



**2022/0272(COD)**

30.6.2023

# **STELLUNGNAHME**

des Ausschusses für Binnenmarkt und Verbraucherschutz

für den Ausschuss für Industrie, Forschung und Energie

zu dem Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen und zur Änderung der Verordnung (EU) 2019/1020 (COM(2022)0454 – C9-0308/2022 – 2022/0272(COD))

Verfasser der Stellungnahme (\*): Morten Løkkegaard

(\*) Assoziierter Ausschuss – Artikel 57 der Geschäftsordnung

PA\_Legam

## KURZE BEGRÜNDUNG

Da der Verfasser der Stellungnahme bereits in dieser Funktion für den IMCO-Ausschuss mit Blick auf die NIS-2-Richtlinie tätig war, betrachtet er das Cyberresilienzgesetz als entscheidenden und nächsten logischen Schritt zur Verbesserung der Cybersicherheit der Europäischen Union. In dem Wissen, dass Cybersicherheit per definitionem nie zu 100 % gegeben sein wird, wird es für wichtig erachtet, alles in unserer Macht Stehende getan wird, um die Zahl der Schwachstellen in der Union zu verringern, weshalb das Cyberresilienzgesetz ein begrüßenswerter nächster Schritt ist. Wir müssen die Cybersicherheit von Produkten mit digitalen Elementen und anderen neuen Produkten wie IoT-Geräten erhöhen, die mittlerweile wie selbstverständlich zum Alltag der europäischen Verbraucher und Unternehmen gehören.

Da der IMCO-Ausschuss für das Funktionieren und die Umsetzung des Binnenmarkts – einschließlich des digitalen Binnenmarkts – und für Verbraucherschutzvorschriften zuständig ist, wurde versucht, Änderungsanträge einzubringen, die darauf abzielen, das Funktionieren des Binnenmarkts zu verbessern und gleichzeitig im Rahmen des Vorschlags für ein hohes Verbraucherschutzniveau zu sorgen, insbesondere was die Anforderungen an die Cybersicherheit von Produkten mit digitalen Elementen anbelangt.

Darüber hinaus wird die Ansicht vertreten, dass einige Aspekte des Vorschlags für eine Verordnung verbessert werden müssen, damit Rechtsklarheit und Kohärenz zwischen den einschlägigen Bestimmungen der vorgeschlagenen Verordnung und anderen Rechtsvorschriften besteht. Dies betrifft insbesondere die NIS-2-Richtlinie, die kürzlich angenommene Verordnung über die allgemeine Produktsicherheit, die Verordnung über künstliche Intelligenz und die Maschinenverordnung sowie eine Reihe einschlägiger delegierter Rechtsakte und Durchführungsrechtsakte. Daher werden Änderungen vorgeschlagen, mit denen die Rechtsklarheit verbessert und zu einer kohärenten, wirksamen und einheitlichen Auslegung und Anwendung der genannten Rechtsvorschriften beigetragen werden soll.

Da Kleinstunternehmen sowie kleine und mittlere Unternehmen wichtige Wirtschaftsakteure des digitalen Markts sind, wurden einige Änderungsanträge vorgebracht, mit denen die Verwaltungsverfahren vereinfacht und der Verwaltungsaufwand für kleine Unternehmen begrenzt werden soll, ohne dabei Abstriche beim Sicherheitsniveau zu machen. Darüber hinaus wurden Änderungsanträge eingebracht, mit denen sichergestellt wird, dass Kleinstunternehmen und KMU spezielle Leitlinien und Beratung bezüglich der Einhaltung der Anforderungen aus dem Cyberresilienzgesetz erhalten.

Zu guter Letzt wurden Änderungsanträge vorgeschlagen, mit denen eine effizientere Kommunikation mit den zuständigen Behörden (nationale Marktüberwachungsbehörden, ENISA) sichergestellt werden soll und die Bestimmungen über die Pflichten und Zuständigkeiten der zuständigen Behörden in Bezug auf Beschwerden, Inspektionen und gemeinsame Tätigkeiten gestärkt werden sollen. In einigen Änderungsanträgen geht es zudem um die Verbesserung der Anforderungen an die Cybersicherheit von Komponenten, die in Endprodukte mit digitalen Elementen integriert werden, wobei die Pflichten von Wirtschaftsakteuren wie etwa Herstellern und Bevollmächtigten festgelegt werden.

Es wird noch einmal betont, dass die Vorlage des Cyberresilienzgesetzes ein logischer nächster Schritt ist, der jetzt erforderlich ist, um die Cyberbedrohungen in der Union stärker

einzudämmen. Mit den vorgeschlagenen Änderungen wurde versucht, das richtige Gleichgewicht zwischen der Sicherstellung eines höheren Cybersicherheitsniveaus zum Nutzen der europäischen Verbraucher und einer in einem angemessenen Verhältnis stehenden Belastung für die Wirtschaft zu finden. Die Cybersicherheit sollte zu einem selbstverständlichen Wettbewerbsparameter im Binnenmarkt werden. Deshalb wurde versucht, den Vorschlag in diesem Sinne anzupassen.

## ÄNDERUNGSANTRÄGE

Der Ausschuss für Binnenmarkt und Verbraucherschutz ersucht den federführenden Ausschuss für Industrie, Forschung und Energie, Folgendes zu berücksichtigen:

### Änderungsantrag 1

#### Vorschlag für eine Verordnung

##### Erwägung 1

###### *Vorschlag der Kommission*

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

###### *Geänderter Text*

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

### Änderungsantrag 2

#### Vorschlag für eine Verordnung

##### Erwägung 7

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

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

### Änderungsantrag 3

#### Vorschlag für eine Verordnung Erwägung 7 a (neu)

Vorschlag der Kommission

Geänderter Text

**(7a) Diese Verordnung sollte nicht für interne Netze eines Produktes mit digitalen Elementen gelten, wenn diese Netze über eigene Endpunkte verfügen, vollständig isoliert und vor externen Datenverbindungen geschützt sind.**

#### Änderungsantrag 4

##### Vorschlag für eine Verordnung Erwägung 7 b (neu)

Vorschlag der Kommission

Geänderter Text

**(7b) Diese Verordnung sollte nicht für Ersatzteile gelten, die ausschließlich dazu bestimmt sind, defekte Teile von Produkten mit digitalen Elementen zu ersetzen, um deren Funktionsfähigkeit wiederherzustellen.**

#### Änderungsantrag 5

##### Vorschlag für eine Verordnung Erwägung 9

Vorschlag der Kommission

Geänderter Text

(9) Diese Verordnung **gewährleistet** ein hohes Niveau der Cybersicherheit von Produkten mit digitalen Elementen. Sie enthält keine Vorschriften für Dienstleistungen wie Software-as-a-Service (SaaS), **mit Ausnahme von Datenfernverarbeitungslösungen, die sich auf ein Produkt mit digitalen Elementen beziehen und als entfernt stattfindende Datenverarbeitung verstanden werden, für die eine Software vom Hersteller selbst oder unter dessen Verantwortung konzipiert und entwickelt wird und ohne die das Produkt mit digitalen Elementen eine seiner Funktionen nicht erfüllen**

(9) Diese Verordnung **stellt** ein hohes Niveau der Cybersicherheit von Produkten mit digitalen Elementen **sicher**. Sie enthält keine Vorschriften für Dienstleistungen wie Software-as-a-Service (SaaS). Mit der [Richtlinie XXX/XXXX (NIS2)] werden Anforderungen an die Cybersicherheit und die Meldung von Sicherheitsvorfällen für wesentliche und wichtige Einrichtungen wie kritische Infrastrukturen festgelegt, um die Resilienz der von ihnen erbrachten Dienste zu erhöhen. Die [Richtlinie XXX/XXXX (NIS2)] gilt für Cloud-Computing-Dienste und Cloud-Dienstmodelle wie SaaS. In den

**könnte.** Mit der [Richtlinie XXX/XXXX (NIS2)] werden Anforderungen an die Cybersicherheit und die Meldung von Sicherheitsvorfällen für wesentliche und wichtige Einrichtungen wie kritische Infrastrukturen festgelegt, um die Resilienz der von ihnen erbrachten Dienste zu erhöhen. Die [Richtlinie XXX/XXXX (NIS2)] gilt für Cloud-Computing-Dienste und Cloud-Dienstmodelle wie SaaS. In den Anwendungsbereich dieser Richtlinie fallen alle Einrichtungen, die Cloud-Computing-Dienste in der Union erbringen und den Schwellenwert für mittlere Unternehmen erreichen oder überschreiten.

Anwendungsbereich dieser Richtlinie fallen alle Einrichtungen, die Cloud-Computing-Dienste in der Union erbringen und den Schwellenwert für mittlere Unternehmen erreichen oder überschreiten.

## Änderungsantrag 6

### Vorschlag für eine Verordnung Erwägung 10

#### *Vorschlag der Kommission*

(10) Um die Innovation oder die Forschung nicht zu behindern, sollte freie und quelloffene Software, die außerhalb einer Geschäftstätigkeit entwickelt oder bereitgestellt wird, nicht unter diese Verordnung fallen. Dies gilt insbesondere für offen geteilte und frei zugängliche, nutzbare, veränderbare und weiterverteilbare Software, einschließlich ihres Quellcodes und ihrer veränderten Versionen. **Im Zusammenhang mit Software ist eine Geschäftstätigkeit möglicherweise nicht nur** dadurch gekennzeichnet, dass für **ein Produkt** ein **Preis** verlangt wird, **sondern auch dadurch, dass** für technische Unterstützungsleistungen **ein Entgelt verlangt wird, dass eine Softwareplattform bereitgestellt wird**, über die der Hersteller andere Dienste monetisiert, oder **dass personenbezogene** Daten zu anderen Zwecken als der alleinigen Verbesserung der Sicherheit, Kompatibilität oder Interoperabilität der Software **verwendet**

#### *Geänderter Text*

(10) **Software und Daten, die offen geteilt werden und die Nutzer kostenlos abrufen, nutzen, verändern und weiter verteilen können, auch in veränderter Form, können zu Forschung und Innovation auf dem Markt beitragen. Eine Untersuchung der Kommission hat zudem ergeben, dass mit freier und quelloffener Software ein Beitrag zum Bruttoinlandsprodukt der Union in Höhe von 65 Mrd. bis 95 Mrd. EUR geleistet werden kann und dass sie erhebliche Wachstumschancen für die europäische Wirtschaft bietet.** Um die Innovation oder die Forschung nicht zu behindern, sollte freie und quelloffene Software, die außerhalb einer Geschäftstätigkeit entwickelt oder bereitgestellt wird, nicht unter diese Verordnung fallen. Dies gilt insbesondere für offen geteilte und frei zugängliche, nutzbare, veränderbare und weiterverteilbare Software, einschließlich ihres Quellcodes und ihrer veränderten Versionen. **Eine Geschäftstätigkeit im Sinne einer Bereitstellung auf dem Markt**

werden.

*kann indes auch* dadurch gekennzeichnet *sein*, dass für *freie und quelloffene Softwarekomponenten ein Entgelt* verlangt wird, *aber* auch *durch eine Monetisierung wie das Verlangen der Zahlung eines Preises* für technische Unterstützungsleistungen *oder für kostenpflichtige Softwareaktualisierungen, sofern es sich dabei nicht um die Deckung tatsächlicher Kosten handelt, durch die Bereitstellung einer Software-Plattform*, über die der Hersteller andere Dienste monetisiert, oder *durch die Verwendung personenbezogener* Daten zu anderen Zwecken als der alleinigen Verbesserung der Sicherheit, Kompatibilität oder Interoperabilität der Software. *Weder die gemeinsame Entwicklung kostenloser oder quelloffener Softwarekomponenten noch ihr Bereitstellung über offene Speicherorte sollten ein Inverkehrbringen oder eine Inbetriebnahme darstellen. Die Umstände, unter denen das Produkt entwickelt wurde, oder die Art und Weise, wie die Entwicklung finanziert wurde, sollten bei der Bestimmung des kommerziellen oder nichtkommerziellen Charakters dieser Tätigkeit nicht berücksichtigt werden. Wird eine quelloffene Software in ein Endprodukt mit digitalen Elementen integriert, das in Verkehr gebracht wird, so sollte der Wirtschaftsakteur, der das Endprodukt mit digitalen Elementen in Verkehr gebracht hat, für die Konformität des Produkts einschließlich der freien und quelloffenen Komponenten verantwortlich sein.*

## Änderungsantrag 7

### Vorschlag für eine Verordnung Erwägung 11

*Vorschlag der Kommission*

(11) Ein sicheres Internet ist für das

AD\1280305DE.docx

*Geänderter Text*

(11) Ein sicheres Internet ist für das

9/113

PE742.490v02-00

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

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

## Änderungsantrag 8

### Vorschlag für eine Verordnung Erwägung 15

#### *Vorschlag der Kommission*

(15) Nach der Delegierten Verordnung (EU) 2022/30 gelten die grundlegenden Anforderungen gemäß Artikel 3 Absatz 3 Buchstabe d (schädliche Auswirkungen auf das Netz und missbräuchliche Nutzung von Netzressourcen), Buchstabe e (personenbezogene Daten und Privatsphäre) und Buchstabe f (Betrug) der

#### *Geänderter Text*

(15) Nach der Delegierten Verordnung (EU) 2022/30 gelten die grundlegenden Anforderungen gemäß Artikel 3 Absatz 3 Buchstabe d (schädliche Auswirkungen auf das Netz und missbräuchliche Nutzung von Netzressourcen), Buchstabe e (personenbezogene Daten und Privatsphäre) und Buchstabe f (Betrug) der

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

## **Änderungsantrag 9**

### **Vorschlag für eine Verordnung Erwägung 18 a (neu)**

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

**(18a) Damit jedoch Einzel- oder Kleinentwickler von Software im Sinne der Empfehlung der Kommission (2003/361/EG) nicht vor schwerwiegende finanzielle Hindernisse gestellt und nicht davon abgehalten werden, das Konzept sowie das Geschäftsmodell auf dem Markt zu testen, sollten diese Unternehmen verpflichtet sein, sich nach besten Kräften darum zu bemühen, während sechs Monaten, nachdem die Software in Verkehr gebracht wurde, die Anforderungen dieser Verordnung zu erfüllen. Diese Sonderregelung soll verhindern, dass hohe Befolgungs- und Markteintrittskosten Unternehmer oder qualifizierte Einzelpersonen abschrecken, die die Entwicklung von Software in der Union in Betracht ziehen. Diese Sonderregelung sollte jedoch nicht für hochkritische Produkte mit digitalen Elementen gelten.**

## Änderungsantrag 10

### Vorschlag für eine Verordnung Erwägung 19

(19) Bestimmte in dieser Verordnung vorgesehene Aufgaben sollten von der ENISA im Einklang mit Artikel 3 Absatz 2 der Verordnung (EU) 2019/881 wahrgenommen werden. Insbesondere sollte die ENISA Meldungen von Herstellern über aktiv ausgenutzte Schwachstellen in Produkten mit digitalen Elementen sowie über Vorfälle, die sich auf die Sicherheit dieser Produkte auswirken, entgegennehmen. Die ENISA sollte diese Meldungen auch an die zuständigen Computer-Notfallteams (CSIRTs) bzw. an die gemäß Artikel [Artikel X] der Richtlinie

(19) Bestimmte in dieser Verordnung vorgesehene Aufgaben sollten von der ENISA im Einklang mit Artikel 3 Absatz 2 der Verordnung (EU) 2019/881 wahrgenommen werden. Insbesondere sollte die ENISA **im Wege einer Frühwarnung** Meldungen von Herstellern über aktiv ausgenutzte Schwachstellen in Produkten mit digitalen Elementen sowie über Vorfälle, die sich **erheblich** auf die Sicherheit dieser Produkte auswirken, entgegennehmen. Die ENISA sollte diese Meldungen auch an die zuständigen Computer-Notfallteams (CSIRTs) bzw. an die gemäß Artikel [Artikel X] der

[Richtlinie XXX/XXXX (NIS2)] benannten zentralen Anlaufstellen der Mitgliedstaaten weiterleiten und die betreffenden Marktüberwachungsbehörden **von den gemeldeten Schwachstellen** unterrichten. Auf der Grundlage der von ihr erfassten Informationen sollte die ENISA alle zwei Jahre einen technischen Bericht über aufkommende Trends in Bezug auf Cybersicherheitsrisiken bei Produkten mit digitalen Elementen erstellen und ihn der in der Richtlinie [Richtlinie XXX/XXXX (NIS2)] genannten Kooperationsgruppe vorlegen. Darüber hinaus sollte die ENISA angesichts ihrer Sachkenntnis und ihres Auftrags in der Lage sein, den Prozess der Durchführung dieser Verordnung zu unterstützen. Sie sollte insbesondere in der Lage sein, gemeinsame Tätigkeiten vorzuschlagen, die von Marktüberwachungsbehörden auf der Grundlage von Hinweisen oder Informationen über eine mögliche Nichtkonformität von Produkten mit digitalen Elementen mit dieser Verordnung in mehreren Mitgliedstaaten durchgeführt werden sollen, oder Produktkategorien zu ermitteln, zu denen gleichzeitige koordinierte Kontrollen organisiert werden sollten. Unter außergewöhnlichen Umständen sollte die ENISA auf Ersuchen der Kommission Bewertungen in Bezug auf bestimmte Produkte mit digitalen Elementen, die ein erhebliches Cybersicherheitsrisiko bergen, durchführen können, wenn ein sofortiges Eingreifen erforderlich ist, um das reibungslose Funktionieren des Binnenmarkts zu bewahren.

Richtlinie [Richtlinie XXX/XXXX (NIS2)] benannten zentralen Anlaufstellen der Mitgliedstaaten weiterleiten und die betreffenden Marktüberwachungsbehörden **unverzüglich über das Vorhandensein einer Schwachstelle und gegebenenfalls über die mögliche Risikominderungsmaßnahme** unterrichten. **Wenn für eine gemeldete Schwachstelle keine Abhilfemaßnahmen verfügbar sind, sollte die ENISA sicherstellen, dass Informationen über die gemeldete Schwachstelle unter Verwendung strenger Sicherheitsprotokolle und nach dem Grundsatz „Kenntnis nur, wenn nötig“ weitergegeben werden.** Auf der Grundlage der von ihr erfassten Informationen sollte die ENISA alle zwei Jahre einen technischen Bericht über aufkommende Trends in Bezug auf Cybersicherheitsrisiken bei Produkten mit digitalen Elementen erstellen und ihn der in der Richtlinie [Richtlinie XXX/XXXX (NIS2)] genannten Kooperationsgruppe vorlegen. Darüber hinaus sollte die ENISA angesichts ihrer Sachkenntnis und ihres Auftrags in der Lage sein, den Prozess der Durchführung dieser Verordnung zu unterstützen. Sie sollte insbesondere in der Lage sein, gemeinsame Tätigkeiten vorzuschlagen, die von Marktüberwachungsbehörden auf der Grundlage von Hinweisen oder Informationen über eine mögliche Nichtkonformität von Produkten mit digitalen Elementen mit dieser Verordnung in mehreren Mitgliedstaaten durchgeführt werden sollen, oder Produktkategorien zu ermitteln, zu denen gleichzeitige koordinierte Kontrollen organisiert werden sollten. Unter außergewöhnlichen Umständen sollte die ENISA auf Ersuchen der Kommission Bewertungen in Bezug auf bestimmte Produkte mit digitalen Elementen, die ein erhebliches Cybersicherheitsrisiko bergen, durchführen können, wenn ein sofortiges Eingreifen erforderlich ist, um das reibungslose

Funktionieren des Binnenmarkts zu bewahren.

## Änderungsantrag 11

### Vorschlag für eine Verordnung Erwägung 20

#### *Vorschlag der Kommission*

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

#### *Geänderter Text*

(20) 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.

## Änderungsantrag 12

### Vorschlag für eine Verordnung Erwägung 22

#### *Vorschlag der Kommission*

(22) Damit Produkte mit digitalen Elementen beim Inverkehrbringen keine Cybersicherheitsrisiken für Personen und Organisationen darstellen, sollten für solche Produkte grundlegende Anforderungen festgelegt werden. Werden solche Produkte nachträglich physisch oder digital in einer Weise verändert, die vom Hersteller nicht vorgesehen ist und die dazu führen kann, dass sie die betreffenden grundlegenden Anforderungen nicht mehr erfüllen, sollte die Veränderung als wesentlich betrachtet werden. Beispielsweise könnten Software-Aktualisierungen und -Reparaturen den

#### *Geänderter Text*

(22) Damit Produkte mit digitalen Elementen beim Inverkehrbringen keine Cybersicherheitsrisiken für Personen und Organisationen darstellen, sollten für solche Produkte grundlegende Anforderungen festgelegt werden. Werden solche Produkte nachträglich physisch oder digital in einer Weise verändert, die vom Hersteller nicht vorgesehen ist und die dazu führen kann, dass sie die betreffenden grundlegenden Anforderungen nicht mehr erfüllen, sollte die Veränderung als wesentlich betrachtet werden. Beispielsweise könnten Software-Aktualisierungen und -Reparaturen **wie**

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

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

### **Änderungsantrag 13**

#### **Vorschlag für eine Verordnung Erwägung 23**

##### *Vorschlag der Kommission*

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

##### *Geänderter Text*

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

eines Dritten durchführt, sollten Veränderungen, die zu wesentlichen Änderungen führen könnten, dem Dritten mitgeteilt werden.

