EUROPÄISCHE
KOMMISSION

Brüssel, den 3.2.2025
C(2025) 618 final

ANNEXES 1 to 2

ANHÄNGE

des

Durchführungsbeschlusses der Kommission

über einen Normungsauftrag an das Europäische Komitee für Normung (CEN), das Europäische Komitee für elektrotechnische Normung (Cenelec) und das Europäische Institut für Telekommunikationsnormen (ETSI) in Bezug auf Produkte mit digitalen Elementen zur Unterstützung der Verordnung (EU) 2024/2847 des Europäischen Parlaments und des Rates vom 23. Oktober 2024 über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen und zur Änderung der Verordnungen (EU) Nr. 168/2013 und (EU) 2019/1020 und der Richtlinie (EU) 2020/1828 (Cyberresilienz-Verordnung)

ANHANG I

Liste der zu erarbeitenden neuen europäischen Normen

Referenzangaben		Frist für die Annahme durch die europäischen Normungs-organisationen
Horizontale Normen für Sicherheitsanforderungen in Bezug auf die Eigenschaften von Produkten mit digitalen Elementen		
1.	Europäische Norm(en) für die Konzeption, Entwicklung und Herstellung von Produkten mit digitalen Elementen, die angesichts der Risiken ein angemessenes Maß an Cybersicherheit gewährleisten	30.8.2026
2.	Europäische Norm(en) für die Bereitstellung von Produkten mit digitalen Elementen ohne bekannte ausnutzbare Schwachstellen auf dem Markt	30.10.2027
3.	Europäische Norm(en) für die Bereitstellung von Produkten mit digitalen Elementen mit einer sicheren Standardkonfiguration auf dem Markt	30.10.2027
4.	Europäische Norm(en) für die Gewährleistung, dass Schwachstellen in Produkten mit digitalen Elementen durch Sicherheitsaktualisierungen behoben werden können	30.10.2027
5.	Europäische Norm(en) für den Schutz von Produkten mit digitalen Elementen vor unbefugtem Zugriff und für die Meldung eines möglichen unbefugten Zugriffs	30.10.2027
6.	Europäische Norm(en) für den Schutz der Vertraulichkeit von Daten, die von einem Produkt mit digitalen Elementen gespeichert, übermittelt oder anderweitig verarbeitet werden	30.10.2027
7.	Europäische Norm(en) für den Schutz der Integrität von Daten, Befehlen, Programmen durch ein Produkt mit digitalen Elementen und seiner Konfiguration vor vom Nutzer nicht genehmigten Manipulationen oder Änderungen sowie für die Meldung von Beschädigungen	30.10.2027
8.	Europäische Norm(en) für die Beschränkung der Verarbeitung personenbezogener oder sonstiger Daten auf nur solche, die angemessen und relevant sind, und auf das für die bestimmungsgemäße Verwendung des Produkts erforderliche Maß („Datenminimierung“)	30.10.2027
9.	Europäische Norm(en) für den Schutz der Verfügbarkeit wesentlicher und grundlegender Funktionen des Produkts mit digitalen Elementen	30.10.2027

10.	Europäische Norm(en) für die Minimierung der negativen Auswirkungen eines Produkts mit digitalen Elementen oder seiner vernetzten Geräte auf die Verfügbarkeit von Diensten, die von anderen Geräten oder Netzen bereitgestellt werden	30.10.2027
11.	Europäische Norm(en) für die Konzeption, Entwicklung und Herstellung von Produkten mit digitalen Elementen mit möglichst geringen Angriffsflächen	30.10.2027
12.	Europäische Norm(en) für die Konzeption, Entwicklung und Herstellung von Produkten mit digitalen Elementen, die die Auswirkungen eines Vorfalls durch geeignete Mechanismen und Techniken zur Minderung der möglichen Ausnutzung verringern	30.10.2027
13.	Europäische Norm(en) für die Bereitstellung sicherheitsbezogener Informationen durch Aufzeichnung und/oder Überwachung einschlägiger interner Vorgänge bei Produkten mit digitalen Elementen mit Opt-out-Mechanismus für den Nutzer	30.10.2027
14.	Europäische Norm(en) für die sichere und einfache Entfernung oder Übermittlung aller Daten und Einstellungen eines Produkts mit digitalen Elementen	30.10.2027
Horizontale Normen für Anforderungen an die Behandlung von Schwachstellen		
15.	Europäische Norm(en) für die Behandlung von Schwachstellen bei Produkten mit digitalen Elementen	30.8.2026
Vertikale Normen für Sicherheitsanforderungen in Bezug auf die Eigenschaften von Produkten mit digitalen Elementen		
16.	Europäische Norm(en) für grundlegende Cybersicherheitsanforderungen an Identitätsmanagementsysteme und Software und Hardware für die Verwaltung des privilegierten Zugangs, auch Lesegeräte zur Authentifizierung und Zugangskontrolle, einschließlich biometrischer Lesegeräte	30.10.2026
17.	Europäische Norm(en) für grundlegende Cybersicherheitsanforderungen an eigenständige und eingebettete Browser	30.10.2026
18.	Europäische Norm(en) für grundlegende Cybersicherheitsanforderungen an Passwortmanager	30.10.2026
19.	Europäische Norm(en) für grundlegende Cybersicherheitsanforderungen an Software für die Suche, Entfernung und Quarantäne von Schadsoftware	30.10.2026
20.	Europäische Norm(en) für grundlegende Cybersicherheitsanforderungen an Produkte mit digitalen Elementen mit der Funktion eines virtuellen privaten Netzes (VPN)	30.10.2026

