Rat der
Europäischen Union

Brüssel, den 29. Mai 2018
(OR. en)

9350/18

Interinstitutionelles Dossier:
2017/0225 (COD)

CYBER 115
TELECOM 152
CODEC 860
COPEN 163
COPS 175
COSI 129
CSC 170
CSCI 80
IND 143
JAI 514
JAIEX 55
POLMIL 61
RELEX 463

VERMERK

Absender:	Vorsitz
Empfänger:	Rat
Nr. Vordok.:	8834/18
Nr. Komm.dok.:	12183/17
Betr.:	Vorschlag für eine VERORDNUNG DES EUROPÄISCHEN PARLAMENTS UND DES RATES über die "EU-Cybersicherheitsagentur" (ENISA) und zur Aufhebung der Verordnung (EU) Nr. 526/2013 sowie über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik ("Rechtsakt zur Cybersicherheit") - Allgemeine Ausrichtung

I. EINLEITUNG

1. Am 13. September 2017 hat die Kommission im Rahmen ihrer Strategie für einen digitalen Binnenmarkt den oben genannten Vorschlag[1], dessen Rechtsgrundlage Artikel 114 AEUV ist, angenommen und dem Rat und dem Europäischen Parlament zugeleitet. Als Teil des sogenannten 'Cybersicherheitspakets' zielt dieser Vorschlag auf ein hohes Niveau an Cybersicherheit, Widerstandsfähigkeit gegen Cyberangriffe und Vertrauen in der Union ab, wodurch das reibungslose Funktionieren des Binnenmarktes gewährleistet werden soll.

2. Im Verordnungsvorschlag werden die Ziele, Aufgaben und organisatorischen Aspekte der ENISA, der EU-Agentur für die Cybersicherheit, festgelegt und wird ein Rahmen für die Einführung von europäischen Systemen für die Cybersicherheitszertifizierung geschaffen, um ein angemessenes Cybersicherheitsniveau von IKT-Produkten und -Diensten in der Union zu gewährleisten. Der Kommissionsvorschlag ist mit einer Folgenabschätzung versehen, in dem bestimmte Politikoptionen, und zwar acht an der Zahl, untersucht werden, die sich auf die Überprüfung der ENISA und die IKT-Cybersicherheitszertifizierung beziehen.

3. Der Verordnungsvorschlag enthält zwei wichtige Komponenten:

   - ein ständiges Mandat für die Agentur mit einem abgegrenzten Aufgabenbereich im Hinblick auf die Erfordernisse im Rahmen der neuen politischen Prioritäten und Instrumente und erneuerte Aufgaben und Funktionen der Agentur, die ermöglichen sollen, dass die Anstrengungen der Mitgliedstaaten, der EU-Organe und anderer Interessenträger in Bezug auf die Gewährleistung eines sicheren Cyberraum wirksam und effizient unterstützt werden ;

   - einen europäischen Rahmen für die Cybersicherheitszertifizierung für IKT-Produkte und -Dienste und Regeln für die europäischen Systeme für die Cybersicherheitszertifizierung, aufgrund deren im Rahmen dieser Systeme ausgestellte Zertifikate in allen Mitgliedstaaten gelten und anerkannt werden und mit denen die derzeitige Marktfragmentierung angegangen wird.

[1] Dokumente 12183/17, 12183/1/17 REV 1 und 12183/2/17 REV 2.

4. Im Oktober 2017 hat der Europäische Rat[2] gefordert, dass die Vorschläge der Kommission zur Cybersicherheit ganzheitlich gestaltet, rechtzeitig vorgelegt und unverzüglich geprüft werden, und zwar auf der Grundlage eines vom Rat zu erstellenden Aktionsplans.

5. Am 12. Dezember 2017 hat der Rat (Allgemeine Angelegenheiten) den Aktionsplan[3] zur Umsetzung der Schlussfolgerungen des Rates[4] zur Gemeinsamen Mitteilung[5] an das Europäische Parlament und den Rat: "Abwehrfähigkeit, Abschreckung und Abwehr: die Cybersicherheit in der EU wirksam erhöhen" angenommen. Der Aktionsplan macht deutlich, dass der Rat bis Juni 2018 eine allgemeine Ausrichtung zu dem Vorschlag erreichen will.

6. Im Europäischen Parlament wurde Angelika NIEBLER (ITRE, EVP) zur Berichterstatterin ernannt. Die Abstimmung im ITRE-Ausschuss ist für den 19. Juni 2018 geplant.

7. Der Europäische Wirtschafts- und Sozialausschuss hat seine Stellungnahme am 14. Februar 2018 angenommen.

II. BERATUNGEN IM RAT

8. Die Kommission hat der horizontalen Gruppe "Fragen des Cyberraums" (im Folgenden "Gruppe") diesen Vorschlag und die dazugehörige Folgenabschätzung am 26. September 2017 erläutert; daraufhin wurde die Folgenabschätzung in der Sitzung der Gruppe vom 20. Oktober 2017 geprüft. Die späteren Beratungen konzentrierten sich auf die operative Leistungsfähigkeit der Agentur und ihren Spielraum für Interaktionen mit den zuständigen nationalen Behörden sowie auf die Auswirkungen des Zertifizierungsrahmens auf den Markt und die Wettbewerbsfähigkeit der Unternehmen. Im Allgemeinen wurden die Folgenabschätzung und der Vorschlag von den Delegationen positiv aufgenommen.

---

2 EUCO 14/17, Nummer 11.
3 Dok. 15748/17.
4 Dok. 14435/17.
5 Dok. 12211/17.

9. Die Gruppe hat im November 2017 unter dem estnischen Vorsitz mit der Erörterung des Vorschlags selbst begonnen und diese unter dem bulgarischen Vorsitz fortgesetzt. Zu diesem Vorschlag wurden 12 Sitzungen abgehalten, aus denen nacheinander acht überarbeitete Fassungen des Vorschlags hervorgingen; angestrebt wird eine Einigung über eine allgemeine Ausrichtung auf der Tagung des TTE-Rates (Telekommunikation) am 8. Juni 2018.

10. Die Beratungsergebnisse der Gruppe vom 14./15. Mai 2018 sowie der überarbeitete Kompromisstext des Vorsitzes sind in der Anlage enthalten. Die Erwägungsgründe wurden an die Änderungen im verfügenden Teil angepasst. Änderungen gegenüber dem Kommissionsvorschlag sind durch **Fettdruck** oder [...] gekennzeichnet. Die Änderungen gegenüber dem letzten Dokument der Gruppe (8834/18) sind in der englischen Fassung durch **Fettdruck und Unterstreichung** und alle Streichungen durch **[...]** gekennzeichnet.

III. FAZIT

11. Im beiliegenden Kompromisstext des Vorsitzes kommt das Bemühen des Vorsitzes und der Mitgliedstaaten um einen ausgewogenen Text zum Ausdruck.

12. Am 25. Mai 2018 hat der Ausschuss der Ständigen Vertreter Einvernehmen über den Kompromisstext des Vorsitzes mit der Maßgabe erzielt, dass Artikel 19 Absatz 5 und Artikel 48 Absatz 5 gemäß der Anlage geändert werden.

13. Der Rat wird daher ersucht, auf seiner Tagung am 8. Juni 2018 eine allgemeine Ausrichtung festzulegen und den Vorsitz zu beauftragen, Verhandlungen mit den Vertretern des Europäischen Parlaments und der Europäischen Kommission Verhandlungen über dieses Dossier aufzunehmen.

ANLAGE

Vorschlag für eine

VERORDNUNG DES EUROPÄISCHEN PARLAMENTS UND DES RATES

über die "*[...] Agentur der Europäischen Union für Cybersicherheit*" (ENISA) und zur Aufhebung der Verordnung (EU) Nr. 526/2013 sowie über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik ("Rechtsakt zur Cybersicherheit")

(Text von Bedeutung für den EWR)

DAS EUROPÄISCHE PARLAMENT UND DER RAT DER EUROPÄISCHEN UNION –

gestützt auf den Vertrag über die Arbeitsweise der Europäischen Union, insbesondere auf Artikel 114,

auf Vorschlag der Europäischen Kommission,

nach Zuleitung des Entwurfs des Gesetzgebungsakts an die nationalen Parlamente,

nach Stellungnahme des Europäischen Wirtschafts- und Sozialausschusses[6],

nach Stellungnahme des Ausschusses der Regionen[7],

gemäß dem ordentlichen Gesetzgebungsverfahren,

---

[6] ABl. C [...] vom [...], S. [...].
[7] ABl. C [...] vom [...], S. [...].

in Erwägung nachstehender Gründe:

(1) Netz- und Informationssysteme sowie Telekommunikationsnetze und -dienste spielen eine lebenswichtige Rolle für die Gesellschaft und sind mittlerweile zum Hauptmotor des Wirtschaftswachstums geworden. Die Informations- und Kommunikationstechnik bildet das Rückgrat der komplexen Systeme, die gesellschaftliche Tätigkeiten unterstützen und unsere Volkswirtschaften in Schlüsselsektoren wie Gesundheit, Energie, Finanzen und Verkehr aufrechterhalten und die insbesondere dafür sorgen, dass der Binnenmarkt reibungslos funktioniert.

(2) Die Nutzung von Netz- und Informationssystemen durch Bürger, Unternehmen und Behörden ist mittlerweile in der Union allgegenwärtig. Digitalisierung und Konnektivität entwickeln sich zu Kernmerkmalen einer ständig steigenden Zahl von Produkten und Dienstleistungen. Mit dem Aufkommen des Internets der Dinge dürften in den nächsten Jahrzehnten Millionen, wenn nicht Milliarden vernetzte digitale Geräte unionsweit Verbreitung finden. Zwar sind immer mehr Geräte mit dem Internet vernetzt, doch verfügen sie über eine nur unzureichende Cybersicherheit, da die Sicherheit und Abwehrfähigkeit dieser Geräte schon bei der Konzeption nicht ausreichend berücksichtigt wurden. Vor diesem Hintergrund führt die geringe Zertifizierung dazu, dass Personen, die IKT-Produkte und -Dienste für unternehmerische oder private Zwecke nutzen, nur unzureichend über deren Cybersicherheitsmerkmale informiert werden, wodurch das Vertrauen in digitale Lösungen untergraben wird.

(3) Mit der zunehmenden Digitalisierung und Vernetzung steigen auch die Cybersicherheitsrisiken, wodurch die Gesellschaft insgesamt anfälliger für Cyberbedrohungen wird und die Gefahren zunehmen, denen Privatpersonen und insbesondere schutzbedürftige Personengruppen wie Kinder ausgesetzt sind. Um dieser Gefahr für die Gesellschaft zu begegnen, gilt es alle für die Erhöhung der Cybersicherheit in der EU notwendigen Maßnahmen zu ergreifen, um die Netz- und Informationssysteme, die Telekommunikationsnetze und die digitalen Produkte, Dienste und Geräte, die von Privatpersonen, Behörden und Unternehmen – von KMU bis zu Betreibern kritischer Infrastrukturen – genutzt werden, vor Cyberbedrohungen zu schützen.

(4) Cyberangriffe nehmen zu und eine Wirtschaft und Gesellschaft, die durch ihre Vernetzung anfälliger für Cyberbedrohungen und -angriffe ist, benötigt daher einen stärkeren Schutz. Auf die häufig grenzüberschreitenden Cyberangriffe reagieren die für die Cybersicherheit zuständigen Behörden jedoch vor allem mit nationalen Strategien, zumal die Zuständigkeiten für die Strafverfolgung an den nationalen Grenzen enden. Cybersicherheitsvorfälle großen Ausmaßes könnten die Bereitstellung wesentlicher Dienste in der gesamten EU empfindlich stören. Vonnöten sind daher effektive Maßnahmen und ein Krisenmanagement auf EU-Ebene, gestützt auf gezielte Strategien, sowie ein breiter angelegtes Instrumentarium für eine europäische Solidarität und gegenseitige Hilfe. Zudem sind eine auf zuverlässigen Daten der Union basierende regelmäßige Überprüfung des Stands der Cybersicherheit und Abwehrfähigkeit in der Union sowie eine systematische Prognose künftiger Entwicklungen, Herausforderungen und Bedrohungen – sowohl auf Unionsebene als auch auf globaler Ebene – für die Entscheidungsträger, die Branche und die Nutzer daher gleichermaßen wichtig.

(5) Angesichts immer größerer Herausforderungen, die sich der Union im Bereich der Cybersicherheit stellen, bedarf es eines umfassenden Maßnahmenpakets, das auf den bisherigen Maßnahmen der Union aufbaut und sich wechselseitig verstärkende Ziele unterstützt. Dies beinhaltet eine weitere Stärkung der Fähigkeiten und der Abwehrbereitschaft der Mitgliedstaaten und Unternehmen sowie eine bessere Zusammenarbeit und Koordinierung zwischen den Mitgliedstaaten und den Organen, Einrichtungen und Stellen der EU. Da Cyberbedrohungen an keinen Grenzen Halt machen, gilt es zudem, die Fähigkeiten auf Unionsebene zu stärken, die einzelstaatliche Maßnahmen vor allem dann ergänzen könnten, wenn es sich um grenzüberschreitende Cybersicherheitsvorfälle und -krisen von großem Ausmaß handelt. Darüber hinaus sind weitere Anstrengungen notwendig, um die Bürgerinnen und Bürger sowie die Unternehmen für Fragen der Cybersicherheit zu sensibilisieren. Ferner ließe sich das Vertrauen in den digitalen Binnenmarkt weiter erhöhen, wenn transparente Informationen über das Niveau der Sicherheit von IKT-Produkten und -Diensten zur Verfügung stünden. Erleichtert werden kann dies durch eine Zertifizierung, für die über nationale Märkte und Sektoren hinaus unionsweit einheitliche Anforderungen und Bewertungskriterien für die Cybersicherheit festgelegt werden.

(6) Im Jahr 2004 verabschiedeten das Europäische Parlament und der Rat die Verordnung (EG) Nr. 460/2004[8] zur Errichtung der ENISA als Beitrag zu den Zielen, innerhalb der Union eine hohe und effektive Netz- und Informationssicherheit zu gewährleisten und eine Kultur der Netz- und Informationssicherheit zu entwickeln, die Bürgern, Verbrauchern, Unternehmen und Behörden zugute kommt. Durch die im Jahr 2008 vom Europäischen Parlament und vom Rat erlassene Verordnung (EG) Nr. 1007/2008[9] wurde das Mandat der Agentur bis März 2012 verlängert. Durch die Verordnung (EG) Nr. 580/2011[10] wurde das Mandat der Agentur nochmals bis zum 13. September 2013 verlängert. Im Jahr 2013 erließen das Europäische Parlament und der Rat die Verordnung (EU) Nr. 526/2013[11] über die Agentur der Europäischen Union für Netz- und Informationssicherheit (ENISA) und zur Aufhebung der Verordnung (EG) Nr. 460/2004, mit der das Mandat der Agentur bis zum Juni 2020 verlängert wurde.

---

8 Verordnung (EG) Nr. 460/2004 des Europäischen Parlaments und des Rates vom 10. März 2004 zur Errichtung der Europäischen Agentur für Netz- und Informationssicherheit (ABl. L 77 vom 13.3.2004, S. 1).

9 Verordnung (EG) Nr. 1007/2008 des Europäischen Parlaments und des Rates vom 24. September 2008 zur Änderung der Verordnung (EG) Nr. 460/2004 zur Errichtung der Europäischen Agentur für Netz- und Informationssicherheit bezüglich deren Bestehensdauer (ABl. L 293 vom 31.10.2008, S. 1).

10 Verordnung (EG) Nr. 580/2011 des Europäischen Parlaments und des Rates vom 8. Juni 2011 zur Änderung der Verordnung (EG) Nr. 460/2004 zur Errichtung der Europäischen Agentur für Netz- und Informationssicherheit bezüglich deren Bestehensdauer (ABl. L 165 vom 24.6.2011, S. 3).

11 Verordnung (EU) Nr. 526/2013 des Europäischen Parlaments und des Rates vom 21. Mai 2013 über die Agentur der Europäischen Union für Netz- und Informationssicherheit (ENISA) und zur Aufhebung der Verordnung (EG) Nr. 460/2004 (ABl. L 165 vom 18.6.2013, S. 41).

(7) Europa hat bereits wichtige Maßnahmen ergriffen, um die Cybersicherheit zu gewährleisten und das Vertrauen in die digitale Technik zu stärken. Im Jahr 2013 wurde eine EU-Cybersicherheitsstrategie verabschiedet, die der Union als Orientierung für strategische Reaktionen auf Cybersicherheitsbedrohungen und -risiken dienen soll. Im Zuge ihrer Bemühungen, den Online-Schutz der Europäerinnen und Europäer zu erhöhen, verabschiedete die Union im Jahr 2016 mit der Richtlinie (EU) 2016/1148 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union den ersten Rechtsakt auf dem Gebiet der Cybersicherheit (im Folgenden die "NIS-Richtlinie"). Mit der NIS-Richtlinie wurden Anforderungen an die nationalen Fähigkeiten im Bereich der Cybersicherheit sowie erstmals Mechanismen zur Stärkung der strategischen und operativen Zusammenarbeit zwischen den Mitgliedstaaten festgelegt sowie Verpflichtungen in Bezug auf die Sicherheitsmaßnahmen und die Meldung von Sicherheitsvorfällen für die Sektoren, die für die Wirtschaft und Gesellschaft lebenswichtig sind (Energie, Verkehr, Wasserwirtschaft, Bankwesen, Finanzmarktinfrastrukturen, Gesundheit, digitale Infrastrukturen) sowie für Anbieter zentraler digitaler Dienste (Suchmaschinen, Cloud-Computing-Dienste und Online-Marktplätze) eingeführt. Eine zentrale Aufgabe bei der Umsetzung dieser Richtlinie wurde dabei der ENISA zugewiesen. Darüber hinaus ist die wirksame Bekämpfung der Cyberkriminalität als ein Aspekt bei der Verfolgung des übergeordneten Ziels einer hohen Cybersicherheit ein wichtiger Schwerpunkt der Europäischen Sicherheitsagenda.

(8) Seit der Verabschiedung der EU-Cybersicherheitsstrategie im Jahr 2013 und der letzten Überarbeitung des Mandats der Agentur hat sich der gesamtpolitische Rahmen deutlich verändert, auch in Bezug auf die größeren Unwägbarkeiten und die geringere Sicherheit im globalen Umfeld. Vor diesem Hintergrund und angesichts der neuen Unionspolitik im Bereich der Cybersicherheit muss das Mandat der ENISA im Hinblick auf ihre neue Rolle in dem veränderten Cybersicherheitsökosystem überarbeitet werden, damit sie die Union wirksam darin unterstützen kann, auf die Herausforderungen im Bereich der Cybersicherheit zu reagieren, die sich aus dieser grundlegend veränderten Bedrohungslandschaft ergeben und für die, wie in der Bewertung der Agentur bestätigt, das laufende Mandat nicht ausreicht.

(9) Die mit dieser Verordnung errichtete Agentur sollte Rechtsnachfolgerin der durch die Verordnung (EG) Nr. 526/2013 errichteten ENISA sein. Die Agentur sollte die Aufgaben wahrnehmen, die ihr mit dieser Verordnung und den Rechtsakten der Union im Bereich der Cybersicherheit übertragen werden, indem sie unter anderem Sachkenntnis bereitstellt, Beratung bietet und die Rolle eines Informations- und Wissenszentrums der Union übernimmt. Sie sollte den Austausch bewährter Verfahren zwischen den Mitgliedstaaten und privaten Interessenträgern fördern, der Europäischen Kommission und den Mitgliedstaaten strategische Vorschläge unterbreiten, als Bezugspunkt für sektorspezifische politische Initiativen der Union im Bereich der Cybersicherheit dienen und die operative Zusammenarbeit zwischen den Mitgliedstaaten sowie zwischen den Mitgliedstaaten und den Organen, Einrichtungen und sonstigen Stellen der Union fördern.

(10) Mit dem Beschluss 2004/97/EG, Euratom, der auf der Tagung des Europäischen Rates vom 13. Dezember 2003 angenommen wurde, legten die Vertreter der Mitgliedstaaten fest, dass die ENISA ihren Sitz in Griechenland in einer von der griechischen Regierung zu bestimmenden Stadt haben soll. Der Sitzmitgliedstaat der Agentur sollte die bestmöglichen Voraussetzungen für eine reibungslose und effiziente Tätigkeit der Agentur gewährleisten. Damit die Agentur ihre Aufgaben ordnungsgemäß und effizient erfüllen, Personal einstellen und binden und die Effizienz der Vernetzungsmaßnahmen steigern kann, ist es unbedingt erforderlich, sie an einem geeigneten Standort anzusiedeln, der unter anderem eine angemessene Verkehrsanbindung sowie Einrichtungen für die Ehepartner und Kinder des Personals der Agentur bietet. Die erforderlichen Modalitäten sollten in einem Abkommen zwischen der Agentur und dem Sitzmitgliedstaat festgelegt werden, das nach Billigung durch den Verwaltungsrat der Agentur geschlossen wird.

(11) Angesichts der zunehmenden Herausforderungen, mit denen die Union im Bereich der Cybersicherheit konfrontiert ist, sollten die Mittelzuweisungen für die Agentur erhöht werden, damit ihre finanzielle und personelle Ausstattung ihrer größeren Rolle und ihren umfangreicheren Aufgaben sowie ihrer wichtigen Stellung im Kreise der Organisationen gerecht werden kann, die das digitale Ökosystem der EU verteidigen.

(12) Die Agentur sollte ein hohes Niveau an Sachkenntnis entwickeln und pflegen und durch ihre Unabhängigkeit, die Qualität ihrer Beratung und der von ihr verbreiteten Informationen, die Transparenz ihrer Verfahren und Arbeitsmethoden sowie die Sorgfalt, mit der sie ihre Aufgaben erfüllt, als Bezugspunkt Vertrauen in den Binnenmarkt schaffen. Die Agentur sollte die Bemühungen der Mitgliedstaaten [...]**unterstützen** und **vorausgreifend zu den Bemühungen** der Union **beitragen** und ihre Aufgaben in uneingeschränkter Zusammenarbeit mit den Organen, Einrichtungen und sonstigen Stellen der Union und den Mitgliedstaaten wahrnehmen. Außerdem sollte sich die Agentur auf die Beiträge des Privatsektors sowie auf die Zusammenarbeit mit diesem und anderen einschlägigen Interessenträgern stützen. Mit einer Reihe von Aufgaben sollte bei gleichzeitiger Wahrung der Flexibilität in ihrer Tätigkeit vorgegeben werden, wie die Agentur ihre Ziele erreichen soll.

(13) Die Agentur sollte die Kommission [...] mit Beratung, Stellungnahmen und Analysen zu allen Angelegenheiten der Union, die mit der Ausarbeitung, Aktualisierung und Überprüfung von Strategien und Rechtsvorschriften im Bereich der Cybersicherheit **und ihren sektorenspezifischen Aspekten** zusammenhängen, unterstützen**, damit die EU-Strategien und Rechtsvorschriften mit Cybersicherheitsdimension zweckdienlicher gestaltet werden und ihre stimmige Umsetzung auf nationaler Ebene ermöglicht wird**. Für sektorspezifische Strategien und Rechtsetzungsinitiativen der Union im Zusammenhang mit der Cybersicherheit sollte die Agentur als Bezugspunkt für Beratung und Sachkenntnis dienen.

(14) Die Agentur hat grundsätzlich die Aufgabe, die einheitliche Umsetzung des einschlägigen Rechtsrahmens, vor allem die wirksame Umsetzung der NIS-Richtlinie, zu unterstützen, was für die Stärkung der Abwehrfähigkeit gegen Cyberangriffe unerlässlich ist. Angesichts der sich rasch weiterentwickelnden Bedrohungen für die Cybersicherheit müssen die Mitgliedstaaten beim Aufbau der Abwehrfähigkeit gegen Cyberangriffe natürlich mit einem umfassenderen und ressortübergreifenden Konzept unterstützt werden.

(15) Die Agentur sollte die Organe, Einrichtungen und sonstigen Stellen der Union sowie die Mitgliedstaaten in ihrem Bemühen um den Auf- und Ausbau der Fähigkeiten und der Bereitschaft zur Verhütung, Erkennung und Bewältigung von Cyber**bedrohungen** [...] und von Sicherheitsvorfällen im Zusammenhang mit der Netz- und Informationssicherheit unterstützen. So sollte die Agentur den Auf- und Ausbau der nationalen CSIRTs unterstützen, damit sie ein unionsweit hohes Maß an Ausgereiftheit erreichen. **Die Tätigkeiten der ENISA im Zusammenhang mit den operativen Kapazitäten der Mitgliedstaaten sollten ausschließlich die eigenen Maßnahmen der Mitgliedstaaten zur Erfüllung ihrer Verpflichtungen aus der NIS-Richtlinie ergänzen und diese folglich nicht ersetzen** [...].

(15a) Zudem sollte die Agentur auf Ersuchen die Ausarbeitung und Aktualisierung von Strategien der Union und der Mitgliedstaaten im Bereich der Netz- und Informationssysteme, insbesondere der Cybersicherheit, unterstützen, deren Verbreitung fördern und deren Umsetzung verfolgen. Die Agentur sollte öffentlichen Stellen auch Ausbildungsmaßnahmen und Ausbildungsmaterial anbieten und gegebenenfalls Ausbilder weiterbilden, um die Mitgliedstaaten darin zu unterstützen, eigene Ausbildungskapazitäten aufzubauen.

(16) Die Agentur sollte die auf der Grundlage der NIS-Richtlinie eingesetzte Kooperationsgruppe bei der Wahrnehmung ihrer Aufgaben unterstützen, indem sie vor allem ihre Sachkenntnis und Beratung zur Verfügung stellt und den Austausch bewährter Verfahren erleichtert, insbesondere was die Ermittlung von Betreibern wesentlicher Dienste durch die Mitgliedstaaten in Bezug auf Risiken und Sicherheitsvorfälle anbelangt, auch mit Blick auf grenzüberschreitende Abhängigkeiten.

(17) Die Agentur sollte als Anreiz für die Zusammenarbeit zwischen dem öffentlichen und privaten Sektor [...] **den Informationsaustausch in und zwischen Sektoren, vor allem in den in Anhang II der Richtlinie (EU) 2016/1148 genannten Sektoren, unterstützen, indem sie bewährte Verfahren und Leitlinien zu den verfügbaren Instrumenten und Verfahren sowie Leitlinien zur Bewältigung rechtlicher Fragen im Zusammenhang mit dem Informationsaustausch bereitstellt, wobei dies beispielsweise durch die Erleichterung des** Aufbaus sektorbezogener Informationsaustausch- und -analysezentren (Information Sharing and Analysis Centres – ISACs) **erreicht werden soll** [...].