Veränderungen, die zu wesentlichen Änderungen führen könnten, dem Dritten mitgeteilt werden. ***In der anschließenden Konformitätsbewertung sollte auf die Veränderungen eingegangen werden, die zu der neuen Bewertung geführt haben, außer wenn sich diese Veränderungen erheblich auf die Konformität anderer Teile des Produkts ausgewirkt haben. Werden Software-Aktualisierungen implementiert, ist der Hersteller nicht verpflichtet, eine weitere Konformitätsbewertung des Produkts mit digitalen Elementen durchzuführen, es sei denn, die Software-Aktualisierung führt zu einer wesentlichen Änderung des Produkts mit digitalen Elementen.***

## Änderungsantrag 14

### Vorschlag für eine Verordnung Erwägung 24 a (neu)

*Vorschlag der Kommission*

*Geänderter Text*

***(24a) Die Hersteller von Produkten mit digitalen Elementen sollten sicherstellen, dass Software-Aktualisierungen auf eine klare und transparente Weise bereitgestellt werden und dass unmissverständlich zwischen Aktualisierungen, die die Sicherheit und die Funktionalität betreffen, unterschieden wird. Während Sicherheitsaktualisierungen dazu dienen, das Risiko eines Produkts mit digitalen Elementen zu verringern, sollte die Übernahme von Funktionalitätsaktualisierungen, die der Hersteller bereitstellt, stets dem Nutzer überlassen sein. Die Hersteller sollten diese Aktualisierungen daher – außer wenn dies technisch unmöglich ist – separat bereitstellen. Die Hersteller sollten den Verbrauchern die Gründe für die einzelnen Aktualisierungen und ihre voraussichtlichen Auswirkungen auf das Produkt mitteilen und ihnen eine klare***

*und einfach zu befolgende Möglichkeit des Verzichts darauf anbieten.*

## **Änderungsantrag 15**

### **Vorschlag für eine Verordnung Erwägung 25**

#### *Vorschlag der Kommission*

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

#### *Geänderter Text*

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

## **Änderungsantrag 16**

### **Vorschlag für eine Verordnung Erwägung 26**

### *Vorschlag der Kommission*

(26) Kritische Produkte mit digitalen Elementen sollten strengeren Konformitätsbewertungsverfahren unterliegen, wobei ein verhältnismäßiger Ansatz gewahrt bleiben sollte. Zu diesem Zweck sollten kritische Produkte mit digitalen Elementen in zwei Klassen unterteilt werden, die das mit diesen Produktkategorien verbundene Cybersicherheitsrisiko widerspiegeln. Ein potenzieller Cybervorfall mit Produkten der Klasse II könnte größere negative Auswirkungen haben als ein Vorfall mit Produkten der Klasse I, beispielsweise wegen der Art ihrer Cybersicherheitsfunktion oder ihrer bestimmungsgemäßen Verwendung in sensiblen Umgebungen, und daher sollten erstere Produkte einem strengeren Konformitätsbewertungsverfahren unterzogen werden.

### *Geänderter Text*

(26) Kritische Produkte mit digitalen Elementen sollten strengeren Konformitätsbewertungsverfahren unterliegen, wobei ein verhältnismäßiger Ansatz gewahrt bleiben sollte. Zu diesem Zweck sollten kritische Produkte mit digitalen Elementen in zwei Klassen unterteilt werden, die das mit diesen Produktkategorien verbundene Cybersicherheitsrisiko widerspiegeln. Ein potenzieller Cybervorfall mit Produkten der Klasse II könnte größere negative Auswirkungen haben als ein Vorfall mit Produkten der Klasse I, beispielsweise wegen der Art ihrer Cybersicherheitsfunktion oder ihrer bestimmungsgemäßen Verwendung in sensiblen Umgebungen, und daher sollten erstere Produkte einem strengeren Konformitätsbewertungsverfahren unterzogen werden. ***Kleine und mittlere Unternehmen sollte das Verfahren für Produkte der Klasse I anwenden dürfen.***

## **Änderungsantrag 17**

### **Vorschlag für eine Verordnung Erwägung 29**

#### *Vorschlag der Kommission*

(29) Produkte mit digitalen Elementen, die nach Artikel 6 der Verordnung<sup>27</sup> [KI-Verordnung] als Hochrisiko-KI-Systeme eingestuft sind und in den Anwendungsbereich der vorliegenden Verordnung fallen, sollten den in der vorliegenden Verordnung festgelegten grundlegenden Anforderungen genügen. Genügen diese Hochrisiko-KI-Systeme den grundlegenden Anforderungen der vorliegenden Verordnung, so sollte davon ausgegangen werden, dass sie die Cybersicherheitsanforderungen gemäß Artikel [Artikel 15] der Verordnung [KI-

#### *Geänderter Text*

(29) ***Produkte mit digitalen Elementen oder unvollständige*** Produkte mit digitalen Elementen, die nach Artikel 6 der Verordnung [KI-Verordnung] als Hochrisiko-KI-Systeme eingestuft sind und in den Anwendungsbereich der vorliegenden Verordnung fallen, sollten den in der vorliegenden Verordnung festgelegten grundlegenden Anforderungen genügen. Genügen diese Hochrisiko-KI-Systeme den grundlegenden Anforderungen der vorliegenden Verordnung, so sollte davon ausgegangen werden, dass sie die

Verordnung] erfüllen, soweit diese Anforderungen von der nach der vorliegenden Verordnung ausgestellten EU-Konformitätserklärung oder Teilen davon abgedeckt sind. Für die Konformitätsbewertungsverfahren zu den grundlegenden Cybersicherheitsanforderungen für ein Produkt mit digitalen Elementen, das unter die vorliegende Verordnung fällt und als Hochrisiko-KI-System eingestuft ist, sollten grundsätzlich anstelle der jeweiligen Bestimmungen der vorliegenden Verordnung die einschlägigen Bestimmungen des **Artikels 43** der Verordnung [KI-Verordnung] Anwendung finden. Diese Regel sollte **jedoch nicht dazu führen, dass die erforderliche Vertrauenswürdigkeit für unter die vorliegende Verordnung fallende kritische Produkte mit digitalen Elementen verringert wird. Deshalb sollten abweichend von dieser Regel Hochrisiko-KI-Systeme**, die in den Anwendungsbereich der Verordnung [KI-Verordnung] fallen und auch als kritische Produkte mit digitalen Elementen **gemäß der vorliegenden Verordnung gelten und auf die das Konformitätsbewertungsverfahren auf der Grundlage einer internen Kontrolle gemäß Anhang VI der Verordnung [KI-Verordnung] angewandt wird, den Konformitätsbewertungsbestimmungen der vorliegenden Verordnung unterliegen, soweit die grundlegenden Anforderungen der vorliegenden Verordnung betroffen sind. In diesem Fall sollten für alle anderen Aspekte, die unter die Verordnung [KI-Verordnung] fallen, die jeweiligen Bestimmungen über die Konformitätsbewertung auf der Grundlage einer internen Kontrolle gemäß Anhang VI der Verordnung [KI-Verordnung] gelten.**

---

<sup>27</sup> Verordnung [KI-Verordnung].

Cybersicherheitsanforderungen gemäß Artikel [Artikel 15] der Verordnung [KI-Verordnung] erfüllen, soweit diese Anforderungen von der nach der vorliegenden Verordnung ausgestellten EU-Konformitätserklärung oder Teilen davon abgedeckt sind. Für die Konformitätsbewertungsverfahren zu den grundlegenden Cybersicherheitsanforderungen für ein Produkt mit digitalen Elementen, das unter die vorliegende Verordnung fällt und als Hochrisiko-KI-System eingestuft ist, sollten grundsätzlich anstelle der jeweiligen Bestimmungen der vorliegenden Verordnung die einschlägigen Bestimmungen des **[anwendbare Bestimmungen]** der Verordnung [KI-Verordnung] Anwendung finden. **Durch** diese Regel sollte **ein hoher Grad von Vertrauenswürdigkeit für unter die vorliegende Verordnung fallende kritische Produkte mit digitalen Elementen geschaffen werden. Bei KI-Systemen mit hohem Risiko**, die in den Anwendungsbereich der Verordnung **[der KI-Verordnung]** fallen und auch als kritische Produkte mit digitalen Elementen **im Sinne dieser Verordnung eingestuft werden, sollte die zuständige sektorspezifische notifizierte Stelle für die Durchführung der Konformitätsbewertung im Rahmen dieser Verordnung verantwortlich sein und das Verwaltungsverfahren leiten, sodass die Wirtschaftsakteure ihren Antrag auf Konformitätsbewertung an eine einzige Aufsichtsbehörde richten können.**

---

<sup>27</sup> Verordnung [KI-Verordnung].

## Änderungsantrag 18

### Vorschlag für eine Verordnung Erwägung 32

#### *Vorschlag der Kommission*

(32) Um sicherzustellen, dass Produkte mit digitalen Elementen sowohl zum Zeitpunkt ihres Inverkehrbringens als auch während ihres gesamten Lebenszyklus sicher sind, müssen grundlegende Anforderungen für die Behandlung von Schwachstellen und grundlegende Cybersicherheitsanforderungen in Bezug auf die Eigenschaften von Produkten mit digitalen Elementen festgelegt werden. Die Hersteller sollten sowohl alle grundlegenden Anforderungen in Bezug auf die Behandlung von Schwachstellen erfüllen und sicherstellen, dass alle ihre Produkte ohne bekannte ausnutzbare Schwachstellen abgegeben werden, als auch bestimmen, welche anderen grundlegenden Anforderungen in Bezug auf die Produkteigenschaften für die betreffende Produktart von Bedeutung sind. Zu diesem Zweck sollten die Hersteller eine Bewertung der Cybersicherheitsrisiken vornehmen, die mit einem Produkt mit digitalen Elementen verbunden sind, um einschlägige Risiken und grundlegende Anforderungen zu ermitteln und geeignete harmonisierte Normen **oder gemeinsame Spezifikationen** angemessen anzuwenden.

## Änderungsantrag 19

### Vorschlag für eine Verordnung Erwägung 33 a (neu)

#### *Vorschlag der Kommission*

#### *Geänderter Text*

(32) Um sicherzustellen, dass Produkte mit digitalen Elementen sowohl zum Zeitpunkt ihres Inverkehrbringens als auch während ihres gesamten Lebenszyklus sicher sind, müssen grundlegende Anforderungen für die Behandlung von Schwachstellen und grundlegende Cybersicherheitsanforderungen in Bezug auf die Eigenschaften von Produkten mit digitalen Elementen festgelegt werden. Die Hersteller sollten sowohl alle grundlegenden Anforderungen in Bezug auf die Behandlung von Schwachstellen erfüllen und sicherstellen, dass alle ihre Produkte ohne bekannte ausnutzbare Schwachstellen abgegeben werden, als auch bestimmen, welche anderen grundlegenden Anforderungen in Bezug auf die Produkteigenschaften für die betreffende Produktart von Bedeutung sind. Zu diesem Zweck sollten die Hersteller eine Bewertung der Cybersicherheitsrisiken vornehmen, die mit einem Produkt mit digitalen Elementen verbunden sind, um einschlägige Risiken und grundlegende Anforderungen zu ermitteln und geeignete harmonisierte Normen angemessen anzuwenden.

**(33a) Damit die Produkte in  
Übereinstimmung mit den gemäß**

*Abschnitt 1 von Anhang I vorgesehenen Anforderungen konzipiert, entwickelt und hergestellt werden, sollten die Hersteller die erforderliche Sorgfalt walten lassen, wenn sie Komponenten, die von Dritten bezogen werden, in Produkte mit digitalen Elementen integrieren. Dies ist der Fall bei Komponenten, die unter Berücksichtigung der Besonderheiten des Produkts angepasst und integriert werden, insbesondere bei freier und quelloffener Software, die nicht gegen eine finanzielle oder andere Form von Vergütung auf den Markt gebracht wurde.*

## Änderungsantrag 20

### Vorschlag für eine Verordnung Erwägung 34

#### *Vorschlag der Kommission*

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

#### *Geänderter Text*

(34) Damit die nationalen CSIRTs und die nach Artikel [X] der Richtlinie [Richtlinie XX/XXXX (NIS2)] benannte zentrale Anlaufstelle die Informationen erhalten, die sie benötigen, um ihre Aufgaben wahrzunehmen und das Gesamtniveau der Cybersicherheit wesentlicher und wichtiger Einrichtungen zu erhöhen, und um das wirksame Funktionieren der Marktüberwachungsbehörden zu gewährleisten, sollten die Hersteller von Produkten mit digitalen Elementen der ENISA **unverzüglich, auf jeden Fall aber innerhalb von 48 Stunden, nachdem sie davon Kenntnis erlangt haben**, aktiv **ausgenutzte** Schwachstellen **im Wege einer Frühwarnung** melden. **Nachdem die Hersteller Kenntnis von einer aktiv ausgenutzten Schwachstelle erlangt haben, die sich erheblich auf die Sicherheit des Produkts mit digitalen Elementen auswirkt, sollten sie der ENISA unverzüglich weitere Einzelheiten über die ausgenutzte Schwachstelle mitteilen. Alle anderen Schwachstellen,**

Schwachstellendatenbank oder einer anderen öffentlich zugänglichen Schwachstellendatenbank offenzulegen.

**die sich nicht wesentlich auf die Sicherheit des Produkts mit digitalen Elementen auswirken, sollten der ENISA gemeldet werden, sobald die Schwachstellen beseitigt wurden.** Da die meisten Produkte mit digitalen Elementen im gesamten Binnenmarkt vermarktet werden, sollte jede ausgenutzte Schwachstelle in einem Produkt mit digitalen Elementen als Bedrohung für das Funktionieren des Binnenmarkts betrachtet werden. Überdies sollten die Hersteller in Erwägung ziehen, behobene Schwachstellen in der gemäß der Richtlinie [Richtlinie XX/XXXX (NIS2)] eingerichteten und von der ENISA verwalteten europäischen Schwachstellendatenbank oder einer anderen öffentlich zugänglichen Schwachstellendatenbank offenzulegen.

## Änderungsantrag 21

### Vorschlag für eine Verordnung Erwägung 34 a (neu)

*Vorschlag der Kommission*

*Geänderter Text*

**(34a) Die ENISA sollte für die Veröffentlichung und Pflege einer Datenbank zu bekannten ausgenutzten Schwachstellen verantwortlich sein. Die Hersteller sollten die Datenbank im Auge behalten und gefundene Schwachstellen in ihren Produkten melden.**

## Änderungsantrag 22

### Vorschlag für eine Verordnung Erwägung 35

*Vorschlag der Kommission*

*Geänderter Text*

(35) Die Hersteller sollten der ENISA auch jeden Vorfall melden, der sich auf die Sicherheit eines Produkts mit digitalen

(35) Die Hersteller sollten der ENISA auch jeden Vorfall **im Wege einer Frühwarnung** melden, der sich **wesentlich**

Elementen auswirkt. Ungeachtet der Verpflichtung wesentlicher und wichtiger Einrichtungen zur Meldung von Sicherheitsvorfällen gemäß der Richtlinie [Richtlinie XXX/XXXX (NIS2)] ist es von entscheidender Bedeutung, dass die ENISA, die von den Mitgliedstaaten gemäß Artikel [X] der Richtlinie [Richtlinie XXX/XXXX (NIS2)] benannten zentralen Anlaufstellen und die Marktüberwachungsbehörden von den Herstellern der Produkte mit digitalen Elementen Informationen erhalten, die es ihnen ermöglichen, die Sicherheit dieser Produkte zu bewerten. Damit die Nutzer rasch auf Vorfälle reagieren können, die sich auf die Sicherheit ihrer Produkte mit digitalen Elementen auswirken, sollten die Hersteller auch ihre Nutzer über solche Vorfälle und gegebenenfalls über Korrekturmaßnahmen informieren, die die Nutzer ergreifen können, um die Auswirkungen des **Vorfalls** zu mindern, und zwar z. B. durch Veröffentlichung einschlägiger Informationen auf ihren Websites oder, falls der Hersteller zu den Nutzern Kontakt aufnehmen kann und die Risiken dies rechtfertigen, durch direkte Kontaktaufnahme zu den Nutzern.

auf die Sicherheit eines Produkts mit digitalen Elementen auswirkt. **Die Hersteller sollten der ENISA unverzüglich, in jedem Fall aber innerhalb von 72 Stunden, nachdem sie Kenntnis von einem Sicherheitsvorfall im Zusammenhang mit dem Produkt mit digitalen Elementen erlangt hat, weitere Einzelheiten zu dem erheblichen Sicherheitsvorfall mitteilen.** Ungeachtet der Verpflichtung wesentlicher und wichtiger Einrichtungen zur Meldung von Sicherheitsvorfällen gemäß der Richtlinie [Richtlinie XXX/XXXX (NIS2)] ist es von entscheidender Bedeutung, dass die ENISA, die von den Mitgliedstaaten gemäß Artikel [X] der Richtlinie [Richtlinie XXX/XXXX (NIS2)] benannten zentralen Anlaufstellen und die Marktüberwachungsbehörden von den Herstellern der Produkte mit digitalen Elementen Informationen erhalten, die es ihnen ermöglichen, die Sicherheit dieser Produkte zu bewerten. Damit die Nutzer rasch auf Vorfälle reagieren können, die sich **erheblich** auf die Sicherheit ihrer Produkte mit digitalen Elementen auswirken, sollten die Hersteller auch ihre Nutzer über solche Vorfälle, **wenn dies angebracht ist und wenn sie davon betroffen sein könnten**, und gegebenenfalls über Korrekturmaßnahmen informieren, die die Nutzer ergreifen können, um die Auswirkungen des **erheblichen 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 Risiken dies rechtfertigen, durch direkte Kontaktaufnahme zu den Nutzern. **Die Hersteller, die eine Schwachstelle in einer Komponente eines Produkts mit digitalen Elementen feststellen, was auch freie und quelloffene Komponenten einschließt, sollten diese Schwachstelle der Person oder dem Unternehmen, die die Komponente wartet, zusammen mit der**

*ergriffenen Korrekturmaßnahme melden.*

## **Änderungsantrag 23**

### **Vorschlag für eine Verordnung Erwägung 37 a (neu)**

*Vorschlag der Kommission*

*Geänderter Text*

***(37a) Gemäß dem WTO-Übereinkommen über technische Handelshemmnisse sollten die WTO-Mitglieder, wenn technische Vorschriften erforderlich sind und einschlägige internationale Normen bestehen, diese Normen als Grundlage für ihre eigenen technischen Vorschriften verwenden. Da mit internationalen Normen bezweckt wird, die Harmonisierung von nationalen und regionalen technischen Vorschriften und Normen zu erleichtern und dadurch nichttarifäre technische Handelshemmnisse abzubauen, ist es wichtig, eine Überlappung der Arbeit von Normungsorganisationen zu verhindern. Da es sich bei der Cybersicherheit um ein globales Problem handelt, sollte sich die Union um eine maximale Angleichung bemühen. Zur Verwirklichung dieses Ziels sollte der Normungsauftrag für diese Verordnung gemäß Artikel 10 der Verordnung (EU) Nr. 1025/2012 darauf abzielen, die Hindernisse für die Akzeptanz von Normen zu verringern, indem ihre Fundstellen im Amtsblatt der EU gemäß Artikel 10 Absatz 6 der Verordnung (EU) Nr. 1025/2012 veröffentlicht werden.***

## **Änderungsantrag 24**

### **Vorschlag für eine Verordnung Erwägung 37 b (neu)**

**(37b) In Anbetracht des breiten Anwendungsbereichs dieser Verordnung stellt die frühzeitige Ausarbeitung von harmonisierten Normen eine große Herausforderung dar. Um die Sicherheit der Produkte mit digitalen Komponenten auf dem Unionsmarkt so schnell wie möglich zu erhöhen, sollte die Kommission für einen beschränkten Zeitraum zu erklären befugt werden, dass die vorhandenen internationalen Normen für die Cybersicherheit von Produkten den Anforderungen dieser Richtlinie genügen. Diese Normen sollten als Normen veröffentlicht werden, für die eine Konformitätsvermutung besteht.**

## Änderungsantrag 25

### Vorschlag für eine Verordnung Erwägung 38

(38) Um die Bewertung der Konformität mit den in dieser Verordnung festgelegten Anforderungen zu erleichtern, sollte eine Konformitätsvermutung für Produkte mit digitalen Elementen gelten, die harmonisierten Normen entsprechen, mit denen die grundlegenden Anforderungen dieser Verordnung in detaillierte technische Spezifikationen umgesetzt werden und die gemäß der Verordnung (EU) Nr. 1025/2012 des Europäischen Parlaments und des Rates<sup>29</sup> angenommen wurden. Die Verordnung (EU) Nr. 1025/2012 enthält ein Verfahren für Einwände gegen harmonisierte Normen, falls diese Normen den Anforderungen der vorliegenden Verordnung nicht in vollem Umfang entsprechen.

(38) Um die Bewertung der Konformität mit den in dieser Verordnung festgelegten Anforderungen zu erleichtern, sollte eine Konformitätsvermutung für Produkte mit digitalen Elementen gelten, die harmonisierten Normen entsprechen, mit denen die grundlegenden Anforderungen dieser Verordnung in detaillierte technische Spezifikationen umgesetzt werden und die gemäß der Verordnung (EU) Nr. 1025/2012 des Europäischen Parlaments und des Rates<sup>29</sup> angenommen wurden. Die Verordnung (EU) Nr. 1025/2012 enthält ein Verfahren für Einwände gegen harmonisierte Normen, falls diese Normen den Anforderungen der vorliegenden Verordnung nicht in vollem Umfang entsprechen. **Durch den Normierungsprozess sollte eine ausgewogene Interessenvertretung und eine wirksame Einbeziehung von**

***Interessenträgern der Zivilgesellschaft, darunter von Verbraucherorganisationen, sichergestellt werden.***

---

<sup>29</sup> 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).

---

<sup>29</sup> 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).

## **Änderungsantrag 26**

### **Vorschlag für eine Verordnung Erwägung 41**

#### *Vorschlag der Kommission*

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

#### *Geänderter Text*

(41) ***Wurde im Amtsblatt der Europäischen Union kein Verweis auf harmonisierte Normen, die den Anforderungen des Anhangs I genügen, gemäß der Verordnung (EU) Nr. 1025/2012 veröffentlicht und ist nicht mit der Veröffentlichung eines solchen Verweises innerhalb eines angemessenen Zeitraums zu rechnen***, sollte die Kommission ***befugt*** sein, im Wege von Durchführungsrechtsakten gemeinsame Spezifikationen festzulegen. Gründe für die Entwicklung solcher gemeinsamen Spezifikationen anstelle der Anwendung harmonisierter Normen könnten die Ablehnung des Normungsauftrags durch die europäischen Normungsorganisationen, unangemessene Verzögerungen bei der Ausarbeitung geeigneter harmonisierter Normen oder eine mangelnde Übereinstimmung entwickelter Normen

Konformität mit den grundlegenden Anforderungen dieser Verordnung zu erleichtern, sollte eine Konformitätsvermutung für Produkte mit digitalen Elementen gelten, die den gemeinsamen Spezifikationen entsprechen, die die Kommission nach dieser Verordnung angenommen hat, um ausführliche technische Spezifikationen für diese Anforderungen zu formulieren.

mit den Anforderungen dieser Verordnung oder mit einem Normungsauftrag der Kommission sein. Um die Bewertung der Konformität mit den grundlegenden Anforderungen dieser Verordnung zu erleichtern, sollte eine Konformitätsvermutung für Produkte mit digitalen Elementen gelten, die den gemeinsamen Spezifikationen entsprechen, die die Kommission nach dieser Verordnung angenommen hat, um ausführliche technische Spezifikationen für diese Anforderungen zu formulieren.