21.	Europäische Norm(en) für grundlegende Cybersicherheitsanforderungen an Netzmanagementsysteme	30.10.2026
22.	Europäische Norm(en) für grundlegende Cybersicherheitsanforderungen an Systeme für die Verwaltung von Sicherheitsinformationen und -ereignissen (SIEM)	30.10.2026
23.	Europäische Norm(en) für grundlegende Cybersicherheitsanforderungen an Bootmanager	30.10.2026
24.	Europäische Norm(en) über grundlegende Cybersicherheitsanforderungen an Software für Public-Key-Infrastrukturen und die Ausstellung digitaler Zertifikate	30.10.2026
25.	Europäische Norm(en) für grundlegende Cybersicherheitsanforderungen an Schnittstellen physischer und virtueller Netze	30.10.2026
26.	Europäische Norm(en) für grundlegende Cybersicherheitsanforderungen an Betriebssysteme	30.10.2026
27.	Europäische Norm(en) für grundlegende Cybersicherheitsanforderungen an Router, Modems für die Internetanbindung und Switches	30.10.2026
28.	Europäische Norm(en) für grundlegende Cybersicherheitsanforderungen an Mikroprozessoren mit sicherheitsbezogenen Funktionen	30.10.2026
29.	Europäische Norm(en) für grundlegende Cybersicherheitsanforderungen an Mikrocontroller mit sicherheitsbezogenen Funktionen	30.10.2026
30.	Europäische Norm(en) für grundlegende Cybersicherheitsanforderungen an anwendungsspezifische integrierte Schaltungen (ASICs) und für FPGAs (*Field Programmable Gate Arrays*) mit sicherheitsbezogenen Funktionen	30.10.2026
31.	Europäische Norm(en) für grundlegende Cybersicherheitsanforderungen an virtuelle Assistenten für die intelligente häusliche Umgebung mit allgemeinem Verwendungszweck	30.10.2026
32.	Europäische Norm(en) für grundlegende Cybersicherheitsanforderungen an intelligente Haushaltsgeräte mit Sicherheitsfunktionen, einschließlich intelligenter Türschlösser, Sicherheitskameras, Babyüberwachungssysteme und Alarmanlagen	30.10.2026

