 Nummer 1 Buchstabe b der Verordnung (EU) Nr. 1025/2012;

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

37. „Cybersicherheitsrisiko“ das Potenzial für Verluste oder Störungen, die durch einen Sicherheitsvorfall verursacht werden, das als eine Kombination des Ausmaßes eines solchen Verlusts oder einer solchen Störung und der Wahrscheinlichkeit des Eintretens des Sicherheitsvorfalls zum Ausdruck gebracht wird;

38. „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;

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

40. „Schwachstelle“ eine Schwäche, Anfälligkeit oder Fehlfunktion eines Produkts mit digitalen Elementen, die bei einer Cyberbedrohung ausgenutzt werden kann;

41. „ausnutzbare Schwachstelle“ eine Schwachstelle, die von einem unbefugten Dritten unter praktischen Betriebsbedingungen wirksam genutzt werden kann;

42. „aktiv ausgenutzte Schwachstelle“ eine Schwachstelle, zu der verlässliche Nachweise dafür vorliegen, dass ein böswilliger Akteur sie in einem System ohne Zustimmung des Systemeigners ausgenutzt hat;

43. „Sicherheitsvorfall“ einen Sicherheitsvorfall gemäß der Begriffsbestimmung in Artikel 6 Nummer 6 der Richtlinie (EU) 2022/2555;

44. „Sicherheitsvorfall mit Auswirkungen auf die Sicherheit des Produkts mit digitalen Elementen“ einen Sicherheitsvorfall, der sich negativ auf die Fähigkeit eines Produkts mit digitalen Elementen auswirkt oder auswirken kann, die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit von Daten oder Funktionen zu schützen;

45. „Beinahe-Vorfall“ einen Beinahe-Vorfall gemäß der Begriffsbestimmung in Artikel 6 Nummer 5 der Richtlinie (EU) 2022/2555;

46. „Cyberbedrohung“ ist eine Cyberbedrohung gemäß der Begriffsbestimmung in Artikel 2 Nummer 8 der Verordnung (EU) 2019/881;

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

48. „freie und quelloffene Software“ eine Software, deren Quellcode offen geteilt wird und die im Rahmen einer kostenlosen Open-Source-Lizenz zur Verfügung gestellt wird, die alle Rechte vorsieht, um sie frei zugänglich, nutzbar, veränderbar und weiterverteilbar zu machen;

49. „Rückruf“ einen Rückruf gemäß der Begriffsbestimmung in Artikel 3 Nummer 22 der Verordnung (EU) 2019/1020;

50. „Rücknahme vom Markt“ eine Rücknahme vom Markt gemäß der Begriffsbestimmung in Artikel 3 Nummer 23 der Verordnung (EU) 2019/1020;

51. „als Koordinator benanntes CSIRT“ ein CSIRT, das gemäß Artikel 12 Absatz 1 der Richtlinie (EU) 2022/2555 als Koordinator benannt wurde.

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 oder Verwendung eines Produkts mit digitalen Elementen, das dieser Verordnung nicht entspricht, bei Messen, Ausstellungen, Vorführungen oder ähnlichen Veranstaltungen, einschließlich Prototypen, sofern das Produkt mit eine sichtbare Kennzeichnung aufweist, die deutlich darauf hinweist, dass es dieser Verordnung nicht entspricht und erst auf dem Markt bereitgestellt werden darf, wenn es dies tut.

(3) Die Mitgliedstaaten verhindern nicht die Bereitstellung auf dem Markt von 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 mit einer sichtbaren Kennzeichnung deutlich darauf hinweist, dass sie dieser Verordnung nicht entspricht und außer zu Testzwecken nicht auf dem Markt verfügbar sein wird.

(4) Absatz 3 gilt nicht für Sicherheitsbauteile im Sinne von anderen Harmonisierungsrechtsvorschriften der Union als dieser Verordnung.

Artikel 5

Beschaffung oder Nutzung von Produkten mit digitalen Elementen

(1) Diese Verordnung hindert die Mitgliedstaaten nicht daran, Produkte mit digitalen Elementen bei der Beschaffung oder Verwendung dieser Produkte für bestimmte Zwecke zusätzlichen Cybersicherheitsanforderungen zu unterwerfen, auch wenn diese Produkte für Zwecke der nationalen Sicherheit oder Verteidigung beschafft oder verwendet werden, sofern diese Anforderungen mit den im Unionsrecht festgelegten Verpflichtungen der Mitgliedstaaten im Einklang stehen und für die Erreichung dieser Zwecke notwendig und verhältnismäßig sind.

(2) Unbeschadet der Richtlinien 2014/24/EU und 2014/25/EU stellen die Mitgliedstaaten bei der Beschaffung von Produkten mit digitalen Elementen, die in den Anwendungsbereich dieser Verordnung fallen, sicher, dass die Einhaltung der grundlegenden Cybersicherheitsanforderungen gemäß Anhang I dieser Verordnung, einschließlich der Fähigkeit der Hersteller, Schwachstellen wirksam zu bewältigen, im Vergabeverfahren berücksichtigt wird.

Artikel 6

Anforderungen an Produkte mit digitalen Elementen

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

a) sie den grundlegenden Cybersicherheitsanforderungen in Anhang I Teil I genügen und unter der Bedingung, dass sie ordnungsgemäß installiert, gewartet und bestimmungsgemäß oder unter vernünftigerweise vorhersehbaren Umständen verwendet werden sowie gegebenenfalls die erforderlichen Sicherheitsaktualisierungen installiert wurden; und

b) die vom Hersteller festgelegten Verfahren den grundlegenden Cybersicherheitsanforderungen in Anhang I Teil II entsprechen.

Artikel 7

Wichtige Produkte mit digitalen Elementen

(1) Produkte mit digitalen Elementen, die die Kernfunktionen einer in Anhang III aufgeführten Produktkategorie aufweisen, gelten als wichtige Produkte mit digitalen Elementen und unterliegen den in Artikel 32 Absätze 2 und 3 genannten Konformitätsbewertungsverfahren. Die Integration eines Produkts mit digitalen Elementen, das die Kernfunktionen einer in Anhang III aufgeführten Produktkategorie aufweist, führt für sich genommen nicht dazu, dass das Produkt, in das es integriert ist, den Konformitätsbewertungsverfahren gemäß Artikel 32 Absätze 2 und 3 unterliegt.

(2) Die in Absatz 1 dieses Artikels genannten Kategorien von Produkten mit digitalen Elementen, die gemäß Anhang III in die Klassen I und II unterteilt sind, erfüllen mindestens eines der folgenden Kriterien:

a) Das Produkt mit digitalen Elementen erfüllt in erster Linie Funktionen, die für die Cybersicherheit anderer Produkte, Netze oder Dienste von entscheidender Bedeutung sind, einschließlich der Sicherung der Authentifizierung und des Zugangs, der Prävention und Erkennung von Eindringen, der Endpunktsicherheit oder des Netzschutzes;

b) das Produkt mit digitalen Elementen erfüllt eine Funktion, die ein erhebliches Risiko nachteiliger Auswirkungen birgt in Bezug auf deren Intensität und Fähigkeit, eine große Zahl anderer Produkte oder die Gesundheit, Sicherheit oder Sicherheit seiner Nutzer durch direkte Manipulation zu stören, zu steuern oder zu schädigen, wie z. B. eine zentrale Systemfunktion, einschließlich Netzmanagement, Konfigurationskontrolle, Virtualisierung oder Verarbeitung personenbezogener Daten.

(3) Der Kommission wird die Befugnis übertragen, gemäß Artikel 61 delegierte Rechtsakte zur Änderung des Anhangs III zu erlassen, um innerhalb jeder Klasse der Kategorien von Produkten mit digitalen Elementen eine neue Kategorie in die Liste aufzunehmen und ihre Definition zu präzisieren, eine Produktkategorie von einer Klasse in die andere zu verschieben 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 cybersicherheitsbezogenen Funktionen oder die Funktion und die Höhe des von Produkten mit digitalen Elementen ausgehenden Cybersicherheitsrisikos gemäß den in Absatz 2 genannten Kriterien des vorliegenden Artikels.

Die in Unterabsatz 1 genannten delegierten Rechtsakte sehen gegebenenfalls einen Übergangszeitraum von mindestens 12 Monaten vor, insbesondere wenn eine neue Kategorie wichtiger Produkte mit digitalen Elementen der Klasse I oder II gemäß Anhang III hinzugefügt oder von der Klasse I in die Klasse II verschoben wird, bevor die einschlägigen Konformitätsbewertungsverfahren gemäß Artikel 32 Absätze 2 und 3 zur Anwendung kommen, es sei denn, ein kürzerer Übergangszeitraum ist aus Gründen äußerster Dringlichkeit gerechtfertigt.

(4) Bis zum 11. Dezember 2025 erlässt die Kommission einen Durchführungsrechtsakt, in dem sie die technische Beschreibung der nach Anhang III zu den Klassen I und II gehörigen Kategorien von Produkten mit digitalen Elementen und die technische Beschreibung der Kategorien von Produkten mit digitalen Elementen gemäß Anhang IV festlegt. Dieser Durchführungsrechtsakt wird nach dem Prüfverfahren gemäß Artikel 62 Absatz 2 erlassen.

Artikel 8

Kritische Produkte mit digitalen Elementen

(1) Der Kommission wird die Befugnis übertragen, gemäß Artikel 61 delegierte Rechtsakte zur Ergänzung dieser Verordnung zu erlassen, um festzulegen, welche Produkte mit digitalen Elementen, die die Kernfunktionen einer in Anhang IV dieser Verordnung aufgeführten Produktkategorie aufweisen, ein europäisches Cybersicherheitszertifikat mindestens der Vertrauenswürdigkeitsstufe „mittel“ im Rahmen eines gemäß der Verordnung (EU) 2019/881 erlassenen europäischen Schemas für die Cybersicherheitszertifizierung erhalten müssen, um die Konformität mit den grundlegenden Cybersicherheitsanforderungen in Anhang I der vorliegenden Verordnung oder Teilen davon nachzuweisen, sofern ein europäisches Schema für die Cybersicherheitszertifizierung für diese Produktkategorien mit digitalen Elementen gemäß der Verordnung (EU) 2019/881 angenommen wurde und den Herstellern zur Verfügung steht. In diesen delegierten Rechtsakten wird die erforderliche Vertrauenswürdigkeitsstufe festgelegt, die in einem angemessenen Verhältnis zum Niveau des Cybersicherheitsrisikos stehen muss, das mit Produkten mit digitalen Elementen verbunden ist, und deren Zweckbestimmung, einschließlich der kritischen Abhängigkeit davon seitens wesentlicher Einrichtungen gemäß Artikel 3 Absatz 1 der Richtlinie (EU) 2022/2555, berücksichtigen muss.

Vor dem Erlass solcher delegierten Rechtsakte führt die Kommission eine Bewertung der potenziellen Auswirkungen der geplanten Maßnahmen auf den Markt durch und konsultiert die einschlägigen Interessenträger, einschließlich der mit der Verordnung (EU) 2019/881 eingerichteten Europäischen Gruppe für die Cybersicherheitszertifizierung. Bei der Bewertung werden die Bereitschaft und die Kapazität der Mitgliedstaaten für die Umsetzung des einschlägigen europäischen Schemas für die Cybersicherheitszertifizierung berücksichtigt. Wurden keine delegierten Rechtsakte gemäß Unterabsatz 1 erlassen, so unterliegen Produkte mit digitalen Elementen, die Kernfunktionen einer Produktkategorie gemäß Anhang IV aufweisen, den Konformitätsbewertungsverfahren gemäß Artikel 32 Absatz 3.

Die in Unterabsatz 1 genannten delegierten Rechtsakte müssen einen Übergangszeitraum von mindestens sechs Monaten vorsehen, es sei denn, ein kürzerer Übergangszeitraum ist aus Gründen äußerster Dringlichkeit gerechtfertigt.

(2) Der Kommission wird die Befugnis übertragen, gemäß Artikel 61 delegierte Rechtsakte zur Änderung von Anhang IV zu erlassen, um Kategorien kritischer Produkte mit digitalen Elementen hinzuzufügen oder zu streichen. Bei der Festlegung solcher Kategorien kritischer Produkte mit digitalen Elementen und der erforderlichen Vertrauenswürdigkeitsstufe gemäß Absatz 1 berücksichtigt die Kommission die in Artikel 7 Absatz 2 genannten Kriterien und stellt sicher, dass die Kategorie von Produkten mit digitalen Elementen mindestens einem der folgenden Kriterien entspricht:

a) Es besteht eine kritische Abhängigkeit wesentlicher Einrichtungen gemäß Artikel 3 der Richtlinie (EU) 2022/2555 von der Kategorie der Produkte mit digitalen Elementen;

b) Sicherheitsvorfälle und ausgenutzte Schwachstellen in Bezug auf die Kategorie von Produkten mit digitalen Elementen könnten zu schwerwiegenden Störungen kritischer Lieferketten im gesamten Binnenmarkt führen.

Vor dem Erlass solcher delegierten Rechtsakte führt die Kommission eine Bewertung der in Absatz 1 genannten Art durch.

Die in Unterabsatz 1 genannten delegierten Rechtsakte müssen einen Übergangszeitraum von mindestens sechs Monaten vorsehen, es sei denn, ein kürzerer Übergangszeitraum ist aus Gründen äußerster Dringlichkeit gerechtfertigt.

Artikel 9

Konsultation der Interessenträger

(1) Bei der Vorbereitung von Maßnahmen für die Durchführung dieser Verordnung konsultiert die Kommission die einschlägigen Interessenträger, wie die einschlägigen Behörden der Mitgliedstaaten, Unternehmen des Privatsektors, einschließlich Kleinstunternehmen und kleiner und mittlerer Unternehmen, die Open-Source-Software-Gemeinschaft, Verbraucherverbände, Hochschulen und einschlägige Agenturen und Einrichtungen der Union sowie auf Unionsebene eingerichtete Expertengruppen, und berücksichtigt deren Ansichten. Insbesondere konsultiert die Kommission in folgenden Fällen gegebenenfalls in folgender strukturierter Weise diese Interessenträger und holt deren Ansichten ein:

a) bei der Erstellung der in Artikel 26 genannten Leitlinien;

b) unbeschadet Artikel 61 bei der Ausarbeitung der technischen Beschreibungen der in Anhang III aufgeführten Produktkategorien gemäß Artikel 7 Absatz 4, bei der Bewertung, ob die Liste der Produktkategorien gemäß Artikel 7 Absatz 3 und Artikel 8 Absatz 2 aktualisiert werden muss, oder bei der Durchführung der Bewertung der potenziellen Auswirkungen auf den Markt gemäß Artikel 8 Absatz 1;

c) bei der Durchführung von Vorbereitungsarbeiten für die Bewertung und Überprüfung dieser Verordnung.

(2) Die Kommission organisiert regelmäßig, mindestens einmal jährlich, Konsultations- und Informationssitzungen, um die Ansichten der in Absatz 1 genannten Interessenträger zur Durchführung dieser Verordnung einzuholen.

Artikel 10

Ausbau der Kompetenzen in einem digitalen Umfeld mit Cyberabwehrfähigkeit

Für die Zwecke dieser Verordnung und um den Bedürfnissen der Fachkräfte bei der Unterstützung der Durchführung dieser Verordnung gerecht zu werden, fördern die Mitgliedstaaten — gegebenenfalls mit Unterstützung der Kommission, des Europäischen Kompetenzzentrums für Cybersicherheit und der ENISA — unter uneingeschränkter Achtung der Verantwortung der Mitgliedstaaten im Bildungsbereich Maßnahmen und Strategien, die auf Folgendes abzielen:

a) Entwicklung von Cybersicherheitskompetenzen und Schaffung organisatorischer und technologischer Instrumente, um eine ausreichende Verfügbarkeit qualifizierter Fachkräfte sicherzustellen, um die Tätigkeiten der Marktüberwachungsbehörden und Konformitätsbewertungsstellen zu unterstützen;

b) Stärkung der Zusammenarbeit zwischen dem Privatsektor und den Wirtschaftsakteuren, unter anderem durch Umschulung oder Weiterbildung der Beschäftigten der Hersteller, den Verbrauchern, den Ausbildungseinrichtungen sowie den öffentlichen Verwaltungen, um jungen Menschen so mehr Möglichkeiten für den Zugang zu Arbeitsplätzen im Cybersicherheitssektor zu eröffnen.

Artikel 11

Allgemeine Produktsicherheit

Abweichend von Artikel 2 Absatz 1 Unterabsatz 3 Buchstabe b der Verordnung (EU) 2023/988 finden Kapitel III Abschnitt 1, Kapitel V und VII sowie die Kapitel IX bis XI der genannten Verordnung Anwendung auf Produkte mit digitalen Elementen in Bezug auf Aspekte und Risiken oder Risikokategorien, die nicht unter die vorliegende Verordnung fallen, sofern diese Produkte keinen besonderen Sicherheitsanforderungen unterliegen, die in anderen „Harmonisierungsrechtsvorschriften der Union“ im Sinne von Artikel 3 Nummer 27 der Verordnung (EU) 2023/988 festgelegt sind.

Artikel 12

Hochrisiko-KI-Systeme

(1) Unbeschadet der Anforderungen in Bezug auf Genauigkeit und Robustheit gemäß Artikel 15 der Verordnung (EU) 2024/1689 gelten Produkte mit digitalen Elementen, die in den Anwendungsbereich der vorliegenden Verordnung fallen und die gemäß Artikel 6 der genannten Verordnung als Hochrisiko-KI-Systeme eingestuft werden, als mit den Cybersicherheitsanforderungen gemäß Artikel 15 der genannten Verordnung konform, wenn

a) diese Produkte die grundlegenden Cybersicherheitsanforderungen gemäß Anhang I Teil I erfüllen;

b) die vom Hersteller festgelegten Verfahren den grundlegenden Cybersicherheitsanforderungen in Anhang I Teil II entsprechen, und

c) die Verwirklichung des gemäß Artikel 15 der Verordnung (EU) 2024/1689 erforderlichen Cybersicherheitsniveaus in der gemäß dieser Verordnung ausgestellten EU-Konformitätserklärung nachgewiesen wird.

(2) Für die in Absatz 1 genannten Produkte mit digitalen Elementen und Cybersicherheitsanforderungen gilt das einschlägige in Artikel 43 der Verordnung (EU) 2024/1689 vorgesehene Konformitätsbewertungsverfahren. Für die Zwecke dieser Bewertung sind die notifizierten Stellen, die gemäß der Verordnung (EU) 2024/1689 dafür zuständig sind, die Konformität der Hochrisiko-KI-Systeme zu kontrollieren, auch dafür zuständig, 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 (EU) 2024/1689 durchgeführten Notifizierungsverfahren geprüft wurde, ob diese notifizierten Stellen die in Artikel 39 der vorliegenden Verordnung festgelegten Anforderungen erfüllen.