(18) Die Agentur sollte die **freiwillig bereitgestellten** nationalen Berichte der CSIRTs und des CERT-EU zusammenstellen und auswerten**, um die Mitgliedstaaten dabei zu unterstützen,** [...] für den Informationsaustausch gemeinsame [...] **Verfahren** aufzustellen, die Sprache festzulegen und terminologische Vereinbarungen zu treffen. Im Rahmen der NIS-Richtlinie, die [...] die Grundlage für den freiwilligen Austausch technischer Informationen auf operativer Ebene **innerhalb** des CSIRTs-Netzes geschaffen hat, sollte die Agentur auch den Privatsektor einbeziehen.

(19) Die Agentur sollte dazu beitragen, dass bei massiven grenzüberschreitenden Cybersicherheitsvorfällen und -krisen eine Reaktion auf EU-Ebene erfolgt. **Diese Aufgabe sollte sie entsprechend ihrem Mandat gemäß dieser Verordnung und einem Ansatz ausführen, der von den Mitgliedstaaten im Zusammenhang mit der Empfehlung der Kommission über die koordinierte Reaktion auf große Cybersicherheitsvorfälle und -krisen festzulegen ist.** Hierzu [...] **könnte auch gehören, dass** sie [...] relevante Informationen zusammenstellt und den Kontakt zwischen dem CSIRTs-Netz und den Fachkreisen sowie den für das Krisenmanagement zuständigen Entscheidungsträgern erleichtert. Zudem könnte die Agentur die Bewältigung von Sicherheitsvorfällen aus technischer Sicht unterstützen, indem sie den Austausch entsprechender technischer Lösungen zwischen den Mitgliedstaaten erleichtert und Beiträge für die Öffentlichkeitsarbeit liefert. Die Agentur sollte den Prozess unterstützen, indem sie die Modalitäten einer solchen Zusammenarbeit im Rahmen [...] **regelmäßig** stattfindender Cybersicherheitsübungen testet.

(20) [...] **Zur Unterstützung der** operativen **Zusammenarbeit** [...] sollte die Agentur im Wege einer strukturierten Zusammenarbeit [...] auf den bei der CERT-EU vorhandenen **technischen und operativen** Sachverstand zurückgreifen. [...] Für die Festlegung der praktischen Aspekte einer solchen Kooperation **und zur Vermeidung von Doppelarbeit** sollten gegebenenfalls zwischen den beiden Organisationen die hierfür notwendigen Modalitäten festgelegt werden.

(21) Entsprechend ihrer [...] Aufgabe**, die operative Zusammenarbeit im Rahmen des CSIRTs-Netzes zu unterstützen,** sollte die Agentur in der Lage sein, die Mitgliedstaaten **auf deren Ersuchen hin** zu unterstützen, **indem sie** beispielsweise **diese** berät**, wie sie ihre Fähigkeiten zur Verhütung, Erkennung und Bewältigung von Sicherheitsvorfällen verbessern können, die** technische [...] **Bewältigung von Sicherheitsvorfällen mit beträchtlichen oder erheblichen Auswirkungen erleichtert** oder Analysen von Bedrohungen und Sicherheitsvorfällen **erstellt**. **Die technische Bewältigung von Sicherheitsvorfällen mit beträchtlichen oder erheblichen Auswirkungen sollte u. a. insbesondere dadurch erleichtert werden, dass die ENISA den freiwilligen Austausch technischer Lösungen zwischen den Mitgliedstaaten unterstützt oder kombinierte technische Informationen – etwa über technische Lösungen, die von den Mitgliedstaaten freiwillig bereitgestellt werden – erstellt.** Der Empfehlung der Kommission über die koordinierte Reaktion auf große Cybersicherheitsvorfälle und -krisen zufolge sollten die Mitgliedstaaten in gutem Glauben untereinander sowie mit der ENISA Informationen über massive Cybersicherheitsvorfälle und -krisen unverzüglich austauschen. Diese Informationen dürften zudem der ENISA **bei der Unterstützung der operativen Zusammenarbeit** helfen [...].

(22) Als Teil der regulären Zusammenarbeit auf technischer Ebene zur Unterstützung der EU-Lageeinschätzung sollte die Agentur auf der Grundlage öffentlich verfügbarer Informationen, ihrer eigenen Analysen und anhand von Berichten, die sie [...] von den CSIRTs der Mitgliedstaaten oder den zentralen Anlaufstellen gemäß der NIS-Richtlinie **(in beiden Fällen auf freiwilliger Basis)**, dem Europäischen Zentrum zur Bekämpfung der Cyberkriminalität (EC3) bei Europol und dem CERT-EU sowie gegebenenfalls dem EU-Zentrum für Informationsgewinnung und -analyse (INTCEN) des Europäischen Auswärtigen Dienstes (EAD) erhalten hat, regelmäßig **und in enger Zusammenarbeit mit den Mitgliedstaaten** den EU-Cybersicherheitslagebericht über Cybervorfälle und -bedrohungen erstellen. Der Bericht sollte den einschlägigen Stellen des Rates, der Kommission, der Hohen Vertreterin der Union für die Gemeinsame Außen- und Sicherheitspolitik und dem CSIRTs-Netz zur Verfügung gestellt werden.

(23) **Die Unterstützung der n**achträglichen technischen Untersuchungen von Sicherheitsvorfällen mit beträchtlichen Auswirkungen [...], die [...] auf Ersuchen der betreffenden Mitgliedstaaten [...] **durch die Agentur erfolgt**, sollte sich auf die Verhütung künftiger Sicherheitsvorfälle konzentrieren[...]. **Die betreffenden Mitgliedstaaten sollten die erforderlichen Informationen bereitstellen, damit die Agentur die technische Untersuchung wirksam unterstützen kann.**

(24) [...]

(25) Die Mitgliedstaaten können die von dem Sicherheitsvorfall betroffenen Unternehmen auffordern, mit der Agentur zusammenzuarbeiten und dieser unbeschadet ihres Rechts, sensible Geschäftsinformationen zu schützen, die notwendigen Informationen und Hilfen zur Verfügung stellen.

(26) Um die Herausforderungen im Bereich der Cybersicherheit besser verstehen und den Mitgliedstaaten und EU-Organen langfristige strategische Beratung anbieten zu können, muss die Agentur aktuelle und neu auftretende Risiken analysieren. Hierzu sollte die Agentur in Zusammenarbeit mit den Mitgliedstaaten und gegebenenfalls Statistikämtern und anderen Stellen einschlägige **öffentlich zugängliche oder freiwillig bereitgestellte** Informationen sammeln und Analysen neu entstehender Technik sowie themenspezifische Bewertungen dazu durchführen, welche gesellschaftlichen, rechtlichen, wirtschaftlichen und regulatorischen Folgen technische Innovationen auf die Netz- und Informationssicherheit, insbesondere die Cybersicherheit, haben. Die Agentur sollte die Mitgliedstaaten sowie die Organe, Einrichtungen und sonstigen Stellen der EU darüber hinaus bei der Ermittlung sich abzeichnender Trends und bei der Vermeidung von [...] Cybersicherheit**svorfällen** unterstützen, indem sie Analysen der Bedrohungen und Sicherheitsvorfälle durchführt.

(27) Um die Abwehrfähigkeit der Union zu stärken, sollte die Agentur Spitzenkompetenzen im Bereich der **Cybers**icherheit der [...] Infrastrukturen**, die die in Anhang II der NIS-Richtlinie aufgeführten Sektoren unterstützen, und der Infrastrukturen, die von den in Anhang III der genannten Richtlinie aufgeführten Anbietern digitaler Dienste genutzt werden,** aufbauen, um so Beratung, Leitlinien und bewährte Verfahren zur Verfügung stellen zu können. Um den Zugang zu besser strukturierten Informationen über Cybersicherheitsrisiken und mögliche Abhilfemaßnahmen zu erleichtern, sollte die Agentur das Informationsportal der Union aufbauen und pflegen, über das der Öffentlichkeit Informationen der Organe, Einrichtungen und sonstigen Stellen der EU und der Mitgliedstaaten zur Cybersicherheit gegeben werden.

(28) Die Agentur sollte dabei mitwirken, die Öffentlichkeit für Cybersicherheitsrisiken zu sensibilisieren, und Leitlinien für bewährte Verfahren zur Verfügung stellen, die sich an Bürger sowie an Organisationen wenden. Darüber hinaus sollte die Agentur einen Beitrag dazu leisten, bewährte Verfahren und Lösungen auf der Ebene von Einzelpersonen und Organisationen zu fördern, indem sie öffentlich verfügbare Informationen über erhebliche Sicherheitsvorfälle sammelt und analysiert und Berichte hierüber erstellt, die Unternehmen und Bürgern als Leitfaden dienen können und die das Niveau der Abwehrbereitschaft und Abwehrfähigkeit insgesamt erhöhen. Ferner sollte die Agentur in Zusammenarbeit mit den Mitgliedstaaten und den Organen, Einrichtungen und sonstigen Stellen der EU regelmäßige öffentliche Aufklärungskampagnen durchführen, die sich an die Endnutzer richten und zum Ziel haben, sicherere Verhaltensweisen der Nutzer im Internet zu fördern, die Nutzer für potenzielle Bedrohungen im Internet – auch für die Cyberkriminalität wie das Abgreifen von Daten (Phishing), Botnets, Finanz- und Bankenbetrug – stärker zu sensibilisieren und einfache Empfehlungen in Bezug auf Authentifizierung und Datenschutz zu geben. Die Agentur sollte eine zentrale Rolle dabei spielen, die Sensibilisierung der Endnutzer für die Sicherheit von Geräten zu forcieren.

(29) Um die im Cybersicherheitssektor tätigen Unternehmen und die Nutzer von Cybersicherheitslösungen zu unterstützen, sollte die Agentur eine "Marktbeobachtungsstelle" aufbauen und pflegen, die die wichtigsten Nachfrage- und Angebotstrends auf dem Cybersicherheitsmarkt regelmäßig analysiert und bekannt macht.

(30) Damit die Agentur ihre Ziele in vollem Umfang verwirklichen kann, sollte sie zu den einschlägigen Organen, Einrichtungen und sonstigen Stellen der EU Kontakt halten – etwa zum CERT-EU, zum Europäischen Zentrum zur Bekämpfung der Cyberkriminalität (EC3) bei Europol, zur Europäischen Verteidigungsagentur (EDA), zur Europäischen Agentur für das Betriebsmanagement von IT-Großsystemen (eu-LISA), zur Europäischen Agentur für Flugsicherheit (EASA)**, zur Agentur für das europäische globale Satellitennavigationssystem (Agentur für das GNSS)** und zu sonstigen EU-Agenturen, die sich mit Fragen der IT-Sicherheit beschäftigen. Für den Austausch von Know-how und bewährten Verfahren und für die Beratung zu Aspekten der Cybersicherheit, die sich auf die Arbeit von Datenschutzbehörden auswirken können, sollte die Agentur auch mit diesen in Verbindung stehen. Vertreter der Strafverfolgungs- und der Datenschutzbehörden auf nationaler Ebene und auf Unionsebene sollten als Vertreter für eine Mitwirkung in der Ständigen Gruppe der Interessenträger der Agentur in Frage kommen. Bei ihren Kontakten mit Strafverfolgungsbehörden in Bezug auf Netz- und Informationssicherheitsaspekte, die sich möglicherweise auf deren Arbeit auswirken, sollte die Agentur vorhandene Informationskanäle und bestehende Netze beachten.

(31) [...] **D**ie Agentur sollte [...] in ihrer Rolle **als** Sekretariat des CSIRTs-Netzes [...] über die in der NIS-Richtlinie festgelegten einschlägigen Aufgaben hinaus die CSIRTs der Mitgliedstaaten und das CERT-EU bei der operativen Zusammenarbeit unterstützen. Zudem sollte sie unter gebührender Berücksichtigung der Standardbetriebsverfahren des CSIRTs-Netzes die Zusammenarbeit zwischen den jeweiligen CSIRTs bei Sicherheitsvorfällen, Angriffen oder Störungen der von den CSIRTs verwalteten oder geschützten Netze oder Infrastrukturen, die mindestens zwei CERTs betreffen oder betreffen können, fördern und unterstützen.

(32) Zur Erhöhung der Abwehrbereitschaft der Union bei Cybersicherheitsvorfällen sollte die Agentur auf Unionsebene [...] **regelmäßige** Cybersicherheitsübungen organisieren und die Mitgliedstaaten sowie die Organe, Einrichtungen und sonstigen Stellen der EU auf deren Ersuchen hin bei der Organisation solcher Übungen unterstützen.

(33) Die Agentur sollte ihre Sachkenntnis im Bereich der Cybersicherheitszertifizierung weiter ausbauen und pflegen, damit sie die Unionspolitik auf diesem Gebiet unterstützen kann. Die Agentur sollte die Nutzung der Cybersicherheitszertifizierung in der Union fördern, auch indem sie zum Aufbau und zur Pflege eines Cybersicherheitszertifizierungsrahmens auf Unionsebene beiträgt, um so die auf mehr Transparenz gestützte Vertrauenswürdigkeit der Cybersicherheit von IKT-Produkten und -Diensten zu erhöhen und damit das Vertrauen in den digitalen Binnenmarkt zu stärken.

(34) Effiziente Cybersicherheitsstrategien sollten sowohl im öffentlichen als auch im privaten Sektor auf sorgfältig entwickelten Risikobewertungsmethoden beruhen. Risikobewertungsmethoden werden auf verschiedenen Ebenen angewandt, ohne dass es eine einheitliche Vorgehensweise für deren effiziente Anwendung gibt. Durch die Förderung und Entwicklung bewährter Verfahren für die Risikobewertung und interoperabler Lösungen für das Risikomanagement innerhalb von Organisationen des öffentlichen und des privaten Sektors wird das Niveau der Cybersicherheit in der Union erhöht. Zu diesem Zweck sollte die Agentur die Zusammenarbeit zwischen Interessenträgern auf Unionsebene unterstützen und Hilfestellung bei deren Bemühungen um die Festlegung und Einführung von europäischen und internationalen Normen für das Risikomanagement und eine messbare Sicherheit in Bezug auf elektronische Produkte, Systeme, Netze und Dienste leisten, die im Zusammenwirken mit Software die Netz- und Informationssysteme bilden.

(35) Die Agentur sollte die Mitgliedstaaten und die Diensteanbieter dazu anspornen, ihre allgemeinen Sicherheitsstandards zu heben, damit alle Internetnutzer die erforderlichen Vorkehrungen für ihre persönliche Cybersicherheit treffen können. So sollten Diensteanbieter und Produkthersteller diese Dienste und Produkte vom Markt nehmen oder umrüsten, wenn sie den Cybersicherheitsstandards nicht genügen. In Zusammenarbeit mit den zuständigen Behörden kann die ENISA Informationen über das Niveau der Cybersicherheit von Produkten und Diensten verbreiten, die auf dem Binnenmarkt angeboten werden, Anbieter und Hersteller verwarnen und sie auffordern, die Sicherheit, auch die Cybersicherheit, ihrer Produkte [...] zu verbessern.

(36) Die Agentur sollte die laufenden Tätigkeiten auf den Gebieten der Forschung, Entwicklung und technologischen Bewertung – insbesondere die im Rahmen der vielfältigen Forschungsinitiativen der Union durchgeführten Tätigkeiten – umfassend berücksichtigen, um die Organe, Einrichtungen und sonstigen Stellen der Union sowie gegebenenfalls die Mitgliedstaaten – auf deren Ersuchen – in Bezug auf den Forschungsbedarf im Bereich der [...] Cybersicherheit [...] zu beraten. **Um den Bedarf und die Prioritäten im Forschungsbereich zu ermitteln, sollte die Agentur auch die einschlägigen Nutzergruppen konsultieren.**

(37) Die [...] Cyber**bedrohungen** bestehen weltweit. Um die **Cybers**icherheitsstandards, einschließlich der Festlegung gemeinsamer Verhaltensnormen, und den Informationsaustausch zu verbessern sowie eine zügigere internationale Zusammenarbeit bei der Abwehr und einen weltweiten gemeinsamen Ansatz für Probleme der Netz- und Informationssicherheit zu fördern, bedarf es einer engeren internationalen Zusammenarbeit. In dieser Hinsicht sollte die Agentur ein stärkeres Engagement der Union und die Zusammenarbeit mit Drittländern und internationalen Organisationen unterstützen, indem sie den einschlägigen Organen, Einrichtungen und sonstigen Stellen der Union gegebenenfalls die erforderlichen Sachkenntnisse und Analysen zur Verfügung stellt.

(38) Die Agentur sollte in der Lage sein, auf Anfragen der Mitgliedstaaten und der Organe, Einrichtungen und sonstigen Stellen der EU, die von den Zielen der Agentur abgedeckt sind, ad hoc mit Rat und Hilfestellung zu reagieren.

(39) In Bezug auf die Führung der Agentur müssen bestimmte Grundsätze umgesetzt werden, um der Gemeinsamen Erklärung und dem Gemeinsamen Konzept zu entsprechen, die von der Interinstitutionellen Arbeitsgruppe zu den dezentralen Einrichtungen der EU im Juli 2012 vereinbart wurden und deren Zweck darin besteht, die Aktivitäten der Agenturen dynamischer zu gestalten und ihre Leistung zu verbessern. Die Gemeinsame Erklärung und das Gemeinsame Konzept sollten, soweit angemessen, in den Arbeitsprogrammen, den Bewertungen und den Berichterstattungs- und Verwaltungsverfahren der Agentur zur Geltung kommen.

(40) Der Verwaltungsrat, der sich aus Vertretern der Mitgliedstaaten und der Kommission zusammensetzt, sollte die allgemeine Ausrichtung der Tätigkeit der Agentur festlegen und dafür sorgen, dass sie ihre Aufgaben im Einklang mit dieser Verordnung wahrnimmt. Der Verwaltungsrat sollte über die erforderlichen Befugnisse verfügen, um den Haushaltsplan zu erstellen und dessen Ausführung zu überprüfen, angemessene Finanzvorschriften und transparente Verfahren für die Entscheidungsfindung der Agentur festzulegen, das einheitliche Programmplanungsdokument der Agentur anzunehmen, sich eine Geschäftsordnung zu geben, den Exekutivdirektor zu ernennen und über die Verlängerung sowie die Beendigung der Amtszeit des Exekutivdirektors zu beschließen.

(41) Damit die Agentur ihre Aufgaben ordnungsgemäß und effizient wahrnehmen kann, sollten die Kommission und die Mitgliedstaaten sicherstellen, dass die Personen, die als Mitglieder des Verwaltungsrats ernannt werden, über angemessenes Fachwissen und Erfahrung in Funktionsbereichen verfügen. Die Kommission und die Mitgliedstaaten sollten sich auch darum bemühen, die Fluktuation bei ihren jeweiligen Vertretern im Verwaltungsrat zu verringern, um die Kontinuität seiner Arbeit sicherzustellen.

(42) Damit die Agentur reibungslos funktioniert, ist es erforderlich, dass ihr Exekutivdirektor aufgrund seiner Verdienste und nachgewiesenen Verwaltungs- und Managementfähigkeiten ernannt wird, über einschlägige Sachkenntnis und Erfahrungen auf dem Gebiet der Cybersicherheit verfügt und seine Aufgaben völlig unabhängig wahrnimmt. Der Exekutivdirektor sollte nach Anhörung der Kommission einen Vorschlag für das Arbeitsprogramm der Agentur ausarbeiten und alle erforderlichen Maßnahmen zu dessen ordnungsgemäßer Durchführung ergreifen. Der Exekutivdirektor sollte einen **dem Verwaltungsrat vorzulegenden** Jahresbericht**, in dem auch die Umsetzung des jährlichen Arbeitsprogramms der Agentur behandelt wird,** ausarbeiten, den Entwurf eines Voranschlags für die Einnahmen und Ausgaben der Agentur erstellen und den Haushaltsplan ausführen. Der Exekutivdirektor sollte zudem die Möglichkeit haben, Ad-hoc-Arbeitsgruppen einzusetzen, die sich mit wissenschaftlichen, technischen, rechtlichen oder wirtschaftlichen Einzelfragen befassen. Der Exekutivdirektor sollte dafür sorgen, dass die Mitglieder der Ad-hoc-Arbeitsgruppen höchsten fachlichen Ansprüchen genügen und dass je nach Einzelfrage gegebenenfalls ein repräsentatives Gleichgewicht zwischen öffentlichen Verwaltungen der Mitgliedstaaten, den Organen der Union und dem Privatsektor einschließlich der Wirtschaft, der Nutzer und wissenschaftlicher Sachverständiger für Netz- und Informationssicherheit gewahrt wird.

(43) Der Exekutivrat sollte dazu beitragen, dass der Verwaltungsrat effektiv arbeiten kann. Im Rahmen seiner vorbereitenden Arbeiten für die Beschlüsse des Verwaltungsrats sollte er die einschlägigen Informationen im Detail prüfen und die sich bietenden Optionen sondieren, zudem sollte er die einschlägigen Beschlüsse des Verwaltungsrats vorbereiten, indem er Beratung und Lösungen anbietet.

(44) Die Agentur sollte über eine Ständige Gruppe der Interessenträger als Beratungsgremium verfügen, um einen regelmäßigen Dialog mit dem Privatsektor, Verbraucherorganisationen und sonstigen Interessenträgern sicherzustellen. Die vom Verwaltungsrat auf Vorschlag des Exekutivdirektors eingesetzte Ständige Gruppe der Interessenträger sollte hauptsächlich Fragen behandeln, die die Beteiligten betreffen, und diese der Agentur zur Kenntnis bringen. Die Zusammensetzung der Ständigen Gruppe der Interessenträger und die dieser Gruppe übertragenen Aufgaben, die vor allem aus dem Entwurf des Arbeitsprogramms hervorgehen, sollten gewährleisten, dass die Interessenträger bei der Tätigkeit der Agentur ausreichend vertreten sind.

(45) Die Agentur sollte Vorschriften zur Vermeidung und Handhabung von Interessenkonflikten haben. Die Agentur sollte die einschlägigen Bestimmungen der Union in Bezug auf den Zugang der Öffentlichkeit zu Dokumenten gemäß der Verordnung (EG) Nr. 1049/2001 des Europäischen Parlaments und des Rates[12] anwenden. Die Verarbeitung personenbezogener Daten durch die Agentur sollte nach der Verordnung (EG) Nr. 45/2001 des Europäischen Parlaments und des Rates vom 18. Dezember 2000 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Gemeinschaft und zum freien Datenverkehr[13] erfolgen. Die Agentur sollte die für die Unionsorgane geltenden Bestimmungen über den Umgang mit Informationen, insbesondere mit sensiblen Informationen und Verschlusssachen der EU, sowie die entsprechenden einzelstaatlichen Rechtsvorschriften befolgen.

---

[12] Verordnung (EG) Nr. 1049/2001 des Europäischen Parlaments und des Rates vom 30. Mai 2001 über den Zugang der Öffentlichkeit zu Dokumenten des Europäischen Parlaments, des Rates und der Kommission (ABl. L 145 vom 31.5.2001, S. 43).

[13] ABl. L 8 vom 12.1.2001, S. 1.

(46) Damit die volle Autonomie und Unabhängigkeit der Agentur gewährleistet ist und sie zusätzliche und neue Aufgaben – auch nicht vorhergesehene Aufgaben in Notfällen – erfüllen kann, sollte die Agentur über einen ausreichenden und eigenständigen Haushalt verfügen, der hauptsächlich durch einen Beitrag der Union und durch Beiträge von Drittländern, die sich an der Arbeit der Agentur beteiligen, finanziert wird. Die Mehrheit der Agenturbediensteten sollte unmittelbar mit der operativen Umsetzung des Mandats der Agentur befasst sein. Dem Sitzmitgliedstaat und anderen Mitgliedstaaten sollte es erlaubt sein, freiwillige Beiträge zu den Einnahmen der Agentur zu leisten. Sämtliche Zuschüsse aus dem Gesamthaushaltsplan der Europäischen Union sollten dem Haushaltsverfahren der Union unterliegen. Ferner sollte die Rechnungsführung der Agentur durch den Rechnungshof geprüft werden, um Transparenz und Rechenschaftspflicht sicherzustellen.

(47) [...]

(48) Die Cybersicherheitszertifizierung spielt eine große Rolle, wenn es darum geht, das Vertrauen in IKT-Produkte und -Dienste zu stärken und deren Sicherheit zu erhöhen. Die Entwicklung des digitalen Binnenmarkts und insbesondere der Datenwirtschaft und des Internets der Dinge kommt nur voran, wenn in der breiten Öffentlichkeit das Vertrauen vorhanden ist, dass diese Produkte und Dienste ein gewisses Maß an Cybersicherheit gewährleisten. Vernetzte und automatisierte Fahrzeuge, elektronische medizinische Geräte, die automatischen Steuerungssysteme der Industrie oder intelligente Netze sind, um nur einige Beispiele zu nennen, Sektoren, in denen die Zertifizierung bereits breiten Einsatz findet oder in naher Zukunft eingesetzt werden soll. Die unter die NIS-Richtlinie fallenden Sektoren sind zudem Sektoren, in denen die Cybersicherheitszertifizierung ein maßgeblicher Faktor ist.

(49) In ihrer Mitteilung aus dem Jahr 2016 "Stärkung der Abwehrfähigkeit Europas im Bereich der Cybersicherheit und Förderung einer wettbewerbsfähigen und innovativen Cybersicherheitsbranche" unterstrich die Kommission die Notwendigkeit hochwertiger, erschwinglicher und interoperabler Produkte und Lösungen für die Cybersicherheit. Allerdings ist das Angebot an IKT-Produkten und -diensten im Binnenmarkt nach wie vor geografisch stark zersplittert. Das liegt daran, dass sich die Cybersicherheitsbranche in Europa überwiegend aufgrund der Nachfrage der nationalen Regierungen entwickelt hat. Zudem gehört der Mangel an interoperablen Lösungen (technischen Normen), Verfahrensweisen und EU-weiten Zertifizierungsmechanismen zu den Defiziten, die den Binnenmarkt im Bereich der Cybersicherheit beeinträchtigen. Dies macht es zum einen für europäische Unternehmen schwerer, im nationalen, europäischen und weltweiten Wettbewerb zu bestehen. Zum anderen verringert sich dadurch das Angebot an tragfähiger und einsetzbarer Cybersicherheitstechnik, auf die Privatpersonen und Unternehmen zugreifen könnten. Auch in der Halbzeitbewertung der Umsetzung der Strategie für den digitalen Binnenmarkt unterstrich die Kommission die Bedeutung sicherer vernetzter Produkte und Systeme und verwies darauf, dass die Schaffung eines europäischen Rahmens für die IKT-Sicherheit, auf dessen Grundlage Vorschriften für die Organisation der IKT-Sicherheitszertifizierung in der Union festgelegt werden, dafür sorgen kann, dass das Vertrauen in den Binnenmarkt erhalten bleibt und die derzeitige Fragmentierung des Cybersicherheitsmarkts eingedämmt wird.