33.	Europäische Norm(en) für grundlegende Cybersicherheitsanforderungen an mit dem Internet verbundenes Spielzeug, das unter die Richtlinie 2009/48/EG fällt und Funktionen zur sozialen Interaktion (z. B. Sprechen oder Filmen) oder zur Ortung aufweist	30.10.2026
34.	Europäische Norm(en) für grundlegende Cybersicherheitsanforderungen an persönliche, am menschlichen Körper tragbare oder angebrachte Produkte, die zum Zwecke der Gesundheitsüberwachung (z. B. Tracking) bestimmt sind und nicht unter die Verordnung (EU) 2017/745 oder die Verordnung (EU) 2017/746 fallen, oder persönliche, am Körper tragbare Produkte, die für die Verwendung durch und für Kinder bestimmt sind	30.10.2026
35.	Europäische Norm(en) für grundlegende Cybersicherheitsanforderungen an Hypervisoren und Container-Runtime-Systeme, die eine virtualisierte Ausführung von Betriebssystemen und ähnlichen Umgebungen unterstützen	30.10.2026
36.	Europäische Norm(en) für grundlegende Cybersicherheitsanforderungen an Firewalls, Angriffserkennungs- und/oder -präventionssysteme, insbesondere einschließlich solcher für den industriellen Einsatz	30.10.2026
37.	Europäische Norm(en) für grundlegende Cybersicherheitsanforderungen an manipulationssichere Mikroprozessoren	30.10.2026
38.	Europäische Norm(en) für grundlegende Cybersicherheitsanforderungen an manipulationssichere Mikrocontroller	30.10.2026
39.	Europäische Norm(en) für grundlegende Cybersicherheitsanforderungen an Hardware-Geräte mit Sicherheitsboxen	30.10.2026
40.	Europäische Norm(en) für grundlegende Cybersicherheitsanforderungen an Smart-Meter-Gateways in intelligenten Messsystemen im Sinne des Artikels 2 Nummer 23 der Richtlinie (EU) 2019/944 des Europäischen Parlaments und des Rates und anderen Geräten für fortgeschrittene Sicherheitszwecke, einschließlich der sicheren Kryptoverarbeitung	30.10.2026
41.	Europäische Norm(en) für grundlegende Cybersicherheitsanforderungen an Chipkarten oder ähnliche Geräte, einschließlich Sicherheitselemente	30.10.2026

ANHANG II

Anforderungen an die europäischen Normen gemäß Artikel 1

1. Anforderungen an die in Auftrag gegebenen europäischen Normen

Ziele

Harmonisierte europäische Normen müssen dem allgemein anerkannten Stand der Technik[1] entsprechen, um die bei der Planung, Konzeption, Entwicklung, Herstellung, Lieferung und Wartung von Produkten mit digitalen Elementen auftretenden Cybersicherheitsrisiken zu minimieren, um so Sicherheitsvorfälle zu verhindern und die Auswirkungen solcher Vorfälle, auch in Bezug auf die Gesundheit und Sicherheit der Nutzer, so gering wie möglich zu halten.

Harmonisierte europäische Normen müssen im erforderlichen Umfang und unter Berücksichtigung des Stands der Technik technologie-, prozess- oder methodengestützte technische Spezifikationen für die Konzeption und Entwicklung von Produkten mit digitalen Elementen, einschließlich Bewertungsverfahren (auch für Erprobung und Überprüfung), sowie objektiv nachprüfbare Kriterien und praktikable Methoden zur Bewertung der Einhaltung dieser Spezifikationen enthalten.

Unterstützende Spezifikationen oder andere Normungsunterlagen (z. B. in Bezug auf Terminologie[2]) sind zu ermitteln und vorzulegen, wenn dies für die Kohärenz und Umsetzung der europäischen Normen nötig ist. Solche unterstützenden Spezifikationen können auch Elemente umfassen, die für die horizontalen und vertikalen Normen nützlich sind, wie z. B. Kataloge von Sicherheitskontrollen, Bedrohungen, Schwachstellen, Angriffsmethoden, Spezifikationen für die Kommunikation und Anweisungen an die Nutzer sowie Bestimmungen zur Barrierefreiheit.

Kohärenz

Unbeschadet erforderlicher Verbesserungen sollten die aufgrund dieses Auftrags entwickelten harmonisierten Normen auf den laufenden Arbeiten zur Unterstützung der Delegierten Verordnung (EU) 2022/30 der Kommission[3] aufbauen. Auf die Besonderheiten der Verordnung (EU) 2024/2847[4] muss jedoch in der Entwicklungsphase umfassend eingegangen werden. Soweit möglich, können CEN, Cenelec und ETSI bereits bestehende Normen und Normungsunterlagen überarbeiten, um sie an die Anforderungen der Cyberresilienz-Verordnung anzupassen.

---

1 Stand der Technik bedeutet nicht unbedingt, dass es sich um Ergebnisse der neuesten wissenschaftlichen Forschung handelt, die sich noch im Versuchsstadium befinden oder technologisch noch nicht ausgereift sind. Der Stand der Technik ist nicht als eine Mindestanforderung für den Marktzugang zu verstehen.

