BERICHT UND ANTRAG

DER REGIERUNG

AN DEN

LANDTAG DES FÜRSTENTUMS LIECHTENSTEIN

BETREFFEND

DIE BESCHLÜSSE NR. 21/2023, 22/2023 UND 27/2023

DES GEMEINSAMEN EWR-AUSSCHUSSES

Richtlinie (EU) 2016/1148 («NIS-Richtlinie»), Verordnung (EU) 2019/881 («ENISA-Verordnung») und Verordnung (EU) 2021/887 des Europäischen Parlaments und des Rates

Behandlung im Landtag	
	Datum
Schlussabstimmung	

Nr. 36/2023

INHALTSVERZEICHNIS

Seite

Beilagen:

- Beschlüsse Nr. 21/2023, 22/2023 und 27/2023 des Gemeinsamen EWR-Ausschusses vom 3. Februar 2023 (inoffizielle Übersetzung des Originals zu Informationszwecken);
- Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Massnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union (ABl. L 202 vom 8.6.2021, S. 1);

- Verordnung (EU) 2019/881 des Europäischen Parlaments und des Rates vom 17. April 2019 über die ENISA (Agentur der Europäischen Union für Cybersicherheit) und über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik und zur Aufhebung der Verordnung (EU) Nr. 526/2013 (ABl. L 151 vom 7.6.2019, S. 15);
- Verordnung (EU) 2021/887 des Europäischen Parlaments und des Rates vom 20. Mai 2021 zur Einrichtung des Europäischen Kompetenzzentrums für Industrie, Technologie und Forschung im Bereich der Cybersicherheit und des Netzwerks nationaler Koordinierungszentren (ABl. L 202 vom 8.6.2021, S. 1).

ZUSAMMENFASSUNG

Am 3. Februar 2023 wurden die Beschlüsse Nr. 21/2023, 22/2023 und 27/2023 des Gemeinsamen EWR-Ausschusses im Bereich Cyber-Sicherheit unterzeichnet. Liechtenstein hat einen Vorbehalt nach Art. 103 des EWR-Abkommens angemeldet, da die Umsetzung der Richtlinie (EU) 2016/1148 bzw. die Durchführung der Verordnungen (EU) 2019/881 und 2021/887 in Liechtenstein den Erlass von Gesetzesbestimmungen bedingt.

Mit Beschluss Nr. 21/2023 des Gemeinsamen EWR-Ausschusses wurde die Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Massnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union («NIS-Richtlinie») in das EWR-Abkommen übernommen.

Die Richtlinie (EU) 2016/1148 sieht den EWR-weiten Aufbau nationaler Kapazitäten für Cybersicherheit sowie eine stärkere Zusammenarbeit der EWR-Mitgliedstaaten vor. Ihr Ziel besteht darin, ein gleichmässig hohes Sicherheitsniveau von Netz- und Informationssystemen im gesamten EWR zu erreichen. Inhaltlich regelt die Richtlinie (EU) 2016/1148 insbesondere Sicherheitsanforderungen und Meldepflichten für Betreiber wesentlicher Dienste und Anbieter digitaler Dienste sowie die Aufgaben und Befugnisse der zuständigen nationalen Behörde in Bezug auf die Überwachung dieser Sicherheitsanforderungen und Meldepflichten. Mit der Richtlinie werden zudem sogenannte Computer-Notfallteams (CSIRTs) eingeführt, welche jeder EWR-Mitgliedstaat benennt und die diesen bei der Bewältigung von Risiken und Sicherheitsvorfällen unterstützen.

Mit Beschluss Nr. 22/2023 des Gemeinsamen EWR-Ausschusses wurde die Verordnung (EU) 2019/881 des Europäischen Parlaments und des Rates vom 17. April 2019 über die ENISA (Agentur der Europäischen Union für Cybersicherheit) und über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik und zur Aufhebung der Verordnung (EU) Nr. 526/2013 in das EWR-Abkommen übernommen.

Mit Beschluss Nr. 27/2023 des Gemeinsamen EWR-Ausschusses wurde die Verordnung (EU) 2021/887 des Europäischen Parlaments und des Rates vom

20. Mai 2021 zur Einrichtung des Europäischen Kompetenzzentrums für Industrie, Technologie und Forschung im Bereich der Cybersicherheit und des Netzwerks nationaler Koordinierungszentren in das EWR-Abkommen übernommen.

Mit der Verordnung (EU) 2021/887 sollen in den EWR-Mitgliedstaaten Nationale Koordinierungszentrum Cybersicherheit geschaffen werden, welche als Teil des Netzwerks nationaler Koordinierungszentren im EWR zusammen mit dem Europäischen Kompetenzzentrum für Cybersicherheit (ECCC) den neuen europäischen institutionellen Rahmen zur Unterstützung der Innovations- und Industriepolitik im Bereich der Cybersicherheit bilden sollen.

Liechtenstein ist zur Übernahme der Richtlinie (EU) 2016/1148 sowie der Verordnungen (EU) 2019/881 und 2021/887 aufgrund seiner EWR-Mitgliedschaft verpflichtet. Die Umsetzung der Richtlinie (EU) 2016/1148 bzw. die Durchführung der Verordnungen (EU) 2019/881 und 2021/887 bedingt den Erlass von Gesetzesbestimmungen. Der entsprechende Bericht und Antrag wurde vom Landtag im März 2023 in erster Lesung behandelt (BuA Nr. 9/2023).[1] Die zweite Lesung und Beschlussfassung dieser Gesetzesvorlagen durch den Landtag soll in der Landtagssitzung im Mai 2023 stattfinden. Als Inkrafttretensdatum ist der 1. Juli 2023 vorgesehen.

Die Beschlüsse Nr. 21/2023, 22/2023 und 27/2023 des Gemeinsamen EWR-Ausschusses vom 3. Februar 2023 bedürfen zu ihrer Gültigkeit der Zustimmung des Landtages, da es sich hierbei um Staatsverträge handelt, durch welchen Verpflichtungen im Sinne von Art. 8 Abs. 2 der Landesverfassung eingegangen werden.

ZUSTÄNDIGES MINISTERIUM

Ministerium für Präsidiales und Finanzen

BETROFFENE STELLE

Stabsstelle Cyber-Sicherheit

---

[1] Bericht und Antrag Nr. 9/2023 betreffend die Schaffung eines Gesetzes über Cybersicherheit (Cyber-Sicherheitsgesetz; CSG) sowie Abänderung des Beschwerdekommissiongesetzes (https://www.llv.li/files/srk/bua_009_2023_bua-csg.pdf).

Vaduz, 03. April 2023

LNR 2023-590

P

Sehr geehrter Herr Landtagspräsident,
Sehr geehrte Frauen und Herren Abgeordnete

Die Regierung gestattet sich, dem Hohen Landtag nachstehenden Bericht und Antrag zu den Beschlüssen Nr. 21/2023, 22/2023 und 27/2023 des Gemeinsamen EWR-Ausschusses vom 3. Februar 2023 zu unterbreiten.

I. BERICHT DER REGIERUNG

1. AUSGANGSLAGE

Am 3. Februar 2023 hat der Gemeinsame EWR–Ausschuss beschlossen, die Richtlinie (EU) 2016/1148 sowie die Verordnungen (EU) 2019/881 und 2021/887 in das EWR-Abkommen zu übernehmen (Beschlüsse Nr. 21/2023, 22/2023 und 27/2023 des Gemeinsamen EWR-Ausschusses).

Die Richtlinie (EU) 2016/1148 ist in den EU-Mitgliedstaaten am 8. August 2016 in Kraft getreten und war in der EU bis zum 9. Mai 2018 umzusetzen. Für die EWR/EFTA-Staaten gilt das Datum des Inkrafttretens des entsprechenden EWR-Übernahmebeschlusses als Umsetzungsfrist für die Richtlinie.

Die Verordnung (EU) 2019/881 ist in den EU-Mitgliedstaaten am 27. Juni 2019 in Kraft getreten. Sie wird mit ihrer Übernahme ins EWR-Abkommen grundsätzlich in

Liechtenstein unmittelbar anwendbar. Allerdings enthält die Verordnung (EU) 2019/881 Bestimmungen, die sich unmittelbar an die EWR-Mitgliedstaaten richten und daher eine Durchführung im liechtensteinischen Recht erfordern.

Die Verordnung (EU) 2021/887 ist in den EU-Mitgliedstaaten am 28. Juni 2021 in Kraft getreten. Sie wird mit ihrer Übernahme ins EWR-Abkommen grundsätzlich in Liechtenstein unmittelbar anwendbar. Allerdings enthält auch die Verordnung (EU) 2021/887 Bestimmungen, die sich unmittelbar an die EWR-Mitgliedstaaten richten und daher eine Durchführung im liechtensteinischen Recht erfordern.

Zur Umsetzung der Richtlinie (EU) 2016/1148 sowie zur Durchführung der Verordnungen 2021/887 wird ein Gesetz über Cybersicherheit (Cyber-Sicherheitsgesetz; CSG) geschaffen sowie das Beschwerdekommissiongesetz abgeändert. Der entsprechende Bericht und Antrag wurde vom Landtag im März 2023 in erster Lesung behandelt (BuA Nr. 9/2023). Die zweite Lesung und Beschlussfassung durch den Landtag soll in der Landtagssitzung im Mai 2023 stattfinden. Als Inkrafttretensdatum ist der 1. Juli 2023 vorgesehen.

Das Inkrafttreten des Beschlusses Nr. 17/2023 des Gemeinsamen EWR-Ausschusses erfordert den Abschluss der Zustimmungsverfahren durch die nationalen Gesetzgeber in den EWR/EFTA-Staaten Norwegen und Liechtenstein.

Der vorliegende Bericht und Antrag und dessen Behandlung dienen dazu, die Zustimmung des Landtags einzuholen.

2. BEGRÜNDUNG DER VORLAGE

Die EWR/Schengen-Kommission des Landtages und die Regierung haben in ihren Sitzungen vom 23. Januar 2023 bzw. vom 31. Januar 2023 befunden, dass die Beschlüsse Nr. 21/2023, 22/2023 und 27/2023 des Gemeinsamen EWR-Ausschusses der Zustimmung des Landtages gemäss Art. 8 Abs. 2 der

Landesverfassung bedürfen, da aufgrund der Richtlinie (EU) 2016/1148 bzw. der Verordnungen (EU) 2019/881 und 2021/887 liechtensteinisches Recht anzupassen ist.

3. SCHWERPUNKT DER VORLAGE

Mit der Richtlinie (EU) 2016/1148 soll EU-weit ein hohes Sicherheitsniveau der Netz- und Informationssysteme erreicht werden. Dazu haben die Mitgliedstaaten unter anderem eine nationale NIS-Strategie zu erarbeiten und bestimmte Unternehmen aus wirtschaftlich oder gesellschaftlich wichtigen Sektoren adäquate Sicherheitsmassnahmen einzuführen und gröbere Störfälle zu melden.

Jeder Mitgliedstaat hat darüber hinaus ein oder mehrere Computer-Notfallteams, sogenannte Computer Security Incident Response Teams (CSIRT), einzurichten, denen u.a. Aufgaben wie die mögliche Entgegennahme von Cyber-Vorfallsmeldungen, die Ausgabe von Frühwarnungen, die Reaktion auf Sicherheitsvorfälle oder auch die dynamische Analyse von Risiken und Vorfällen zukommen.

Weiters sind in den Mitgliedstaaten ein oder mehrere nationale Behörden («NIS-Behörden») einzurichten, die unter anderem die Bewertung der Sicherheit von Netz- und Informationssystemen vornehmen und verbindliche Anweisungen zur Abhilfe bei festgestellten Mängeln erteilen können. Als Verbindungsstelle zwischen den Mitgliedstaaten, der Kooperationsgruppe und dem CSIRT-Netzwerk ist zudem in jedem Mitgliedstaat die Einrichtung einer nationalen zentralen Anlaufstelle («Single Point of Contact»; SPOC) vorgesehen

Die Verordnung (EU) 2019/881 soll massgeblich dazu beitragen, dass IT-Produkte, -Dienste und -Prozesse künftig bereits in ihrer Entwicklung Anforderungen an die Cybersicherheit berücksichtigen und umsetzen. Unter dem Begriff der

Cybersicherheit versteht die Verordnung alle Tätigkeiten, die notwendig sind, um Netz- und Informationssysteme, die Nutzer solcher Systeme und sonstige betroffene Personen vor Cyberbedrohungen zu schützen.

Die Verordnung (EU) 2019/881 besteht im Wesentlichen aus zwei Teilen:

- Sie stärkt die Rolle der Agentur der Europäischen Union für Cybersicherheit («ENISA») und stattet sie mit einem dauerhaften Mandat aus.[2]
- Zum anderen führt sie einen Europäischen Zertifizierungsrahmen für Cybersicherheit ein, wobei die ENISA auch dabei eine massgebliche Rolle spielen soll. Die Verordnung selbst enthält noch keine operationalisierbaren Schemata für Zertifizierungen. Vielmehr sollen diese von der ENISA erst auf der Grundlage der Verordnung entwickelt werden.

Im Hinblick auf die Weiterentwicklung der Cybersicherheitslandschaft haben die Europäische Kommission und andere im September 2017 eine gemeinsame Mitteilung vorgelegt, die darauf abzielt, die Widerstandsfähigkeit, Abschreckung und Reaktion der EU auf Cyberangriffe weiter zu stärken. In der Mitteilung wird als strategisches Interesse anerkannt, wesentliche technologische Kapazitäten im Bereich der Cybersicherheit zu erhalten und weiterzuentwickeln, um den digitalen Binnenmarkt (DSM) zu sichern.

Vor diesem Hintergrund wurde die Verordnung (EU) 2021/887 erlassen, durch die ein Europäisches Kompetenzzentrum für Industrie, Technologie und Forschung im Bereich der Cybersicherheit (ECCC) eingesetzt wird. Dadurch soll insbesondere die grenzüberschreitende Zusammenarbeit im Bereich Cybersicherheit im EWR

[2] Die ENISA wurde bereits 2004 als die «Europäische Agentur für Netz- und Informationssicherheit» gegründet. Mit der Verordnung (EU) 2019/881 wurden die Tätigkeitsfelder der ENISA ausgebaut.

gefördert werden. Das Kompetenzzentrum soll auch Teile des Programms «Digitales Europa» umsetzen, indem es Fördergelder vergibt.

Liechtenstein nimmt am Programm Digitales Europa (2021-2027) teil (siehe BuA 124/2020, S. 47 ff.).

4. UMSETZUNG

Zur Umsetzung der Richtlinie (EU) 2016/1148 sowie zur Durchführung der Verordnungen 2021/887 wird ein Gesetz über Cybersicherheit (Cyber-Sicherheitsgesetz; CSG) geschaffen sowie das Beschwerdekommissionsgesetz angepasst.

Der entsprechende Bericht und Antrag wurde vom Landtag im März 2023 in erster Lesung behandelt (BuA Nr. 9/2023). Die zweite Lesung und Beschlussfassung durch den Landtag soll in der Landtagssitzung im Mai 2023 erfolgen.

Als Inkrafttretensdatum ist der 1. Juli 2023 vorgesehen.

Betreffend die Durchführung der Verordnung (EU) 2019/881 sind noch weitere Abklärungen mit anderen EU-Staaten hinsichtlich der praktischen Durchführung erforderlich. Hier vor allem in Bezug auf die möglichen Ausgestaltungsvarianten der gemäss Art. 58 der Verordnung (EU) 2019/881 einzurichtenden nationalen Behörde für die Cybersicherheitszertifzierungen.

5. VERHÄLTNIS ZUR SCHWEIZ

Auf das bilaterale Verhältnis zur Schweiz ergeben sich keine Auswirkungen.

Im Bereich der Cyber-Sicherheit arbeitet die Schweiz mit den EWR-Mitgliedstaaten zusammen. Durch die Einrichtung des CSIRT und der zentralen Anlaufstelle (SPOC)

werden in Liechtenstein die Strukturen im Bereich der Cyber-Sicherheit geschaffen, die in der Schweiz unter anderem mit dem Nationalen Zentrum für Cybersicherheit (National Cyber Security Centre; NCSC) bereits seit Jahren bestehen.

Neben der Teilnahme an den einschlägigen EWR-Gremien ist eine enge Zusammenarbeit im Bereich der Cyber-Sicherheit sowohl auf strategischer wie auch auf operativer Ebene mit der Schweiz geplant.

Die Regierung ist gemeinsam mit der EWR/Schengen-Kommission des Landtages zur Auffassung gelangt, dass die Beschlüsse Nr. 21/2023, 22/2023 und 27/2023 des Gemeinsamen EWR-Ausschusses vom 3. Februar 2023 betreffend die Übernahme der Richtlinie (EU) 2016/1148 sowie der Verordnungen (EU) 2019/881 und 2021/887 in das EWR-Abkommen dem Hohen Landtag gemäss Art. 8 Abs. 2 der Landesverfassung zur Zustimmung vorzulegen ist.

Weiters wirft die Vorlage keine verfassungsmässigen Fragen auf.

6. AUSWIRKUNGEN AUF VERWALTUNGSTÄTIGKEIT UND RESSOURCENEINSATZ

6.1 Neue und veränderte Kernaufgaben

Die Übernahme und Umsetzung bzw. Durchführung der Richtlinie (EU) 2016/1148 sowie der Verordnungen (EU) 2019/881 und 2021/887 bedingen den Aufbau nationaler Kapazitäten für Cybersicherheit sowie eine stärkere Zusammenarbeit der EWR-Mitgliedstaaten.

Daher wird eine nationale Behörde als zentrale Anlaufstelle und Verbindungsstelle zur Gewährleistung der grenzüberschreitenden Zusammenarbeit mit

internationalen Gruppen und Gremien eingerichtet. Mit dieser Funktion wird die Stabsstelle Cyber-Sicherheit (SCS) betraut.

Zudem wird ein nationales Koordinierungszentrum Cybersicherheit geschaffen, welches als Teil des Netzwerks nationaler Koordinierungszentren im EWR zusammen mit dem Europäischen Kompetenzzentrum für Cybersicherheit (ECCC) den neuen europäischen institutionellen Rahmen zur Unterstützung der Innovations- und Industriepolitik im Bereich der Cybersicherheit bildet.

6.2 Personelle, finanzielle, organisatorische und räumliche Auswirkungen

Die personellen und finanziellen Anforderungen können vorerst mit den vorhandenen Personen und Mitteln bewältigt werden.

6.3 Betroffene UNO-Nachhaltigkeitsziele und Auswirkungen auf deren Umsetzung (SDGs)

Betroffen von der Übernahme und Umsetzung bzw. Durchführung der Richtlinie (EU) 2016/1148 sowie der Verordnungen (EU) 2019/881 und 2021/887 sind insbesondere die folgenden UNO-Nachhaltigkeitsziele (SDGs):

Betroffenes Ziel	**Relevante Unterziele**	**Zu erwartende Auswirkungen durch die Regierungsvorlage**
SDG 5 Geschlechtergleichheit	5.b, 5.1, 5.5	Funktionierende und cybersichere Netz- und Informationssysteme spielen eine zentrale Rolle für das Funktionieren des staatlichen Gemeinwesens. Die Sicherstellung ihrer Verlässlichkeit und Sicherheit ist auch wesentlicher Baustein für die Nutzung von

		Grundlagentechnologien, insbesondere der Informations- und Kommunikationstechnologien, um die Selbstbestimmung der Frauen zu fördern. Auch bei der Erstellung der nationalen Strategie von Netz- und Informationssystemen wird der Gender Dimension Rechnung getragen: Zum einen durch die Zusammensetzung der Personen/Arbeitsgruppe, die mit der Erarbeitung der Strategie betraut werden, und zum anderen dadurch, dass diese Dimension bei der inhaltlichen Erarbeitung der Strategie berücksichtigt wird. Ebenso wird das Thema bei der Sensibilisierung gem. Art. 13 Abs. 1 Bst. h entsprechend berücksichtigt. Zudem soll durch ein Angebot von Ausbildung und Training die volle und wirksame Teilhabe von Frauen und ihre Chancengleichheit bei der Übernahme von Führungsrollen auf allen Ebenen der Entscheidungsfindung sichergestellt werden.
SDG 6 Sauberes Wasser und Sanitäreinrichtungen	6.3, 6.4, 6.5, 6.6	Wasserbewirtschaftung zählt zur kritischen Infrastruktur und ist besonders zu schützen. Durch externe Einflüsse,

		insbesondere Sicherheitsvorfälle kann diese gefährdet werden. Die vorgesehenen Massnahmen dienen auch dem Schutz der angeführten Ziele.
SDG 8 Menschenwürdige Arbeit und Wirtschaftswachstum	8.2, 8.3, 8.10	Durch hohe Cyber-Standards technologische Modernisierung und Innovation erreichen, die gleichzeitig notwendiger Schutz zum Wachstum von Kleinst-, Klein- und Mittelunternehmen sind. Darüber hinaus werden die Kapazitäten der nationalen Finanzinstitutionen gestärkt und geschützt.
SDG 9 Industrie, Innovation und Infrastruktur	9.1, 9.4	Zu einer hochwertigen, verlässlichen, nachhaltigen und widerstandsfähigen Infrastruktur verpflichten, Infrastrukturen modernisieren um sie cybersicher und damit nachhaltig zu machen. Anreize setzen für Marktteilnehmer, die Infrastruktur zu modernisieren, um sie nachhaltig zu machen, mit effizienterem Ressourceneinsatz.
SDG 16 Frieden, Gerechtigkeit und starke Institutionen	16.3, 16.6, 16.10, 16.a	Sichere Netz- und Informationssysteme spielen eine zentrale Rolle für das Funktionieren des staatlichen Gemeinwesens. Dies betrifft auch den Schutz der Rechtsstaatlichkeit, Sicherung

		leistungsfähiger Institutionen, Schutz der Grundfreiheiten, insbesondere durch Schutz des öffentlichen Zugangs zu Informationen. Die internationale Zusammenarbeit ist insbesondere im Bereich der Cyberkriminalität essentiell, da diese selten auf einen Staat beschränkt ist.