(50) Derzeit werden IKT-**Prozesse,** -Produkte und -Dienste im Hinblick auf ihre Cybersicherheit kaum zertifiziert. Wenn dies doch der Fall ist, geschieht es meist auf Ebene der Mitgliedstaaten oder im Rahmen brancheneigener Programme. So wird ein von einer nationalen Cybersicherheitsbehörde ausgestelltes Zertifikat nicht grundsätzlich auch von anderen Mitgliedstaaten anerkannt. Unternehmen müssen somit ihre Produkte und Dienste möglicherweise in mehreren Mitgliedstaaten, in denen sie tätig sind, zertifizieren lassen, um beispielsweise an einer nationalen Ausschreibung teilzunehmen. Auch wenn immer neue Systeme entstehen, scheint es kein kohärentes und ganzheitliches Konzept zu geben, das sich mit horizontalen Fragen der Cybersicherheit, etwa im Bereich des Internets der Dinge, befasst. Die vorhandenen Systeme weisen im Hinblick auf Produkterfassung, Vertrauenswürdigkeitsstufen, wesentliche Kriterien und tatsächliche Nutzung erhebliche Mängel und Unterschiede auf.

(51) In der Vergangenheit wurden bereits einige Anstrengungen unternommen, um zu einer gegenseitigen Anerkennung der Zertifikate in Europa zu gelangen. Diese waren jedoch nur zum Teil erfolgreich. Das in dieser Hinsicht wichtigste Beispiel ist die in der Gruppe hoher Beamter für die Sicherheit der Informationssysteme (SOG-IS) getroffene Vereinbarung über die gegenseitige Anerkennung (MRA). Auch wenn diese Vereinbarung das wichtigste Vorbild für die Zusammenarbeit und gegenseitige Anerkennung auf dem Gebiet der Sicherheitszertifizierung ist, [...] umfasst die Gruppe nur einen Teil der EU-Mitgliedstaaten. Dies hat aus Binnenmarktsicht zur Folge, dass die Vereinbarungen der Gruppe nur begrenzt wirksam sind.

(52) Vor diesem Hintergrund gilt es, einen europäischen Rahmen für die Cybersicherheitszertifizierung aufzubauen, auf dessen Grundlage die Anforderungen an die zu entwickelnden europäischen Systeme zur Zertifizierung der Cybersicherheit festgelegt werden, damit die Zertifikate **und EU-Konformitätserklärungen** für die IKT-Produkte und -Dienste in allen Mitgliedstaaten anerkannt und verwendet werden können. Mit einem europäischen Rahmen werden zwei Ziele verfolgt: einerseits dürfte er dazu beitragen, das Vertrauen in IKT-Produkte und -Dienste zu erhöhen, die nach solchen Systemen zertifiziert wurden, und andererseits dürften sich so vielfältige, sich widersprechende oder überlappende nationale System für die Cybersicherheitszertifizierung vermeiden lassen, was die Kosten für auf dem digitalen Binnenmarkt tätige Unternehmen senkt. Die Systeme sollten nichtdiskriminierend sein und sich auf internationale bzw. europäische Normen stützen, sofern diese Normen nicht unwirksam oder unangemessen im Hinblick auf die Erreichung der legitimen Ziele der EU in diesem Bereich sind.

(53) Die Kommission sollte befugt sein, für bestimmte Gruppen von IKT**-Prozessen,** -Produkten und -Diensten europäische Systeme für die Cybersicherheitszertifizierung anzunehmen. Diese Systeme sollten von nationalen [...] **B**ehörden für die **Cybersicherheitsz**ertifizierung umgesetzt und überwacht werden, und die im Rahmen dieser Systeme erteilten Zertifikate sollten unionsweit gültig sein und anerkannt werden. Die von der Industrie oder sonstigen privaten Organisationen betriebenen Zertifizierungssysteme fallen nicht in den Anwendungsbereich dieser Verordnung. Die Stellen, die solche Systeme betreiben, können der Kommission jedoch vorschlagen, ihre Systeme als Grundlage für ein europäisches System in Betracht zu ziehen und sie als ein solches zu genehmigen.

(54) Das Unionsrecht, in dem bestimmte Vorschriften zur Zertifizierung von IKT-Produkten und -Diensten festgelegt sind, bleibt von den Bestimmungen dieser Verordnung unberührt. So enthält die Datenschutz-Grundverordnung Festlegungen für Zertifizierungsverfahren und Datenschutzsiegel und -prüfzeichen, die dem Nachweis dienen, dass die für die Datenverarbeitung Verantwortlichen und die Auftragsverarbeiter bei der Verarbeitung von Daten die Bestimmungen der Verordnung einhalten. Solche Zertifizierungsverfahren sowie Datenschutzsiegel und -prüfzeichen sollten den betroffenen Personen einen raschen Überblick über das Datenschutzniveau einschlägiger Produkte und Dienstleistungen ermöglichen. Die Zertifizierung von Datenverarbeitungsvorgängen, die unter die Datenschutz-Grundverordnung fallen, auch wenn solche Vorgänge in Produkte und Dienste eingebettet sind, bleibt von dieser Verordnung unberührt.

(55) Mit den europäischen Systemen für die Cybersicherheitszertifizierung sollte gewährleistet werden, dass die nach solchen Systemen zertifizierten IKT**-Prozesse,** -Produkte und -Dienste bestimmten Anforderungen genügen**, um** [...] die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit gespeicherter, übermittelter oder verarbeiteter Daten, Funktionen oder Dienste, die von diesen Produkten, Prozessen, Diensten und Systemen angeboten oder über diese zugänglich gemacht werden**, während deren gesamten Lebenszyklus** im Sinne dieser Verordnung zu [...] **schützen**. In dieser Verordnung können nicht alle Anforderungen an die Cybersicherheit sämtlicher IKT**-Prozesse,** -Produkte und -Dienste im Einzelnen festgelegt werden. Die Vielfalt der IKT**-Prozesse,** -Produkte und -Dienste und die damit zusammenhängenden Anforderungen an die Cybersicherheit ist so groß, dass es sehr schwierig ist, allgemeine Anforderungen an die Cybersicherheit für alle Eventualitäten festzulegen. Es gilt daher, ein breit gefasstes und allgemeines Konzept der Cybersicherheit für die Zwecke der Zertifizierung zu verabschieden, ergänzt durch besondere Cybersicherheitsziele, die bei der Konzeption der europäischen Systeme für die Cybersicherheitszertifizierung berücksichtigt werden müssen. Die Modalitäten, wie diese Ziele für bestimmte IKT**-Prozesse,** -Produkte und -Dienste erreicht werden, sollten dann weiter im Einzelnen auf der Grundlage des jeweiligen von der Kommission angenommenen Zertifizierungssystems festgelegt werden, etwa durch Verweise auf Normen oder technische Spezifikationen**, wenn keine angemessenen Normen verfügbar sind**.

(55a) Die in einem europäischen System für die Cybersicherheitszertifizierung zu verwendenden technischen Spezifikationen sollten unter Beachtung der in Anhang II der Verordnung (EU) 1025/2012 verankerten Grundsätze bestimmt werden. Gewisse Abweichungen von diesen Grundsätzen könnten jedoch in hinreichend begründeten Fällen als notwendig erachtet werden, wenn diese technischen Spezifikationen in einem europäischen System für die Cybersicherheitszertifizierung in der Vertrauenswürdigkeitsstufe "hoch" verwendet werden sollen. Die Gründe für solche Abweichungen müssen veröffentlicht werden.

(55b) Die Konformitätsbewertung ist ein Verfahren, mit dem bewertet wird, ob bestimmte Anforderungen an einen IKT-Prozess, ein IKT-Produkt oder einen IKT-Dienst erfüllt werden. Dieses Verfahren wird von einem unabhängigen Dritten, bei dem es sich nicht um den Hersteller des Produkts oder den Diensteanbieter handelt, durchgeführt. Nach der erfolgreichen Bewertung eines IKT-Prozesses, -Produktes und -Dienstes beginnt das Verfahren zur Ausstellung eines Zertifikats. Dieses Verfahren sollte als Bestätigung gelten, dass die entsprechende Bewertung ordnungsgemäß durchgeführt wurde. Je nach Vertrauenswürdigkeitsstufe sollte im europäischen System für die Cybersicherheitszertifizierung angegeben werden, ob ein Zertifikat von einer privaten oder einer öffentlichen Stelle ausgestellt wird. Die Konformitätsbewertung und die Zertifizierung an sich garantieren nicht, dass die zertifizierten IKT-Produkte und -Dienste die Kriterien der Cybersicherheit erfüllen. Es handelt sich vielmehr um ein Verfahren und eine technische Methodik, um zu bescheinigen, dass die IKT-Produkte und -Dienste geprüft wurden und bestimmte Anforderungen an die Cybersicherheit erfüllen, wie sie anderweitig, beispielsweise in technischen Normen, festgelegt sind .

(55c) Die Auswahl der angemessenen Zertifizierungsstufe und der dazugehörigen Sicherheitsanforderungen durch die Zertifikatsnutzer sollte auf der Grundlage einer Risikoanalyse der Verwendung des IKT-Prozesses, -Produktes und -Dienstes erfolgen. Die Vertrauenswürdigkeitsstufe sollte daher in einem angemessenen Verhältnis zu dem mit der beabsichtigten Verwendung eines IKT-Prozesses, -Produktes und -Dienstes verbundenen Risiko stehen.

(55d) In einem europäische System für die Cybersicherheitszertifizierung kann eine Konformitätsbewertung vorgesehen werden, die unter der alleinigen Verantwortung des Herstellers oder Anbieters von IKT-Produkten und -Diensten durchzuführen ist (Selbstbewertung der Konformität). In diesem Fall reicht es aus, dass der Hersteller oder Anbieter selbst alle Überprüfungen vornimmt, um sicherzustellen, dass die IKT-Prozesse, -Produkte und -Dienste mit dem Zertifizierungssystem konform sind. Diese Art der Konformitätsbewertung sollte für IKT-Produkte und -Dienste von geringer Komplexität (z. B. einfache Konzeption und einfacher Herstellungsmechanismus), die ein geringes Risiko für das öffentliche Interesse darstellen, als angemessen angesehen werden. Zudem können nur IKT-Produkte und -Dienste, die der Vertrauenswürdigkeitsstufe "niedrig" entsprechen, einer Selbstbewertung der Konformität unterzogen werden.

(55e) Ein europäische System für die Cybersicherheitszertifizierung kann sowohl die Zertifizierung als auch die Selbstbewertung der Konformität von IKT-Produkten und -Diensten zulassen. In diesem Fall sollten im System klare und verständliche Instrumente für Verbraucher oder andere Nutzer vorgesehen werden, mit denen sie zwischen Produkten und Diensten, die unter der Verantwortung des Herstellers oder Anbieters bewertet werden, und Produkten und Diensten, die von einem Dritten zertifiziert werden, unterscheiden können.

(55f) Der Hersteller oder Anbieter von IKT-Produkten und -Diensten, der eine Selbstbewertung der Konformität durchführt, sollte die EU-Konformitätserklärung im Rahmen des Konformitätsbewertungsverfahrens abfassen und unterzeichnen. Bei der EU-Konformitätserklärung handelt es sich um das Dokument, welches bestätigt, dass das betreffende IKT-Produkt oder der betreffende IKT-Dienst die Anforderungen des Systems erfüllt. Durch die Abfassung und Unterzeichnung der EU-Konformitätserklärung übernimmt der Hersteller oder Anbieter die Verantwortung dafür, dass das IKT-Produkt oder der IKT-Dienst die rechtlichen Anforderungen des Systems erfüllt. Eine Kopie der EU-Konformitätserklärung sollte der nationalen Cybersicherheitszertifizierungsbehörde und der ENISA vorgelegt werden.

(55g) Der Hersteller oder Anbieter von IKT-Produkten und -Diensten sollte die EU-Konformitätserklärung und die technische Dokumentation mit allen einschlägigen Informationen in Bezug auf die Konformität der IKT-Produkte oder -Dienste mit einem System während eines Zeitraums, der im betreffenden europäischen System für die Cybersicherheitszertifizierung festgelegt ist, für die zuständige nationale Cybersicherheitszertifizierungsbehörde bereithalten. In der technischen Dokumentation sollten die geltenden Anforderungen aufgeführt werden und die Konzeption, Herstellung und Funktionsweise des IKT-Produkts oder -Dienstes erfasst werden, soweit sie für die Bewertung von Belang sind. Die technische Dokumentation sollte so erstellt werden, dass es möglich ist, die Konformität eines IKT-Produkts oder Dienstes mit den einschlägigen Anforderungen zu bewerten.

(55h) Die Mitgliedstaaten und die Organisationen von Interessenträgern sollten befugt sein, der Europäischen Gruppe für die Cybersicherheitszertifizierung die Ausarbeitung eines möglichen Systems vorzuschlagen. Die Organisationen von Interessenträgern sind Organisationen von Wirtschafts- und Verbrauchervertretern, darunter auch Vertreter von KMU-Organisationen, die ein berechtigtes Interesse an der Entwicklung eines bestimmten europäischen Systems für die Cybersicherheitszertifizierung haben. Solche Vorschläge sollten unter Berücksichtigung der Kriterien geprüft werden, die von der Europäischen Gruppe für die Cybersicherheitszertifizierung anhand von Leitlinien auf der Grundlage der Faktoren Transparenz, Offenheit, Unparteilichkeit, Konsens, Wirksamkeit, Relevanz und Kohärenz erarbeitet wurden.

(56) Die Kommission **und die Gruppe** sollten befugt sein, die ENISA mit der **raschen** Ausarbeitung möglicher Zertifizierungssysteme für bestimmte IKT**-Prozesse**, -Produkte und -Dienste zu beauftragen. Die Kommission sollte dann befugt sein, auf der Grundlage des von der ENISA vorgeschlagenen möglichen Systems das europäische System für die Cybersicherheitszertifizierung mittels eines Durchführungsrechtsakts anzunehmen. Unter Berücksichtigung des allgemeinen Zwecks und der in dieser Verordnung festgelegten Sicherheitsziele sollte in den von der Kommission angenommenen europäischen Systemen für die Cybersicherheitszertifizierung Mindestbestimmungen in Bezug auf den Gegenstand, den Anwendungsbereich und die Funktionsweise des einzelnen Systems festgelegt werden. Hierunter fallen u. a. Anwendungsbereich und Ziel der Cybersicherheitszertifizierung, darunter auch die Kategorien von IKT**-Prozesse,** -Produkten und -Diensten, detaillierte Spezifikationen der Anforderungen an die Cybersicherheit, etwa durch Verweise auf Normen oder technische Spezifikationen, die jeweiligen Bewertungskriterien und -verfahren sowie die beabsichtigte Vertrauenswürdigkeitsstufe **(**"niedrig", "mittel" bzw. "hoch"**) sowie gegebenenfalls die Bewertungsniveaus**.

(56a) Die Vertrauenswürdigkeit eines europäischen Zertifizierungssystems ist die Grundlage für das Vertrauen, dass ein IKT-Prozess, -Produkt oder -Dienst den Sicherheitsanforderungen eines spezifischen europäischen Systems für die Cybersicherheitszertifizierung genügt. Um die Kohärenz des Rahmens für zertifizierte IKT-Prozesse, -Produkte und -Dienste zu gewährleisten, kann ein europäisches System für die Cybersicherheitszertifizierung die Vertrauenswürdigkeitsstufen für europäische Cybersicherheitszertifikate und EU-Konformitätserklärungen, die im Rahmen dieses Systems ausgestellt werden, angeben. Jedes Zertifikat kann sich auf eine der Vertrauenswürdigkeitsstufen "niedrig", "mittel" oder "hoch" beziehen, wohingegen sich die EU-Konformitätserklärung nur auf die Vertrauenswürdigkeitsstufe "niedrig" beziehen kann. Die Vertrauenswürdigkeitsstufen geben einen entsprechenden Aufwand für die Bewertung vor und sind durch Bezugnahme auf die diesbezüglichen technischen Spezifikationen, Normen und Verfahren einschließlich technischer Prüfungen, deren Zweck in der Minderung oder Prävention der Gefahr von Cybervorfällen besteht, gekennzeichnet. Jede Vertrauenswürdigkeitsstufe sollte in den verschiedenen sektoralen Bereichen, in denen die Zertifizierung angewandt wird, einheitlich sein.

(56b) In einem europäisches System für die Cybersicherheitszertifizierung können je nach Strenge und Gründlichkeit der verwendeten Evaluierungsmethode mehrere Bewertungsniveaus angegeben werden, die jeweils einer der Vertrauenswürdigkeitsstufen entsprechen sollten und mit einer entsprechende Kombination von Vertrauenswürdigkeitskomponenten verknüpft sein sollten. Für alle Vertrauenswürdigkeitsstufen sollte das IKT-Produkt oder der IKT-Dienst eine Reihe sicherer Funktionen enthalten, die im System festgelegt sind, so u. a. eine voreingestellte sichere Konfiguration, signierten Code, ein sicheres Updateverfahren und Reduzierung von Exploits und eine vollständige Absicherung des Stapel/Heap-Speichers. Diese Funktionen sollten weiterentwickelt und gepflegt werden, wobei sicherheitsorientierte Entwicklungskonzepte und dazugehörige Instrumente zu verwenden sind, um sicherzustellen, dass wirksame Mechanismen (Software und Hardware) zuverlässig integriert werden. Bei der Vertrauenswürdigkeitsstufe "niedrig" sollte sich die Bewertung mindestens auf die folgenden Vertrauenswürdigkeitskomponenten stützen: Die Bewertung sollte mindestens eine Überprüfung der technischen Dokumentation des IKT-Produktes oder -Dienstes durch die Konformitätsbewertungsstelle umfassen. Betrifft die Zertifizierung IKT-Prozesse, sollte auch das Verfahren zur Konzipierung, Entwicklung und Pflege eines IKT-Produktes oder -Dienstes einer technischen Überprüfung unterzogen werden Ist in einem europäisches System für die Cybersicherheitszertifizierung eine Selbstbewertung der Konformität vorgesehen, so sollte es genügen, wenn der Hersteller oder Anbieter eine Selbstbewertung der Konformität des IKT-Prozesses, -Produktes oder -Dienstes mit dem Zertifizierungssystem vornimmt. Bei der Vertrauenswürdigkeitsstufe "mittel" sollte sich die Bewertung – zusätzlich zu den Komponenten bei der Vertrauenswürdigkeitsstufe "niedrig" – mindestens auf eine Überprüfung der Konformität der Sicherheitsfunktionen des IKT-Produkts oder -Dienstes mit seiner technischen Dokumentation stützen. Bei der Vertrauenswürdigkeitsstufe "hoch" sollte sich die Bewertung – zusätzlich zu den Komponenten bei der Vertrauenswürdigkeitsstufe "mittel" – mindestens auf einen Wirksamkeitstest stützen, bei dem die Widerstandsfähigkeit der Sicherheitsfunktionen des IKT-Produkts oder -Dienstes gegen Akteure mit umfangreichen Fähigkeiten und Ressourcen, die gründlich vorbereitete Cyberattacken durchführen.

(56c) Bei der Ausarbeitung der möglichen Systeme sollte die ENISA alle in Frage kommenden Interessenträger konsultieren, so beispielsweise europäische Normungsorganisationen, zuständige nationale Behörden, Organisationen, die auf Abkommen über die gegenseitige Anerkennung wie das MRA der SOG-IS beruhen, KMU, Verbraucherorganisationen und Interessenträger ökologischer und sozialer Interessen.

(56d) Die Agentur sollte eine eigene Website unterhalten, auf der sie über die europäischen Systeme für die Cybersicherheitszertifizierung informiert und für diese wirbt und auf der u. a. die Anträge für die Ausarbeitung eines möglichen europäischen Systems für die Cybersicherheitszertifizierung und das Feedback im Rahmen des Konsultationsverfahrens, das von der ENISA in der Ausarbeitungsphase durchgeführt wird, zur Verfügung stehen. Auf dieser Website sollten auch Informationen über die Zertifikate und die nach dieser Verordnung ausgestellten EU-Konformitäts-erklärungen bereitgestellt werden.

(57) Der Rückgriff auf eine europäische Cybersicherheitszertifizierung **und eine EU-Konformitätserklärung** sollte freiwillig bleiben, sofern in Rechtsvorschriften der Union oder in **entsprechend dem Unionsrecht erlassenen** einzelstaatlichen Rechtsvorschriften nichts anderes festgelegt ist. **Falls es keine harmonisierten Rechtsvorschriften gibt, können die Mitgliedstaaten nationale technische Vorschriften gemäß der Richtlinie (EU) 215/1535 erlassen, in denen die verbindliche Zertifizierung im Rahmen eines europäischen Systems für die Cybersicherheitszertifizierung vorgesehen ist. Die Mitgliedstaaten können auch im Zusammenhang mit öffentlichen Ausschreibungen und der Richtlinie 2014/214/EU auf eine europäische Cybersicherheitszertifizierung zurückgreifen.** [...]

(57a) Mit Blick auf die Ziele dieser Verordnung und zur Vermeidung einer Fragmentierung des Binnenmarkts sollten nationale Systeme oder Verfahren für die Cybersicherheitszertifizierung für die IKT-Produkte und -Dienste, die unter ein europäisches System für die Cybersicherheitszertifizierung fallen, ab dem Zeitpunkt unwirksam werden, den die Kommission in einem Durchführungsrechtsakt festlegt. Zudem sollten die Mitgliedstaaten keine neuen nationalen Systeme für die Cybersicherheitszertifizierung der IKT-Produkte und -Dienste einführen, die bereits unter ein geltendes europäisches System für die Cybersicherheitszertifizierung fallen. Allerdings sollte es den Mitgliedstaaten freistehen, aus Gründen der nationalen Sicherheit nationale Zertifizierungssysteme einzuführen oder beizubehalten.

(58) Sobald ein europäisches System für die Cybersicherheitszertifizierung verabschiedet worden ist, sollten Hersteller von IKT-Produkten und Anbieter von IKT-Diensten die Zertifizierung ihrer Produkte oder Dienste bei einer Konformitätsbewertungsstelle ihrer Wahl beantragen können. Die Konformitätsbewertungsstellen sollten, sofern sie bestimmten in dieser Verordnung festgelegten Anforderungen genügen, von einer Akkreditierungsstelle akkreditiert werden. Die Akkreditierung sollte für eine Höchstdauer von fünf Jahren erfolgen und unter denselben Bedingungen verlängert werden können, sofern die Konformitätsbewertungsstelle die Anforderungen erfüllt. Die Akkreditierungsstellen sollten die einer Konformitätsbewertungsstelle erteilte Akkreditierung **beschränken, aussetzen oder** widerrufen, wenn die Voraussetzungen für die Akkreditierung nicht oder nicht mehr erfüllt werden oder wenn eine Konformitätsbewertungsstelle Maßnahmen ergreift, die nicht mit dieser Verordnung vereinbar sind.

(59) [...] **Die** Mitgliedstaaten **sollten** eine [...] **oder mehrere B**ehörden für die Cybersicherheitszertifizierung [...] benennen, die die [...] Einhaltung **der sich aus dieser Verordnung ergebenden Verpflichtungen** [...] beaufsichtigt [...]. **Wenn ein Mitgliedstaat es für angemessen hält, können die Aufgaben auch bereits bestehenden Behörden zugewiesen werden. Ein Mitgliedstaat sollte auch im gegenseitigen Einvernehmen mit einem anderen Mitgliedstaat beschließen können, eine oder mehrere Aufsichtsbehörden im Hoheitsgebiet dieses anderen Mitgliedstaats zu benennen. Die Behörden sollten insbesondere die Verpflichtungen der in ihrem jeweiligen Hoheitsgebiet niedergelassenen Hersteller oder Anbieter von IKT-Produkten und -Diensten in Bezug auf die EU-Konformitätserklärung überwachen und durchsetzen, die nationalen Akkreditierungsstellen bei der Überwachung und Beaufsichtigung der Tätigkeiten der Konformitätsbewertungsstellen durch Bereitstellung von Sachkenntnis und einschlägigen Informationen unterstützen, Konformitätsbewertungsstellen ermächtigen, ihre Aufgaben wahrzunehmen, wenn sie in einem System festgelegte zusätzliche Anforderungen erfüllen, und einschlägige Entwicklungen auf dem Gebiet der Cybersicherheitszertifizierung verfolgen** [...]. Die nationalen [...] **B**ehörden für die **Cybersicherheitsz**ertifizierung sollten Beschwerden bearbeiten, die von natürlichen oder juristischen Personen in Bezug auf **die von ihnen ausgestellten Zertifikate oder** die von Konformitätsbewertungsstellen [...] ausgestellten Zertifikate **für die Vertrauenswürdigkeitsstufe "hoch"** eingereicht werden, den Beschwerdegegenstand, soweit angemessen, untersuchen und den Beschwerdeführer über die Fortschritte und das Ergebnis der Untersuchung innerhalb einer angemessenen Frist unterrichten. Darüber hinaus sollten sie mit anderen nationalen [...] **B**ehörden für die **Cybersicherheitsz**ertifizierung und anderen öffentlichen Stellen zusammenarbeiten, auch indem sie Informationen über die etwaige Nichtkonformität von IKT-Produkten und -Diensten mit den Anforderungen dieser Verordnung oder bestimmten europäischen Systemen für die Cybersicherheitszertifizierung austauschen.

(60) Für eine einheitliche Anwendung des europäischen Rahmens für die Cybersicherheitszertifizierung sollte eine europäische Gruppe für die Cybersicherheitszertifizierung (im Folgenden die "Gruppe") eingesetzt werden, die sich aus **Vertretern der** nationalen [...] **B**ehörden für die **Cybersicherheitsz**ertifizierung **oder anderer zuständiger nationaler Behörden** zusammensetzt. Die Gruppe sollte vor allem die Kommission bei ihren Tätigkeiten zur Gewährleistung einer einheitlichen Umsetzung und Anwendung des europäischen Rahmens für die Cybersicherheitszertifizierung beraten und unterstützen, die Agentur bei der Ausarbeitung der möglichen Cybersicherheitszertifizierungssysteme unterstützen und mit ihr eng zusammenarbeiten, der Kommission empfehlen, die Agentur mit der Ausarbeitung eines möglichen europäischen Systems für die Cybersicherheitszertifizierung zu beauftragen, sowie Stellungnahmen **an die Agentur zu möglichen Systemen und** an die Kommission zur Pflege und Überprüfung vorhandener europäischer Systeme für die Cybersicherheitszertifizierung abgeben.