## Änderungsantrag 27

### Vorschlag für eine Verordnung Erwägung 43

#### *Vorschlag der Kommission*

(43) Die CE-Kennzeichnung bringt die Konformität eines Produkts zum Ausdruck und ist das sichtbare Ergebnis eines ganzen Prozesses, der die Konformitätsbewertung im weiteren Sinne umfasst. Die allgemeinen Grundsätze für die CE-Kennzeichnung sind in der Verordnung (EG) Nr. 765/2008 des Europäischen Parlaments und des Rates<sup>30</sup> festgelegt. Die Vorschriften für die Anbringung der CE-Kennzeichnung auf Produkten mit digitalen Elementen sollten in der vorliegenden Verordnung festgelegt werden. Die CE-Kennzeichnung sollte die einzige Kennzeichnung sein, die die Übereinstimmung der Produkte mit digitalen Elementen mit den Anforderungen dieser Verordnung garantiert.

#### *Geänderter Text*

(43) Die CE-Kennzeichnung bringt die Konformität eines Produkts zum Ausdruck und ist das sichtbare Ergebnis eines ganzen Prozesses, der die Konformitätsbewertung im weiteren Sinne umfasst. Die allgemeinen Grundsätze für die CE-Kennzeichnung sind in der Verordnung (EG) Nr. 765/2008 des Europäischen Parlaments und des Rates<sup>30</sup> festgelegt. Die Vorschriften für die Anbringung der CE-Kennzeichnung auf Produkten mit digitalen Elementen sollten in der vorliegenden Verordnung festgelegt werden. Die CE-Kennzeichnung sollte die einzige Kennzeichnung sein, die die Übereinstimmung der Produkte mit digitalen Elementen mit den Anforderungen dieser Verordnung garantiert. ***Ein unvollständiges Produkt mit digitalen Elementen darf jedoch nicht mit der CE-Kennzeichnung gemäß dieser Verordnung versehen werden, unbeschadet der Kennzeichnungsvorschriften, die sich aus anderen geltenden Rechtsvorschriften der Union ergeben. Für unvollständige Produkte mit digitalen Elementen sollten***

**die Hersteller eine EU-Einbauerklärung erstellen.**

---

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

---

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

## Änderungsantrag 28

### Vorschlag für eine Verordnung Erwägung 45

#### *Vorschlag der Kommission*

(45) In der Regel **solte** die Konformitätsbewertung von Produkten mit digitalen Elementen vom Hersteller in eigener Verantwortung nach dem Verfahren auf der Grundlage von Modul A des Beschlusses Nr. 768/2008/EG durchgeführt werden. Der Hersteller sollte die Flexibilität behalten, ein strengeres Konformitätsbewertungsverfahren unter Einbeziehung eines Dritten zu wählen. Ist das Produkt als kritisches Produkt der Klasse I eingestuft, so ist eine zusätzliche Vertrauenswürdigkeitsprüfung erforderlich, um die Konformität mit den grundlegenden Anforderungen dieser Verordnung nachzuweisen. Der Hersteller sollte die von der Kommission in einem Durchführungsrechtsakt ausgewiesenen harmonisierten Normen, **gemeinsamen Spezifikationen** oder Systeme für die Cybersicherheitszertifizierung gemäß der Verordnung (EU) 2019/881 verwenden, wenn er die Konformitätsbewertung in eigener Verantwortung durchführen möchte (Modul A). Verwendet der Hersteller solche harmonisierten Normen, **gemeinsamen Spezifikationen** oder Systeme für die Cybersicherheitszertifizierung nicht, so sollte eine Konformitätsbewertung unter

#### *Geänderter Text*

(45) In der Regel **sollten die Anforderungen für** die Konformitätsbewertung von Produkten mit digitalen Elementen **risikobasiert sein; in diesem Zusammenhang könnte die Bewertung in vielen Fällen** vom Hersteller in eigener Verantwortung nach dem Verfahren auf der Grundlage von Modul A des Beschlusses Nr. 768/2008/EG durchgeführt werden. Der Hersteller sollte die Flexibilität behalten, ein strengeres Konformitätsbewertungsverfahren unter Einbeziehung eines Dritten zu wählen. Ist das Produkt als kritisches Produkt der Klasse I eingestuft, so ist eine zusätzliche Vertrauenswürdigkeitsprüfung erforderlich, um die Konformität mit den grundlegenden Anforderungen dieser Verordnung nachzuweisen. Der Hersteller sollte die von der Kommission in einem Durchführungsrechtsakt ausgewiesenen harmonisierten Normen oder Systeme für die Cybersicherheitszertifizierung gemäß der Verordnung (EU) 2019/881 verwenden, wenn er die Konformitätsbewertung in eigener Verantwortung durchführen möchte (Modul A). Verwendet der Hersteller solche harmonisierten Normen oder Systeme für die

Beteiligung eines Dritten durchgeführt werden. Unter Berücksichtigung des Verwaltungsaufwands für die Hersteller und der Tatsache, dass die Cybersicherheit in der Konzeptions- und Entwicklungsphase materieller und immaterieller Produkte mit digitalen Elementen eine wichtige Rolle spielt, wurden Konformitätsbewertungsverfahren auf der Grundlage der Module B und C oder des Moduls H des Beschlusses Nr. 768/2008/EG als am besten geeignet ausgewählt, um die Konformität kritischer Produkte mit digitalen Elementen auf verhältnismäßige und wirksame Weise zu bewerten. Der Hersteller, der die Konformitätsbewertung durch Dritte durchführen lässt, kann das Verfahren auswählen, das seinem Konzeptions- und Herstellungsprozess am besten entspricht. Angesichts des noch größeren Cybersicherheitsrisikos, das mit der Verwendung von Produkten verbunden ist, die als kritische Produkte der Klasse II eingestuft sind, sollte an deren Konformitätsbewertung stets ein Dritter beteiligt werden.

Cybersicherheitszertifizierung nicht, so sollte eine Konformitätsbewertung unter Beteiligung eines Dritten durchgeführt werden. Unter Berücksichtigung des Verwaltungsaufwands für die Hersteller und der Tatsache, dass die Cybersicherheit in der Konzeptions- und Entwicklungsphase materieller und immaterieller Produkte mit digitalen Elementen eine wichtige Rolle spielt, wurden Konformitätsbewertungsverfahren auf der Grundlage der Module B und C oder des Moduls H des Beschlusses Nr. 768/2008/EG als am besten geeignet ausgewählt, um die Konformität kritischer Produkte mit digitalen Elementen auf verhältnismäßige und wirksame Weise zu bewerten. Der Hersteller, der die Konformitätsbewertung durch Dritte durchführen lässt, kann das Verfahren auswählen, das seinem Konzeptions- und Herstellungsprozess am besten entspricht. Angesichts des noch größeren Cybersicherheitsrisikos, das mit der Verwendung von Produkten verbunden ist, die als kritische Produkte der Klasse II eingestuft sind, sollte an deren Konformitätsbewertung stets ein Dritter beteiligt werden.

## **Änderungsantrag 29**

### **Vorschlag für eine Verordnung Erwägung 46 a (neu)**

*Vorschlag der Kommission*

*Geänderter Text*

***(46a) Wenn Produkte mit digitalen Elementen gleichwertig sind, kann eines dieser Produkte für die Zwecke bestimmter Konformitätsbewertungsverfahren als repräsentativ für eine Produktfamilie oder -kategorie angesehen werden.***

## **Änderungsantrag 30**

## Vorschlag für eine Verordnung Erwägung 55

### *Vorschlag der Kommission*

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

### *Geänderter Text*

(55) Nach der Verordnung (EU) 2019/1020 führen die Marktüberwachungsbehörden die Marktüberwachung im Hoheitsgebiet des jeweiligen Mitgliedstaats durch. Die vorliegende Verordnung sollte die Mitgliedstaaten nicht daran hindern, zu entscheiden, welche Behörden für die Wahrnehmung dieser Aufgaben zuständig sind. Jeder Mitgliedstaat sollte in seinem Hoheitsgebiet eine oder mehrere Marktüberwachungsbehörden benennen. Die Mitgliedstaaten können beschließen, eine bestehende oder eine neue Behörde als Marktüberwachungsbehörde zu benennen, einschließlich der in Artikel *8 der Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates 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)* genannten zuständigen nationalen Behörden oder der in Artikel 58 der Verordnung (EU) 2019/881 genannten benannten nationalen Behörden für die Cybersicherheitszertifizierung. Die Wirtschaftsakteure sollten umfassend mit den Marktüberwachungsbehörden und anderen zuständigen Behörden zusammenarbeiten. Jeder Mitgliedstaat sollte die Kommission und die anderen Mitgliedstaaten über seine Marktüberwachungsbehörden und deren jeweilige Zuständigkeitsbereiche unterrichten und dafür sorgen, dass diese über die erforderlichen Ressourcen und Fähigkeiten für die Durchführung der Überwachungsaufgaben im Zusammenhang mit der vorliegenden Verordnung verfügen. Nach Artikel 10

Marktüberwachungsbehörden in verschiedenen Mitgliedstaaten zu unterstützen.

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.

## Änderungsantrag 31

### Vorschlag für eine Verordnung Erwägung 56 a (neu)

*Vorschlag der Kommission*

*Geänderter Text*

***(56a) Damit Wirtschaftsakteure, bei denen es sich um KMU oder Kleinstunternehmen handelt, in der Lage sind, mit den durch diese Verordnung auferlegten neuen Verpflichtungen umzugehen, sollte die Kommission ihnen leicht verständliche Leitlinien und Beratung zur Verfügung stellen, zum Beispiel über einen direkten Kanal, über den Sachverständige bei Fragen kontaktiert werden können, wobei zu berücksichtigen ist, dass Vereinfachungen erforderlich sind und der Verwaltungsaufwand begrenzt werden muss. Bei der Ausarbeitung solcher Leitlinien sollte die Kommission den Bedürfnissen der KMU Rechnung tragen, um die administrativen und finanziellen Belastungen auf ein Minimum zu beschränken und gleichzeitig die Einhaltung dieser Verordnung zu erleichtern. Die Kommission sollte die einschlägigen Interessenträger konsultieren, die Fachkenntnisse auf dem Gebiet der Cybersicherheit besitzen.***

## Änderungsantrag 32

## Vorschlag für eine Verordnung

### Erwägung 58

#### *Vorschlag der Kommission*

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

#### *Geänderter Text*

(58) In bestimmten Fällen kann ein Produkt mit digitalen Elementen, das dieser Verordnung entspricht, dennoch ein erhebliches Cybersicherheitsrisiko oder ein Risiko für die Gesundheit oder Sicherheit von Personen, für die Erfüllung der Pflichten aus dem Unionsrecht oder dem nationalen Recht zum Schutz der Grundrechte, für die Verfügbarkeit, Integrität oder Vertraulichkeit von Diensten, die über ein elektronisches Informationssystem von wesentlichen Einrichtungen der in *Anhang I der Richtlinie (EU) 2022/2555 (NIS-2-Richtlinie)* genannten Art angeboten werden, oder für andere Aspekte des Schutzes öffentlicher Interessen darstellen. Daher müssen Vorschriften festgelegt werden, die die Minderung solcher Risiken gewährleisten. Infolgedessen sollten die Marktüberwachungsbehörden Maßnahmen treffen, mit denen sie den Wirtschaftsakteur dazu verpflichten, in Abhängigkeit vom Risiko dafür zu sorgen, dass das Produkt dieses Risiko nicht mehr birgt, oder aber es zurückzurufen oder vom Markt zu nehmen. Sobald eine Marktüberwachungsbehörde den freien Verkehr eines Produkts auf diese Weise einschränkt bzw. untersagt, sollte der Mitgliedstaat die Kommission und die anderen Mitgliedstaaten unverzüglich unter Angabe von Gründen und Argumenten für die Entscheidung in Kenntnis setzen. Ergreift eine Marktüberwachungsbehörde solche Maßnahmen gegen Produkte, von denen ein Risiko ausgeht, so sollte die Kommission unverzüglich Konsultationen mit den Mitgliedstaaten und dem bzw. den betroffenen Wirtschaftsakteur(en) aufnehmen und die nationale Maßnahme bewerten. Anhand der Ergebnisse dieser Bewertung sollte die Kommission entscheiden, ob die nationale Maßnahme

gerechtfertigt ist oder nicht. Die Kommission sollte ihren Beschluss an alle Mitgliedstaaten richten und ihn diesen und dem bzw. den betroffenen Wirtschaftsakteur(en) unverzüglich mitteilen. Wird die Maßnahme als gerechtfertigt erachtet, kann die Kommission auch die Annahme von Vorschlägen zur Überarbeitung der betreffenden Rechtsvorschriften der Union in Erwägung ziehen.

gerechtfertigt ist oder nicht. Die Kommission sollte ihren Beschluss an alle Mitgliedstaaten richten und ihn diesen und dem bzw. den betroffenen Wirtschaftsakteur(en) unverzüglich mitteilen. Wird die Maßnahme als gerechtfertigt erachtet, kann die Kommission auch die Annahme von Vorschlägen zur Überarbeitung der betreffenden Rechtsvorschriften der Union in Erwägung ziehen.

### Änderungsantrag 33

#### Vorschlag für eine Verordnung Erwägung 59

##### *Vorschlag der Kommission*

(59) Bei Produkten mit digitalen Elementen, die ein erhebliches Cybersicherheitsrisiko bergen und bei denen Grund zu der Annahme besteht, dass sie dieser Verordnung nicht entsprechen, oder bei Produkten, die zwar dieser Verordnung entsprechen, aber andere große Risiken bergen, wie Risiken für die Gesundheit oder Sicherheit von Personen, die Grundrechte oder die Erbringung der Dienste von wesentlichen Einrichtungen der in **[Anhang I** der Richtlinie **XXX/XXXX (NIS2)**] genannten Art, kann die Kommission die ENISA ersuchen, eine Bewertung vorzunehmen. Auf der Grundlage dieser Bewertung kann die Kommission im Wege von Durchführungsrechtsakten Korrekturmaßnahmen oder einschränkende Maßnahmen auf Unionsebene erlassen, einschließlich der Anordnung der Rücknahme des betroffenen Produkts vom Markt oder seines Rückrufs innerhalb einer der Art des Risikos angemessenen Frist. Ein solches Eingreifen der Kommission ist nur unter außergewöhnlichen Umständen geboten, die ein sofortiges Eingreifen zur Bewahrung des reibungslosen Funktionierens des Binnenmarkts

##### *Geänderter Text*

(59) Bei Produkten mit digitalen Elementen, die ein erhebliches Cybersicherheitsrisiko bergen und bei denen Grund zu der Annahme besteht, dass sie dieser Verordnung nicht entsprechen, oder bei Produkten, die zwar dieser Verordnung entsprechen, aber andere große Risiken bergen, wie Risiken für die Gesundheit oder Sicherheit von Personen, die Grundrechte oder die Erbringung der Dienste von wesentlichen Einrichtungen der in **Anhang I** der Richtlinie **(EU) 2022/2555 (NIS-2-Richtlinie)** genannten Art, kann die Kommission die ENISA ersuchen, eine Bewertung vorzunehmen. Auf der Grundlage dieser Bewertung kann die Kommission im Wege von Durchführungsrechtsakten Korrekturmaßnahmen oder einschränkende Maßnahmen auf Unionsebene erlassen, einschließlich der Anordnung der Rücknahme des betroffenen Produkts vom Markt oder seines Rückrufs innerhalb einer der Art des Risikos angemessenen Frist. Ein solches Eingreifen der Kommission ist nur unter außergewöhnlichen Umständen geboten, die ein sofortiges Eingreifen zur Bewahrung des reibungslosen Funktionierens des Binnenmarkts

rechtfertigen, und nur dann, wenn die Überwachungsbehörden keine wirksamen Maßnahmen ergriffen haben, um Abhilfe zu schaffen. Solche außergewöhnlichen Umstände können Notfälle sein, in denen beispielsweise ein nichtkonformes Produkt vom Hersteller in mehreren Mitgliedstaaten in großem Umfang auf dem Markt bereitgestellt und auch in Schlüsselsektoren von Einrichtungen verwendet wird, die in den Anwendungsbereich der **[Richtlinie XXX/XXXX (NIS2)]** fallen, und es bekannte Schwachstellen aufweist, die von böswilligen Akteuren ausgenutzt werden und für die der Hersteller keine verfügbaren Patches bereitstellt. Die Kommission darf in solchen Notfällen nur während der Dauer der außergewöhnlichen Umstände und nur solange eingreifen, wie die Nichtkonformität mit dieser Verordnung oder die großen Risiken fortbestehen.

rechtfertigen, und nur dann, wenn die Überwachungsbehörden keine wirksamen Maßnahmen ergriffen haben, um Abhilfe zu schaffen. Solche außergewöhnlichen Umstände können Notfälle sein, in denen beispielsweise ein nichtkonformes Produkt vom Hersteller in mehreren Mitgliedstaaten in großem Umfang auf dem Markt bereitgestellt und auch in Schlüsselsektoren von Einrichtungen verwendet wird, die in den Anwendungsbereich der **Richtlinie (EU) 2022/2555 (NIS-2-Richtlinie)** fallen, und es bekannte Schwachstellen aufweist, die von böswilligen Akteuren ausgenutzt werden und für die der Hersteller keine verfügbaren Patches bereitstellt. Die Kommission darf in solchen Notfällen nur während der Dauer der außergewöhnlichen Umstände und nur solange eingreifen, wie die Nichtkonformität mit dieser Verordnung oder die großen Risiken fortbestehen.

## Änderungsantrag 34

### Vorschlag für eine Verordnung Erwägung 62

#### *Vorschlag der Kommission*

(62) Damit der Rechtsrahmen erforderlichenfalls angepasst werden kann, sollte der Kommission die Befugnis übertragen werden, gemäß Artikel 290 AEUV Rechtsakte zu erlassen, um die Liste kritischer Produkte in Anhang III zu aktualisieren und die Definitionen dieser Produktkategorien festzulegen. Der Kommission sollte die Befugnis übertragen werden, gemäß dem genannten Artikel Rechtsakte zu erlassen, um Produkte mit digitalen Elementen festzulegen, die unter andere Unionsvorschriften fallen, mit denen dasselbe Schutzniveau wie mit dieser Verordnung erreicht wird, und um festzustellen, ob eine Einschränkung oder ein Ausschluss vom Anwendungsbereich

#### *Geänderter Text*

(62) Damit der Rechtsrahmen erforderlichenfalls angepasst werden kann, sollte der Kommission die Befugnis übertragen werden, gemäß Artikel 290 AEUV Rechtsakte zu erlassen, um die Liste kritischer Produkte in Anhang III zu aktualisieren und die Definitionen dieser Produktkategorien festzulegen. Der Kommission sollte die Befugnis übertragen werden, gemäß dem genannten Artikel Rechtsakte zu erlassen, um Produkte mit digitalen Elementen festzulegen, die unter andere Unionsvorschriften fallen, mit denen dasselbe Schutzniveau wie mit dieser Verordnung erreicht wird, und um festzustellen, ob eine Einschränkung oder ein Ausschluss vom Anwendungsbereich

dieser Verordnung notwendig wäre, und gegebenenfalls den Umfang dieser Einschränkung festzulegen. Der Kommission sollte auch die Befugnis übertragen werden, gemäß dem genannten Artikel Rechtsakte zu erlassen, um möglicherweise die Zertifizierung bestimmter hochkritischer Produkte mit digitalen Elementen auf der Grundlage der in dieser Verordnung festgelegten Kritikalitätskriterien sowie die Mindestangaben für die EU-Konformitätserklärung und die Ergänzung der in die technische Dokumentation aufzunehmenden Elemente vorzuschreiben. Es ist von besonderer Bedeutung, dass die Kommission im Zuge ihrer Vorbereitungsarbeit angemessene Konsultationen, auch auf der Ebene von Sachverständigen, durchführt, die mit den Grundsätzen im Einklang stehen, die in der Interinstitutionellen Vereinbarung vom 13. April 2016 über bessere Rechtsetzung<sup>33</sup> niedergelegt wurden. Um insbesondere für eine gleichberechtigte Beteiligung an der Vorbereitung delegierter Rechtsakte zu sorgen, erhalten das Europäische Parlament und der Rat alle Dokumente zur gleichen Zeit wie die Sachverständigen der Mitgliedstaaten, und ihre Sachverständigen haben systematisch Zugang zu den Sitzungen der Sachverständigengruppen der Kommission, die mit der Vorbereitung der delegierten Rechtsakte befasst sind.

---

<sup>33</sup> ABl. L 123 vom 12.5.2016, S. 1.

## **Änderungsantrag 35**

### **Vorschlag für eine Verordnung Erwägung 63**

#### *Vorschlag der Kommission*

(63) Zur Gewährleistung einheitlicher Bedingungen für die Durchführung dieser Verordnung sollten der Kommission

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 möglicherweise die **freiwillige** Zertifizierung bestimmter hochkritischer Produkte mit digitalen Elementen auf der Grundlage der in dieser Verordnung festgelegten Kritikalitätskriterien sowie die Mindestangaben für die EU-Konformitätserklärung und die Ergänzung der in die technische Dokumentation aufzunehmenden Elemente vorzuschreiben. Es ist von besonderer Bedeutung, dass die Kommission im Zuge ihrer Vorbereitungsarbeit angemessene Konsultationen, auch auf der Ebene von Sachverständigen, durchführt, die mit den Grundsätzen im Einklang stehen, die in der Interinstitutionellen Vereinbarung vom 13. April 2016 über bessere Rechtsetzung<sup>33</sup> niedergelegt wurden. Um insbesondere für eine gleichberechtigte Beteiligung an der Vorbereitung delegierter Rechtsakte zu sorgen, erhalten das Europäische Parlament und der Rat alle Dokumente zur gleichen Zeit wie die Sachverständigen der Mitgliedstaaten, und ihre Sachverständigen haben systematisch Zugang zu den Sitzungen der Sachverständigengruppen der Kommission, die mit der Vorbereitung der delegierten Rechtsakte befasst sind.