Die Regierung geht davon aus, dass sich die Umsetzung des Vorhabens insgesamt auf 16 SDGs positiv auswirken wird. Gleichzeitig wird nicht mit negativen Auswirkungen auf die SDGs gerechnet.

6.4 Evaluation

Es ist keine Frist für eine Evaluation vorgesehen.

II. ANTRAG DER REGIERUNG

Aufgrund der vorstehenden Ausführungen unterbreitet die Regierung dem Landtag den

A n t r a g ,

der Hohe Landtag wolle den Beschlüssen Nr. 21/2023, 22/2023 und 27/2023 des Gemeinsamen EWR-Ausschusses zur Übernahme der Richtlinie (EU) 2016/1148 sowie der Verordnungen (EU) 2019/881 und 2021/887 in das EWR-Abkommen die Zustimmung erteilen.

Genehmigen Sie, sehr geehrter Herr Landtagspräsident, sehr geehrte Frauen und Herren Abgeordnete, den Ausdruck der vorzüglichen Hochachtung.

REGIERUNG DES
FÜRSTENTUMS LIECHTENSTEIN

gez. Dr. Daniel Risch

Liechtensteinisches Landesgesetzblatt

Jahrgang 2023 Nr. .. ausgegeben am ...

Kundmachung

vom ... 2023

des Beschlusses Nr. 21/2023 des Gemeinsamen EWR-Ausschusses

Beschluss des Gemeinsamen EWR-Ausschusses: 3. Februar 2023
Zustimmung des Landtags: ... [1]
Inkrafttreten für das Fürstentum Liechtenstein: ...

Aufgrund von Art. 3 Bst. k des Kundmachungsgesetzes vom 17. April 1985, LGBl. 1985 Nr. 41, in der Fassung des Gesetzes vom 22. März 1995, LGBl. 1995 Nr. 101, macht die Regierung im Anhang den Beschluss Nr. 21/2023 des Gemeinsamen EWR-Ausschusses kund.

Fürstliche Regierung:
gez. *Dr. Daniel Risch*
Fürstlicher Regierungschef

[1] Bericht und Antrag der Regierung Nr. 36/2023.

Anhang

Beschluss des Gemeinsamen EWR-Ausschusses Nr. 21/2023

vom 3. Februar 2023

zur Änderung des Anhangs XI (Elektronische Kommunikation, audiovisuelle Dienste und Informationsgesellschaft) und des Protokolls 37 (mit der Liste gemäss Art. 101) des EWR-Abkommens

Der Gemeinsame EWR-Ausschuss –

gestützt auf das Abkommen über den Europäischen Wirtschaftsraum (im Folgenden "EWR-Abkommen"), insbesondere auf Art. 98,

in Erwägung nachstehender Gründe:

1. Die Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Massnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union[2] ist in das EWR-Abkommen aufzunehmen.
2. Die Durchführungsverordnung (EU) 2018/151 der Kommission vom 30. Januar 2018 über Vorschriften für die Anwendung der Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates hinsichtlich der weiteren Festlegung der von Anbietern digitaler Dienste beim Risikomanagement in Bezug auf die Sicherheit von Netz- und Informationssystemen zu berücksichtigenden Elemente und der Parameter für die Feststellung erheblicher Auswirkungen eines Sicherheitsvorfalls[3] ist in das EWR-Abkommen aufzunehmen.
3. Damit das Abkommen reibungslos funktioniert, ist Protokoll 37 zum EWR-Abkommen auf die mit der Richtlinie (EU) 2016/1148 eingerichtete Kooperationsgruppe auszudehnen.

---

[2] ABl. L 194 vom 19.7.2016, S. 1.
[3] ABl. L 26 vom 31.1.2018, S. 48.

4. Anhang XI und Protokoll 37 zum EWR-Abkommen sollten daher entsprechend geändert werden -

hat folgenden Beschluss erlassen:

Art. 1

In Anhang XI des EWR-Abkommens wird nach Nummer 5cp (Verordnung (EU) Nr. 526/2013 des Europäischen Parlaments und des Rates) Folgendes eingefügt:

"5cpa. **32016 L 1148**: Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Massnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union (ABl. L 194 vom 19.7.2016, S. 1).

Modalitäten für die Beteiligung der EFTA-Staaten gemäss Art. 101 des Abkommens:

Die EFTA-Staaten beteiligen sich in vollem Umfang an der Kooperationsgruppe und verfügen dort mit Ausnahme des Stimmrechts über dieselben Rechte und Pflichten wie EU-Mitgliedstaaten."

5cpaa. **32018 R 0151**: Durchführungsverordnung (EU) 2018/151 der Kommission vom 30. Januar 2018 über Vorschriften für die Anwendung der Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates hinsichtlich der weiteren Festlegung der von Anbietern digitaler Dienste beim Risikomanagement in Bezug auf die Sicherheit von Netz- und Informationssystemen zu berücksichtigenden Elemente und der Parameter für die Feststellung erheblicher Auswirkungen eines Sicherheitsvorfalls (ABl. L 26 vom 31.1.2018, S. 48)."

Art. 2

In Protokoll 37 zum EWR-Abkommen wird folgende Nummer angefügt:

"47. Die Kooperationsgruppe (Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Massnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union)."

Art. 3

Der Wortlaut der Richtlinie (EU) 2016/1148 und der Durchführungsverordnung (EU) 2018/151 in isländischer und norwegischer Sprache, der in der EWR-Beilage des Amtsblatts der Europäischen Union veröffentlicht wird, ist verbindlich.

Art. 4

Dieser Beschluss tritt am 4. Februar 2023 in Kraft, sofern alle Mitteilungen nach Art. 103 Abs. 1 des EWR-Abkommens vorliegen.[4]

Art. 5

Dieser Beschluss wird im EWR-Abschnitt und in der EWR-Beilage des Amtsblattes der Europäischen Union veröffentlicht.

Geschehen zu Brüssel am 3. Februar 2023.

(*Es folgen die Unterschriften*)

[4] Das Bestehen verfassungsrechtlicher Anforderungen wurde mitgeteilt.

Liechtensteinisches Landesgesetzblatt

Jahrgang 2023 Nr. .. ausgegeben am ...

Kundmachung

vom ... 2023

des Beschlusses Nr. 22/2023 des Gemeinsamen EWR-Ausschusses

Beschluss des Gemeinsamen EWR-Ausschusses: 3. Februar 2023
Zustimmung des Landtags: ... [1]
Inkrafttreten für das Fürstentum Liechtenstein: ...

Aufgrund von Art. 3 Bst. k des Kundmachungsgesetzes vom 17. April 1985, LGBl. 1985 Nr. 41, in der Fassung des Gesetzes vom 22. März 1995, LGBl. 1995 Nr. 101, macht die Regierung im Anhang den Beschluss Nr. 22/2023 des Gemeinsamen EWR-Ausschusses kund.

Fürstliche Regierung:
gez. *Dr. Daniel Risch*
Fürstlicher Regierungschef

[1] Bericht und Antrag der Regierung Nr. 36/2023.

Anhang

Beschluss des Gemeinsamen EWR-Ausschusses Nr. 22/2023

vom 3. Februar 2023

zur Änderung des Anhangs XI (Elektronische Kommunikation, audiovisuelle Dienste und Informationsgesellschaft) und des Protokolls 37 (mit der Liste gemäss Art. 101) des EWR-Abkommens

Der Gemeinsame EWR-Ausschuss –

gestützt auf das Abkommen über den Europäischen Wirtschaftsraum (im Folgenden "EWR-Abkommen"), insbesondere auf Art. 98,

in Erwägung nachstehender Gründe:

1. Die Verordnung (EU) 2019/881 des Europäischen Parlaments und des Rates vom 17. April 2019 über die ENISA (Agentur der Europäischen Union für Cybersicherheit) und über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik und zur Aufhebung der Verordnung (EU) Nr. 526/2013 (Rechtsakt zur Cybersicherheit)[2] ist in das EWR-Abkommen aufzunehmen.
2. Mit der Verordnung (EU) 2019/881 wird die Verordnung (EU) Nr. 526/2013 des Europäischen Parlaments und des Rates[3] aufgehoben, die in das EWR-Abkommen aufgenommen wurde und daher aus diesem zu streichen ist.
3. Anhang XI und Protokoll 37 zum EWR-Abkommen sollten daher entsprechend geändert werden -

hat folgenden Beschluss erlassen:

---

[2] ABl. L 151 vom 7.6.2019, S. 15.
[3] ABl. L 165 vom 18.6.2013, S. 41.

Art. 1

In Anhang XI des EWR-Abkommens erhält der Text von Nummer 5cp (Verordnung (EU) Nr. 526/2013 des Europäischen Parlaments und des Rates) folgende Fassung:

"**32019 R 0881**: Verordnung (EU) 2019/881 des Europäischen Parlaments und des Rates vom 17. April 2019 über die ENISA (Agentur der Europäischen Union für Cybersicherheit) und über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik und zur Aufhebung der Verordnung (EU) Nr. 526/2013 (Rechtsakt zur Cybersicherheit) (ABl. L 151 vom 7.6.2019, S. 15).

Der Wortlaut der Verordnung ist für die Zwecke dieses Abkommens mit folgenden Anpassungen zu verstehen:

(a) Ungeachtet der Bestimmungen von Protokoll 1 zum Abkommen bezeichnen in der Verordnung der Ausdruck "Mitgliedstaat(en)" und sonstige Ausdrücke, die sich auf deren in der Verordnung genannte Behörden beziehen, neben ihrer Bedeutung in der Verordnung auch die EFTA-Staaten und deren Behörden, sofern unten nichts anderes bestimmt ist.

(b) Hinsichtlich der EFTA-Staaten unterstützt die Agentur gegebenenfalls die EFTA-Überwachungsbehörde bzw. den Ständigen Ausschuss bei der Erfüllung ihrer jeweiligen Aufgaben.

(c) Hinsichtlich der EFTA-Staaten sind Bezugnahmen auf das Unionsrecht als Bezugnahmen auf das EWR-Abkommen zu verstehen.

(d) In Art. 14 wird folgender Absatz angefügt:

"5. Die EFTA-Staaten beteiligen sich in vollem Umfang am Verwaltungsrat und verfügen dort mit Ausnahme des Stimmrechts über dieselben Rechte und Pflichten wie EU-Mitgliedstaaten."

(e) In Art. 28 wird folgender Absatz angefügt:

"4. Die Verordnung (EG) Nr. 1049/2001 gilt für die Zwecke der Anwendung dieser Verordnung auch für Dokumente der Agentur, die die EFTA-Staaten betreffen."

(f) In Art. 30 wird folgender Absatz angefügt:

"3. Die EFTA-Staaten beteiligen sich an dem in Abs. 1 Bst. a genannten Beitrag der Union. Für diesen Zweck gelten die Verfahren des Art. 82 Abs. 1 Bst. a des EWR-Abkommens und des Protokolls 32 zum Abkommen sinngemäss."

(g) In Art. 34 wird folgender Absatz angefügt:

"Abweichend von Art. 12 Abs. 2 Bst. a und Art. 82 Abs. 3 Bst. a der Beschäftigungsbedingungen für die sonstigen Bediensteten können

Staatsangehörige der EFTA-Staaten, die die bürgerlichen Ehrenrechte uneingeschränkt besitzen, vom Exekutivdirektor der Agentur auf Vertragsbasis eingestellt werden."

(h) In Art. 35 wird folgender Absatz angefügt:

"Die EFTA-Staaten räumen der Agentur und ihrem Personal Vorrechte und Befreiungen ein, die den im Protokoll über die Vorrechte und Befreiungen der Europäischen Union aufgeführten entsprechen."

(i) In Art. 40 wird folgender Absatz angefügt:

"3. Abweichend von Art. 12 Abs. 2 Bst. e, Art. 82 Abs. 3 Bst. e und Art. 85 Abs. 3 der Beschäftigungsbedingungen für die sonstigen Bediensteten der Europäischen Union betrachtet die Agentur im Hinblick auf das eigene Personal die Sprachen nach Art. 129 Abs. 1 des EWR-Abkommens als Sprachen der Union nach Art. 55 Abs. 1 des Vertrags über die Europäische Union."

(j) In Art. 62 wird folgender Absatz angefügt:

"6. Die EFTA-Staaten geniessen volle Mitwirkungsrechte in der Europäischen Gruppe für die Cybersicherheitszertifizierung, mit Ausnahme des Stimmrechts.""

Art. 2

In Protokoll 37 zum EWR-Abkommen wird folgende Nummer angefügt:

"48. Europäische Gruppe für die Cybersicherheitszertifizierung (Verordnung (EU) 2019/881 des Europäischen Parlaments und des Rates)."

Art. 3

Der Wortlaut der Verordnung (EU) 2019/881 in isländischer und in norwegischer Sprache, der in der EWR-Beilage des Amtsblatts der Europäischen Union veröffentlicht wird, ist verbindlich.

Art. 4

Dieser Beschluss tritt am 4. Februar 2023 in Kraft, sofern alle Mitteilungen nach Art. 103 Abs. 1 des EWR-Abkommens vorliegen[4], oder am Tag des Inkrafttretens des Beschlusses des Gemeinsamen EWR-Ausschusses Nr. 21/2023 vom 3. Februar 2023, je nachdem, welcher Zeitpunkt der spätere ist.

Art. 5

Dieser Beschluss wird im EWR-Abschnitt und in der EWR-Beilage des Amtsblattes der Europäischen Union veröffentlicht.

Geschehen zu Brüssel am 3. Februar 2023.

(*Es folgen die Unterschriften*)

[4] Das Bestehen verfassungsrechtlicher Anforderungen wurde mitgeteilt.

Gemeinsame Erklärung der Vertragsparteien zum Beschluss Nr. 22/2023 zur Aufnahme der Verordnung (EG) Nr. 2019/881 des Europäischen Parlaments und des Rates in das Abkommen

Die Vertragsparteien erkennen an, dass die Aufnahme dieses Aktes die unmittelbare Anwendung des Protokolls Nr. 7[5] über die Vorrechte und Befreiungen der Europäischen Union auf Staatsangehörige der EFTA-Staaten im Hoheitsgebiet jedes Mitgliedstaats der Europäischen Union gemäss Art. 11 dieses Protokolls unberührt lässt.

[5] ABl. C 326 vom 26.10.2012, S. 266.

Liechtensteinisches Landesgesetzblatt

Jahrgang 2023 Nr. .. ausgegeben am ...

Kundmachung

vom ... 2023

des Beschlusses Nr. 27/2023 des Gemeinsamen EWR-Ausschusses

Beschluss des Gemeinsamen EWR-Ausschusses: 3. Februar 2023
Zustimmung des Landtags: ... [1]
Inkrafttreten für das Fürstentum Liechtenstein: ...

Aufgrund von Art. 3 Bst. k des Kundmachungsgesetzes vom 17. April 1985, LGBl. 1985 Nr. 41, in der Fassung des Gesetzes vom 22. März 1995, LGBl. 1995 Nr. 101, macht die Regierung im Anhang den Beschluss Nr. 27/2023 des Gemeinsamen EWR-Ausschusses kund.

Fürstliche Regierung:
gez. *Dr. Daniel Risch*
Fürstlicher Regierungschef

[1] Bericht und Antrag der Regierung Nr. 36/2023.

Anhang

Beschluss des Gemeinsamen EWR-Ausschusses Nr. 27/2023

vom 3. Februar 2023

zur Änderung des Protokolls 31 zum EWR-Abkommen über die Zusammenarbeit in bestimmten Bereichen ausserhalb der vier Freiheiten

Der Gemeinsame EWR-Ausschuss –

gestützt auf das Abkommen über den Europäischen Wirtschaftsraum (im Folgenden "EWR-Abkommen"), insbesondere auf die Art. 86 und Art. 98,

in Erwägung nachstehender Gründe:

1. Die Zusammenarbeit der Vertragsparteien des EWR-Abkommens sollte auf die Verordnung (EU) 2021/887 des Europäischen Parlaments und des Rates vom 20. Mai 2021 zur Einrichtung des Europäischen Kompetenzzentrums für Industrie, Technologie und Forschung im Bereich der Cybersicherheit und des Netzwerks nationaler Koordinierungszentren[2] ausgeweitet werden.
2. Protokoll 31 zum EWR-Abkommen sollte daher geändert werden, um diese erweiterte Zusammenarbeit ab dem 1. Januar 2023 zu ermöglichen -

hat folgenden Beschluss erlassen:

Art. 1

In Art. 2 des Protokolls 31 zum EWR-Abkommen wird nach Nummer 7 (Transeuropäische Telekommunikationsnetze) folgende Nummer eingefügt:

"8. (a) Die EFTA-Staaten beteiligen sich ab dem 1. Januar 2023 an den Massnahmen, denen folgender Rechtsakt zugrunde liegt:

---

[2] ABl. L 202 vom 8.6.2021, S. 1.

- **32021 R 0887**: Verordnung (EU) 2021/887 des Europäischen Parlaments und des Rates vom 20. Mai 2021 zur Einrichtung des Europäischen Kompetenzzentrums für Industrie, Technologie und Forschung im Bereich der Cybersicherheit und des Netzwerks nationaler Koordinierungszentren (ABl. L 202 vom 8.6.2021, S. 1).

(b) Die EFTA-Staaten beteiligen sich uneingeschränkt an den Arbeiten des Verwaltungsrates und haben innerhalb des Verwaltungsrates die gleichen Rechte und Pflichten wie die EU-Mitgliedstaaten mit Ausnahme des Stimmrechts.

(c) Staatsangehörige der EFTA-Staaten kommen als Mitglieder der strategischen Beratungsgruppe in Betracht.

(d) Abweichend von Art. 12 Abs. 2 Bst. a und Art. 82 Abs. 3 Bst. a der Beschäftigungsbedingungen für die sonstigen Bediensteten der Europäischen Union können Staatsangehörige der EFTA-Staaten, die im Besitz ihrer vollen staatsbürgerlichen Rechte sind, vom Exekutivdirektor des Kompetenzzentrums auf Vertragsbasis eingestellt werden.

(e) Abweichend von Art. 12 Abs. 2 Bst. e, Art. 82 Abs. 3 Bst. e und Art. 85 Abs. 3 der Beschäftigungsbedingungen für die sonstigen Bediensteten der Europäischen Union betrachtet das Kompetenzzentrum im Hinblick auf das eigene Personal die Sprachen nach Art. 129 Abs. 1 des Abkommens als Sprachen der Union nach Art. 55 Abs. 1 des Vertrags über die Europäische Union.