(60a) Die Gruppe sollte den Austausch von bewährten Verfahren und Sachkenntnissen zwischen den nationalen Behörden für die Cybersicherheitszertifizierung, die für die Ermächtigung der Konformitätsbewertungsstellen und die Ausstellung von Zertifikaten zuständig sind, erleichtern. Die Gruppe sollte im Zusammenhang mit der Ausarbeitung eines möglichen Systems und seiner Umsetzung die Entwicklung eines Mechanismus der gegenseitigen Begutachtung für Stellen, die europäische Cybersicherheitszertifikate für die Vertrauenswürdigkeitsstufe "hoch" ausstellen, unterstützen. Bei solchen gegenseitigen Begutachtungen sollte insbesondere bewertet werden, ob die betreffenden Stellen über angemessene Sachkenntnisse verfügen und ihre Aufgaben einheitlich ausführen. Die Ergebnisse der gegenseitigen Begutachtungen sollten veröffentlicht werden. Diese Stellen können geeignete Maßnahmen ergreifen, um ihre Verfahren und Sachkenntnisse anzupassen.

(61) Zur Sensibilisierung und um die Akzeptanz künftiger EU-Cybersicherheitssysteme zu erhöhen, kann die Europäische Kommission allgemeine und sektorspezifische Cybersicherheitsleitlinien herausgeben, die sich beispielsweise auf bewährte Verfahren oder verantwortungsvolles Verhalten im Bereich der Cybersicherheit beziehen, und dabei die Vorteile der Verwendung zertifizierter IKT-Produkte und -Dienste hervorheben.

(61a) Da die IKT-Lieferketten weltumspannend sind, kann die Union zur weiteren Erleichterung des Handels gemäß Artikel 218 AEUV Abkommen über die gegenseitige Anerkennung von Zertifikaten schließen, die im Rahmen von Systemen ausgestellt wurden, die gemäß dem europäischen Rahmen für die Cybersicherheitszertifizierung eingerichtet wurden. Die Kommission kann unter Berücksichtigung der Ratschläge der ENISA und der europäischen Gruppe für die Cybersicherheitszertifizierung die Aufnahme entsprechender Verhandlungen empfehlen. In jedem System sollten spezifische Bedingungen für die gegenseitige Anerkennung mit Drittländern vorgesehen werden.

(62) [...]

(63) [...]

(64) Zur Gewährleistung einheitlicher Bedingungen für die Durchführung dieser Verordnung sollten der Kommission Durchführungsbefugnisse übertragen werden, wenn dies in dieser Verordnung vorgesehen ist. Diese Befugnisse sollten nach Maßgabe der Verordnung (EU) Nr. 182/2011 des Europäischen Parlaments und des Rates ausgeübt werden.

(65) Die Durchführungsrechtsakte über die europäischen Systeme für die Cybersicherheitszertifizierung von IKT-Produkten und -Diensten, die Modalitäten für die Durchführung von [...] **Untersuchungen** durch die Agentur sowie die Umstände, Formate und Verfahren der Notifizierung akkreditierter Konformitätsbewertungsstellen durch die nationalen [...] **B**ehörden für die **Cybersicherheitsz**ertifizierung bei der Kommission sollten nach dem Prüfverfahren erlassen werden.

(66) Die Tätigkeit der Agentur sollte unabhängig bewertet werden. Die Bewertung sollte sich darauf beziehen, inwieweit die Agentur ihre Ziele erreicht, wie sie arbeitet und inwieweit ihre Aufgaben relevant sind. Zudem sollten Wirkung, Wirksamkeit und Effizienz des europäischen Rahmens für Cybersicherheitszertifizierung bewertet werden.

(67) Die Verordnung (EG) Nr. 526/2013 sollte aufgehoben werden.

(68) Da die Ziele dieser Verordnung von den Mitgliedstaaten nicht ausreichend verwirklicht werden können, sondern vielmehr auf Unionsebene besser zu verwirklichen sind, kann die Union im Einklang mit dem in Artikel 5 des Vertrags über die Europäische Union verankerten Subsidiaritätsprinzip tätig werden. Entsprechend dem in demselben Artikel genannten Grundsatz der Verhältnismäßigkeit geht diese Verordnung nicht über das für die Verwirklichung dieser Ziele erforderliche Maß hinaus –

HABEN FOLGENDE VERORDNUNG ERLASSEN:

TITEL I
ALLGEMEINE BESTIMMUNGEN

Artikel 1

Gegenstand und Geltungsbereich

(1) Um das ordnungsgemäße Funktionieren des Binnenmarkts zu gewährleisten und um gleichzeitig in der Union ein hohes Niveau in der Cybersicherheit, bei der Fähigkeit zur Abwehr gegen Cyberangriffe und beim Vertrauen in die Cybersicherheit zu erreichen, wird in dieser Verordnung Folgendes festgelegt:

a) die Ziele, Aufgaben und organisatorischen Aspekte der "[...] **Agentur der Europäischen Union für Cybersicherheit**" (ENISA), im Folgenden die "Agentur", und

b) ein Rahmen für die Festlegung europäischer Zertifizierungssysteme für die Cybersicherheit, mit dem für IKT-**Prozesse,** Produkte und Dienste in der Union ein angemessenes Maß an Cybersicherheit gewährleistet werden soll. Dieser Rahmen gilt unbeschadet der in anderen Rechtsakten der Union festgelegten Bestimmungen in Bezug auf eine freiwillige oder verbindliche Zertifizierung.

(2) **Von dieser Verordnung unberührt bleiben die Zuständigkeiten der Mitgliedstaaten im Bereich der Cybersicherheit sowie auf jeden Fall Tätigkeiten in Bezug auf die öffentliche Sicherheit, die Landesverteidigung, die nationale Sicherheit und das staatliche Handeln im strafrechtlichen Bereich.**

Artikel 2

Begriffsbestimmungen

Für die Zwecke dieser Verordnung gelten folgende Begriffsbestimmungen:

1. "Cybersicherheit" umfasst alle Tätigkeiten, die notwendig sind, um Netz- und Informationssysteme, deren Nutzer und betroffene Personen vor Cyberbedrohungen zu schützen;

2. "Netz- und Informationssystem" bezeichnet ein System im Sinne von Artikel 4 Nummer 1 der Richtlinie (EU) 2016/1148;

3. "nationale Strategie für die Sicherheit von Netz- und Informationssystemen" bezeichnet einen Rahmen im Sinne von Artikel 4 Nummer 3 der Richtlinie (EU) 2016/1148;

4. "Betreiber wesentlicher Dienste" bezeichnet eine öffentliche oder private Einrichtung im Sinne von Artikel 4 Nummer 4 der Richtlinie (EU) 2016/1148;

5. "Anbieter digitaler Dienste" bezeichnet eine juristische Person, die einen digitalen Dienst im Sinne von Artikel 4 Nummer 6 der Richtlinie (EU) 2016/1148 anbietet;

6. "Sicherheitsvorfall" bezeichnet ein Ereignis im Sinne von Artikel 4 Nummer 7 der Richtlinie (EU) 2016/1148;

7. "Bewältigung von Sicherheitsvorfällen" bezeichnet alle Verfahren im Sinne von Artikel 4 Nummer 8 der Richtlinie (EU) 2016/1148;

8. "Cyberbedrohung" bezeichnet einen möglichen Umstand oder ein mögliches Ereignis, der bzw. das Netz- und Informationssysteme, deren Nutzer und betroffene Personen **schädigen, stören oder anderweitig** beeinträchtigen könnte;

9. "europäisches System für die Cybersicherheitszertifizierung" bezeichnet ein umfassendes, auf Unionsebene festgelegtes Paket von Vorschriften, technischen Anforderungen, Normen und Verfahren für die Zertifizierung **oder Konformitätsbewertung** von **Prozessen,** Produkten und Diensten der Informations- und Kommunikationstechnik (IKT), die von diesem System erfasst werden;

9a. "nationales System für die Cybersicherheitszertifizierung" bezeichnet ein umfassendes, von einer nationalen Behörde ausgearbeitetes und erlassenes Paket von Vorschriften, technischen Anforderungen, Normen und Verfahren für die Zertifizierung oder Konformitätsbewertung von IKT-Prozessen, -Produkten und -Diensten, die von diesem System erfasst werden;

10. "europäisches Cybersicherheitszertifikat" bezeichnet ein [...] Dokument, in dem bescheinigt wird, dass **ein bestimmter IKT-Prozess,** ein bestimmtes IKT-Produkt oder ein bestimmter IKT-Dienst **im Hinblick auf die Erfüllung** besonderer **Sicherheitsa**nforderungen, die in einem europäischen System für die Cybersicherheitszertifizierung festgelegt sind, [...] **bewertet wurde**;

11. "IKT-Produkt [...]" bezeichnet ein Element oder eine Gruppe von Elementen der Netz- und Informationssysteme;

11a. "IKT-Dienst" bezeichnet einen Dienst, der vollständig oder überwiegend aus der Übertragung, Speicherung, Abfrage oder Verarbeitung von Informationen mittels Netz- und Informationssystemen besteht;

11b. "IKT-Prozess" bezeichnet jegliche Tätigkeiten, mit denen ein ITK-Produkt oder -Dienst konzipiert, entwickelt, bereitgestellt oder gepflegt werden soll;

12. "Akkreditierung" bezeichnet die Akkreditierung im Sinne von Artikel 2 Nummer 10 der Verordnung (EG) Nr. 765/2008;

13. "nationale Akkreditierungsstelle" bezeichnet eine nationale Akkreditierungsstelle im Sinne von Artikel 2 Nummer 11 der Verordnung (EG) Nr. 765/2008;

14. "Konformitätsbewertung" bezeichnet die Konformitätsbewertung im Sinne von Artikel 2 Nummer 12 der Verordnung (EG) Nr. 765/2008;

15. "Konformitätsbewertungsstelle" bezeichnet eine Konformitätsbewertungsstelle im Sinne von Artikel 2 Nummer 13 der Verordnung (EG) Nr. 765/2008;

16. "Norm" bezeichnet eine Norm im Sinne von Artikel 2 Nummer 1 der Verordnung (EU) Nr. 1025/2012.

16a. "technische Spezifikation" bezeichnet ein Dokument, in dem die technischen Anforderungen vorgeschrieben sind, denen ein IKT-Prozess, -Produkt oder -Dienst genügen muss;

16b. "Vertrauenswürdigkeitsstufe" bezeichnet die Grundlage für das Vertrauen, dass ein IKT-Prozess, -Produkt oder -Dienst den Sicherheitsanforderungen eines spezifischen europäischen Systems für die Cybersicherheitszertifizierung genügt, und gibt an, auf welchem Niveau der Prozess, das Produkt oder der Dienst bei der Bewertung eingestuft wurde; mit der Vertrauenswürdigkeitsstufe wird nicht die Sicherheit eines IKT-Prozesses, -Produktes oder -Dienstes gemessen.

TITEL II

ENISA – die "*[...] die Agentur der Europäischen Union für Cybersicherheit*"

KAPITEL I

MANDAT *[...] UND* ZIELE *[...]*

Artikel 3

Mandat

(1) Die Agentur nimmt die ihr mit dieser Verordnung zugewiesenen Aufgaben mit dem Ziel wahr, zu einem hohen Maß an Cybersicherheit [...] **in** der **gesamten** Union beizutragen**, indem sie insbesondere die Mitgliedstaaten und die Organe, Einrichtungen und sonstigen Stellen der Union bei der Verbesserung der Cybersicherheit unterstützt**. **Die Agentur dient den Organen, Einrichtungen und sonstigen Stellen der Union als Bezugspunkt für Beratung und Sachkenntnis im Bereich Cybersicherheit.**

(2) Die Agentur nimmt die Aufgaben wahr, die ihr durch Rechtsakte der Union übertragen wurden, mit denen die Rechts- und Verwaltungsvorschriften der Mitgliedstaaten auf dem Gebiet der Cybersicherheit angeglichen werden sollen.

(2a) Die Agentur handelt bei der Wahrnehmung ihrer Aufgaben unabhängig und berücksichtigt umfassend die auf nationaler Ebene vorhandene Sachkenntnis der zuständigen Behörden der Mitgliedstaaten, wobei Doppelarbeit zu vermeiden ist.

(3) [...]

Artikel 4

Ziele

(1) Die Agentur soll aufgrund ihrer Unabhängigkeit, der wissenschaftlichen und technischen Qualität ihrer Beratung und Unterstützung, der von ihr bereitgestellten Informationen, der Transparenz ihrer operativen Verfahren und Arbeitsmethoden sowie der Sorgfalt bei der Wahrnehmung ihrer Aufgaben als Kompetenzzentrum in Fragen der Cybersicherheit dienen.

(2) Die Agentur unterstützt die Organe, Einrichtungen und sonstigen Stellen der Union sowie die Mitgliedstaaten bei der Ausarbeitung und Umsetzung von Strategien **der Union** im Zusammenhang mit der Cybersicherheit**, wozu auch sektorenbezogene Strategien zur Cybersicherheit gehören**.

(3) Die Agentur fördert unionsweit den Kapazitätsaufbau und die Abwehrbereitschaft, indem sie die **Organe, Einrichtungen und sonstigen Stellen der** Union, die Mitgliedstaaten sowie öffentliche und private Interessenträger dabei unterstützt, den Schutz ihrer Netz- und Informationssysteme zu verbessern**, Fähigkeiten zur Abwehr von Cyberangriffen und Reaktionskapazitäten aufzubauen und zu verbessern** und Fähigkeiten und Kompetenzen auf dem Gebiet der Cybersicherheit aufzubauen [...].

(4) Die Agentur fördert auf Unionsebene die Zusammenarbeit und Koordinierung zwischen den Mitgliedstaaten, den Organen, Einrichtungen und sonstigen Stellen der Union sowie den einschlägigen **private und öffentlichen** Interessenträgern [...] in Fragen, die im Zusammenhang mit der Cybersicherheit stehen.

(5) Die Agentur [...] **trägt zum Ausbau der** Cybersicherheitskapazitäten auf Unionsebene **bei** [...], um – vor allem bei grenzüberschreitenden Sicherheitsvorfällen – die [...] Mitgliedstaaten [...] **bei der** Vermeidung von Cyberbedrohungen oder [...] **der** Reaktion darauf **zu unterstützen** [...].

(6) Die Agentur fördert die Nutzung der Zertifizierung**, um der Fragmentierung der Zertifizierungssysteme in der EU vorzubeugen**. Die Agentur [...] **trägt insbesondere** zum Aufbau und zur Pflege eines Cybersicherheitszertifizierungsrahmens auf Unionsebene im Sinne des Titels III dieser Verordnung **bei** [...], um die auf mehr Transparenz gestützte Vertrauenswürdigkeit der Cybersicherheit von IKT-Produkten und -Diensten zu erhöhen und damit das Vertrauen in den digitalen Binnenmarkt zu stärken.

(7) Die Agentur fördert ein hohes Problembewusstsein der Bürger und Unternehmen in Fragen der Cybersicherheit.

KAPITEL IA
AUFGABEN

Artikel 5

[...] ***Entwicklung und Umsetzung der Unionspolitik und des Unionsrechts***

Die Agentur trägt zur Entwicklung und Umsetzung der Unionspolitik und des Unionsrechts bei, indem sie

(1) insbesondere durch unabhängige Stellungnahmen und durch vorbereitende Arbeiten zur Ausarbeitung und Überprüfung der Unionspolitik und des Unionsrechts auf dem Gebiet der Cybersicherheit Beratung und Unterstützung gewährt und indem sie sektorspezifische Strategien und Rechtsetzungsinitiativen im Bereich der Cybersicherheit vorlegt;

(2) die Mitgliedstaaten darin unterstützt, die Unionspolitik und das Unionsrecht auf dem Gebiet der Cybersicherheit, vor allem im Zusammenhang mit der Richtlinie (EU) 2016/1148, kohärent umzusetzen, auch durch Stellungnahmen, Leitlinien, Beratung und bewährte Verfahren zu Themen wie Risikomanagement, Meldung von Sicherheitsvorfällen und Informationsaustausch, und indem sie den Austausch bewährter Verfahren in diesem Bereich zwischen den zuständigen Behörden erleichtert;

(3) ihre Sachkenntnis und Unterstützung in die Arbeit der nach Artikel 11 der Richtlinie (EU) 2016/1148 eingesetzten Kooperationsgruppe einbringt;

(4) Folgendes unterstützt:

1. die Entwicklung und Umsetzung der Unionspolitik im Bereich der elektronischen Identität und Vertrauensdienste, vor allem durch Beratung und technische Leitlinien sowie durch die Erleichterung des Austauschs bewährter Verfahren zwischen den zuständigen Behörden;

2. die Förderung eines höheren Sicherheitsniveaus in der elektronischen Kommunikation, auch indem sie ihre Sachkenntnis und Beratung anbietet und den Austausch bewährter Verfahren zwischen den zuständigen Behörden erleichtert;

(5) die regelmäßige Überprüfung der Unionspolitik unterstützt und dazu einen Jahresbericht über die Stand der Umsetzung des jeweiligen Rechtsrahmens vorlegt in Bezug auf:

a) die Meldungen von Sicherheitsvorfällen durch die Mitgliedstaaten über die zentrale Anlaufstelle der Kooperationsgruppe nach Artikel 10 Absatz 3 der Richtlinie (EU) 2016/1148;

b) die Meldungen von Sicherheitsverletzungen und Integritätsverlusten bei Vertrauensdiensteanbietern, die der Agentur auf der Grundlage von Artikel 19 Absatz 3 der Verordnung (EU) Nr. 910/2014 von den Aufsichtsstellen übermittelt werden;

c) die Meldungen von Sicherheits**vorfällen** [...] durch Unternehmen, die öffentliche Kommunikationsnetze oder öffentlich zugängliche elektronische Kommunikationsdienste betreiben, die der Agentur von den zuständigen Behörden auf der Grundlage von Artikel 40 der [Richtlinie über den Europäischen Kodex für elektronische Kommunikation] übermittelt werden.

Artikel 6

[...] ***Kapazitätsaufbau***

(1) Die Agentur unterstützt

a) die Mitgliedstaaten bei ihren Bemühungen zur Verhütung, Erkennung und Analyse und zur Stärkung ihrer Kapazitäten für die Bewältigung von [...] **Cyberbedrohungen** und **Cybersicherheits**vorfällen [...], indem sie ihnen das erforderliche Wissen und die notwendigen Sachkenntnisse zur Verfügung stellt;

b) die Organe, Einrichtungen und sonstigen Stellen der Union bei ihren Bemühungen zur Verhütung, Erkennung und Analyse und zur Stärkung ihrer Kapazitäten für die Bewältigung von **Cyberbedrohungen** und **Cybersicherheits**vorfällen [...], indem sie **insbesondere** das CERT für die Organe, Agenturen und sonstigen Einrichtungen der Union (CERT-EU) angemessen unterstützt;

c) die Mitgliedstaaten auf deren Ersuchen beim Aufbau nationaler Computer-Notfallteams (CSIRTs) nach Artikel 9 Absatz 5 der Richtlinie (EU) 2016/1148;

d) die Mitgliedstaaten auf deren Ersuchen bei der Ausarbeitung nationaler Strategien für die Sicherheit von Netz- und Informationssystemen nach Artikel 7 Absatz 2 der Richtlinie (EU) 2016/1148; zudem fördert die Agentur die unionsweite Verbreitung dieser Strategien und verfolgt deren Umsetzung, um bewährte Verfahren bekannt zu machen;

e) die Organe der Union bei der Ausarbeitung und Überprüfung von Unionsstrategien zur Cybersicherheit, fördert deren Verbreitung und verfolgt die Fortschritte bei deren Umsetzung;

f) die CSIRTs der Mitgliedstaaten und der Union bei der Anhebung des Niveaus ihrer Fähigkeiten, auch durch die Förderung des Dialogs und Informationsaustauschs, damit jedes CSIRT entsprechend dem Stand der Technik einen gemeinsamen Satz an Minimalfähigkeiten hat und entsprechend der bewährten Praxis arbeitet;

g) die Mitgliedstaaten durch die Organisation [...] **regelmäßiger** Cybersicherheitsübungen auf Unionsebene nach Artikel 7 Absatz 6 und durch die Abgabe von Empfehlungen, die sie aus der Auswertung der Übungen und der bei diesen gemachten Erfahrungen ableitet;

h) einschlägige öffentliche Stellen, indem sie diesen, gegebenenfalls in Zusammenarbeit mit Interessenträgern, Fortbildungen zur Cybersicherheit anbietet;

i) die Kooperationsgruppe [...] **beim** Austausch bewährter Verfahren, vor allem zur Ermittlung der Betreiber wesentlicher Dienste durch die Mitgliedstaaten, auch im Zusammenhang mit grenzüberschreitenden Abhängigkeiten, im Hinblick auf Risiken und Sicherheitsvorfälle, nach Artikel 11 Absatz 3 Buchstabe l der Richtlinie (EU) 2016/1148.

(2) Die Agentur [...] **unterstützt den Informationsaustausch in und zwischen Sektoren**, vor allem in den in Anhang II der Richtlinie (EU) 2016/1148 genannten Sektoren, indem sie bewährte Verfahren und Leitlinien zu den verfügbaren Instrumenten und Verfahren sowie zur Bewältigung rechtlicher Fragen im Zusammenhang mit dem Informationsaustausch bereitstellt.

Artikel 7

[...] ***Operative Zusammenarbeit auf Unionsebene***

(1) Die Agentur unterstützt die operative Zusammenarbeit zwischen den **Mitgliedstaaten** und [...] **Organe, Einrichtungen und sonstigen** Stellen **der Union** untereinander und zwischen den Interessenträgern.

(2) Die Agentur arbeitet auf operativer Ebene mit den Organen, Einrichtungen und sonstigen Stellen der Union zusammen und entwickelt Synergien mit diesen Stellen, zu denen auch das CERT-EU sowie die für Cyberkriminalität und die Aufsicht über den Datenschutz zuständigen Stellen zählen, um Fragen von gemeinsamem Interesse anzugehen, unter anderem durch

a) den Austausch von Know-how und bewährten Verfahren;

b) die Bereitstellung von Beratung und Leitlinien zu einschlägigen Themen im Zusammenhang mit der Cybersicherheit;

c) die Festlegung praktischer Modalitäten für die Wahrnehmung besonderer Aufgaben in Absprache mit der Kommission.

(3) Die Agentur führt die Sekretariatsgeschäfte des CSIRTs-Netzes nach Artikel 12 Absatz 2 der Richtlinie (EU) 2016/1148 und erleichtert [...] **in dieser Eigenschaft** den Informationsaustausch und die Zusammenarbeit zwischen dessen Mitgliedern.

(4) Die Agentur [...] **fördert die** operative Zusammenarbeit innerhalb des CSIRTs-Netzes [...] und unterstützt **dabei** die Mitgliedstaaten **auf deren Ersuchen hin**, indem sie

a) diese berät, wie sie ihre Fähigkeiten zur Verhütung, Erkennung und Bewältigung von Sicherheitsvorfällen verbessern können;

b) [...] **die technische Bewältigung von** Sicherheitsvorfällen mit beträchtlichen oder erheblichen Auswirkungen [...] **erleichtert, insbesondere auch durch die Unterstützung der freiwilligen Weitergabe technischer Lösungen zwischen den Mitgliedstaaten**;

c) Anfälligkeiten [...] und Sicherheitsvorfälle analysiert.

ca) die nachträglichen technischen Untersuchungen von Sicherheitsvorfällen mit beträchtlichen oder erheblichen Auswirkungen gemäß der Richtlinie (EU) 2016/1148 unterstützt.

Bei der Wahrnehmung dieser Aufgaben arbeiten die Agentur und das CERT-EU in strukturierter Weise zusammen, um [...] Synergien nutzen zu können **und Doppelarbeit zu vermeiden**.

(5) [...]

[...]

(6) Die Agentur organisiert auf Unionsebene [...] **regelmäßige** Cybersicherheitsübungen und unterstützt die Mitgliedstaaten und die Organe, Einrichtungen und sonstigen Stellen der EU auf deren Ersuchen hin bei der Organisation solcher Übungen. [...] **Diese** Übungen auf Unionsebene **können** technische, operative [...] **oder** strategische Elemente umfassen [...]. **Alle zwei Jahre wird eine Großübung organisiert, die all diese Element enthält.** Die Agentur unterstützt gemeinsam mit den betreffenden [...] **Organisationen** gegebenenfalls auch die Organisation sektorspezifischer Cybersicherheitsübungen[...]**, wobei diese Organisationen** an den Cybersicherheitsübungen auf Unionsebene teilnehmen können.

(7) Die Agentur erstellt **in enger Zusammenarbeit mit den Mitgliedstaaten** regelmäßig einen technischen Lagebericht über die Cybersicherheit in der EU auf der Grundlage von frei zugänglichen Informationen, eigenen Analysen und Berichten, die ihr u. a. übermittelt werden von den CSIRTs der Mitgliedstaaten [...] oder den zentralen Anlaufstellen im Sinne der NIS-Richtlinie (**beide auf freiwilliger Basis** [...]) sowie dem bei Europol angesiedelten Europäischen Zentrum zur Bekämpfung der Cyberkriminalität (EC3) und dem CERT-EU.

(8) Die Agentur trägt zur Entwicklung gemeinsamer Maßnahmen bei, mit denen auf Ebene der Union und der Mitgliedstaaten auf massive, grenzüberschreitende Cybersicherheitsvorfälle oder Cyberkrisen reagiert werden kann, indem sie insbesondere:

a) **auf freiwilliger Grundlage bereitgestellte** Berichte aus nationalen Quellen als Beitrag zu einer gemeinsamen Lageerfassung zusammenstellt;

b) für einen effizienten Informationsfluss und Mechanismen sorgt, die zwischen dem CSIRTs-Netz und den fachlichen und politischen Entscheidungsträgern auf EU-Ebene eine abgestufte Vorgehensweise ermöglichen;

c) **auf Ersuchen von Mitgliedstaaten** die technische Bewältigung eines Sicherheitsvorfalls oder einer Krise [...] **erleichtert**, **insbesondere** auch durch die [...] **Unterstützung** der **freiwilligen** Weitergabe technischer Lösungen zwischen den Mitgliedstaaten

d) **die Organen, Einrichtungen und sonstigen Stellen der Union und auf Ersuchen die Mitgliedstaaten bei der** öffentlichen Kommunikation im Umfeld des Sicherheitsvorfalls oder der Krise unterstützt;

e) die **Mitgliedstaaten auf deren Ersuchen hin beim Testen der** Kooperationspläne für die Reaktion auf solche Sicherheitsvorfälle oder Krisen [...] **unterstützt**.