2 Alle auf der Grundlage dieses Auftrags erarbeiteten europäischen Normen müssen auf einer einheitlichen Terminologie beruhen. Außerdem müssen die unterstützenden Spezifikationen zur Terminologie so weit wie möglich auf der auf internationaler Ebene und insbesondere in internationalen Normen festgelegten Terminologie aufbauen.

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

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

Unbeschadet erforderlicher Verbesserungen stellen CEN, Cenelec und ETSI sicher, dass die aufgestellten europäischen Normen gegebenenfalls mit anderen europäischen und harmonisierten Normen, die in den verschiedenen einschlägigen Sektoren entwickelt wurden oder werden, im Einklang stehen, insbesondere mit denjenigen, die sich auf Produkte beziehen, die unter EU-Rechtsvorschriften wie die Richtlinie 2006/42/EG des Europäischen Parlaments und des Rates[5], die Verordnungen (EU) 2023/1230[6], (EU) 2024/1689[7], (EU) 2023/1781[8] oder unter die gemäß der Verordnung (EU) 2019/881 des Europäischen Parlaments und des Rates[9] entwickelten oder in Entwicklung befindlichen EU-Systeme für die Cybersicherheitszertifizierung fallen. Darüber hinaus sollten CEN, Cenelec und ETSI sicherstellen, dass die aufgrund dieses Beschlusses aufgestellten harmonisierten Normen mit den Verpflichtungen der Union aus internationalen Übereinkünften und Verträgen im Einklang stehen.

Anwendungsbereich der europäischen Normen

In jeder harmonisierten europäischen Norm müssen ihr Anwendungsbereich und die in ihren Anwendungsbereich fallenden Produkte eindeutig angegeben werden, und es ist aufzuführen, welche Risiken abgedeckt werden und welche anderen einschlägigen Risiken nicht abgedeckt werden. Wenn eine harmonisierte europäische Norm nicht alle grundlegenden Anforderungen an die in ihren Anwendungsbereich fallenden Produkte abdeckt, so sind in der Norm die nicht vollständig abgedeckten grundlegenden Anforderungen anzugeben. Wenn eine harmonisierte europäische Norm die nach einer umfassenden Analyse ermittelten Risiken, die sich auf eine der grundlegenden Anforderungen beziehen, die sie abdecken soll und die für die in ihren Anwendungsbereich fallenden Produkte gelten, nicht mindert, so sind die mit dieser Norm die nicht geminderten Risiken anzugeben und es sind soweit möglich nichtnormative Informationen darüber zu geben, wie diesen Risiken auf andere Weise begegnet werden könnte.

Die in Auftrag gegebenen harmonisierten Normen müssen zumindest Bestimmungen in Bezug auf die Definition der Sicherheitsprobleme, die Sicherheitsziele, die technischen Spezifikationen der Sicherheitsanforderungen und die Bewertungsmethode enthalten.

---

5 Richtlinie 2006/42/EG des Europäischen Parlaments und des Rates vom 17. Mai 2006 über Maschinen und zur Änderung der Richtlinie 95/16/EG (ABl. L 157 vom 9.6.2006, S. 24, ELI: http://data.europa.eu/eli/dir/2006/42/oj).

6 Verordnung (EU) 2023/1230 des Europäischen Parlaments und des Rates vom 14. Juni 2023 über Maschinen und zur Aufhebung der Richtlinie 2006/42/EG des Europäischen Parlaments und des Rates und der Richtlinie 73/361/EWG des Rates (ABl. L 165 vom 29.6.2023, S. 1, ELI: http://data.europa.eu/eli/reg/2023/1230/oj).

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

8 Verordnung (EU) 2023/1781 des Europäischen Parlaments und des Rates vom 13. September 2023 zur Schaffung eines Rahmens für Maßnahmen zur Stärkung des europäischen Halbleiter-Ökosystems und zur Änderung der Verordnung (EU) 2021/694 (Chip-Gesetz) (ABl. L 229 vom 18.9.2023, S. 1, ELI: http://data.europa.eu/eli/reg/2023/1781/oj).

9 Verordnung (EU) 2019/881 des Europäischen Parlaments und des Rates vom 17. April 2019 über die ENISA (Agentur der Europäischen Union für Cybersicherheit) und über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik und zur Aufhebung der Verordnung (EU) Nr. 526/2013 (Rechtsakt zur Cybersicherheit) (ABl. L 151 vom 7.6.2019, S. 15, ELI: http://data.europa.eu/eli/reg/2019/881/oj).