(f) Die EFTA-Staaten räumen dem Kompetenzzentrum und ihrem Personal Vorrechte und Befreiungen ein, die den im Protokoll über die Vorrechte und Befreiungen der Europäischen Union aufgeführten entsprechen.

(g) Die 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 gilt für die Zwecke der Anwendung der Verordnung (EU) 2021/696 für Dokumente des Kompetenzzentrums, die auch EFTA-Staaten betreffen.

(h) Gemäss Art. 79 Abs. 3 des Abkommens gilt Teil VII (Institutionelle Bestimmungen) des Abkommens für diesen Absatz."

Art. 2

Dieser Beschluss tritt am Tag nach Eingang der letzten Mitteilung gemäss Art. 103 Abs. 1 des EWR-Abkommens[3] in Kraft.

Er gilt ab dem 1. Januar 2023.

Art. 3

Dieser Beschluss wird im EWR-Abschnitt und in der EWR-Beilage des Amtsblattes der Europäischen Union veröffentlicht.

Geschehen zu Brüssel am 3. Februar 2023.

(*Es folgen die Unterschriften*)

[3] Das Bestehen verfassungsrechtlicher Anforderungen wurde mitgeteilt.

Gemeinsame Erklärung der Vertragsparteien zum Beschluss Nr. 27/2023 zur Aufnahme der Verordnung (EG) Nr. 2021/887 des Europäischen Parlaments und des Rates in das EWR-Abkommen

Die Vertragsparteien erkennen an, dass die Aufnahme dieses Aktes die unmittelbare Anwendung des Protokolls Nr. 7[4] über die Vorrechte und Befreiungen der Europäischen Union auf Staatsangehörige der EFTA-Staaten im Hoheitsgebiet jedes Mitgliedstaats der Europäischen Union gemäss Art. 11 dieses Protokolls unberührt lässt.

[4] ABl. C 326 vom 26.10.2012, S. 266.

I

(Gesetzgebungsakte)

RICHTLINIEN

RICHTLINIE (EU) 2016/1148 DES EUROPÄISCHEN PARLAMENTS UND DES RATES

vom 6. Juli 2016

über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union

DAS EUROPÄISCHE PARLAMENT UND DER RAT DER EUROPÄISCHEN UNION —

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

auf Vorschlag der Europäischen Kommission,

nach Zuleitung des Entwurfs des Gesetzgebungsakts an die nationalen Parlamente,

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

gemäß dem ordentlichen Gesetzgebungsverfahren ([2]),

in Erwägung nachstehender Gründe:

(1) Netz- und Informationssysteme mit den zugehörigen Diensten spielen eine zentrale Rolle in der Gesellschaft. Für wirtschaftliche und gesellschaftliche Tätigkeiten und insbesondere für das Funktionieren des Binnenmarkts ist es von entscheidender Bedeutung, dass sie verlässlich und sicher sind.

(2) Die Tragweite, Häufigkeit und Auswirkungen von Sicherheitsvorfällen nehmen zu und stellen eine erhebliche Bedrohung für den störungsfreien Betrieb von Netz- und Informationssystemen dar. Diese Systeme können auch zu einem Angriffsziel vorsätzlich schädigender Handlungen werden, die auf die Störung oder den Ausfall des Betriebs der Systeme gerichtet sind. Solche Sicherheitsvorfälle können die Ausübung wirtschaftlicher Tätigkeiten beeinträchtigen, beträchtliche finanzielle Verluste verursachen, das Vertrauen der Nutzer untergraben und der Wirtschaft der Union großen Schaden zufügen.

(3) Netz- und Informationssysteme, allen voran das Internet, spielen eine tragende Rolle bei der Erleichterung des grenzüberschreitenden Waren-, Dienstleistungs- und Personenverkehrs. Aufgrund dieses transnationalen Charakters können schwere Störungen solcher Systeme — unabhängig davon, ob sie beabsichtigt oder unbeabsichtigt sind und wo sie auftreten — einzelne Mitgliedstaaten und die Union insgesamt in Mitleidenschaft ziehen. Sichere Netz- und Informationssysteme sind daher unerlässlich für das reibungslose Funktionieren des Binnenmarkts.

(4) Auf der Grundlage der beträchtlichen Fortschritte, die im Rahmen des Europäischen Forums der Mitgliedstaaten zur Förderung von Gesprächen und des Austauschs bewährter Vorgehensweisen, unter anderem zur Entwicklung von Grundsätzen für die europäische Zusammenarbeit bei Cyberkrisen, erzielt worden sind, sollte eine Kooperationsgruppe aus Vertretern der Mitgliedstaaten, der Kommission und der Agentur der Europäischen Union für Netz- und Informationssicherheit (ENISA) eingesetzt werden, um die strategische Zusammenarbeit

([1]) ABl. C 271vom 19.9.2013, S. 133.
([2]) Standpunkt des Europäischen Parlaments vom 13. März 2014 (noch nicht im Amtsblatt veröffentlicht)] und Standpunkt des Rates in erster Lesung vom 17. Mai 2016 (noch nicht im Amtsblatt veröffentlicht). Standpunkt des Europäischen Parlaments vom 6. Juli 2016 (noch nicht im Amtsblatt veröffentlicht).

zwischen den Mitgliedstaaten im Bereich der Sicherheit von Netz- und Informationssystemen zu unterstützen und zu erleichtern. Damit eine solche Gruppe wirksam sein kann und alle Beteiligten einbezogen werden, muss jeder Mitgliedstaat über Minimalfähigkeiten und eine Strategie verfügen, die in seinem Hoheitsgebiet ein hohes Sicherheitsniveau von Netz- und Informationssystemen gewährleisten. Außerdem sollten für Betreiber wesentlicher Dienste und Anbieter digitaler Dienste Sicherheitsanforderungen und Meldepflichten gelten, damit eine Kultur des Risikomanagements gefördert wird und sichergestellt ist, dass die gravierendsten Sicherheitsvorfälle gemeldet werden.

(5) Die bestehenden Fähigkeiten reichen nicht aus, um ein hohes Sicherheitsniveau von Netz- und Informationssystemen in der Union zu gewährleisten. Aufgrund des sehr unterschiedlichen Niveaus der Abwehrbereitschaft verfolgen die Mitgliedstaaten uneinheitliche Ansätze innerhalb der Union. Dies führt dazu, dass Verbraucher und Unternehmen ein unterschiedliches Schutzniveau genießen und die Sicherheit von Netz- und Informationssystemen in der Union generell untergraben wird. Wegen fehlender gemeinsamer Anforderungen für Betreiber wesentlicher Dienste und Anbieter digitaler Dienste kann wiederum kein umfassender, wirksamer Mechanismus für die Zusammenarbeit auf Unionsebene geschaffen werden. Universitäten und Forschungszentren müssen eine entscheidende Rolle spielen, wenn es darum geht, Forschung, Entwicklung und Innovationen in diesen Bereichen voranzutreiben.

(6) Um wirksam auf die Herausforderungen im Bereich der Sicherheit von Netz- und Informationssystemen reagieren zu können, ist deshalb ein umfassender Ansatz auf Unionsebene erforderlich, der gemeinsame Mindestanforderungen für Kapazitätsaufbau und -planung, Informationsaustausch, Zusammenarbeit sowie gemeinsame Sicherheitsanforderungen für Betreiber wesentlicher Dienste und Anbieter digitaler Dienste beinhaltet. Jedoch sind Betreiber wesentlicher Dienste und Anbieter digitaler Dienste nicht daran gehindert, strengere Sicherheitsmaßnahmen anzuwenden, als sie in dieser Richtlinie vorgesehen sind.

(7) Um alle einschlägigen Vorfälle und Risiken abdecken zu können, sollte diese Richtlinie sowohl für Betreiber wesentlicher Dienste als auch für Anbieter digitaler Dienste gelten. Die den Betreibern wesentlicher Dienste und den Anbietern digitaler Dienste auferlegten Verpflichtungen sollten hingegen nicht für Unternehmen gelten, die öffentliche Kommunikationsnetze oder öffentlich zugängliche elektronische Kommunikationsdienste im Sinne der Richtlinie 2002/21/EG des Europäischen Parlaments und des Rates ([1]) bereitstellen und die den besonderen Sicherheits- und Integritätsanforderungen jener Richtlinie unterliegen; die Verpflichtungen sollten auch nicht für Vertrauensdiensteanbieter im Sinne der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates ([2]) gelten, die den Sicherheitsanforderungen jener Verordnung unterliegen.

(8) Die Möglichkeit der Mitgliedstaaten, die für die Wahrung seiner wesentlichen Sicherheitsinteressen und den Schutz der öffentlichen Ordnung und der öffentlichen Sicherheit erforderlichen Maßnahmen zu ergreifen und die Ermittlung, Feststellung und Verfolgung von Straftaten zuzulassen, sollte von dieser Richtlinie unberührt bleiben. Nach Artikel 346 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV) ist kein Mitgliedstaat verpflichtet, Auskünfte zu erteilen, deren Preisgabe seines Erachtens seinen wesentlichen Sicherheitsinteressen widerspricht. In diesem Zusammenhang sind der Beschluss 2013/488/EU des Rates ([3]) sowie Geheimhaltungsvereinbarungen oder informelle Geheimhaltungsvereinbarungen wie das sogenannte Traffic Light Protocol (TLP) von Bedeutung.

(9) Für bestimmte Wirtschaftssektoren gelten bereits sektorspezifische Rechtsakte der Union, die Vorschriften im Zusammenhang mit der Sicherheit von Netz- und Informationssystemen beinhalten; für weitere Wirtschaftssektoren kann dies künftig der Fall sein. Wann immer solche Unionsrechtsakte Bestimmungen enthalten, mit denen Anforderungen in Bezug auf die Sicherheit von Netz- und Informationssystemen oder die Meldung von Sicherheitsvorfällen auferlegt werden, sollten diese Bestimmungen gelten, wenn sie Anforderungen vorsehen, die hinsichtlich ihrer Wirkung den in dieser Richtlinie enthaltenen Verpflichtungen mindestens gleichwertig sind. Die Mitgliedstaaten sollten dann die Bestimmungen des betreffenden sektorspezifischen Unionsrechtsakts anwenden, einschließlich der Bestimmungen über die gerichtliche Zuständigkeit, und nicht das in dieser Richtlinie festgelegte Verfahren zur Ermittlung der Betreiber wesentlicher Dienste durchführen. In diesem Zusammenhang sollten die Mitgliedstaaten die Kommission über die Anwendung solcher Lex-specialis-Bestimmungen unterrichten. Bei der Feststellung, ob die in sektorspezifischen Unionsrechtsakten enthaltenen Anforderungen in Bezug auf die Sicherheit von Netz- und Informationssystemen und die Meldung von Sicherheitsvorfällen den in dieser Richtlinie enthaltenen Anforderungen gleichwertig sind, sollten ausschließlich die Bestimmungen der einschlägigen Unionsrechtsakte und ihre Anwendung in den Mitgliedstaaten berücksichtigt werden.

(10) Im Bereich der Schifffahrt umfassen die Sicherheitsanforderungen für Unternehmen, Schiffe, Hafeneinrichtungen, Häfen und Schiffsverkehrsdienste nach Rechtsakten der Union sämtliche Tätigkeiten einschließlich der Funk- und Telekommunikationssysteme, Computersysteme und Netze. Ein Teil der verbindlichen Verfahren beinhaltet das Melden sämtlicher Vorfälle und sollte daher insoweit als Lex specialis betrachtet werden, als diese Anforderungen den entsprechenden Bestimmungen dieser Richtlinie mindestens gleichwertig sind.

([1]) Richtlinie 2002/21/EG des Europäischen Parlaments und des Rates vom 7. März 2002 über einen gemeinsamen Rechtsrahmen für elektronische Kommunikationsnetze und -dienste (Rahmenrichtlinie) (ABl. L 108 vom 24.4.2002, S. 33).

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

([3]) Beschluss 2013/488/EU des Rates vom 23. September 2013 über die Sicherheitsvorschriften für den Schutz von EU-Verschlusssachen (ABl. L 274 vom 15.10.2013, S. 1).

(11) Bei der Ermittlung von Betreibern im Schifffahrtsektor sollten die Mitgliedstaaten den geltenden und künftigen internationalen Codes und Leitlinien Rechnung tragen, insbesondere den von der Internationalen Seeschifffahrtsorganisation ausgearbeiteten, um einzelnen Betreibern gegenüber ein kohärentes Vorgehen zu gewährleisten.

(12) Die Regulierung und die Aufsicht in den Sektoren der Banken- und Finanzmarktinfrastrukturen sind auf Unionsebene durch die Verwendung des Primär- und Sekundärrechts der Union sowie der Normen, die gemeinsam mit den Europäischen Aufsichtsbehörden ausgearbeitet wurden, in hohem Maße harmonisiert. Innerhalb der Bankenunion werden die Anwendung und die Beaufsichtigung dieser Anforderungen durch den Einheitlichen Aufsichtsmechanismus sichergestellt. In Mitgliedstaaten, die nicht Teil der Bankenunion sind, gewährleisten dies die einschlägigen Bankenaufsichtsbehörden der Mitgliedstaaten. Darüber hinaus sorgt in anderen Bereichen der Regulierung des Finanzsektors das Europäische Finanzaufsichtssystem für ein hohes Maß an Gemeinsamkeit und Annäherung bei der Aufsichtspraxis. Die Europäische Wertpapier- und Marktaufsichtsbehörde übt außerdem die direkte Aufsicht über bestimmte Einrichtungen, d. h. über Kreditratingagenturen und Transaktionsregister aus.

(13) Das operationelle Risiko macht einen großen Teil der Aufsichtsvorschriften und der Kontrolle in den Sektoren Banken- und Finanzmarktinfrastrukturen aus. Davon erfasst sind sämtliche Tätigkeiten einschließlich der Sicherheit, Integrität und Robustheit von Netz- und Informationssystemen. Die Anforderungen für diese Systeme, die oft über die Anforderungen aus dieser Richtlinie hinausgehen, sind in einer Reihe von Unionsrechtsakten festgelegt; hierzu zählen unter anderem: Vorschriften über den Zugang zur Tätigkeit von Kreditinstituten und die Beaufsichtigung von Kreditinstituten und Wertpapierfirmen und Vorschriften über die Aufsichtsanforderungen an Kreditinstitute und Wertpapierfirmen, die Anforderungen zum operationellen Risiko enthalten, Vorschriften über Märkte für Finanzinstrumente, die Anforderungen zur Risikobewertung für Wertpapierfirmen und für geregelte Märkte enthalten, Vorschriften über OTC-Derivate, zentrale Gegenparteien und Transaktionsregister, die Anforderungen zum operationellen Risiko für zentrale Gegenparteien und Transaktionsregister enthalten, sowie Vorschriften zur Verbesserung der Wertpapierlieferungen und -abrechnungen in der Union und über Zentralverwahrer, die ebenfalls Anforderungen zum operationellen Risiko enthalten. Darüber hinaus sind Anforderungen in Bezug auf die Meldung von Sicherheitsvorfällen Teil der üblichen Aufsichtspraxis im Finanzsektor und sind oft in den Handbüchern über die Aufsicht enthalten. Die Mitgliedstaaten sollten bei ihrer Anwendung der Lex specialis diesen Regeln und Anforderungen Rechnung tragen.

(14) Wie die Europäische Zentralbank in ihrer Stellungnahme vom 25. Juli 2014 [1] festgestellt hat, berührt die Richtlinie nicht die bestehenden unionsrechtlichen Bestimmungen zur Überwachung von Zahlungsverkehrs- und Abwicklungssystemen durch das Eurosystem. Die für eine derartige Überwachung verantwortlichen Behörden sollten ihre Erfahrungen in Angelegenheiten der Sicherheit von Netz- und Informationssystemen mit den nach dieser Richtlinie zuständigen Behörden austauschen. Gleiches gilt für die Mitgliedstaaten, die zwar nicht Mitglied des Euroraums, wohl aber des Europäischen Systems der Zentralbanken sind, und die eine Überwachung der Zahlungsverkehrs- und Abwicklungssysteme auf der Grundlage nationaler Gesetze und Vorschriften vornehmen.

(15) Ein Online-Marktplatz ermöglicht es Verbrauchern und Unternehmern, Online-Kaufverträge oder Online-Dienstleistungsverträge mit Unternehmern abzuschließen, und ist der endgültige Bestimmungsort für den Abschluss dieser Verträge. Er sollte sich nicht auf Online-Dienste erstrecken, die lediglich als Vermittler für Drittdienste fungieren, durch die letztlich ein Vertrag geschlossen werden kann. Er sollte sich deshalb nicht auf Online-Dienste erstrecken, die die Preise für bestimmte Produkte oder Dienste bei verschiedenen Unternehmern miteinander vergleichen und den Nutzer anschließend an den bevorzugten Unternehmer weiterleiten, damit er das Produkt dort kauft. Die von dem Online-Marktplatz bereitgestellten IT-Dienste können die Verarbeitung von Transaktionen, die Aggregation von Daten oder die Erstellung von Nutzerprofilen einschließen. Als Online Stores tätige Application Stores, die den digitalen Vertrieb von Anwendungen oder Software-Programmen von Dritten ermöglichen, sollten als eine Art Online-Marktplatz betrachtet werden.

(16) Eine Online-Suchmaschine ermöglicht es dem Nutzer, Suchen grundsätzlich auf allen Websites anhand einer Abfrage zu einem beliebigen Thema vorzunehmen. Sie kann alternativ dazu auf Websites in einer bestimmten Sprache beschränkt sein. Die Definition des Begriffs „Online-Suchmaschine" in dieser Richtlinie sollte sich nicht auf Suchfunktionen erstrecken, die auf den Inhalt einer bestimmten Website beschränkt sind, unabhängig davon, ob die Suchfunktion durch eine externe Suchmaschine bereitgestellt wird. Sie sollte sich auch nicht auf Online-Dienste erstrecken, die die Preise für bestimmte Produkte oder Dienste bei verschiedenen Unternehmern miteinander vergleichen und den Nutzer anschließend an den bevorzugten Unternehmer weiterleiten, damit er das Produkt dort kauft.

(17) Cloud-Computing-Dienste umfassen eine breite Palette von Tätigkeiten, die auf unterschiedliche Weise erbracht werden können. Für die Zwecke dieser Richtlinie sind unter dem Begriff „Cloud-Computing-Dienste" Dienste zu verstehen, die den Zugang zu einem skalierbaren und elastischen Pool gemeinsam nutzbarer Rechenressourcen ermöglichen. Zu diesen Rechenressourcen zählen Ressourcen wie Netze, Server oder sonstige Infrastruktur, Speicher, Anwendungen und Dienste. Der Begriff „skalierbar" bezeichnet Rechenressourcen, die unabhängig von ihrem geografischen Standort vom Anbieter des Cloud-Dienstes flexibel zugeteilt werden, damit Nachfrageschwankungen bewältigt werden können. Der Begriff „elastischer Pool" wird verwendet, um die Rechenressourcen zu beschreiben, die entsprechend der Nachfrage bereitgestellt und freigegeben werden, damit die verfügbaren

[1] ABl. C 352 vom 7.10.2014, S. 4.

Ressourcen je nach Arbeitsaufkommen rasch auf- bzw. abgebaut werden können. Der Begriff „gemeinsam nutzbar" wird verwendet, um die Rechenressourcen zu beschreiben, die einer Vielzahl von Nutzern bereitgestellt werden, die über einen gemeinsamen Zugang auf den Dienst zugreifen, wobei jedoch die Verarbeitung für jeden Nutzer separat erfolgt, obwohl der Dienst von derselben elektronischen Einrichtung erbracht wird.

(18) Die Funktion eines Internet-Knotens (IXP) besteht in der Zusammenschaltung von Netzen. Ein IXP ermöglicht keinen Netzzugang und fungiert weder als Transit-Anbieter noch als Carrier. Ein IXP erbringt auch keine anderen Dienste, die in keinem Zusammenhang mit der Zusammenschaltung stehen, was einen IXP-Betreiber jedoch nicht daran hindert, Dienste anzubieten, bei denen dieser Zusammenhang nicht gegeben ist. Ein IXP dient zur Zusammenschaltung von Netzen, die technisch und organisatorisch getrennt sind. Der Begriff „autonomes System" wird verwendet, um ein in technischer Hinsicht eigenständiges Netz zu beschreiben.