(3) Abweichend von Absatz 2 des vorliegenden Artikels unterliegen die in Anhang III der vorliegenden Verordnung aufgeführten wichtigen Produkte mit digitalen Elementen, die den Konformitätsbewertungsverfahren gemäß Artikel 32 Absatz 2 Buchstaben a und b und Artikel 32 Absatz 3 der vorliegenden Verordnung unterliegen, sowie in Anhang IV der vorliegenden Verordnung aufgeführte kritische Produkte mit digitalen Elementen, die gemäß Artikel 8 Absatz 1 der vorliegenden Verordnung ein europäisches Cybersicherheitszertifikat erhalten müssen oder — in Ermangelung eines solchen Zertifikats — die den Konformitätsbewertungsverfahren gemäß Artikel 32 Absatz 3 der vorliegenden Verordnung unterliegen, und auch nach Artikel 6 der Verordnung (EU) 2024/1689 als Hochrisiko-KI-Systeme eingestuft sind und für die das Konformitätsbewertungsverfahren auf der Grundlage einer internen Kontrolle gemäß Anhang VI der Verordnung (EU) 2024/1689 gilt, den in der vorliegenden Verordnung vorgesehenen Konformitätsbewertungsverfahren, soweit dies die in der vorliegenden Verordnung festgelegten grundlegenden Cybersicherheitsanforderungen betrifft.

(4) Hersteller von Produkten mit digitalen Elementen gemäß Absatz 1 können an den KI-Reallaboren gemäß Artikel 57 der Verordnung (EU) 2024/1689 teilnehmen.

KAPITEL II

PFLICHTEN DER WIRTSCHAFTSAKTEURE UND BESTIMMUNGEN IN BEZUG AUF FREIE UND QUELLOFFENE SOFTWARE

Artikel 13

Pflichten der Hersteller

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

(2) Für die Zwecke der Erfüllung von Absatz 1 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 Sicherheitsvorfälle, auch in Bezug auf die Gesundheit und Sicherheit der Nutzer, so gering wie möglich zu halten.

(3) Die Bewertung des Cybersicherheitsrisikos wird während eines gemäß Absatz 8 festzulegenden Unterstützungszeitraums dokumentiert und gegebenenfalls aktualisiert. Diese Bewertung des Cybersicherheitsrisikos umfasst mindestens eine Analyse der Cybersicherheitsrisiken auf der Grundlage der Zweckbestimmung und der vernünftigerweise vorhersehbaren Verwendung des Produkts mit digitalen Elementen, wie der Betriebsumgebung oder der zu schützenden Anlagen, wobei die voraussichtliche Nutzungsdauer des Produkts berücksichtigt wird. In der Bewertung des Cybersicherheitsrisikos wird angegeben, ob und gegebenenfalls in welcher Weise die Sicherheitsanforderungen gemäß Anhang I Teil I Nummer 2 auf das einschlägige Produkt mit digitalen Elementen anwendbar sind und wie diese Anforderungen auf der Grundlage der Bewertung des Cybersicherheitsrisikos umgesetzt werden. Ferner ist anzugeben, wie der Hersteller Anhang I Teil I Nummer 1 anzuwenden hat und welche Anforderungen an die Behandlung von Schwachstellen in Anhang I Teil II festgelegt sind.

(4) Wenn er ein Produkt mit digitalen Elementen in den Verkehr bringt, nimmt der Hersteller die Bewertung der Cybersicherheitsrisiken gemäß Absatz 3 in die gemäß Artikel 31 und Anhang VII vorgeschriebene technische Dokumentation auf. Bei Produkten mit digitalen Elementen gemäß Artikel 12, die auch anderen Unionsrechtsvorschriften unterliegen, kann die Bewertung der Cybersicherheitsrisiken auch Teil der in den betreffenden Unionsrechtsvorschriften geforderten Risikobewertungen sein. Sind bestimmte grundlegende Cybersicherheitsanforderungen nicht auf das Produkt mit digitalen Elementen anwendbar, so nimmt der Hersteller eine klare Begründung hierfür in diese technische Dokumentation auf.

(5) 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, sodass solche Komponenten die Cybersicherheit des Produkts mit digitalen Elementen nicht beeinträchtigen, auch nicht bei der Integration von freier und quelloffener Software, die nicht im Rahmen einer Geschäftstätigkeit auf dem Markt bereitgestellt wurde.

(6) Sobald der Hersteller eine Schwachstelle in einer in das Produkt mit digitalen Elementen integrierten Komponente, einschließlich einer quelloffenen Komponente, feststellt, meldet er die Schwachstelle der Person oder Einrichtung, die diese Komponente herstellt oder wartet, und behandelt und behebt die Schwachstelle gemäß den in Anhang I Teil II festgelegten Anforderungen an die Behandlung von Schwachstellen. Haben Hersteller eine Software- oder Hardware-Änderung entwickelt, um die Schwachstelle in dieser Komponente zu beheben, teilen sie den betreffenden Code oder die einschlägigen Unterlagen der Person oder Stelle, die die Komponente herstellt oder wartet, gegebenenfalls in einem maschinenlesbaren Format mit.

(7) Der Hersteller dokumentiert systematisch und in einer der Art der Cybersicherheitsrisiken angemessenen Weise alle relevanten 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 Bewertung der Cybersicherheitsrisiken des Produkts.

(8) Wenn sie ein Produkt mit digitalen Elementen in den Verkehr bringen und während der erwarteten Produktlebensdauer und des Unterstützungszeitraums stellen die Hersteller sicher, dass Schwachstellen dieses Produkts, einschließlich seiner Komponenten, wirksam und im Einklang mit den grundlegenden Cybersicherheitsanforderungen in Anhang I Teil II behandelt werden.

Die Hersteller legen den Unterstützungszeitraum so fest, dass er die Dauer der voraussichtlichen Nutzung des Produkts widerspiegelt, wobei sie insbesondere angemessenen Erwartungen der Nutzer, der Art des Produkts, einschließlich seiner Zweckbestimmung, sowie den einschlägigen Rechtsvorschriften der Union zur Festlegung der Lebensdauer von Produkten mit digitalen Elementen Rechnung tragen. Bei der Festlegung des Unterstützungszeitraums können die Hersteller auch die Unterstützungszeiträume für Produkte mit digitalen Elementen mit einer ähnlichen Funktion, die von anderen Herstellern in den Verkehr gebracht werden, die Verfügbarkeit der Betriebsumgebung, die Unterstützungszeiträume für integrierte Komponenten, die Kernfunktionen erbringen und von Dritten bezogen werden, sowie die einschlägigen Leitlinien der gemäß Artikel 52 Absatz 15 eingesetzten besondere Gruppe zur administrativen Zusammenarbeit (ADCO) und der Kommission berücksichtigen. Die zur Bestimmung des Unterstützungszeitraums zu berücksichtigenden Aspekte werden in einer Weise berücksichtigt, die die Verhältnismäßigkeit gewährleistet.

Unbeschadet Unterabsatz 2 beträgt der Unterstützungszeitraum mindestens fünf Jahre. Wird davon ausgegangen, dass das Produkt mit digitalen Elementen weniger als fünf Jahre im Betrieb ist, muss der Unterstützungszeitraum der voraussichtlichen Nutzungsdauer entsprechen.

Unter Berücksichtigung der ADCO-Empfehlungen gemäß Artikel 52 Absatz 16 kann die Kommission gemäß Artikel 61 delegierte Rechtsakte erlassen, um diese Verordnung durch die Festlegung des Mindestunterstützungszeitraums für bestimmte Produktkategorien zu ergänzen, wenn die Marktüberwachungsdaten auf unangemessene Unterstützungszeiträume hindeuten.

Die Hersteller nehmen die Informationen, die bei der Bestimmung des Unterstützungszeitraums eines Produkts mit digitalen Elementen berücksichtigt wurden, in die technische Dokumentation gemäß Anhang VII auf.

Die Hersteller haben geeignete Strategien und Verfahren, darunter eine Strategie für die koordinierte Offenlegung von Schwachstellen gemäß Anhang I Teil II Nummer 5, um potenzielle Schwachstellen in dem Produkt mit digitalen Elementen, die von internen oder externen Quellen gemeldet werden, zu bearbeiten und zu beheben.

(9) Die Hersteller gewährleisten, dass jede Sicherheitsaktualisierung gemäß Anhang I Teil II Nummer 8, die den Nutzern während des Unterstützungszeitraums zur Verfügung gestellt wurde, nach ihrer Bereitstellung für mindestens zehn Jahre oder für die verbleibende Dauer des Unterstützungszeitraums, je nachdem, welcher Zeitraum länger ist, verfügbar bleibt.

(10) Hat ein Hersteller nachfolgende wesentlich geänderte Versionen eines Softwareprodukts in den Verkehr gebracht, so kann er die Sicherstellung der Einhaltung der in Anhang I Teil II Nummer 2 festgelegten grundlegenden Cybersicherheitsanforderung auf die Version beschränken, die der Hersteller zuletzt in den Verkehr gebracht hat, sofern die Nutzer der zuvor in den Verkehr gebrachten Version kostenlos Zugang zu der zuletzt in den Verkehr gebrachten Version haben und ihnen keine zusätzlichen Kosten für die Anpassung der Hardware- und Softwareumgebung entstehen, in der sie die Originalversion dieses Produkts verwenden.

(11) Die Hersteller können öffentliche Softwarearchive unterhalten, die den Nutzern den Zugang zu historischen Versionen erleichtern. In diesen Fällen werden die Nutzer klar und in leicht zugänglicher Form über die Risiken im Zusammenhang mit der Verwendung nicht unterstützter Software informiert.

(12) Bevor sie ein Produkt mit digitalen Elementen in den Verkehr bringen, erstellen die Hersteller die in Artikel 31 genannte technische Dokumentation.

Sie führen die gewählten Konformitätsbewertungsverfahren gemäß Artikel 32 durch oder lassen sie durchführen.

Ist mit diesem Konformitätsbewertungsverfahren nachgewiesen worden, dass das Produkt mit digitalen Elementen den grundlegenden Cybersicherheitsanforderungen in Anhang I Teil I genügt und die vom Hersteller festgelegten Verfahren den grundlegenden Cybersicherheitsanforderungen in Anhang I Teil II genügen, so stellen die Hersteller die EU-Konformitätserklärung gemäß Artikel 28 aus und bringen die CE-Kennzeichnung gemäß Artikel 30 an.

(13) Die Hersteller bewahren die technische Dokumentation und die EU-Konformitätserklärung nach dem Inverkehrbringen des Produkts mit digitalen Elementen mindestens zehn Jahre lang oder für die Dauer des Unterstützungszeitraums, je nachdem, welcher Zeitraum länger ist, für die Marktüberwachungsbehörden auf.

(14) Die Hersteller gewährleisten durch geeignete Verfahren, dass die Konformität von Produkten mit digitalen Elementen mit dieser Verordnung bei einer Serienherstellung sichergestellt bleibt. Die Hersteller berücksichtigen 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 Schemata für die Cybersicherheitszertifizierung oder der in Artikel 27 genannten gemeinsamen Spezifikationen, die bei der Erklärung der Konformität des Produkts mit digitalen Elementen zugrunde gelegt oder bei der Überprüfung seiner Konformität angewandt wurden.

(15) Die Hersteller gewährleisten, dass ihre Produkte mit digitalen Elementen eine Typen-, Chargen- oder Seriennummer oder ein anderes Kennzeichen zu ihrer Identifikation tragen, oder, falls dies nicht möglich ist, dass die diese Informationen auf der Verpackung oder in den dem Produkt mit digitalen Elementen beigefügten Unterlagen angegeben werden.

(16) Die Hersteller geben den Namen, den eingetragenen Handelsnamen oder die eingetragene Handelsmarke des Herstellers, die Postanschrift, die E-Mail-Adresse oder andere digitale Kontaktangaben sowie, soweit vorhanden, die Website, unter der der Hersteller zu erreichen ist, 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. Diese Informationen werden auch in die in Informationen und Anleitungen für den Nutzer gemäß Anhang II aufgenommen. Die Kontaktangaben sind in einer Sprache abzufassen, die von den Nutzern und den Marktüberwachungsbehörden leicht verstanden werden kann.

(17) Für die Zwecke dieser Verordnung benennen die Hersteller eine zentrale Anlaufstelle, die es den Nutzern ermöglicht, direkt und schnell mit ihnen zu kommunizieren, auch um die Meldung von Schwachstellen des Produkts mit digitalen Elementen zu erleichtern.

Die Hersteller stellen sicher, dass die zentrale Anlaufstelle von den Nutzern leicht ermittelt werden kann. Sie nehmen die zentrale Anlaufstelle auch in die Informationen und Anleitungen für die Nutzer gemäß Anhang II auf.

Die zentrale Anlaufstelle ermöglicht es den Nutzern, ihr bevorzugtes Kommunikationsmittel zu wählen, wobei diese Mittel nicht auf automatisierte Instrumente beschränkt werden dürfen.

(18) Die Hersteller gewährleisten, dass den Produkten mit digitalen Elementen die in Anhang II genannten Informationen und Anleitungen für den Nutzer in Papierform oder elektronischer Form beigefügt sind. Diese Informationen und Anleitungen müssen in einer Sprache bereitgestellt werden, die von den Nutzern und den Marktüberwachungsbehörden leicht verstanden werden kann. Sie müssen klar, verständlich, deutlich und lesbar sein. Sie müssen die sichere Installation, den sicheren Betrieb und die sichere Verwendung der Produkte mit digitalen Elementen ermöglichen. Die Hersteller stellen die Informationen und Anleitungen für den Nutzer gemäß Anhang II nach dem Inverkehrbringen des Produkts mit digitalen Elementen mindestens zehn Jahre lang oder für die Dauer des Unterstützungszeitraums, je nachdem, welcher Zeitraum länger ist, den Nutzern zur Verfügung. Werden diese Informationen und Anleitungen online bereitgestellt, so stellen die Hersteller sicher, dass sie zugänglich, benutzerfreundlich und mindestens zehn Jahre lang nach dem Inverkehrbringen des Produkts mit digitalen Elementen oder während des Unterstützungszeitraums, je nachdem, welcher Zeitraum länger ist, online verfügbar sind.

(19) Die Hersteller stellen sicher, dass das Enddatum des in Absatz 8 genannten Unterstützungszeitraums, zum Zeitpunkt des Kaufs in leicht zugänglicher Weise und sofern zutreffend auf dem Produkt mit digitalen Elementen, seiner Verpackung oder mit digitalen Mitteln klar und verständlich angegeben wird, wobei mindestens der Monat und das Jahr anzugeben sind.

Sofern dies angesichts der Art des Produkts mit digitalen Elementen technisch machbar ist, zeigen die Hersteller den Nutzern eine Mitteilung an, um sie darüber zu unterrichten, dass das Ende des Unterstützungszeitraums ihres Produkts mit digitalen Elementen erreicht ist.

(20) Die Hersteller fügen dem Produkt mit digitalen Elementen entweder eine Kopie der EU-Konformitätserklärung oder eine vereinfachte EU-Konformitätserklärung bei. Wird nur eine vereinfachte EU-Konformitätserklärung bereitgestellt, muss darin die genaue Internetadresse angegeben sein, unter der die vollständige EU-Konformitätserklärung eingesehen werden kann.

(21) Ab dem Inverkehrbringen und während des Unterstützungszeitraums 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 Cybersicherheitsanforderungen 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.

(22) Die Hersteller übermitteln der Marktüberwachungsbehörde auf deren begründetes Verlangen in Papierform oder in elektronischer Form in einer für diese 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 Cybersicherheitsanforderungen in Anhang I erforderlich sind. Die Hersteller arbeiten mit dieser Behörde auf deren Verlangen bei allen Maßnahmen zur Abwendung der Cybersicherheitsrisiken zusammen, die mit dem von ihnen in den Verkehr gebrachten Produkt mit digitalen Elementen verbunden sind.

(23) Ein Hersteller, der seine Betriebstätigkeit einstellt und infolgedessen nicht in der Lage ist, diese Verordnung zu erfüllen, unterrichtet vor dem Wirksamwerden der Betriebseinstellung die einschlägigen Marktüberwachungsbehörden sowie — mit allen verfügbaren Mitteln und soweit möglich — die Nutzer der einschlägigen in den Verkehr gebrachten Produkte mit digitalen Elementen über die bevorstehende Einstellung der Betriebstätigkeit.

(24) Die Kommission kann im Wege von Durchführungsrechtsakten unter Berücksichtigung europäischer oder internationaler Normen und bewährter Verfahren das Format und die Elemente der Software-Stückliste gemäß Anhang I Teil II Nummer 1 festlegen. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 62 Absatz 2 genannten Prüfverfahren erlassen.

(25) Um die Abhängigkeit der Mitgliedstaaten und der Union insgesamt von Softwarekomponenten und insbesondere von Komponenten, die als freie und quelloffene Software gelten, zu bewerten, kann die ADCO beschließen, für bestimmte Kategorien von Produkten mit digitalen Elementen eine unionsweite Bewertung der Abhängigkeit durchzuführen. Zu diesem Zweck können die Marktüberwachungsbehörden die Hersteller solcher Kategorien von Produkten mit digitalen Elementen auffordern, die entsprechenden Software-Stücklisten gemäß Anhang I Teil II Nummer 1 vorzulegen. Auf der Grundlage dieser Informationen können die Marktüberwachungsbehörden der ADCO anonymisierte und aggregierte Informationen über Softwareabhängigkeiten zur Verfügung stellen. Die ADCO legt der gemäß Artikel 14 der Richtlinie (EU) 2022/2555 eingesetzten Kooperationsgruppe einen Bericht über die Ergebnisse der Abhängigkeitsbewertung vor.

Artikel 14

Meldepflichten der Hersteller

(1) Ein Hersteller meldet jede aktiv ausgenutzte Schwachstelle, die in dem Produkt mit digitalen Elementen enthalten ist und von der er Kenntnis erlangt, gleichzeitig dem gemäß Absatz 7 als Koordinator benannten CSIRT und der ENISA. Der Hersteller meldet diese aktiv ausgenutzte Schwachstelle über die gemäß Artikel 16 eingerichtete einheitliche Meldeplattform.