Artikel 8

*[...] **Markt,** [...] **Cybersicherheitszertifizierung und** [...] **Normung***

Die Agentur

a) unterstützt und fördert die Entwicklung und Umsetzung der Unionspolitik auf dem Gebiet der Cybersicherheitszertifizierung von IKT**-Prozessen,** -Produkten und -Diensten, wie in Titel III dieser Verordnung festgelegt, indem sie

1. mögliche europäische Cybersicherheitszertifizierungssysteme für die IT-Sicherheit von IKT**-Prozessen,** -Produkten und -Diensten **in Zusammenarbeit mit der Branche und** nach Artikel 44 dieser Verordnung ausarbeitet;

2. die Kommission bei der Wahrnehmung der Sekretariatsgeschäfte der nach Artikel 53 eingesetzten Gruppe für die Cybersicherheitszertifizierung unterstützt;

3. in Zusammenarbeit mit nationalen [...] **B**ehörden für die [...] **Cybersicherheitsz**ertifizierung und der Branche Leitlinien zusammenstellt und veröffentlicht sowie bewährte Verfahren im Zusammenhang mit den Anforderungen an die Cybersicherheit von IKT-Produkten und -Diensten entwickelt;

3a. in Fällen, in denen keine Normen zur Verfügung stehen, geeignete technische Spezifikationen nach Artikel 47 Absatz 1 Buchstabe b empfiehlt, die der Entwicklung europäischer Systeme für die Cybersicherheitszertifizierung dienen;

3b. anhand der Zusammenstellung und Veröffentlichung von Leitlinien zu einem hinreichenden Kapazitätsaufbau im Zusammenhang mit den Bewertungs- und Zertifizierungsverfahren beiträgt, sowie die Mitgliedstaaten auf deren Ersuchen hin unterstützt;

b) erleichtert die Ausarbeitung und Übernahme europäischer und internationaler Normen für das Risikomanagement und die Sicherheit von IKT-**Prozessen,** -Produkten und -Diensten [...]**;**

ba) bietet nach Artikel 19 Absatz 2 der Richtlinie (EU) 2016/1148 in Zusammenarbeit mit den Mitgliedstaaten Beratung an und erlässt Leitlinien für die technischen Bereiche, die sich auf die Sicherheitsanforderungen für Betreiber wesentlicher Dienste und Anbieter digitaler Dienste beziehen, sowie für bereits vorhandene Normen, auch nationale Normen der Mitgliedstaaten;

c) führt regelmäßig Analysen der wichtigsten Angebots- und Nachfragetrends auf dem Cybersicherheitsmarkt durch, um den Cybersicherheitsmarkt in der Union zu fördern.

Artikel 9

[...] ***Wissen*** [...] *und* ***Informationen*** [...]

Die Agentur

a) führt Analysen neu entstehender Technik durch und bietet themenspezifische Bewertungen der von den technischen Innovationen zu erwartenden gesellschaftlichen, rechtlichen, wirtschaftlichen und regulatorischen Auswirkungen auf die Cybersicherheit;

b) führt langfristige strategische Analysen der Cybersicherheitsbedrohungen und Sicherheitsvorfälle durch, um neu auftretende Trends erkennen und dazu beitragen zu können, [...] Cybersicherheit**svorfälle** zu vermeiden;

c) stellt in Zusammenarbeit mit den Sachverständigen der Behörden der Mitgliedstaaten Beratung, Leitlinien und bewährte Verfahren für die Sicherheit der Netz- und Informationssysteme zur Verfügung, vor allem für die Sicherheit [...] der Infrastrukturen, die die in Anhang II der Richtlinie (EU) 2016/1148 aufgeführten Sektoren unterstützen**, und der Infrastrukturen, die von den in Anhang III der genannten Richtlinie aufgeführten Anbietern digitaler Dienste genutzt werden**;

d) bündelt die von den Organen, Einrichtungen und sonstigen Stellen der Union **sowie auf freiwilliger Grundlage von den Mitgliedstaaten und privaten und öffentlichen Interessenträgern** bereitgestellten Informationen zur IT-Sicherheit, ordnet diese Informationen und stellt sie über ein eigenes Portal der Öffentlichkeit zur Verfügung;

e) [...]

f) erhebt und analysiert öffentlich verfügbare Informationen über signifikante Sicherheitsvorfälle und stellt Berichte mit dem Ziel zusammen, den Unternehmen und Bürgern unionsweit Orientierungshilfen an die Hand zu geben

g) [...].

Artikel 9a

Sensibilisierung und Ausbildung

Die Agentur

a) sensibilisiert die Öffentlichkeit für Cybersicherheitsrisiken und stellt Leitlinien für bewährte Vorgehensweisen für einzelne Nutzer zur Verfügung, die sich an Bürger und Organisationen richten;

b) organisiert in Zusammenarbeit mit den Mitgliedstaaten, den Organen, Einrichtungen und sonstigen Stellen der Union und der Branche regelmäßige Aufklärungskampagnen, um die Cybersicherheit und ihre Sichtbarkeit in der Union zu erhöhen;

c) unterstützt die Mitgliedstaaten bei ihren Anstrengungen zur Sensibilisierung zu Cybersicherheit und zur Förderung der Ausbildung zu Cybersicherheit;

d) unterstützt eine engere Koordinierung und den Austausch bewährter Vorgehensweisen zwischen den Mitgliedstaaten in Bezug auf Ausbildung und Sensibilisierung zu Cybersicherheit, indem sie die Einrichtung und Unterhaltung eines Netzes von Bildungskontaktstellen erleichtert.

Artikel 10

*[...] **Forschung und Innovation***

Im Zusammenhang mit der Forschung und Innovation

a) berät die Agentur die Union und die Mitgliedstaaten zum Forschungsbedarf und zu den Forschungsprioritäten im Bereich der Cybersicherheit, damit die Voraussetzung für wirksame Reaktionen auf die gegenwärtigen oder sich abzeichnenden Risiken und Bedrohungen, auch in Bezug auf neue und aufkommende Informations- und Kommunikationstechnik (IKT), geschaffen und die Techniken zur Risikovermeidung genutzt werden können;

b) beteiligt sich die Agentur dort, wo die Kommission ihr die einschlägigen Befugnisse übertragen hat, an der Durchführungsphase von Förderprogrammen für Forschung und Innovation oder als Begünstige.

Artikel 11

[...] ***Internationale Zusammenarbeit***

Die Agentur unterstützt die Bemühungen der Union um Zusammenarbeit mit Drittländern und internationalen Organisationen, um die internationale Zusammenarbeit in Angelegenheiten der Cybersicherheit zu fördern, indem sie

a) soweit zweckmäßig – bei der Organisation von internationalen Übungen als Beobachterin mitwirkt, die Ergebnisse solcher Übungen analysiert und sie dem Verwaltungsrat vorlegt;

b) [...] **innerhalb der einschlägigen Rahmen für internationale Zusammenarbeit** den Austausch bewährter Verfahren [...] erleichtert;

c) der Kommission auf deren Ersuchen mit Sachkenntnis zur Seite steht**;**

ca) die Kommission in Zusammenarbeit mit der nach Artikel 53 eingesetzten Europäischen Gruppe für die Cybersicherheitszertifizierung bei Fragen zu Abkommen über die gegenseitige Anerkennung von Cybersicherheitszertifikaten mit Drittländern berät und unterstützt.

KAPITEL II
AUFBAU DER AGENTUR

Artikel 12

Struktur

Die Verwaltungs- und Leitungsstruktur der Agentur setzt sich wie folgt zusammen:

a) einem Verwaltungsrat, der die in Artikel 14 genannten Funktionen ausübt;

b) einem Exekutivrat, der die in Artikel 18 genannten Funktionen ausübt;

c) einem Exekutivdirektor, der die in Artikel 19 genannten Zuständigkeiten wahrnimmt;

d) einer Ständigen Gruppe der Interessenträger, die die in Artikel 20 genannten Funktionen ausübt**;**

da) einem Netz der nationalen Verbindungsbeamten, das die in Artikel 20 genannten Funktionen ausübt.

ABSCHNITT 1
VERWALTUNGSRAT

Artikel 13

Zusammensetzung des Verwaltungsrats

(1) Dem Verwaltungsrat gehören je ein Vertreter jedes Mitgliedstaats und zwei von der Kommission ernannte Vertreter an. Alle Vertreter verfügen über Stimmrecht.

(2) Jedes Mitglied des Verwaltungsrats hat einen Stellvertreter, der das Mitglied im Fall seiner Abwesenheit vertritt.

(3) Die Mitglieder des Verwaltungsrats und ihre Stellvertreter werden aufgrund ihrer Kenntnisse auf dem Gebiet der Cybersicherheit ernannt, wobei ihren einschlägigen Management-, Verwaltungs- und Haushaltsführungskompetenzen Rechnung zu tragen ist. Die Kommission und die Mitgliedstaaten bemühen sich, die Fluktuation bei ihren Vertretern im Verwaltungsrat gering zu halten, um die Kontinuität der Arbeit des Verwaltungsrats sicherzustellen. Die Kommission und die Mitgliedstaaten setzen sich für eine ausgewogene Vertretung von Frauen und Männern im Verwaltungsrat ein.

(4) Die Amtszeit der Mitglieder des Verwaltungsrats und ihrer Stellvertreter beträgt vier Jahre. Sie kann verlängert werden.

Artikel 14

Aufgaben des Verwaltungsrats

(1) Der Verwaltungsrat

a) bestimmt die allgemeine Ausrichtung der Tätigkeit der Agentur und sorgt auch dafür, dass die Agentur bei ihrer Arbeit die in dieser Verordnung niedergelegten Vorschriften und Grundsätze beachtet. Er sorgt zudem für die Abstimmung der Arbeit der Agentur mit den Tätigkeiten, die von den Mitgliedstaaten und auf Unionsebene durchgeführt werden;

b) nimmt den Entwurf des in Artikel 21 genannten einheitlichen Programmplanungsdokuments der Agentur an, bevor dieser der Kommission zur Stellungnahme vorgelegt wird;

c) nimmt – unter Berücksichtigung der Stellungnahme der Kommission – das einheitliche Programmplanungsdokument der Agentur nach Artikel 17 mit der Zweidrittelmehrheit seiner Mitglieder an;

ca) überwacht die Umsetzung der im einheitlichen Programmplanungsdokument enthaltenen mehrjährigen und jährlichen Programmplanung ;

d) stellt mit der Zweidrittelmehrheit seiner Mitglieder den jährlichen Haushaltsplan der Agentur fest und übt andere Funktionen in Bezug auf den Haushalt der Agentur gemäß Kapitel III aus;

e) bewertet und genehmigt den konsolidierten Jahresbericht über die Tätigkeiten der Agentur und übermittelt den Bericht zusammen mit seiner Bewertung bis zum 1. Juli des folgenden Jahres dem Europäischen Parlament, dem Rat, der Kommission und dem Rechnungshof. Der Jahresbericht enthält den Jahresabschluss und Ausführungen darüber, inwiefern die Agentur die vorgegebenen Leistungsindikatoren erfüllt hat. Der Jahresbericht wird veröffentlicht;

f) erlässt nach Artikel 29 die für die Agentur geltende Finanzregelung;

g) nimmt eine Betrugsbekämpfungsstrategie an, die den diesbezüglichen Risiken entspricht und an einer Kosten-Nutzen-Analyse der durchzuführenden Maßnahmen orientiert ist;

h) erlässt Vorschriften zur Unterbindung und Bewältigung von Interessenkonflikten bei seinen Mitgliedern;

i) sorgt ausgehend von den Erkenntnissen und Empfehlungen, die sich aus den Untersuchungen des Europäischen Amtes für Betrugsbekämpfung (OLAF) und den verschiedenen internen und externen Prüfberichten und Bewertungen ergeben haben, für angemessene Folgemaßnahmen;

j) gibt sich eine Geschäftsordnung;

k) nimmt nach Absatz 2 in Bezug auf das Personal der Agentur die Befugnisse wahr, die der Anstellungsbehörde durch das Statut der Beamten der Europäischen Union bzw. der Stelle, die zum Abschluss der Dienstverträge ermächtigt ist, durch die Beschäftigungsbedingungen für die sonstigen Bediensteten der Europäischen Union übertragen wurden ("Befugnisse der Anstellungsbehörde");

l) erlässt gemäß dem Verfahren des Artikels 110 des Statuts der Beamten Durchführungsbestimmungen zum Statut der Beamten und zu den Beschäftigungsbedingungen für die sonstigen Bediensteten;

m) ernennt den Exekutivdirektor und verlängert gegebenenfalls dessen Amtszeit oder enthebt ihn nach Artikel 33 seines Amtes;

n) ernennt einen Rechnungsführer, bei dem es sich um den Rechnungsführer der Kommission handeln kann, der in der Wahrnehmung seiner Aufgaben völlig unabhängig ist;

o) fasst unter Berücksichtigung der Tätigkeitserfordernisse der Agentur und unter Beachtung der Grundsätze einer wirtschaftlichen Haushaltsführung alle Beschlüsse über die Schaffung und, falls notwendig, Änderung der Organisationsstruktur der Agentur;

p) genehmigt den Abschluss von Arbeitsvereinbarungen nach Artikel 7 und Artikel 39.

(2) Der Verwaltungsrat fasst gemäß nach Artikel 110 des Statuts der Beamten, einen Beschluss auf der Grundlage von Artikel 2 Absatz 1 des Statuts der Beamten und von Artikel 6 der Beschäftigungsbedingungen für die sonstigen Bediensteten, mit dem er die einschlägigen Befugnisse einer Anstellungsbehörde dem Exekutivdirektor überträgt und die Bedingungen festlegt, unter denen die Befugnisübertragung ausgesetzt werden kann. Der Exekutivdirektor kann diese Befugnisse einer nachgeordneten Ebene übertragen.

(3) Wenn außergewöhnliche Umstände dies erfordern, kann der Verwaltungsrat durch Beschluss die Übertragung der Befugnisse der Anstellungsbehörde auf den Exekutivdirektor sowie die von diesem vorgenommene Weiterübertragung von Befugnissen vorübergehend aussetzen und die Befugnisse selbst ausüben oder sie einem seiner Mitglieder oder einem anderen Bediensteten als dem Exekutivdirektor übertragen.

Artikel 15

Vorsitz des Verwaltungsrats

Der Verwaltungsrat wählt aus dem Kreis seiner Mitglieder mit der Zweidrittelmehrheit seiner Mitglieder einen Vorsitzenden und einen stellvertretenden Vorsitzenden für die Dauer von vier Jahren, wobei eine einmalige Wiederwahl zulässig ist. Endet jedoch ihre Mitgliedschaft im Verwaltungsrat während ihrer Amtszeit, so endet auch ihre Amtszeit automatisch am selben Tag. Der stellvertretende Vorsitzende tritt im Fall der Verhinderung des Vorsitzenden von Amts wegen an dessen Stelle.

Artikel 16

Sitzungen des Verwaltungsrats

(1) Der Verwaltungsrat wird von seinem Vorsitzenden einberufen.

(2) Der Verwaltungsrat tritt mindestens zweimal jährlich zu einer ordentlichen Sitzung zusammen. Auf Antrag des Vorsitzenden, der Kommission oder mindestens eines Drittels seiner Mitglieder tritt er darüber hinaus zu außerordentlichen Sitzungen zusammen.

(3) Der Exekutivdirektor nimmt an den Sitzungen des Verwaltungsrats ohne Stimmrecht teil.

(4) Mitglieder der Ständigen Gruppe der Interessenträger können auf Einladung des Vorsitzes an den Sitzungen des Verwaltungsrats ohne Stimmrecht teilnehmen.

(5) Die Mitglieder des Verwaltungsrats und ihre Stellvertreter können sich nach Maßgabe seiner Geschäftsordnung von Beratern oder Experten unterstützen lassen.

(6) Die Sekretariatsgeschäfte des Verwaltungsrats werden von der Agentur wahrgenommen.

Artikel 17

Vorschriften für die Abstimmung im Verwaltungsrat

(1) Der Verwaltungsrat fasst seine Beschlüsse mit der Mehrheit seiner Mitglieder.

(2) Für die Annahme des einheitlichen Programmplanungsdokuments und des jährlichen Haushaltsplans sowie für die Ernennung, die Verlängerung der Amtszeit oder die Abberufung des Exekutivdirektors ist eine Mehrheit von zwei Dritteln aller Mitglieder des Verwaltungsrats erforderlich.

(3) Jedes Mitglied hat eine Stimme. In Abwesenheit eines Mitglieds kann sein Stellvertreter dessen Stimmrecht ausüben.

(4) Der Vorsitzende nimmt an den Abstimmungen teil.

(5) Der Exekutivdirektor nimmt nicht an den Abstimmungen teil.

(6) Die näheren Einzelheiten der Abstimmungsmodalitäten, insbesondere die Voraussetzungen, unter denen ein Mitglied im Namen eines anderen Mitglieds handeln kann, werden in der Geschäftsordnung des Verwaltungsrats festgelegt.

ABSCHNITT 2
EXEKUTIVRAT

Artikel 18

Exekutivrat

(1) Der Verwaltungsrat wird von einem Exekutivrat unterstützt.

(2) Der Exekutivrat

a) bereitet die Beschlussvorlagen für den Verwaltungsrat vor;

b) stellt zusammen mit dem Verwaltungsrat sicher, dass ausgehend von den Ergebnissen und Empfehlungen im Rahmen der Untersuchungen des OLAF und der externen oder internen Prüfberichte und Bewertungen angemessene Folgemaßnahmen getroffen werden;

c) unterstützt und berät unbeschadet der Aufgaben des Exekutivdirektors nach Artikel 19 den Exekutivdirektor bei der Umsetzung der verwaltungs- und haushaltsbezogenen Beschlüsse des Verwaltungsrats.

(3) Der Exekutivrat besteht aus fünf Mitgliedern, die aus den Reihen der Mitglieder des Verwaltungsrats ernannt werden; darunter befinden sich der Vorsitzende des Verwaltungsrats, der zugleich auch Vorsitzender des Exekutivrats sein kann, und einer der Vertreter der Kommission. Der Exekutivdirektor nimmt an den Sitzungen des Exekutivrats ohne Stimmrecht teil.

(4) Die Amtszeit der Mitglieder des Exekutivrats beträgt vier Jahre. Sie kann verlängert werden.

(5) Der Exekutivrat tritt mindestens einmal alle drei Monate zusammen. Der Vorsitzende des Exekutivrats beruft auf Antrag der Mitglieder zusätzliche Sitzungen ein.

(6) Der Verwaltungsrat legt die Geschäftsordnung des Exekutivrats fest.

(7) [...]

ABSCHNITT 3
EXEKUTIVDIREKTOR

Artikel 19

Zuständigkeiten des Exekutivdirektors

(1) Die Agentur wird von ihrem Exekutivdirektor geleitet, der bei der Wahrnehmung seiner Aufgaben unabhängig ist. Der Exekutivdirektor ist gegenüber dem Verwaltungsrat rechenschaftspflichtig.

(2) Der Exekutivdirektor erstattet dem Europäischen Parlament über die Erfüllung seiner Aufgaben Bericht, wenn er dazu aufgefordert wird. Der Rat kann den Exekutivdirektor auffordern, über die Erfüllung seiner Aufgaben Bericht zu erstatten.

(3) Der Exekutivdirektor ist dafür verantwortlich,

a) die laufenden Geschäfte der Agentur zu führen;

b) die vom Verwaltungsrat gefassten Beschlüsse umzusetzen;

c) den Entwurf des einheitlichen Programmplanungsdokuments auszuarbeiten und dem Verwaltungsrat vor der Übermittlung an die Kommission vorzulegen;

d) das einheitliche Programmplanungsdokument umzusetzen und dem Verwaltungsrat hierüber Bericht zu erstatten;

e) den konsolidierten Jahresbericht über die Tätigkeit der Agentur**, einschließlich der Umsetzung des jährlichen Arbeitsprogramms,** auszuarbeiten und dem Verwaltungsrat zur Bewertung und Annahme vorzulegen;

f) einen Aktionsplan mit Folgemaßnahmen zu den Schlussfolgerungen der nachträglichen Bewertungen auszuarbeiten und alle zwei Jahre der Kommission über die erzielten Fortschritte Bericht zu erstatten;

g) einen Aktionsplan mit Folgemaßnahmen zu den Schlussfolgerungen interner oder externer Prüfberichte sowie der Untersuchungen des Europäischen Amtes für Betrugsbekämpfung (OLAF) auszuarbeiten und der Kommission zweimal jährlich und dem Verwaltungsrat regelmäßig über die erzielten Fortschritte Bericht zu erstatten;

h) den Entwurf der für die Agentur geltenden Finanzregelung auszuarbeiten;

i) den Entwurf des Voranschlags der Einnahmen und Ausgaben der Agentur auszuarbeiten und ihren Haushaltsplan auszuführen;

j) die finanziellen Interessen der Union durch vorbeugende Maßnahmen gegen Betrug, Korruption und sonstige rechtswidrige Handlungen, durch wirksame Kontrollen und, falls Unregelmäßigkeiten festgestellt werden, durch Einziehung zu Unrecht gezahlter Beträge sowie gegebenenfalls durch Verhängung wirksamer, verhältnismäßiger und abschreckender verwaltungsrechtlicher und finanzieller Sanktionen zu schützen;

k) eine Betrugsbekämpfungsstrategie für die Agentur auszuarbeiten und dem Verwaltungsrat zur Genehmigung vorzulegen;

l) Kontakte zur Wirtschaft und zu Verbraucherorganisationen im Hinblick auf einen regelmäßigen Dialog mit den einschlägigen Interessenträgern aufzubauen und zu pflegen;

la) einen regelmäßigen Austausch mit den Organen, Einrichtungen und sonstigen Stellen der Union über deren Tätigkeiten im Bereich Cybersicherheit zu führen, um die Kohärenz bei der Weiterentwicklung und Umsetzung der EU-Politik sicherzustellen;

m) sonstige dem Exekutivdirektor durch diese Verordnung übertragene Aufgaben wahrzunehmen.

(4) Soweit erforderlich kann der Exekutivdirektor im Rahmen des Mandats der Agentur sowie entsprechend ihren Zielen und Aufgaben Ad-hoc-Arbeitsgruppen aus Sachverständigen – auch von den zuständigen Behörden der Mitgliedstaaten – einsetzen. Der Verwaltungsrat wird hiervon vorab unterrichtet. Die Verfahren, die insbesondere die Zusammensetzung dieser Arbeitsgruppen, die Bestellung der Sachverständigen der Arbeitsgruppen durch den Exekutivdirektor und die Arbeitsweise der Arbeitsgruppen betreffen, werden in den internen Verfahrensvorschriften der Agentur festgelegt.

(5) Der Exekutivdirektor **kann auf der Grundlage einer angemessenen Kosten-Nutzen-Analyse erforderlichenfalls** beschließen, [...] **eine oder mehrere Außenstellen** in einem oder mehreren Mitgliedstaaten [...]**einzurichten**, damit die Agentur ihre Aufgaben effizient und wirksam wahrnehmen kann. Bevor er über die Einrichtung einer Außenstelle beschließt, **ersucht der Exekutivdirektor den/die betreffenden Mitgliedstaat(en), einschließlich des Mitgliedstaats, in dem die Agentur ihren Sitz hat, um eine Stellungnahme, und er**holt [...] die vorherige Zustimmung der Kommission [...] **und** des Verwaltungsrats [...] ein. **Im Falle von Meinungsverschiedenheiten bei der Konsultation zwischen dem Exekutivdirektor und den betreffenden Mitgliedstaaten werden die strittigen Fragen dem Rat zur Erörterung vorgelegt.** In dem Beschluss wird der Umfang der in der Außenstelle auszuübenden Tätigkeiten so festgelegt, dass unnötige Kosten und eine Überschneidung der Verwaltungsfunktionen mit denen der Agentur vermieden werden.[...] **Die Anzahl der Mitarbeiter in allen Außenstellen ist möglichst gering zu halten und darf insgesamt nicht 40 % der Anzahl der Mitarbeiter im Mitgliedstaat, in dem die Agentur ihren Sitz hat, überschreiten. [...] Die Anzahl der Mitarbeiter in jeder Außenstelle darf nicht 10 % der Anzahl der Mitarbeiter im Mitgliedstaat, in dem die Agentur ihren Sitz hat, überschreiten.**

ABSCHNITT 4
STÄNDIGE GRUPPE DER INTERESSENVERTRETER

Artikel 20

Ständige Gruppe der Interessenvertreter

(1) Der Verwaltungsrat setzt auf Vorschlag des Exekutivdirektors eine Ständige Gruppe der Interessenträger ein, die sich aus anerkannten Sachverständigen als Vertreter der einschlägigen Interessenträger zusammensetzt, darunter die IKT-Branche, Anbieter öffentlich zugänglicher elektronischer Kommunikationsnetze oder -dienste, **Betreiber wesentlicher Dienste,** Verbrauchergruppen, wissenschaftliche Sachverständige für die Cybersicherheit sowie Vertreter der zuständigen Behörden, die gemäß der [Richtlinie über den Europäischen Kodex für elektronische Kommunikation] notifiziert wurden, sowie Strafverfolgungsbehörden und Datenschutz-Aufsichtsbehörden.

(2) Die Verfahren für die Ständige Gruppe der Interessenträger, die insbesondere die Anzahl, die Zusammensetzung, die Ernennung der Mitglieder durch den Verwaltungsrat, den Vorschlag des Exekutivdirektors und die Arbeitsweise der Gruppe betreffen, werden in den internen Verfahrensvorschriften der Agentur festgelegt und öffentlich bekannt gemacht.

(3) Den Vorsitz der Ständigen Gruppe der Interessenträger führt der Exekutivdirektor oder eine vom Exekutivdirektor jeweils ernannte Person.

(4) Die Amtszeit der Mitglieder der Ständigen Gruppe der Interessenträger beträgt zweieinhalb Jahre. Die Mitglieder des Verwaltungsrats dürfen nicht Mitglieder der Ständigen Gruppe der Interessenträger sein. Sachverständige der Kommission und aus den Mitgliedstaaten können an den Sitzungen der Ständigen Gruppe der Interessenträger teilnehmen und an ihrer Arbeit mitwirken. Vertreter anderer Stellen, die vom Exekutivdirektor für relevant erachtet werden und die der Ständigen Gruppe der Interessenträger nicht angehören, können zur Teilnahme an den Sitzungen der Ständigen Gruppe der Interessenträger und zur Mitarbeit an ihrer Arbeit eingeladen werden.