(19) Die Mitgliedstaaten sollten dafür zuständig sein, zu ermitteln, welche Einrichtungen die Kriterien der Definition des Begriffs „Betreiber wesentlicher Dienste" erfüllen. Damit ein einheitlicher Ansatz gewährleistet ist, sollte die Definition des Begriffs „Betreiber wesentlicher Dienste" in allen Mitgliedstaaten kohärent angewendet werden. Hierzu sieht diese Richtlinie Folgendes vor: Bewertung der Einrichtungen, die in spezifischen Sektoren und Teilsektoren tätig sind; Festlegung einer Liste wesentlicher Dienste; Prüfung einer gemeinsamen Liste sektorübergreifender Faktoren, um zu bestimmen, ob ein potenzieller Sicherheitsvorfall eine erhebliche Störung bewirken würde; Konsultationsprozess unter Einbeziehung der betreffenden Mitgliedstaaten im Falle von Einrichtungen, die in mehr als einem Mitgliedstaat Dienste erbringen, sowie Unterstützung der Kooperationsgruppe im Rahmen des Verfahrens der Ermittlung. Damit dafür gesorgt ist, dass etwaige Marktveränderungen genau berücksichtigt werden, sollte die Liste der ermittelten Betreiber von den Mitgliedstaaten regelmäßig überprüft und bei Bedarf aktualisiert werden. Ferner sollten die Mitgliedstaaten der Kommission die Informationen vorlegen, die erforderlich sind, um zu bewerten, inwieweit diese gemeinsame Methodik eine einheitliche Anwendung der Begriffsbestimmung durch die Mitgliedstaaten ermöglicht hat.

(20) Während des Verfahrens zur Ermittlung von Betreibern wesentlicher Dienste sollten die Mitgliedstaaten zumindest für jeden in dieser Richtlinie genannten Teilsektor beurteilen, welche Dienste als für die Aufrechterhaltung kritischer gesellschaftlicher und wirtschaftlicher Tätigkeiten wesentlich zu betrachten sind, und beurteilen, ob die Einrichtungen, die in den Sektoren und Teilsektoren im Rahmen dieser Richtlinie aufgeführt sind und diese Dienste erbringen, die Kriterien zur Ermittlung der Betreiber erfüllen. Bei der Beurteilung, ob eine Einrichtung einen Dienst erbringt, der für die Aufrechterhaltung kritischer gesellschaftlicher oder wirtschaftlicher Tätigkeiten wesentlich ist, sollte ausreichen, dass geprüft wird, ob die betreffende Einrichtung einen Dienst erbringt, der in der Liste der wesentlichen Dienste aufgeführt ist. Außerdem sollte dargelegt werden, dass die Erbringung des wesentlichen Dienstes von Netz- und Informationssystemen abhängt. Ferner sollten die Mitgliedstaaten bei der Beurteilung, ob ein Sicherheitsvorfall erhebliche Störungen der Bereitstellung des Dienstes bewirken würde, eine Reihe von sektorübergreifenden Faktoren und gegebenenfalls auch sektorspezifische Faktoren berücksichtigen.

(21) Für die Zwecke der Ermittlung von Betreibern wesentlicher Dienste setzt eine Niederlassung in einem Mitgliedstaat die effektive und tatsächliche Ausübung einer Tätigkeit durch eine feste Einrichtung voraus. Die Rechtsform einer solchen Einrichtung, gleich, ob es sich um eine Zweigstelle oder eine Tochtergesellschaft mit eigener Rechtspersönlichkeit handelt, ist dabei unerheblich.

(22) Es ist möglich, dass Einrichtungen in den in dieser Richtlinie aufgeführten Sektoren und Teilsektoren sowohl wesentliche als auch nicht wesentliche Dienste erbringen. Beispielsweise erbringen im Luftverkehrssektor die Flughäfen Dienste, die von einem Mitgliedstaat als wesentlich betrachtet werden könnten, wie etwa das Start-und Landebahn-Management, jedoch auch eine Reihe von Diensten, die als nicht wesentlich betrachtet werden könnten, wie die Bereitstellung von Einkaufsbereichen. Betreiber wesentlicher Dienste sollten den spezifischen Sicherheitsanforderungen nur in Bezug auf die als wesentlich geltenden Dienste unterworfen sein. Zum Zwecke der Ermittlung von Betreibern sollten die Mitgliedstaaten deshalb eine Liste der Dienste erstellen, die als wesentlich betrachtet werden.

(23) Die Liste der Dienste sollte alle im Hoheitsgebiet eines Mitgliedstaats erbrachten Dienste enthalten, die die Anforderungen nach dieser Richtlinie erfüllen. Der betreffende Mitgliedstaat sollte die Möglichkeit haben, das bestehende Verzeichnis zu ändern, indem er neue Dienste aufnimmt. Die Liste der Dienste sollte den Mitgliedstaaten als Bezugspunkt für die Ermittlung von Betreibern wesentlicher Dienste dienen. Zweck der Liste ist es, die in einem bestimmten in dieser Richtlinie genannten Sektor als wesentlich geltenden Arten von Diensten auszuweisen und sie damit von den nicht wesentlichen Tätigkeiten abzugrenzen, für die eine in einem beliebigen Sektor tätige Einrichtung zuständig sein könnte. Die von jedem Mitgliedstaat erstellte Liste der Dienste wäre ein weiterer Beitrag zur Beurteilung der Regelungspraxis der einzelnen Mitgliedstaaten im Hinblick auf das Ziel, ein insgesamt kohärentes Verfahren der Ermittlung auf der Ebene der Mitgliedstaaten zu gewährleisten.

(24) Bietet eine Einrichtung einen wesentlichen Dienst in zwei oder mehr Mitgliedstaaten an, sollten diese Mitgliedstaaten zur Ermittlung des Betreibers untereinander bilaterale oder multilaterale Beratungen aufnehmen. Dieser Konsultationsprozess soll ihnen dabei helfen, die kritische Rolle des Betreibers im Hinblick auf grenzüberschreitende Auswirkungen zu beurteilen, und soll somit jedem beteiligten Mitgliedstaat ermöglichen, sich zu den Risiken zu äußern, die seiner Ansicht nach mit den angebotenen Diensten verbunden sind. Die betroffenen Mitgliedstaaten sollten den Ansichten der jeweils anderen Mitgliedstaaten in diesem Verfahren Rechnung tragen, und sie sollten in diesem Zusammenhang die Unterstützung der Kooperationsgruppe anfordern können.

(25) Als Ergebnis des Ermittlungsprozesses sollten die Mitgliedstaaten nationale Maßnahmen erlassen, in denen bestimmt wird, welche Einrichtungen Pflichten im Zusammenhang mit Netz- und Informationssystemen unterliegen. Dies könnte durch die Festlegung eines Verzeichnisses sämtlicher Betreiber wesentlicher Dienste oder durch die Annahme nationaler Maßnahmen einschließlich objektiv quantifizierbarer Kriterien wie beispielsweise Leistung des Betreibers oder Anzahl der Nutzer erfolgen, die die Festlegung derjenigen Einrichtungen ermöglichen, die Pflichten im Hinblick auf Netz- und Informationssysteme unterliegen. Die nationalen Maßnahmen, gleich, ob sie bereits gelten oder im Rahmen dieser Richtlinie angenommen werden, sollten sämtliche rechtlichen und administrativen Maßnahmen und Strategien umfassen, die die Ermittlung von Betreibern wesentlicher Dienste im Sinne dieser Richtlinie ermöglichen.

(26) Als Indikator für die Bedeutung der ermittelten Betreiber wesentlicher Dienste für den jeweiligen Sektor sollten die Mitgliedstaaten der Anzahl und der Größe dieser Betreiber Rechnung tragen, beispielsweise gemessen an deren Marktanteil oder der produzierten oder transportierten Datenmenge, ohne dabei verpflichtet zu sein, Informationen preiszugeben, aus denen hervorgeht, welche Betreiber ermittelt wurden.

(27) Um festzustellen, ob ein Sicherheitsvorfall zu erheblichen Störungen bei der Bereitstellung eines wesentlichen Dienstes führen würde, sollten die Mitgliedstaaten eine Reihe unterschiedlicher Faktoren berücksichtigen, wie die Anzahl der Nutzer, die diesen Dienst zu privaten oder beruflichen Zwecken in Anspruch nehmen. Die Nutzung dieses Dienstes kann unmittelbar, mittelbar oder durch Vermittlung erfolgen. Bei der Beurteilung, in welchem Ausmaß und wie lange sich ein Sicherheitsvorfall auf wirtschaftliche und gesellschaftliche Tätigkeiten oder die öffentliche Sicherheit auswirken könnte, sollten die Mitgliedstaaten außerdem die Zeitspanne abschätzen, die voraussichtlich vergeht, bevor die Unterbrechung nachteilige Auswirkungen hätte.

(28) Zusätzlich zu den sektorübergreifenden Faktoren sollten auch sektorspezifische Faktoren berücksichtigt werden, um zu bestimmen, ob ein Sicherheitsvorfall zu erheblichen Störungen bei der Bereitstellung eines Dienstes führen würde. Bei Energieversorgern könnten hierzu die Menge oder der Anteil der landesweit produzierten Energie gehören, bei Öllieferanten die Fördermenge pro Tag, beim Luftverkehr, einschließlich Flughäfen und Luftfahrtunternehmen, Schienenverkehr und bei Seehäfen der Anteil des landesweiten Verkehrsvolumens und die Anzahl der Passagiere oder der Frachtdienste pro Jahr, bei Bank- oder Finanzmarktinfrastrukturen deren Systemrelevanz aufgrund der Bilanzsumme oder des Anteils dieser Bilanzsumme am BIP, im Gesundheitsbereich die Anzahl der vom Anbieter jährlich versorgten Patienten, bei der Wassergewinnung, -aufbereitung und -versorgung die Wassermenge, die Anzahl und die Arten der belieferten Verbraucher, einschließlich beispielsweise Krankenhäuser, öffentliche Dienstleister oder Einzelpersonen sowie das Vorhandensein alternativer Wasserquellen zur Versorgung desselben geografischen Gebiets.

(29) Um ein hohes Sicherheitsniveau von Netz- und Informationssystemen zu erreichen und aufrechtzuerhalten, sollte jeder Mitgliedstaat über eine nationale Strategie zur Sicherheit von Netz- und Informationssystemen verfügen, in der die strategischen Ziele sowie konkrete politische Maßnahmen vorgesehen sind.

(30) Angesichts der unterschiedlichen nationalen Verwaltungsstrukturen und zur Beibehaltung bereits bestehender sektorbezogener Vereinbarungen oder von Aufsichts- oder Regulierungsstellen der Union sowie zur Vermeidung von Doppelarbeit sollten die Mitgliedstaaten befugt sein, mehr als eine nationale Behörde zu benennen, die für die Erfüllung der Aufgaben im Zusammenhang mit der Sicherheit von Netz- und Informationssystemen von Betreibern wesentlicher Dienste und Anbietern digitaler Dienste gemäß dieser Richtlinie verantwortlich sind.

(31) Zur Erleichterung der grenzüberschreitenden Zusammenarbeit und Kommunikation und um die effektive Umsetzung dieser Richtlinie zu ermöglichen, ist es notwendig, dass jeder Mitgliedstaat unbeschadet sektorbezogener regulatorischer Vereinbarungen eine nationale zentrale Anlaufstelle benennt, die für die Koordinierung im Zusammenhang mit der Sicherheit von Netz-und Informationssystemen und für die grenzüberschreitende Zusammenarbeit auf Unionsebene zuständig ist. Die zuständigen Behörden und die zentralen Anlaufstellen sollten mit angemessenen technischen, finanziellen und personellen Ressourcen ausgestattet sein, um die ihnen übertragenen Aufgaben wirksam und effizient erfüllen und somit die Ziele dieser Richtlinie erreichen zu können. Da mit dieser Richtlinie durch den Aufbau von Vertrauen ein besseres Funktionieren des Binnenmarkts bezweckt wird, müssen die Stellen der Mitgliedstaaten wirksam mit den Wirtschaftsteilnehmern zusammenarbeiten können und über entsprechende Strukturen verfügen.

(32) Sicherheitsvorfälle sollten den zuständigen Behörden oder den Computer-Notfallteams (CSIRTs — Computer Security Incident Response Teams) gemeldet werden. Sicherheitsvorfälle sollten nicht unmittelbar den zentralen Anlaufstellen gemeldet werden, es sei denn, diese üben außerdem die Funktion einer zuständigen Behörde oder eines CSIRT aus. Eine zuständige Behörde oder ein CSIRT sollte allerdings in der Lage sein, die zentrale Anlaufstelle damit zu beauftragen, Meldungen über Sicherheitsvorfälle an die zentralen Anlaufstellen anderer betroffener Mitgliedstaaten weiterzuleiten.

(33) Damit sichergestellt ist, dass die Mitgliedstaaten und die Kommission wirksam informiert werden, sollte die zentrale Anlaufstelle der Kooperationsgruppe einen zusammenfassenden Bericht vorlegen, der anonymisiert sein sollte, um die Vertraulichkeit der Meldungen und der Identität der Betreiber wesentlicher Dienste oder der Anbieter digitaler Dienste zu wahren, da die Identität der meldenden Einrichtungen für den Austausch bewährter Verfahren innerhalb der Kooperationsgruppe nicht erforderlich ist. In dem zusammenfassenden Bericht sollten Informationen über die Anzahl der eingegangenen Meldungen sowie Angaben über die Art der gemeldeten Sicherheitsvorfälle, wie beispielsweise die Arten der Sicherheitsverletzungen, deren Schwere oder Dauer, enthalten sein.

(34) Die Mitgliedstaaten sollten über angemessene technische und organisatorische Fähigkeiten zur Prävention, Erkennung, Reaktion und Abschwächung von Sicherheitsvorfällen und Risiken bei Netz- und Informationssystemen verfügen. Die Mitgliedstaaten sollten daher gewährleisten, dass sie über gut funktionierende CSIRTs — auch Computer-Notfallteams (CERTs — Computer Emergency Response Teams) genannt — verfügen, die die grundlegenden Anforderungen zur Gewährleistung wirksamer und kompatibler Fähigkeiten zur Bewältigung von Vorfällen und Risiken und einer effizienten Zusammenarbeit auf Unionsebene erfüllen. Damit alle Arten von Betreibern wesentlicher Dienste und von Anbietern digitaler Dienste diese Fähigkeiten und diese Zusammenarbeit nutzen können, sollten die Mitgliedstaaten sicherstellen, dass alle Arten von einem eingerichteten CSIRT abgedeckt sind. Wegen der Bedeutung der internationalen Zusammenarbeit zur Cybersicherheit sollten die CSIRTs sich zusätzlich zum durch diese Richtlinie geschaffenen CSIRTs-Netzwerk an internationalen Kooperationsnetzen beteiligen können.

(35) Da die meisten Netz- und Informationssysteme privat betrieben werden, ist die Zusammenarbeit zwischen dem privaten und dem öffentlichen Sektor von zentraler Bedeutung. Die Betreiber wesentlicher Dienste und die Anbieter digitaler Dienste sollten angehalten werden, sich eines eigenen informellen Kooperationsmechanismus zur Gewährleistung der Sicherheit von Netz- und Informationssystemen zu bedienen. Die Kooperationsgruppe sollte gegebenenfalls relevante Interessenträger zu Beratungen einladen können. Zur wirksamen Unterstützung des Austauschs von Informationen und bewährten Verfahren muss unbedingt sichergestellt werden, dass Betreiber wesentlicher Dienste und Anbieter digitaler Dienste, die an einem solchen Austausch beteiligt sind, keine Benachteiligung aufgrund ihrer Zusammenarbeit erfahren.

(36) Die ENISA sollte die Mitgliedstaaten und die Kommission mit Fachkompetenz, als Berater und als Mittler für den Austausch bewährter Verfahren unterstützen. Insbesondere sollte die Kommission die ENISA bei der Anwendung dieser Richtlinie zurate ziehen, und die Mitgliedstaaten sollten berechtigt sein, die ENISA zurate zu ziehen. Um Kapazitäten und Fachwissen unter den Mitgliedstaaten aufbauen zu können, sollte die Kooperationsgruppe auch als Instrument für den Austausch bewährter Verfahren, für die Beratung über Fähigkeiten und die Abwehrbereitschaft der Mitgliedstaaten dienen und damit ihren Mitgliedern — auf freiwilliger Basis — bei der Evaluierung der nationalen Strategien für die Sicherheit von Netz- und Informationssystemen, beim Kapazitätsaufbau und bei der Evaluierung von Übungen zur Sicherheit von Netz- und Informationssystemen helfen.

(37) Bei der Anwendung dieser Richtlinie sollten die Mitgliedstaaten gegebenenfalls bestehende Organisationsstrukturen oder -strategien nutzen oder anpassen können.

(38) Die jeweiligen Aufgaben der Kooperationsgruppe und der ENISA bedingen einander und ergänzen sich. Im Einklang mit ihrem in der Verordnung (EU) Nr. 526/2013 des Europäischen Parlaments und des Rates ([1]) festgelegten Ziel, nämlich die Organe, Einrichtungen und sonstigen Stellen der Union und die Mitgliedstaaten dabei zu unterstützen, die politischen Maßnahmen durchzuführen, die erforderlich sind, um die rechtlichen und regulatorischen Anforderungen in Bezug auf die Sicherheit von Netz- und Informationssystemen gemäß den geltenden und künftigen Rechtsakten der Union zu erfüllen, sollte die ENISA die Kooperationsgruppe bei der Ausführung ihrer Aufgaben unterstützen. Die ENISA sollte insbesondere in den Bereichen Unterstützung leisten, die ihren eigenen, in der Verordnung (EU) Nr. 526/2013 festgelegten Aufgaben entsprechen, nämlich Strategien zur Sicherheit von Netz- und Informationssystemen zu analysieren, die Organisation und Durchführung von Übungen zur Sicherheit von Netz- und Informationssystemen auf Unionsebene zu unterstützen und Informationen und bewährte Verfahren in den Bereichen Öffentlichkeitsarbeit und Fortbildung auszutauschen. Die ENISA sollte außerdem an der Entwicklung von Leitlinien für sektorspezifische Kriterien zur Bestimmung der Bedeutung der Auswirkungen eines Sicherheitsvorfalls beteiligt sein.

([1]) 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).

(39) Zur Förderung verbesserter Sicherheit von Netz- und Informationssystemen sollte die Kooperationsgruppe gegebenenfalls mit den einschlägigen Organen, Einrichtungen und sonstigen Stellen der Union zusammenarbeiten, um Know-how und bewährte Verfahren mit ihnen auszutauschen und sie bezüglich Sicherheitsaspekten der Netz- und Informationssysteme, die Auswirkungen auf ihre Arbeit haben könnten, zu beraten, wobei die geltenden Vereinbarungen für den Austausch von einem eingeschränkten Zugang unterliegenden Informationen einzuhalten sind. Bei ihrer Zusammenarbeit mit Strafverfolgungsbehörden im Zusammenhang mit Sicherheitsaspekten der Netz- und Informationssysteme, die sich möglicherweise auf ihre Arbeit auswirken, sollte die Kooperationsgruppe vorhandene Informationskanäle und bestehende Netze beachten.

(40) Informationen über Sicherheitsvorfälle sind für die allgemeine Öffentlichkeit und Unternehmen, insbesondere für kleine und mittlere Unternehmen, zunehmend von Bedeutung. In manchen Fällen werden derartige Informationen bereits über das Internet auf nationaler Ebene in der jeweiligen Landessprache und mit besonderem Schwerpunkt auf Sicherheitsvorfälle und Sicherheitsereignisse mit nationalem Bezug bereitgestellt. Da Unternehmen immer stärker grenzüberschreitend tätig sind und die Bürger Online-Dienste nutzen, sollten die Informationen über Sicherheitsvorfälle auf Unionsebene in aggregierter Form bereitgestellt werden. Das Sekretariat des CSIRTs-Netzwerks wird aufgefordert, eine Website zu unterhalten oder eine entsprechende Seite auf einer bestehenden Website einzustellen, auf der allgemeine Informationen über größere in der Union aufgetretene Sicherheitsvorfälle mit einem besonderen Schwerpunkt auf die Interessen und den Bedarf von Unternehmen der allgemeinen Öffentlichkeit zur Verfügung gestellt werden. CSIRTs, die sich am CSIRTs-Netzwerk beteiligen, werden aufgefordert, freiwillig die auf dieser Website zu veröffentlichenden Informationen bereitzustellen, ohne vertrauliche oder sensible Informationen darin aufzunehmen.