(2) Für die Zwecke der Mitteilung gemäß Absatz 1 legt der Hersteller Folgendes vor:

a) unverzüglich, in jedem Fall aber innerhalb von 24 Stunden, nachdem der Hersteller davon Kenntnis erlangt hat, eine Frühwarnung über eine aktiv ausgenutzte Schwachstelle unter Angabe der Mitgliedstaaten, in deren Hoheitsgebiet das Produkt mit digitalen Elementen des Herstellers seiner Kenntnis nach bereitgestellt wurde;

b) sofern die einschlägigen Informationen nicht bereits vorgelegt wurden, unverzüglich, in jedem Fall aber innerhalb von 72 Stunden, nachdem der Hersteller Kenntnis von der aktiv ausgenutzten Schwachstelle erlangt hat, eine Meldung von Schwachstellen, die allgemeine Informationen, soweit verfügbar, über das betreffende Produkt mit digitalen Elementen, über die allgemeine Art der Ausnutzung und der betreffenden Schwachstelle sowie über alle ergriffenen Korrektur- oder Risikominderungsmaßnahmen sowie Korrektur- oder Abhilfemaßnahmen, die Nutzer ergreifen können, enthält und in der gegebenenfalls auch angegeben wird, als wie sensibel der Hersteller die gemeldeten Informationen ansieht;

c) sofern die einschlägigen Informationen nicht bereits vorgelegt wurden, spätestens 14 Tage, nachdem eine Korrektur- oder Risikominderungsmaßnahme zur Verfügung steht, einen Abschlussbericht, der mindestens Folgendes enthält:

   i) eine Beschreibung der Schwachstelle, einschließlich ihres Schweregrads und ihrer Auswirkungen,

   ii) falls verfügbar, Informationen über jeden böswilligen Akteur, der die Schwachstelle ausgenutzt hat oder ausnutzt,

   iii) Informationen über die Sicherheitsaktualisierung oder andere Korrekturmaßnahmen, die zur Behebung der Schwachstelle zur Verfügung gestellt wurden.

(3) Ein Hersteller meldet jeden schwerwiegenden Sicherheitsvorfall, der sich auf die Sicherheit des Produkts mit digitalen Elementen auswirkt und von der er Kenntnis erlangt, gleichzeitig dem gemäß Absatz 7 als Koordinator benannten CSIRT und der ENISA. Der Hersteller meldet diesen Sicherheitsvorfall über die gemäß Artikel 16 eingerichtete einheitliche Meldeplattform.

(4) Für die Zwecke der Mitteilung gemäß Absatz 3 legt der Hersteller Folgendes vor:

a) unverzüglich und in jedem Fall innerhalb von 24 Stunden, nachdem der Hersteller davon Kenntnis erlangt hat, eine Frühwarnung über einen schwerwiegenden Sicherheitsvorfall, der sich auf die Sicherheit des Produkts mit digitalen Elementen auswirkt, wobei zumindest anzugeben ist, ob der Verdacht besteht, dass der Sicherheitsvorfall auf rechtswidrige oder böswillige Handlungen zurückzuführen ist, wobei gegebenenfalls auch die Mitgliedstaaten anzugeben sind, in deren Hoheitsgebiet das Produkt mit digitalen Elementen des Herstellers seiner Kenntnis nach bereitgestellt wurde;

b) sofern die einschlägigen Informationen nicht bereits übermittelt wurden, unverzüglich, in jedem Fall aber innerhalb von 72 Stunden, nachdem der Hersteller von dem Sicherheitsvorfall Kenntnis erlangt hat, eine Meldung des Sicherheitsvorfalls, die allgemeine Informationen, soweit verfügbar, über die Art des Sicherheitsvorfalls, eine erste Bewertung des Sicherheitsvorfalls sowie ergriffene Korrektur- oder Risikominderungsmaßnahmen und Korrektur- oder Abhilfemaßnahmen, die Nutzer ergreifen können, enthält und in der gegebenenfalls auch angegeben wird, als wie sensibel der Hersteller die gemeldeten Informationen ansieht;

c) sofern die einschlägigen Informationen nicht bereits übermittelt wurden, innerhalb eines Monats nach Übermittlung der Meldung des Sicherheitsvorfalls gemäß Buchstabe b einen Abschlussbericht, der mindestens Folgendes enthält:

   i) eine ausführliche Beschreibung des Sicherheitsvorfalls, einschließlich seines Schweregrads und seiner Auswirkungen;

   ii) Angaben zur Art der Bedrohung bzw. zugrunde liegenden Ursache, die wahrscheinlich den Sicherheitsvorfall ausgelöst hat;

   iii) Angaben zu den getroffenen und laufenden Abhilfemaßnahmen.

(5) Für die Zwecke von Absatz 3 gilt ein Sicherheitsvorfall, der Auswirkungen auf die Sicherheit des Produkts mit digitalen Elementen hat, als schwerwiegend, wenn

a) er sich negativ auf die Fähigkeit eines Produkts mit digitalen Elementen auswirkt oder auswirken kann, die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit von sensiblen oder wichtigen Daten oder Funktionen zu schützen, oder

b) er zur Einführung oder Ausführung eines böswilligen Codes in einem Produkt mit digitalen Elementen oder im Netzwerk und Informationssystem eines Nutzers des Produkts mit digitalen Elementen geführt hat oder dazu führen kann.

(6) Erforderlichenfalls kann das als Koordinator benannte CSIRT, dass ursprünglich die Meldung erhält, die Hersteller auffordern, einen Zwischenbericht über relevante Statusaktualisierungen über die aktiv genutzte Schwachstelle oder den schwerwiegenden Sicherheitsvorfall, der sich auf die Sicherheit des Produkts mit digitalen Elementen auswirkt, vorzulegen.

(7) Die Meldungen gemäß den Absätzen 1 und 3 des vorliegenden Artikels werden über die in Artikel 16 genannte einheitliche Meldeplattform unter Verwendung eines der in Artikel 16 Absatz 1 genannten Endpunkte für die elektronische Meldung übermittelt. Die Meldung wird über den Endpunkt für die elektronische Meldung des CSIRT übermittelt, der als Koordinator des Mitgliedstaats benannt wurde, in dem die Hersteller ihre Hauptniederlassung in der Union haben, und ist gleichzeitig für die ENISA zugänglich.

Für die Zwecke dieser Verordnung wird davon ausgegangen, dass ein Hersteller seine Hauptniederlassung in der Union in dem Mitgliedstaat hat, in dem die Entscheidungen im Zusammenhang mit der Cybersicherheit seiner Produkte mit digitalen Elementen überwiegend getroffen werden. Kann ein solcher Mitgliedstaat nicht bestimmt werden, so gilt als Mitgliedstaat der Hauptniederlassung der Mitgliedstaat, in dem der betreffende Hersteller die Niederlassung mit der höchsten Beschäftigtenzahl in der Union hat.

Hat ein Hersteller keine Hauptniederlassung in der Union, so übermittelt er die in den Absätzen 1 und 3 genannten Meldungen unter Verwendung des Endpunkts für die elektronische Meldung des in dem Mitgliedstaat als Koordinator benannten CSIRT, der gemäß folgender Reihenfolge und auf der Grundlage der dem Hersteller zur Verfügung stehenden Informationen bestimmt wurde:

a) der Mitgliedstaat, in dem der Bevollmächtigte niedergelassen ist, der für die meisten Produkte mit digitalen Elementen des Herstellers im Namen des Herstellers handelt;

b) der Mitgliedstaat, in dem der Einführer niedergelassen ist, der die meisten Produkte mit digitalen Elementen dieses Herstellers in den Verkehr bringt;

c) der Mitgliedstaat, in dem der Händler niedergelassen ist, der die meisten Produkte mit digitalen Elementen dieses Herstellers auf dem Markt bereitstellt;

d) der Mitgliedstaat, in dem sich die meisten Nutzer von Produkten mit digitalen Elementen dieses Herstellers befinden.

In Bezug auf Unterabsatz 3 Buchstabe d kann ein Hersteller Meldungen im Zusammenhang mit späteren aktiv ausgenutzten Schwachstellen oder schwerwiegenden Sicherheitsvorfällen, die sich auf die Sicherheit des Produkts mit digitalen Elementen auswirken, an dasselbe CSIRT richten, das als Koordinator benannt wurde und dem er zuerst Meldung erstattet hat.

(8) Nachdem der Hersteller Kenntnis von einer aktiv ausgenutzten Schwachstelle oder einem schwerwiegenden Sicherheitsvorfall, der sich auf die Sicherheit des Produkts mit digitalen Elementen auswirkt, erlangt hat, informiert er die betroffenen Nutzer des Produkts mit digitalen Elementen und gegebenenfalls alle Nutzer über diese Schwachstelle oder diesen schwerwiegenden Sicherheitsvorfall und erforderlichenfalls über jegliche Risikominderungsmaßnahmen und Korrekturmaßnahmen, die die Nutzer ergreifen können, um die Auswirkungen dieser Schwachstellen oder Sicherheitsvorfälle zu mindern, gegebenenfalls in einem strukturierten, maschinenlesbaren Format, das leicht automatisch zu verarbeiten ist. Versäumt es der Hersteller, die Nutzer des Produkts mit digitalen Elementen rechtzeitig zu informieren, können die als Koordinatoren benannten CSIRTs diese Informationen den Nutzern zur Verfügung stellen, wenn sie dies für verhältnismäßig und erforderlich halten, um die Auswirkungen dieser Schwachstellen oder Sicherheitsvorfälle zu verhindern oder abzumildern.

(9) Bis zum 11. Dezember 2025 erlässt die Kommission einen delegierten Rechtsakt gemäß Artikel 61 der vorliegenden Verordnung zur Ergänzung dieser Verordnung durch Festlegung der Modalitäten und Bedingungen für die Anwendung der Cybersicherheitsgründe im Zusammenhang mit der Verzögerung der Verbreitung von Meldungen gemäß Artikel 16 Absatz 2 der vorliegenden Verordnung. Die Kommission arbeitet bei der Ausarbeitung des Entwurfs des delegierten Rechtsakts mit dem gemäß Artikel 15 der Richtlinie (EU) 2022/2555 eingerichteten CSIRTs-Netzwerk und der ENISA zusammen.

(10) Die Kommission kann im Wege von Durchführungsrechtsakten das Format und die Verfahren für die in diesem Artikel sowie in den Artikeln 15 und 16 genannten Meldungen präzisieren. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 62 Absatz 2 genannten Prüfverfahren erlassen. Die Kommission arbeitet bei der Ausarbeitung der Entwürfe von Durchführungsrechtsakten mit dem CSIRTs-Netzwerk und der ENISA zusammen.

Artikel 15

Freiwillige Meldungen

(1) Hersteller sowie andere natürliche oder juristische Personen können jede in einem Produkt mit digitalen Elementen enthaltene Schwachstelle sowie Cyberbedrohungen, die sich auf das Risikoprofil eines Produkts mit digitalen Elementen auswirken könnten, freiwillig einem als Koordinator benannten CSIRT oder der ENISA melden.

(2) Hersteller sowie andere natürliche oder juristische Personen können jeden Sicherheitsvorfall, der sich auf die Sicherheit des Produkts mit digitalen Elementen auswirkt, sowie Beinahe-Vorfälle, die zu einem solchen Sicherheitsvorfall hätten führen können, auf freiwilliger Basis einem als Koordinator benannten CSIRT oder der ENISA melden.

(3) Das als Koordinator benannte CSIRT oder die ENISA bearbeitet die in den Absätze 1 und 2 genannten Meldungen nach dem in Artikel 16 vorgesehenen Verfahren.

Das als Koordinator benannte CSIRT kann verpflichtende Meldungen vorrangig vor freiwilligen Meldungen bearbeiten.

(4) Meldet eine andere natürliche oder juristische Person als der Hersteller gemäß Absatz 1 oder 2 eine aktiv ausgenutzte Schwachstelle oder einen schwerwiegenden Sicherheitsvorfall mit Auswirkungen auf die Sicherheit eines Produkts mit digitalen Elementen, so unterrichtet das als Koordinator benannte CSIRT den Hersteller unverzüglich.

(5) Die als Koordinator benannten CSIRTs und die ENISA stellen die Vertraulichkeit und den angemessenen Schutz der von einer meldenden natürlichen oder juristischen Person übermittelten Informationen sicher. Unbeschadet der Verhütung, Ermittlung, Aufdeckung und Verfolgung von Straftaten dürfen die freiwilligen Meldungen nicht dazu führen, dass der meldenden natürlichen oder juristischen Person zusätzliche Pflichten auferlegt werden, die nicht für sie gegolten hätten, wenn sie die Meldung nicht übermittelt hätte.

Artikel 16

Einrichtung einer einheitlichen Meldeplattform

(1) Für die Zwecke der Meldungen gemäß Artikel 14 Absätze 1 und 3 und Artikel 15 Absätze1 und 2 und zur Vereinfachung der Meldepflichten der Hersteller richtet die ENISA eine einheitliche Meldeplattform ein. Der laufende Betrieb dieser einheitlichen Meldeplattform wird von der ENISA gesteuert und aufrechterhalten. Die Architektur der einheitlichen Meldeplattform muss es den Mitgliedstaaten und der ENISA ermöglichen, ihre eigenen Endpunkte für die elektronische Meldung einzurichten.

(2) Nach Erhalt einer Meldung leitet das als Koordinator benannte CSIRT, das die Meldung ursprünglich erhält, die Meldung über die einheitliche Meldeplattform unverzüglich an die als Koordinatoren benannten CSIRT weiter, in deren Hoheitsgebiet das Produkt mit digitalen Elementen nach Angaben des Herstellers bereitgestellt wurde.

Unter außergewöhnlichen Umständen und insbesondere auf Antrag des Herstellers und angesichts des vom Hersteller gemäß Artikel 14 Absatz 2 Buchstabe a der vorliegenden Verordnung angegebenen Grades der Sensibilität der gemeldeten Informationen kann die Verbreitung der Meldung aus berechtigten Gründen im Zusammenhang mit der Cybersicherheit so lange, wie unbedingt erforderlich, hinausgeschoben werden, auch wenn eine Schwachstelle einem koordinierten Verfahren zur Offenlegung von Schwachstellen gemäß Artikel 12 Absatz 1 der Richtlinie (EU) 2022/2555 unterliegt. Beschließt ein CSIRT, eine Meldung zurückzuhalten, so unterrichtet es die ENISA unverzüglich über die Entscheidung und legt sowohl eine Begründung für die Zurückhaltung der Meldung als auch eine Angabe dazu vor, wann es die Meldung gemäß dem in diesem Absatz festgelegten Verfahren verbreiten wird. Die ENISA kann das CSIRT bei der Anwendung von Cybersicherheitsgründen im Zusammenhang mit der Verzögerung der Verbreitung der Meldung unterstützen.

Unter besonderen außergewöhnlichen Umständen, wenn der Hersteller in der Mitteilung gemäß Artikel 14 Absatz 2 Buchstabe b Folgendes angibt:

a) dass die gemeldete Schwachstelle von einem böswilligen Akteur aktiv ausgenutzt wurde und den verfügbaren Informationen zufolge in keinem anderen Mitgliedstaat als dem der als Koordinator benannten CSIRT, der der Hersteller die Schwachstelle gemeldet hat, ausgenutzt wurde;

b) dass eine sofortige weitere Verbreitung der gemeldeten Schwachstelle wahrscheinlich zur Bereitstellung von Informationen führen würde, deren Offenlegung den wesentlichen Interessen des betreffenden Mitgliedstaats zuwiderlaufen würde; oder

c) dass die gemeldete Schwachstelle ein unmittelbares hohes Cybersicherheitsrisiko darstellt, das sich aus der weiteren Verbreitung ergibt,

werden nur die Informationen darüber, dass der Hersteller eine Meldung vorgenommen hat, die allgemeinen Informationen über das Produkt, die Informationen über die allgemeine Art der Ausnutzung und die Informationen, dass Sicherheitsgründe geltend gemacht wurden, gleichzeitig der ENISA zur Verfügung gestellt, bis die vollständige Meldung an die betreffenden CSIRTs und die ENISA weitergeleitet wird. Ist die ENISA auf der Grundlage dieser Informationen der Auffassung, dass ein Systemrisiko für die Sicherheit des Binnenmarkts besteht, empfiehlt sie dem CSIRT, bei dem die Meldung eingegangen ist, die vollständige Meldung an die anderen als Koordinatoren benannten CSIRTs und an die ENISA selbst weiterzuleiten.

(3) Nach Erhalt einer Meldung über eine aktiv ausgenutzte Schwachstelle in einem Produkt mit digitalen Elementen oder über einen schwerwiegenden Sicherheitsvorfall, der sich auf die Sicherheit eines Produkts mit digitalen Elementen auswirkt, stellen die als Koordinatoren benannten CSIRTs den Marktüberwachungsbehörden ihres jeweiligen Mitgliedstaats die gemeldeten Informationen zur Verfügung, die diese benötigen, damit sie ihren Verpflichtungen gemäß dieser Verordnung nachkommen können.

(4) Die ENISA ergreift geeignete und verhältnismäßige technische, operative und organisatorische Maßnahmen, um die Risiken für die Sicherheit der einheitlichen Meldeplattform und der über die einheitliche Meldeplattform übermittelten oder verbreiteten Informationen zu bewältigen. Sie meldet dem CSIRTs-Netzwerk und der Kommission unverzüglich jeden Sicherheitsvorfall, der die einheitliche Meldeplattform betrifft.

(5) Die ENISA stellt in Zusammenarbeit mit dem CSIRTs-Netzwerk Spezifikationen für die technischen, operativen und organisatorischen Maßnahmen für die Einrichtung, die Pflege und den sicheren Betrieb der einheitlichen Meldeplattform gemäß Absatz 1bereit und setzt sie um, einschließlich zumindest der Sicherheitsvorkehrungen im Zusammenhang mit der Einrichtung, dem Betrieb und der Wartung der einheitlichen Meldeplattform sowie der von den als Koordinatoren auf nationaler Ebene benannten CSIRTs und der ENISA auf Unionsebene eingerichteten Endpunkte für die elektronische Meldung, einschließlich Verfahrensaspekten, um sicherzustellen, dass Informationen über diese Schwachstellen im Einklang mit strengen Sicherheitsprotokollen und nach dem Grundsatz „Kenntnis nur, wenn nötig“ weitergegeben werden, wenn für eine gemeldete Schwachstelle keine Korrektur- oder Risikominderungsmaßnahmen verfügbar sind.

(6) Wurde ein CSIRT, das als Koordinator benannt wurde, im Rahmen eines koordinierten Verfahrens zur Offenlegung von Schwachstellen gemäß Artikel 12 Absatz 1 der Richtlinie (EU) 2022/2555 auf eine aktiv ausgenutzte Schwachstelle aufmerksam gemacht, so kann das als Koordinator benannte CSIRT, das die Meldung ursprünglich erhalten hat, die Verbreitung der betreffenden Meldung über die einheitliche Meldeplattform aus berechtigten Gründen im Zusammenhang mit der Cybersicherheit um einen Zeitraum aufschieben, der nicht länger als unbedingt erforderlich ist, bis die beteiligten Parteien der koordinierten Offenlegung von Schwachstellen ihre Zustimmung zur Offenlegung erteilt haben. Diese Anforderung hindert die Hersteller nicht daran, eine solche Schwachstelle freiwillig nach dem in diesem Artikel festgelegten Verfahren zu melden.