(5) Die Ständige Gruppe der Interessenträger berät die Agentur bei der Durchführung ihrer Tätigkeiten. Sie berät insbesondere den Exekutivdirektor bei der Ausarbeitung eines Vorschlags für das Arbeitsprogramm der Agentur und bei der Gewährleistung der Kommunikation mit den einschlägigen Interessenträgern bezüglich aller Fragen im Zusammenhang mit dem Arbeitsprogramm.

(5a) Die Ständige Gruppe der Interessenträger unterrichtet den Verwaltungsrat regelmäßig über ihre Tätigkeiten.

ABSCHNITT 4A
NETZ DER NATIONALEN VERBINDUNGSBEAMTEN

Artikel 20a

Netz der nationalen Verbindungsbeamten

(1) Der Verwaltungsrat richtet auf Vorschlag des Exekutivdirektors ein Netz der nationalen Verbindungsbeamten ein, das sich aus Vertretern der Mitgliedstaaten zusammensetzt.

(2) Das Netz der nationalen Verbindungsbeamten setzt sich aus Vertretern aller Mitgliedstaaten zusammen. Jeder Mitgliedstaat bestellt einen Vertreter. Die Sitzungen des Netzes können in verschiedenen Expertenformaten abgehalten werden.

(3) Das Netz der nationalen Verbindungsbeamten erleichtert vor allem den Informationsaustausch zwischen der ENISA und den Mitgliedstaaten. Es unterstützt insbesondere die ENISA dabei, ihre Tätigkeiten, Erkenntnisse und Empfehlungen in der gesamten Union bei den einschlägigen Interessenträgern bekannt zu machen.

(4) Die nationalen Verbindungsbeamten dienen als zentrale Kontaktstellen auf nationaler Ebene, um die Zusammenarbeit zwischen der ENISA und den nationalen Experten im Rahmen der Umsetzung der Arbeitsprogramms der ENISA zu erleichtern.

(5) Während die nationalen Verbindungsbeamten eng mit den Vertretern ihres jeweiligen Staates im Verwaltungsrat zusammenarbeiten sollen, darf das Netz selbst nicht dieselbe Arbeit leisten wie der Verwaltungsrat oder andere Gremien der Union.

(6) Die Funktionen und Verfahren des Netzes der nationalen Verbindungsbeamten werden in den internen Verfahrensvorschriften der Agentur festgelegt und veröffentlicht.

ABSCHNITT 5
ARBEITSWEISE

Artikel 21

Einheitliches Programmplanungsdokument

(1) Die Agentur handelt in Übereinstimmung mit einem einheitlichen Programmplanungsdokument, das ihre jährliche und mehrjährige Programmplanung mit allen ihren geplanten Tätigkeiten enthält.

(2) Jedes Jahr erstellt der Exekutivdirektor einen Entwurf des einheitlichen Programmplanungsdokuments mit der jährlichen und mehrjährigen Programmplanung und der entsprechenden Personal- und Finanzplanung nach Artikel 32 der Delegierten Verordnung (EU) Nr. 1271/2013 der Kommission[14] und unter Berücksichtigung der von der Kommission festgelegten Leitlinien.

(3) Bis zum 30. November eines jeden Jahres nimmt der Verwaltungsrat das in Absatz 1 genannte einheitliche Programmplanungsdokument an und leitet es spätestens bis zum 31. Januar des Folgejahres sowie jede spätere Aktualisierung dieses Dokuments an das Europäische Parlament, den Rat und die Kommission weiter.

(4) Das einheitliche Programmplanungsdokument wird nach der endgültigen Feststellung des Gesamthaushaltsplans der Union endgültig und ist, erforderlichenfalls, entsprechend anzupassen.

(5) Das Jahresarbeitsprogramm enthält detaillierte Ziele und Angaben zu den erwarteten Ergebnissen, einschließlich Erfolgsindikatoren. Es enthält zudem eine Beschreibung der zu finanzierenden Maßnahmen sowie Angaben zur Höhe der für die einzelnen Maßnahmen vorgesehenen finanziellen und personellen Ressourcen gemäß den Grundsätzen der maßnahmenbezogenen Aufstellung des Haushaltsplans und des maßnahmenbezogenen Managements. Das Jahresarbeitsprogramm muss mit dem mehrjährigen Arbeitsprogramm nach Absatz 7 im Einklang stehen. Es ist klar darin anzugeben, welche Aufgaben im Vergleich zum vorangegangenen Haushaltsjahr hinzugefügt, verändert oder gestrichen wurden.

---

[14] Delegierte Verordnung (EU) Nr. 1271/2013 der Kommission vom 30. September 2013 über die Rahmenfinanzregelung für Einrichtungen gemäß Artikel 208 der Verordnung (EU, Euratom) Nr. 966/2012 des Europäischen Parlaments und des Rates (ABl. L 328 vom 7.12.2013, S. 42).

(6) Der Verwaltungsrat ändert das angenommene Jahresarbeitsprogramm, wenn der Agentur eine neue Aufgabe übertragen wird. Wesentliche Änderungen des jährlichen Arbeitsprogramms werden nach demselben Verfahren angenommen wie das ursprüngliche jährliche Arbeitsprogramm. Der Verwaltungsrat kann dem Exekutivdirektor die Befugnis übertragen, nicht wesentliche Änderungen am Jahresarbeitsprogramm vorzunehmen.

(7) Im mehrjährigen Arbeitsprogramm der Agentur wird die strategische Gesamtplanung einschließlich der Ziele, erwarteten Ergebnisse und Leistungsindikatoren festgelegt. Es umfasst auch die Ressourcenplanung mit einem mehrjährigen Finanz- und Personalplan.

(8) Die Ressourcenplanung wird jährlich aktualisiert. Die strategische Programmplanung ist zu aktualisieren, wann immer dies geboten erscheint und insbesondere wenn dies notwendig ist, um dem Ergebnis der in Artikel 56 genannten Bewertung Rechnung zu tragen.

Artikel 22

Interessenerklärung

(1) Die Mitglieder des Verwaltungsrats, der Exekutivdirektor und die von den Mitgliedstaaten auf Zeit abgeordneten Beamten geben eine Verpflichtungserklärung und eine Interessenerklärung ab, aus der hervorgeht, ob direkte oder indirekte Interessen bestehen, die ihre Unabhängigkeit beeinträchtigen könnten. Die Erklärungen müssen der Wahrheit entsprechen und vollständig sein; sie werden jedes Jahr schriftlich abgegeben und, wann immer erforderlich, aktualisiert.

(2) Die Mitglieder des Verwaltungsrats, der Exekutivdirektor und externe Sachverständige, die in den Ad-hoc-Arbeitsgruppen mitwirken, geben spätestens zu Beginn jeder Sitzung eine wahrheitsgetreue und vollständige Erklärung über alle Interessen ab, die ihre Unabhängigkeit in Bezug auf die Tagesordnungspunkte beeinträchtigen könnten, und beteiligen sich nicht an den Diskussionen und den Abstimmungen über solche Punkte.

(3) Die Agentur legt in ihren internen Verfahrensvorschriften die praktischen Einzelheiten der Vorschriften über Interessenerklärungen nach den Absätzen 1 und 2 fest.

Artikel 23

Transparenz

(1) Die Agentur übt ihre Tätigkeiten mit einem hohen Maß an Transparenz und im Einklang mit Artikel 25 aus.

(2) Die Agentur stellt sicher, dass die Öffentlichkeit sowie interessierte Kreise angemessene, objektive, zuverlässige und leicht zugängliche Informationen, insbesondere zu ihren eigenen Arbeitsergebnissen, erhalten. Ferner veröffentlicht sie die nach Artikel 22 abgegebenen Interessenerklärungen.

(3) Der Verwaltungsrat kann auf Vorschlag des Exekutivdirektors gestatten, dass interessierte Kreise als Beobachter an bestimmten Tätigkeiten der Agentur teilnehmen.

(4) Die Agentur legt in ihren internen Verfahrensvorschriften die praktischen Einzelheiten für die Anwendung der in den Absätzen 1 und 2 genannten Transparenzregelungen fest.

Artikel 24

Vertraulichkeit

(1) Unbeschadet des Artikels 25 gibt die Agentur Informationen, die bei ihr eingehen oder von ihr verarbeitet werden und die auf begründetes Ersuchen ganz oder teilweise vertraulich behandelt werden sollen, nicht an Dritte weiter.

(2) Die Mitglieder des Verwaltungsrats, der Exekutivdirektor, die Mitglieder der Ständigen Gruppe der Interessenträger, die externen Sachverständigen der Ad-hoc-Arbeitsgruppen sowie das Personal der Agentur, einschließlich der von den Mitgliedstaaten auf Zeit abgeordneten Beamten, unterliegen auch nach Beendigung ihrer Tätigkeit den Vertraulichkeitsbestimmungen des Artikels 339 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV).

(3) Die Agentur legt in ihren internen Verfahrensvorschriften die praktischen Einzelheiten für die Anwendung der in den Absätzen 1 und 2 genannten Vertraulichkeitsregelungen fest.

(4) Soweit es zur Erfüllung der Aufgaben der Agentur erforderlich ist, beschließt der Verwaltungsrat, die Agentur zum Umgang mit Verschlusssachen zu ermächtigen. In diesem Fall legt der Verwaltungsrat im Einvernehmen mit den Dienststellen der Kommission interne Verfahrensvorschriften zur Anwendung der Sicherheitsgrundsätze, die in den Beschlüssen (EU, Euratom) 2015/443[15] und 2015/444[16] der Kommission niedergelegt sind, fest. Diese Vorschriften betreffen unter anderem die Bestimmungen über den Austausch, die Verarbeitung und die Speicherung von Verschlusssachen.

---

15 Beschluss (EU, Euratom) 2015/443 der Kommission vom 13. März 2015 über Sicherheit in der Kommission (ABl. L 72 vom 17.3.2015, S. 41).

16 Beschluss (EU, Euratom) 2015/444 der Kommission vom 13. März 2015 über die Sicherheitsvorschriften für den Schutz von EU-Verschlusssachen (ABl. L 72 vom 17.3.2015, S. 53).

Artikel 25

Zugang zu Dokumenten

(1) Die Verordnung (EG) Nr. 1049/2001 findet Anwendung auf die Dokumente der Agentur.

(2) Der Verwaltungsrat legt innerhalb von sechs Monaten nach Errichtung der Agentur die Modalitäten zur Durchführung der Verordnung (EG) Nr. 1049/2001 fest.

(3) Gegen Entscheidungen der Agentur nach Artikel 8 der Verordnung (EG) Nr. 1049/2001 kann nach Maßgabe von Artikel 228 AEUV bzw. 263 AEUV Beschwerde beim Bürgerbeauftragten eingelegt oder Klage beim Gerichtshof der Europäischen Union erhoben werden.

KAPITEL III

AUFSTELLUNG UND GLIEDERUNG DES HAUSHALTSPLANS

Artikel 26

Aufstellung des Haushaltsplans

(1) Der Exekutivdirektor erstellt jedes Jahr den Entwurf des Voranschlags der Einnahmen und Ausgaben der Agentur für das folgende Haushaltsjahr und legt ihn dem Verwaltungsrat zusammen mit dem Entwurf des Stellenplans vor. Einnahmen und Ausgaben müssen ausgeglichen sein.

(2) Der Verwaltungsrat erstellt jedes Jahr auf der Grundlage des nach Absatz 1 erstellten Entwurfs des Voranschlags der Einnahmen und Ausgaben einen Voranschlag der Einnahmen und Ausgaben der Agentur für das folgende Haushaltsjahr.

(3) Der Verwaltungsrat übermittelt jedes Jahr bis zum 31. Januar der Kommission und den Drittländern, mit denen die Union Abkommen nach Artikel 39 geschlossen hat, den in Absatz 2 genannten Voranschlag, der Teil des Entwurfs des einheitlichen Programmplanungsdokuments ist.

(4) Die Kommission setzt aufgrund dieses Voranschlags die von ihr für erforderlich erachteten Mittelansätze für den Stellenplan und den Betrag des Zuschusses aus dem Gesamthaushaltsplan in den Haushaltsplanentwurf der Union ein, den sie nach den Artikeln 313 und 314 AEUV dem Europäischen Parlament und dem Rat vorlegt.

(5) Das Europäische Parlament und der Rat bewilligen die Mittel für den Beitrag für die Agentur.

(6) Das Europäische Parlament und der Rat legen den Stellenplan der Agentur fest.

(7) Der Haushaltsplan der Agentur wird zusammen mit dem einheitlichen Programmplanungsdokument vom Verwaltungsrat angenommen. Er wird endgültig, sobald der Gesamthaushaltsplan der Union endgültig festgestellt ist. Gegebenenfalls nimmt der Verwaltungsrat eine Anpassung des Haushaltsplans der Agentur und des einheitlichen Programmplanungsdokuments entsprechend dem Gesamthaushaltsplan der Union vor.

Artikel 27

Gliederung des Haushaltsplans

(1) Unbeschadet sonstiger Ressourcen gliedern sich die Einnahmen der Agentur wie folgt:

a) ein Beitrag aus dem Haushalt der Union;

b) Einnahmen, die konkreten Ausgabenpositionen im Einklang mit der in Artikel 29 genannten Finanzregelung zugewiesen werden;

c) Unionsmittel in Form von Übertragungsvereinbarungen oder Ad-hoc-Finanzhilfen im Einklang mit der in Artikel 29 genannten Finanzregelung der Agentur und den Bestimmungen der einschlägigen Instrumente zur Unterstützung der Unionspolitik;

d) Beiträge von Drittländern, die sich nach Artikel 39 an der Arbeit der Agentur beteiligen;

e) freiwillige Zahlungen oder Sachleistungen von Mitgliedstaaten; Mitgliedstaaten, die einen freiwilligen Beitrag leisten, können aufgrund dessen keine bestimmten Rechte oder Dienstleistungen beanspruchen.

(2) Die Ausgaben der Agentur umfassen Aufwendungen für Personal, Verwaltung, technische Unterstützung, Infrastruktur, Betriebskosten und Ausgaben, die sich aus Verträgen mit Dritten ergeben.

Artikel 28

Ausführung des Haushaltsplans

(1) Der Exekutivdirektor trägt die Verantwortung für die Ausführung des Haushaltsplans der Agentur.

(2) Der interne Rechnungsprüfer der Kommission übt gegenüber der Agentur dieselben Befugnisse wie gegenüber den Kommissionsdienststellen aus.

(3) Bis zum 1. März des jeweils folgenden Haushaltsjahres (1. März des Jahres n+1) übermittelt der Rechnungsführer der Agentur dem Rechnungsführer der Kommission und dem Rechnungshof den vorläufigen Jahresabschluss.

(4) Nach Eingang der Bemerkungen des Rechnungshofes zum vorläufigen Jahresabschluss der Agentur, erstellt der Rechnungsführer in eigener Verantwortung den endgültigen Jahresabschluss der Agentur.

(5) Der Exekutivdirektor legt den endgültigen Jahresabschluss dem Verwaltungsrat zur Stellungnahme vor.

(6) Der Exekutivdirektor übermittelt den Bericht über die Haushaltsführung und das Finanzmanagement bis zum 31. März des Jahres n+1 dem Europäischen Parlament, dem Rat, der Kommission und dem Rechnungshof.

(7) Der Rechnungsführer leitet den endgültigen Jahresabschluss zusammen mit der Stellungnahme des Verwaltungsrats bis zum 1. Juli des Jahres n+1 dem Europäischen Parlament, dem Rat, der Kommission und dem Rechnungshof zu.

(8) Gleichzeitig mit der Übermittlung des endgültigen Jahresabschlusses leitet der Rechnungsführer auch dem Rechnungshof eine Erklärung über die Vollständigkeit dieses endgültigen Jahresabschlusses mit Kopie an den Rechnungsführer der Kommission zu.

(9) Der Exekutivdirektor veröffentlicht den endgültigen Jahresabschluss bis zum 15. November des Folgejahres.

(10) Der Exekutivdirektor übermittelt dem Rechnungshof zum 30. September des Jahres n+1 eine Antwort auf dessen Bemerkungen und leitet eine Kopie dieser Antwort auch dem Verwaltungsrat und der Kommission zu.

(11) Der Exekutivdirektor übermittelt dem Europäischen Parlament auf dessen Anfrage nach Artikel 165 Absatz 3 der Haushaltsordnung alle Informationen, die für die ordnungsgemäße Abwicklung des Entlastungsverfahrens für das betreffende Haushaltsjahr erforderlich sind.

(12) Auf Empfehlung des Rates erteilt das Europäische Parlament dem Direktor vor dem 15. Mai des Jahres n+2 Entlastung für die Ausführung des Haushaltsplans für das Jahr n.

Artikel 29

Finanzregelung

Der Verwaltungsrat erlässt nach Konsultation der Kommission die für die Agentur geltende Finanzregelung. Die Finanzregelung darf von der Delegierten Verordnung (EU) Nr. 1271/2013 nur abweichen, wenn dies für den Betrieb der Agentur eigens erforderlich ist und die Kommission vorher ihre Zustimmung erteilt hat.

Artikel 30

Betrugsbekämpfung

(1) Zur Erleichterung der Bekämpfung von Betrug, Korruption und sonstigen rechtswidrigen Handlungen gemäß der Verordnung 883/2013 des Europäischen Parlaments und des Rates[17] tritt die Agentur binnen sechs Monaten nach Aufnahme ihrer Tätigkeit der Interinstitutionellen Vereinbarung vom 25. Mai 1999 über die internen Untersuchungen des Europäischen Amtes für Betrugsbekämpfung (OLAF) bei und erlässt die einschlägigen Vorschriften, die für sämtliche Mitarbeiter der Agentur gelten, nach dem Muster im Anhang der genannten Vereinbarung.

(2) Der Rechnungshof ist befugt, bei allen Empfängern von Finanzhilfen sowie bei Auftragnehmern und Unterauftragnehmern, die Unionsmittel von der Agentur erhalten haben, Rechnungsprüfungen anhand von Unterlagen und vor Ort durchzuführen.

[17] Verordnung (EU, Euratom) Nr. 883/2013 des Europäischen Parlaments und des Rates vom 11. September 2013 über die Untersuchungen des Europäischen Amtes für Betrugsbekämpfung (OLAF) und zur Aufhebung der Verordnung (EG) Nr. 1073/1999 des Europäischen Parlaments und des Rates und der Verordnung (Euratom) Nr. 1074/1999 des Rates (ABl. L 248 vom 18.9.2013, S. 1).

(3) Das OLAF kann gemäß den Bestimmungen und Verfahren der Verordnung 883/2013 des Europäischen Parlaments und des Rates und der Verordnung (Euratom, EG) Nr. 2185/96 des Rates[18] vom 11. November 1996 betreffend die Kontrollen und Überprüfungen vor Ort durch die Kommission zum Schutz der finanziellen Interessen der Union vor Betrug und anderen Unregelmäßigkeiten Untersuchungen, einschließlich Kontrollen und Überprüfungen vor Ort, durchführen, um festzustellen, ob im Zusammenhang mit von der Agentur gewährten Finanzhilfen oder von ihr finanzierten Aufträgen ein Betrugs- oder Korruptionsdelikt oder eine sonstige rechtswidrige Handlung zum Nachteil der finanziellen Interessen der Union vorliegt.

(4) Unbeschadet der Absätze 1, 2 und 3 müssen Kooperationsvereinbarungen mit Drittländern und internationalen Organisationen, Verträge, Finanzhilfevereinbarungen und Finanzhilfebeschlüsse der Agentur Bestimmungen enthalten, die den Rechnungshof und das OLAF ausdrücklich ermächtigen, derartige Rechnungsprüfungen und Untersuchungen im Rahmen ihrer jeweiligen Zuständigkeiten durchzuführen.

KAPITEL IV
PERSONAL DER AGENTUR

Artikel 31

Allgemeine Bestimmungen

Für das Personal der Agentur gelten das Statut der Beamten, die Beschäftigungsbedingungen für die sonstigen Bediensteten und die im gegenseitigen Einvernehmen der Organe der Union erlassenen Regelungen zur Durchführung dieser Bestimmungen.

---

18 Verordnung (Euratom, EG) Nr. 2185/96 des Rates vom 11. November 1996 betreffend die Kontrollen und Überprüfungen vor Ort durch die Kommission zum Schutz der finanziellen Interessen der Europäischen Gemeinschaften vor Betrug und anderen Unregelmäßigkeiten (ABl. L 292 vom 15.11.1996, S. 2).

Artikel 32

Vorrechte und Befreiungen

Das dem Vertrag über die Europäische Union und dem AEUV beigefügte Protokoll Nr. 7 über die Vorrechte und Befreiungen der Europäischen Union findet auf die Agentur und ihr Personal Anwendung.

Artikel 33

Exekutivdirektor

(1) Der Exekutivdirektor wird als Zeitbediensteter der Agentur nach Artikel 2 Buchstabe a der Beschäftigungsbedingungen für die sonstigen Bediensteten eingestellt.

(2) Der Exekutivdirektor wird vom Verwaltungsrat aus einer Liste von Kandidaten, die die Kommission im Anschluss an ein offenes und transparentes Auswahlverfahren vorgeschlagen hat, ernannt.

(3) Beim Abschluss des Vertrags des Exekutivdirektors wird die Agentur durch den Vorsitzenden des Verwaltungsrats vertreten.

(4) Vor der Ernennung wird der vom Verwaltungsrat ausgewählte Kandidat aufgefordert, eine Erklärung vor dem zuständigen Ausschuss des Europäischen Parlaments abzugeben und Fragen der Mitglieder zu beantworten.

(5) Die Amtszeit des Exekutivdirektors beträgt [...] **vier** Jahre. Zum Ende dieses Zeitraums nimmt die Kommission eine Bewertung vor, bei der die Leistung des Exekutivdirektors und die künftigen Aufgaben und Herausforderungen der Agentur berücksichtigt werden.

(6) Der Verwaltungsrat beschließt über die Ernennung, die Verlängerung der Amtszeit oder die Abberufung des Exekutivdirektors mit der Zweidrittelmehrheit seiner stimmberechtigten Mitglieder.

(7) Der Verwaltungsrat kann auf Vorschlag der Kommission unter Berücksichtigung der Bewertung nach Absatz 5 die Amtszeit des Exekutivdirektors einmal um höchstens [...] **vier** Jahre verlängern.

(8) Der Verwaltungsrat unterrichtet das Europäische Parlament über seine Absicht, die Amtszeit des Exekutivdirektors zu verlängern. Innerhalb von drei Monaten vor der Verlängerung der Amtszeit gibt der Exekutivdirektor, sofern er dazu aufgefordert wird, vor dem zuständigen Ausschuss des Europäischen Parlaments eine Erklärung ab und beantwortet Fragen der Mitglieder.

(9) Ein Exekutivdirektor, dessen Amtszeit verlängert wurde, darf nicht an einem anderen Auswahlverfahren für dieselbe Stelle teilnehmen.

(10) Der Direktor kann nur durch einen Beschluss des Verwaltungsrats [...] seines Amtes enthoben werden.

Artikel 34

Abgeordnete nationale Sachverständige und andere Bedienstete

(1) Die Agentur kann auf abgeordnete nationale Sachverständige oder sonstiges Personal zurückgreifen, das nicht von der Agentur selbst beschäftigt wird. Für dieses Personal gelten das Statut der Beamten und die Beschäftigungsbedingungen für die sonstigen Bediensteten nicht.

(2) Der Verwaltungsrat beschließt eine Regelung über zur Agentur abgeordnete nationale Sachverständige.

KAPITEL V
ALLGEMEINE BESTIMMUNGEN

Artikel 35

Rechtsform der Agentur

(1) Die Agentur ist eine Einrichtung der Union und besitzt Rechtspersönlichkeit.

(2) Die Agentur besitzt in jedem Mitgliedstaat die weitestgehende Rechts- und Geschäftsfähigkeit, die juristischen Personen nach einzelstaatlichem Recht zuerkannt ist. Es kann insbesondere bewegliches und unbewegliches Vermögen erwerben und veräußern und ist vor Gericht parteifähig [...].

(3) Die Agentur wird von ihrem Exekutivdirektor vertreten.

Artikel 36

Haftung der Agentur

(1) Die vertragliche Haftung der Agentur bestimmt sich nach dem für den betreffenden Vertrag geltenden Recht.

(2) Für Entscheidungen aufgrund einer Schiedsklausel in einem von der Agentur geschlossenen Vertrag ist der Gerichtshof der Europäischen Union zuständig.

(3) Im Bereich der außervertraglichen Haftung ersetzt die Agentur den durch sie selbst oder ihre Bediensteten in Ausübung ihrer Tätigkeit verursachten Schaden nach den allgemeinen Grundsätzen, die den Rechtsordnungen der Mitgliedstaaten gemeinsam sind.

(4) In Streitsachen über den Schadensersatz ist der Gerichtshof der Europäischen Union zuständig.

(5) Die persönliche Haftung der Bediensteten gegenüber der Agentur bestimmt sich nach den für sie geltenden Beschäftigungsbedingungen.

Artikel 37

Sprachenregelung

(1) Für die Agentur gilt die Verordnung Nr. 1 des Rates[19]. Die Mitgliedstaaten und die anderen von ihnen benannten Stellen können sich an die Agentur in einer Amtssprache der Organe der Union ihrer Wahl wenden und erhalten eine Antwort in dieser Sprache.

(2) Die für die Arbeit der Agentur erforderlichen Übersetzungsdienste werden vom Übersetzungszentrum für die Einrichtungen der Europäischen Union erbracht.

Artikel 38

Schutz personenbezogener Daten

(1) Die Verarbeitung personenbezogener Daten durch die Agentur unterliegt der Verordnung (EG) Nr. 45/2001 des Europäischen Parlaments und des Rates[20].

(2) Der Verwaltungsrat beschließt die Durchführungsbestimmungen nach Artikel 24 Absatz 8 der Verordnung (EG) Nr. 45/2001. Der Verwaltungsrat kann zusätzliche Maßnahmen, die für die Anwendung der Verordnung (EG) Nr. 45/2001 durch die Agentur erforderlich sind, festlegen.

---

19 Verordnung Nr. 1 zur Regelung der Sprachenfrage für die Europäische Atomgemeinschaft (ABl. 17 vom 6.10.1958, S. 401).

20 Verordnung (EG) Nr. 45/2001 des Europäischen Parlaments und des Rates vom 18. Dezember 2000 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Gemeinschaft und zum freien Datenverkehr (ABl. L 8 vom 12.1.2001, S. 1).