Hinsichtlich der Definition der Sicherheitsprobleme müssen die in Auftrag gegebenen harmonisierten Normen in Bezug auf die von ihnen abgedeckten Bedrohungen und die Konzepte und Annahmen, auf denen sie beruhen, transparent sein und den Herstellern bei der Ermittlung und Spezifizierung von Bedrohungen, Konzepten und Annahmen nützlich sein. Dies kann beispielsweise durch die Entwicklung von neuen oder Bezugnahme auf bestehende Kataloge von Sicherheitskontrollen, Bedrohungen, Angriffsmethoden und Schwachstellen sowie durch eine Diskussion über angemessene Annahmen erreicht werden.

In den Sicherheitszielen werden der Anwendungsbereich des Zielprodukts oder -dienstes und die Sicherheitseigenschaften, denen entsprochen werden soll, ausgehend von den grundlegenden Anforderungen der Cyberresilienz-Verordnung festgelegt. In den normativen Aussagen der harmonisierten Norm müssen die beabsichtigten Lösungen für die ermittelten Risiken (Sicherheitsprobleme) präzise formuliert werden. Die Methode zur Ermittlung der Sicherheitsziele beruht auf bestehenden Normen für die Festlegung von Ansätzen für die Risikoanalyse. Es wird erwartet, dass aus den harmonisierten Normen der Zusammenhang zwischen den Sicherheitszielen und den ermittelten Risiken (Sicherheitsproblemen) ersichtlich wird.

In der Spezifikation der Sicherheitsanforderungen ist das erwünschte Cybersicherheitsverhalten zu beschrieben, das für das Zielprodukt oder den Zieldienst erwartet wird. Soweit möglich, müssen die Normen eine Vielzahl von Sicherheitsniveaus abdecken, die den verschiedenen erwarteten Marktbedürfnissen Rechnung tragen, z. B. unterschiedliche Zweckbestimmungen, Betriebsumgebungen oder Nutzerkategorien (z. B. Verbraucher, Unternehmen, kritische Einrichtungen).

Die Bewertungsmethode besteht aus einer Reihe von Bewertungsverfahren, die erforderlich sind, um das Ziel anhand der zuvor festgelegten Anforderungen der technischen Spezifikationen zu bewerten. Darin wird festgelegt, wie das Ziel bewertet werden soll, um das erforderliche Sicherheitsniveau nachzuweisen. Sie umfasst zumindest die Begriffsbestimmung der Bewertungsmethodik und der Zusammensetzungsmethodik (falls zutreffend) und die Festlegung der erwarteten Bewertungsergebnisse.

Alle mit diesem Beschluss in Auftrag gegebenen harmonisierten europäischen Normen werden so ausgearbeitet, dass sie leicht im *Amtsblatt der Europäischen Union* veröffentlicht werden können.

2. Anforderungen an einzelne europäische Normen

2.1 Horizontale Cybersicherheitsnormen in Bezug auf die Eigenschaften von Produkten mit digitalen Elementen (Anhang I Einträge 1-14)

Durch die Entwicklung horizontaler harmonisierter Normen zu verschiedenen Aspekten und Mechanismen der Cybersicherheit von Produkten wird i) die Entwicklung weiterer detaillierter vertikaler harmonisierter Normen für bestimmte Produkte oder Produktarten unterstützt und es werden ii) die Hersteller bei der Festlegung und Umsetzung der für ihre jeweiligen Produkte geltenden Sicherheitsanforderungen unterstützt, insbesondere für Produkte, die von keinen bestehenden oder geplanten vertikalen Normen erfasst werden. Abweichungen von den horizontalen harmonisierten Normen müssen hinreichend begründet werden.

Die harmonisierten europäischen Normen für die Konzeption, Entwicklung und Herstellung von Produkten mit digitalen Elementen, die angesichts der Risiken ein angemessenes Cybersicherheitsniveau gewährleisten (Anhang I Eintrag 1), dienen als Rahmen für alle in Abschnitt 1 dieses Anhangs festgelegten Elemente und geben die wichtigsten Elemente vor,

die in anderen Produktsicherheitsnormen für die Zwecke der Cyberresilienz-Verordnung enthalten sein müssen.