(41) Gelten die betreffenden Informationen nach Vorschriften der Union und der Mitgliedstaaten über das Geschäftsgeheimnis als vertraulich, sollte deren Vertraulichkeit bei den in dieser Richtlinie vorgesehenen Tätigkeiten und bei der Erreichung der darin gesetzten Ziele sichergestellt werden.

(42) Übungen, bei denen Szenarien für Sicherheitsvorfälle in Echtzeit simuliert werden, sind wesentlich, um die Abwehrbereitschaft der Mitgliedstaaten und deren Zusammenarbeit im Bereich der Sicherheit von Netz- und Informationssystemen zu prüfen. Der von der ENISA unter Beteiligung der Mitgliedstaaten koordinierte Übungszyklus Cyber Europe ist ein nützliches Instrument zur Prüfung und für die Abfassung von Empfehlungen dazu, wie auf Unionsebene die Reaktion auf Sicherheitsvorfälle mit der Zeit verbessert werden sollte. In Anbetracht dessen, dass die Mitgliedstaaten gegenwärtig nicht verpflichtet sind, Übungen zu planen oder an ihnen teilzunehmen, sollte die Schaffung des CSIRTs-Netzwerks im Rahmen dieser Richtlinie es den Mitgliedstaaten ermöglichen, auf der Grundlage präziser Planungen und strategischer Entscheidungen an Übungen teilzunehmen. Die durch diese Richtlinie eingesetzte Kooperationsgruppe sollte die strategischen Entscheidungen für Übungen diskutieren, insbesondere, aber nicht ausschließlich, diejenigen, die die Regelmäßigkeit der Übungen und die Ausgestaltung der Szenarien betreffen. Im Einklang mit ihrem Mandat sollte die ENISA die Organisation und die Durchführung der unionsweiten Übungen unterstützen, indem sie die Kooperationsgruppe und das CSIRTs-Netzwerk mit ihrer Fachkompetenz berät.

(43) Angesichts des globalen Charakters von Sicherheitsproblemen, die Netz- und Informationssysteme beeinträchtigen, bedarf es einer engeren internationalen Zusammenarbeit, damit die Sicherheitsstandards und der Informationsaustausch verbessert werden können und ein gemeinsames umfassendes Konzept für Sicherheitsfragen gefördert werden kann.

(44) Die Verantwortung für die Gewährleistung der Sicherheit von Netz-und Informationssystemen liegt in erheblichem Maße bei den Betreibern wesentlicher Dienste oder den Anbietern digitaler Dienste. Durch geeignete rechtliche Anforderungen und freiwillige Branchenpraxis sollte eine Risikomanagementkultur gefördert und entwickelt werden, die unter anderem die Risikobewertung und die Anwendung von Sicherheitsmaßnahmen, die den jeweiligen Risiken angemessen sind, umfassen sollte. Ferner ist es für ein Funktionieren der Kooperationsgruppe und des CSIRTs-Netzwerks von großer Bedeutung, verlässliche gleiche Ausgangsbedingungen zu schaffen, damit eine wirksame Zusammenarbeit aller Mitgliedstaaten sichergestellt ist.

(45) Diese Richtlinie gilt nur für öffentliche Verwaltungen, die als Betreiber wesentlicher Dienste ermittelt werden. Daher sind die Mitgliedstaaten für die Gewährleistung der Sicherheit von Netz- und Informationssystemen der öffentlichen Verwaltungen verantwortlich, die nicht in den Anwendungsbereich dieser Richtlinie fallen.

(46) Die Maßnahmen für das Risikomanagement umfassen Maßnahmen zur Ermittlung jeder Gefahr eines Vorfalls, zur Verhinderung, Aufdeckung und Bewältigung von Sicherheitsvorfällen sowie der Minderung ihrer Folgen. Die Sicherheit von Netz- und Informationssystemen umfasst die Sicherheit gespeicherter, übermittelter und verarbeiteter Daten.

(47) Zuständige Behörden sollten weiterhin nationale Leitlinien festlegen können, die die Umstände betreffen, unter denen Betreiber wesentlicher Dienste verpflichtet sind, Sicherheitsvorfälle zu melden.

(48) Viele Unternehmen in der Union verlassen sich bei der Bereitstellung ihrer Dienste auf Anbieter digitaler Dienste. Da manche digitale Dienste für ihre Nutzer, darunter auch Betreiber wesentlicher Dienste, eine wichtige Ressource darstellen könnten und da derartigen Nutzern möglicherweise nicht immer Alternativen zur Verfügung stehen, sollte diese Richtlinie auch für die Anbieter derartiger Dienste gelten. Die Sicherheit, Verfügbarkeit und Verlässlichkeit der in dieser Richtlinie aufgeführten Art von digitalen Diensten sind für das reibungslose Funktionieren vieler Unternehmen von wesentlicher Bedeutung. Eine Störung eines solchen digitalen Dienstes könnte die Bereitstellung anderer, von ihnen abhängiger Dienste verhindern und somit wesentliche wirtschaftliche und gesellschaftliche Tätigkeiten in der Union beeinträchtigen. Derartige digitale Dienste könnten daher für das reibungslose Funktionieren von Unternehmen, die von diesen Diensten abhängen, und darüber hinaus für die Beteiligung derartiger Unternehmen am Binnenmarkt und am grenzüberschreitenden Handel in der gesamten Union eine wesentliche Rolle spielen. Die Anbieter digitaler Dienste, die unter diese Richtlinie fallen, sind diejenigen, von denen angenommen wird, dass sie digitale Dienste anbieten, von denen viele Unternehmen in der Union zunehmend abhängig sind.

(49) Angesichts der Bedeutung ihrer Dienste für die Tätigkeit anderer Unternehmen in der Union sollten Anbieter digitaler Dienste ein Sicherheitsniveau gewährleisten, das der Höhe des Risikos für die Sicherheit der von ihnen gebotenen Dienste angemessen ist. In der Praxis ist das Risiko für den Betreiber wesentlicher Dienste, die oft für die Aufrechterhaltung kritischer gesellschaftlicher und wirtschaftlicher Tätigkeiten von wesentlicher Bedeutung sind, höher als das Risiko für den Anbieter digitaler Dienste. Daher sollten die an Anbieter digitaler Dienste gestellten Sicherheitsanforderungen geringer sein. Anbietern digitaler Dienste sollte es freigestellt sein, die Maßnahmen zu ergreifen, die sie für die Bewältigung der Risiken für die Sicherheit ihrer Netz- und Informationssysteme für angemessen halten. Aufgrund des grenzüberschreitenden Charakters ihrer Tätigkeiten sollten die Anbieter digitaler Dienste einem auf Unionsebene stärker harmonisierten Konzept unterliegen. Durchführungsrechtsakte sollten die Spezifikation und die Umsetzung derartiger Maßnahmen erleichtern.

(50) Zwar sind Hersteller von Hardware und Softwareentwickler keine Betreiber wesentlicher Dienste oder Anbieter digitaler Dienste, jedoch verstärken ihre Produkte die Sicherheit von Netz- und Informationssystemen. Daher spielen sie eine wichtige Rolle dabei, die Betreiber wesentlicher Dienste und die Anbieter digitaler Dienste in die Lage zu versetzen, ihre Netz- und Informationssysteme sichern zu können. Derartige Hardware- und Softwareprodukte unterliegen bereits geltenden Produkthaftungsvorschriften.

(51) Zu den von Betreibern wesentlicher Dienste und Anbietern digitaler Dienste zu ergreifenden technischen und organisatorischen Maßnahmen sollte nicht die Verpflichtung gehören, bestimmte geschäftliche Informationen und Produkte der Kommunikationstechnik in bestimmter Weise zu konzipieren, zu entwickeln oder herzustellen.

(52) Die Betreiber wesentlicher Dienste und die Anbieter digitaler Dienste sollten die Sicherheit der von ihnen verwendeten Netz- und Informationssysteme gewährleisten. Dabei handelt es sich hauptsächlich um private Netz- und Informationssysteme, die entweder von internem IT-Personal verwaltet werden oder deren Sicherheit Dritten anvertraut wurde. Die Sicherheitsanforderungen und die Meldepflicht sollten für die einschlägigen Betreiber wesentlicher Dienste und Anbieter digitaler Dienste unabhängig davon gelten, ob sie ihre Netz- und Informationssysteme intern warten oder diese Aufgabe ausgliedern.

(53) Damit keine unverhältnismäßige finanzielle und administrative Belastung für Betreiber wesentlicher Dienste und Anbieter digitaler Dienste entsteht, sollten die Verpflichtungen in einem angemessenen Verhältnis zu den Risiken stehen, denen das betreffende Netz- und Informationssystem ausgesetzt ist; dabei wird dem bei solchen Maßnahmen geltenden neuesten Stand Rechnung getragen. Im Fall von Anbietern digitaler Dienste sollten diese Bestimmungen nicht für Kleinst- und Kleinunternehmen gelten.

(54) Nehmen öffentliche Verwaltungen in den Mitgliedstaaten die Dienste von Anbietern digitaler Dienste in Anspruch, insbesondere Cloud-Computing-Dienste, so verlangen sie möglicherweise vom Anbieter derartiger Dienste zusätzliche Sicherheitsmaßnahmen über das üblicherweise von Anbietern digitaler Dienste gemäß dieser Richtlinie Angebotene hinaus. Sie sollten berechtigt sein, dies über vertragliche Verpflichtungen zu regeln.

(55) Die in dieser Richtlinie enthaltenen Begriffsbestimmungen für Online-Marktplatz, Online-Suchmaschinen und Cloud-Computing-Dienste gelten für die besonderen Zwecke dieser Richtlinie und unbeschadet anderer Rechtsakte.

(56) Diese Richtlinie sollte die Mitgliedstaaten nicht daran hindern, nationale Maßnahmen zu erlassen, die öffentliche Stellen dazu verpflichten, besondere Sicherheitsanforderungen zu erfüllen, wenn sie mit Cloud-Computing-Diensten Verträge schließen. Jede dieser nationalen Maßnahmen sollte für die betreffende öffentliche Stelle und nicht für den Anbieter des Cloud-Computing-Dienstes gelten.

(57) Wegen der grundlegenden Unterschiede zwischen Betreibern wesentlicher Dienste, insbesondere wegen deren unmittelbarer Verbindung mit einer physischen Infrastruktur, und Anbietern digitaler Dienste, insbesondere wegen deren grenzüberschreitender Art, sollte die Richtlinie in Bezug auf das Maß der Harmonisierung im Hinblick auf diese beiden Gruppen jeweils einen unterschiedlichen Ansatz verfolgen. Bei Betreibern wesentlicher Dienste sollten die Mitgliedstaaten in der Lage sein, die relevanten Betreiber zu bestimmen und an sie strengere Anforderungen zu stellen als die in dieser Richtlinie festgelegten. Die Mitgliedstaaten sollten keine Anbieter digitaler Dienste bestimmen, da diese Richtlinie im Rahmen ihres Geltungsbereichs für alle Anbieter digitaler Dienste gelten sollte. Darüber hinaus sollten diese Richtlinie und die auf ihrer Grundlage erlassenen Durchführungsrechtsakte ein hohes Maß an Harmonisierung im Hinblick auf die Sicherheitsanforderungen und Meldepflichten für Anbieter digitaler Dienste gewährleisten. Das sollte zu einer einheitlichen Behandlung der Anbieter digitaler Dienste in der Union führen, die ihrer Art und der Höhe des Risikos, dem sie unterliegen könnten, angemessen ist.

(58) Diese Richtlinie sollte die Mitgliedstaaten nicht daran hindern, Einrichtungen, die keine Anbieter digitaler Dienste innerhalb des Geltungsbereichs dieser Richtlinie sind, unbeschadet der den Mitgliedstaaten nach Unionsrecht auferlegten Pflichten Sicherheitsanforderungen und Meldepflichten aufzuerlegen.

(59) Die zuständigen Behörden sollten dafür Sorge tragen, dass informelle, vertrauenswürdige Kanäle für den Informationsaustausch erhalten bleiben. Bei der Bekanntmachung von Sicherheitsvorfällen, die den zuständigen Behörden gemeldet werden, sollte das Interesse der Öffentlichkeit, über Bedrohungen informiert zu werden, sorgfältig gegen einen möglichen wirtschaftlichen Schaden bzw. einen Imageschaden abgewogen werden, der den Betreibern wesentlicher Dienste oder den Anbietern digitaler Dienste, die solche Vorfälle melden, entstehen kann. Bei der Erfüllung der Meldepflichten sollten die zuständigen Behörden und die CSIRTs besonders darauf achten, dass Informationen über die Anfälligkeit von Produkten bis zur Veröffentlichung der entsprechenden Sicherheitsfixes streng vertraulich bleiben.

(60) Anbieter digitaler Dienste sollten weniger strikten reaktiven Aufsichtstätigkeiten (ex post) unterliegen, die durch die Art ihrer Dienste und Tätigkeiten gerechtfertigt sind. Die betreffenden zuständigen Behörden sollten daher nur dann tätig werden, wenn ihnen z. B. durch den Anbieter digitaler Dienste selbst, durch eine andere zuständige Behörde — auch der eines anderen Mitgliedstaats — oder durch einen Nutzer des Dienstes Nachweise dafür vorgelegt werden, dass ein Anbieter digitaler Dienste die Anforderungen dieser Richtlinie nicht erfüllt, vor allem dann, wenn sich ein Sicherheitsvorfall ereignet hat. Die zuständige Behörde sollte daher keine generelle Verpflichtung zur Beaufsichtigung von Anbietern digitaler Dienste haben.

(61) Die zuständigen Behörden sollten mit den für die Erfüllung ihrer Aufgaben erforderlichen Mitteln ausgestattet sein; sie sollten auch befugt sein, hinreichende Auskünfte einzuholen, damit sie die Sicherheit von Netz- und Informationssystemen beurteilen können.

(62) Sicherheitsvorfälle können das Ergebnis krimineller Handlungen sein, die durch Unterstützung der Koordination und der Zusammenarbeit zwischen den Betreibern wesentlicher Dienste, den Anbietern digitaler Dienste, den zuständigen Behörden und den Strafverfolgungsbehörden verhindert, aufgedeckt und strafrechtlich verfolgt werden. Wenn der Verdacht besteht, dass ein Sicherheitsvorfall im Zusammenhang mit schweren kriminellen Handlungen nach Unionsrecht oder nationalem Recht steht, so sollten die Mitgliedstaaten die Betreiber wesentlicher Dienste und die Anbieter digitaler Dienste dazu anhalten, diese Sicherheitsvorfälle mit einem mutmaßlichen schwerwiegenden kriminellen Hintergrund den entsprechenden Strafverfolgungsbehörden zu melden. Gegebenenfalls ist die Unterstützung durch das Europäische Zentrum zur Bekämpfung der Cyberkriminalität (EC3) und der ENISA bei der Koordinierung zwischen den zuständigen Behörden und den Strafverfolgungsbehörden der verschiedenen Mitgliedstaaten wünschenswert.

(63) Häufig ist bei Sicherheitsvorfällen der Schutz personenbezogener Daten nicht mehr gewährleistet. Deshalb sollten die zuständigen Behörden und die Datenschutzbehörden zusammenarbeiten und Informationen zu allen einschlägigen Fragen austauschen, um Verletzungen des Schutzes personenbezogener Daten aufgrund von Sicherheitsvorfällen zu begegnen.

(64) Ein Anbieter digitaler Dienste sollte der gerichtlichen Zuständigkeit des Mitgliedstaats unterliegen, in dem der betreffende Anbieter digitaler Dienste seine Hauptniederlassung in der Union hat; dies ist im Allgemeinen der Ort, an dem er seinen Hauptsitz in der Union hat. Eine Niederlassung setzt die effektive und tatsächliche Ausübung einer Tätigkeit durch eine feste Einrichtung voraus. Die Rechtsform einer solchen Einrichtung, gleich, ob es sich um eine Zweigstelle oder eine Tochtergesellschaft mit eigener Rechtspersönlichkeit handelt, ist dabei unerheblich. Dieses Kriterium sollte nicht davon abhängen, ob sich der physische Standort der Netz- und der

Informationssysteme an einem bestimmten Ort befindet; das Vorhandensein und die Nutzung derartiger Systeme stellen an sich keine derartige Hauptniederlassung dar und sind daher kein Kriterium für die Bestimmung der Hauptniederlassung.

(65) Bietet ein Anbieter digitaler Dienste, der keine Niederlassung in der Union hat, Dienste in der Union an, so sollte er einen Vertreter benennen. Um festzustellen, ob ein solcher Anbieter digitaler Dienste in der Union Dienste anbietet, sollte geprüft werden, ob er offensichtlich beabsichtigt, Personen in einem oder mehreren Mitgliedstaaten Dienste anzubieten. Die bloße Zugänglichkeit der Website eines Anbieters digitaler Dienste oder eines Vermittlers von der Union aus oder einer E-Mail-Adresse oder anderer Kontaktdaten sind zur Feststellung einer solchen Absicht ebenso wenig ausreichend wie die Verwendung einer Sprache, die in dem Drittland, in dem der Anbieter digitaler Dienste niedergelassen ist, allgemein gebräuchlich ist. Jedoch können andere Faktoren wie die Verwendung einer Sprache oder Währung, die in einem oder mehreren Mitgliedstaaten gebräuchlich ist, in Verbindung mit der Möglichkeit, Dienste in dieser anderen Sprache zu bestellen, oder die Erwähnung von Kunden oder Nutzern in der Union darauf hindeuten, dass der Anbieter digitaler Dienste beabsichtigt, in der Union Dienste anzubieten. Der Vertreter sollte im Auftrag des Anbieters digitaler Dienste handeln, und es sollte für die zuständigen Behörden oder die CSIRTs möglich sein, mit ihm Kontakt aufzunehmen. Der Vertreter sollte vom Anbieter digitaler Dienste ausdrücklich schriftlich beauftragt werden, im Rahmen der Pflichten des Letztgenannten gemäß dieser Richtlinie in dessen Auftrag zu handeln; hierzu zählt auch das Melden von Sicherheitsvorfällen.

(66) Die Normung von Sicherheitsanforderungen ist ein vom Markt ausgehender Vorgang. Um die Sicherheitsstandards einander anzunähern, sollten die Mitgliedstaaten die Anwendung oder Einhaltung konkreter Normen fördern, damit ein hohes Sicherheitsniveau von Netz- und Informationssystemen auf Unionsebene gewährleistet wird. Die ENISA sollte den Mitgliedstaaten mit Leitlinien beratend zur Seite stehen. Zu diesem Zweck könnte es hilfreich sein, harmonisierte Normen auszuarbeiten; dies sollte nach der Verordnung (EU) Nr. 1025/2012 des Europäischen Parlaments und des Rates ([1]) geschehen.

(67) Einrichtungen, die nicht in den Geltungsbereich dieser Richtlinie fallen, können mit Sicherheitsvorfällen konfrontiert sein, die sich in erheblichem Maße auf die von ihnen bereitgestellten Dienste auswirken. Sind diese Einrichtungen der Ansicht, dass es im öffentlichen Interesse liegt, das Auftreten derartiger Sicherheitsvorfälle zu melden, sollten sie dies auf freiwilliger Basis tun können. Solche Meldungen sollten von der zuständigen Behörde oder dem CSIRT bearbeitet werden, wenn diese Bearbeitung keinen unverhältnismäßigen oder ungebührlichen Aufwand für die betreffenden Mitgliedstaaten darstellt.

(68) Zur Gewährleistung einheitlicher Bedingungen für die Durchführung dieser Richtlinie sollten der Kommission Durchführungsbefugnisse zur Festlegung der Verfahrensmodalitäten, die für das Funktionieren der Kooperationsgruppe erforderlich sind, und der Sicherheitsanforderungen und Meldepflichten für Anbieter digitaler Dienste übertragen werden. Diese Befugnisse sollten im Einklang mit der Verordnung (EU) Nr. 182/2011 des Europäischen Parlaments und des Rates ([2]) ausgeübt werden. Wenn die Kommission Durchführungsrechtsakte zu Verfahrensmodalitäten, die für das Funktionieren der Kooperationsgruppe erforderlich sind, erlässt, sollte sie der Stellungnahme der ENISA so weit wie möglich Rechnung tragen.