---

<sup>33</sup> ABl. L 123 vom 12.5.2016, S. 1.

#### *Geänderter Text*

(63) Zur Gewährleistung einheitlicher Bedingungen für die Durchführung dieser Verordnung sollten der Kommission

Durchführungsbefugnisse in Bezug auf Folgendes übertragen werden: Festlegung des Formats und der Elemente der Software-Stückliste, Präzisierung der Art der Angaben, des Formats und des Verfahrens der Meldungen über aktiv ausgenutzte Schwachstellen und Sicherheitsvorfälle, die Hersteller der ENISA übermitteln, Ausweisung der nach der Verordnung (EU) 2019/881 angenommenen europäischen Systeme für die Cybersicherheitszertifizierung, die zum Nachweis der Konformität mit den grundlegenden Anforderungen in Anhang I dieser Verordnung oder Teilen davon verwendet werden können, Annahme gemeinsamer Spezifikationen für die grundlegenden Anforderungen in Anhang I, Festlegung technischer Spezifikationen für Piktogramme oder andere Kennzeichnungen in Bezug auf die Sicherheit von Produkten mit digitalen Elementen sowie Mechanismen zur Förderung ihrer Verwendung, Entscheidung über Korrekturmaßnahmen oder einschränkende Maßnahmen auf Unionsebene unter außergewöhnlichen Umständen, die ein sofortiges Eingreifen rechtfertigen, um das reibungslose Funktionieren des Binnenmarkts zu bewahren. Diese Befugnisse sollten im Einklang mit der Verordnung (EU) Nr. 182/2011 des Europäischen Parlaments und des Rates<sup>34</sup> ausgeübt werden.

---

<sup>34</sup> 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).

Durchführungsbefugnisse in Bezug auf Folgendes übertragen werden: Festlegung des Formats und der Elemente der Software-Stückliste, Präzisierung der Art der Angaben, des Formats und des Verfahrens der Meldungen über aktiv ausgenutzte Schwachstellen und Sicherheitsvorfälle, die Hersteller **auf der Grundlage der bewährten Verfahren der Branche** der ENISA übermitteln, Ausweisung der nach der Verordnung (EU) 2019/881 angenommenen europäischen Systeme für die Cybersicherheitszertifizierung, die zum Nachweis der Konformität mit den grundlegenden Anforderungen in Anhang I dieser Verordnung oder Teilen davon verwendet werden können, Annahme gemeinsamer Spezifikationen für die grundlegenden Anforderungen in Anhang I, Festlegung technischer Spezifikationen für Piktogramme oder andere Kennzeichnungen in Bezug auf die Sicherheit von Produkten mit digitalen Elementen sowie Mechanismen zur Förderung ihrer Verwendung, Entscheidung über Korrekturmaßnahmen oder einschränkende Maßnahmen auf Unionsebene unter außergewöhnlichen Umständen, die ein sofortiges Eingreifen rechtfertigen, um das reibungslose Funktionieren des Binnenmarkts zu bewahren. Diese Befugnisse sollten im Einklang mit der Verordnung (EU) Nr. 182/2011 des Europäischen Parlaments und des Rates<sup>34</sup> ausgeübt werden.

---

<sup>34</sup> 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).

## Änderungsantrag 36

### Vorschlag für eine Verordnung Erwägung 69

#### *Vorschlag der Kommission*

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

#### *Geänderter Text*

(69) Den Wirtschaftsakteuren sollte ausreichend Zeit für die Anpassung an die Anforderungen dieser Verordnung eingeräumt werden. Diese Verordnung sollte ab dem [36 Monate nach dem Datum ihres Inkrafttretens] gelten.

## Änderungsantrag 37

### Vorschlag für eine Verordnung Artikel 1 – Absatz 1 – Einleitung

#### *Vorschlag der Kommission*

**Mit dieser Verordnung wird Folgendes festgelegt:**

#### *Geänderter Text*

**Das Ziel der vorliegenden Verordnung besteht darin, die Funktionsweise des Binnenmarktes zu verbessern und zugleich für ein hohes Verbraucherschutzniveau und eine hohe Cybersicherheit zu sorgen.**

**Mit dieser Verordnung werden harmonisierte Vorschriften in Bezug auf Folgendes festgelegt:**

## Änderungsantrag 38

### Vorschlag für eine Verordnung Artikel 1 – Absatz 1 – Buchstabe a

#### *Vorschlag der Kommission*

a) **Vorschriften für** das Inverkehrbringen von Produkten mit digitalen Elementen, um die

#### *Geänderter Text*

a) das Inverkehrbringen von Produkten mit digitalen Elementen, um die Cybersicherheit solcher Produkte

Cybersicherheit solcher Produkte *zu gewährleisten*;

*sicherzustellen*;

### Änderungsantrag 39

#### Vorschlag für eine Verordnung Artikel 1 – Absatz 1 – Buchstabe d

*Vorschlag der Kommission*

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

*Geänderter Text*

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

### Änderungsantrag 40

#### Vorschlag für eine Verordnung Artikel 2 – Absatz 1

*Vorschlag der Kommission*

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

*Geänderter Text*

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

### Änderungsantrag 41

#### Vorschlag für eine Verordnung Artikel 2 – Absatz 5 a (neu)

*Vorschlag der Kommission*

*Geänderter Text*

*(5a) Diese Verordnung gilt nicht für freie und quelloffene Software, einschließlich ihres Quellcodes und ihrer modifizierten Versionen, es sei denn, diese Software wird im Rahmen einer kommerziellen Tätigkeit zur Verfügung gestellt, indem*

- i) ein Entgelt für ein Produkt erhoben wird;*
- ii) eine Softwareplattform bereitgestellt wird, die von anderen Diensten abhängt, die der Hersteller gegen eine Vergütung anbietet;*
- iii) die von der Software erzeugten personenbezogenen Daten zu anderen Zwecken als ausschließlich zur Verbesserung der Sicherheit, Kompatibilität oder Interoperabilität der Software verwendet werden;*
- iv) ein Entgelt für technische Unterstützungsdienste verlangt wird.*

*Die Konformität von freien und quelloffenen Produktkomponenten ist vom Hersteller des Produkts, in dem sie enthalten sind, sicherzustellen.*

## **Änderungsantrag 42**

### **Vorschlag für eine Verordnung Artikel 2 – Absatz 5 b (neu)**

*Vorschlag der Kommission*

*Geänderter Text*

*(5b) Diese Verordnung gilt nicht für interne Netze eines Produktes mit digitalen Elementen, wenn diese Netze über eigene Endpunkte verfügen, vollständig isoliert und vor externen Datenverbindungen geschützt sind.*

## **Änderungsantrag 43**

### **Vorschlag für eine Verordnung Artikel 2 – Absatz 5 c (neu)**

*Vorschlag der Kommission*

*Geänderter Text*

*(5c) Diese Verordnung gilt nicht für Ersatzteile, die ausschließlich dazu bestimmt sind, defekte Teile von Produkten mit digitalen Elemente zu ersetzen, um deren Funktionsfähigkeit*

*wiederherzustellen.*

#### **Änderungsantrag 44**

##### **Vorschlag für eine Verordnung Artikel 3 – Absatz 1 – Nummer 1**

*Vorschlag der Kommission*

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

*Geänderter Text*

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

#### **Änderungsantrag 45**

##### **Vorschlag für eine Verordnung Artikel 3 – Absatz 1 – Nummer 2**

*Vorschlag der Kommission*

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

*Geänderter Text*

**entfällt**

#### **Änderungsantrag 46**

##### **Vorschlag für eine Verordnung Artikel 3 – Absatz 1 – Nummer 6 a (neu)**

*Vorschlag der Kommission*

**6a. „quelloffene Software“ eine Software, die unter einer Lizenz vertrieben wird, die es den Nutzern erlaubt, sie frei auszuführen, zu kopieren, zu verbreiten, zu untersuchen, zu verändern und zu verbessern sowie sie als**

*Geänderter Text*

*Komponente in andere Produkte zu integrieren, sie als Dienstleistung anzubieten oder kommerzielle Unterstützung dafür zu leisten;*

#### **Änderungsantrag 47**

##### **Vorschlag für eine Verordnung Artikel 3 – Absatz 1 – Nummer 18**

*Vorschlag der Kommission*

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

*Geänderter Text*

*(Betrifft nicht die deutsche Fassung.)*

#### **Änderungsantrag 48**

##### **Vorschlag für eine Verordnung Artikel 3 – Absatz 1 – Nummer 19**

*Vorschlag der Kommission*

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

*Geänderter Text*

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

#### **Änderungsantrag 49**

##### **Vorschlag für eine Verordnung Artikel 3 – Absatz 1 – Nummer 23 a (neu)**

*Vorschlag der Kommission*

*Geänderter Text*

**23a. „Rückruf“ ein Rückruf im Sinne von Artikel 3 Nummer 22 der**

## Änderungsantrag 50

### Vorschlag für eine Verordnung Artikel 3 – Absatz 1 – Nummer 26

*Vorschlag der Kommission*

*Geänderter Text*

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

*entfällt*

## Änderungsantrag 51

### Vorschlag für eine Verordnung Artikel 3 – Absatz 1 – Nummer 31

*Vorschlag der Kommission*

*Geänderter Text*

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

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

## Änderungsantrag 52

### Vorschlag für eine Verordnung Artikel 3 – Absatz 1 – Nummer 39

*Vorschlag der Kommission*

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

*Geänderter Text*

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

**Änderungsantrag 53**

**Vorschlag für eine Verordnung  
Artikel 3 – Absatz 1 – Nummer 40 a (neu)**

*Vorschlag der Kommission*

*Geänderter Text*

**40a. „unvollständiges Produkt mit digitalen Elementen“ ein materieller Gegenstand, der nicht eigenständig funktionieren kann und nur zu dem Zweck hergestellt wird, in ein Produkt mit digitalen Elementen oder ein anderes unvollständiges Produkt mit digitalen Elementen eingebaut oder mit diesem zusammengefügt zu werden, und der nur unter Berücksichtigung der Art und Weise, wie er in ein vorgesehenes Endprodukt mit digitalen Elementen eingebaut wird, wirksam auf seine Konformität bewertet werden kann;**

**Änderungsantrag 54**

**Vorschlag für eine Verordnung  
Artikel 3 – Absatz 1 – Nummer 40 b (neu)**

*Vorschlag der Kommission*

*Geänderter Text*

**40b. „Lebenszyklus“ der Zeitraum vom Inverkehrbringen oder der Inbetriebnahme eines unter diese Verordnung fallenden Produkts bis zu seiner Entsorgung, einschließlich des Zeitraums, in dem es tatsächlich genutzt werden kann, und der Phasen des**

*Transports, des Zusammenbaus, der Demontage, der Außerbetriebnahme, der Verschrottung oder anderer vom Hersteller vorgesehener physischer oder digitaler Veränderungen.*

## Änderungsantrag 55

### Vorschlag für eine Verordnung Artikel 4 – Absatz 1

#### *Vorschlag der Kommission*

(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.

#### *Geänderter Text*

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

## Änderungsantrag 56

### Vorschlag für eine Verordnung Artikel 4 – Absatz 2

#### *Vorschlag der Kommission*

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

#### *Geänderter Text*

(2) Die Mitgliedstaaten ***dürfen*** die Präsentation und Verwendung eines Produkts mit digitalen Elementen, ***eines Prototyps eines Produkts mit digitalen Elementen oder eines unvollständigen Produkts mit digitalen Elementen***, das dieser Verordnung nicht entspricht, ***nicht*** bei Messen, Ausstellungen und Vorführungen oder ähnlichen Veranstaltungen ***untersagen, sofern das Produkt mit digitalen Elementen ausschließlich zu Präsentationszwecken im Rahmen der Veranstaltung verwendet wird und ein sichtbares Schild deutlich darauf hinweist, dass es dieser Verordnung nicht entspricht.***

## Änderungsantrag 57

### Vorschlag für eine Verordnung Artikel 4 – Absatz 3

#### *Vorschlag der Kommission*

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

#### *Geänderter Text*

(3) Die Mitgliedstaaten **dürfen** nicht die Bereitstellung **eines unvollständigen Produkts mit digitalen Elementen oder eines Prototyps eines Produkts mit digitalen Elementen, das** dieser Verordnung nicht entspricht, **untersagen**, sofern **es nur in einer nicht serienmäßigen Version zu Testzwecken bereitgestellt wird** und eine sichtbare Kennzeichnung deutlich darauf hinweist, dass **es** dieser Verordnung nicht entspricht und außer zu Testzwecken nicht auf dem Markt bereitgestellt wird.

## Änderungsantrag 58

### Vorschlag für eine Verordnung Artikel 4 – Absatz 3 a (neu)

#### *Vorschlag der Kommission*

#### *Geänderter Text*

**(3a) Diese Verordnung hindert die Mitgliedstaaten nicht daran, Produkte mit digitalen Elementen im Einklang mit den Rechtsvorschriften der Mitgliedstaaten oder der Union zusätzlichen Maßnahmen zu unterwerfen, wenn diese konkreten Produkte für militärische Zwecke, Verteidigungszwecke oder Zwecke der nationalen Sicherheit verwendet werden und diese Maßnahmen für die Erfüllung dieser Zwecke notwendig und angemessen sind.**

## Änderungsantrag 59

### Vorschlag für eine Verordnung Artikel 5 – Absatz 1 – Nummer 1

*Vorschlag der Kommission*

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

*Geänderter Text*

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

## **Änderungsantrag 60**

### **Vorschlag für eine Verordnung Artikel 6 – Absatz 1**

*Vorschlag der Kommission*

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

*Geänderter Text*

(1) Produkte mit digitalen Elementen, die zu einer in Anhang III aufgeführten Kategorie gehören, gelten als kritische Produkte mit digitalen Elementen. **Nur** Produkte, die die Kernfunktionen einer in Anhang III dieser Verordnung aufgeführten Kategorie aufweisen, gelten als Produkte, die unter diese Kategorie fallen. Die Kategorien kritischer Produkte mit digitalen Elementen werden gemäß Anhang III unter Berücksichtigung des mit diesen Produkten verbundenen Cybersicherheitsrisikos in die Klassen I und II unterteilt. **Die Integration einer Komponente einer höheren Kritikalitätsklasse in ein Produkt mit geringerer Kritikalität ändert nicht zwangsläufig die Kritikalität des Produkts, in das die Komponente integriert wird.**

## **Änderungsantrag 61**

### **Vorschlag für eine Verordnung Artikel 6 – Absatz 2 – Buchstabe b**

*Vorschlag der Kommission*

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

*Geänderter Text*

b) die bestimmungsgemäße Verwendung in **kritischen Anwendungen** in **sensiblen Umgebungen** oder durch wesentliche Einrichtungen der im Anhang [Anhang I] der Richtlinie [Richtlinie XXX/XXXX (NIS2)] genannten Art;

**Änderungsantrag 62**

**Vorschlag für eine Verordnung  
Artikel 6 – Absatz 2 – Buchstabe c**

*Vorschlag der Kommission*

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

*Geänderter Text*

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

**Änderungsantrag 63**

**Vorschlag für eine Verordnung  
Artikel 6 – Absatz 4**

*Vorschlag der Kommission*

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

*Geänderter Text*

(4) Kritische Produkte mit digitalen Elementen unterliegen den Konformitätsbewertungsverfahren nach Artikel 24 Absätze 2 und 3.  
***Kleinstunternehmen und kleine Unternehmen können ausnahmsweise das in Artikel 24 Absatz 2 genannte Verfahren anwenden.***

**Änderungsantrag 64**

**Vorschlag für eine Verordnung  
Artikel 6 – Absatz 5 – Einleitung**

*Vorschlag der Kommission*

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

*Geänderter Text*

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

**Änderungsantrag 65**

**Vorschlag für eine Verordnung  
Artikel 8 – Absatz 1**

*Vorschlag der Kommission*

(1) Produkte mit digitalen Elementen, die nach Artikel [Artikel 6] der Verordnung [KI-Verordnung] als Hochrisiko-KI-Systeme eingestuft sind, in den Anwendungsbereich der vorliegenden Verordnung fallen und die grundlegenden Anforderungen in Anhang I Abschnitt 1 der vorliegenden Verordnung erfüllen, gelten – sofern die vom Hersteller festgelegten Verfahren die grundlegenden Anforderungen in Anhang I Abschnitt 2 erfüllen – unbeschadet der anderen in dem genannten Artikel aufgeführten

*Geänderter Text*

(1) **Produkte mit digitalen Elementen oder unvollständige** Produkte mit digitalen Elementen, die nach Artikel [Artikel 6] der Verordnung [KI-Verordnung] als Hochrisiko-KI-Systeme eingestuft sind, in den Anwendungsbereich der vorliegenden Verordnung fallen und die grundlegenden Anforderungen in Anhang I Abschnitt 1 der vorliegenden Verordnung erfüllen, gelten – sofern die vom Hersteller festgelegten Verfahren die grundlegenden Anforderungen in Anhang I Abschnitt 2 erfüllen – unbeschadet der anderen in dem

Anforderungen in Bezug auf Genauigkeit und Robustheit als mit den Cybersicherheitsanforderungen gemäß Artikel [Artikel 15] der Verordnung [KI-Verordnung] konform, soweit das Erreichen des nach diesen Anforderungen erforderlichen Schutzniveaus durch die nach der vorliegenden Verordnung ausgestellte EU-Konformitätserklärung nachgewiesen wird.

genannten Artikel aufgeführten Anforderungen in Bezug auf Genauigkeit und Robustheit als mit den Cybersicherheitsanforderungen gemäß Artikel [Artikel 15] der Verordnung [KI-Verordnung] konform, soweit das Erreichen des nach diesen Anforderungen erforderlichen Schutzniveaus durch die nach der vorliegenden Verordnung ausgestellte EU-Konformitätserklärung nachgewiesen wird.

## Änderungsantrag 66

### Vorschlag für eine Verordnung Artikel 8 – Absatz 2

#### *Vorschlag der Kommission*

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

#### *Geänderter Text*

(2) Für die in Absatz 1 genannten Produkte und Cybersicherheitsanforderungen gilt das einschlägige Konformitätsbewertungsverfahren gemäß **den [geltenden Bestimmungen]** der Verordnung [KI-Verordnung]. Für die Zwecke dieser Bewertung sind die notifizierten Stellen, die gemäß der Verordnung [KI-Verordnung] berechtigt sind, die Konformität der Hochrisiko-KI-Systeme zu kontrollieren, auch berechtigt, im Rahmen der vorliegenden Verordnung die Konformität der Hochrisiko-KI-Systeme mit den Anforderungen in Anhang I der vorliegenden Verordnung zu kontrollieren.

## Änderungsantrag 67

### Vorschlag für eine Verordnung Artikel 8 – Absatz 3

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

**entfällt**

## Änderungsantrag 68

### Vorschlag für eine Verordnung Artikel 9 – Absatz 1

Maschinenprodukte, die in den Anwendungsbereich der Verordnung [Vorschlag für eine Maschinenverordnung] fallen, bei denen es sich um Produkte mit digitalen Elementen im Sinne der vorliegenden Verordnung handelt und für die auf der Grundlage der vorliegenden Verordnung eine EU-Konformitätserklärung ausgestellt wurde, gelten in Bezug auf den Schutz vor Korruption und die Sicherheit und Zuverlässigkeit von Steuerungssystemen als konform mit den grundlegenden Gesundheits- und

Maschinenprodukte, die in den Anwendungsbereich der Verordnung [Vorschlag für eine Maschinenverordnung] fallen, bei denen es sich um Produkte mit digitalen Elementen **oder unvollständige Produkte mit digitalen Elementen** im Sinne der vorliegenden Verordnung handelt und für die auf der Grundlage der vorliegenden Verordnung eine EU-Konformitätserklärung ausgestellt wurde, gelten in Bezug auf den Schutz vor Korruption und die Sicherheit und Zuverlässigkeit von Steuerungssystemen als konform mit den grundlegenden

Sicherheitsanforderungen in Anhang [Anhang III Abschnitte 1.1.9 und 1.2.1] der Verordnung [Vorschlag für eine Maschinenverordnung], sofern das Erreichen des nach diesen Anforderungen erforderlichen Schutzniveaus mit der nach der vorliegenden Verordnung ausgestellten EU-Konformitätserklärung nachgewiesen wird.

Gesundheits- und Sicherheitsanforderungen in Anhang [Anhang III Abschnitte 1.1.9 und 1.2.1] der Verordnung [Vorschlag für eine Maschinenverordnung], sofern das Erreichen des nach diesen Anforderungen erforderlichen Schutzniveaus mit der nach der vorliegenden Verordnung ausgestellten EU-Konformitätserklärung nachgewiesen wird.