Artikel 39

Zusammenarbeit mit Drittländern und internationalen Organisationen

(1) Die Agentur kann mit den zuständigen Behörden von Drittländern und mit internationalen Organisationen zusammenarbeiten, soweit dies zur Verwirklichung der Ziele dieser Verordnung erforderlich ist. Zu diesem Zweck kann die Agentur, nach vorheriger Genehmigung durch die Kommission, Arbeitsvereinbarungen mit den Behörden von Drittländern und internationalen Organisationen treffen. Diese Vereinbarungen begründen keine rechtlichen Verpflichtungen für die Union und ihre Mitgliedstaaten.

(2) Die Agentur steht der Beteiligung von Drittländern offen, die entsprechende Übereinkünfte mit der Europäischen Union getroffen haben. Gemäß den einschlägigen Bestimmungen dieser Übereinkünfte werden Vereinbarungen getroffen, die insbesondere Art, Umfang und Form einer Beteiligung dieser Länder an der Tätigkeit der Agentur festlegen; hierzu zählen auch Bestimmungen über die Beteiligung an den von der Agentur durchgeführten Initiativen, finanzielle Beiträge und Personal. In Personalfragen müssen derartige Vereinbarungen in jedem Fall mit dem Beamtenstatut vereinbar sein.

(3) Der Verwaltungsrat verabschiedet eine Strategie für die Beziehungen zu Drittländern oder internationalen Organisationen in Bezug auf Angelegenheiten, für die die Agentur zuständig ist. Die Kommission stellt durch den Abschluss einer entsprechenden Arbeitsvereinbarung mit dem Exekutivdirektor der Agentur sicher, dass die Agentur im Rahmen ihres Mandats und des bestehenden institutionellen Rahmens handelt.

Artikel 40

Sicherheitsvorschriften für den Schutz von Verschlusssachen und nicht als Verschlusssache eingestuften vertraulichen Informationen

In Absprache mit der Kommission legt die Agentur die für sie geltenden Sicherheitsvorschriften fest, mit denen die in den Sicherheitsvorschriften der Kommission für den Schutz von Verschlusssachen der Europäischen Union und nicht als Verschlusssache eingestuften sensiblen Informationen enthaltenen Sicherheitsgrundsätze angewandt werden, die in den Beschlüssen (EU, Euratom) 2015/443 und 2015/444 festgelegt sind. Dies betrifft unter anderem die Bestimmungen über den Austausch, die Verarbeitung und die Speicherung derartiger Informationen.

Artikel 41

Sitzabkommen und Arbeitsbedingungen

(1) Die notwendigen Regelungen über die Unterbringung der Agentur in dem Mitgliedstaat, in dem sie ihren Sitz hat, und über die Einrichtungen, die von diesem Mitgliedstaat zur Verfügung zu stellen sind, sowie die besonderen Vorschriften, die im Sitzmitgliedstaat der Agentur für den Exekutivdirektor, die Mitglieder des Verwaltungsrats, das Personal der Agentur und für Familienangehörige dieser Personen gelten, werden in einem Sitzabkommen festgelegt, das nach Billigung durch den Verwaltungsrat zwischen der Agentur und dem Sitzmitgliedstaat spätestens am [zwei Jahre nach Inkrafttreten dieser Verordnung] geschlossen wird.

(2) Der Sitzmitgliedstaat der Agentur gewährleistet die [...] Voraussetzungen für das reibungslose Funktionieren der Agentur, einschließlich der Erreichbarkeit des Standortes, des Vorhandenseins adäquater Bildungseinrichtungen für die Kinder der Mitglieder des Personals und eines angemessenen Zugangs zu Arbeitsmarkt, Sozialversicherung und medizinischer Versorgung für Kinder und Ehegatten.

Artikel 42

Verwaltungskontrolle

Die Tätigkeit der Agentur unterliegt der Aufsicht des Bürgerbeauftragten nach Artikel 228 AEUV.

TITEL III
ZERTIFIZIERUNGSRAHMEN FÜR DIE CYBERSICHERHEIT

Artikel 43

Der Europäische Zertifizierungsrahmen für die Cybersicherheit

(1) **Der Europäische Zertifizierungsrahmen für die Cybersicherheit wird geschaffen, um die Voraussetzungen für einen funktionierenden Binnenmarkt zu verbessern, indem die Cybersicherheit in der Europäische Union erhöht wird. Im Hinblick auf die Schaffung eines digitalen Binnenmarkts für IKT-Prozesse, -Produkte und -Dienste setzt er die Regeln für einen harmonisierten Ansatz auf EU-Ebene für europäische Systeme für die Cybersicherheitszertifizierung.**

(2) **Der Europäische Zertifizierungsrahmen für die Cybersicherheit legt einen Mechanismus zur Schaffung** europäischer Systeme für die Cybersicherheitszertifizierung und zur Bescheinigung, dass die nach einem solchen System **bewerteten** IKT-**Prozesse**, -Produkte und -Dienste den festgelegten **Sicherheits**anforderungen [...] genügen, **mit dem Ziel** fest, die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit von gespeicherten, übermittelten oder verarbeiteten Daten, Funktionen oder Diensten, die von diesen Produkten, Prozessen **und** Diensten [...] angeboten oder über diese zugänglich gemacht werden, **während deren gesamten Lebenszyklus zu schützen**.

Artikel 44

Ausarbeitung und Annahme eines europäischen Systems für die Cybersicherheitszertifizierung

(1) Im Auftrag der Kommission oder der **nach Artikel 53 eingesetzten Europäischen Gruppe für die Cybersicherheitszertifizierung (im Folgenden die "Gruppe")** arbeitet die ENISA ein mögliches europäisches System für die Cybersicherheitszertifizierung aus, das den in den Artikeln 45, 46 und 47 genannten Anforderungen genügt.

(1a) Die Ausarbeitung eines möglichen europäischen Systems für die Cybersicherheitszertifizierung kann der Gruppe von Mitgliedstaaten oder von Organisationen von Interessenträgern vorgeschlagen werden. Die Gruppe bewertet diese Vorschläge anhand von Kriterien, die sie mithilfe der Leitlinien nach Artikel 53 Absatz 3 Buchstabe ca festlegt, und kann die ENISA mit der Ausarbeitung eines möglichen europäischen Systems für die Cybersicherheitszertifizierung beauftragen.

(2) Bei der Ausarbeitung der möglichen Systeme nach Absatz 1 konsultiert die ENISA alle in Frage kommenden Interessenträger **im Wege transparenter Konsultationsprozesse** und arbeitet eng mit der Gruppe zusammen. Die Gruppe leistet der ENISA die [...] Unterstützung und fachliche Beratung für die Ausarbeitung des möglichen Systems **und gibt vor dessen Vorlage bei der Kommission eine Stellungnahme zu dem möglichen System ab**. **Die ENISA stellt sicher, dass die möglichen Systeme mit den geltenden harmonisierten Normen im Einklang stehen, die für die Akkreditierung der Konformitätsbewertungsstellen herangezogen werden.**

(3) Die ENISA **berücksichtigt die Stellungnahme der Gruppe weitestgehend, bevor sie** der Kommission das nach Absatz 2 ausgearbeitete mögliche europäische System für die Cybersicherheitszertifizierung vorlegt.

(4) Auf der Grundlage des von der ENISA ausgearbeiteten möglichen Systems kann die Kommission nach Artikel 55 Absatz 2 Durchführungsrechtsakte erlassen, in denen für IKT-**Prozesse**, -Produkte und -Dienste, die die Anforderungen der Artikel 45, 46 und 47 erfüllen, europäische Systeme für die Cybersicherheitszertifizierung festgelegt werden.

(5) [...]

Artikel 44a

Pflege eines europäischen Systems für die Cybersicherheitszertifizierung

(1) Die Agentur unterhält eine eigene Website, auf der sie über die europäischen Systeme für die Cybersicherheitszertifizierung, Zertifikate und nach Artikel 47a ausgestellten EU-Konformitätserklärungen informiert und für diese wirbt.

(2) In enger Zusammenarbeit mit der Gruppe überprüft die Agentur mindestens alle fünf Jahre die angenommenen europäischen Systeme für die Cybersicherheitszertifizierung, wobei sie die Rückmeldungen seitens der Interessenträger berücksichtigt. Wenn dies als erforderlich erachtet wird, kann die Kommission oder die Gruppe die Agentur beauftragen, den Prozess zur Entwicklung eines überarbeiteten möglichen Systems nach Artikel 44 Absätze 2 und 3 einzuleiten.

Artikel 45

Sicherheitsziele der europäischen Systeme für die Cybersicherheitszertifizierung

Für die Cybersicherheitszertifizierung wird ein europäisches System konzipiert, das – soweit zutreffend – **mindestens** folgenden Sicherheitsziele [...] **verwirklicht**:

a) Gespeicherte, übermittelte oder anderweitig verarbeitete Daten werden **während des gesamten Lebenszyklus des Prozesses, des Produkts oder des Dienstes** gegen eine zufällige oder unbefugte Speicherung, Verarbeitung oder Preisgabe sowie gegen einen zufälligen oder unbefugten Zugriff geschützt.

b) Gespeicherte, übermittelte oder anderweitig verarbeitete Daten werden **während des gesamten Lebenszyklus des Prozesses, des Produkts oder des Dienstes** gegen eine zufällige oder unbefugte Zerstörung, [...] Verlust oder Änderung **oder mangelnde Verfügbarkeit** geschützt.

c) [...] Befugte Personen, Programme oder Maschinen haben ausschließlich Zugriff auf die Daten, Dienste oder Funktionen, zu denen sie zugangsberechtigt sind.

d) Es wird protokolliert, auf welche Daten, Dienste oder Funktionen zu welchem Zeitpunkt und von wem **zugegriffen** wurde und welche Daten, Funktionen oder Dienste zu welchem Zeitpunkt von wem [...] **genutzt oder anderweitig verarbeitet** wurden.

e) Es [...] kann überprüft werden, auf welche Daten, Dienste oder Funktionen zu welchem Zeitpunkt und von wem zugegriffen wurde oder wer zu welchem Zeitpunkt Daten, Dienste oder Funktionen genutzt **oder anderweitig verarbeitet** hat.

f) Bei einem physischen oder technischen Sicherheitsvorfall werden die Daten, Dienste und Funktionen zeitnah wieder verfügbar gemacht und der Zugang zu ihnen zeitnah wieder hergestellt.

g) [...] IKT-**Prozesse**, -Produkte und -Dienste werden mit aktueller Software **und Hardware**, die keine **allgemein** bekannten Schwachstellen aufweis**en**, bereitgestellt und mit Mechanismen für sichere [...] Updates ausgestattet.

ga) IKT-Prozesse, -Produkte und -Dienste werden im Einklang mit den Sicherheitsanforderungen entwickelt, hergestellt und geliefert, die in dem jeweiligen System aufgeführt sind.

Artikel 46

Vertrauenswürdigkeitsstufen der europäischen Systeme für die Cybersicherheitszertifizierung

(1) Ein europäisches System für die Cybersicherheitszertifizierung kann für [...] IKT-**Prozesse,** -Produkte und -Dienste eine oder mehrere der Vertrauenswürdigkeitsstufen "niedrig", "mittel" und/oder "hoch" angeben. **Die Vertrauenswürdigkeitsstufe steht in einem angemessenen Verhältnis zu dem mit der beabsichtigten Verwendung eines IKT-Prozesses, -Produktes und -Dienstes verbundenen Risiko.**

(2) Die Vertrauenswürdigkeitsstufen "niedrig", "mittel" und "hoch" [...] **beziehen sich auf ein Zertifikat oder eine EU-Konformitätserklärung, die im Rahmen eines europäischen Systems für die Cybersicherheitszertifizierung ausgestellt wurden, das für jede Vertrauenswürdigkeitsstufe entsprechende Sicherheitsauflagen einschließlich der Sicherheitsfunktionen und den entsprechenden Aufwand für die Bewertung eines IKT-Prozesses, -Produktes und -Dienstes vorgibt. Das Zertifikat oder die EU-Konformitätserklärung ist unter Bezugnahme auf die diesbezüglichen technischen Spezifikationen, Normen und Verfahren einschließlich technischer Prüfungen, deren Zweck in der Minderung oder Prävention der Gefahr von Cybervorfällen besteht, folgendermaßen gekennzeichnet:**

a) **ein europäisches Cybersicherheitszertifikat oder eine EU-Konformitätserklärung für die** Vertrauenswürdigkeitsstufe "niedrig" **bietet die Gewissheit, dass die IKT-Prozesse, -Produkte und -Dienste die jeweiligen Sicherheitsauflagen einschließlich der Sicherheitsfunktionen erfüllen und einer Bewertung unterzogen wurden, die darauf ausgerichtet ist, die bekannten grundlegenden Risiken für Cybervorfälle und Cyberangriffe möglichst gering zu halten. Zur Evaluierung gehört mindestens eine Überprüfung der technischen Dokumentation, oder, falls dies nicht anwendbar ist, alternative Tätigkeiten mit gleicher Wirkung** [...]**;**

b) **ein europäisches Cybersicherheitszertifikat für die** Vertrauenswürdigkeitsstufe "mittel" **bietet die Gewissheit, dass die IKT-Prozesse, -Produkte und -Dienste die jeweiligen Sicherheitsauflagen einschließlich der Sicherheitsfunktionen erfüllen und einer Bewertung unterzogen wurden, die darauf ausgerichtet ist, bekannte Cyberrisiken, Cybervorfälle und Cyberangriffe seitens Akteuren mit begrenzten Fähigkeiten und Ressourcen möglichst gering zu halten. Die Bewertung beinhaltet mindestens die Überprüfung, dass öffentlich bekannte Schwachstellen nicht vorliegen, und die Prüfung, dass die IKT-Prozesse, -Produkte und -Dienste die erforderlichen Sicherheitsfunktionen korrekt durchführen; falls dies nicht anwendbar ist, enthält sie stattdessen alternative Tätigkeiten mit gleicher Wirkung** [...]**;**

c) **ein europäisches Cybersicherheitszertifikat für die** Vertrauenswürdigkeitsstufe "hoch" **bietet die Gewissheit, dass die IKT-Prozesse, -Produkte und -Dienste die jeweiligen Sicherheitsauflagen einschließlich der Sicherheitsfunktionen erfüllen und einer Bewertung unterzogen wurden, die darauf ausgerichtet ist, das Risiko hochmoderner Cyberangriffe durch Akteure mit umfangreichen Fähigkeiten und Ressourcen möglichst gering zu halten. Die Bewertung beinhaltet mindestens die Überprüfung, dass öffentlich bekannte Schwachstellen nicht vorliegen, die Prüfung, dass die IKT-Prozesse, -Produkte und -Dienste die erforderlichen Sicherheitsfunktionen auf dem neueste technischen Stand korrekt durchführen, und die Beurteilung ihrer Widerstandsfähigkeit gegen kompetente Angreifer mittels Penetrationstests; falls dies nicht anwendbar ist, enthält sie stattdessen alternative Tätigkeiten mit gleicher Wirkung** [...].

(2a) In einem europäisches System für die Cybersicherheitszertifizierung können je nach Strenge und Gründlichkeit der Evaluierungsmethode mehrere Bewertungsniveaus angegeben werden. Jedes Bewertungsniveau entspricht einer der Vertrauenswürdigkeitsstufen und wird durch eine entsprechende Kombination von Vertrauenswürdigkeitskomponenten definiert.

Artikel 47

Elemente der europäischen Systeme für die Cybersicherheitszertifizierung

(1) Ein europäisches System für die Cybersicherheitszertifizierung muss mindestens folgende Elemente enthalten:

a) Gegenstand und Umfang des Zertifizierung**ssystems**, darunter auch Art oder Kategorie der erfassten IKT**- Prozesse,** -Produkte und -Dienste **sowie eine Darstellung, wie das Zertifizierungssystem den Bedürfnissen der voraussichtlichen Zielgruppen entspricht**;

b) [...] Bezugnahme auf **die für die Bewertung maßgeblichen** internationalen, **europäischen oder nationalen** Normen**. Sind keine Normen verfügbar, wird auf die** [...] technischen Spezifikationen**, die die Auflagen des Anhangs II der Verordnung 1025/2012 erfüllen, oder wenn solche nicht verfügbar sind, auf die im System festgelegten technischen Spezifikationen oder Cybersicherheitsanforderungen Bezug genommen**;

c) gegebenenfalls eine oder mehrere Vertrauenswürdigkeitsstufen;

ca) falls anwendbar, spezielle oder zusätzliche Anforderungen an die Konformitätsbewertungsstellen, um deren technische Kompetenz für die Evaluierung der Cybersicherheitsanforderungen zu gewährleisten;

d) besondere Bewertungskriterien und -methoden sowie Bewertungsarten für den Nachweis, dass die in Artikel 45 festgelegten Ziele eingehalten werden;

e) **falls anwendbar,** für die Zertifizierung erforderliche Informationen, die ein Antragsteller der Konformitätsbewertungsstelle vorzulegen hat **oder auf andere Weise zur Verfügung zu stellen ist**;

f) Bedingungen für die Verwendung von Siegeln oder Kennzeichen, sofern das System solche vorsieht;

g) Vorschriften für die Überwachung der Einhaltung der mit dem Zertifikat **oder der EU-Konformitätserklärung** verbundenen Anforderungen,[...] einschließlich der Mechanismen für den Nachweis der beständigen Einhaltung der festgelegten Cybersicherheitsanforderungen;

h) **falls anwendbar,** Bedingungen für die Gewährung **und Verlängerung eines Zertifikats sowie die** Aufrechterhaltung, Fortführung, Ausweitung **oder** Verringerung des Zertifizierungsumfangs;

i) Vorschriften, die greifen, wenn die zertifizierten **oder selbstbewerteten** IKT-Produkte und -Dienste den [...]Anforderungen **des Systems** nicht genügen;

j) Vorschriften für die Meldung und Behandlung bislang nicht erkannter Cybersicherheitsschwachstellen von IKT-**Prozessen,** -Produkten und -Diensten;

k) **falls anwendbar,** Vorschriften für die Konformitätsbewertungsstellen über die Aufbewahrung von Aufzeichnungen;

l) Angabe nationaler oder **internationaler** Systeme für die Cybersicherheitszertifizierung für dieselbe Art oder Kategorie von IKT-**Prozessen,** -Produkten und -Diensten**, Sicherheitsanforderungen und Evaluierungskriterien und -methoden**;

m) Inhalt des ausgestellten Zertifikats **oder der EU-Konformitätserklärung;**

ma) Zeitraum für die Speicherung der EU-Konformitätserklärung und der technischen Dokumentation sämtlicher einschlägiger Informationen durch den Hersteller oder Anbieter von IKT-Produkten und -Diensten;

mb) maximale Gültigkeitsdauer der Zertifikate;

mc) Offenlegungspolitik für erteilte, geänderte und entzogene Zertifikate;

md) Bedingungen für die auf Gegenseitigkeit beruhende Anerkennung von Zertifizierungssystemen von Drittländern;

me) falls anwendbar, Regeln für einen Mechanismus der gegenseitigen Begutachtung für die Stellen, die im Einklang mit Artikel 48 Absatz 4a europäische Cybersicherheitszertifikate für die hohe Vertrauenswürdigkeitsstufe ausstellen.

(2) Die für das System festgelegten Anforderungen dürfen in keinem Widerspruch zu geltenden rechtlichen Anforderungen stehen, vor allem nicht zu solchen Anforderungen, die sich aus harmonisiertem Unionsrecht ergeben.

(3) Soweit dies in einem Rechtsakt der Union so festgelegt ist, kann eine Zertifizierung **oder eine EU-Konformitätserklärung** auf der Grundlage eines europäischen Systems für die Cybersicherheitszertifizierung für den Nachweis der Konformitätsvermutung mit den Anforderungen jenes Rechtsakts verwendet werden.

(4) Mangels harmonisierter Rechtsvorschriften der Union kann auch ein Mitgliedstaat festlegen, dass ein europäisches System für die Cybersicherheitszertifizierung für die Feststellung der Konformitätsvermutung mit den rechtlichen Anforderungen verwendet werden kann.

Artikel 47a

Selbstbewertung der Konformität

(1) Ein europäisches System für die Cybersicherheitszertifizierung kann die Durchführung einer Konformitätsbewertung unter der alleinigen Verantwortung des Herstellers oder Anbieters von IKT-Produkten und -Diensten zulassen. Eine derartige Konformitätsbewertung gilt nur für IKT-Produkte und -Dienste mit niedrigem Risiko, die der Vertrauenswürdigkeitsstufe "niedrig" entsprechen.

(2) Der Hersteller oder Anbieter von IKT-Produkten und -Diensten kann eine EU-Konformitätserklärung ausstellen, die bestätigt, dass die Erfüllung der im System festgelegten Anforderungen nachgewiesen wurde. Durch die Abfassung einer solchen Erklärung übernimmt der Hersteller oder Anbieter der IKT-Produkte oder -Dienste die Verantwortung dafür, dass das IKT-Produkt bzw. der IKT-Dienst den in diesem System festgelegten Anforderungen entspricht.

(3) Der Hersteller oder Anbieter von IKT-Produkten und -Diensten hält die EU-Konformitätserklärung und die technische Dokumentation mit allen einschlägigen Informationen in Bezug auf die Konformität der IKT-Produkte oder -Dienste mit einem System während eines Zeitraums, der im entsprechenden europäischen System für die Cybersicherheitszertifizierung festgelegt ist, für die in Artikel 50 Absatz 1 genannte nationale Cybersicherheitszertifizierungsbehörde bereit. Eine Kopie der EU-Konformitätserklärung ist der nationalen Cybersicherheitszertifizierungsbehörde und der ENISA vorzulegen.

(4) Sofern im Unionsrecht oder im innerstaatlichen Recht der Mitgliedstaaten nicht anders bestimmt, ist die Ausstellung der EU-Konformitätserklärung freiwillig.

(5) Eine nach diesem Artikel ausgestellte EU-Konformitätserklärung wird in allen Mitgliedstaaten anerkannt.

Artikel 48

Cybersicherheitszertifizierung

(1) Für IKT-**Prozesse,** -Produkte und -Dienste, die auf der Grundlage eines nach Artikel 44 angenommenen europäischen Systems für die Cybersicherheitszertifizierung zertifiziert wurden, gilt die Vermutung der Konformität mit den Anforderungen dieses Systems.

(2) Sofern im Unionsrecht **oder im innerstaatlichen Recht der Mitgliedstaaten** nicht anders bestimmt, ist die Zertifizierung freiwillig.

(3) Ein europäisches Cybersicherheitszertifikat nach diesem Artikel **mit der Vertrauenswürdigkeitsstufe "niedrig" oder "mittel"** wird von den in Artikel 51 genannten Konformitätsbewertungsstellen auf der Grundlage der Kriterien des nach Artikel 44 angenommenen europäischen Systems für die Cybersicherheitszertifizierung ausgestellt.

(4) Abweichend von Absatz 3 kann in hinreichend begründeten Fällen ein einzelnes europäisches System für die Cybersicherheitszertifizierung vorsehen, dass ein im Rahmen dieses Systems erteiltes europäisches Cybersicherheitszertifikat nur von einer öffentlichen Stelle ausgestellt werden kann. Bei einer solchen [...] Stelle muss es sich um eine der folgenden Stellen handeln:

a) eine nationale **Cybersicherheits**zertifizierungsbehörde nach Artikel 50 Absatz 1;

b) eine als Konformitätsbewertungsstelle akkreditierte **öffentliche** Stelle nach Artikel 51 Absatz 1 [...]

c) [...].

(4a) Ist im Rahmen eines europäischen Systems für die Cybersicherheitszertifizierung nach Artikel 44 die Vertrauenswürdigkeitsstufe "hoch" erforderlich, kann das Zertifikat nur von einer nationalen Cybersicherheitszertifizierungsbehörde nach Artikel 50 Absatz 1 oder unter folgenden Bedingungen von einer Konformitätsbewertungsstelle nach Artikel 51 ausgestellt werden:

a) wenn die nationale Cybersicherheitszertifizierungsbehörde zuvor für jedes einzelne, von einer Konformitätsbewertungsstelle ausgestellte Zertifikat ihre Zustimmung erteilt hat; oder

b) wenn die nationale Cybersicherheitszertifizierungsbehörde diese Aufgabe zuvor allgemein einer Konformitätsbewertungsstelle übertragen hat.

(5) Die natürliche oder juristische Person, die ihre IKT**-Prozesse,** -Produkte oder -Dienste zur Zertifizierung einreicht, hat der in Artikel 51 genannten Konformitätsbewertungsstelle **oder der in Artikel 50 genannten nationalen Cybersicherheitszertifizierungsbehörde – sofern diese Behörde die Stelle ist, die das Zertifikat erteilt –** alle für das Zertifizierungsverfahren notwendigen Informationen vorzulegen.

(5a) Der Inhaber eines Zertifikats informiert die Stelle, die das Zertifikat ausgestellt hat, über etwaige später festgestellte Schwachstellen oder Unregelmäßigkeiten hinsichtlich der Sicherheit des zertifizierten IKT-Prozesses, -Produkts oder -Dienstes, die sich auf die mit der Zertifizierung verbundenen Anforderungen auswirken könnten. Die Stelle leitet diese Informationen unverzüglich an die nationale Cybersicherheitszertifizierungsbehörde weiter.

(6) Zertifikate werden für **die im jeweiligen Zertifizierungssystem festgelegte** [...] **D**auer erteilt und können [...] verlängert werden, sofern die einschlägigen Voraussetzungen weiterhin erfüllt sind.

(7) Ein nach diesem Artikel ausgestelltes europäisches Cybersicherheitszertifikat wird in allen Mitgliedstaaten anerkannt.

Artikel 49

Nationale Cybersicherheitszertifizierungssysteme und Cybersicherheitszertifikate

(1) Unbeschadet des Absatzes 3 werden nationale Systeme für die Cybersicherheitszertifizierung und die zugehörigen Verfahren für die IKT**-Prozesse,** -Produkte und -Dienste, die unter ein europäisches System für die Cybersicherheitszertifizierung fallen, ab dem Zeitpunkt unwirksam, der in dem nach Artikel 44 Absatz 4 erlassenen Durchführungsrechtsakt festgelegt ist. Nationale Systeme für die Cybersicherheitszertifizierung und die zugehörigen Verfahren für die IKT**-Prozesse,** -Produkte und -Dienste, die nicht unter ein europäisches System für die Cybersicherheitszertifizierung fallen, bleiben bestehen.