Artikel 17

Sonstige Bestimmungen im Zusammenhang mit der Berichterstattung

(1) Die ENISA kann dem Europäischen Netzwerk der Verbindungsorganisationen für Cyberkrisen (EU-CyCLONe), das durch Artikel 16 der Richtlinie (EU) 2022/2555 eingerichtet wurde, die gemäß Artikel 14 Absätze 1 und 3 und Artikel 15 Absätze 1 und 2 der vorliegenden Verordnung gemeldeten Informationen, sofern diese Informationen für das koordinierte Management massiver Cybersicherheitsvorfälle und -krisen auf operativer Ebene von Bedeutung sind. Für die Zwecke der Bestimmung dieser Bedeutung kann die ENISA gegebenenfalls technische Analysen des CSIRTs-Netzwerks berücksichtigen.

(2) Ist eine Sensibilisierung der Öffentlichkeit erforderlich, um einen schwerwiegenden Sicherheitsvorfall mit Auswirkungen auf die Sicherheit des Produkts mit digitalen Elementen zu verhindern oder zu mindern oder um einen laufenden Sicherheitsvorfall zu bewältigen, oder liegt die Offenlegung des Sicherheitsvorfalls anderweitig im öffentlichen Interesse, so kann das als Koordinator des betreffenden Mitgliedstaats benannte CSIRT nach Konsultation des betreffenden Herstellers und gegebenenfalls in Zusammenarbeit mit der ENISA die Öffentlichkeit über den Sicherheitsvorfall informieren oder den Hersteller auffordern, dies zu tun.

(3) Die ENISA erstellt auf der Grundlage der nach Artikel 14 Absätze 1 und 3 und Artikel 15 Absätze 1 und 2 der vorliegenden Verordnung eingegangenen Meldungen alle 24 Monate einen technischen Bericht über aufkommende Trends der Cybersicherheitsrisiken bei Produkten mit digitalen Elementen und legt ihn der gemäß Artikel 14 der Richtlinie (EU) 2022/2555 eingerichteten Kooperationsgruppe vor. Der erste solche Bericht wird innerhalb von 24 Monaten nach Beginn der Geltung der in Artikel 14 Absätze 1 und 3 festgelegten Pflichten vorgelegt. Die ENISA nimmt einschlägige Informationen aus ihren technischen Berichten in ihren Bericht über den Stand der Cybersicherheit in der Union gemäß Artikel 18 der Richtlinie (EU) 2022/2555 auf.

(4) Die bloße Meldung gemäß Artikel 14 Absätze 1 und 3 und Artikel 15 Absätze 1 und 2 begründet keine höhere Haftung der meldenden natürlichen oder juristischen Person.

(5) Sobald eine Sicherheitsaktualisierung oder eine andere Form von Korrektur- oder Risikominderungsmaßnahme verfügbar ist, nimmt die ENISA im Einvernehmen mit dem Hersteller des betreffenden Produkts mit digitalen Elementen die gemäß Artikel 14 Absatz 1 oder Artikel 15 Absatz 1 der vorliegenden Verordnung gemeldete öffentlich bekannte Schwachstelle in die gemäß Artikel 12 Absatz 2 der Richtlinie (EU) 2022/2555 eingerichtete europäische Schwachstellendatenbank auf.

(6) Die als Koordinatoren benannten CSIRTs bieten Helpdesk-Unterstützung für Hersteller und insbesondere Hersteller, die als Kleinstunternehmen oder als kleine oder mittlere Unternehmen gelten, in Bezug auf die Meldepflichten gemäß Artikel 14.

Artikel 18

Bevollmächtigte

(1) Ein Hersteller kann schriftlich einen Bevollmächtigten benennen.

(2) Die in Artikel 13 Absatz 1 bis Absatz 11, Artikel 13 Absatz 12 Unterabsatz 1 und Artikel 13 Absatz 14 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 Bevollmächtigte legt den Marktüberwachungsbehörden auf Verlangen eine Kopie des Auftrags vor. Der Auftrag muss es dem Bevollmächtigten ermöglichen, mindestens folgende Aufgaben wahrzunehmen:

a) Bereithaltung der in Artikel 28 genannten EU-Konformitätserklärung und der in Artikel 31 genannten technischen Dokumentation für die Marktüberwachungsbehörden mindestens zehn Jahre lang ab dem Inverkehrbringen des Produkts mit digitalen Elementen oder für den Unterstützungszeitraum, je nachdem, welcher Zeitraum länger ist;

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 19

Pflichten der Einführer

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

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

a) der Hersteller die geeigneten Konformitätsbewertungsverfahren nach Artikel 32 durchgeführt hat;

b) der Hersteller die technische Dokumentation erstellt hat;

c) das Produkt mit digitalen Elementen mit der in Artikel 30 genannten CE-Kennzeichnung versehen ist und ihm die EU-Konformitätserklärung gemäß Artikel 13 Absatz 20 sowie die Informationen und Anleitungen für den Nutzer gemäß Anhang II in einer Sprache, die von den Nutzern und den Marktüberwachungsbehörden leicht verstanden werden kann, beigefügt sind;

d) der Hersteller die in Artikel 13 Absätze 15, 16 und 19 genannten Anforderungen erfüllt.

Für die Zwecke dieses Absatzes müssen die Einführer in der Lage sein, die erforderlichen Unterlagen zum Nachweis der Erfüllung der in diesem Artikel festgelegten Anforderungen vorzulegen.

(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 dieser Verordnung nicht genügen, bringt er das Produkt erst dann in den Verkehr, wenn die Konformität dieses Produkts und der vom Hersteller festgelegten Verfahren mit dieser Verordnung hergestellt ist. Wenn das Produkt mit digitalen Elementen ein erhebliches Cybersicherheitsrisiko birgt, unterrichtet der Einführer zudem den Hersteller und die Marktüberwachungsbehörden hiervon.

Hat ein Einführer Grund zu der Annahme, dass ein Produkt mit digitalen Elementen angesichts nichttechnischer Risikofaktoren ein erhebliches Cybersicherheitsrisiko darstellen könnte, so unterrichtet er die Marktüberwachungsbehörden hiervon. Nach Erhalt dieser Informationen befolgen die Marktüberwachungsbehörden die in Artikel 54 Absatz 2 genannten Verfahren.

(4) Die Einführer geben ihren Namen, ihren eingetragenen Handelsnamen oder ihre eingetragene Handelsmarke, ihre Postanschrift, ihre E-Mail-Adresse oder andere digitale Kontaktmöglichkeiten sowie gegebenenfalls die Website, unter der sie zu erreichen sind, entweder auf dem Produkt mit digitalen Elementen selbst oder 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) Einführer, denen bekannt ist oder die Grund zu der Annahme haben, dass ein Produkt mit digitalen Elementen, das sie in den Verkehr gebracht haben, dieser Verordnung nicht entspricht, ergreifen unverzüglich die erforderlichen Korrekturmaßnahmen, um sicherzustellen, dass die Konformität dieses Produkts mit digitalen Elementen mit dieser Verordnung hergestellt wird oder um gegebenenfalls das Produkt vom Markt zu nehmen oder zurückzurufen

Sobald die Einführer von einer Schwachstelle in dem Produkt mit digitalen Elementen Kenntnis erhalten, informieren sie 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.

(6) Die Einführer halten ab dem Inverkehrbringen des Produkts mit digitalen Elementen mindestens zehn Jahre lang oder für den Unterstützungszeitraum, je nachdem, welcher Zeitraum länger ist, ein Exemplar der EU-Konformitätserklärung für die Marktüberwachungsbehörden bereit und sorgen dafür, dass sie diesen die technische Dokumentation auf Verlangen vorlegen können.

(7) 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 Cybersicherheitsanforderungen in Anhang I Teil I und der vom Hersteller festgelegten Verfahren mit den grundlegenden

Cybersicherheitsanforderungen in Anhang I Teil II erforderlich sind. Sie arbeiten mit dieser Behörde auf deren Verlangen bei allen Maßnahmen zur Abwendung der Cybersicherheitsrisiken zusammen, die mit einem von ihnen in den Verkehr gebrachten Produkt mit digitalen Elementen verbunden sind.

(8) 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 einschlägigen Marktüberwachungsbehörden sowie — mit allen verfügbaren Mitteln und soweit möglich — die Nutzer der in den Verkehr gebrachten Produkte mit digitalen Elementen.

Artikel 20

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 13 Absätze 15, 16, 18, 19 und 20 sowie Artikel 19 Absatz 4 erfüllt haben und dem Händler alle erforderlichen Dokumente zur Verfügung gestellt haben.

(3) Ist ein Händler der Auffassung oder hat er ausgehend von den ihm vorliegenden Informationen Grund zu der Annahme, dass ein Produkt mit digitalen Elementen oder die vom Hersteller festgelegten Verfahren den grundlegenden Cybersicherheitsanforderungen 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 mit dieser Verordnung hergestellt ist. Wenn das Produkt mit digitalen Elementen ein erhebliches Cybersicherheitsrisiko birgt, unterrichtet der Händler zudem unverzüglich den Hersteller und die Marktüberwachungsbehörden hiervon.

(4) Händler, denen bekannt ist oder die ausgehend von den ihnen vorliegenden Informationen 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 dieser Verordnung nicht entsprechen, sorgen dafür, dass 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.

Sobald die Händler von einer Schwachstelle in dem Produkt mit digitalen Elementen Kenntnis erhalten, informieren sie 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 dieser Verordnung 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 ausgehend von den ihm vorliegenden Informationen-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 unverzüglich die einschlägigen Marktüberwachungsbehörden sowie — mit allen verfügbaren Mitteln und soweit möglich — die Nutzer der in den Verkehr gebrachten Produkte mit digitalen Elementen.

Artikel 21

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 den Artikeln 13 und 14 genannten Pflichten, wenn dieser Einführer oder Händler ein Produkt mit digitalen Elementen unter seinem eigenen Namen oder seiner eigenen Marke in den Verkehr bringt oder eine wesentliche Änderung an einem bereits in den Verkehr gebrachten Produkt mit digitalen Elementen vornimmt.

Artikel 22

Sonstige Fälle, in denen die Pflichten der Hersteller gelten

(1) 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 und dieses Produkt auf dem Markt bereitstellt, gilt für die Zwecke dieser Verordnung als Hersteller.

(2) Die in Absatz 1 des vorliegenden Artikels genannte Person unterliegt den in den Artikeln 13 und 14 festgelegten Pflichten für den Teil des Produkts mit digitalen Elementen, 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 23

Identifizierung der Wirtschaftsakteure

(1) Die Wirtschaftsakteure übermitteln den Marktüberwachungsbehörden auf Anfrage folgende Informationen:

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

b) sofern verfügbar, 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.

Artikel 24

Pflichten der Verwalter quelloffener Software

(1) Verwalter quelloffener Software entwickeln und dokumentieren auf überprüfbare Weise eine Cybersicherheitsstrategie, um die Entwicklung eines sicheren Produkts mit digitalen Elementen sowie einen wirksamen Umgang mit Schwachstellen durch die Entwickler dieses Produkts zu fördern. Diese Strategie fördert auch die freiwillige Meldung von Schwachstellen gemäß Artikel 15 durch die Entwickler dieses Produkts und trägt den Besonderheiten des Verwalters quelloffener Software und den rechtlichen und organisatorischen Vorkehrungen, denen er unterliegt, Rechnung. Diese Strategie umfasst insbesondere Aspekte im Zusammenhang mit der Dokumentation, Behebung und Beseitigung von Schwachstellen und fördert den Austausch von Informationen über aufgedeckte Schwachstellen innerhalb der Open-Source-Gemeinschaft.

(2) Verwalter quelloffener Software arbeiten auf deren Verlangen mit den Marktüberwachungsbehörden zusammen, um die Cybersicherheitsrisiken zu mindern, die von einem Produkt mit digitalen Elementen ausgehen, das als freie und quelloffene Software gilt.

Auf begründetes Verlangen einer Marktüberwachungsbehörde übermitteln Verwalter quelloffener Software dieser Behörde in einer für diese Behörde leicht verständlichen Sprache die in Absatz 1 genannten Unterlagen in Papierform oder in elektronischer Form.

(3) Die in Artikel 14 Absatz 1 festgelegten Verpflichtungen gelten für Verwalter quelloffener Software, soweit sie an der Entwicklung der Produkte mit digitalen Elementen beteiligt sind. Die in Artikel 14 Absätze 3 und 8 festgelegten Verpflichtungen gelten für Verwalter quelloffener Software, soweit schwerwiegende Sicherheitsvorfälle, die sich auf die Sicherheit von Produkten mit digitalen Elementen auswirken, Netz- und Informationssysteme beeinträchtigen, die von den Verwaltern quelloffener Software für die Entwicklung solcher Produkte bereitgestellt werden.

Artikel 25

Sicherheitsbescheinigung für freie und quelloffene Software

Um die in Artikel 13 Absatz 5 festgelegte Sorgfaltspflicht zu erleichtern, insbesondere in Bezug auf Hersteller, die freie und quelloffene Softwarekomponenten in ihre Produkte mit digitalen Elementen integrieren, wird der Kommission die Befugnis übertragen, gemäß Artikel 61 delegierte Rechtsakte zu erlassen, um diese Verordnung durch die Einführung freiwilliger Programme zur Bescheinigung der Sicherheit zu ergänzen, die es den Entwicklern oder Nutzern von Produkten mit digitalen Elementen, die als freie und quelloffene Software gelten, sowie anderen Dritten ermöglichen, die Konformität dieser Produkte mit allen oder bestimmten grundlegenden Cybersicherheitsanforderungen oder sonstigen in dieser Verordnung festgelegten Verpflichtungen zu bewerten.

Artikel 26

Leitlinien

(1) Um die Durchführung zu erleichtern und ihre Kohärenz sicherzustellen, veröffentlicht die Kommission Leitlinien, um die Wirtschaftsakteure bei der Anwendung dieser Verordnung zu unterstützen, wobei ein besonderer Schwerpunkt auf der Erleichterung der Einhaltung durch Kleinstunternehmen und kleine und mittlere Unternehmen liegt.

(2) Beabsichtigt die Kommission, Leitlinien gemäß Absatz 1 bereitzustellen, so geht sie mindestens auf folgende Aspekte ein:

a) den Anwendungsbereich dieser Verordnung mit besonderem Schwerpunkt auf Datenfernverarbeitungslösungen und freier und quelloffener Software,

b) die Anwendung von Unterstützungszeiträumen in Bezug auf bestimmte Kategorien von Produkten mit digitalen Elementen;

c) Leitlinien für Hersteller, die dieser Verordnung unterliegen und auch anderen Harmonisierungsrechtsvorschriften der Union als dieser Verordnung oder anderen damit zusammenhängenden Rechtsakten der Union unterliegen;

d) den Begriff der wesentlichen Änderung.

Die Kommission führt ferner eine leicht zugängliche Liste der gemäß dieser Verordnung erlassenen delegierten Rechtsakte und Durchführungsrechtsakte.

(3) Bei der Ausarbeitung der Leitlinien gemäß diesem Artikel konsultiert die Kommission die einschlägigen Interessenträger.

KAPITEL III

KONFORMITÄT DES PRODUKTS MIT DIGITALEN ELEMENTEN

Artikel 27

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 Cybersicherheitsanforderungen in Anhang I vermutet, soweit diese Anforderungen von den betreffenden Normen oder Teilen davon abgedeckt sind.

Die Kommission fordert gemäß Artikel 10 Absatz 1 der Verordnung (EU) Nr. 1025/2012 eine oder mehrere europäische Normungsorganisationen auf, harmonisierte Normen für die in Anhang I dieser Verordnung aufgeführten grundlegenden Cybersicherheitsanforderungen auszuarbeiten. Bei der Ausarbeitung von Normungsanträgen für diese Verordnung bemüht sich die Kommission, bestehende europäische und internationale Normen für Cybersicherheit zu berücksichtigen, die in Kraft sind oder gerade entwickelt werden, um die Entwicklung harmonisierter Normen im Einklang mit der Verordnung (EU) Nr. 1025/2012 zu vereinfachen.

(2) Die Kommission kann Durchführungsrechtsakte annehmen, durch die gemeinsame Spezifikationen zu technischen Anforderungen festgelegt werden, deren Befolgung es ermöglicht, die in Anhang I festgelegten grundlegenden Cybersicherheitsanforderungen an Produkte mit digitalen Elementen im Anwendungsbereich dieser Verordnung zu erfüllen.

Diese Durchführungsrechtsakte dürfen nur erlassen werden, wenn die folgenden Bedingungen erfüllt sind:

a) die Kommission hat gemäß Artikel 10 Absatz 1 der Verordnung (EU) Nr. 1025/2012 eine oder mehrere europäische Normungsorganisationen aufgefordert, eine harmonisierte Norm für die in Anhang I aufgeführten grundlegenden Cybersicherheitsanforderungen zu erarbeiten, und:

   i) der Auftrag wurde nicht angenommen,

   ii) die harmonisierten Normen, die dieser Antrag betrifft, werden nicht im Rahmen der in Übereinstimmung mit Artikel 10 Absatz 1 der Verordnung (EU) Nr. 1025/2012 gesetzten Frist geliefert, oder

   iii) die harmonisierten Normen entsprechen nicht dem Auftrag, und

b) im *Amtsblatt der Europäischen Union* wurde kein Verweis im Einklang mit der Verordnung (EU) Nr. 1025/2012 auf harmonisierte Normen, die den einschlägigen grundlegenden Cybersicherheitsanforderungen nach Anhang I der vorliegenden Verordnung genügen, veröffentlicht, und es ist nicht zu erwarten, dass ein solcher Verweis innerhalb eines angemessenen Zeitraums veröffentlicht wird.

Diese Durchführungsrechtsakte werden gemäß dem in Artikel 62 Absatz 2 genannten Prüfverfahren erlassen.

(3) Vor der Ausarbeitung eines Entwurfs des in Absatz 2 des vorliegenden Artikels genannten Durchführungsrechtsakts teilt die Kommission dem in Artikel 22 der Verordnung (EU) Nr. 1025/2012 genannten Ausschuss mit, dass sie die Bedingungen nach Absatz 2 des vorliegenden Artikels als erfüllt erachtet.

(4) Bei der Ausarbeitung eines Entwurfs des in Absatz 2 genannten Durchführungsrechtsakt berücksichtigt die Kommission die Standpunkte der einschlägigen Gremien und konsultiert alle einschlägigen Interessenträger ordnungsgemäß.

(5) Bei Produkten mit digitalen Elementen und vom Hersteller festgelegten Verfahren, die mit den gemeinsamen Spezifikationen übereinstimmen, die durch den in Absatz 2 dieses Artikels genannten Durchführungsrechtsakt festgelegt wurden, wird eine Konformität mit den grundlegenden Cybersicherheitsanforderungen in Anhang I vermutet, soweit die gemeinsamen Spezifikationen oder Teile davon diese Anforderungen abdecken.