## Änderungsantrag 69

### Vorschlag für eine Verordnung Artikel 10 – Absatz -1 (neu)

*Vorschlag der Kommission*

*Geänderter Text*

***(-1) Softwarehersteller, die als Kleinstunternehmen im Sinne der Empfehlung 2003/361/EG der Kommission gelten, bemühen sich nach besten Kräften, die Anforderungen dieser Verordnung innerhalb von sechs Monaten nach dem Inverkehrbringen einer Software zu erfüllen. Diese Bestimmung gilt jedoch nicht für hochkritische Produkte mit digitalen Elementen.***

## Änderungsantrag 70

### Vorschlag für eine Verordnung Artikel 10 – Absatz 1

*Vorschlag der Kommission*

*Geänderter Text*

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

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

## Änderungsantrag 71

### Vorschlag für eine Verordnung Artikel 10 – Absatz 4

#### *Vorschlag der Kommission*

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

#### *Geänderter Text*

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

## Änderungsantrag 72

### Vorschlag für eine Verordnung Artikel 10 – Absatz 4 a (neu)

#### *Vorschlag der Kommission*

#### *Geänderter Text*

**(4a) Die Komponentenhersteller stellen dem Hersteller der Endprodukte bei der Lieferung der Komponenten die Informationen und Unterlagen zur Verfügung, die zur Einhaltung der Anforderungen aus dieser Verordnung erforderlich sind. Die betreffenden Informationen werden kostenlos bereitgestellt.**

## Änderungsantrag 73

### Vorschlag für eine Verordnung Artikel 10 – Absatz 6 – Unterabsatz 1

#### *Vorschlag der Kommission*

#### *Geänderter Text*

**Wenn sie ein** Produkt mit digitalen Elementen **in Verkehr bringen** und während der erwarteten Produktlebensdauer oder während eines

**Beim Inverkehrbringen eines** Produkt mit digitalen Elementen und während der **zum Zeitpunkt des Inverkehrbringens** erwarteten Produktlebensdauer oder

Zeitraums von fünf Jahren ab dem Inverkehrbringen des Produkts, je nachdem, welcher Zeitraum **kürzer** ist, stellen die Hersteller sicher, dass Schwachstellen dieses Produkts wirksam und im Einklang mit den grundlegenden Anforderungen in Anhang I Abschnitt 2 behandelt werden.

während eines Zeitraums von fünf Jahren ab dem Inverkehrbringen des Produkts, je nachdem, welcher Zeitraum **länger** ist, stellen die Hersteller sicher, dass Schwachstellen dieses Produkts wirksam und im Einklang mit den grundlegenden Anforderungen in Anhang I Abschnitt 2 behandelt werden, **sofern dies in ihrer Macht steht**.

## Änderungsantrag 74

### Vorschlag für eine Verordnung Artikel 10 – Absatz 7 – Unterabsatz 3 a (neu)

*Vorschlag der Kommission*

*Geänderter Text*

***Werden Software-Aktualisierungen implementiert, ist der Hersteller nicht verpflichtet, eine weitere Konformitätsbewertung des Produkts mit digitalen Elementen durchzuführen, es sei denn, die Software-Aktualisierung führt zu einer wesentlichen Änderung des Produkts mit digitalen Elementen im Sinne von Artikel 3 Nummer 31 dieser Verordnung.***

## Änderungsantrag 75

### Vorschlag für eine Verordnung Artikel 10 – Absatz 9

*Vorschlag der Kommission*

*Geänderter Text*

(9) Die Hersteller gewährleisten durch geeignete Verfahren, dass die Konformität von Produkten mit digitalen Elementen bei einer Serienherstellung sichergestellt bleibt. Der Hersteller berücksichtigt in angemessener Weise etwaige Änderungen am Entwicklungs- und Herstellungsverfahren oder an der Konzeption oder den Merkmalen des Produkts mit digitalen Elementen sowie Änderungen der harmonisierten Normen,

(9) Die Hersteller gewährleisten durch geeignete Verfahren, dass die Konformität von Produkten mit digitalen Elementen bei einer Serienherstellung sichergestellt bleibt. Der Hersteller berücksichtigt in angemessener Weise etwaige Änderungen am Entwicklungs- und Herstellungsverfahren oder an der Konzeption oder den Merkmalen des Produkts mit digitalen Elementen sowie Änderungen der harmonisierten Normen,

der europäischen Systeme für die Cybersicherheitszertifizierung oder der in Artikel 19 genannten gemeinsamen Spezifikationen, die bei der Erklärung der Konformität des Produkts mit digitalen Elementen zugrunde gelegt oder bei der Überprüfung seiner Konformität angewandt wurden.

der europäischen Systeme für die Cybersicherheitszertifizierung oder der in Artikel 19 genannten gemeinsamen Spezifikationen, die bei der Erklärung der Konformität des Produkts mit digitalen Elementen zugrunde gelegt oder bei der Überprüfung seiner Konformität angewandt wurden. ***Wenn neue Erkenntnisse, Techniken oder Normen verfügbar werden, die zum Zeitpunkt der Konzeption eines Serienprodukts noch nicht verfügbar waren, kann der Hersteller in Betracht ziehen, diese Verbesserungen fortlaufend für künftige Produktgenerationen zu übernehmen.***

## Änderungsantrag 76

### Vorschlag für eine Verordnung Artikel 10 – Absatz 9 a (neu)

*Vorschlag der Kommission*

*Geänderter Text*

***(9a) Die Hersteller müssen die voraussichtliche Produktlebensdauer ihrer Produkte in klarer und verständlicher Form öffentlich mitteilen.***

## Änderungsantrag 77

### Vorschlag für eine Verordnung Artikel 10 – Absatz 12

*Vorschlag der Kommission*

*Geänderter Text*

(12) Ab dem Inverkehrbringen und während der erwarteten Produktlebensdauer oder während eines Zeitraums von fünf Jahren ab dem Inverkehrbringen eines Produkts mit digitalen Elementen, je nachdem, welcher Zeitraum ***kürzer*** ist, ergreifen die Hersteller, denen bekannt ist oder die Grund zu der Annahme haben, dass das Produkt mit digitalen Elementen oder die vom Hersteller festgelegten Verfahren den

(12) Ab dem Inverkehrbringen und während der erwarteten Produktlebensdauer oder während eines Zeitraums von fünf Jahren ab dem Inverkehrbringen eines Produkts mit digitalen Elementen, je nachdem, welcher Zeitraum ***länger*** ist, ergreifen die Hersteller, denen bekannt ist oder die Grund zu der Annahme haben, dass das Produkt mit digitalen Elementen oder die vom Hersteller festgelegten Verfahren den

grundlegenden Anforderungen in Anhang I nicht genügen, unverzüglich die erforderlichen Korrekturmaßnahmen, um die Konformität dieses Produkts mit digitalen Elementen oder der Prozesse des Herstellers herzustellen oder um gegebenenfalls das Produkt vom Markt zu nehmen oder zurückzurufen.

## Änderungsantrag 78

### Vorschlag für eine Verordnung Artikel 11 – Absatz 1

#### *Vorschlag der Kommission*

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

## Änderungsantrag 79

### Vorschlag für eine Verordnung Artikel 11 – Absatz 1 a (neu)

grundlegenden Anforderungen in Anhang I nicht genügen, unverzüglich die erforderlichen Korrekturmaßnahmen, um die Konformität dieses Produkts mit digitalen Elementen oder der Prozesse des Herstellers herzustellen oder um gegebenenfalls das Produkt vom Markt zu nehmen oder zurückzurufen.

#### *Geänderter Text*

(1) Der Hersteller meldet der ENISA **mittels einer Frühwarnung** unverzüglich, jedenfalls aber innerhalb von **48** Stunden, nachdem er davon Kenntnis erlangt hat, jede aktiv ausgenutzte Schwachstelle, die in dem Produkt mit digitalen Elementen enthalten ist.

*Vorschlag der Kommission*

*Geänderter Text*

**(1a) Nachdem der Hersteller Kenntnis von einer aktiv ausgenutzten Schwachstelle erlangt hat, die sich erheblich auf die Sicherheit des Produkts mit digitalen Elementen auswirkt, muss er der ENISA unverzüglich weitere Einzelheiten über die ausgenutzte Schwachstellen mitteilen.**

## **Änderungsantrag 80**

### **Vorschlag für eine Verordnung Artikel 11 – Absatz 1 b (neu)**

*Vorschlag der Kommission*

*Geänderter Text*

**(1b) Alle anderen Schwachstellen, die sich nicht wesentlich auf die Sicherheit des Produkts mit digitalen Elementen auswirken, müssen der ENISA gemeldet werden, sobald die Schwachstellen beseitigt wurden.**

## **Änderungsantrag 81**

### **Vorschlag für eine Verordnung Artikel 11 – Absatz 1 c (neu)**

*Vorschlag der Kommission*

*Geänderter Text*

**(1c) Die Meldung muss Einzelheiten zu dieser Schwachstelle und gegebenenfalls zu den ergriffenen Korrektur- oder Minderungsmaßnahmen sowie zu den empfohlenen Risikominderungsmaßnahmen enthalten. Sofern dem keine berechtigten Gründe in Bezug auf das Cybersicherheitsrisiko entgegenstehen, leitet die ENISA die Meldung nach dem Eingang unverzüglich an das für die Zwecke der koordinierten Offenlegung von Schwachstellen gemäß Artikel [Artikel X] der**

***Richtlinie [Richtlinie XXX/XXXX (NIS2)] benannte CSIRT der betreffenden Mitgliedstaaten weiter und unterrichtet umgehend die Marktüberwachungsbehörde über das Vorhandensein einer Schwachstelle und gegebenenfalls über die möglichen Risikominderungsmaßnahmen. Wenn für eine gemeldete Schwachstelle keine Korrektur- oder Abhilfemaßnahmen verfügbar sind, stellt die ENISA sicher, dass die Informationen über die gemeldete Schwachstelle unter Verwendung strenger Sicherheitsprotokolle und nach dem Grundsatz „Kenntnis nur, wenn nötig“ weitergegeben werden.***

## Änderungsantrag 82

### Vorschlag für eine Verordnung Artikel 11 – Absatz 2

#### *Vorschlag der Kommission*

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

#### *Geänderter Text*

(2) Der Hersteller meldet der ENISA unverzüglich, **in jedem Fall** aber innerhalb von 24 Stunden, nachdem er davon Kenntnis erlangt hat, **mittels einer Frühwarnung** jeden Vorfall, der sich **erheblich** auf die Sicherheit des Produkts mit digitalen Elementen auswirkt. **Der Hersteller teilt der ENISA unverzüglich, in jedem Fall aber innerhalb von 72 Stunden, nachdem er Kenntnis von einem Sicherheitsvorfall im Zusammenhang mit dem Produkt mit digitalen Elementen erlangt hat, weitere Einzelheiten zu dem erheblichen Sicherheitsvorfall mit.** Die ENISA leitet die Meldungen unverzüglich an die gemäß Artikel [Artikel X] der Richtlinie [Richtlinie XXX/XXXX (NIS2)] benannte zentrale Anlaufstelle der betroffenen Mitgliedstaaten weiter und unterrichtet **unverzüglich** die Marktüberwachungsbehörde von den gemeldeten **erheblichen**

oder ob er davon ausgeht, dass der Vorfall grenzüberschreitende Auswirkungen hat.

**Sicherheitsvorfällen**, sofern dem keine berechtigten Gründe in Bezug auf das Cybersicherheitsrisiko entgegenstehen. Die Meldung eines Vorfalls enthält Informationen, **die unbedingt erforderlich sind, um die zuständige Behörde von dem Vorfall in Kenntnis zu setzen, und, sofern dies relevant und dem Risiko angemessen ist, Angaben** über die Schwere und die Auswirkungen des Vorfalls und gegebenenfalls Angaben dazu, ob der Hersteller den Verdacht hat, dass der Vorfall durch rechtswidrige oder böswillige Handlungen verursacht wurde, oder ob er davon ausgeht, dass der Vorfall grenzüberschreitende Auswirkungen hat. **Die bloße Meldung begründet keine höhere Haftung des meldenden Unternehmens.**

### Änderungsantrag 83

#### Vorschlag für eine Verordnung Artikel 11 – Absatz 2 a (neu)

*Vorschlag der Kommission*

*Geänderter Text*

**(2a) Bei Wirtschaftsakteuren, die auch als wesentliche Einrichtungen oder wichtige Einrichtungen im Sinne der NIS-2-Richtlinie eingestuft werden und ihre Meldung von Vorfällen gemäß der NIS-2-Richtlinie übermitteln, sollte davon ausgegangen werden, dass sie die Anforderungen nach Absatz 2 dieses Artikels erfüllen.**

### Änderungsantrag 84

#### Vorschlag für eine Verordnung Artikel 11 – Absatz 3

*Vorschlag der Kommission*

*Geänderter Text*

(3) Die ENISA übermittelt dem Europäischen Netzwerk der

(3) Die ENISA übermittelt dem Europäischen Netzwerk der

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

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

## Änderungsantrag 85

### Vorschlag für eine Verordnung Artikel 11 – Absatz 4

#### *Vorschlag der Kommission*

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

#### *Geänderter Text*

(4) Der Hersteller informiert die Nutzer des Produkts mit digitalen Elementen unverzüglich, nachdem er Kenntnis davon erlangt hat, **gegebenenfalls** über den **erheblichen** Vorfall, **sofern sie davon wahrscheinlich nachteilig davon berührt werden**, und erforderlichenfalls über **Risikominderungs- und** Korrekturmaßnahmen, die der Nutzer ergreifen kann, um die Auswirkungen des **erheblichen Vorfalls in Bezug auf die möglicherweise betroffenen Daten und den potenziellen Schaden** zu **verringern**.

## Änderungsantrag 86

### Vorschlag für eine Verordnung Artikel 11 – Absatz 4 a (neu)

#### *Vorschlag der Kommission*

#### *Geänderter Text*

**(4a) Die in den Absätzen 1, 2 und 4 festgelegten Verpflichtungen gelten während der Lebensdauer des Produkts. Während der erwarteten Lebensdauer des Produkts stellt der Hersteller kostenlos Sicherheitsaktualisierungen zur**

**Verfügung, die nur für Produkte mit digitalen Elementen gelten, für die der Hersteller eine EU-Konformitätserklärung gemäß Artikel 20 dieser Verordnung ausgestellt hat.**

## Änderungsantrag 87

### Vorschlag für eine Verordnung Artikel 11 – Absatz 5

#### *Vorschlag der Kommission*

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

#### *Geänderter Text*

(5) **Nachdem** die Kommission **Interessenträger und die Computer-Notfallteams (CSIRT) konsultiert hat**, kann **sie** im Wege von Durchführungsrechtsakten die Art der Angaben sowie das Format und Verfahren für die nach den Absätzen 1 und 2 übermittelten Meldungen präzisieren. Diese Durchführungsrechtsakte **stützen sich auf europäische und internationale Normen und** werden gemäß dem in Artikel 51 Absatz 2 genannten Prüfverfahren erlassen.

## Änderungsantrag 88

### Vorschlag für eine Verordnung Artikel 11 – Absatz 6

#### *Vorschlag der Kommission*

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

#### *Geänderter Text*

(6) Die ENISA erstellt auf der Grundlage der nach den Absätzen 1 und 2 eingegangenen Meldungen alle zwei Jahre einen technischen Bericht über aufkommende Trends der Cybersicherheitsrisiken bei Produkten mit digitalen Elementen und legt ihn der in Artikel **14** der Richtlinie **(EU) 2022/2555** genannten Kooperationsgruppe vor. Der erste solche Bericht wird innerhalb von 24 Monaten nach Beginn der Geltung der in den Absätzen 1 und 2 festgelegten

in den Absätzen 1 und 2 festgelegten Pflichten vorgelegt.

Pflichten vorgelegt.

## Änderungsantrag 89

### Vorschlag für eine Verordnung Artikel 11 – Absatz 7

#### *Vorschlag der Kommission*

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

#### *Geänderter Text*

(7) Sobald der Hersteller eine Schwachstelle in einer in das Produkt mit digitalen Elementen integrierten Komponente, einschließlich einer **quelloffenen Komponente**, feststellt, meldet er die Schwachstelle **und die ergriffenen Korrektur- oder Minderungsmaßnahmen** der Person oder Einrichtung, die diese Komponente wartet. **Dies entbindet weder den Hersteller von der Verpflichtung, die Konformität des Produkts mit den Anforderungen dieser Verordnung aufrechtzuerhalten, noch entstehen dadurch Verpflichtungen für die Entwickler von Komponenten mit freiem und offenem Quellcode, die in keiner vertraglichen Beziehung zu dem genannten Hersteller stehen.**

## Änderungsantrag 90

### Vorschlag für eine Verordnung Artikel 12 – Absatz 3 – Einleitung

#### *Vorschlag der Kommission*

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

#### *Geänderter Text*

(3) Ein Bevollmächtigter nimmt die Aufgaben wahr, die in dem vom Hersteller erteilten Auftrag festgelegt sind. **Er stellt den Marktüberwachungsbehörden auf Anfrage eine Kopie des Auftrags zur Verfügung.** Der Auftrag muss es dem Bevollmächtigten ermöglichen, mindestens folgende Aufgaben wahrzunehmen:

## Änderungsantrag 91

### Vorschlag für eine Verordnung Artikel 12 – Absatz 3 – Buchstabe a a (neu)

*Vorschlag der Kommission*

*Geänderter Text*

**aa) Unterrichtung des Herstellers, wenn der Bevollmächtigte Grund zu der Annahme hat, dass ein Produkt mit digitalen Elementen ein Cybersicherheitsrisiko darstellt;**

## Änderungsantrag 92

### Vorschlag für eine Verordnung Artikel 12 – Absatz 3 – Buchstabe b

*Vorschlag der Kommission*

*Geänderter Text*

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

b) Übermittlung aller zum Nachweis der **Sicherheit und der** Konformität des Produkts mit digitalen Elementen erforderlichen Informationen und Unterlagen an eine Marktüberwachungsbehörde auf deren begründetes Verlangen **und in einer Sprache, die für diese Behörde leicht verständlich ist;**

## Änderungsantrag 93

### Vorschlag für eine Verordnung Artikel 12 – Absatz 3 – Buchstabe c

*Vorschlag der Kommission*

*Geänderter Text*

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.

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

## Änderungsantrag 94

### Vorschlag für eine Verordnung Artikel 13 – Absatz 2 – Buchstabe c a (neu)

*Vorschlag der Kommission*

*Geänderter Text*

**ca) der Hersteller alle Dokumente, durch die die Erfüllung der in diesem Artikel genannten Anforderungen belegt wird, erhalten hat und dass sie zur Überprüfung während eines Zeitraums von zehn Jahren verfügbar sind.**

## Änderungsantrag 95

### Vorschlag für eine Verordnung Artikel 13 – Absatz 3

*Vorschlag der Kommission*

*Geänderter Text*

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

(3) Ist ein Einführer **aufgrund der ihm vorliegenden Informationen** der Auffassung oder hat er **aufgrund dieser Informationen** Grund zu der Annahme, dass ein Produkt mit digitalen Elementen oder die vom Hersteller festgelegten Verfahren den grundlegenden Anforderungen in Anhang I nicht genügen, bringt er das Produkt erst dann in Verkehr, wenn die Konformität dieses Produkts und der vom Hersteller festgelegten Verfahren mit den grundlegenden Anforderungen in Anhang I hergestellt ist. Wenn das Produkt mit digitalen Elementen ein erhebliches Cybersicherheitsrisiko birgt, unterrichtet der Einführer zudem den Hersteller und die Marktüberwachungsbehörden hiervon.

## Änderungsantrag 96

### Vorschlag für eine Verordnung Artikel 13 – Absatz 4

*Vorschlag der Kommission*

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

*Geänderter Text*

*(Betrifft nicht die deutsche Fassung.)*

**Änderungsantrag 97**

**Vorschlag für eine Verordnung  
Artikel 13 – Absatz 6 – Unterabsatz 1**

*Vorschlag der Kommission*

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

*Geänderter Text*

Einführer, denen bekannt ist oder die Grund zu der Annahme haben, dass ein Produkt mit digitalen Elementen, das sie in Verkehr gebracht haben, oder die von dessen Hersteller festgelegten Verfahren den grundlegenden Anforderungen in Anhang I nicht genügen, ergreifen unverzüglich die erforderlichen Korrekturmaßnahmen, um die Konformität dieses Produkts mit digitalen Elementen und der vom Hersteller festgelegten Verfahren mit den grundlegenden Anforderungen in Anhang I herzustellen oder um gegebenenfalls das Produkt vom Markt zu nehmen oder zurückzurufen. ***Auf der Grundlage einer Risikobewertung werden die Händler und Endnutzer rechtzeitig darüber informiert, welche Maßnahmen sie bei Nichteinhaltung der Verpflichtungen und welche Maßnahmen sie zur Risikominderung ergreifen können.***

## Änderungsantrag 98

### Vorschlag für eine Verordnung Artikel 14 – Absatz 2 – Buchstabe b a (neu)

*Vorschlag der Kommission*

*Geänderter Text*

**ba) sie vom Hersteller oder Einführer alle gemäß dieser Verordnung erforderlichen Informationen und Dokumente erhalten haben.**

## Änderungsantrag 99

### Vorschlag für eine Verordnung Artikel 16 – Absatz 1

*Vorschlag der Kommission*

*Geänderter Text*

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

Eine natürliche oder juristische Person, bei der es sich nicht um den Hersteller, Einführer oder Händler handelt und die **im Rahmen ihrer beruflichen Tätigkeit** eine wesentliche Änderung an dem Produkt mit digitalen Elementen vornimmt **und das Produkt auf dem Markt bereitstellt**, gilt für die Zwecke dieser Verordnung als Hersteller.