Anstatt sich nur auf die gemeinsamen Mindestaspekte zu konzentrieren, sollen die horizontalen harmonisierten Normen einen umfassenden und nützlichen Überblick über die einschlägigen Sicherheitsmechanismen bieten, die für Produkte gelten können, die in den Anwendungsbereich der Cyberresilienz-Verordnung fallen. Alle in Auftrag gegebenen harmonisierten europäischen Normen müssen – soweit zutreffend – Bestimmungen über die sichere Softwareentwicklung enthalten. Aus der Norm muss daher eindeutig hervorgehen, welchen Anwendungsbereich jede normative Aussage hat.

Bei der Betrachtung, welche Produkte für die Zwecke der Entwicklung horizontaler Normen in den Anwendungsbereich der Cyberresilienz-Verordnung fallen, berücksichtigen CEN, Cenelec und ETSI gegebenenfalls, dass die in Anhang I der vorgeschlagenen Cyberresilienz-Verordnung festgelegten grundlegenden Anforderungen für Produkte mit digitalen Elementen gelten werden, die auch in den Anwendungsbereich anderer Rechtsvorschriften der Union fallen, wie z. B. elektronische Patientendatensysteme, Hochrisiko-KI-Systeme gemäß der Verordnung (EU) 2024/1689, Maschinenprodukte gemäß der Richtlinie 2006/42/EG des Europäischen Parlaments und des Rates und der Verordnung (EU) 2023/1230 oder vertrauenswürdige Chips gemäß der Verordnung (EU) 2023/1781.

2.2 Anforderungen an die Behandlung von Schwachstellen bei Produkten mit digitalen Elementen (Anhang I Eintrag 15)

Harmonisierte europäische Normen für Anforderungen an die Handhabung von Schwachstellen müssen Spezifikationen für Verfahren zur Behandlung von Schwachstellen enthalten, die alle relevanten Produktkategorien abdecken und von den Herstellern der Produkte mit digitalen Elementen einzuführen sind. Solche Verfahren müssen es dem Hersteller ermöglichen,

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

b) im Hinblick auf die Risiken im Zusammenhang mit den Produkten mit digitalen Elementen unverzüglich Schwachstellen zu behandeln und zu beheben, unter anderem durch Bereitstellung von Sicherheitsaktualisierungen; soweit technisch machbar, müssen neue Sicherheitsaktualisierungen getrennt von den Funktionsaktualisierungen bereitgestellt werden;

c) die Sicherheit des Produkts mit digitalen Elementen regelmäßig und wirksam zu testen und zu überprüfen;

d) sobald eine Sicherheitsaktualisierung bereitgestellt worden ist, Informationen über beseitigte Schwachstellen zu teilen und zu veröffentlichen, einschließlich einer Beschreibung der Schwachstellen mit Angaben, anhand deren die Nutzer das betroffene Produkt mit digitalen Elementen, die Auswirkungen der Schwachstellen und ihre Schwere erkennen können, sowie eindeutige und verständliche Informationen, die den Nutzern helfen, die Schwachstellen zu beheben; in hinreichend begründeten Fällen, in denen die Hersteller der Auffassung sind, dass die Risiken der Veröffentlichung die Vorteile in Bezug auf die Sicherheit überwiegen, können sie die Veröffentlichung von Informationen über eine behobene Schwachstelle so lange aufschieben, bis den Nutzern die Möglichkeit gegeben wurde, den entsprechenden Patch anzuwenden;

e) eine Strategie für die koordinierte Offenlegung von Schwachstellen aufzustellen und umzusetzen;

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

g) Mechanismen für die sichere Verbreitung von Aktualisierungen für Produkte mit digitalen Elementen bereitzustellen, damit Schwachstellen rechtzeitig und im Falle von Sicherheitsaktualisierungen gegebenenfalls automatisch behoben oder eingedämmt werden;

h) dafür zu sorgen, dass Sicherheitsaktualisierungen, die zur Bewältigung festgestellter Sicherheitsprobleme zur Verfügung stehen, unverzüglich und – sofern zwischen Hersteller und gewerblichem Nutzer in Bezug auf ein maßgeschneidertes Produkt mit digitalen Elementen nichts anderes vereinbart wurde – kostenlos verbreitet werden, zusammen mit Hinweisen und einschlägigen Informationen, auch über zu treffende mögliche Maßnahmen.