(69) Wenn die Kommission Durchführungsrechtsakte zu Sicherheitsanforderungen für Anbieter digitaler Dienste erlässt, sollte sie der Stellungnahme der ENISA weitestgehend Rechnung tragen und Interessenträger anhören. Darüber hinaus wird die Kommission aufgefordert, den folgenden Beispielen Rechnung zu tragen: im Zusammenhang mit der Sicherheit der Systeme und Anlagen: physische Sicherheit und Sicherheit des Umfelds, Sicherheit des Materials, Kontrolle des Zugangs zu Netz- und Informationssystemen sowie Integrität der Netz- und Informationssysteme; im Hinblick auf die Bewältigung von Sicherheitsvorfällen: Verfahren für die Bewältigung von Sicherheitsvorfällen, Kapazitäten zum Aufspüren von Sicherheitsvorfällen, Meldung und Mitteilung von Sicherheitsvorfällen; in Bezug auf Betriebskontinuitätsmanagement: Strategie für die Verfügbarkeit der Dienste sowie Notfallpläne, Kapazitäten zur Wiederherstellung im Falle eines Systemabsturzes; und in Bezug auf Überwachung, Überprüfung und Erprobung: Strategien für die Überwachung und Protokollierung, Beübung von Notfallplänen, Erprobung der Netz- und Informationssysteme, Sicherheitsbewertungen und Überwachung der Einhaltung der Anforderungen.

(70) Bei der Durchführung dieser Richtlinie sollte die Kommission gegebenenfalls zu den einschlägigen sektoralen Ausschüssen und einschlägigen Einrichtungen auf Unionsebene in den von dieser Richtlinie betroffenen Bereichen Kontakt halten.

([1]) Verordnung (EU) Nr. 1025/2012 des Europäischen Parlaments und des Rates vom 25. Oktober 2012 zur europäischen Normung, zur Änderung der Richtlinien 89/686/EWG und 93/15/EWG des Rates sowie der Richtlinien 94/9/EG, 94/25/EG, 95/16/EG, 97/23/EG, 98/34/EG, 2004/22/EG, 2007/23/EG, 2009/23/EG und 2009/105/EG des Europäischen Parlaments und des Rates und zur Aufhebung des Beschlusses 87/95/EWG des Rates und des Beschlusses Nr. 1673/2006/EG des Europäischen Parlaments und des Rates (ABl. L 316 vom 14.11.2012, S. 12).

([2]) Verordnung (EU) Nr. 182/2011 des Europäischen Parlaments und des Rates vom 16. Februar 2011 zur Festlegung der allgemeinen Regeln und Grundsätze, nach denen die Mitgliedstaaten die Wahrnehmung der Durchführungsbefugnisse durch die Kommission kontrollieren (ABl. L 55 vom 28.2.2011, S. 13).

(71) Die Kommission sollte diese Richtlinie regelmäßig in Abstimmung mit betroffenen Interessenträgern überprüfen, insbesondere um festzustellen, ob sie veränderten gesellschaftlichen, politischen oder technischen Bedingungen oder veränderten Marktbedingungen anzupassen ist.

(72) Der Austausch von Informationen über Risiken und Vorfälle in der Kooperationsgruppe und im CSIRTs-Netzwerk und die Einhaltung der Verpflichtung zur Meldung von Sicherheitsvorfällen bei den zuständigen nationalen Behörden oder den CSIRTs könnte die Verarbeitung personenbezogener Daten erfordern. Diese Verarbeitung sollte mit der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates ([1]) und der Verordnung (EG) Nr. 45/2001 des Europäischen Parlaments und des Rates ([2]) vereinbar sein. Bei der Anwendung dieser Richtlinie sollte je nach Einzelfall die Verordnung (EG) Nr. 1049/2001 des Europäischen Parlaments und des Rates ([3]) gelten.

(73) Der Europäische Datenschutzbeauftragte wurde gemäß Artikel 28 Absatz 2 der Verordnung (EG) Nr. 45/2001 konsultiert und hat am 14. Juni 2013 eine Stellungnahme ([4]) abgegeben.

(74) Da das Ziel dieser Richtlinie, nämlich ein hohes gemeinsames Sicherheitsniveau von Netz- und Informationssystemen in der Union zu erreichen, von den Mitgliedstaaten nicht ausreichend verwirklicht werden kann, sondern vielmehr wegen der Wirkung der Maßnahme auf Unionsebene besser zu verwirklichen ist, kann die Union in 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 Richtlinie nicht über das für die Verwirklichung dieses Ziels erforderliche Maß hinaus.

(75) Diese Richtlinie steht mit den in der Charta der Grundrechte der Europäischen Union anerkannten Grundrechten und Grundsätzen, insbesondere der Achtung des Privatlebens und der Kommunikation, dem Schutz personenbezogener Daten, der unternehmerischen Freiheit, dem Eigentumsrecht, dem Recht auf einen wirksamen Rechtsbehelf und dem Recht, gehört zu werden, im Einklang. Diese Richtlinie sollte im Einklang mit diesen Rechten und Grundsätzen umgesetzt werden —

HABEN FOLGENDE RICHTLINIE ERLASSEN:

KAPITEL I

ALLGEMEINE BESTIMMUNGEN

Artikel 1

Gegenstand und Anwendungsbereich

(1) Mit dieser Richtlinie werden Maßnahmen festgelegt, mit denen ein hohes gemeinsames Sicherheitsniveau von Netz- und Informationssystemen in der Union erreicht werden soll, um so das Funktionieren des Binnenmarkts zu verbessern.

(2) Zu diesem Zweck sieht diese Richtlinie Folgendes vor:

a) die Pflicht für alle Mitgliedstaaten, eine nationale Strategie für die Sicherheit von Netz- und Informationssystemen festzulegen;

b) die Schaffung einer Kooperationsgruppe, um die strategische Zusammenarbeit und den Informationsaustausch zwischen den Mitgliedstaaten zu unterstützen und zu erleichtern und Vertrauen zwischen ihnen aufzubauen;

c) die Schaffung eines Netzwerks von Computer-Notfallteams (CSIRTs-Netzwerk — Computer Security Incident Response Teams Network), um zum Aufbau von Vertrauen zwischen den Mitgliedstaaten beizutragen und eine rasche und wirksame operative Zusammenarbeit zu fördern;

([1]) Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (ABl. L 281 vom 23.11.1995, S. 31).
([2]) 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).
([3]) 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).
([4]) ABl. C 32 vom 4.2.2014, S. 19.

d) Sicherheitsanforderungen und Meldepflichten für die Betreiber wesentlicher Dienste und für Anbieter digitaler Dienste;

e) die Pflicht für die Mitgliedstaaten, nationale zuständige Behörden, zentrale Anlaufstellen und CSIRTs mit Aufgaben im Zusammenhang mit der Sicherheit von Netz- und Informationssystemen zu benennen.

(3) Die in dieser Richtlinie vorgesehenen Sicherheitsanforderungen und Meldepflichten gelten nicht für Unternehmen, die den Anforderungen der Artikel 13a und 13b der Richtlinie 2002/21/EG unterliegen, und nicht für Vertrauensdiensteanbieter, die den Anforderungen des Artikels 19 der Verordnung (EU) Nr. 910/2014 unterliegen.

(4) Diese Richtlinie gilt unbeschadet der Richtlinie 2008/114/EG des Rates ([1]) und der Richtlinien 2011/93/EU ([2]) und 2013/40/EU des Europäischen Parlaments und des Rates ([3]).

(5) Unbeschadet des Artikels 346 AEUV werden Informationen, die gemäß den Vorschriften der Union und der Mitgliedstaaten, wie z. B. Vorschriften über das Geschäftsgeheimnis, vertraulich sind, mit der Kommission und anderen zuständigen Behörden nur ausgetauscht, wenn dieser Austausch für die Anwendung dieser Richtlinie erforderlich ist. Die auszutauschenden Informationen werden auf das beschränkt, was für das verfolgte Ziel relevant und angemessen ist. Bei diesem Informationsaustausch werden die Vertraulichkeit der Informationen gewahrt sowie die Sicherheit und die geschäftlichen Interessen der Betreiber wesentlicher Dienste und der Anbieter digitaler Dienste geschützt.

(6) Diese Richtlinie berührt nicht die von den Mitgliedstaaten getroffenen Maßnahmen zum Schutz ihrer grundlegenden staatlichen Funktionen, insbesondere Maßnahmen zum Schutz der nationalen Sicherheit, einschließlich Maßnahmen zum Schutz von Informationen, deren Preisgabe nach Erachten der Mitgliedstaaten ihren wesentlichen Sicherheitsinteressen widerspricht, und zur Aufrechterhaltung von Recht und Ordnung, insbesondere zur Ermöglichung der Ermittlung, Aufklärung und Verfolgung von Straftaten.

(7) Wird nach Maßgabe eines sektorspezifischen Rechtsakts der Union von den Betreibern wesentlicher Dienste oder den Anbietern digitaler Dienste gefordert, entweder die Sicherheit ihrer Netz- und Informationssysteme oder die Meldung von Sicherheitsvorfällen zu gewährleisten, und sind diese Anforderungen in ihrer Wirkung den in dieser Richtlinie enthaltenen Pflichten mindestens gleichwertig, so gelten die einschlägigen Bestimmungen jenes sektorspezifischen Rechtsakts der Union.

Artikel 2

Verarbeitung personenbezogener Daten

(1) Die Verarbeitung personenbezogener Daten gemäß dieser Richtlinie erfolgt nach Maßgabe der Richtlinie 95/46/EG.

(2) Die Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Union gemäß dieser Richtlinie erfolgt nach Maßgabe der Verordnung (EG) Nr. 45/2001.

Artikel 3

Mindestharmonisierung

Unbeschadet des Artikels 16 Absatz 10 und ihrer Verpflichtungen nach dem Unionsrecht können die Mitgliedstaaten Bestimmungen erlassen oder aufrechterhalten, mit denen ein höheres Sicherheitsniveau von Netz- und Informationssystemen erreicht werden soll.

([1]) Richtlinie 2008/114/EG des Rates vom 8. Dezember 2008 über die Ermittlung und Ausweisung europäischer kritischer Infrastrukturen und die Bewertung der Notwendigkeit, ihren Schutz zu verbessern (ABl. L 345 vom 23.12.2008, S. 75).

([2]) Richtlinie 2011/93/EU des Europäischen Parlaments und des Rates vom 13. Dezember 2011 zur Bekämpfung des sexuellen Missbrauchs und der sexuellen Ausbeutung von Kindern sowie der Kinderpornografie sowie zur Ersetzung des Rahmenbeschlusses 2004/68/JI des Rates (ABl. L 335 vom 17.12.2011, S. 1).

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

Artikel 4

Begriffsbestimmungen

Für die Zwecke dieser Richtlinie bezeichnet der Ausdruck

1. „Netz- und Informationssystem“

   a) ein elektronisches Kommunikationsnetz im Sinne des Artikels 2 Buchstabe a der Richtlinie 2002/21/EG,

   b) eine Vorrichtung oder eine Gruppe miteinander verbundener oder zusammenhängender Vorrichtungen, die einzeln oder zu mehreren auf der Grundlage eines Programms die automatische Verarbeitung digitaler Daten durchführen, oder

   c) digitale Daten, die von den — in den Buchstaben a und b genannten — Elementen zum Zwecke ihres Betriebs, ihrer Nutzung, ihres Schutzes und ihrer Pflege gespeichert, verarbeitet, abgerufen oder übertragen werden;

2. „Sicherheit von Netz- und Informationssystemen“ die Fähigkeit von Netz- und Informationssystemen, auf einem bestimmten Vertrauensniveau alle Angriffe abzuwehren, die die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit gespeicherter oder übermittelter oder verarbeiteter Daten oder entsprechender Dienste, die über diese Netz- und Informationssysteme angeboten werden bzw. zugänglich sind, beeinträchtigen;

3. „nationale Strategie für die Sicherheit von Netz- und Informationssystemen“ ein Rahmen mit strategischen Zielen und Prioritäten für die Sicherheit von Netz- und Informationssystemen auf nationaler Ebene;

4. „Betreiber wesentlicher Dienste“ eine öffentliche oder private Einrichtung einer in Anhang II genannten Art, die den Kriterien des Artikels 5 Absatz 2 entspricht;

5. „digitaler Dienst“ einen Dienst im Sinne des Artikels 1 Absatz 1 Buchstabe b der Richtlinie (EU) 2015/1535 des Europäischen Parlaments und des Rates ([1]), der einer in Anhang III genannten Art entspricht;

6. „Anbieter digitaler Dienste“ eine juristische Person, die einen digitalen Dienst anbietet;

7. „Sicherheitsvorfall“ alle Ereignisse, die tatsächlich nachteilige Auswirkungen auf die Sicherheit von Netz- und Informationssystemen haben;

8. „Bewältigung von Sicherheitsvorfällen“ alle Verfahren zur Unterstützung der Erkennung, Analyse und Eindämmung von Sicherheitsvorfällen sowie die Reaktion darauf;

9. „Risiko“ alle mit vernünftigem Aufwand feststellbaren Umstände oder Ereignisse, die potenziell nachteilige Auswirkungen auf die Sicherheit von Netz- und Informationssystemen haben;

10. „Vertreter“ eine in der Union niedergelassene natürliche oder juristische Person, die ausdrücklich benannt wurde, um im Auftrag eines nicht in der Union niedergelassenen Anbieters digitaler Dienste zu handeln, und an die sich eine nationale zuständige Behörde oder ein CSIRT — statt an den Anbieter digitaler Dienste — hinsichtlich der Pflichten dieses Anbieters digitaler Dienste gemäß dieser Richtlinie wenden kann;

11. „Norm“ eine Norm im Sinne des Artikels 2 Nummer 1 der Verordnung (EU) Nr. 1025/2012;

12. „Spezifikation“ eine technische Spezifikation im Sinne des Artikels 2 Nummer 4 der Verordnung (EU) Nr. 1025/2012;

13. „Internet-Knoten“ („IXP“ — Internet Exchange Point) eine Netzeinrichtung, die die Zusammenschaltung von mehr als zwei unabhängigen autonomen Systemen ermöglicht, in erster Linie zur Erleichterung des Austauschs von Internet-Datenverkehr; ein IXP dient nur der Zusammenschaltung autonomer Systeme; ein IXP setzt nicht voraus, dass der Internet-Datenverkehr zwischen zwei beliebigen teilnehmenden autonomen Systemen über ein drittes autonomes System läuft; auch wird der betreffende Datenverkehr weder verändert noch anderweitig beeinträchtigt;

14. „Domain-Namen-System (DNS)“ ein hierarchisch unterteiltes Bezeichnungssystem in einem Netz zur Beantwortung von Anfragen zu Domain-Namen;

([1]) Richtlinie (EU) 2015/1535 des Europäischen Parlaments und des Rates vom 9. September 2015 über ein Informationsverfahren auf dem Gebiet der technischen Vorschriften und der Vorschriften für die Dienste der Informationsgesellschaft (ABl. L 241 vom 17.9.2015, S. 1).

15. „DNS-Diensteanbieter“ eine Einrichtung, die DNS-Dienste im Internet anbietet;

16. „Top-Level-Domain-Name-Registry“ eine Einrichtung, die die Registrierung von Internet-Domain-Namen innerhalb einer spezifischen Top-Level-Domain (TLD) verwaltet und betreibt;

17. „Online-Marktplatz“ einen digitalen Dienst, der es Verbrauchern und/oder Unternehmern im Sinne des Artikels 4 Absatz 1 Buchstabe a bzw. Buchstabe b der Richtlinie 2013/11/EU des Europäischen Parlaments und des Rates ([1]) ermöglicht, Online-Kaufverträge oder Online-Dienstleistungsverträge mit Unternehmern entweder auf der Website des Online-Marktplatzes oder auf der Website eines Unternehmers, die von dem Online-Marktplatz bereitgestellte Rechendienste verwendet, abzuschließen;

18. „Online-Suchmaschine“ einen digitalen Dienst, der es Nutzern ermöglicht, Suchen grundsätzlich auf allen Websites oder auf Websites in einer bestimmten Sprache anhand einer Abfrage zu einem beliebigen Thema in Form eines Stichworts, einer Wortgruppe oder einer anderen Eingabe vorzunehmen, und der daraufhin Links anzeigt, über die Informationen im Zusammenhang mit dem angeforderten Inhalt gefunden werden können;

19. „Cloud-Computing-Dienst“ einen digitalen Dienst, der den Zugang zu einem skalierbaren und elastischen Pool gemeinsam nutzbarer Rechenressourcen ermöglicht.

Artikel 5

Ermittlung der Betreiber wesentlicher Dienste

(1) Die Mitgliedstaaten ermitteln bis zum 9. November 2018 für jeden in Anhang II genannten Sektor und Teilsektor die Betreiber wesentlicher Dienste mit einer Niederlassung in ihrem Hoheitsgebiet.

(2) Die in Artikel 4 Nummer 4 genannten Kriterien zur Ermittlung von Betreibern wesentlicher Dienste sind folgende:

a) Eine Einrichtung stellt einen Dienst bereit, der für die Aufrechterhaltung kritischer gesellschaftlicher und/oder wirtschaftlicher Tätigkeiten unerlässlich ist;

b) die Bereitstellung dieses Dienstes ist abhängig von Netz- und Informationssystemen; und

c) ein Sicherheitsvorfall würde eine erhebliche Störung bei der Bereitstellung dieses Dienstes bewirken.

(3) Für die Zwecke des Absatzes 1 erstellt jeder Mitgliedstaat eine Liste der in Absatz 2 Buchstabe a genannten Dienste.

(4) Stellt eine Einrichtung einen in Absatz 2 Buchstabe a genannten Dienst in zwei oder mehr Mitgliedstaaten bereit, so nehmen diese Mitgliedstaaten für die Zwecke des Absatzes 1 Konsultationen miteinander auf. Diese Konsultation erfolgt, bevor eine Entscheidung über die Ermittlung getroffen wird.

(5) Die Mitgliedstaaten überprüfen die Liste der ermittelten Betreiber wesentlicher Dienste regelmäßig, mindestens jedoch alle zwei Jahre nach dem 9. Mai 2018, und aktualisieren diese gegebenenfalls.

(6) Im Einklang mit den in Artikel 11 genannten Aufgaben hat die Kooperationsgruppe die Aufgabe, die Mitgliedstaaten dabei zu unterstützen, einen einheitlichen Ansatz für die Ermittlung der Betreiber wesentlicher Dienste zu verfolgen.

(7) Für die Zwecke der Überprüfung gemäß Artikel 23 übermitteln die Mitgliedstaaten bis zum 9. November 2018 und danach alle zwei Jahre der Kommission die Informationen, die sie benötigt, um die Umsetzung dieser Richtlinie zu bewerten, insbesondere ob die Mitgliedstaaten bei der Ermittlung der Betreiber wesentlicher Dienste einen einheitlichen Ansatz verfolgen. Diese Informationen müssen mindestens Folgendes umfassen:

a) die nationalen Maßnahmen zur Ermittlung der Betreiber wesentlicher Dienste;

([1]) Richtlinie 2013/11/EU des Europäischen Parlaments und des Rates vom 21. Mai 2013 über die alternative Beilegung verbraucherrechtlicher Streitigkeiten und zur Änderung der Verordnung (EG) Nr. 2006/2004 und der Richtlinie 2009/22/EG (Richtlinie über alternative Streitbeilegung in Verbraucherangelegenheiten) (ABl. L 165 vom 18.6.2013, S. 63).

b) die Liste der Dienste gemäß Absatz 3;

c) die Zahl der Betreiber wesentlicher Dienste, die in jedem der in Anhang II genannten Sektoren ermittelt werden, und einen Hinweis auf ihre Bedeutung für den jeweiligen Sektor;

d) soweit vorhanden, Schwellenwerte zur Bestimmung des einschlägigen Versorgungsgrads unter Bezugnahme auf die Zahl der Nutzer, die den jeweiligen Dienst gemäß Artikel 6 Absatz 1 Buchstabe a in Anspruch nehmen oder unter Bezugnahme auf die Bedeutung des betreffenden Betreibers wesentlicher Dienste gemäß Artikel 6 Absatz 1 Buchstabe f.