## Änderungsantrag 100

### Vorschlag für eine Verordnung Artikel 18 – Absatz 1 a (neu)

*Vorschlag der Kommission*

*Geänderter Text*

**(1a) Die Kommission fordert eine oder mehrere Normungsorganisationen gemäß Artikel 10 Absatz 1 der Verordnung (EU) Nr. 1025/2012 auf, für die in Anhang I festgelegten Anforderungen Entwürfe für harmonisierte Normen auszuarbeiten.**

## Änderungsantrag 101

### Vorschlag für eine Verordnung Artikel 18 – Absatz 4 a (neu)

*Vorschlag der Kommission*

*Geänderter Text*

**(4a) In Übereinstimmung mit Artikel 10 Absatz 1 der Verordnung (EU) Nr. 1025/2012 strebt die Kommission bei der Ausarbeitung des Normungsantrags für Produkte im Anwendungsbereich dieser Verordnung eine höchstmögliche Harmonisierung mit bereits bestehenden oder demnächst geltenden internationaler Normen für Cybersicherheit an. In den ersten drei Jahren nach dem Geltungsbeginn dieser Verordnung ist die Kommission befugt, eine bestehende internationale Norm als gleichwertig zu den Anforderungen dieser Verordnung zu erklären, ohne dass sie auf europäischer Ebene geändert wird, sofern die Sicherheit der Produkte mit digitalen Elementen durch die Einhaltung solcher Normen hinreichend erhöht wird und die Norm von einer der europäischen Normungsorganisationen als separate Version veröffentlicht wird.**

## Änderungsantrag 102

### Vorschlag für eine Verordnung Artikel 19 – Absatz 1

*Vorschlag der Kommission*

*Geänderter Text*

**Gibt es keine harmonisierten Normen gemäß Artikel 18 oder ist die Kommission der Auffassung, dass die einschlägigen harmonisierten Normen nicht ausreichen, um die Anforderungen dieser Verordnung zu erfüllen oder dem Normungsauftrag der Kommission gerecht zu werden, oder treten unangemessene Verzögerungen im Normungsverfahren auf oder wird der Auftrag der Kommission zur Ausarbeitung harmonisierter Normen von**

**(1) Die Kommission kann Durchführungsrechtsakte annehmen, durch die gemeinsame Spezifikationen zu technischen Anforderungen festgelegt werden, deren Befolgung es ermöglicht, die in Anhang I für Produkte im Anwendungsbereich dieser Verordnung festgelegten wesentlichen Sicherheits- und Gesundheitsanforderungen zu erfüllen. Diese Durchführungsrechtsakte werden nur erlassen, wenn die folgenden**

*den europäischen Normungsorganisationen nicht angenommen, so wird der Kommission die Befugnis übertragen, im Wege von Durchführungsrechtsakten gemeinsame Spezifikationen für die grundlegenden Anforderungen in Anhang I anzunehmen. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 51 Absatz 2 genannten Prüfverfahren erlassen.*

*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 Anforderungen zu erarbeiten, und:*

- i) der Antrag wurde nicht angenommen oder*
- 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 genügen nicht dem Antrag; und*

*b) im Amtsblatt der Europäischen Union wurde kein Verweis im Einklang mit der Verordnung (EU) Nr. 1025/2012 auf harmonisierte Normen, die den Anforderungen nach Anhang I 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 48 Absatz 3 genannten Prüfverfahren erlassen.*

**Änderungsantrag 103**

**Vorschlag für eine Verordnung  
Artikel 19 – Absatz 1 a (neu)**

*Vorschlag der Kommission*

*Geänderter Text*

**(1a) Vor der Ausarbeitung eines Entwurfs des in Absatz 3 genannten Durchführungsrechtsakts teilt die Kommission dem in Artikel 22 der Verordnung (EU) Nr. 1025/2012 genannten Ausschuss mit, dass sie die Bedingungen nach Absatz 3 als erfüllt erachtet.**

**Änderungsantrag 104**

**Vorschlag für eine Verordnung  
Artikel 19 – Absatz 1 b (neu)**

*Vorschlag der Kommission*

*Geänderter Text*

**(1b) Bei der Ausarbeitung eines Entwurfs des in Absatz 1 genannten Durchführungsrechtsakt berücksichtigt die Kommission die Standpunkte der einschlägigen Gremien bzw. Sachverständigengruppe und konsultiert alle einschlägigen Interessenträger ordnungsgemäß.**

**Änderungsantrag 105**

**Vorschlag für eine Verordnung  
Artikel 19 – Absatz 1 c (neu)**

*Vorschlag der Kommission*

*Geänderter Text*

**(1c) Wenn eine harmonisierte Norm von einer europäischen Normungsorganisation angenommen und der Kommission zum Zwecke der Veröffentlichung des Normverweises im Amtsblatt der Europäischen Union vorgeschlagen wird, bewertet die Kommission die harmonisierte Norm in Übereinstimmung mit Verordnung**

*(EU) Nr. 1025/2012. Wenn ein Verweis auf eine harmonisierte Norm im Amtsblatt der Europäischen Union der Europäischen Union veröffentlicht wird, hebt die Kommission die in Absatz 1 genannten Durchführungsrechtsakte oder Teile davon auf, die dieselben Anforderungen wie die harmonisierte Norm regeln.*

## Änderungsantrag 106

### Vorschlag für eine Verordnung Artikel 19 – Absatz 1 d (neu)

*Vorschlag der Kommission*

*Geänderter Text*

*(1d) Ist ein Mitgliedstaat der Auffassung, dass eine gemeinsame Spezifikation den Anforderungen nach Anhang I nicht vollständig entspricht, so setzt er die Kommission mittels einer ausführlichen Erläuterung davon in Kenntnis. Die Kommission beurteilt diese ausführliche Erläuterung und kann gegebenenfalls den Durchführungsrechtsakt, durch den die betreffende gemeinsame Spezifikation festgelegt wurde, ändern.*

## Änderungsantrag 107

### Vorschlag für eine Verordnung Artikel 20 – Absatz 2

*Vorschlag der Kommission*

*Geänderter Text*

(2) Die EU-Konformitätserklärung entspricht in ihrem Aufbau dem Muster in Anhang IV und enthält die in den einschlägigen Konformitätsbewertungsverfahren gemäß Anhang VI angegebenen Elemente. Eine solche Erklärung wird *laufend* aktualisiert. Sie wird in *der* Sprache *bzw. den Sprachen* abgefasst, die *der Mitgliedstaat*

(2) Die EU-Konformitätserklärung entspricht in ihrem Aufbau dem Muster in Anhang IV und enthält die in den einschlägigen Konformitätsbewertungsverfahren gemäß Anhang VI angegebenen Elemente. Eine solche Erklärung wird – *soweit erforderlich* – aktualisiert. Sie wird in *einer* Sprache abgefasst, die *für die*

*vorschreibt*, in dem das Produkt mit digitalen Elementen in Verkehr gebracht oder auf dem Markt bereitgestellt wird.

*Behörden des Mitgliedstaats*, in dem das Produkt mit digitalen Elementen in Verkehr gebracht oder auf dem Markt bereitgestellt wird, *leicht verständlich ist*.

## Änderungsantrag 108

### Vorschlag für eine Verordnung Artikel 20 a (neu)

*Vorschlag der Kommission*

*Geänderter Text*

#### *Artikel 20a*

##### *EU-Einbauerklärung für unvollständige Produkte mit digitalen Elementen*

- (1) Die EU-Einbauerklärung wird vom Hersteller gemäß Artikel 10 Absatz 7 ausgestellt und besagt, dass die Erfüllung der in Anhang I festgelegten grundlegenden Anforderungen nachgewiesen wurde.*
- (2) Die EU-Einbauerklärung entspricht in ihrem Aufbau dem Muster in Anhang IVa (neu). Soweit erforderlich wird eine solche Erklärung aktualisiert. Sie wird in der Sprache bzw. den Sprachen abgefasst, die der Mitgliedstaat vorschreibt, in dem das unvollständige Produkt mit digitalen Elementen in Verkehr gebracht oder bereitgestellt wird.*
- (3) Wenn das unvollständige Produkt mit digitalen Elementen einem oder mehreren Rechtsakten der Union unterliegt und eine EU-Einbauerklärung erforderlich ist, wird für alle diese Rechtsakte eine einzige EU-Einbauerklärung erstellt. In dieser Erklärung werden die betreffenden Rechtsvorschriften der Union samt ihren Fundstellen im Amtsblatt angegeben.*
- (4) Der Kommission wird die Befugnis übertragen, delegierte Rechtsakte gemäß Artikel 50 zu erlassen, um diese Verordnung durch das Hinzufügen von*

*Aspekten zum Mindestinhalt der EU-Einbauerklärung gemäß Anhang IVa (neu) zu ergänzen, um technologischen Entwicklungen Rechnung zu tragen.*

## Änderungsantrag 109

### Vorschlag für eine Verordnung Artikel 22 – Absatz 1

#### *Vorschlag der Kommission*

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

#### *Geänderter Text*

(1) Die CE-Kennzeichnung ist gut sichtbar, leserlich und dauerhaft auf dem Produkt mit digitalen Elementen anzubringen. Falls die Art des Produkts mit digitalen Elementen dies nicht zulässt oder nicht rechtfertigt, wird die CE-Kennzeichnung auf der Verpackung und der dem Produkt mit digitalen Elementen beigefügten EU-Konformitätserklärung gemäß Artikel 20 angebracht. Bei Produkten mit digitalen Elementen in Form von Software wird die CE-Kennzeichnung entweder auf der EU-Konformitätserklärung gemäß Artikel 20 oder auf der das Softwareprodukt begleitenden Website angebracht. ***Im letzteren Fall muss der relevante Abschnitt der Website für Verbraucher einfach verständlich und direkt zugänglich sein.***

## Änderungsantrag 110

### Vorschlag für eine Verordnung Artikel 22 – Absatz 3

#### *Vorschlag der Kommission*

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

#### *Geänderter Text*

(3) Die CE-Kennzeichnung wird vor dem Inverkehrbringen des Produkts mit digitalen Elementen angebracht. Ihr kann ein Piktogramm oder ein anderes Zeichen folgen, das ***die Verbraucher*** auf ein besonderes Risiko oder eine besondere

in Durchführungsrechtsakten gemäß Absatz 6 festgelegt werden.

Verwendung hinweist, die in Durchführungsrechtsakten gemäß Absatz 6 festgelegt werden.

## Änderungsantrag 111

### Vorschlag für eine Verordnung Artikel 22 – Absatz 5

#### *Vorschlag der Kommission*

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

#### *Geänderter Text*

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

## Änderungsantrag 112

### Vorschlag für eine Verordnung Artikel 22 – Absatz 6

#### *Vorschlag der Kommission*

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

#### *Geänderter Text*

(6) Die Kommission kann im Wege von **delegierten Rechtsakten** technische Spezifikationen für **Etikettierungssysteme, einschließlich harmonisierter Etiketten**, Piktogramme oder andere Kennzeichen in Bezug auf die Sicherheit von Produkten mit digitalen Elementen sowie Mechanismen zur Förderung ihrer Verwendung **durch Unternehmen und Verbraucher und zur Sensibilisierung der Öffentlichkeit für die Sicherheit von**

**Produkten mit digitalen Elementen** festlegen. Diese *delegierten Rechtsakte* werden gemäß dem in Artikel 50 genannten *Verfahren* erlassen.

## **Änderungsantrag 113**

### **Vorschlag für eine Verordnung Artikel 22 – Absatz 6 a (neu)**

*Vorschlag der Kommission*

*Geänderter Text*

**(6a) Ein unvollständiges Produkt mit digitalen Elementen wird unbeschadet der Kennzeichnungsvorschriften, die sich aus anderen geltenden Rechtsvorschriften der Union ergeben, nicht mit der CE-Kennzeichnung gemäß dieser Verordnung versehen.**

## **Änderungsantrag 114**

### **Vorschlag für eine Verordnung Artikel 22 – Absatz 6 b (neu)**

*Vorschlag der Kommission*

*Geänderter Text*

**(6b) Die Kommission nimmt Leitlinien an und berät Wirtschaftsakteure – insbesondere solchen, die als KMU oder Kleinstunternehmen einzustufen sind – zur Durchführung dieser Verordnung. Die Leitlinien und Ratschläge zielen insbesondere darauf ab, den Verwaltungsaufwand und die finanzielle Belastung zu vereinfachen und zu begrenzen und gleichzeitig eine wirksame und kohärente Anwendung der vorliegenden Verordnung im Einklang mit dem allgemeinen Ziel der Gewährleistung der Produktsicherheit und des Verbraucherschutzes sicherzustellen. Die Kommission sollte die einschlägigen Interessenträger konsultieren, die Fachkenntnisse auf dem Gebiet der Cybersicherheit besitzen.**

## Änderungsantrag 115

### Vorschlag für eine Verordnung Artikel 23 – Absatz 2

#### *Vorschlag der Kommission*

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

#### *Geänderter Text*

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

## Änderungsantrag 116

### Vorschlag für eine Verordnung Artikel 23 – Absatz 3

#### *Vorschlag der Kommission*

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

#### *Geänderter Text*

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

## Änderungsantrag 117

### Vorschlag für eine Verordnung Artikel 23 – Absatz 5

#### *Vorschlag der Kommission*

(5) Der Kommission wird die Befugnis übertragen, gemäß Artikel 50 delegierte Rechtsakte zu erlassen, mit denen diese Verordnung um die Elemente ergänzt wird,

#### *Geänderter Text*

(5) Der Kommission wird die Befugnis übertragen, gemäß Artikel 50 delegierte Rechtsakte zu erlassen, mit denen diese Verordnung um die Elemente ergänzt wird,

die in die technische Dokumentation gemäß Anhang V aufzunehmen sind, um den technischen Entwicklungen und den Entwicklungen bei der Durchführung dieser Verordnung Rechnung zu tragen.

die in die technische Dokumentation gemäß Anhang V aufzunehmen sind, um den technischen Entwicklungen und den Entwicklungen bei der Durchführung dieser Verordnung Rechnung zu tragen.

***Die Kommission bemüht sich, den Verwaltungsaufwand insbesondere für Kleinstunternehmen sowie kleine und mittlere Unternehmen so gering wie möglich zu halten.***

## **Änderungsantrag 118**

### **Vorschlag für eine Verordnung Artikel 24 – Absatz 1 – Buchstabe c a (neu)**

*Vorschlag der Kommission*

*Geänderter Text*

***ca) Erstellung eines europäischen Schemas für die Cybersicherheitszertifizierung, angenommen gemäß Artikel 18 Absatz 4 der Verordnung (EU) 2019/881,***

## **Änderungsantrag 119**

### **Vorschlag für eine Verordnung Artikel 24 – Absatz 3 – Buchstabe b**

*Vorschlag der Kommission*

*Geänderter Text*

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

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

## **Änderungsantrag 120**

### **Vorschlag für eine Verordnung Artikel 24 – Absatz 3 – Buchstabe b a (neu)**

*Vorschlag der Kommission*

*Geänderter Text*

***ba) gegebenenfalls Erstellung eines europäischen Schemas für die***

## **Änderungsantrag 121**

### **Vorschlag für eine Verordnung Artikel 24 – Absatz 4 a (neu)**

*Vorschlag der Kommission*

*Geänderter Text*

***(4a) Für Produkte, für die die harmonisierten Rechtsvorschriften der Union auf der Grundlage des neuen Rechtsrahmens gelten, muss der Hersteller die in diesen Rechtsakten geforderte Konformitätsbewertung durchführen. Für diese Produkte gelten die in Kapitel III aufgeführten Anforderungen.***

## **Änderungsantrag 122**

### **Vorschlag für eine Verordnung Artikel 24 – Absatz 5**

*Vorschlag der Kommission*

*Geänderter Text*

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

(5) Die notifizierte Stellen berücksichtigen bei der Festsetzung der Gebühren für die Konformitätsbewertung die besonderen Interessen und Bedürfnisse von Kleinunternehmen sowie kleinen und mittleren Unternehmen und senken diese Gebühren proportional zu deren besonderen Interessen und Bedürfnissen. ***Die Kommission ergreift Maßnahmen, um für zugänglichere und erschwinglichere Verfahren zu sorgen und eine angemessene finanzielle Unterstützung im Rahmen bestehender Unionsprogramme sicherzustellen, damit insbesondere die Belastung von Kleinunternehmen sowie kleinen und mittleren Unternehmen verringert wird.***

## **Änderungsantrag 123**

### **Vorschlag für eine Verordnung Artikel 24 – Absatz 5 a (neu)**

*Vorschlag der Kommission*

*Geänderter Text*

**(5a) Bei Produkten mit digitalen Elementen, die in den Anwendungsbereich dieser Verordnung fallen und die von Kreditinstituten, die der Richtlinie 2013/36/EU unterliegen, in Verkehr gebracht oder in Betrieb genommen werden, wird die Konformitätsbewertung im Rahmen des Verfahrens durchgeführt, auf das in den Artikeln 97 bis 101 der genannten Richtlinie Bezug genommen wird.**

## **Änderungsantrag 124**

### **Vorschlag für eine Verordnung Artikel 24 a (neu)**

*Vorschlag der Kommission*

*Geänderter Text*

#### **Artikel 24a**

**Wenn Produkte mit digitalen Elementen über gleichwertige Hardware oder Software verfügen, kann ein Produktmodell für die Zwecke der folgenden Konformitätsbewertungsverfahren als repräsentativ für eine Produktfamilie gelten:**

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

von Modul C) gemäß Anhang VI.

## Änderungsantrag 125

### Vorschlag für eine Verordnung Artikel 27 – Absatz 5

*Vorschlag der Kommission*

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

*Geänderter Text*

(5) **Die notifizierenden** Behörden **wahren** die Vertraulichkeit der von ihnen erlangten Informationen, **einschließlich der Rechte des geistigen Eigentums, der vertraulichen Geschäftsinformationen und der Geschäftsgeheimnisse.**

## Änderungsantrag 126

### Vorschlag für eine Verordnung Artikel 27 – Absatz 6 a (neu)

*Vorschlag der Kommission*

*Geänderter Text*

(6a) **Die notifizierenden Behörden müssen Verwaltungsaufwand und Gebühren, insbesondere für KMU, so gering wie möglich halten.**

## Änderungsantrag 127

### Vorschlag für eine Verordnung Artikel 29 – Absatz 7 a (neu)

*Vorschlag der Kommission*

*Geänderter Text*

(7a) **Die Mitgliedstaaten und die Kommission treffen geeignete Maßnahmen, um eine ausreichende Verfügbarkeit qualifizierter Fachkräfte sicherzustellen und so Engpässe bei den Tätigkeiten der Konformitätsbewertungsstellen so gering wie möglich zu halten.**

## Änderungsantrag 128

### Vorschlag für eine Verordnung Artikel 29 – Absatz 10

#### *Vorschlag der Kommission*

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

#### *Geänderter Text*

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

## Änderungsantrag 129

### Vorschlag für eine Verordnung Artikel 29 – Absatz 12

#### *Vorschlag der Kommission*

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

#### *Geänderter Text*

(12) **Die** Konformitätsbewertungsstellen üben ihre Tätigkeiten im Einklang mit einer Reihe kohärenter, gerechter und angemessener Geschäftsbedingungen **in Übereinstimmung mit Artikel 37 Absatz 2** aus, wobei sie insbesondere in Bezug auf Gebühren die Interessen **von Kleinstunternehmen sowie kleinen und mittleren Unternehmen** berücksichtigen.

## Änderungsantrag 130

**Vorschlag für eine Verordnung**  
**Artikel 36 – Absatz 3**

*Vorschlag der Kommission*

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

*Geänderter Text*

(3) Die Kommission stellt sicher, dass alle im Verlauf ihrer Untersuchungen erlangten **Informationen, einschließlich Rechte an geistigem Eigentum, vertrauliche Geschäftsinformationen und Geschäftsgeheimnisse**, vertraulich behandelt werden.

**Änderungsantrag 131**

**Vorschlag für eine Verordnung**  
**Artikel 37 – Absatz 2**

*Vorschlag der Kommission*

(2) Die Konformitätsbewertungen werden unter Wahrung der Verhältnismäßigkeit durchgeführt, wobei unnötige Belastungen der Wirtschaftsakteure vermieden werden. Die Konformitätsbewertungsstellen üben ihre Tätigkeiten unter gebührender Berücksichtigung der Größe eines Unternehmens, der Branche, in der es tätig ist, seiner Struktur, des Grads der Komplexität der betroffenen Produkttechnologie und des Massenfertigungs- oder Seriencharakters des Fertigungsprozesses aus.

*Geänderter Text*

(2) Die Konformitätsbewertungen werden unter Wahrung der Verhältnismäßigkeit durchgeführt, wobei unnötige Belastungen der Wirtschaftsakteure, **mit einem besonderen Augenmerk auf KMU**, vermieden werden. Die Konformitätsbewertungsstellen üben ihre Tätigkeiten unter gebührender Berücksichtigung der Größe eines Unternehmens, der Branche, in der es tätig ist, seiner Struktur, des Grads der Komplexität **und der Risikoexposition des betreffenden Produkttyps** und der betroffenen Produkttechnologie und des Massenfertigungs- oder Seriencharakters des Fertigungsprozesses aus.

**Änderungsantrag 132**

**Vorschlag für eine Verordnung**  
**Artikel 37 – Absatz 5**

*Vorschlag der Kommission*

(5) Hat eine notifizierte Stelle bereits eine Bescheinigung ausgestellt und stellt

*Geänderter Text*

(5) Hat eine notifizierte Stelle bereits eine Bescheinigung ausgestellt und stellt

im Rahmen der Überwachung der Konformität fest, dass das Produkt die in dieser Verordnung festgelegten Anforderungen nicht mehr erfüllt, fordert sie den Hersteller auf, angemessene Korrekturmaßnahmen zu ergreifen, und **setzt** die Bescheinigung **falls nötig** aus oder widerruft sie.

**sie** im Rahmen der Überwachung der Konformität fest, dass das Produkt die in dieser Verordnung festgelegten Anforderungen nicht mehr erfüllt, fordert sie den Hersteller auf, angemessene Korrekturmaßnahmen zu ergreifen, und **schränkt** die Bescheinigung **ein, setzt sie** aus oder widerruft sie, **sofern dies erforderlich ist**.

### Änderungsantrag 133

#### Vorschlag für eine Verordnung Artikel 40 – Absatz 1

##### *Vorschlag der Kommission*

(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.

##### *Geänderter Text*

(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, **wobei auch dem Erfordernis, den Verwaltungsaufwand und die Gebühren zu verringern, Rechnung getragen wird**.

### Änderungsantrag 134

#### Vorschlag für eine Verordnung Artikel 40 – Absatz 2

##### *Vorschlag der Kommission*

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

##### *Geänderter Text*

(2) Die Mitgliedstaaten sorgen dafür, dass sich die von ihnen notifizierten Stellen direkt oder über benannte Vertreter auf eine Weise an der Arbeit dieser Gruppe beteiligen, **wobei auch dem Erfordernis, den Verwaltungsaufwand und die Gebühren zu verringern, Rechnung getragen wird**.