(2) Die Mitgliedstaaten führen keine neuen nationalen Systeme für die Cybersicherheitszertifizierung von IKT**-Prozesse,** -Produkten und -Diensten ein, die unter ein geltendes europäisches System für die Cybersicherheitszertifizierung fallen.

(3) Vorhandene Zertifikate, die auf der Grundlage nationaler Systeme für die Cybersicherheitszertifizierung ausgestellt wurden **und unter ein europäische Systeme für die Cybersicherheitszertifizierung fallen**, bleiben bis zum Ende ihrer Geltungsdauer gültig.

Artikel 50

Nationale [...]* Cybersicherheits*zertifizierungsbehörde

(1) Jeder Mitgliedstaat benennt eine **oder mehrere** nationale [...] **Cybersicherheits**zertifizierungsbehörden **in seinem Hoheitsgebiet oder in gegenseitigem Einverständnis mit einem anderen Mitgliedstaat eine oder mehrere Behörden mit Sitz in diesem anderen Mitgliedstaat, die für die Aufsichtsaufgaben im benennenden Mitgliedstaat zuständig sein sollen.**

(2) Jeder Mitgliedstaat teilt der Kommission die Namen der benannten Behörde**n sowie die ihnen zugewiesenen Aufgaben** mit.

(3) **Unbeschadet des Artikels 48 Absatz 4 Buchstabe a und Absatz 4a ist j**ede nationale [...] **Cybersicherheits**zertifizierungsbehörde im Hinblick auf ihre Organisation, Finanzierungsentscheidungen, Rechtsform und Entscheidungsfindung unabhängig von den Stellen, die sie beaufsichtigt.

(3a) Die Mitgliedstaaten stellen sicher, dass bei den Tätigkeiten der nationalen Cybersicherheitszertifizierungsbehörden im Zusammenhang mit der Ausstellung von Zertifikaten nach Artikel 48 Absatz 4 Buchstabe a und Absatz 4a eine strenge Trennung der Aufgaben und Zuständigkeiten von den Aufsichtstätigkeiten nach diesem Artikel gewahrt wird und dass beide Tätigkeiten unabhängig voneinander durchgeführt werden.

(4) Die Mitgliedstaaten sorgen für eine angemessene Ausstattung der nationalen [...] **Cybersicherheits**zertifizierungsbehörden, damit diese ihre Befugnisse ausüben und die ihnen übertragenen Aufgaben wirksam und effizient wahrnehmen können.

(5) Im Hinblick auf eine wirksame Durchführung dieser Verordnung sollten diese Behörden in der nach Artikel 53 eingesetzten Europäischen Gruppe für die Cybersicherheitszertifizierung in aktiver, wirksamer, effizienter und sicherer Weise mitarbeiten.

(6) Die nationalen [...] **Cybersicherheits**zertifizierungsbehörden haben folgende Aufgaben:

a) [...]

aa) Überwachung und Durchsetzung der in Artikel 47a Absätze 2 und 3 und im entsprechenden europäischen System für die Cybersicherheitszertifizierung festgelegten Verpflichtungen der in ihrem jeweiligen Hoheitsgebiet niedergelassenen Hersteller oder Anbieter von IKT-Produkten und -Diensten;

b) [...] **unbeschadet des Artikels 51 Absatz 1b Unterstützung der nationalen Akkreditierungsstellen bei der Überwachung und Beaufsichtigung** der Tätigkeiten der Konformitätsbewertungsstellen für die Zwecke dieser Verordnung [...];

ba) Überwachung und Beaufsichtigung der Tätigkeiten der in Artikel 48 Absatz 4 genannten Stellen;

bb) Ermächtigung der Konformitätsbewertungsstellen nach Artikel 51 Absatz 1b und Beschränkung, Aussetzung und Entzug bestehender Ermächtigungen bei Verstößen gegen die Anforderungen dieser Verordnung;

c) Bearbeitung von Beschwerden, die von natürlichen oder juristischen Personen in Bezug auf Zertifikate eingereicht werden, die von **der nationalen Cybersicherheitszertifizierungs-behörde oder nach Artikel 48 Absatz 4a von den Konformitätsbewertungsstellen** [...] ausgestellt wurden, Untersuchung des Beschwerdegegenstands, soweit angemessen, und Unterrichtung des Beschwerdeführers über die Fortschritte und das Ergebnis der Untersuchung innerhalb einer angemessenen Frist;

d) Zusammenarbeit mit anderen nationalen [...] **Cybersicherheits**zertifizierungsbehörden und anderen öffentlichen Stellen; dies beinhaltet auch den Informationsaustausch über die etwaige Nichtkonformität von IKT**-Prozessen,** -Produkten und -Diensten mit den Anforderungen dieser Verordnung oder bestimmten europäischen Systemen für die Cybersicherheitszertifizierung;

e) Verfolgung einschlägiger Entwicklungen auf dem Gebiet der Cybersicherheitszertifizierung.

(7) Jede nationale [...] **Cybersicherheits**zertifizierungsbehörde hat mindestens die folgenden Befugnisse:

a) Sie kann die Konformitätsbewertungsstellen, [...] die Inhaber europäischer Cybersicherheitszertifikate **und die Aussteller von EU-Konformitätserklärungen** auffordern, ihr sämtliche Auskünfte zu erteilen, die sie für die Erfüllung ihrer Aufgaben benötigt;

b) sie kann Untersuchungen in Form von Rechnungsprüfungen bei den Konformitätsbewertungsstellen, [...] den Inhabern europäischer Cybersicherheitszertifikate **und den Ausstellern von EU-Konformitätserklärungen** durchführen, um die Einhaltung der Bestimmungen des Titels III zu überprüfen;

c) sie kann im Einklang mit einzelstaatlichem Recht geeignete Maßnahmen ergreifen, um sicherzustellen, dass die Konformitätsbewertungsstellen, [...] die Inhaber von Zertifikaten **und die Aussteller von EU-Konformitätserklärungen** den Anforderungen dieser Verordnung oder eines europäischen Systems für die Cybersicherheitszertifizierung genügen;

d) sie erhält Zugang zu den Räumlichkeiten von Konformitätsbewertungsstellen und von Inhabern europäischer Cybersicherheitszertifikate zum Zweck der Durchführung von Untersuchungen im Einklang mit den Verfahrensvorschriften der Union oder des Mitgliedstaats;

e) sie kann im Einklang mit einzelstaatlichem Recht Zertifikate widerrufen, die **von der nationalen Cybersicherheitszertifizierungsbehörde oder nach Artikel 48 Absatz 4a von den Konformitätsbewertungsstellen ausgestellt wurden, wenn sie** den Anforderungen dieser Verordnung oder eines europäischen Systems für die Cybersicherheitszertifizierung nicht genügen;

f) sie kann nach Artikel 54 und im Einklang mit einzelstaatlichem Recht Strafen verhängen und die unverzügliche Beendigung der Verletzung der in dieser Verordnung festgelegten Verpflichtungen anordnen.

(8) Die nationalen [...] **Cybersicherheits**zertifizierungsbehörden arbeiten untereinander und mit der Kommission zusammen und tauschen insbesondere Informationen, Erfahrungen und bewährte Verfahren im Zusammenhang mit der Cybersicherheitszertifizierung und technischen Fragen in Bezug auf die Cybersicherheit von IKT**-Prozessen,** -Produkten und -Diensten aus.

Artikel 51

Konformitätsbewertungsstellen

(1) Die Konformitätsbewertungsstellen werden von den nach der Verordnung (EG) Nr. 765/2008 benannten nationalen Akkreditierungsstellen nur dann akkreditiert, wenn sie die im Anhang dieser Verordnung aufgeführten Anforderungen erfüllen.

(1a) Falls eine nationale Cybersicherheitszertifizierungsbehörde nach Artikel 48 Absatz 4 Buchstabe a und Absatz 4a ein europäisches Cybersicherheitszertifikat ausstellt, wird die Zertifizierungsstelle der nationalen Cybersicherheitszertifizierungsbehörde nach Absatz 1 als Konformitätsbewertungsstelle akkreditiert.

(1b) Die Konformitätsbewertungsstellen werden gegebenenfalls von der nationalen Cybersicherheitszertifizierungsbehörde ermächtigt, ihre Aufgaben wahrzunehmen, wenn diese Stellen im europäischen Zertifizierungssystem niedergelegten speziellen oder zusätzlichen Anforderungen nach Artikel 47 Absatz 1 Buchstabe ca genügen.

(2) Die Akkreditierung wird für eine Höchstdauer von fünf Jahren erteilt und kann unter denselben Bedingungen verlängert werden, sofern die Konformitätsbewertungsstelle die Anforderungen dieses Artikels erfüllt. Die Akkreditierungsstellen **treffen innerhalb einer angemessenen Frist alle angebrachten Maßnahmen, um** eine Akkreditierung einer Konformitätsbewertungsstelle nach Absatz 1 **zu beschränken, auszusetzen oder zu** widerrufen, wenn die Voraussetzungen für die Akkreditierung nicht oder nicht mehr erfüllt sind oder wenn eine Konformitätsbewertungsstelle Maßnahmen ergreift, die gegen diese Verordnung verstoßen.

Artikel 52

Notifizierung

(1) Für jedes nach Artikel 44 angenommene europäische System für die Cybersicherheitszertifizierung notifizieren die nationalen [...] **Cybersicherheits**zertifizierungsbehörden der Kommission die Konformitätsbewertungsstellen, die für die Erteilung von Zertifikaten entsprechend den in Artikel 46 genannten Vertrauenswürdigkeitsstufen akkreditiert **und gegebenenfalls nach Artikel 51 Absatz 1b ermächtigt** wurden, sowie unverzüglich etwaige diesbezügliche Änderungen.

(2) Ein Jahr nach Inkrafttreten eines europäischen Systems für die Cybersicherheitszertifizierung veröffentlicht die Kommission im Amtsblatt der Europäischen Union eine Liste der notifizierten Konformitätsbewertungsstellen.

(3) Geht der Kommission nach Ablauf der in Absatz 2 genannten Frist eine Notifizierung zu, so veröffentlicht sie die Änderungen an der in Absatz 2 genannten Liste innerhalb von zwei Monaten ab dem Zeitpunkt des Eingangs dieser Notifizierung im Amtsblatt der Europäischen Union.

(4) Eine nationale [...] **Cybersicherheits**zertifizierungsbehörde kann bei der Kommission die Streichung einer von diesem Mitgliedstaat notifizierten Konformitätsbewertungsstelle aus der in Absatz 2 genannten Liste beantragen. Die Kommission veröffentlicht im Amtsblatt der Europäischen Union die entsprechenden Änderungen der Liste innerhalb eines Monats ab dem Zeitpunkt, zu dem der Antrag der nationalen [...] **Cybersicherheits**zertifizierungsbehörde eingegangen ist.

(5) Die Kommission kann im Wege von Durchführungsrechtsakten Einzelheiten, Form und Verfahren für die Notifizierungen nach Absatz 1 festlegen. Diese Durchführungsrechtsakte werden nach dem in Artikel 55 Absatz 2 genannten Prüfverfahren erlassen.

Artikel 53

Europäische Gruppe für die Cybersicherheitszertifizierung

(1) Die Europäische Gruppe für die Cybersicherheitszertifizierung (im Folgenden die "Gruppe") wird eingesetzt.

(2) Die Gruppe setzt sich aus **Vertretern der** nationalen [...] Behörden für die **Cybersicherheits**zertifizierung oder **Vertretern anderer einschlägiger nationaler Behörden** zusammen. [...] **Ein Mitglied der Gruppe darf nicht mehr als einen anderen Mitgliedstaat vertreten.**

(3) Die Gruppe hat folgende Aufgaben:

a) Sie berät und unterstützt die Kommission bei ihren Tätigkeiten zur Gewährleistung einer einheitlichen Umsetzung und Anwendung dieses Titels, insbesondere in politischen Fragen der Cybersicherheitszertifizierung, bei der Koordinierung von Politikkonzepten und bei der Ausarbeitung europäischer Systeme für die Cybersicherheitszertifizierung;

b) sie unterstützt und berät die ENISA bei der Ausarbeitung eines möglichen Systems nach Artikel 44 und arbeitet hierbei mit der ENISA zusammen;

ba) sie gibt nach Artikel 44 eine Stellungnahme zu dem möglichen System ab;

c) sie [...] **beauftragt** die Agentur mit der Ausarbeitung eines möglichen europäischen Systems für die Cybersicherheitszertifizierung nach Artikel 44;

ca) sie erarbeitet und verabschiedet Leitlinien für Kriterien für die Bewertung der Vorschläge zur Erstellung eines möglichen Systems, die [...] der Gruppe nach Artikel 44 Absatz 1a unterbreitet werden;

d) sie gibt an die Kommission gerichtete Stellungnahmen zur Pflege und Überprüfung vorhandener europäischer Systeme für die Cybersicherheitszertifizierung ab;

e) sie prüft die einschlägigen Entwicklungen auf dem Gebiet der Cybersicherheitszertifizierung und tauscht Informationen über bewährte Verfahren für Cybersicherheitszertifizierungssysteme aus;

f) sie erleichtert die Zusammenarbeit zwischen den nationalen [...] Behörden für die **Cybersicherheits**zertifizierung nach diesem Titel im Wege **des Kapazitätsaufbaus** und des Informationsaustauschs, vor allem durch die Festlegung von Methoden für einen effizienten Austausch von Informationen über alle Fragen der Cybersicherheitszertifizierung;

fa) sie leistet Unterstützung bei der Durchführung des Mechanismus der gegenseitigen Begutachtung gemäß den Regeln, die für ein Europäischen Cybersicherheits-zertifizierungssystem nach Artikel 47 Absatz 1 Buchstabe md gelten.

(4) Die Kommission führt **als Moderatorin** den Vorsitz der Gruppe und nimmt mit Unterstützung der ENISA nach Artikel 8 Buchstabe a deren Sekretariatsgeschäfte wahr.

Artikel 53a

Recht auf Beschwerde bei der nationalen [...] Cybersicherheitszertifizierungsbehörde

(1) Natürliche und juristische Personen haben das Recht, bei der nationalen Cybersicherheitszertifizierungsbehörde eine Beschwerde wegen eines von derselben Behörde oder nach Artikel 48 Absatz 4a von Konformitätsbewertungsstellen ausgestellten Zertifikats einzureichen.

(2) Die nationale Cybersicherheitszertifizierungsbehörde, bei der die Beschwerde eingereicht wurde, unterrichtet den Beschwerdeführer über den Stand und die Ergebnisse der Beschwerde einschließlich der Möglichkeit eines gerichtlichen Rechtsbehelfs nach Artikel 53b.

Artikel 53b

Recht auf einen wirksamen gerichtlichen Rechtsbehelf

(1) Natürliche und juristische Personen haben das Recht auf einen wirksamen gerichtlichen Rechtsbehelf gegen eine sie betreffende rechtsverbindliche Entscheidung einer nationalen Cybersicherheitszertifizierungsbehörde.

(2) Natürliche und juristische Personen haben das Recht auf einen wirksamen gerichtlichen Rechtsbehelf, wenn sich die nationale Cybersicherheitszertifizierungsbehörde nicht mit einer Beschwerde befasst.

(3) Eine Klage gegen eine nationale Cybersicherheitszertifizierungsbehörde wird bei den Gerichten des Mitgliedstaates erhoben, in dem die Behörde ihren Sitz hat.

Artikel 54

Sanktionen

Die Mitgliedstaaten erlassen Vorschriften über Sanktionen, die bei Verstößen gegen diesen Titel und die europäischen Systeme für die Cybersicherheitszertifizierung zu verhängen sind, und treffen alle für die Anwendung der Sanktionen erforderlichen Maßnahmen. Die vorgesehenen Sanktionen müssen wirksam, verhältnismäßig und abschreckend sein. Die Mitgliedstaaten teilen der Kommission diese Vorschriften und Maßnahmen [bis zum … /unverzüglich] mit und melden ihr etwaige spätere Änderungen.

TITEL IV
SCHLUSSBESTIMMUNGEN

Artikel 55

Ausschussverfahren

(1) Die Kommission wird von einem Ausschuss unterstützt. Dieser Ausschuss ist ein Ausschuss im Sinne der Verordnung (EU) Nr. 182/2011.

(2) Wird auf diesen Absatz Bezug genommen, so gilt Artikel **5 Absatz** 4 **Buchstabe b** der Verordnung (EU) Nr. 182/2011.

Artikel 56

Bewertung und Überarbeitung

(1) Spätestens fünf Jahre nach dem in Artikel 58 genannten Zeitpunkt und danach alle fünf Jahre bewertet die Kommission die Wirkung, Wirksamkeit und Effizienz der Agentur und ihrer Arbeitsmethoden und prüft, ob das Mandat der Agentur möglicherweise geändert werden muss und welche finanziellen Auswirkungen eine solche Änderung hätte. In der Bewertung werden alle Rückmeldungen an die Agentur in Bezug auf ihre Tätigkeiten berücksichtigt. Gelangt die Kommission zu der Auffassung, dass Ziele, Mandat und Aufgaben der Agentur deren Fortbestehen nicht länger rechtfertigen, kann sie eine Änderung dieser Verordnung im Hinblick auf die für die Agentur geltenden Bestimmungen vorschlagen.

(2) Die Bewertung erstreckt sich auch auf die Wirkung, Wirksamkeit und Effizienz der Bestimmungen des Titels III im Hinblick auf die Ziele, für IKT-Produkte und -Dienste in der Union ein angemessenes Maß an Cybersicherheit und einen besser funktionierenden Binnenmarkt zu gewährleisten.

(3) Die Kommission übermittelt den Bewertungsbericht zusammen mit ihren Schlussfolgerungen dem Europäischen Parlament, dem Rat und dem Verwaltungsrat. Die Ergebnisse des Bewertungsberichts werden öffentlich bekannt gemacht.

Artikel 57

Aufhebung und Rechtsnachfolge

(1) Die Verordnung (EG) Nr. 526/2013 wird mit Wirkung vom [...] aufgehoben.

(2) Bezugnahmen auf die Verordnung (EG) Nr. 526/2013 und auf die ENISA gelten als Bezugnahmen auf diese Verordnung und auf die Agentur.

(3) Die Agentur ist in Bezug auf das Eigentum und alle Übereinkünfte, rechtlichen Verpflichtungen, Beschäftigungsverträge, finanziellen Verpflichtungen und Verbindlichkeiten Rechtsnachfolger der durch die Verordnung (EG) Nr. 526/2013 errichteten Agentur. Alle vom Verwaltungsrat und vom Exekutivrat getroffenen Entscheidungen bleiben gültig, sofern sie den Bestimmungen dieser Verordnung nicht zuwiderlaufen.

(4) Die Agentur wird zum [...] auf unbegrenzte Zeit errichtet.

(5) Der nach Artikel 24 Absatz 4 der Verordnung (EG) Nr. 526/2013 ernannte Exekutivdirektor bleibt für die restliche Dauer seiner Amtszeit der Exekutivdirektor der Agentur.

(6) Die nach Artikel 6 der Verordnung (EG) Nr. 526/2013 ernannten Mitglieder des Verwaltungsrats und ihre Stellvertreter bleiben für die restliche Dauer ihrer Amtszeit Mitglieder des Verwaltungsrats der Agentur und deren Stellvertreter.

Artikel 58

Inkrafttreten

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

(1a) Diese Verordnung gilt ab dem […] mit Ausnahme der Artikel 50, 51, 52, 53a, 53b und 54, die ab dem [24 Monate nach ihrer Veröffentlichung im Amtsblatt der Europäischen Union] gelten.

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

Geschehen zu Brüssel am […]

Im Namen des Europäischen Parlaments	*Im Namen des Rates*
Der Präsident	*Der Präsident*

ANFORDERUNGEN AN KONFORMITÄTSBEWERTUNGSSTELLEN

Konformitätsbewertungsstellen, die akkreditiert werden möchten, müssen folgende Anforderungen erfüllen:

1. Eine Konformitätsbewertungsstelle muss nach nationalem Recht gegründet und mit Rechtspersönlichkeit ausgestattet sein.

2. Bei einer Konformitätsbewertungsstelle muss es sich um einen unabhängigen Dritten handeln, der mit der Einrichtung oder den IKT-Produkten und -Diensten, die er bewertet, in keinerlei Verbindung steht.

3. Eine Stelle, die einem Wirtschaftsverband oder einem Fachverband angehört und die IKT-Produkte oder -Dienste bewertet, an deren Entwurf, Herstellung, Bereitstellung, Montage, Verwendung oder Wartung Unternehmen beteiligt sind, die von diesem Verband vertreten werden, kann als Konformitätsbewertungsstelle gelten, sofern ihre Unabhängigkeit sowie das Fehlen jedweder Interessenkonflikte nachgewiesen sind.

4. Eine Konformitätsbewertungsstelle, ihre oberste Leitungsebene und die für die Erfüllung der Konformitätsbewertungsaufgaben zuständigen Mitarbeiter dürfen weder Konstrukteur, Hersteller, Lieferant, Installateur, Käufer, Eigentümer, Verwender oder Wartungsbetrieb der zu bewertenden IKT-Produkte oder -Dienste noch Bevollmächtigter einer dieser Parteien sein. Dies schließt nicht die Verwendung von bereits einer Konformitäts-bewertung unterzogenen Produkten, die für die Tätigkeit der Konformitätsbewertungsstelle nötig sind, oder die Verwendung solcher Produkte zum persönlichen Gebrauch aus.

5. Eine Konformitätsbewertungsstelle, ihre oberste Leitungsebene und die für die Erfüllung der Konformitätsbewertungsaufgaben zuständigen Mitarbeiter dürfen weder direkt an Entwurf, Herstellung bzw. Bau, Vermarktung, Installation, Verwendung oder Instandsetzung dieser IKT-Produkte oder -Dienste beteiligt sein, noch die an diesen Tätigkeiten beteiligten Parteien vertreten. Sie dürfen sich nicht mit Tätigkeiten befassen, die ihre Unabhängigkeit bei der Beurteilung oder ihre Integrität im Zusammenhang mit den Konformitätsbewertungstätigkeiten, für die sie benannt sind, beeinträchtigen können. Dies gilt besonders für Beratungsdienste.

6. Die Konformitätsbewertungsstellen müssen sicherstellen, dass Tätigkeiten ihrer Zweigunternehmen oder Unterauftragnehmer die Vertraulichkeit, Objektivität oder Unparteilichkeit ihrer Konformitätsbewertungstätigkeiten nicht beeinträchtigen.

7. Die Konformitätsbewertungsstellen und ihre Mitarbeiter müssen die Konformitätsbewertungstätigkeiten mit höchster beruflicher Integrität und der erforderlichen fachlichen Kompetenz in dem betreffenden Bereich durchführen; sie dürfen keinerlei Einflussnahme, insbesondere finanzieller Art, ausgesetzt sein, die sich auf ihre Beurteilung oder die Ergebnisse ihrer Konformitätsbewertungsarbeit auswirken könnte, insbesondere keiner Einflussnahme durch Personen oder Personengruppen, die ein Interesse am Ergebnis dieser Tätigkeiten haben.

8. Eine Konformitätsbewertungsstelle muss in der Lage sein, die bei der Konformitätsbewertung anfallenden Aufgaben, die ihr mit dieser Verordnung übertragen wurden, auszuführen, unabhängig davon, ob diese Aufgaben von ihr selbst oder in ihrem Namen und unter ihrer Verantwortung ausgeführt werden.

9. Eine Konformitätsbewertungsstelle muss jederzeit, für jedes Konformitätsbewertungsverfahren und für jede Art, Kategorie und Unterkategorie von IKT-Produkten oder -Diensten über Folgendes verfügen:

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

b) Beschreibungen von Verfahren, nach denen die Konformitätsbewertung durchgeführt wird, um sicherzustellen, dass die Verfahren transparent sind und wiederholt werden können. Sie muss über angemessene Regelungen und Verfahren verfügen, bei denen zwischen den Aufgaben, die sie als notifizierte Stelle wahrnimmt, und anderen Tätigkeiten unterschieden wird;

c) Verfahren zur Durchführung von Tätigkeiten, bei denen die Größe eines Unternehmens, die Branche, in der es tätig ist, seine Struktur, der Grad an Komplexität der jeweiligen Technologie der ICT-Produkte oder -Dienste und der Umstand, dass es sich um Massenfertigung oder Serienproduktion handelt, gebührend berücksichtigt werden.

10. Eine Konformitätsbewertungsstelle muss über die erforderlichen Mittel zur angemessenen Erledigung der technischen und administrativen Aufgaben verfügen, die mit der Konformitätsbewertung verbunden sind, und Zugang zu allen benötigten Ausrüstungen und Einrichtungen haben.

11. Die Mitarbeiter, die für die Durchführung der Konformitätsbewertungstätigkeiten zuständig sind, besitzen:

a) eine solide Fach- und Berufsausbildung, die alle Tätigkeiten für die Konformitätsbewertung umfasst;

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

c) angemessene Kenntnis und angemessenes Verständnis der geltenden Anforderungen und Prüfnormen;

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

12. Die Unparteilichkeit der Konformitätsbewertungsstellen, ihrer obersten Führungsebene und ihres Bewertungspersonals muss garantiert sein.

13. Die Vergütung für die oberste Leitungsebene und das bewertende Personal der Konformitätsbewertungsstelle darf sich nicht nach der Anzahl der durchgeführten Bewertungen oder deren Ergebnissen richten.

14. Die Konformitätsbewertungsstellen müssen eine Haftpflichtversicherung abschließen, sofern die Haftpflicht nicht aufgrund der nationalen Rechtsvorschriften vom Staat übernommen wird oder der Mitgliedstaat selbst unmittelbar für die Konformitätsbewertung verantwortlich ist.

15. Informationen, welche die Mitarbeiter einer Konformitätsbewertungsstelle bei der Durchführung ihrer Aufgaben nach dieser Verordnung oder einer nationalen Durchführungsvorschrift erhalten, fallen unter die berufliche Schweigepflicht, außer gegenüber den zuständigen Behörden der Mitgliedstaaten, in denen sie ihre Tätigkeiten ausüben.

16. Die Konformitätsbewertungsstellen müssen die Anforderungen der **einschlägigen** Norm erfüllen**, die gemäß der Verordnung (EG) 765/2008 für die Akkreditierung der Konformitätsbewertungsstellen, die die Zertifizierung von Prozessen, Produkten oder Dienstleistungen vornehmen, harmonisiert wird**[...]**.**

17. Die Konformitätsbewertungsstellen müssen sicherstellen, dass die für die Konformitätsbewertung eingesetzten Prüflabors den Anforderungen der **einschlägigen** Norm entsprechen, **die gemäß der Verordnung (EG) 765/2008 für die Akkreditierung der Labors, die Tests vornehmen, harmonisiert wird**[...].