Um zur Bereitstellung vergleichbarer Informationen beizutragen, kann die Kommission — unter größtmöglicher Berücksichtigung der Stellungnahme der ENISA — geeignete technische Leitlinien zu den Parametern für die in diesem Absatz genannten Informationen festlegen.

Artikel 6

Erhebliche Störung

(1) Bei der Bestimmung des Ausmaßes einer Störung gemäß Artikel 5 Absatz 2 Buchstabe c berücksichtigen die Mitgliedstaaten mindestens die folgenden sektorübergreifenden Faktoren:

a) Zahl der Nutzer, die den von der jeweiligen Einrichtung angebotenen Dienst in Anspruch nehmen;

b) Abhängigkeit anderer in Anhang II genannter Sektoren von dem von dieser Einrichtung angebotenen Dienst;

c) mögliche Auswirkungen von Sicherheitsvorfällen — hinsichtlich Ausmaß und Dauer — auf wirtschaftliche und gesellschaftliche Tätigkeiten oder die öffentliche Sicherheit;

d) Marktanteil dieser Einrichtung;

e) geografische Ausbreitung des Gebiets, das von einem Sicherheitsvorfall betroffen sein könnte;

f) Bedeutung der Einrichtung für die Aufrechterhaltung des Dienstes in ausreichendem Umfang, unter Berücksichtigung der Verfügbarkeit von alternativen Mitteln für die Bereitstellung des jeweiligen Dienstes.

(2) Bei der Bestimmung, ob ein Sicherheitsvorfall eine erhebliche Störung bewirken würde, berücksichtigen die Mitgliedstaaten gegebenenfalls auch sektorspezifische Faktoren.

KAPITEL II

NATIONALE RAHMEN FÜR DIE SICHERHEIT VON NETZ- UND INFORMATIONSSYSTEMEN

Artikel 7

Nationale Strategie für die Sicherheit von Netz- und Informationssystemen

(1) Jeder Mitgliedstaat legt eine nationale Strategie für die Sicherheit von Netz- und Informationssystemen fest, in der die strategischen Ziele und angemessene Politik- und Regulierungsmaßnahmen bestimmt werden, mit denen ein hohes Sicherheitsniveau von Netz- und Informationssystemen erreicht und aufrechterhalten werden soll, und die mindestens die in Anhang II genannten Sektoren und die in Anhang III genannten Dienste abdeckt. Die nationale Strategie für die Sicherheit von Netz-und Informationssystemen behandelt insbesondere die folgenden Aspekte:

a) die Ziele und Prioritäten der nationalen Strategie für die Sicherheit von Netz- und Informationssystemen;

b) einen Steuerungsrahmen zur Erreichung der Ziele und Prioritäten der nationalen Strategie für die Sicherheit von Netz- und Informationssystemen, einschließlich der Aufgaben und Zuständigkeiten der staatlichen Stellen und der anderen einschlägigen Akteure;

c) die Bestimmung von Maßnahmen zur Abwehrbereitschaft, Reaktion und Wiederherstellung, einschließlich der Zusammenarbeit zwischen dem öffentlichen und dem privaten Sektor;

d) eine Aufstellung der Ausbildungs-, Aufklärungs- und Schulungsprogramme im Zusammenhang mit der nationalen Strategie für die Sicherheit von Netz- und Informationssystemen;

e) eine Angabe der Forschungs- und Entwicklungspläne im Zusammenhang mit der nationalen Strategie für die Sicherheit von Netz- und Informationssystemen;

f) einen Risikobewertungsplan zur Bestimmung von Risiken;

g) eine Liste der verschiedenen Akteure, die an der Umsetzung der nationalen Strategie für die Sicherheit von Netz- und Informationssystemen beteiligt sind.

(2) Die Mitgliedstaaten können die ENISA um Unterstützung bei der Ausarbeitung der nationalen Strategien für die Sicherheit von Netz- und Informationssystemen ersuchen.

(3) Die Mitgliedstaaten teilen ihre nationalen Strategien für die Sicherheit von Netz- und Informationssystemen der Kommission innerhalb von drei Monaten nach ihrer Festlegung mit. Dabei können die Mitgliedstaaten die Elemente der Strategie, die die nationale Sicherheit berühren, ausklammern.

Artikel 8

Nationale zuständige Behörden und zentrale Anlaufstelle

(1) Jeder Mitgliedstaat benennt eine oder mehrere für die Sicherheit von Netz- und Informationssystemen zuständige nationale Behörden (im Folgenden „zuständige Behörde“), die mindestens die in Anhang II genannten Sektoren und die in Anhang III genannten Dienste abdecken. Die Mitgliedstaaten können diese Funktion einer oder mehreren bereits bestehenden Behörden zuweisen.

(2) Die zuständigen Behörden überwachen die Anwendung dieser Richtlinie auf nationaler Ebene.

(3) Jeder Mitgliedstaat benennt eine für die Sicherheit von Netz- und Informationssystemen zuständige nationale zentrale Anlaufstelle (im Folgenden „zentrale Anlaufstelle“). Die Mitgliedstaaten können diese Funktion einer bestehenden Behörde zuweisen. Benennt ein Mitgliedstaat nur eine zuständige Behörde, so ist diese zuständige Behörde auch die zentrale Anlaufstelle.

(4) Die zentrale Anlaufstelle dient als Verbindungsstelle zur Gewährleistung der grenzüberschreitenden Zusammenarbeit der Behörden der Mitgliedstaaten und der Zusammenarbeit mit den entsprechenden Behörden in anderen Mitgliedsaaten sowie mit der in Artikel 11 genannten Kooperationsgruppe und dem in Artikel 12 genannten CSIRTs-Netzwerk.

(5) Die Mitgliedstaaten gewährleisten, dass die zuständigen Behörden und zentralen Anlaufstellen mit angemessenen Ressourcen ausgestattet sind, damit sie die ihnen übertragenen Aufgaben wirksam und effizient wahrnehmen können und die Ziele dieser Richtlinie somit erreicht werden. Die Mitgliedstaaten stellen eine wirksame, effiziente und sichere Zusammenarbeit der benannten Vertreter in der Kooperationsgruppe sicher.

(6) Die zuständigen Behörden und die zentrale Anlaufstelle konsultieren gegebenenfalls und nach Maßgabe des nationalen Rechts die zuständigen nationalen Strafverfolgungsbehörden und nationalen Datenschutzbehörden und arbeiten mit ihnen zusammen.

(7) Die Mitgliedstaaten teilen der Kommission unverzüglich die Benennung der zuständigen Behörde und der zentralen Anlaufstelle, deren Aufgaben sowie etwaige spätere Änderungen dieser Angaben mit. Die Mitgliedstaaten machen die Benennung der zuständigen Behörde und der zentralen Anlaufstelle öffentlich bekannt. Die Kommission veröffentlicht eine Liste der benannten zentralen Anlaufstellen.

Artikel 9

Computer-Notfallteams (CSIRTs)

(1) Jeder Mitgliedstaat benennt ein oder mehrere CSIRTs, die die Anforderungen des Anhangs I Nummer 1 erfüllen und mindestens die in Anhang II genannten Sektoren und die in Anhang III genannten Dienste abdecken und die für die Bewältigung von Risiken und Vorfällen nach einem genau festgelegten Ablauf zuständig sind. Ein CSIRT kann innerhalb einer zuständigen Behörde eingerichtet werden.

(2) Die Mitgliedstaaten gewährleisten, dass die CSIRTs mit angemessenen Ressourcen ausgestattet sind, damit sie ihre in Anhang I Nummer 2 aufgeführten Aufgaben wirksam erfüllen können.

Die Mitgliedstaaten stellen sicher, dass ihre CSIRTs in dem in Artikel 12 genannten CSIRTs-Netzwerk wirksam, effizient und sicher zusammenarbeiten.

(3) Die Mitgliedstaaten stellen sicher, dass ihre CSIRTs Zugang zu einer angemessenen, sicheren und robusten Kommunikations- und Informationsinfrastruktur auf nationaler Ebene haben.

(4) Die Mitgliedstaaten unterrichten die Kommission über den Zuständigkeitsbereich der CSIRTs sowie über die wichtigsten Elemente der Verfahren ihrer CSIRTs zur Bewältigung von Sicherheitsvorfällen.

(5) Die Mitgliedstaaten können die ENISA um Unterstützung bei der Einsetzung nationaler CSIRTs ersuchen.

Artikel 10

Zusammenarbeit auf nationaler Ebene

(1) Handelt es sich bei der zuständigen Behörde, der zentralen Anlaufstelle und dem CSIRT desselben Mitgliedstaats um getrennte Einrichtungen, so arbeiten sie bei der Erfüllung der in dieser Richtlinie festgelegten Pflichten zusammen.

(2) Die Mitgliedstaaten stellen sicher, dass entweder die zuständigen Behörden oder die CSIRTs die gemäß dieser Richtlinie übermittelten Meldungen von Sicherheitsvorfällen erhalten. Entscheidet ein Mitgliedstaat, dass die CSIRTs keine Meldungen erhalten, so wird den CSIRTs in dem zur Erfüllung ihrer Aufgaben erforderlich Umfang Zugang zu den Daten über Sicherheitsvorfälle gewährt, die von Betreibern wesentlicher Dienste gemäß Artikel 14 Absätze 3 und 5 oder von Anbietern digitaler Dienste gemäß Artikel 16 Absätze 3 und 6 gemeldet werden.

(3) Die Mitgliedstaaten stellen sicher, dass die zuständigen Behörden oder die CSIRTs die zentralen Anlaufstellen über die gemäß dieser Richtlinie übermittelten Meldungen von Sicherheitsvorfällen unterrichten.

Bis zum 9. August 2018 und danach jährlich legt die zentrale Anlaufstelle der Kooperationsgruppe einen zusammenfassenden Bericht über die eingegangenen Meldungen, einschließlich der Zahl der Meldungen und der Art der gemeldeten Sicherheitsvorfälle, und über die gemäß Artikel 14 Absätze 3 und 5 und Artikel 16 Absätze 3 und 6 ergriffenen Maßnahmen vor.

KAPITEL III

ZUSAMMENARBEIT

Artikel 11

Kooperationsgruppe

(1) Zur Unterstützung und Erleichterung der strategischen Zusammenarbeit sowie des Informationsaustauschs zwischen den Mitgliedstaaten zum Aufbau von Vertrauen und zur Erreichung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union wird eine Kooperationsgruppe eingesetzt.

Die Kooperationsgruppe nimmt ihre Aufgaben auf der Grundlage von zweijährlichen Arbeitsprogrammen gemäß Absatz 3 Unterabsatz 2 wahr.

(2) Die Kooperationsgruppe setzt sich aus Vertretern der Mitgliedstaaten, der Kommission und der ENISA zusammen.

Gegebenenfalls kann die Kooperationsgruppe Vertreter der maßgeblichen Interessengruppen einladen, an ihren Arbeiten teilzunehmen.

Die Sekretariatsgeschäfte werden von der Kommission geführt.

(3) Die Kooperationsgruppe hat folgende Aufgaben:

a) Bereitstellung strategischer Leitlinien für die Tätigkeiten des gemäß Artikel 12 errichteten CSIRTs-Netzwerks;

b) Austausch von bewährten Verfahren über den Informationsaustausch im Zusammenhang mit der Meldung von Sicherheitsvorfällen gemäß Artikel 14 Absätze 3 und 5 sowie Artikel 16 Absätze 3 und 6;

c) Austausch bewährter Verfahren zwischen den Mitgliedstaaten und — in Zusammenarbeit mit der ENISA — Unterstützung der Mitgliedstaaten beim Kapazitätenaufbau zur Gewährleistung der Sicherheit von Netz- und Informationssystemen;

d) Erörterung der Fähigkeiten und der Abwehrbereitschaft der Mitgliedstaaten und Bewertung — auf freiwilliger Basis — der nationalen Strategien für die Sicherheit von Netz- und Informationssystemen und der Wirksamkeit der CSIRTs sowie Bestimmung bewährter Verfahren;

e) Austausch von Informationen und bewährten Verfahren zu Sensibilisierung und Schulung;

f) Austausch von Informationen und bewährten Verfahren zu Forschung und Entwicklung bezüglich der Sicherheit von Netz- und Informationssystemen;

g) gegebenenfalls Erfahrungsaustausch zu Angelegenheiten der Sicherheit von Netz- und Informationssystemen mit den einschlägigen Organen, Einrichtungen und sonstigen Stellen der Union;

h) Erörterung der in Artikel 19 genannten Normen und Spezifikationen mit Vertretern der einschlägigen europäischen Normungsorganisationen;

i) Sammlung von Informationen über bewährte Verfahren bei Risiken und Sicherheitsvorfällen;

j) jährliche Prüfung der in Artikel 10 Absatz 3 Unterabsatz 2 genannten zusammenfassenden Berichte;

k) Erörterung der durchgeführten Arbeiten im Zusammenhang mit Übungen für die Sicherheit von Netz- und Informationssystemen, Ausbildungsprogrammen und Schulung, einschließlich der Arbeit der ENISA;

l) Austausch bewährter Verfahren — mit Unterstützung der ENISA — zur Ermittlung der Betreiber wesentlicher Dienste durch die Mitgliedstaaten, auch im Zusammenhang mit grenzüberschreitenden Abhängigkeiten, im Hinblick auf Risiken und Sicherheitsvorfälle;

m) Erörterung der Modalitäten für die Berichterstattung über die Meldung von Sicherheitsvorfällen gemäß den Artikeln 14 und 16.

Bis spätestens 9. Februar 2018 und danach alle zwei Jahre erstellt die Kooperationsgruppe ein Arbeitsprogramm bezüglich der Maßnahmen, die zur Umsetzung ihrer Ziele und Aufgaben im Einklang mit den Zielen dieser Richtlinie zu ergreifen sind;

(4) Für die Zwecke der Überprüfung gemäß Artikel 23 erstellt die Kooperationsgruppe bis zum 9. August 2018 und danach alle eineinhalb Jahre einen Bericht, in dem die im Rahmen der strategischen Zusammenarbeit nach diesem Artikel gewonnenen Erfahrungen bewertet werden.

(5) Die Kommission erlässt Durchführungsrechtsakte zur Festlegung der Verfahrensmodalitäten, die für das Funktionieren der Kooperationsgruppe erforderlich sind. Diese Durchführungsrechtsakte werden nach dem in Artikel 22 Absatz 2 genannten Prüfverfahren erlassen.

Für die Zwecke des Unterabsatzes 1 legt die Kommission dem in Artikel 22 Absatz 1 genannten Ausschuss den ersten Entwurf eines Durchführungsrechtsakts spätestens am 9. Februar 2017 vor.

Artikel 12

CSIRTs-Netzwerk

(1) Um zum Aufbau von Vertrauen zwischen den Mitgliedstaaten beizutragen und eine rasche und wirksame operative Zusammenarbeit zu fördern, wird ein Netzwerk der nationalen CSIRTs errichtet.

(2) Das CSIRTs-Netzwerk setzt sich aus Vertretern der CSIRTs der Mitgliedstaaten und des CERT-EU zusammen. Die Kommission nimmt als Beobachter am CSIRTs-Netzwerk teil. Die ENISA führt die Sekretariatsgeschäfte und unterstützt aktiv die Zusammenarbeit zwischen den CSIRTs.

(3) Das CSIRTs-Netzwerk hat folgende Aufgaben:

a) Informationsaustausch zu den Diensten, Tätigkeiten und Kooperationsfähigkeiten der CSIRTs;

b) auf Antrag des Vertreters eines CSIRT eines von einem Sicherheitsvorfall potenziell betroffenen Mitgliedstaats Austausch und Erörterung von wirtschaftlich nicht sensiblen Informationen im Zusammenhang mit diesem Vorfall und damit verbundenen Risiken; das CSIRT eines jeden Mitgliedstaats kann jedoch die Beteiligung an diesen Erörterungen ablehnen, wenn die Gefahr einer Beeinträchtigung der Untersuchung des Vorfalls besteht;

c) Austausch und Bereitstellung auf freiwilliger Basis von nicht vertraulichen Informationen zu einzelnen Sicherheitsvorfällen;

d) auf Antrag des Vertreters des CSIRT eines Mitgliedstaats Erörterung und — sofern möglich — Ausarbeitung einer koordinierten Reaktion auf einen Sicherheitsvorfall, der im Gebiet dieses Mitgliedstaats festgestellt wurde;

e) Unterstützung der Mitgliedstaaten bei der Bewältigung grenzüberschreitender Sicherheitsvorfälle auf der Grundlage einer freiwilligen gegenseitigen Unterstützung;

f) Erörterung, Sondierung und Bestimmung weiterer Formen der operativen Zusammenarbeit, unter anderem im Zusammenhang mit

   i) Kategorien von Risiken und Sicherheitsvorfällen,

   ii) Frühwarnungen,

   iii) gegenseitiger Unterstützung,

   iv) Grundsätzen und Modalitäten der Koordinierung bei der Reaktion der Mitgliedstaaten auf grenzüberschreitende Risiken und Vorfälle;

g) Unterrichtung der Kooperationsgruppe über seine Tätigkeiten und über die gemäß Buchstabe f erörterten weiteren Formen der operativen Zusammenarbeit und Ersuchen um Leitlinien dafür;

h) Erörterung der aus den Übungen zur Sicherheit von Netz- und Informationssystemen — auch den von der ENISA organisierten derartigen Übungen — gezogenen Lehren;

i) auf Antrag eines einzelnen CSIRT Erörterung der Fähigkeiten und der Abwehrbereitschaft dieses CSIRT;

j) Erstellung von Leitlinien zur Erleichterung der Konvergenz der operativen Verfahrensweisen in Bezug auf die Anwendung der Bestimmungen dieses Artikels betreffend die operative Zusammenarbeit.

(4) Für die Zwecke der Überprüfung gemäß Artikel 23 erstellt das CSIRTs-Netzwerk bis zum 9. August 2018 und danach alle eineinhalb Jahre einen Bericht, in dem die im Rahmen der operativen Zusammenarbeit nach diesem Artikel gewonnenen Erfahrungen, wozu auch Schlussfolgerungen und Empfehlungen gehören, bewertet werden. Dieser Bericht wird auch der Kooperationsgruppe übermittelt.

(5) Das CSIRTs-Netzwerk gibt sich eine Geschäftsordnung.

Artikel 13

Internationale Zusammenarbeit

Die Union kann im Einklang mit Artikel 218 AEUV internationale Übereinkünfte mit Drittländern oder internationalen Organisationen schließen, in denen deren Beteiligung an bestimmten Tätigkeiten der Kooperationsgruppe ermöglicht und geregelt wird. In solchen Übereinkünften wird der Notwendigkeit zur Gewährleistung eines angemessenen Schutzes von Daten Rechnung getragen.

KAPITEL IV

SICHERHEIT DER NETZ- UND INFORMATIONSSYSTEME DER BETREIBER WESENTLICHER DIENSTE

Artikel 14

Sicherheitsanforderungen und Meldung von Sicherheitsvorfällen

(1) Die Mitgliedstaaten stellen sicher, dass die Betreiber wesentlicher Dienste geeignete und verhältnismäßige technische und organisatorische Maßnahmen ergreifen, um die Risiken für die Sicherheit der Netz- und Informationssysteme, die sie für ihre Tätigkeiten nutzen, zu bewältigen. Diese Maßnahmen müssen unter Berücksichtigung des Stands der Technik ein Sicherheitsniveau der Netz- und Informationssysteme gewährleisten, das dem bestehenden Risiko angemessen ist.

(2) Die Mitgliedstaaten stellen sicher, dass die Betreiber wesentlicher Dienste geeignete Maßnahmen ergreifen, um den Auswirkungen von Sicherheitsvorfällen, die die Sicherheit der von ihnen für die Bereitstellung dieser wesentlichen Dienste genutzten Netz- und Informationssysteme beeinträchtigen, vorzubeugen beziehungsweise diese so gering wie möglich zu halten, damit die Verfügbarkeit dieser Dienste gewährleistet wird.