### Änderungsantrag 135

**Vorschlag für eine Verordnung**  
**Artikel 41 – Absatz 3**

*Vorschlag der Kommission*

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

*Geänderter Text*

(3) Die Marktüberwachungsbehörden arbeiten gegebenenfalls mit den nach Artikel 58 der Verordnung (EU) 2019/881 benannten nationalen Behörden für die Cybersicherheitszertifizierung zusammen und tauschen regelmäßig Informationen mit ihnen aus. Bei der Beaufsichtigung der Umsetzung der Meldepflichten nach Artikel 11 der vorliegenden Verordnung arbeiten die benannten Marktüberwachungsbehörden wirksam mit der ENISA zusammen. **Die Marktüberwachungsbehörden können die ENISA um technische Beratung zu Fragen im Zusammenhang mit der Durchführung und Durchsetzung dieser Verordnung ersuchen; dies gilt auch für Untersuchungen gemäß Artikel 43, bei denen die Marktüberwachungsbehörden die ENISA um eine nicht verbindliche Bewertung der Konformität von Produkten mit digitalen Elementen ersuchen können.**

**Änderungsantrag 136**

**Vorschlag für eine Verordnung**  
**Artikel 41 – Absatz 7**

*Vorschlag der Kommission*

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

*Geänderter Text*

(7) Die Kommission fördert den **regelmäßigen und strukturierten** Erfahrungsaustausch zwischen den benannten Marktüberwachungsbehörden, **auch über eine spezielle Gruppe für die Verwaltungszusammenarbeit bei der Marktüberwachung (ADCO-Gruppe), die gemäß Absatz 11 dieses Artikels eingerichtet wird.**

## Änderungsantrag 137

### Vorschlag für eine Verordnung Artikel 41 – Absatz 8

*Vorschlag der Kommission*

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

*Geänderter Text*

(8) Die **Kommission nimmt Leitlinien an und gibt** Wirtschaftsakteuren – **insbesondere solchen, die als KMU oder Kleinstunternehmen einzustufen sind** – Ratschläge für die Durchführung dieser Verordnung. **Die Leitlinien und Ratschläge zielen insbesondere darauf ab, den Verwaltungsaufwand und die finanzielle Belastung zu vereinfachen und zu begrenzen und gleichzeitig eine wirksame und kohärente Anwendung im Einklang mit dem allgemeinen Ziel der Gewährleistung der Produktsicherheit und des Verbraucherschutzes sicherzustellen.**

## Änderungsantrag 138

### Vorschlag für eine Verordnung Artikel 41 – Absatz 8 a (neu)

*Vorschlag der Kommission*

*Geänderter Text*

(8a) **Die Marktüberwachungsbehörden müssen in der Lage sein, Beschwerden von Verbrauchern gemäß Artikel 11 der Verordnung (EU) 2019/1020 entgegenzunehmen, indem sie auch klare und zugängliche Mechanismen einrichten, um die Meldung von Schwachstellen, Vorfällen und Cyberbedrohungen zu erleichtern.**

## Änderungsantrag 139

### Vorschlag für eine Verordnung Artikel 41 – Absatz 11

*Vorschlag der Kommission*

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

*Geänderter Text*

(11) Im Hinblick auf die einheitliche Anwendung dieser Verordnung wird gemäß Artikel 30 Absatz 2 der Verordnung (EU) 2019/1020 eine besondere Gruppe zur administrativen Zusammenarbeit (ADCO) eingesetzt, **um in Bezug auf die Umsetzung der Bestimmungen dieser Verordnung eine strukturierte Zusammenarbeit zu erleichtern und die Verfahren der Marktüberwachungsbehörden innerhalb der Union zu straffen**. Die ADCO **hat insbesondere die in Artikel 32 Absatz 2 der Verordnung (EU) 2019/1020 genannten Aufgaben und** setzt sich aus Vertretern der benannten Marktüberwachungsbehörden, **der ENISA** und gegebenenfalls Vertretern der zentralen Verbindungsstellen zusammen. **Die ADCO kommt in regelmäßigen Abständen und gegebenenfalls auf ordnungsgemäß begründeten Antrag der Kommission, der ENISA oder eines Mitgliedstaats zusammen und stimmt ihre Tätigkeit mit anderen bestehenden Tätigkeiten der Union im Bereich der Marktüberwachung und der Verbrauchersicherheit ab und arbeitet bei Bedarf mit anderen Netzen, Gruppen und Behörden der Union zusammen. Die ADCO kann Sachverständige und andere Dritte, darunter Verbraucherverbände, zur Teilnahme an ihren Sitzungen einladen.**

**Änderungsantrag 140**

**Vorschlag für eine Verordnung  
Artikel 41 – Absatz 11 a (neu)**

*Vorschlag der Kommission*

*Geänderter Text*

**(11a) Für Produkte mit digitalen Elementen, die in den Anwendungsbereich dieser Verordnung**

*fallen und von Finanzinstituten vertrieben, in Betrieb genommen oder verwendet werden, die den einschlägigen Rechtsvorschriften der Union über Finanzdienstleistungen unterliegen, ist die Marktüberwachungsbehörde für die Zwecke dieser Verordnung die für die Finanzaufsicht über diese Institute gemäß den entsprechenden Rechtsvorschriften zuständige Behörde.*

## **Änderungsantrag 141**

### **Vorschlag für eine Verordnung Artikel 42 – Absatz 1**

#### *Vorschlag der Kommission*

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

#### *Geänderter Text*

Soweit dies für die Bewertung der Konformität von Produkten mit digitalen Elementen und der von deren Herstellern festgelegten Verfahren mit den grundlegenden Anforderungen in Anhang I erforderlich ist, erhalten die Marktüberwachungsbehörden auf begründeten Antrag Zugang zu den Daten, die für die Bewertung der Konzeption, Entwicklung, Herstellung und die Behandlung von Schwachstellen solcher Produkte erforderlich sind, einschließlich der betreffenden internen Unterlagen des jeweiligen Wirtschaftsakteurs. ***Soweit erforderlich und in Übereinstimmung mit Artikel 52 Absatz 1 Buchstabe a wird die Bewertung in einer sicheren, kontrollierten Umgebung durchgeführt, die vom Hersteller festgelegt wird.***

## **Änderungsantrag 142**

### **Vorschlag für eine Verordnung Artikel 43 – Absatz 1 – Unterabsatz 2**

#### *Vorschlag der Kommission*

Gelangt die Marktüberwachungsbehörde

#### *Geänderter Text*

Gelangt die Marktüberwachungsbehörde

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

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

***Bevor die genannte Bewertung durchgeführt wird, kann die Marktüberwachungsbehörde erforderlichenfalls und unter Berücksichtigung des Umfangs des Cybersicherheitsrisikos den betreffenden Akteur auffordern, die Bereitstellung des Produkts auf dem Markt für den Zeitraum der genannten Bewertung unverzüglich auszusetzen oder einzuschränken.***

## Änderungsantrag 143

### Vorschlag für eine Verordnung Artikel 43 – Absatz 4 – Unterabsatz 1

#### *Vorschlag der Kommission*

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

#### *Geänderter Text*

Ergreift der Hersteller eines Produkts mit digitalen Elementen innerhalb der in Absatz 1 Unterabsatz 2 genannten Frist keine angemessenen Korrekturmaßnahmen **oder stufen die einschlägigen Behörden der Mitgliedstaaten das Produkt als Bedrohung der nationalen Sicherheit ein**, so treffen die Marktüberwachungsbehörden alle geeigneten vorläufigen Maßnahmen, um die Bereitstellung des Produkts auf ihrem nationalen Markt zu untersagen oder einzuschränken, das Produkt vom Markt zu nehmen oder es zurückzurufen.

## Änderungsantrag 144

### Vorschlag für eine Verordnung Artikel 45 – Absatz 1

#### *Vorschlag der Kommission*

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

#### *Geänderter Text*

(1) Hat die Kommission – auch aufgrund von Informationen der **zuständigen Behörden der Mitgliedstaaten, der gemäß der Richtlinie (EU) 2022/2555 benannten oder eingerichteten Computer-Notfallteams (CSIRT) oder der** ENISA – hinreichende Gründe zu der Annahme, dass ein Produkt mit digitalen Elementen, das ein erhebliches Cybersicherheitsrisiko birgt, den Anforderungen dieser Verordnung nicht genügt, so **fordert** sie die zuständigen Marktüberwachungsbehörden **auf**, eine Konformitätsbewertung durchzuführen und die in Artikel 43 genannten Verfahren anzuwenden.

## Änderungsantrag 145

### Vorschlag für eine Verordnung Artikel 45 – Absatz 2

#### *Vorschlag der Kommission*

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

#### *Geänderter Text*

(2) Unter Umständen, die ein sofortiges Eingreifen rechtfertigen, um das reibungslose Funktionieren des Binnenmarkts zu **wahren**, und wenn die Kommission Gründe zu der Annahme hat, dass das in Absatz 1 genannte Produkt **nach wie vor** den Anforderungen dieser Verordnung nicht genügt und die zuständigen Marktüberwachungsbehörden keine wirksamen Maßnahmen ergriffen haben, **ersucht** die Kommission die ENISA, eine Bewertung der Konformität vorzunehmen. Die Kommission unterrichtet die betreffenden Marktüberwachungsbehörden hierüber. Die

Marktüberwachungsbehörden hierüber. Die betroffenen Wirtschaftsakteure arbeiten im erforderlichen Umfang mit der ENISA zusammen.

betroffenen Wirtschaftsakteure arbeiten im erforderlichen Umfang mit der ENISA zusammen.

## Änderungsantrag 146

### Vorschlag für eine Verordnung Artikel 46 – Absatz 1

#### *Vorschlag der Kommission*

(1) Stellt die Marktüberwachungsbehörde eines Mitgliedstaats nach einer Bewertung gemäß Artikel 43 fest, dass ein Produkt mit digitalen Elementen und die vom Hersteller festgelegten Verfahren, obwohl sie dieser Verordnung entsprechen, ein erhebliches Cybersicherheitsrisiko bergen und darüber hinaus ein Risiko für die Gesundheit oder Sicherheit von Personen, für die Erfüllung der Pflichten aus dem Unionsrecht oder dem nationalen Recht zum Schutz der Grundrechte, für die Verfügbarkeit, Integrität oder Vertraulichkeit von Diensten, die über ein elektronisches Informationssystem von wesentlichen Einrichtungen der in *[Anhang I der Richtlinie XXX/XXXX (NIS2)]* genannten Art angeboten werden, oder für andere Aspekte des Schutzes öffentlicher Interessen darstellen, so fordert sie den betroffenen *Akteur* auf, alle geeigneten Maßnahmen zu treffen, damit das Produkt mit digitalen Elementen und die vom betreffenden Hersteller festgelegten Verfahren bei seinem Inverkehrbringen dieses Risiko nicht mehr bergen, oder um das Produkt mit digitalen Elementen innerhalb einer der Art des Risikos angemessenen Frist vom Markt zu nehmen oder zurückzurufen.

#### *Geänderter Text*

(1) Stellt die Marktüberwachungsbehörde eines Mitgliedstaats nach einer Bewertung gemäß Artikel 43 fest, dass ein Produkt mit digitalen Elementen und die vom Hersteller festgelegten Verfahren, obwohl sie dieser Verordnung entsprechen, ein erhebliches Cybersicherheitsrisiko bergen und darüber hinaus ein Risiko für die Gesundheit oder Sicherheit von Personen, für die Erfüllung der Pflichten aus dem Unionsrecht oder dem nationalen Recht zum Schutz der Grundrechte, für die Verfügbarkeit, Integrität oder Vertraulichkeit von Diensten, die über ein elektronisches Informationssystem von wesentlichen Einrichtungen der in *Anhang I der Richtlinie (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)* genannten Art angeboten werden, oder für andere Aspekte des Schutzes öffentlicher Interessen darstellen, so fordert sie den betroffenen *Wirtschaftsakteur* auf, alle geeigneten Maßnahmen zu treffen, damit das Produkt mit digitalen Elementen und die vom betreffenden Hersteller festgelegten Verfahren bei seinem Inverkehrbringen dieses Risiko nicht mehr bergen, oder um

das Produkt mit digitalen Elementen innerhalb einer der Art des Risikos angemessenen Frist vom Markt zu nehmen oder zurückzurufen.

## Änderungsantrag 147

### Vorschlag für eine Verordnung Artikel 46 – Absatz 2

#### *Vorschlag der Kommission*

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

#### *Geänderter Text*

(2) Der Hersteller oder andere einschlägige **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.

## Änderungsantrag 148

### Vorschlag für eine Verordnung Artikel 46 – Absatz 6

#### *Vorschlag der Kommission*

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

#### *Geänderter Text*

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

## Änderungsantrag 149

## Vorschlag für eine Verordnung Artikel 46 – Absatz 7

### *Vorschlag der Kommission*

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

### *Geänderter Text*

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

## Änderungsantrag 150

### Vorschlag für eine Verordnung Artikel 48 – Absatz 1

#### *Vorschlag der Kommission*

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

#### *Geänderter Text*

(1) Die Marktüberwachungsbehörden **führen** mit anderen einschlägigen Behörden **regelmäßig gemeinsame** Tätigkeiten zur Gewährleistung der Cybersicherheit und des Verbraucherschutzes in Bezug auf bestimmte in Verkehr gebrachte oder auf dem Markt bereitgestellte Produkte mit digitalen Elementen **durch**, insbesondere in Bezug auf Produkte, bei denen häufig Cybersicherheitsrisiken festgestellt werden. **Diese Tätigkeiten umfassen auch die Inspektion von Produkten, die unter einer verdeckten Identität erworben wurden.**

## Änderungsantrag 151

### Vorschlag für eine Verordnung Artikel 48 – Absatz 2

#### *Vorschlag der Kommission*

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

#### *Geänderter Text*

(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, die in den Anwendungsbereich dieser Verordnung fallen, möglicherweise in mehreren Mitgliedstaaten den Anforderungen dieser Verordnung nicht entsprechen, durchgeführt werden sollen.

## Änderungsantrag 152

### Vorschlag für eine Verordnung Artikel 49 – Absatz 1

#### *Vorschlag der Kommission*

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

#### *Geänderter Text*

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

## Änderungsantrag 153

### Vorschlag für eine Verordnung Artikel 49 – Absatz 2

#### *Vorschlag der Kommission*

(2) Sofern die betreffenden Marktüberwachungsbehörden nichts anderes vereinbaren, werden solche

#### *Geänderter Text*

(2) Sofern die betreffenden Marktüberwachungsbehörden nichts anderes vereinbaren, werden solche

Sweeps von der Kommission koordiniert. Der Koordinator des Sweeps **kann** die aggregierten Ergebnisse **gegebenenfalls veröffentlichen**.

Sweeps von der Kommission koordiniert. Der Koordinator des Sweeps **veröffentlicht gegebenenfalls** die aggregierten Ergebnisse.

## Änderungsantrag 154

### Vorschlag für eine Verordnung Artikel 49 – Absatz 3

#### *Vorschlag der Kommission*

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

#### *Geänderter Text*

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

## Änderungsantrag 155

### Vorschlag für eine Verordnung Artikel 49 – Absatz 5

#### *Vorschlag der Kommission*

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

#### *Geänderter Text*

(5) Die Marktüberwachungsbehörden **laden** Kommissionsbeamte und weitere von der Kommission autorisierte Begleitpersonen zur Teilnahme an Sweeps **ein**.

## Änderungsantrag 156

### Vorschlag für eine Verordnung Artikel 49 a (neu)

#### *Vorschlag der Kommission*

#### *Geänderter Text*

#### **Artikel 49a**

### ***Bereitstellung technischer Beratung***

- (1) Die Kommission ernennt im Wege eines Durchführungsrechtsakts eine Sachverständigengruppe, die die Marktüberwachungsbehörden in Fragen der Durchführung und Durchsetzung dieser Verordnung fachlich berät. In dem Durchführungsrechtsakt werden unter anderem die Einzelheiten zu der Zusammensetzung der Gruppe, ihrer Arbeitsweise und der Vergütung ihrer Mitglieder festgelegt. Die Sachverständigengruppe nimmt auf Ersuchen einer Marktüberwachungsbehörde, die eine Untersuchung gemäß Artikel 43 durchführt, insbesondere nicht verbindliche Bewertungen zu Produkten mit digitalen Elementen vor, bewertet die Liste kritischer Produkte gemäß Anhang II und äußert sich gegebenenfalls über die etwaige erforderliche Aktualisierung dieser Liste.***
- (2) Die Sachverständigengruppe setzt sich aus unabhängigen Sachverständigen zusammen, die auf der Grundlage ihrer wissenschaftlichen oder technischen Expertise von der Kommission für ein dreijähriges erneuerbares Mandat ernannt werden.***
- (3) Die Kommission ernennt eine Anzahl von Sachverständigen, die sie für ausreichend hält, um den voraussichtlichen Bedarf zu decken.***
- (4) Die Kommission ergreift die erforderlichen Maßnahmen, um Interessenkonflikte zu bewältigen bzw. zu verhindern. Die Interessenerklärungen der Mitglieder der Sachverständigengruppe werden öffentlich zugänglich gemacht.***
- (5) Die bestellten Sachverständigen müssen ihre Aufgaben mit einem Höchstmaß an Professionalität, Unabhängigkeit, Unparteilichkeit und Objektivität erfüllen.***

**(6) Bei der Verabschiedung von Standpunkten, Einschätzungen und Berichten versucht die Sachverständigengruppe, einen Konsens zu erzielen. Kann kein Konsens erzielt werden, werden die Entscheidungen mit einfacher Mehrheit der Gruppenmitglieder getroffen.**

## **Änderungsantrag 157**

### **Vorschlag für eine Verordnung Artikel 53 – Absatz 1**

#### *Vorschlag der Kommission*

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

#### *Geänderter Text*

(1) Die Mitgliedstaaten erlassen Vorschriften über Sanktionen, die bei Verstößen der Wirtschaftsakteure gegen diese Verordnung zu verhängen sind, und treffen alle für die Durchsetzung der Sanktionen erforderlichen Maßnahmen. Die vorgesehenen Sanktionen müssen wirksam, verhältnismäßig und abschreckend sein **und den Besonderheiten von Kleinstunternehmen sowie kleinen und mittleren Unternehmen Rechnung tragen.**

## **Änderungsantrag 158**

### **Vorschlag für eine Verordnung Artikel 53 – Absatz 6 – Buchstabe a a (neu)**

#### *Vorschlag der Kommission*

#### *Geänderter Text*

**aa) ob der Verstoß ist unbeabsichtigt ist,**

## **Änderungsantrag 159**

### **Vorschlag für eine Verordnung Artikel 53 – Absatz 6 – Buchstabe b**

*Vorschlag der Kommission*

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

*Geänderter Text*

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

## **Änderungsantrag 160**

### **Vorschlag für eine Verordnung Artikel 53 – Absatz 6 – Buchstabe c**

*Vorschlag der Kommission*

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

*Geänderter Text*

c) Größe und Marktanteil des Akteurs, der den Verstoß begangen hat, **wobei der Umfang der Risiken, Folgen und finanziellen Besonderheiten von Kleinstunternehmen sowie kleinen und mittleren Unternehmen berücksichtigt werden;**

## **Änderungsantrag 161**

### **Vorschlag für eine Verordnung Artikel 53 – Absatz 6 – Buchstabe c a (neu)**

*Vorschlag der Kommission*

*Geänderter Text*

**ca) das anschließende Verhalten des Betreibers, nachdem er von dem jeweiligen Verstoß erfahren hat, einschließlich der Frage, ob der Betreiber, nachdem er Kenntnis von dem Verstoß erlangt hat, alle geeigneten Korrekturmaßnahmen sowie nach vernünftigem Ermessen erforderliche Maßnahmen ergriffen hat, um mögliche negative Auswirkungen zu verhindern oder möglichst gering zu halten.**

## **Änderungsantrag 162**

**Vorschlag für eine Verordnung  
Kapitel VII a (neu)**

*Vorschlag der Kommission*

*Geänderter Text*

**MASSNAHMEN ZUR  
INNOVATIONSFÖRDERUNG**

**Änderungsantrag 163**

**Vorschlag für eine Verordnung  
Artikel 53 a (neu)**

*Vorschlag der Kommission*

*Geänderter Text*

**Artikel 53a**

**Reallabore**

***Die Kommission und die ENISA können ein europäisches Reallabor unter freiwilliger Beteiligung der Hersteller von Produkten mit digitalen Elementen einrichten, um:***

- a) eine kontrollierte Umgebung schaffen, die die Ausarbeitung, Erprobung und Validierung des Konzepts und die Entwicklung und Herstellung von Produkten mit digitalen Elementen erleichtert, bevor sie nach einem spezifischen Plan in Verkehr gebracht oder in Betrieb genommen werden,***
- b) eine spezielle praktische Unterstützung für Wirtschaftsakteure bereitzustellen, auch durch Leitlinien oder bewährte Verfahren, die die Erfüllung der in Anhang I aufgeführten grundlegenden Anforderungen betreffen;***
- c) einen Beitrag zum faktengestützten Wissenserwerb zu aufsichtsrechtlichen Fragen zu leisten.***

**Änderungsantrag 164**

**Vorschlag für eine Verordnung  
Artikel 54 – Überschrift**

*Vorschlag der Kommission*

*Geänderter Text*

Änderung der Verordnung (EU) 2019/1020

Änderung der Verordnung (EU) 2019/1020  
**und der Richtlinie 2020/1828/EG**

## **Änderungsantrag 165**

**Vorschlag für eine Verordnung**  
**Artikel 54 – Absatz 1 a (neu)**

*Vorschlag der Kommission*

*Geänderter Text*

**(1a) In Anhang I der  
Richtlinie 2020/1828/EG wird folgende  
Nummer eingefügt:**

**„67.**

**[Verordnung XXX][Cyberresilienz  
gesetz]“**

## **Änderungsantrag 166**

**Vorschlag für eine Verordnung**  
**Artikel 54 a (neu)**

*Vorschlag der Kommission*

*Geänderter Text*

### **Artikel 54a**

**Delegierte Verordnung (EU) 2022/30**

**Die vorliegende Verordnung ist so  
konzipiert, dass alle Produkte, die unter  
die in Artikel 3 Absatz 3 Buchstaben d, e  
und f der Richtlinie 2014/53/EU  
festgelegten grundlegenden  
Anforderungen – wie in der Delegierten  
Verordnung (EU) 2022/30 beschrieben –  
fallen, der vorliegenden Verordnung  
entsprechen. Um Rechtssicherheit zu  
schaffen, wird die Delegierte Verordnung  
(EU) 2022/30 mit Inkrafttreten der  
vorliegenden Verordnung aufgehoben.**