2.3 Vertikale Cybersicherheitsnormen in Bezug auf die Eigenschaften von Produkten mit digitalen Elementen (Anhang I Einträge 16-41)

Vertikale harmonisierte europäische Normen in Bezug auf die Eigenschaften von Produkten mit digitalen Elementen müssen Spezifikationen für die Cybersicherheitsanforderungen wichtiger oder kritischer Produkte im Sinne der Anhänge III und IV der Cyberresilienz-Verordnung enthalten.

Vertikale harmonisierte Normen dienen der Umsetzung und Weiterentwicklung der Bestimmungen der in Auftrag gegebenen horizontalen Normen, die in Anhang I Einträge 1 bis 15 aufgeführt sind, wobei auch relevante Unterschiede zu berücksichtigen sind, die sich aus der Zweckbestimmung und der vernünftigerweise vorhersehbaren Verwendung ergeben. In Anbetracht der zeitlichen Planung für die verschiedenen Normungsunterlagen müssen vertikale Normen mit der horizontalen Norm für die Konzeption, Entwicklung und Herstellung von Produkten mit digitalen Elementen, die angesichts der Risiken ein angemessenes Cybersicherheitsniveau gewährleisten (Anhang I Eintrag 1), und gegebenenfalls auch mit der horizontalen Norm für die Behandlung von Schwachstellen bei Produkten mit digitalen Elementen (Anhang I Eintrag 15) vereinbar sein. Das Ziel der Abstimmung der vertikalen Normen mit den in Anhang I Einträge 2 bis 14 aufgeführten horizontalen Normen ist dabei ebenfalls zu berücksichtigen, weil erwartet wird, dass sich die Normen im Laufe der Zeit im regelmäßigen Überprüfungsverfahren annähern werden.

Bei den Produkten, die unter Anhang IV der Cyberresilienz-Verordnung fallen und für die es technische Bereiche oder Schutzprofile gibt, sind in den aufgestellten harmonisierten Normen die bestehenden europäischen Systeme für die Cybersicherheitszertifizierung zu berücksichtigen die im Rahmen der Verordnung (EU) 2019/881 entwickelt wurden oder werden, insbesondere das auf den Gemeinsamen Kriterien beruhende europäische System für die Cybersicherheitszertifizierung (EUCC).

Die im Rahmen dieses Auftrags entwickelten vertikalen harmonisierten Normen (Anhang I Einträge 16-41), die speziell Produkte betreffen, die einer Konformitätsbewertung durch Dritte unterliegen (wichtige oder kritische Produkte), müssen einem risikobasierten Sicherungsansatz entsprechen, sodass Anwendungsfälle mit niedrigerem Risiko nur einem

Validierungsverfahren unterliegen können, wogegen Anwendungsfälle mit höherem Risiko (in zunehmendem Maße) einem strengeren Überprüfungsverfahren unterzogen werden.

Solche harmonisierten europäischen Normen müssen die einschlägigen Risiken, die für eine bestimmte Zweckbestimmung oder eine bestimmte nach vernünftigem Ermessen vorhersehbare Verwendung ermittelt wurden, angemessen abdecken und daher auf einer umfassenden Risikoanalyse beruhen, die bei der Entwicklung jeder harmonisierten Norm durchzuführen ist.

Außerdem kann durch die Entwicklung vertikaler harmonisierter Normen, die eine breite Palette von Produkten oder Produktkategorien (z. B. operative Technik) betreffen, auch die strukturierte und kohärente Entwicklung produktspezifischer vertikaler harmonisierter Normen im Rahmen dieses Auftrags unterstützt und erleichtert werden, sofern keine Unklarheiten hinsichtlich der Anforderungen, des Anwendungsbereichs, der abgedeckten Risiken und der nicht abgedeckten Risiken bestehen. Solche breit angelegten vertikalen harmonisierten Normen müssen die mit einer bestimmten Zweckbestimmung und einer bestimmten vernünftigerweise vorhersehbaren Verwendung verbundenen Risiken zumindest teilweise abdecken und müssen durch weitere, detailliertere und produktspezifische harmonisierte Normen ergänzt werden, damit eine Konformitätsvermutung für eine begrenztere Produktdefinition begründet werden kann, wobei die zusätzlichen oder besonderen Risiken im Zusammenhang mit diesen Produkten und ihren einschlägigen Zweckbestimmungen und vernünftigerweise vorhersehbaren Verwendungen abgedeckt sein müssen.