(6) Wird eine harmonisierte Norm von einer europäischen Normungsorganisation angenommen und der Kommission zur Veröffentlichung ihrer Fundstelle im *Amtsblatt der Europäischen Union* vorgeschlagen, so bewertet die Kommission diese harmonisierte Norm gemäß der Verordnung (EU) Nr. 1025/2012. Wenn eine Fundstelle einer harmonisierten Norm im *Amtsblatt der Europäischen Union* der Europäischen Union veröffentlicht wird, hebt die Kommission die in Absatz 2 des vorliegenden Artikels genannten Durchführungsrechtsakte oder Teile davon auf, die dieselben grundlegenden Cybersicherheitsanforderungen wie die harmonisierte Norm regeln.

(7) Ist ein Mitgliedstaat der Auffassung, dass eine gemeinsame Spezifikation den grundlegenden Cybersicherheitsanforderungen nach Anhang I nicht vollständig entspricht, so setzt er die Kommission mittels einer ausführlichen Erläuterung davon in Kenntnis. Die Kommission bewertet die ausführliche Erläuterung und kann gegebenenfalls den Durchführungsrechtsakt, durch den die betreffende gemeinsame Spezifikation festgelegt wurde, ändern.

(8) 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 europäischen Schemas für die Cybersicherheitszertifizierung ausgestellt wurde, wird eine Konformität mit den grundlegenden Cybersicherheitsanforderungen in Anhang I vermutet, sofern die EU-Konformitätserklärung oder das europäische Cybersicherheitszertifikat oder Teile davon diese Anforderungen abdecken.

(9) Der Kommission wird die Befugnis übertragen, delegierte Rechtsakte gemäß Artikel 61 zu erlassen, um diese Verordnung durch die Ausweisung der gemäß der Verordnung (EU) 2019/881 angenommenen europäischen Schemata für die Cybersicherheitszertifizierung zu ergänzen, die zum Nachweis der Konformität von Produkten mit digitalen Elementen mit den grundlegenden Cybersicherheitsanforderungen in Anhang I oder Teilen davon verwendet werden können. Darüber hinaus wird durch die Ausstellung eines im Rahmen eines solchen Schemas ausgestellten europäischen Cybersicherheitszertifikats mindestens der Vertrauenswürdigkeitsstufe „mittel“ die in Artikel 32 Absatz 2 Buchstaben a und b und Artikel 32 Absatz 3 Buchstaben a und b vorgesehene Pflicht des Herstellers, für die betreffenden Anforderungen eine Konformitätsbewertung durch Dritte durchführen zu lassen, aufgehoben.

Artikel 28

EU-Konformitätserklärung

(1) Die EU-Konformitätserklärung wird vom Hersteller gemäß Artikel 13 Absatz 12 ausgestellt und besagt, dass die Erfüllung der grundlegenden Cybersicherheitsanforderungen in Anhang I nachgewiesen worden ist.

(2) Die EU-Konformitätserklärung entspricht in ihrem Aufbau dem Muster in Anhang V und enthält die in den einschlägigen Konformitätsbewertungsverfahren gemäß Anhang VIII angegebenen Elemente. Eine solche Erklärung wird nach Bedarf aktualisiert. Sie wird in den Sprachen abgefasst, die der Mitgliedstaat vorschreibt, in dem das Produkt mit digitalen Elementen in den Verkehr gebracht oder auf dem Markt bereitgestellt wird.

Die vereinfachte EU-Konformitätserklärung nach Artikel 13 Absatz 20 entspricht in ihrem Aufbau dem Muster in Anhang VI. Sie wird in den Sprachen abgefasst, die der Mitgliedstaat vorschreibt, in dem das Produkt mit digitalen Elementen in den 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 Unionsrechtsvorschriften ausgestellt. In dieser Erklärung sind die betreffenden Rechtsakte der Union samt ihren Fundstellen im Amtsblatt anzugeben.

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

(5) Der Kommission wird die Befugnis übertragen, gemäß Artikel 61 delegierte Rechtsakte zur Ergänzung dieser Verordnung zu erlassen, um angesichts der technischen Entwicklungen zu den in Anhang V aufgeführten Mindestangaben für die EU-Konformitätserklärung neue Elemente hinzuzufügen.

Artikel 29

Allgemeine Grundsätze der CE-Kennzeichnung

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

Artikel 30

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 28 angebracht. Bei Produkten mit digitalen Elementen in Form von Software wird die CE-Kennzeichnung entweder auf der EU-Konformitätserklärung gemäß Artikel 28 oder auf der das Softwareprodukt begleitenden Website angebracht. Im letzteren Fall muss der relevante Abschnitt der Website für Verbraucher leicht und direkt zugänglich sein.

(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 Cybersicherheitsrisiko oder eine besondere Verwendung hinweist, die in den 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 32 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 Harmonisierungsrechtsvorschriften der Union als diese Verordnung fällt, in denen die CE-Kennzeichnung ebenfalls vorgesehen ist, bedeutet die CE-Kennzeichnung, dass das Produkt auch die Anforderungen dieser anderen Harmonisierungsrechtsvorschriften der Union erfüllt.

(6) Die Kommission kann im Wege von Durchführungsrechtsakten technische Spezifikationen für Etiketten, Piktogramme oder andere Kennzeichen in Bezug auf die Sicherheit von Produkten mit digitalen Elementen, deren Unterstützungszeiträume sowie Mechanismen zur Förderung ihrer Verwendung und zur Sensibilisierung der Öffentlichkeit für die Sicherheit von Produkten mit digitalen Elementen festlegen. Bei der Ausarbeitung der Entwürfe von Durchführungsrechtsakten konsultiert die Kommission die einschlägigen Interessenträger und, falls sie bereits gemäß Artikel 52 Absatz 15 eingerichtet wurde, die ADCO. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 62 Absatz 2 genannten Prüfverfahren erlassen.

Artikel 31

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 Cybersicherheitsanforderungen in Anhang I genügen. Sie enthält zumindest die in Anhang VII genannten Angaben.

(2) Die technische Dokumentation wird vor dem Inverkehrbringen des Produkts mit digitalen Elementen erstellt und gegebenenfalls, zumindest während des Unterstützungszeitraums, laufend aktualisiert.

(3) Bei Produkten mit digitalen Elementen gemäß Artikel 12, die auch anderen Rechtsakten der Union unterliegen, in denen eine technische Dokumentation vorgesehen ist, wird eine einzige technische Dokumentation erstellt, die die in Anhang VII genannten Informationen sowie die nach den anderen Rechtsakten der Union 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 61 delegierte Rechtsakte zu erlassen, mit denen diese Verordnung durch Hinzufügung von Elementen ergänzt wird, die in die technische Dokumentation gemäß Anhang VII aufzunehmen sind, um den technischen Entwicklungen und den Entwicklungen bei der Durchführung dieser Verordnung Rechnung zu tragen. Zu diesem Zweck bemüht sich die Kommission, sicherzustellen, dass der Verwaltungsaufwand für Kleinstunternehmen sowie kleine und mittlere Unternehmen verhältnismäßig ist.

Artikel 32

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 Cybersicherheitsanforderungen in Anhang I erfüllt sind. Der Hersteller erbringt den Nachweis der Konformität mit den grundlegenden Cybersicherheitsanforderungen anhand eines der folgenden Verfahren:

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

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

c) Konformitätsbewertung auf der Grundlage einer umfassenden Qualitätssicherung (auf der Grundlage von Modul H) gemäß Anhang VIII; oder

d) sofern verfügbar und anwendbar, ein europäisches Schema für die Cybersicherheitszertifizierung gemäß Artikel 27 Absatz 9.

(2) Hat der Hersteller bei der Bewertung der Konformität eines wichtigen Produkts mit digitalen Elementen, das in Klasse I gemäß Anhang III fällt, und der von dessen Hersteller festgelegten Verfahren mit den grundlegenden Cybersicherheitsanforderungen in Anhang I harmonisierte Normen, gemeinsame Spezifikationen oder europäische Systeme für die Cybersicherheitszertifizierung mindestens der Vertrauenswürdigkeitsstufe „mittel“ gemäß Artikel 27 nicht oder nur zum Teil angewandt oder sind solche harmonisierten Normen, gemeinsamen Spezifikationen oder europäischen Schemata für die Cybersicherheitszertifizierung nicht vorhanden, so sind die Produkte mit digitalen Elementen und die vom Hersteller festgelegten Verfahren im Hinblick auf die grundlegenden Cybersicherheitsanforderungen einem der folgenden Verfahren zu unterziehen:

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

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

(3) Handelt es sich bei dem Produkt um ein wichtiges Produkt mit digitalen Elementen, das in Klasse II gemäß Anhang III fällt, so erbringt der Hersteller den Nachweis der Konformität mit den grundlegenden Cybersicherheitsanforderungen in Anhang I anhand eines der folgenden Verfahren:

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

b) eine Konformitätsbewertung auf der Grundlage einer umfassenden Qualitätssicherung (auf der Grundlage von Modul H) gemäß Anhang VIII, oder

c) sofern verfügbar und anwendbar, ein europäisches Schema für die Cybersicherheitszertifizierung gemäß Artikel 27 Absatz 9 der vorliegenden Verordnung mindestens auf der Vertrauenswürdigkeitsstufe „mittel“ gemäß der Verordnung (EU) 2019/881.

(4) Bei in Anhang IV aufgeführten kritischen Produkten mit digitalen Elementen wird der Nachweis der Konformität mit den grundlegenden Cybersicherheitsanforderungen in Anhang I anhand eines der folgenden Verfahren erbracht:

a) ein europäisches Schema für die Cybersicherheitszertifizierung gemäß Artikel 8 Absatz 1 oder

b) wenn die Bedingungen des Artikels 8 Absatz 1 nicht erfüllt sind, eines der in Absatz 3 genannten Verfahren.

(5) Hersteller von Produkten mit digitalen Elementen, die als freie und quelloffene Software gelten und in die in Anhang III aufgeführten Kategorien fallen, können die Konformität mit den grundlegenden Cybersicherheitsanforderungen in Anhang I anhand eines der in Absatz 1 dieses Artikels genannten Verfahren nachweisen, sofern die in Artikel 31 genannte technische Dokumentation zum Zeitpunkt des Inverkehrbringens dieser Produkte der Öffentlichkeit zugänglich gemacht wird.

(6) Bei der Festlegung der Gebühren für die Konformitätsbewertung werden die besonderen Interessen und Bedürfnisse von Kleinstunternehmen und kleinen und mittleren Unternehmen, einschließlich Start-up-Unternehmen, berücksichtigt, und diese Gebühren werden proportional zu deren besonderen Interessen und Bedürfnissen gesenkt.

Artikel 33

Unterstützungsmaßnahmen für Kleinstunternehmen sowie kleine und mittlere Unternehmen, einschließlich Start-up-Unternehmen

(1) Die Mitgliedstaaten ergreifen gegebenenfalls die folgenden Maßnahmen, die auf die Bedürfnisse von Kleinst- und Kleinunternehmen zugeschnitten sind:

a) Organisation spezifischer Sensibilisierungs- und Schulungsmaßnahmen für die Anwendung dieser Verordnung,

b) Einrichtung eines speziellen Kommunikationskanals für Kleinst- und Kleinunternehmen sowie gegebenenfalls für lokale Behörden, um Beratung zur Durchführung dieser Verordnung zu leisten und Rückfragen zu klären,

c) Unterstützung von Prüf- und Konformitätsbewertungstätigkeiten, bei Bedarf auch mit Unterstützung des Europäischen Kompetenzzentrums für Cybersicherheit.

(2) Die Mitgliedstaaten können, soweit erforderlich, Reallabore für Cyberresilienz einrichten. In solchen Reallaboren sind kontrollierte Prüfumgebungen für innovative Produkte mit digitalen Elementen vorgesehen, um deren Entwicklung, Entwurf, Validierung und Erprobung zum Zwecke der Einhaltung dieser Verordnung für einen begrenzten Zeitraum vor dem Inverkehrbringen zu erleichtern. Die Kommission und gegebenenfalls die ENISA können technische Unterstützung, Beratung und Instrumente für die Einrichtung und den Betrieb von Reallaboren bereitstellen. Die Reallabore werden unter direkter Aufsicht, Leitung und Unterstützung durch die Marktüberwachungsbehörden eingerichtet. Die Mitgliedstaaten unterrichten die Kommission und die anderen Marktüberwachungsbehörden über die Einrichtung eines Reallabors über die ADCO. Die Reallabore lassen die Aufsichts- und Abhilfebefugnisse der zuständigen Behörden unberührt. Die Mitgliedstaaten stellen einen offenen, fairen und transparenten Zugang zu Reallaboren sicher und erleichtern insbesondere Kleinst- und Kleinunternehmen, einschließlich Start-up-Unternehmen, den Zugang.

(3) Im Einklang mit Artikel 26 stellt die Kommission Leitlinien für Kleinstunternehmen sowie kleine und mittlere Unternehmen in Bezug auf die Durchführung dieser Verordnung bereit.

(4) Die Kommission informiert über verfügbare finanzielle Unterstützung im Rechtsrahmen bestehender Unionsprogramme, um insbesondere Kleinst- und Kleinunternehmen finanziell zu entlasten.

(5) Kleinst- und Kleinunternehmen können alle in Anhang VII genannten Elemente der technischen Dokumentation in einem vereinfachten Format vorlegen. Zu diesem Zweck legt die Kommission im Wege von Durchführungsrechtsakten das vereinfachte Formular für die technische Dokumentation fest, das auf die Bedürfnisse von Kleinst- und Kleinunternehmen zugeschnitten ist, einschließlich der Art und Weise, wie die in Anhang VII aufgeführten Elemente vorzulegen sind. Entscheidet sich ein Kleinst- oder ein Kleinunternehmen für eine vereinfachte Bereitstellung der in Anhang VII vorgeschriebenen Informationen, so verwendet es das in diesem Absatz genannte Formular. Die notifizierten Stellen akzeptieren dieses Formular für die Zwecke der Konformitätsbewertung.

Diese Durchführungsrechtsakte werden gemäß dem in Artikel 62 Absatz 2 genannten Prüfverfahren erlassen.

Artikel 34

Abkommen über die gegenseitige Anerkennung

Unter Berücksichtigung des Niveaus der technischen Entwicklung und des Konzepts für die Konformitätsbewertung eines Drittlands kann die Union im Einklang mit Artikel 218 AEUV Abkommen über die gegenseitige Anerkennung mit Drittländern schließen, um den internationalen Handel zu fördern und zu erleichtern.

KAPITEL IV

NOTIFIZIERUNG VON KONFORMITÄTSBEWERTUNGSSTELLEN

Artikel 35

Notifizierung

(1) Die Mitgliedstaaten notifizieren der Kommission und den anderen Mitgliedstaaten die Stellen, die befugt sind, Konformitätsbewertungen gemäß dieser Verordnung durchzuführen.

(2) Die Mitgliedstaaten sorgen bis zum 11. Dezember 2026 dafür, dass es in der Union eine ausreichende Zahl notifizierter Stellen gibt, die Konformitätsbewertungen durchführen können, um Engpässe und Hindernisse mit Blick auf den Marktzugang zu verhindern.

Artikel 36

Notifizierende Behörden

(1) Jeder Mitgliedstaat benennt eine notifizierende Behörde, die für die Einrichtung und Durchführung der erforderlichen Verfahren für die Bewertung, Benennung und Notifizierung von Konformitätsbewertungsstellen und für deren Überwachung, einschließlich der Einhaltung des Artikels 41, zuständig ist.

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

(3) Falls die notifizierende Behörde die in Absatz 1 dieses Artikels genannte Bewertung, Notifizierung oder Überwachung an eine nichtstaatliche Stelle delegiert oder ihr auf andere Weise überträgt, so muss diese Stelle eine juristische Person sein und Artikel 37 entsprechend genügen. Außerdem muss diese Stelle Vorsorge zur Deckung von aus ihrer Tätigkeit entstehenden Haftungsansprüchen treffen.

(4) Die notifizierende Behörde trägt die volle Verantwortung für die von der in Absatz 3 genannten Stelle durchgeführten Tätigkeiten.

Artikel 37

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 38

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 die in Absatz 1 genannte Information der Öffentlichkeit zugänglich.

Artikel 39

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 mit digitalen Elementen, 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 ein solcher unabhängiger Dritter gelten, sofern ihre Unabhängigkeit sowie das Fehlen jedweder Interessenkonflikte nachgewiesen sind.

(4) Eine Konformitätsbewertungsstelle, ihre oberste Leitungsebene und die für die Erfüllung der Konformitätsbewertungsaufgaben zuständigen Mitarbeiter dürfen nicht Konstrukteur, Entwickler, Hersteller, Lieferant, Einführer, Händler, 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, Einfuhr, Vertrieb, Vermarktung, Installation, Verwendung oder Wartung dieser Produkte mit digitalen Elementen, die sie bewerten, 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 stellen sicher, 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 VIII 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) das erforderliche Personal mit Fachkenntnis und ausreichender einschlägiger Erfahrung, um die bei der Konformitätsbewertung anfallenden Aufgaben zu erfüllen;

b) Beschreibungen von Verfahren, nach denen die Konformitätsbewertung durchgeführt werden muss, 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.

Eine Konformitätsbewertungsstelle 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 grundlegenden Cybersicherheitsanforderungen gemäß Anhang I, der geltenden harmonisierten Normen und gemeinsamen Spezifikationen 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 ihres Mitgliedstaats 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 VIII 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 51 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) Die Konformitätsbewertungsstellen üben ihre Tätigkeiten im Einklang mit einer Reihe kohärenter, gerechter, verhältnismäßiger und angemessener Geschäftsbedingungen aus, wobei sie unnötige Belastungen der Wirtschaftsakteure vermeiden und insbesondere in Bezug auf Gebühren die Interessen von Kleinstunternehmen sowie von kleinen und mittleren Unternehmen berücksichtigen.

Artikel 40

Vermutung der Konformität von 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 39 erfüllt, soweit die geltenden Normen diese Anforderungen abdecken.

Artikel 41

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 39 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 42

Antrag auf Notifizierung

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

(2) Dem Antrag werden eine Beschreibung der Konformitätsbewertungstätigkeiten, des Konformitätsbewertungsverfahrens bzw. der Konformitätsbewertungsverfahren und des Produkts oder der Produkte mit digitalen Elementen, für die diese Stelle Kompetenz beansprucht, sowie, falls zutreffend, eine Akkreditierungsurkunde beigelegt, die von einer nationalen Akkreditierungsstelle ausgestellt wurde und in der diese bescheinigt, dass die Konformitätsbewertungsstelle die Anforderungen in Artikel 39 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 in Artikel 39 erfüllt.