## **Änderungsantrag 167**

**Vorschlag für eine Verordnung**  
**Artikel 57 – Absatz 2**

*Vorschlag der Kommission*

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

*Geänderter Text*

Sie gilt ab dem [36 Monate nach dem Datum des Inkrafttretens dieser Verordnung]. **Für Produkte mit kritischen Elementen gelten die Kapitel II, III, V und VII frühestens** ab dem [20 Monate nach dem Datum *der Veröffentlichung der im Rahmen der für die Zwecke dieser Verordnung erforderlichen Normung ausgearbeiteten harmonisierten Normen*].  
**Spätestens sechs Monate nach Inkrafttreten dieser Verordnung gibt die Kommission Leitlinien für die Anwendung der Anforderungen aus dieser Verordnung auf immaterielle Produkte heraus.**

**Änderungsantrag 168**

**Vorschlag für eine Verordnung**  
**Anhang I – Teil 1 – Nummer 3 – Einleitung**

*Vorschlag der Kommission*

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

*Geänderter Text*

(3) Auf der Grundlage der **Bewertung von Cyberrisiken** gemäß Artikel 10 Absatz 2 müssen Produkte mit digitalen Elementen, soweit zutreffend,

**Änderungsantrag 169**

**Vorschlag für eine Verordnung**  
**Anhang I – Teil 1 – Nummer 3 – Buchstabe - a (neu)**

*Vorschlag der Kommission*

**-a) ohne bekannte ausnutzbare Schwachstellen gegenüber einem externen Gerät oder Netz in Verkehr gebracht werden,**

*Geänderter Text*

## Änderungsantrag 170

### Vorschlag für eine Verordnung Anhang I – Teil 1 – Nummer 3 – Buchstabe a

#### *Vorschlag der Kommission*

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

#### *Geänderter Text*

a) mit einer sicheren Standardkonfiguration ausgeliefert werden,

## Änderungsantrag 171

### Vorschlag für eine Verordnung Anhang I – Teil 1 – Nummer 3 – Buchstabe c

#### *Vorschlag der Kommission*

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

#### *Geänderter Text*

c) die Vertraulichkeit gespeicherter, übermittelter oder anderweitig verarbeiteter personenbezogener oder sonstiger Daten schützen, z. B. durch Verschlüsselung, **Tokenisierung, kompensierende Kontrollen oder anderen angemessenen Schutz von relevanten** Daten, die gespeichert sind oder gerade verwendet oder übermittelt werden, durch modernste Mechanismen,

## Änderungsantrag 172

### Vorschlag für eine Verordnung Anhang I – Teil 1 – Nummer 3 – Buchstabe d

#### *Vorschlag der Kommission*

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

#### *Geänderter Text*

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

*unbefugten Zugriff* melden,

### Änderungsantrag 173

#### Vorschlag für eine Verordnung

##### Anhang I – Teil 1 – Nummer 3 – Buchstabe f

###### *Vorschlag der Kommission*

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

###### *Geänderter Text*

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

### Änderungsantrag 174

#### Vorschlag für eine Verordnung

##### Anhang I – Teil 1 – Nummer 3 – Buchstabe i

###### *Vorschlag der Kommission*

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

###### *Geänderter Text*

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

### Änderungsantrag 175

#### Vorschlag für eine Verordnung

##### Anhang I – Teil 1 – Nummer 3 – Buchstabe j

###### *Vorschlag der Kommission*

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

###### *Geänderter Text*

j) sicherheitsbezogene Informationen **bereitstellen, indem sie auf Wunsch des Nutzers Aufzeichnungs- und/oder Überwachungsmöglichkeiten lokal und auf Geräteebene für einschlägige interne** Vorgänge **bieten**, wie Zugang zu Daten, Diensten oder Funktionen;

## Änderungsantrag 176

### Vorschlag für eine Verordnung Anhang I – Teil 1 – Nummer 3 – Buchstabe k

#### *Vorschlag der Kommission*

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

#### *Geänderter Text*

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

## Änderungsantrag 177

### Vorschlag für eine Verordnung Anhang I – Teil 1 – Nummer 3 – Buchstabe k a (neu)

#### *Vorschlag der Kommission*

#### *Geänderter Text*

***ka) so konzipiert, entwickelt und hergestellt werden, dass eine sichere Einstellung und ein mögliches Recycling am Ende des Lebenszyklus möglich ist, unter anderem dadurch, dass die Nutzer alle Daten auf sichere Weise entfernen und dauerhaft löschen können.***

## Änderungsantrag 178

### Vorschlag für eine Verordnung Anhang I – Teil 2 – Absatz 1 – Nummer 2

#### *Vorschlag der Kommission*

(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;

#### *Geänderter Text*

(2) im Hinblick auf die Risiken im Zusammenhang mit den Produkten mit digitalen Elementen unverzüglich ***kritische und schwerwiegende*** Schwachstellen behandeln und beheben, unter anderem durch Bereitstellung von Sicherheitsaktualisierungen, ***oder die Gründe für die Nichtbehebung der***

*Schwachstelle dokumentieren;*

## Änderungsantrag 179

### Vorschlag für eine Verordnung Anhang I – Teil 2 – Absatz 1 – Nummer 4

*Vorschlag der Kommission*

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

*Geänderter Text*

(4) sobald eine Sicherheitsaktualisierung bereitgestellt worden ist, Informationen über **bekannte** beseitigte Schwachstellen veröffentlichen **oder gemäß den bewährten Verfahren der Branche bekanntmachen**, 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 **klare und zugängliche** Informationen, die den Nutzern helfen, die Schwachstellen zu beheben;

## Änderungsantrag 180

### Vorschlag für eine Verordnung Anhang I – Teil 2 – Absatz 1 – Nummer 4 a (neu)

*Vorschlag der Kommission*

*Geänderter Text*

**(4a) Informationen über Fehlerbehebungen und Schwachstellen auf kontrollierte Weise weitergeben und offenlegen, wobei sie den Grundsatz der Schadensminderung und der Wahrung von Geschäftsgeheimnissen durch eine verantwortungsvolle Offenlegung von Schwachstellen gegenüber den Akteuren, die die Schwachstelle beheben können, beachten müssen und sicherstellen, dass diese Informationen nicht öffentlich zugänglich gemacht werden, um dem Risiko aus dem Weg zu gehen, dass versehentlich potenzielle Angreifer informiert werden;**

## Änderungsantrag 181

### Vorschlag für eine Verordnung Anhang I – Teil 2 – Absatz 1 – Nummer 7

#### *Vorschlag der Kommission*

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

#### *Geänderter Text*

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

## Änderungsantrag 182

### Vorschlag für eine Verordnung Anhang I – Teil 2 – Absatz 1 – Nummer 8

#### *Vorschlag der Kommission*

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

#### *Geänderter Text*

(8) dafür sorgen, dass **für** Sicherheits-Patches oder Aktualisierungen, die **nach vernünftigem Ermessen** zur Bewältigung festgestellter Sicherheitsprobleme **verfügbar gemacht werden können, dass Mittel und Wege vorhanden sind, über die Nutzer sie** unverzüglich und kostenlos **oder zu transparenten und nichtdiskriminierenden Preisen erhalten können**, zusammen mit Hinweisen und einschlägigen Informationen, auch über zu treffende mögliche Maßnahmen.

## Änderungsantrag 183

### Vorschlag für eine Verordnung Anhang II – Absatz 1 – Nummer 2

#### *Vorschlag der Kommission*

2. **die** Kontaktstelle, bei der Informationen über Cybersicherheitslücken des Produkts gemeldet werden können und

#### *Geänderter Text*

2. **eine zentrale** Kontaktstelle, bei der Informationen über Cybersicherheitslücken des Produkts gemeldet werden können und

entgegengenommen werden;

entgegengenommen werden;

### **Änderungsantrag 184**

#### **Vorschlag für eine Verordnung Anhang II – Absatz 1 – Nummer 5**

*Vorschlag der Kommission*

*Geänderter Text*

5. *alle bekannten oder vorhersehbaren Umstände im Zusammenhang mit der bestimmungsgemäßen Verwendung des Produkts mit digitalen Elementen oder dessen vernünftigerweise vorhersehbaren Fehlanwendung, die zu erheblichen Cybersicherheitsrisiken führen können;*

*entfällt*

### **Änderungsantrag 185**

#### **Vorschlag für eine Verordnung Anhang II – Absatz 1 – Nummer 6**

*Vorschlag der Kommission*

*Geänderter Text*

6. ob und gegebenenfalls wo die Software-Stückliste *abrufbar ist*;

6. ob und gegebenenfalls wo die Software-Stückliste *von den zuständigen Behörden abgerufen werden kann*;

### **Änderungsantrag 186**

#### **Vorschlag für eine Verordnung Anhang II – Absatz 1 – Nummer 8**

*Vorschlag der Kommission*

*Geänderter Text*

8. die Art der vom Hersteller angebotenen technischen Sicherheitsunterstützung, bis wann sie zur Verfügung steht *und zumindest bis wann die Nutzer Sicherheitsaktualisierungen erwarten können*;

8. die Art der vom Hersteller angebotenen technischen Sicherheitsunterstützung, bis wann sie zur Verfügung steht;

### **Änderungsantrag 187**

**Vorschlag für eine Verordnung  
Anhang II – Absatz 1 – Nummer 8 a (neu)**

*Vorschlag der Kommission*

*Geänderter Text*

**8a. das erwartete Enddatum des Lebenszyklus des Produkts, das gegebenenfalls deutlich auf der Verpackung des Produkts angebracht ist, und bis zu dem der Hersteller die wirksame Behebung von Schwachstellen und die Bereitstellung von Sicherheitsaktualisierungen gewährleistet;**

**Änderungsantrag 188**

**Vorschlag für eine Verordnung  
Anhang II – Absatz 1 – Nummer 9 – Buchstabe a**

*Vorschlag der Kommission*

*Geänderter Text*

**a) welche Maßnahmen bei der ersten Inbetriebnahme und während der gesamten Lebensdauer des Produkts getroffen werden müssen, um dessen sichere Verwendung zu gewährleisten,** *entfällt*

**Änderungsantrag 189**

**Vorschlag für eine Verordnung  
Anhang II – Absatz 1 – Nummer 9 – Buchstabe b**

*Vorschlag der Kommission*

*Geänderter Text*

**b) wie sich Änderungen am Produkt auf die Datensicherheit auswirken können,** *entfällt*

**Änderungsantrag 190**

**Vorschlag für eine Verordnung  
Anhang II – Absatz 1 – Nummer 9 – Buchstabe c a (neu)**

*Vorschlag der Kommission*

*Geänderter Text*

**ca) das erwartete Enddatum des Lebenszyklus des Produkts und der Zeitpunkt, bis zu dem der Hersteller die wirksame Behebung von Schwachstellen und die Bereitstellung von Sicherheitsaktualisierungen gewährleistet;**

### **Änderungsantrag 191**

#### **Vorschlag für eine Verordnung Anhang II – Absatz 1 – Nummer 9 – Buchstabe d**

*Vorschlag der Kommission*

*Geänderter Text*

**d) wie eine sichere Außerbetriebnahme des Produkts erfolgt und wie Nutzerdaten sicher entfernt werden können.**

**entfällt**

### **Änderungsantrag 192**

#### **Vorschlag für eine Verordnung Anhang III – Klasse I – Nummer 3 a (neu)**

*Vorschlag der Kommission*

*Geänderter Text*

**3a. Plattformen für Authentifizierung, Autorisierung und Protokollierung (Triple-A-Systeme);**

### **Änderungsantrag 193**

#### **Vorschlag für eine Verordnung Anhang III – Klasse I – Nummer 15**

*Vorschlag der Kommission*

*Geänderter Text*

15. physische Netzschnittstellen;

15. physische **und virtuelle** Netzschnittstellen;

## Änderungsantrag 194

### Vorschlag für eine Verordnung Anhang III – Klasse I – Nummer 18

*Vorschlag der Kommission*

*Geänderter Text*

18. **Router, Modems für die Internetanbindung und Switches, die nicht zur Klasse II gehören;**

**entfällt**

## Änderungsantrag 195

### Vorschlag für eine Verordnung Anhang III – Klasse I – Nummer 23

*Vorschlag der Kommission*

*Geänderter Text*

23. **industrielles Internet** der Dinge (IIoT), **das** nicht zur Klasse II gehört.

23. **industrielle Produkte mit digitalen Elementen, die als Teil des Internets** der Dinge (IIoT) **bezeichnet werden können,** **der** nicht zur Klasse II gehört.

## Änderungsantrag 196

### Vorschlag für eine Verordnung Anhang III – Klasse II – Nummer 4

*Vorschlag der Kommission*

*Geänderter Text*

4. Firewalls, Angriffserkennungs- und/oder -präventionssysteme für den industriellen Einsatz;

4. Firewalls, **Sicherheits-Gateways**, Angriffserkennungs- und/oder -präventionssysteme für den industriellen Einsatz;

## Änderungsantrag 197

### Vorschlag für eine Verordnung Anhang III – Klasse II – Nummer 7

*Vorschlag der Kommission*

*Geänderter Text*

7. Router, Modems für die Internetanbindung und Switches für den industriellen Einsatz;

7. Router, Modems für die Internetanbindung und Switches für den industriellen Einsatz **und andere**

*Netzknoten, die für die Erbringung des Konnektivitätsdienstes erforderlich sind;*

## **Änderungsantrag 198**

### **Vorschlag für eine Verordnung Anhang IV a (neu)**

*Vorschlag der Kommission*

*Geänderter Text*

#### **ANHANG IVa**

#### **EU-EINBAUERKLÄRUNG FÜR UNVOLLSTÄNDIGE PRODUKTE MIT DIGITALEN ELEMENTEN**

*Die EU-Einbauerklärung für unvollständige Produkte mit digitalen Elementen gemäß Artikel 20a muss alle folgenden Angaben enthalten:*

- 1. den Namen und den Typ sowie alle zusätzlichen Informationen, die eine eindeutige Identifizierung des unvollständigen Produkts mit digitalen Elementen ermöglichen;*
- 2. den Gegenstand der Erklärung (Identifizierung des unvollständigen Produkts zwecks Rückverfolgbarkeit; dies kann gegebenenfalls ein Foto umfassen);*
- 3. eine Erklärung, dass das beschriebene unvollständige Produkt den einschlägigen Harmonisierungsrechtsvorschriften der Union entspricht;*
- 4. Verweise auf alle einschlägigen Rechtsakte der Union, einschließlich ihrer Fundstellen;*
- 5. weitere Angaben:*

*Unterzeichnet für und im Namen von:*

.....

*(Ort und Datum der Ausstellung)*

*(Name, Funktion) (Unterschrift)*

## **Änderungsantrag 199**

**Vorschlag für eine Verordnung**  
**Anhang V – Absatz 1 – Nummer 1 – Buchstabe a**

*Vorschlag der Kommission*

*Geänderter Text*

- a) *seiner Zweckbestimmung,* **entfällt**

**Änderungsantrag 200**

**Vorschlag für eine Verordnung**  
**Anhang V – Absatz 1 – Nummer 2**

*Vorschlag der Kommission*

*Geänderter Text*

2. *eine Beschreibung der Konzeption, Entwicklung und Herstellung des Produkts und der Verfahren zur Behandlung von Schwachstellen, einschließlich* **entfällt**

- a) *vollständiger Informationen über die Konzeption und Entwicklung des Produkts mit digitalen Elementen, gegebenenfalls mit Zeichnungen und Schemata und/oder einer Beschreibung der Systemarchitektur, aus der hervorgeht, wie Softwarekomponenten aufeinander aufbauen, miteinander zusammenwirken und sich in die Gesamtverarbeitung integrieren;*
- b) *vollständiger Informationen und Spezifikationen bezüglich der vom Hersteller festgelegten Verfahren zur Behandlung von Schwachstellen, einschließlich der Software-Stückliste, des Konzepts für die koordinierte Offenlegung von Schwachstellen, des Nachweises der Bereitstellung einer Kontaktadresse für die Meldung der Schwachstellen und einer Beschreibung der gewählten technischen Lösungen für die sichere Verbreitung von Aktualisierungen;*
- c) *vollständiger Informationen und Spezifikationen bezüglich der Herstellungs- und Überwachungsprozesse*

*des Produkts mit digitalen Elementen und der Validierung dieser Prozesse;*

## **Änderungsantrag 201**

### **Vorschlag für eine Verordnung Anhang V – Absatz 1 – Nummer 3**

*Vorschlag der Kommission*

3. eine Bewertung der Cybersicherheitsrisiken, die bei der Konzeption, Entwicklung, Herstellung, Lieferung und Wartung des Produkts mit digitalen Elementen nach Artikel 10 dieser Verordnung berücksichtigt werden;

*Geänderter Text*

3. eine **Erklärung oder eine Zusammenfassung der Cybersicherheitsrisiken, die bei der Konzeption, Entwicklung, Herstellung, Lieferung und Wartung des Produkts mit digitalen Elementen nach Artikel 10 dieser Verordnung berücksichtigt werden, sowie auf begründeten Antrag einer Marktüberwachungsbehörde, sofern dies erforderlich ist, damit diese Behörde die Einhaltung der grundlegenden Anforderungen nach Anhang I überprüfen kann, eine detaillierte** Bewertung der Cybersicherheitsrisiken, die bei der Konzeption, Entwicklung, Herstellung, Lieferung und Wartung des Produkts mit digitalen Elementen nach Artikel 10 dieser Verordnung berücksichtigt werden;

## **ANHANG: LISTE DER EINRICHTUNGEN UND PERSONEN, VON DENEN DER BERICHTERSTATTER BEITRÄGE ERHALTEN HAT**

Die folgende Liste wurde auf rein freiwilliger Basis unter der ausschließlichen Verantwortung des Verfassers der Stellungnahme erstellt. Der Verfasser der Stellungnahme hat im Zuge der Ausarbeitung des Entwurfs einer Stellungnahme Informationen von folgenden Einrichtungen und Personen erhalten:

Einrichtung bzw. Person
Apple
Bundesverband der Deutschen Industrie
BEUC
BSA The Software Alliance
Dänischer Industrieverband
Digital Europe
ETNO
Kaspersky
Microsoft
Samsung
TIC Council
Xiaomi

## VERFAHREN DES MITBERATENDEN AUSSCHUSSES

<b>Titel</b>	Horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen und Änderung der Verordnung (EU) 2019/1020		
<b>Bezugsdokumente – Verfahrensnummer</b>	COM(2022)0454 – C9-0308/2022 – 2022/0272(COD)		
<b>Federführender Ausschuss</b> Datum der Bekanntgabe im Plenum	ITRE 9.11.2022		
<b>Stellungnahme von</b> Datum der Bekanntgabe im Plenum	IMCO 9.11.2022		
<b>Assoziierte Ausschüsse - Datum der Bekanntgabe im Plenum</b>	20.4.2023		
<b>Verfasser der Stellungnahme</b> Datum der Benennung	Morten Løkkegaard 16.12.2022		
<b>Prüfung im Ausschuss</b>	2.3.2023	25.4.2023	23.5.2023
<b>Datum der Annahme</b>	29.6.2023		
<b>Ergebnis der Schlussabstimmung</b>	+: –: 0:	41 1 0	
<b>Zum Zeitpunkt der Schlussabstimmung anwesende Mitglieder</b>	Alex Agius Saliba, Andrus Ansip, Pablo Arias Echeverría, Alessandra Basso, Biljana Borzan, Vlad-Marius Botoș, Anna Cavazzini, Dita Charanzová, Deirdre Clune, David Cormand, Alexandra Geese, Maria Grapini, Svenja Hahn, Krzysztof Hetman, Virginie Joron, Eugen Jurzyca, Arba Kokalari, Kateřina Konečná, Andrey Kovatchev, Maria-Manuel Leitão-Marques, Antonius Manders, Beata Mazurek, Leszek Miller, Anne-Sophie Pelletier, Miroslav Radačovský, René Repasi, Christel Schaldemose, Andreas Schwab, Tomislav Sokol, Ivan Štefanec, Kim Van Sparrentak, Marion Walsmann		
<b>Zum Zeitpunkt der Schlussabstimmung anwesende Stellvertreter</b>	Marco Campomenosi, Maria da Graça Carvalho, Geoffroy Didier, Francisco Guerreiro, Tsvetelina Penkova, Catharina Rinzema, Kosma Złotowski		
<b>Zum Zeitpunkt der Schlussabstimmung anwesende Stellv. (Art. 209 Abs. 7)</b>	Asger Christensen, Nicolás González Casares, Grzegorz Tobiszowski		

## NAMENTLICHE SCHLUSSABSTIMMUNG IM MITBERATENDEN AUSSCHUSS

41	+
ECR	Beata Mazurek, Grzegorz Tobiszowski, Kosma Złotowski
ID	Alessandra Basso, Marco Campomenosi, Virginie Joron
NI	Miroslav Radačovský
PPE	Pablo Arias Echeverría, Maria da Graça Carvalho, Deirdre Clune, Geoffroy Didier, Krzysztof Hetman, Arba Kokalari, Andrey Kovatchev, Antonius Manders, Andreas Schwab, Tomislav Sokol, Ivan Štefanec, Marion Walsmann
Renew	Andrus Ansip, Vlad-Marius Botoș, Dita Charanzová, Asger Christensen, Svenja Hahn, Catharina Rinzema
S&D	Alex Agius Saliba, Biljana Borzan, Nicolás González Casares, Maria Grapini, Maria-Manuel Leitão-Marques, Leszek Miller, Tsvetelina Penkova, René Repasi, Christel Schaldemose
The Left	Kateřina Konečná, Anne-Sophie Pelletier
Verts/ALE	Anna Cavazzini, David Cormand, Alexandra Geese, Francisco Guerreiro, Kim Van Sparrentak

1	-
ECR	Eugen Jurzyca

0	0

Erklärung der benutzten Zeichen:

+ : dafür

- : dagegen

0 : Enthaltung