Artikel 43

Notifizierungsverfahren

(1) Die notifizierenden Behörden notifizieren nur Konformitätsbewertungsstellen, die die Anforderungen in Artikel 39 erfüllen.

(2) Die notifizierende Behörde unterrichtet die Kommission und die anderen Mitgliedstaaten mittels des von der Kommission entwickelten und verwalteten Informationssystems 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 mit digitalen Elementen sowie die einschlägige Bestätigung der Kompetenz.

(4) Beruht eine Notifizierung nicht auf einer Akkreditierungsurkunde gemäß Artikel 42 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 in Artikel 39 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 relevanten Änderungen der Notifizierung informiert.

Artikel 44

Kennnummern und Verzeichnisse notifizierter Stellen

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

Selbst wenn eine Stelle gemäß mehreren Rechtsakten 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 45

Änderungen der Notifizierungen

(1) Falls eine notifizierende Behörde feststellt oder davon unterrichtet wird, dass eine notifizierte Stelle die Anforderungen in Artikel 39 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 Aufhebung 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 46

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 47

Operative Pflichten der notifizierten Stellen

(1) Die notifizierten Stellen führen die Konformitätsbewertungen im Einklang mit den Konformitätsbewertungsverfahren gemäß Artikel 32 und Anhang VIII 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 der Unternehmen, insbesondere in Bezug auf Kleinstunternehmen sowie kleine und mittlere Unternehmen, der Branche, in der sie tätig sind, ihrer Struktur, ihres Grads der Komplexität und des Cybersicherheitsrisikos der betroffenen Produkte mit digitalen Elementen und Technologien 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 der Produkte mit digitalen Elementen mit 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 27 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 mit digitalen Elementen 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 48

Einspruch gegen Entscheidungen notifizierter Stellen

Die Mitgliedstaaten stellen sicher, dass ein Einspruchsverfahren gegen die Entscheidungen der notifizierten Stellen vorgesehen ist.

Artikel 49

Meldepflichten der notifizierten Stellen

(1) Die notifizierten Stellen melden der notifizierenden Behörde

a) alle Verweigerungen, Einschränkungen, Aussetzungen und Aufhebung 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 mit digitalen Elementen nachgehen, einschlägige Informationen über negative und auf Verlangen auch über positive Ergebnisse von Konformitätsbewertungen.

Artikel 50

Erfahrungsaustausch

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

Artikel 51

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 52

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 gemäß Absatz 2 dieses Artikels benannten Marktüberwachungsbehörden sind auch für die Durchführung von Marktüberwachungstätigkeiten im Zusammenhang mit den in Artikel 24 genannten Verpflichtungen für Verwalter quelloffener Software zuständig. Stellt eine Marktüberwachungsbehörde fest, dass ein Verwalter quelloffener Software die in dem genannten Artikel festgelegten Verpflichtungen nicht erfüllt, so fordert sie den Verwalter quelloffener Software auf, sicherzustellen, dass alle geeigneten Korrekturmaßnahmen ergriffen werden. Die Verwalter quelloffener Software stellen im Rahmen ihrer Verpflichtungen gemäß dieser Verordnung sicher, dass alle geeigneten Korrekturmaßnahmen ergriffen werden.

(4) 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 14 der vorliegenden Verordnung arbeiten die benannten Marktüberwachungsbehörden mit den als Koordinatoren benannten CSIRTs und der ENISA zusammen und tauschen mit ihnen regelmäßig Informationen aus.

(5) Die Marktaufsichtsbehörden können den als Koordinator benannten CSIRT oder die ENISA um technische Beratung in Fragen der Durchführung und Durchsetzung dieser Verordnung ersuchen. Bei der Durchführung einer Untersuchung gemäß Artikel 54 können die Marktüberwachungsbehörden den als Koordinator benannten CSIRT oder die ENISA um eine Analyse zur Untermauerung der Konformitätsbewertung von Produkten mit digitalen Elementen ersuchen.

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

(7) 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 10, 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.

(8) Die Mitgliedstaaten sorgen dafür, dass die benannten Marktüberwachungsbehörden mit angemessenen finanziellen und technischen Ressourcen, gegebenenfalls auch mit Tools zur Prozessautomatisierung, sowie mit personellen Ressourcen, die über die notwendigen Cybersicherheitskompetenzen verfügen, ausgestattet werden, damit sie ihre Aufgaben im Rahmen dieser Verordnung wahrnehmen können.

(9) Die Kommission fördert und erleichtert den Erfahrungsaustausch zwischen den benannten Marktüberwachungsbehörden.

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

(11) Die Marktüberwachungsbehörden informieren die Verbraucher gemäß Artikel 11 der Verordnung (EU) 2019/1020 darüber, wo Beschwerden einzureichen sind, die auf eine Nichteinhaltung dieser Verordnung hindeuten könnten, und stellen den Verbrauchern Informationen darüber zur Verfügung, wo und wie sie Zugang zu Mechanismen haben, um die Meldung von Schwachstellen, Sicherheitsvorfällen und Cyberbedrohungen, die Produkte mit digitalen Elementen betreffen können, zu erleichtern.

(12) Die Marktüberwachungsbehörden müssen gegebenenfalls die Zusammenarbeit mit einschlägigen Interessenträgern, darunter Wissenschafts-, Forschungs- und Verbraucherorganisationen, erleichtern.

(13) 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.

(14) Bei Produkten mit digitalen Elementen, die in den Anwendungsbereich der vorliegenden Verordnung fallen und gemäß Artikel 6 der Verordnung (EU) 2024/1689 als Hochrisiko-KI-Systeme eingestuft sind, sind die für die Zwecke der genannten Verordnung benannten Marktüberwachungsbehörden auch für die nach der vorliegenden Verordnung erforderlichen Marktüberwachungstätigkeiten zuständig. Die nach der Verordnung (EU) 2024/1689 benannten Marktüberwachungsbehörden arbeiten gegebenenfalls mit den nach der vorliegenden Verordnung benannten Marktüberwachungsbehörden und — bezüglich der Aufsicht über die Umsetzung der Meldepflichten nach Artikel 14 der vorliegenden Verordnung — mit den als Koordinatoren benannten CSIRTs und der ENISA zusammen. Die nach der Verordnung (EU) 2024/1689 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.

(15) Im Hinblick auf die einheitliche Anwendung dieser Verordnung wird gemäß Artikel 30 Absatz 2 der Verordnung (EU) 2019/1020 die ADCO eingesetzt. Die ADCO setzt sich aus Vertretern der benannten Marktüberwachungsbehörden und gegebenenfalls Vertretern der zentralen Verbindungsstellen zusammen. Die ADCO befasst sich auch mit spezifischen Fragen zu den Marktüberwachungstätigkeiten im Zusammenhang mit den Verpflichtungen für Verwalter quelloffener Software.

(16) Die Marktüberwachungsbehörden überwachen, wie die Hersteller bei der Festlegung des Unterstützungszeitraums für ihre Produkte mit digitalen Elementen die in Artikel 13 Absatz 8 genannten Kriterien angewandt haben.

Die ADCO veröffentlicht in öffentlich zugänglicher und benutzerfreundlicher Form einschlägige Statistiken über Kategorien von Produkten mit digitalen Elementen, einschließlich der vom Hersteller gemäß Artikel 13 Absatz 8 festgelegten durchschnittlichen Unterstützungszeiträume, und stellt Leitlinien bereit, die indikative Unterstützungszeiträume für Kategorien von Produkten mit digitalen Elementen enthalten.

Wenn die Daten auf unzureichende Unterstützungszeiträume für bestimmte Kategorien von Produkten mit digitalen Elementen hindeuten, kann die ADCO den Marktüberwachungsbehörden empfehlen, ihre Tätigkeiten auf solche Kategorien von Produkten mit digitalen Elementen zu konzentrieren.

Artikel 53

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 Cybersicherheitsanforderungen in Anhang I erforderlich ist, erhalten die Marktüberwachungsbehörden auf begründeten Antrag in einer für sie leicht verständlichen Sprache 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 betroffenen Wirtschaftsakteurs.

Artikel 54

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

(1) Hat die Marktüberwachungsbehörde eines Mitgliedstaats hinreichenden Grund zu der Annahme, dass ein Produkt mit digitalen Elementen, einschließlich der Behandlung von Schwachstellen, ein erhebliches Cybersicherheitsrisiko birgt, so führt sie unverzüglich, gegebenenfalls in Zusammenarbeit mit dem einschlägigen CSIRT, eine Konformitätsbewertung des betreffenden Produkts im Hinblick auf die in dieser Verordnung festgelegten Anforderungen durch. Die betroffenen Wirtschaftsakteure arbeiten im erforderlichen Umfang mit der Marktüberwachungsbehörde zusammen.

Gelangt die Marktüberwachungsbehörde im Verlauf dieser Bewertung 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 Marktüberwachungsbehörde vorgeschriebenen, der Art des Cybersicherheitsrisikos angemessenen Frist alle geeigneten Korrekturmaßnahmen zu ergreifen, um die Konformität des Produkts mit digitalen Elementen mit diesen Anforderungen herzustellen oder um das Produkt vom Markt zu nehmen oder es zurückzurufen.

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

(2) Bei der Bestimmung der Erheblichkeit eines Cybersicherheitsrisikos gemäß Absatz 1 berücksichtigen die Marktüberwachungsbehörden auch nichttechnische Risikofaktoren, insbesondere solche, die infolge koordinierter Risikobewertungen in Bezug auf die Sicherheit der Lieferketten auf Unionsebene gemäß Artikel 22 der Richtlinie (EU) 2022/2555 festgelegt wurden. Hat eine Marktüberwachungsbehörde hinreichenden Grund zu der Annahme, dass ein Produkt mit digitalen Elementen angesichts nichttechnischer Risikofaktoren ein erhebliches Cybersicherheitsrisiko birgt, unterrichtet sie die gemäß Artikel 8 der Richtlinie (EU) 2022/2555 benannten oder eingerichteten zuständigen Behörden und arbeitet mit diesen Behörden bei Bedarf zusammen.

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

(4) Der Wirtschaftsakteur 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.

(5) Ergreift der Wirtschaftsakteur 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 mit digitalen Elementen auf ihrem nationalen Markt zu untersagen oder einzuschränken, das Produkt vom Markt zu nehmen oder es zurückzurufen.

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

(6) Die in Absatz 5 genannten Informationen enthalten alle verfügbaren Einzelheiten, insbesondere die notwendigen Daten für die Identifizierung des nichtkonformen Produkts mit digitalen Elementen, die Herkunft dieses 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 mit digitalen Elementen oder die vom Hersteller festgelegten Verfahren erfüllen nicht die grundlegenden Cybersicherheitsanforderungen in Anhang I;

b) Mängel in den harmonisierten Normen, den europäischen Schemata für die Cybersicherheitszertifizierung oder den gemeinsamen Spezifikationen gemäß Artikel 27.

(7) 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 mit digitalen Elementen sowie über ihre Einwände, falls sie die ihnen mitgeteilte nationale Maßnahme ablehnen.

(8) Erhebt weder ein Mitgliedstaat noch die Kommission innerhalb von drei Monaten nach Eingang der in Absatz 5 dieses Artikels genannten Notifizierung einen Einwand gegen eine vorläufige Maßnahme eines Mitgliedstaats, so gilt diese Maßnahme als gerechtfertigt. Die Verfahrensrechte des betreffenden Wirtschaftsakteurs nach Artikel 18 der Verordnung (EU) 2019/1020 bleiben hiervon unberührt.

(9) Die Marktüberwachungsbehörden aller Mitgliedstaaten tragen dafür Sorge, dass unverzüglich geeignete einschränkende Maßnahmen in Bezug auf das betreffende Produkt mit digitalen Elementen ergriffen werden, indem sie beispielsweise dieses Produkt von ihrem Markt rücknehmen.

Artikel 55

Schutzklauselverfahren der Union

(1) Erhebt ein Mitgliedstaat innerhalb von drei Monaten nach Eingang der in Artikel 54 Absatz 5 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 54 Absatz 5 genannten Unterrichtung, ob die nationale Maßnahme gerechtfertigt ist oder nicht und teilt dem betreffenden Mitgliedstaat diese 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. Wird die nationale Maßnahme als nicht gerechtfertigt erachtet, so muss der betreffende Mitgliedstaat sie zurücknehmen.

(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 11 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 Schema für die Cybersicherheitszertifizierung gemäß Artikel 27 zurückgeführt, so prüft die Kommission, ob ein gemäß Artikel 27 Absatz 9 angenommener delegierter Rechtsakt, in dem die Konformitätsvermutung in Bezug auf dieses Zertifizierungsschemas 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 27 zurückgeführt, so prüft die Kommission, ob ein gemäß Artikel 27 Absatz 2 angenommener Durchführungsrechtsakt, in dem die gemeinsamen Spezifikationen festgelegt worden sind, zu ändern oder aufzuheben ist.

Artikel 56

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

(1) Hat die Kommission — auch aufgrund von Informationen der ENISA — hinreichenden Grund zu der Annahme, dass ein Produkt mit digitalen Elementen, das ein erhebliches Cybersicherheitsrisiko birgt, den Anforderungen dieser Verordnung nicht genügt, so informiert sie die einschlägigen Marktüberwachungsbehörden. Führen die Marktüberwachungsbehörden eine Konformitätsbewertung dieses Produkts mit digitalen Elementen, das hinsichtlich seiner Konformität mit den Anforderungen dieser Verordnung ein erhebliches Cybersicherheitsrisiko bergen kann, durch, so finden die in den Artikeln 54 und 55 genannten Verfahren Anwendung.

(2) Hat die Kommission hinreichenden Grund zu der Annahme, dass ein Produkt mit digitalen Elementen angesichts nichttechnischer Risikofaktoren ein erhebliches Cybersicherheitsrisiko birgt, unterrichtet sie die einschlägigen Marktüberwachungsbehörden und gegebenenfalls die gemäß Artikel 8 der Richtlinie (EU) 2022/2555 benannten oder eingerichteten zuständigen Behörden und arbeitet mit diesen Behörden bei Bedarf zusammen. Die Kommission prüft auch die Relevanz der ermittelten Risiken für dieses Produkt mit digitalen Elementen im Hinblick auf ihre Aufgaben im Zusammenhang mit den koordinierten Risikobewertungen in Bezug auf die Sicherheit der Lieferketten auf Unionsebene gemäß Artikel 22 der Richtlinie (EU) 2022/2555 und konsultiert erforderlichenfalls die gemäß Artikel 14 der Richtlinie (EU) 2022/2555 eingesetzte Kooperationsgruppe und die ENISA.

(3) Unter Umständen, die ein sofortiges Eingreifen rechtfertigen, um das reibungslose Funktionieren des Binnenmarkts zu bewahren, und wenn die Kommission hinreichenden Grund zu der Annahme hat, dass das in Absatz 1 genannte Produkt mit digitalen Elementen weiterhin den Anforderungen dieser Verordnung nicht genügt und die einschlägigen Marktüberwachungsbehörden keine wirksamen Maßnahmen ergriffen haben, nimmt die Kommission eine Bewertung der Konformität vor und kann die ENISA um eine Analyse zur Untermauerung der Bewertung ersuchen. Die Kommission unterrichtet die einschlägigen Marktüberwachungsbehörden hierüber. Die betroffenen Wirtschaftsakteure arbeiten im erforderlichen Umfang mit der ENISA zusammen.

(4) Auf der Grundlage der Bewertung nach Absatz 3 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 Wirtschaftsakteure.

(5) Auf der Grundlage der in Absatz 4 dieses Artikels genannten Konsultation kann die Kommission Durchführungsrechtsakte über Korrekturmaßnahmen oder einschränkende Maßnahmen auf Unionsebene erlassen, einschließlich der Forderung der Rücknahme vom Markt oder des Rückrufs der betreffenden Produkte mit digitalen Elementen innerhalb einer der Art des Risikos angemessenen Frist. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 62 Absatz 2 genannten Prüfverfahren erlassen.

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

(7) Die Absätze 3 bis 6 gelten für die Dauer der außergewöhnlichen Umstände, die das Eingreifen der Kommission gerechtfertigt haben, solange die Konformität des betreffenden Produkts mit digitalen Elementen mit dieser Verordnung nicht hergestellt worden ist.

Artikel 57

Konforme Produkte mit digitalen Elementen, die ein erhebliches Cybersicherheitsrisiko bergen

(1) Die Marktüberwachungsbehörde eines Mitgliedstaats fordert einen Wirtschaftsakteur auf, alle geeigneten Maßnahmen zu ergreifen, wenn sie nach einer Bewertung gemäß Artikel 54 feststellt, dass ein Produkt mit digitalen Elementen und die vom Hersteller festgelegten Verfahren zwar dieser Verordnung entsprechen, jedoch ein erhebliches Cybersicherheitsrisiko sowie folgende Risiken bergen:

a) Risiko für die Gesundheit oder Sicherheit von Personen,

b) Risiko für die Erfüllung der Pflichten aus dem Unionsrecht oder dem nationalen Recht zum Schutz der Grundrechte,

c) Risiko für die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit von Diensten, die über ein elektronisches Informationssystem von in Artikel 3 Absatz 1 der Richtlinie (EU) 2022/2555 genannten wesentlichen Einrichtungen angeboten werden oder

d) Risiko für andere Aspekte des Schutzes öffentlicher Interessen.

Die in Unterabsatz 1 genannten Maßnahmen können Maßnahmen umfassen, mit denen sichergestellt wird, dass das betreffende Produkt mit digitalen Elementen und die vom Hersteller festgelegten Verfahren die relevanten Risiken nicht mehr bergen, wenn das betreffende Produkt mit digitalen Elementen auf dem Markt bereitgestellt, vom Markt rückgenommen oder zurückgerufen wird, und müssen der Art dieser Risiken angemessen sein.

(2) Der Hersteller oder andere betreffende Wirtschaftsakteure 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 den in Absatz 4 genannten Beschluss an die Mitgliedstaaten.

(6) Hat die Kommission — auch aufgrund von Informationen der ENISA — hinreichenden Grund zu der Annahme, dass ein Produkt mit digitalen Elementen, obwohl es dieser Verordnung entspricht, die in Absatz 1 dieses Artikels genannten Risiken birgt, so unterrichtet sie die einschlägige(n) Marktüberwachungsbehörde(n) und kann sie auffordern, eine Bewertung durchzuführen und die in Artikel 54 und in den Absätzen 1, 2 und 3 dieses Artikels genannten Verfahren anzuwenden.

(7) Unter Umständen, die ein sofortiges Eingreifen rechtfertigen, um das reibungslose Funktionieren des Binnenmarkts zu bewahren, und wenn die Kommission hinreichenden Grund zu der Annahme hat, dass das in Absatz 6 genannte Produkt mit digitalen Elementen weiterhin die in Absatz 1 genannten Risiken birgt und die einschlägigen Marktüberwachungsbehörden keine wirksamen Maßnahmen ergriffen haben, nimmt die Kommission eine Bewertung der Risiken, die dieses Produkt mit digitalen Elementen birgt, vor und kann die ENISA um eine Analyse zur Untermauerung dieser Bewertung ersuchen und unterrichtet die einschlägigen Marktüberwachungsbehörden hierüber. Die betroffenen Wirtschaftsakteure arbeiten im erforderlichen Umfang mit der ENISA zusammen.

(8) Auf der Grundlage der Bewertung 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 Wirtschaftsakteure.

(9) Auf der Grundlage der in Absatz 8 des vorliegenden Artikels genannten Konsultation kann die Kommission Durchführungsrechtsakte über Korrekturmaßnahmen oder einschränkende Maßnahmen auf Unionsebene erlassen, einschließlich der Forderung der Rücknahme vom Markt oder des Rückrufs der betreffenden Produkte mit digitalen Elementen innerhalb einer der Art des Risikos angemessenen Frist. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 62 Absatz 2 genannten Prüfverfahren erlassen.

(10) Die Kommission unterrichtet den bzw. die betroffenen Wirtschaftsakteure unverzüglich über die in Absatz 9 genannten Durchführungsrechtsakte. 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 mit digitalen Elementen weiterhin die in Absatz 1 genannten Risiken birgt.

Artikel 58

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 CE-Kennzeichnung wurde unter Nichteinhaltung der Artikel 29 und 30 angebracht;

b) die CE-Kennzeichnung wurde nicht angebracht;

c) die EU-Konformitätserklärung wurde nicht ausgestellt;

d) die EU-Konformitätserklärung wurde nicht ordnungsgemäß ausgestellt;

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

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 59

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 den Verkehr gebrachte oder auf dem Markt bereitgestellte Produkte mit digitalen Elementen vereinbaren, insbesondere in Bezug auf Produkte mit digitalen Elementen, bei denen häufig Cybersicherheitsrisiken festgestellt werden.

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

(3) Die Marktüberwachungsbehörden und gegebenenfalls 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 gegebenenfalls die Kommission machen die Vereinbarung über gemeinsame Tätigkeiten einschließlich der Namen der Beteiligten der Öffentlichkeit zugänglich.

Artikel 60

Koordinierte Kontrollen (Sweeps)

(1) Die Marktüberwachungsbehörden führen zur Prüfung der Einhaltung dieser Verordnung oder zur Feststellung von Verstößen gegen diese Verordnung gleichzeitige koordinierte Kontrollen („Sweeps“) zu bestimmten Produkten mit digitalen Elementen durch. Diese Sweeps können auch die Inspektion von Produkten mit digitalen Elementen umfassen, die unter einer falschen Identität erworben wurden.

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

(3) Bestimmt die ENISA in Wahrnehmung ihrer Aufgaben, auch aufgrund der gemäß Artikel 14 Absätze 1 und 3 eingegangenen Meldungen, Kategorien von Produkten mit digitalen Elementen, zu denen Sweeps organisiert werden können, so legt sie dem in Absatz 2 dieses Artikels genannten Koordinator einen Vorschlag für Sweeps zur Prüfung durch die Marktüberwachungsbehörden vor.

(4) Bei der Durchführung von Sweeps können die beteiligten Marktüberwachungsbehörden die Ermittlungsbefugnisse nach den Artikeln 52 bis 58 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 61

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 5 Unterabsatz 2, Artikel 7 Absatz 3, Artikel 8 Absätze 1 und 2, Artikel 13 Absatz 8 Unterabsatz 4, Artikel 14 Absatz 9, Artikel 25, Artikel 27 Absatz 9, Artikel 28 Absatz 5 und Artikel 31 Absatz 5 wird der Kommission für einen Zeitraum von fünf Jahren ab dem 10. Dezember 2024 übertragen. Die Kommission erstellt spätestens neun Monate vor Ablauf des Zeitraums von fünf Jahren einen Bericht über die Befugnisübertragung. Die Befugnisübertragung verlängert sich stillschweigend um Zeiträume gleicher Länge, es sei denn, das Europäische Parlament oder der Rat widersprechen einer solchen Verlängerung spätestens drei Monate vor Ablauf des jeweiligen Zeitraums.

(3) Die Befugnisübertragung gemäß Artikel 2 Absatz 5 Unterabsatz 2, Artikel 7 Absatz 3, Artikel 8 Absätze 1 und 2, Artikel 13 Absatz 8 Unterabsatz 4, Artikel 14 Absatz 9, Artikel 25, Artikel 27 Absatz 9, Artikel 28 Absatz 5 und Artikel 31 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 5 Unterabsatz 2, Artikel 7 Absatz 3, Artikel 8 Absätze 1 oder 2, Artikel 13 Absatz 8 Unterabsatz 4, Artikel 14 Absatz 9, Artikel 25, Artikel 27 Absatz 9, Artikel 28 Absatz 5 oder Artikel 31 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 62

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 63

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 (EU) 2016/943 des Europäischen Parlaments und des Rates ([37]) 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 64

Sanktionen

(1) Die Mitgliedstaaten erlassen Vorschriften über Sanktionen, die bei Verstößen gegen diese Verordnung zu verhängen sind, und treffen alle für die Umsetzung der Sanktionen erforderlichen Maßnahmen. Die vorgesehenen Sanktionen müssen wirksam, verhältnismäßig und abschreckend sein. Die Mitgliedstaaten teilen der Kommission diese Vorschriften und Maßnahmen unverzüglich mit und melden ihr unverzüglich alle diesbezüglichen Änderungen.

(2) Bei Nichteinhaltung der in Anhang I festgelegten grundlegenden Cybersicherheitsanforderungen oder Verstößen gegen die in den Artikeln 13 und 14 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.

(3) Bei Verstößen gegen die in den Artikeln 18 bis 23, Artikel 28, Artikel 30 Absätze 1 bis 4, Artikel 31 Absätze 1 bis 4, Artikel 32 Absätze 1, 2 und 3, Artikel 33 Absatz 5 und Artikeln 39, 41, 47, 49 und 53 festgelegten Pflichten 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.

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

([37]) 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).

(5) 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 dieselben oder andere Marktüberwachungsbehörden demselben Wirtschaftsakteur für einen ähnlichen Verstoß Geldbußen auferlegt haben,

c) Größe, insbesondere im Hinblick auf Kleinstunternehmen sowie kleine und mittlere Unternehmen, einschließlich Start-up-Unternehmen, und Marktanteil des Wirtschaftsakteurs, der den Verstoß begangen hat.

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

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

(8) In Abhängigkeit vom Rechtssystem des betreffenden Mitgliedstaats können die Vorschriften über Geldbußen je nach den dort geltenden Regeln so angewandt werden, dass die Geldbußen 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.

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

(10) Abweichend von den Absätzen 3 bis 9 gelten die in diesen Absätzen genannten Geldbußen nicht für

a) Hersteller, die als Kleinst- oder Kleinunternehmen gelten, und zwar in Bezug auf die Nichteinhaltung der in Artikel 14 Absatz 2 Buchstabe a oder Artikel 14 Absatz 4 Buchstabe a genannten Frist,

b) Verwalter quelloffener Software bei jedem Verstoß gegen diese Verordnung.

Artikel 65

Verbandsklagen

Richtlinie (EU) 2020/1828 findet Anwendung auf Verbandsklagen gegen Zuwiderhandlungen durch Wirtschaftsakteure gegen Bestimmungen dieser Verordnung, die die Kollektivinteressen der Verbraucher beeinträchtigen oder zu beeinträchtigen drohen.

KAPITEL VIII

ÜBERGANGS- UND SCHLUSSBESTIMMUNGEN

Artikel 66

Änderung der Verordnung (EU) 2019/1020

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

„72. Verordnung (EU) 2024/2847 des Europäischen Parlaments und des Rates (*).

(*) Verordnung (EU) 2024/2847 des Europäischen Parlaments und des Rates vom 23. Oktober 2024 über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen und zur Änderung der Verordnung (EU) Nr. 168/2013 und der Verordnung (EU) 2019/1020 und der Richtlinie (EU) 2020/1828 (Cyberresilienzgesetz) (ABl. L, 2024/2847, 20.11.2024, ELI: http://data.europa.eu/eli/reg/2024/2847/oj).“

Artikel 67

Änderung der Richtlinie (EU) 2020/1828

In Anhang I der Richtlinie (EU) 2020/1828 wird folgende Nummer angefügt:

„(69) Verordnung (EU) 2024/2847 des Europäischen Parlaments und des Rates (*).

(*) Verordnung (EU) 2024/2847 des Europäischen Parlaments und des Rates vom 23. Oktober 2024 über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen und zur Änderung der Verordnung (EU) Nr. 168/2013 und der Verordnung (EU) 2019/1020 und der Richtlinie (EU) 2020/1828 (Cyberresilienzgesetz) (ABl. L, 2024/2847, 20.11.2024, ELI: http://data.europa.eu/eli/reg/2024/2847/oj).“

Artikel 68

Änderungen der Verordnung (EU) Nr. 168/2013

In Anhang II Teil C1 der Verordnung (EU) Nr. 168/2013 des Europäischen Parlaments und des Rates ([38]) wird in der Tabelle folgender Eintrag angefügt:

”

16	18	Schutz des Fahrzeugs gegen Cyberangriffe		x	x	x	x	x	x	x	x	x	x	x	x	x	x	X

“

Artikel 69

Übergangsbestimmungen

(1) EU-Baumusterprüfbescheinigungen und Zulassungen, die in Bezug auf Cybersicherheitsanforderungen für Produkte mit digitalen Elementen erteilt wurden, die anderen Harmonisierungsrechtsvorschriften der Union als der vorliegenden Verordnung unterliegen, bleiben bis zum 11. Juni 2028 gültig, sofern sie nicht vor diesem Zeitpunkt ablaufen oder sofern in anderen Harmonisierungsrechtsvorschriften der Union nichts anderes festgelegt ist; in letzterem Fall bleiben sie gemäß den letztgenannten Rechtsvorschriften gültig.

(2) Produkte mit digitalen Elementen, die vor dem 11. Dezember 2027 in den Verkehr gebracht wurden, unterliegen den in dieser Verordnung festgelegten Anforderungen nur dann, wenn nach diesem Zeitpunkt diese Produkte einer wesentlichen Änderung unterliegen.

(3) Abweichend von Absatz 2 des vorliegenden Artikels gelten die in Artikel 14 festgelegten Pflichten für alle Produkte mit digitalen Elementen, die in den Anwendungsbereich dieser Verordnung fallen und vor dem 11. Dezember 2027 in den Verkehr gebracht wurden.

Artikel 70

Bewertung und Überprüfung

(1) Bis zum 11. Dezember 2030 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.

(2) Bis zum 11. September 2028 legt die Kommission nach Konsultation der ENISA und des CSIRT-Netzes dem Europäischen Parlament und dem Rat einen Bericht vor, in dem sie die Wirksamkeit der einheitlichen Meldeplattform gemäß Artikel 16 sowie die Auswirkungen der Geltendmachung der in Artikel 16 Absatz 2 genannten Gründen der Cybersicherheit durch die als Koordinatoren benannten CSIRTs auf die Wirksamkeit der einheitlichen Meldeplattform im Hinblick auf die rechtzeitige Übermittlung eingegangener Meldungen an andere einschlägige CSIRTs bewertet.

Artikel 71

Inkrafttreten und Geltungsbeginn

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

([38]) Verordnung (EU) Nr. 168/2013 des Europäischen Parlaments und des Rates vom 15. Januar 2013 über die Genehmigung und Marktüberwachung von zwei- oder dreirädrigen und vierrädrigen Fahrzeugen (ABl. L 60 vom 2.3.2013, S. 52).

(2) Diese Verordnung gilt ab dem 11. Dezember 2027.

Artikel 14 gilt jedoch ab dem 11. September 2026, und Kapitel IV (Artikel 35 bis 51) gilt ab dem 11. Juni 2026.

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

Geschehen zu Straßburg am 23. Oktober 2024.

Im Namen des Europäischen Parlaments	*Im Namen des Rates*
Die Präsidentin	*Der Präsident*
R. METSOLA	ZSIGMOND B. P.

ANHANG I

GRUNDLEGENDE CYBERSECURITYANFORDERUNGEN

Teil I Cybersicherheitsanforderungen 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) Auf der Grundlage der Bewertung der Cybersicherheitsrisiken gemäß Artikel 13 Absatz 2 müssen Produkte mit digitalen Elementen, soweit zutreffend,

a) ohne bekannte ausnutzbare Schwachstellen auf dem Markt bereitgestellt werden,

b) mit einer sicheren Standardkonfiguration auf dem Markt bereitgestellt werden, sofern zwischen dem Hersteller und dem gewerblichen Nutzer in Bezug auf ein maßgeschneidertes Produkt mit digitalen Elementen nichts anderes vereinbart wurde, und die Möglichkeit bieten, das Produkt in seinen ursprünglichen Zustand zurückzusetzen,

c) sicherstellen, dass Schwachstellen durch Sicherheitsaktualisierungen behoben werden können, gegebenenfalls auch durch automatische Sicherheitsaktualisierungen, die als Standardeinstellung innerhalb eines angemessenen Zeitrahmens installiert werden sowie über einen klaren und benutzerfreundlichen Opt-out-Mechanismus verfügen, bei dem die Nutzer über verfügbare Aktualisierungen informiert werden und sie vorübergehend verschieben können;

d) durch geeignete Kontrollmechanismen Schutz vor unbefugtem Zugriff bieten, darunter u. a. zumindest Authentifizierungs-, Identitäts- oder Zugangsverwaltungssysteme, und einen möglicherweise unbefugten Zugriff melden,

e) 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 und durch den Einsatz anderer technischer Mittel,

f) 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 und deren Beschädigung melden,

g) die Verarbeitung personenbezogener oder sonstiger Daten auf solche, die angemessen und von Bedeutung sind, und auf das für die Zweckbestimmung des Produkts mit digitalen Elementen erforderliche Maß beschränken („Datenminimierung“),

h) die Verfügbarkeit wesentlicher und grundlegender Funktionen, auch nach einem Sicherheitsvorfall, einschließlich über Abwehr- und Eindämmungsmaßnahmen gegen Überlastungsangriffe auf Server (Denial-of-Service-Angriffe), sicherstellen,

i) die negativen Auswirkungen von den Produkten selbst oder von vernetzten Geräten auf die Verfügbarkeit der von anderen Geräten oder Netzen bereitgestellten Dienste minimieren,

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

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

l) sicherheitsbezogene Informationen durch Aufzeichnung und/oder Überwachung einschlägiger interner Vorgänge wie Zugang zu Daten, Diensten oder Funktionen und Änderungen daran bereitstellen und den Nutzern einen Opt-out-Mechanismus zur Verfügung stellen,

m) den Nutzern die Möglichkeit bieten, alle Daten und Einstellungen dauerhaft sicher und einfach zu löschen, und, wenn diese Daten auf andere Produkte oder Systeme übertragen werden können, sicherstellen, dass dies auf sichere Weise geschieht.

Teil II Anforderungen an die Behandlung von Schwachstellen

Die Hersteller von Produkten mit digitalen Elementen müssen

(1) Schwachstellen und Komponenten der Produkte mit digitalen Elementen ermitteln und dokumentieren, u. a. durch Erstellung einer Software-Stückliste in einem gängigen maschinenlesbaren Format, aus der zumindest die obersten Abhängigkeiten der Produkte 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; soweit technisch machbar, müssen neue Sicherheitsaktualisierungen getrennt von den Funktionsaktualisierungen bereitgestellt werden;

(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 teilen und 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 eindeutige und verständliche Informationen, die den Nutzern helfen, die Schwachstellen zu beheben; in hinreichend begründeten Fällen, in denen die Hersteller der Auffassung sind, dass die Risiken der Veröffentlichung die Vorteile in Bezug auf die Sicherheit überwiegen, können sie die Veröffentlichung von Informationen über eine behobene Schwachstelle so lange aufschieben, bis den Nutzern die Möglichkeit gegeben wurde, den entsprechenden Patch anzuwenden;

(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 Schwachstellen rechtzeitig und im Falle von Sicherheitsaktualisierungen gegebenenfalls automatisch behoben oder eingedämmt werden;

(8) dafür sorgen, dass Sicherheitsaktualisierungen, die zur Bewältigung festgestellter Sicherheitsprobleme zur Verfügung stehen, unverzüglich und — sofern zwischen dem Hersteller und dem gewerblichen Nutzer in Bezug auf ein maßgeschneidertes Produkt mit digitalen Elementen nichts anderes vereinbart wurde — 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 des Herstellers, die Postanschrift, E-Mail-Adresse oder andere digitale Kontaktmöglichkeit und, falls vorhanden, Website, unter denen der Hersteller erreichbar ist;
2. die zentrale Kontaktstelle, bei der Informationen über Schwachstellen des Produkts mit digitalen Elementen gemeldet werden können und entgegengenommen werden und das Konzept für die koordinierte Offenlegung von Schwachstellen zu finden ist;
3. Name und Typ sowie alle zusätzlichen Informationen, die eine eindeutige Identifizierung des Produkts mit digitalen Elementen ermöglichen;
4. die Zweckbestimmung des Produkts mit digitalen Elementen, 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 Zweckbestimmung des Produkts mit digitalen Elementen oder dessen vernünftigerweise vorhersehbaren Fehlanwendung, die zu erheblichen Cybersicherheitsrisiken führen können;
6. gegebenenfalls die Internetadresse, unter der die EU-Konformitätserklärung abrufbar ist;
7. die Art der vom Hersteller angebotenen technischen Sicherheitsunterstützung und das Enddatum des Unterstützungszeitraums, in dem die Nutzer die Behebung von Schwachstellen und den Erhalt von Sicherheitsaktualisierungen erwarten können;
8. 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 mit digitalen Elementen getroffen werden müssen, um dessen sichere Verwendung sicherzustellen,
   b) wie sich Änderungen am Produkt mit digitalen Elementen auf die Datensicherheit auswirken können,
   c) wie sicherheitsrelevante Aktualisierungen installiert werden können,
   d) wie eine sichere Außerbetriebnahme des Produkts mit digitalen Elementen erfolgt und wie Nutzerdaten sicher entfernt werden können;
   e) wie die Standardeinstellung, die die automatische Installation von Sicherheitsaktualisierungen gemäß Anhang I Teil I Buchstabe c ermöglicht, deaktiviert werden kann;
   f) wie der Integrator die grundlegenden Cybersicherheitsanforderungen in Anhang I und die Anforderungen an die technische Dokumentation in Anhang VII erfüllen kann, wenn das Produkt mit digitalen Elementen für die Integration in andere Produkte mit digitalen Elementen bestimmt ist;
9. für den Fall, dass der Hersteller dem Nutzer die Software-Stückliste zur Verfügung stellt, wo auf die Software-Stückliste zugegriffen werden kann.

ANHANG III

WICHTIGE PRODUKTE MIT DIGITALEN ELEMENTEN

Klasse I

1. Identitätsmanagementsysteme sowie Software und Hardware für die Verwaltung privilegierter Zugänge bzw. Zugriffe, einschließlich Lesegeräte für die Authentifizierung und Zugangskontrolle, auch biometrische Lesegeräte
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. Systeme für die Verwaltung von Sicherheitsinformationen und -ereignissen (SIEM)
8. Bootmanager
9. Public-Key-Infrastrukturen und Software für die Ausstellung digitaler Zertifikate
10. physische und virtuelle Netzschnittstellen
11. Betriebssysteme
12. Router, Modems für die Internetanbindung und Switches
13. Mikroprozessoren mit sicherheitsrelevanten Funktionen
14. Mikrocontroller mit sicherheitsrelevanten Funktionen
15. anwendungsspezifische integrierte Schaltungen (ASIC) und FPGA (Field Programmable Gate Array) mit sicherheitsrelevanten Funktionen
16. virtuelle Assistenten für die intelligente häusliche Umgebung mit allgemeinem Zweck
17. Produkte für die intelligente häusliche Umgebung mit Sicherheitsfunktionen, einschließlich intelligenter Türschlösser, Sicherheitskameras, Babyüberwachungssysteme und Alarmanlagen
18. mit dem Internet verbundenes Spielzeug, das unter die Richtlinie 2009/48/EG des Europäischen Parlaments und des Rates [1] fällt und über Funktionen zur sozialen Interaktion (z. B. sprechen oder filmen) oder zur Ortung verfügt
19. am Körper tragbare Produkte, die zum Zwecke der Gesundheitsüberwachung (z. B. Tracking) bestimmt sind und nicht unter die Verordnungen (EU) 2017/745 oder (EU) 2017/746 fallen, oder am Körper tragbare Produkte, die für die Verwendung durch und für Kinder bestimmt sind

Klasse II

1. Hypervisoren und Container-Runtime-Systeme, die eine virtualisierte Ausführung von Betriebssystemen und ähnlichen Umgebungen unterstützen
2. Firewalls, Intrusion-Detection-Systeme und Intrusion-Prevention-Systeme
3. manipulationssichere Mikroprozessoren
4. manipulationssichere Mikrocontroller

[1] Richtlinie 2009/48/EG des Europäischen Parlaments und des Rates vom 18. Juni 2009 über die Sicherheit von Spielzeug (ABl. L 170 vom 30.6.2009, S. 1).

ANHANG IV

KRITISCHE PRODUKTE MIT DIGITALEN ELEMENTEN

1. Hardwaregeräte mit Sicherheitsboxen
2. Smart-Meter-Gateways in intelligenten Messsystemen im Sinne des Artikels 2 Nummer 23 der Richtlinie (EU) 2019/944 des Europäischen Parlaments und des Rates ([1]) sowie andere Geräte für fortgeschrittene Sicherheitszwecke, einschließlich der sicheren Kryptoverarbeitung
3. Chipkarten oder ähnliche Geräte, einschließlich Sicherheitselemente

([1]) Richtlinie (EU) 2019/944 des Europäischen Parlaments und des Rates vom 5. Juni 2019 mit gemeinsamen Vorschriften für den Elektrizitätsbinnenmarkt und zur Änderung der Richtlinie 2012/27/EU (ABl. L 158 vom 14.6.2019, S. 125).

ANHANG V

EU-KONFORMITÄTSERKLÄRUNG

Die EU-Konformitätserklärung gemäß Artikel 28 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 mit digitalen Elementen 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 VI

VEREINFACHTE EU-KONFORMITÄTSERKLÄRUNG

Die vereinfachte EU-Konformitätserklärung nach Artikel 13 Absatz 20 hat folgenden Wortlaut:

Hiermit erklärt … [Name des Herstellers], dass der Typ des Produkts mit digitalen Elementen … [Bezeichnung des Typs des Produkts mit digitalen Elementen] der Verordnung (EU) 2024/2847 ([1]) entspricht.

Der vollständige Text der EU-Konformitätserklärung kann unter der folgenden Internetadresse abgerufen werden: …

([1]) ABl. L, 2024/2847, 20.11.2024, ELI: http://data.europa.eu/eli/reg/2024/2847/oj.

ANHANG VII

INHALT DER TECHNISCHEN DOKUMENTATION

Die in Artikel 31 genannte technische Dokumentation muss mindestens die folgenden Informationen enthalten, soweit sie für das betreffende Produkt mit digitalen Elementen von Bedeutung sind:

1. eine allgemeine Beschreibung des Produkts mit digitalen Elementen, einschließlich
   a) seiner Zweckbestimmung,
   b) Softwareversionen, die sich auf die Erfüllung der grundlegenden Cybersicherheitsanforderungen 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 mit digitalen Elementen und der Verfahren zur Behandlung von Schwachstellen, einschließlich
   a) erforderlicher 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) erforderlicher 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) erforderlicher 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 13 berücksichtigt werden, einschließlich der Frage, inwieweit die grundlegenden Cybersicherheitsanforderungen gemäß Anhang I Teil I Anwendung finden;
4. einschlägige Informationen, die bei der Festlegung des Unterstützungszeitraums gemäß Artikel 13 Absatz 8 des Produkts mit digitalen Elementen berücksichtigt wurden;
5. eine Aufstellung der vollständig oder teilweise angewandten harmonisierten Normen, deren Fundstellen im *Amtsblatt der Europäischen Union* veröffentlicht wurden, der in Artikel 27 dieser Verordnung genannten gemeinsamen Spezifikationen oder der in Artikel 27 Absatz 8 dieser Verordnung genannten europäischen Schemata für die Cybersicherheitszertifizierung, angenommen gemäß der Verordnung (EU) 2019/881, und, falls keine solchen harmonisierten Normen, gemeinsamen Spezifikationen und europäischen Schemata für die Cybersicherheitszertifizierung angewandt werden, Beschreibungen der Lösungen, mit denen die grundlegenden Cybersicherheitsanforderungen in Anhang I Teile I und II erfüllt werden, mit einer Aufstellung sonstiger angewandter einschlägiger technischer Spezifikationen. Bei einer teilweisen Anwendung harmonisierter Normen, gemeinsamer Spezifikationen oder europäischer Schemata für die Cybersicherheitszertifizierung ist in der technischen Dokumentation anzugeben, welche Teile angewandt wurden;
6. Berichte über die Tests und Prüfungen, die durchgeführt wurden, um die Konformität des Produkts mit digitalen Elementen und der Verfahren zur Behandlung von Schwachstellen mit den geltenden grundlegenden Cybersicherheitsanforderungen in Anhang I Teile I und II zu überprüfen;
7. ein Exemplar der EU-Konformitätserklärung;
8. gegebenenfalls auf begründetes Verlangen der Marktüberwachungsbehörde die Software-Stückliste, sofern dies erforderlich ist, damit diese Behörde die Einhaltung der grundlegenden Cybersicherheitsanforderungen in Anhang I überprüfen kann.

ANHANG VIII

KONFORMITÄTSBEWERTUNGSVERFAHREN

Teil I 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 des vorliegenden Teils festgelegten Pflichten erfüllt sowie gewährleistet und auf eigene Verantwortung erklärt, dass die Produkte mit digitalen Elementen allen grundlegenden Cybersicherheitsanforderungen in Anhang I Teil I genügen und dass der Hersteller die grundlegenden Cybersicherheitsanforderungen in Anhang I Teil II erfüllt.

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

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 Cybersicherheitsanforderungen in Anhang I Teile I und II gewährleisten.

4. Konformitätskennzeichnung und Konformitätserklärung

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

   4.2. Der Hersteller stellt für jedes Produkt mit digitalen Elementen eine schriftliche EU-Konformitätserklärung gemäß Artikel 28 aus und hält sie zusammen mit der technischen Dokumentation für einen Zeitraum von zehn Jahren ab dem Inverkehrbringen des Produkts mit digitalen Elementen oder während des Unterstützungszeitraums, je nachdem, welcher Zeitraum länger ist, 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 einschlägigen Behörden auf Verlangen zur Verfügung gestellt.

5. Bevollmächtigte

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

Teil II 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 mit digitalen Elementen und die vom Hersteller festgelegten Verfahren zur Behandlung von Schwachstellen untersucht und prüft und sodann bescheinigt, dass ein Produkt mit digitalen Elementen den grundlegenden Cybersicherheitsanforderungen in Anhang I Teil I genügt und dass der Hersteller die grundlegenden Cybersicherheitsanforderungen in Anhang I Teil II erfüllt.

2. Die EU-Baumusterprüfung erfolgt als Bewertung der Eignung der technischen Konzeption und Entwicklung des Produkts mit digitalen Elementen 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).

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

   Der Antrag enthält

   3.1. den Namen und die Anschrift des Herstellers sowie, wenn der Antrag vom Bevollmächtigten eingereicht wird, den Namen und die Anschrift des Bevollmächtigten;

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

   3.3. die technische Dokumentation, anhand deren die Konformität des Produkts mit digitalen Elementen mit den geltenden grundlegenden Cybersicherheitsanforderungen in Anhang I Teil I und die Verfahren des Herstellers zur Behandlung von Schwachstellen gemäß Anhang I Teil II bewertet werden können; 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 mit digitalen Elementen zu erfassen, soweit sie für die Bewertung von Bedeutung sind. Die technische Dokumentation enthält gegebenenfalls zumindest die in Anhang VII aufgeführten Elemente;

3.4. 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 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.

4. Die notifizierte Stelle

4.1. prüft die technische Dokumentation und die zusätzlichen Nachweise, um die Übereinstimmung der technischen Konzeption und Entwicklung des Produkts mit digitalen Elementen mit den grundlegenden Cybersicherheitsanforderungen in Anhang I Teil I und der vom Hersteller festgelegten Verfahren zur Behandlung von Schwachstellen mit den grundlegenden Cybersicherheitsanforderungen in Anhang I Teil II zu bewerten;

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

4.3. führt geeignete Untersuchungen und Prüfungen durch bzw. veranlasst diese, um festzustellen, ob die Lösungen aus den einschlägigen harmonisierten Normen oder technischen Spezifikationen im Hinblick auf die Anforderungen in Anhang I korrekt angewandt worden sind, sofern sich der Hersteller für ihre Anwendung entschieden hat;

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

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

5. 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.

6. Entsprechen das Baumuster und die Verfahren zur Behandlung von Schwachstellen den grundlegenden Cybersicherheitsanforderungen 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 einschlägigen Informationen, anhand deren sich die Konformität der hergestellten oder entwickelten Produkte mit digitalen Elementen 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 Cybersicherheitsanforderungen in Anhang I, so verweigert die notifizierte Stelle die Ausstellung einer EU-Baumusterprüfbescheinigung und unterrichtet den Antragsteller darüber, wobei sie ihre Weigerung ausführlich begründet.

7. 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 Cybersicherheitsanforderungen in Anhang I 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 Cybersicherheitsanforderungen 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.

8. Die notifizierte Stelle führt regelmäßig Audits durch, um sicherzustellen, dass die in Anhang I Teil II aufgeführten Verfahren zur Behandlung von Schwachstellen angemessen umgesetzt werden.

9. Jede notifizierte Stelle unterrichtet ihre notifizierenden Behörden über die EU-Baumusterprüfbescheinigungen und 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 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 etwaige Ergänzungen dazu, die sie verweigert, zurückgenommen, ausgesetzt oder auf andere Weise eingeschränkt hat, und auf Verlangen über die Bescheinigungen und Ergänzungen dazu, die sie ausgestellt hat.

   Auf Verlangen erhalten die Kommission, die Mitgliedstaaten und die anderen notifizierten Stellen ein Exemplar der EU-Baumusterprüfbescheinigungen und jeglicher 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.

10. Der Hersteller hält ein Exemplar der EU-Baumusterprüfbescheinigung samt Anhängen und Ergänzungen zusammen mit der technischen Dokumentation zehn Jahre lang nach dem Inverkehrbringen des Produkts mit digitalen Elementen oder während des Unterstützungszeitraums je nachdem, welcher Zeitraum länger ist, für die nationalen Behörden bereit.

11. Der Bevollmächtigte des Herstellers kann den in Nummer 3 genannten Antrag einreichen und die in den Nummern 7 und 10 genannten Pflichten erfüllen, falls die einschlägigen Verpflichtungen in dem Auftrag festgelegt sind.

Teil III 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 dieses Teils festgelegten Pflichten erfüllt sowie sicherstellt und erklärt, dass die betreffenden Produkte mit digitalen Elementen dem in der EU-Baumusterprüfbescheinigung beschriebenen Baumuster entsprechen und den grundlegenden Cybersicherheitsanforderungen in Anhang I Teil I genügen und er die grundlegenden Cybersicherheitsanforderungen in Anhang I Teil II erfüllt.

2. Herstellung

   Der Hersteller trifft alle erforderlichen Maßnahmen, damit die Konformität der hergestellten Produkte mit digitalen Elementen mit dem in der EU-Baumusterprüfbescheinigung beschriebenen zugelassenen Baumuster und den grundlegenden Cybersicherheitsanforderungen in Anhang I Teil I durch die Herstellung und ihre Überwachung gewährleistet ist, und stellt sicher, dass er die grundlegenden Cybersicherheitsanforderungen in Anhang I Teil II erfüllt.

3. Konformitätskennzeichnung und Konformitätserklärung

   3.1. Der Hersteller bringt an jedem einzelnen Produkt mit digitalen Elementen, das mit dem in der EU-Baumusterprüfbescheinigung beschriebenen Baumuster übereinstimmt und die in dieser Verordnung festgelegten geltenden Anforderungen 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 mit digitalen Elementen oder während des Unterstützungszeitraums, je nachdem, welcher Zeitraum länger ist, für die nationalen Behörden bereit. Aus der Konformitätserklärung muss hervorgehen, für welches Produktmodell sie ausgestellt wurde. Ein Exemplar der Konformitätserklärung wird den einschlägigen Behörden auf Verlangen zur Verfügung gestellt.

4. Bevollmächtigter

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

Teil IV 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 festgelegten Pflichten erfüllt sowie gewährleistet und auf eigene Verantwortung erklärt, dass die betreffenden Produkte mit digitalen Elementen oder Produktkategorien den grundlegenden Cybersicherheitsanforderungen in Anhang I Teil I und die vom Hersteller festgelegten Verfahren zur Behandlung von Schwachstellen den grundlegenden Anforderungen in Anhang I Teil II 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 Endabnahme und Prüfung der betreffenden Produkte mit digitalen Elementen und für die Behandlung von Schwachstellen, erhält dessen Wirksamkeit während des Unterstützungszeitraums 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 mit digitalen Elementen.

Der Antrag enthält

a) den Namen und die Anschrift des Herstellers sowie, wenn der Antrag vom Bevollmächtigten eingereicht wird, den Namen und die Anschrift des Bevollmächtigten;

b) die technische Dokumentation jeweils für ein Modell jeder herzustellenden oder zu entwickelnden Kategorie von Produkten mit digitalen Elementen; die technische Dokumentation enthält gegebenenfalls zumindest die in Anhang VII aufgeführten Elemente;

c) die Dokumentation zum Qualitätssicherungssystem;

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

3.2. Das Qualitätssicherungssystem gewährleistet die Konformität des Produkts mit digitalen Elementen mit den grundlegenden Cybersicherheitsanforderungen in Anhang I Teil I und die Konformität der vom Hersteller festgelegten Verfahren zur Behandlung von Schwachstellen mit den grundlegenden Anforderungen in Anhang I Teil II.

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:

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

b) 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 mit digitalen Elementen geltenden grundlegenden Cybersicherheitsanforderungen in Anhang I Teil I erfüllt werden;

c) verfahrenstechnische Spezifikationen, einschließlich der angewandten Normen, sowie bei nicht vollständiger Anwendung der einschlägigen harmonisierten Normen oder technischen Spezifikationen die Mittel, mit denen gewährleistet werden soll, dass die für den Hersteller geltenden grundlegenden Cybersicherheitsanforderungen in Anhang I Teil II erfüllt werden;

d) 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 mit digitalen Elementen angewandt werden;

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

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

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

h) 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 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 und verfügt über Kenntnisse der in dieser Verordnung festgelegten geltenden Anforderungen. Das Audit umfasst auch einen Kontrollbesuch in den Räumlichkeiten des Herstellers, falls es solche gibt. Das Auditteam überprüft die in Nummer 3.1 Buchstabe b genannte technische Dokumentation, um sich zu vergewissern, dass der Hersteller in der Lage ist, die in dieser Verordnung festgelegten anwendbaren Anforderungen zu erkennen und die erforderlichen Prüfungen durchzuführen, damit die Übereinstimmung des Produkts mit digitalen Elementen 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

a) die Unterlagen über das Qualitätssicherungssystem,

b) die im Qualitätssicherungssystem für den Konzeptionsteil vorgesehenen Qualitätsberichte wie Ergebnisse von Analysen, Berechnungen und Prüfungen,

c) die im Qualitätssicherungssystem für den Fertigungsteil vorgesehenen Qualitätsberichte wie Kontrollberichte, Prüf- und Kalibrierungsdaten und Berichte über die Qualifikation der in diesem Bereich beschäftigten Mitarbeiter.

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 mit digitalen Elementen, das den Anforderungen in Anhang I Teil I 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 mit digitalen Elementen oder während des Unterstützungszeitraums, je nachdem, welcher Zeitraum länger ist, für die nationalen Behörden bereit. Aus der Konformitätserklärung muss hervorgehen, für welches Produktmodell sie ausgestellt wurde.

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

6. Der Hersteller hält für einen Zeitraum von mindestens zehn Jahren nach dem Inverkehrbringen des Produkts mit digitalen Elementen oder während des Unterstützungszeitraums, je nachdem, welcher Zeitraum länger ist, folgende Unterlagen für die nationalen Behörden bereit:

a) die technische Dokumentation nach Nummer 3.1,

b) die Unterlagen über das Qualitätssicherungssystem nach Nummer 3.1,

c) die Änderung nach Nummer 3.5 in ihrer genehmigten Form,

d) die Entscheidungen und Berichte der notifizierten Stelle nach den Nummern 3.5 und 4.3.

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 in den Nummern 3.1, 3.5, 5 und 6 genannten Verpflichtungen des Herstellers können von seinem Bevollmächtigten in seinem Auftrag und unter seiner Verantwortung erfüllt werden, sofern die einschlägigen Verpflichtungen im Auftrag festgelegt sind.

Zu diesem Rechtsakt wurde eine Erklärung abgegeben, die im ABl. C, 2024/6786, 20.11.2024, ELI: http://data.europa.eu/eli/C/2024/6786/oj, zu finden ist.