(3) Die Mitgliedstaaten stellen sicher, dass die Betreiber wesentlicher Dienste der zuständigen Behörde oder dem CSIRT Sicherheitsvorfälle, die erhebliche Auswirkungen auf die Verfügbarkeit der von ihnen bereitgestellten wesentlichen Dienste haben, unverzüglich melden. Die Meldungen müssen die Informationen enthalten, die es der zuständigen Behörde oder dem CSIRT ermöglichen, zu bestimmen, ob der Sicherheitsvorfall grenzübergreifende Auswirkungen hat. Mit der Meldung wird keine höhere Haftung der meldenden Partei begründet.

(4) Zur Feststellung des Ausmaßes der Auswirkungen eines Sicherheitsvorfalls werden insbesondere folgende Parameter berücksichtigt:

a) Zahl der von der Unterbrechung der Erbringung des wesentlichen Dienstes betroffenen Nutzer;

b) Dauer des Sicherheitsvorfalls;

c) geografische Ausbreitung in Bezug auf das von dem Sicherheitsvorfall betroffene Gebiet.

(5) Auf der Grundlage der in der Meldung durch den Betreiber wesentlicher Dienste bereitgestellten Informationen unterrichtet die zuständige Behörde oder das CSIRT den bzw. die anderen betroffenen Mitgliedstaaten, sofern der Vorfall erhebliche Auswirkungen auf die Verfügbarkeit wesentlicher Dienste in jenem Mitgliedstaat hat. Dabei wahrt die zuständige Behörde oder das CSIRT im Einklang mit dem Unionsrecht oder mit den dem Unionsrecht entsprechenden nationalen Rechtsvorschriften die Sicherheit und das wirtschaftliche Interesse des Betreibers wesentlicher Dienste sowie die Vertraulichkeit der in dessen Meldung bereitgestellten Informationen.

Wenn es nach den Umständen möglich ist, stellt die zuständige Behörde oder das CSIRT dem die Meldung erstattenden Betreiber wesentlicher Dienste einschlägige Informationen für die weitere Behandlung der Meldung, wie etwa Informationen, die für die wirksame Bewältigung des Sicherheitsvorfalls von Nutzen sein könnten, zur Verfügung.

Auf Ersuchen der zuständigen Behörde oder des CSIRT leitet die zentrale Anlaufstelle die in Unterabsatz 1 genannten Meldungen an die zentralen Anlaufstellen der anderen betroffenen Mitgliedstaaten weiter.

(6) Nach Anhörung des meldenden Betreibers wesentlicher Dienste können die zuständige Behörde oder das CSIRT die Öffentlichkeit über einzelne Sicherheitsvorfälle unterrichten, sofern die Sensibilisierung der Öffentlichkeit zur Verhütung von Sicherheitsvorfällen oder zur Bewältigung aktueller Sicherheitsvorfälle erforderlich ist.

(7) Die im Rahmen der Kooperationsgruppe gemeinsam handelnden zuständigen Behörden können Leitlinien zu den Umständen, unter denen die Betreiber wesentlicher Dienste Sicherheitsvorfälle melden müssen, ausarbeiten und annehmen; dies gilt auch für die Parameter zur Feststellung des Ausmaßes der Auswirkungen eines Sicherheitsvorfalls gemäß Absatz 4.

Artikel 15

Umsetzung und Durchsetzung

(1) Die Mitgliedstaaten stellen sicher, dass die zuständigen Behörden über die Befugnisse und Mittel verfügen, die erforderlich sind, um zu bewerten, ob die Betreiber wesentlicher Dienste ihren Pflichten nach Artikel 14 nachkommen und inwieweit sich dies auf die Sicherheit der Netz- und Informationssysteme auswirkt.

(2) Die Mitgliedstaaten stellen sicher, dass die zuständigen Behörden über die Befugnisse und Mittel verfügen, um von den Betreibern wesentlicher Dienste verlangen zu können, dass sie

a) die zur Bewertung der Sicherheit ihrer Netz- und Informationssysteme erforderlichen Informationen, einschließlich der dokumentierten Sicherheitsmaßnahmen, zur Verfügung stellen;

b) Nachweise für die wirksame Umsetzung der Sicherheitsmaßnahmen zur Verfügung stellen, wie etwa die Ergebnisse einer von der zuständigen Behörde oder einem qualifizierten Prüfer durchgeführten Sicherheitsüberprüfung, und im letztgenannten Fall die Ergebnisse der Überprüfung einschließlich der zugrunde gelegten Nachweise der zuständigen Behörde zur Verfügung stellen.

Bei der Anforderung dieser Informationen oder Nachweise nennt die zuständige Behörde den Zweck und gibt an, welche Informationen verlangt werden.

(3) Im Anschluss an die Bewertung der in Absatz 2 genannten Informationen oder an die Ergebnisse der Sicherheitsüberprüfungen kann die zuständige Behörde den Betreibern wesentlicher Dienste verbindliche Anweisungen zur Abhilfe der festgestellten Mängel erteilen.

(4) Bei der Bearbeitung von Sicherheitsvorfällen, die zur Verletzung des Schutzes personenbezogener Daten führen, arbeitet die zuständige Behörde eng mit den Datenschutzbehörden zusammen.

KAPITEL V

SICHERHEIT DER NETZ- UND INFORMATIONSSYSTEME DER ANBIETER DIGITALER DIENSTE

Artikel 16

Sicherheitsanforderungen und Meldung von Sicherheitsvorfällen

(1) Die Mitgliedstaaten stellen sicher, dass die Anbieter digitaler Dienste geeignete und verhältnismäßige technische und organisatorische Maßnahmen ergreifen, um die Risiken für die Sicherheit der Netz- und Informationssysteme, die sie im Rahmen der Bereitstellung der in Anhang III aufgeführten Dienste innerhalb der Union nutzen, zu bewältigen. Diese Maßnahmen müssen unter Berücksichtigung des Stands der Technik ein Sicherheitsniveau der Netz- und Informationssysteme gewährleisten, das dem bestehenden Risiko angemessen ist, wobei Folgendem Rechnung getragen wird:

a) Sicherheit der Systeme und Anlagen,

b) Bewältigung von Sicherheitsvorfällen,

c) Business continuity management,

d) Überwachung, Überprüfung und Erprobung,

e) Einhaltung der internationalen Normen.

(2) Die Mitgliedstaaten stellen sicher, dass die Anbieter digitaler Dienste Maßnahmen treffen, um den Auswirkungen von Sicherheitsvorfällen, die die Sicherheit ihrer Netze und Informationssysteme beeinträchtigen, auf die in Anhang III genannten, innerhalb der Union erbrachten Dienste vorzubeugen beziehungsweise diese so gering wie möglich zu halten, damit die Verfügbarkeit dieser Dienste gewährleistet wird.

(3) Die Mitgliedstaaten stellen sicher, dass die Anbieter digitaler Dienste der zuständigen Behörde oder dem CSIRT jeden Sicherheitsvorfall, der erhebliche Auswirkungen auf die Bereitstellung eines der in Anhang III genannten, von ihnen innerhalb der Union erbrachten Dienste hat, unverzüglich melden. Die Meldungen müssen die Informationen enthalten, die es der zuständigen Behörde oder dem CSIRT ermöglichen, das Ausmaß etwaiger grenzübergreifender Auswirkungen des Sicherheitsvorfalls festzustellen. Mit der Meldung wird keine höhere Haftung der meldenden Partei begründet.

(4) Zur Feststellung, ob die Auswirkungen eines Sicherheitsvorfalls erheblich sind, werden insbesondere folgende Parameter berücksichtigt:

a) die Zahl der von dem Sicherheitsvorfall betroffenen Nutzer, insbesondere der Nutzer, die den Dienst für die Bereitstellung ihrer eigenen Dienste benötigen;

b) Dauer des Sicherheitsvorfalls;

c) geografische Ausbreitung in Bezug auf das von dem Sicherheitsvorfall betroffene Gebiet;

d) Ausmaß der Unterbrechung der Bereitstellung des Dienstes;

e) Ausmaß der Auswirkungen auf wirtschaftliche und gesellschaftliche Tätigkeiten.

Die Pflicht zur Meldung eines Sicherheitsvorfalls gilt nur, wenn der Anbieter digitaler Dienste Zugang zu den Informationen hat, die benötigt werden, um die Auswirkung eines Sicherheitsvorfalls gemessen an den Parametern gemäß Unterabsatz 1 zu bewerten.

(5) Nimmt ein Betreiber wesentlicher Dienste für die Bereitstellung eines Dienstes, der für die Aufrechterhaltung kritischer gesellschaftlicher oder wirtschaftlicher Tätigkeiten von wesentlicher Bedeutung ist, die Dienste eines Dritten als Anbieter digitaler Dienste in Anspruch, so ist jede erhebliche Auswirkung auf die Verfügbarkeit der wesentlichen Dienste, die von einem den Anbieter digitaler Dienste beeinträchtigenden Sicherheitsvorfall verursacht wurde, von diesem Betreiber zu melden.

(6) Gegebenenfalls und insbesondere, wenn der in Absatz 3 genannte Sicherheitsvorfall zwei oder mehr Mitgliedstaaten betrifft, unterrichtet die zuständige Behörde oder das CSIRT, der bzw. dem die Meldung erstattet wurde, die anderen betroffenen Mitgliedstaaten. Dabei wahren die zuständigen Behörden, die CSIRTs und die zentralen Anlaufstellen im Einklang mit dem Unionsrecht oder mit den dem Unionsrecht entsprechenden nationalen Rechtsvorschriften die Sicherheit und das wirtschaftliche Interesse des Anbieters digitaler Dienste sowie die Vertraulichkeit der bereitgestellten Informationen.

(7) Nach Anhörung des betreffenden Anbieters digitaler Dienste können die zuständige Behörde oder das CSIRT, der bzw. dem die Meldung erstattet wurde, und gegebenenfalls die Behörden oder die CSIRTs anderer betroffener Mitgliedstaaten die Öffentlichkeit über einzelne Sicherheitsvorfälle unterrichten oder verlangen, dass der Anbieter digitaler Dienste dies unternimmt, sofern die Sensibilisierung der Öffentlichkeit zur Verhütung von Sicherheitsvorfällen oder zur Bewältigung aktueller Sicherheitsvorfälle erforderlich ist, oder wenn die Offenlegung des Sicherheitsvorfalls auf sonstige Weise im öffentlichen Interesse liegt.

(8) Die Kommission erlässt Durchführungsrechtsakte, um die in Absatz 1 genannten Elemente und die in Absatz 4 aufgeführten Parameter genauer zu bestimmen. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 22 Absatz 2 genannten Prüfverfahren bis zum 9. August 2017 erlassen.

(9) Die Kommission kann Durchführungsrechtsakte zur Festlegung der Form und des Verfahrens, welche für Meldepflichten gelten, erlassen. Diese Durchführungsrechtsakte werden nach dem in Artikel 22 Absatz 2 genannten Prüfverfahren erlassen.

(10) Die Mitgliedstaaten erlegen unbeschadet des Artikels 1 Absatz 6 den Anbietern digitaler Dienste keine weiteren Sicherheits- oder Meldepflichten auf.

(11) Kapitel V gilt nicht für Kleinstunternehmen und kleine Unternehmen im Sinne der Empfehlung 2003/361/EG der Kommission ([1]).

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

Artikel 17

Umsetzung und Durchsetzung

(1) Die Mitgliedstaaten stellen sicher, dass die zuständigen Behörden erforderlichenfalls im Wege von Ex-post-Überwachungsmaßnahmen tätig werden, wenn ihnen Nachweise dafür vorlegt werden, dass ein Anbieter digitaler Dienste die in Artikel 16 niedergelegten Anforderungen nicht einhält. Derartige Nachweise können von der zuständigen Behörde eines anderen Mitgliedstaats, in dem der Dienst bereitgestellt wird, vorgelegt werden.

(2) Für die Zwecke des Absatzes 1 müssen die zuständigen Behörden über die erforderlichen Befugnisse und Mittel verfügen, um von den Anbietern digitaler Dienste zu verlangen,

a) die zur Beurteilung der Sicherheit ihrer Netz- und Informationssysteme erforderlichen Informationen, einschließlich der nachweislichen Sicherheitsmaßnahmen, zur Verfügung zu stellen;

b) bei jedem Fall von Nichteinhaltung der in Artikel 16 niedergelegten Anforderungen Abhilfe zu schaffen.

(3) Hat ein Anbieter digitaler Dienste seine Hauptniederlassung oder einen Vertreter in einem Mitgliedstaat, aber seine Netz- und Informationssysteme befinden sich in einem oder mehreren anderen Mitgliedstaaten, so arbeiten die zuständige Behörde des Mitgliedstaats der Hauptniederlassung oder des Vertreters und die zuständigen Behörden der betreffenden anderen Mitgliedstaaten zusammen und unterstützen einander. Diese Unterstützung und Zusammenarbeit kann den Informationsaustausch zwischen den betreffenden zuständigen Behörden und das Ersuchen umfassen, die in Absatz 2 genannten Überwachungsmaßnahmen zu ergreifen.

Artikel 18

Gerichtliche Zuständigkeit und Territorialität

(1) Für die Zwecke dieser Richtlinie gilt, dass ein Anbieter digitaler Dienste der gerichtlichen Zuständigkeit des Mitgliedstaats unterliegt, in dem er seine Hauptniederlassung hat. Es gilt, dass ein Anbieter digitaler Dienste seine Hauptniederlassung in einem Mitgliedstaat hat, wenn er seinen Hauptsitz in diesem Mitgliedstaat hat.

(2) Ein Anbieter digitaler Dienste, der nicht in der Union niedergelassen ist, aber innerhalb der Union in Anhang III aufgeführte Dienste bereitstellt, benennt einen Vertreter in der Union. Der Vertreter muss in einem der Mitgliedstaaten niedergelassen sein, in denen die Dienste angeboten werden. Es gilt, dass ein Anbieter digitaler Dienste der gerichtlichen Zuständigkeit des Mitgliedstaats unterliegt, in dem der Vertreter niedergelassen ist.

(3) Die Benennung eines Vertreters durch den Anbieter digitaler Dienste erfolgt unbeschadet etwaiger rechtlicher Schritte gegen den Anbieter digitaler Dienste.

KAPITEL VI

NORMUNG UND FREIWILLIGE MELDUNG

Artikel 19

Normung

(1) Um eine einheitliche Anwendung des Artikels 14 Absätze 1 und 2 und des Artikels 16 Absätze 1 und 2 zu gewährleisten, fördern die Mitgliedstaaten ohne Auferlegung oder willkürliche Bevorzugung der Verwendung einer bestimmten Technologieart die Anwendung europäischer oder international anerkannter Normen und Spezifikationen für die Sicherheit von Netz- und Informationssystemen.

(2) In Zusammenarbeit mit den Mitgliedstaaten bietet die ENISA Beratung und erlässt Leitlinien zu den technischen Bereichen, die in Bezug auf Absatz 1 in Betracht zu ziehen sind, sowie zu den bereits bestehenden Normen — einschließlich der nationalen Normen der Mitgliedstaaten —, mit denen diese Bereiche abgedeckt werden könnten.

Artikel 20

Freiwillige Meldung

(1) Unbeschadet des Artikels 3 können Einrichtungen, die nicht als Betreiber wesentlicher Dienste ermittelt wurden und die keine Anbieter digitaler Dienste sind, auf freiwilliger Basis Sicherheitsvorfälle melden, die erhebliche Auswirkungen auf die Verfügbarkeit der von ihnen angebotenen Dienste haben.

(2) Bei der Bearbeitung dieser Meldungen werden die Mitgliedstaaten gemäß dem in Artikel 14 vorgesehenen Verfahren tätig. Die Mitgliedstaaten können Pflichtmeldungen vorrangig vor freiwilligen Meldungen bearbeiten. Freiwillige Meldungen werden nur bearbeitet, wenn diese Bearbeitung keinen unverhältnismäßigen oder unzumutbaren Aufwand für die betreffenden Mitgliedstaaten darstellt.

Eine freiwillige Meldung darf nicht dazu führen, dass der meldenden Einrichtung Pflichten auferlegt werden, die nicht für sie gegolten hätten, wenn sie den Vorfall nicht gemeldet hätte.

KAPITEL VII

SCHLUSSBESTIMMUNGEN

Artikel 21

Sanktionen

Die Mitgliedstaaten erlassen Vorschriften über Sanktionen für Verstöße gegen die nach dieser Richtlinie erlassenen nationalen Bestimmungen und treffen alle erforderlichen Maßnahmen, um deren Anwendung sicherzustellen. Die vorgesehenen Sanktionen müssen wirksam, angemessen und abschreckend sein. Die Mitgliedstaaten teilen der Kommission diese Vorschriften und Maßnahmen bis zum 9. Mai 2018 mit und melden ihr unverzüglich etwaige spätere Änderungen.

Artikel 22

Ausschussverfahren

(1) Die Kommission wird von dem Ausschuss für die Sicherheit von Netz- und Informationssystemen unterstützt. Dieser Ausschuss ist ein Ausschuss im Sinne der Verordnung (EU) Nr. 182/2011.

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

Artikel 23

Überprüfung

(1) Die Kommission legt dem Europäischen Parlament und dem Rat bis zum 9. Mai 2019 einen Bericht vor, in dem die Kohärenz der Ansätze der Mitgliedstaaten für die Ermittlung der Betreiber wesentlicher Dienste bewertet wird.

(2) Die Kommission überprüft regelmäßig die Anwendung dieser Richtlinie und erstattet dem Europäischen Parlament und dem Rat Bericht. Zu diesem Zweck berücksichtigt die Kommission im Hinblick auf die weitere Förderung der strategischen und operativen Zusammenarbeit die Berichte der Kooperationsgruppe und des CSIRTs-Netzwerks über die auf strategischer und operativer Ebene gemachten Erfahrungen. Bei ihrer Überprüfung bewertet die Kommission ferner die in den Anhängen II und III enthaltenen Listen und die Kohärenz bei der Ermittlung der Betreiber wesentlicher Dienste und der Dienste in den in Anhang II genannten Sektoren. Der erste Bericht wird bis zum 9. Mai 2021 vorgelegt.

Artikel 24

Übergangsmaßnahmen

(1) Unbeschadet des Artikels 25 beginnen die Kooperationsgruppe und das CSIRTs-Netzwerk mit der Erfüllung ihrer in Artikel 11 Absatz 3 beziehungsweise Artikel 12 Absatz 3 niedergelegten Aufgaben bis zum 9. Februar 2017 mit dem Ziel, den Mitgliedstaaten weitere Optionen für eine angemessene Zusammenarbeit während des Übergangszeitraums zu ermöglichen.

(2) Im Zeitraum vom 9. Februar 2017 bis zum 9. November 2018 erörtert die Kooperationsgruppe im Hinblick auf die Unterstützung der Mitgliedstaaten bei einem kohärenten Ansatz für den Prozess der Ermittlung der Betreiber wesentlicher Dienste das Verfahren, den Inhalt und die Art der nationalen Maßnahmen, die die Ermittlung der Betreiber wesentlicher Dienste in einem spezifischen Sektor gemäß den in den Artikeln 5 und 6 festgelegten Kriterien gestatten. Die Kooperationsgruppe erörtert ferner auf Ersuchen eines Mitgliedstaats einen Entwurf spezifischer nationaler Maßnahmen dieses Mitgliedstaats, die die Ermittlung von Betreibern wesentlicher Dienste in einem spezifischen Sektor gemäß den in den Artikeln 5 und 6 festgelegten Kriterien gestatten.

(3) Bis zum 9. Februar 2017 sorgen die Mitgliedstaaten für die Zwecke dieses Artikels für ihre angemessene Vertretung in der Kooperationsgruppe und im CSIRTs-Netzwerk.

Artikel 25

Umsetzung

(1) Die Mitgliedstaaten erlassen und veröffentlichen bis zum 9. Mai 2018 die Rechts- und Verwaltungsvorschriften, die erforderlich sind, um dieser Richtlinie nachzukommen. Sie setzen die Kommission unverzüglich davon in Kenntnis.

Sie wenden diese Maßnahmen ab dem 10. Mai 2018 an.

Bei Erlass dieser Vorschriften nehmen die Mitgliedstaaten in den Vorschriften selbst oder durch einen Hinweis bei der amtlichen Veröffentlichung auf diese Richtlinie Bezug. Die Mitgliedstaaten regeln die Einzelheiten dieser Bezugnahme.

(2) Die Mitgliedstaaten teilen der Kommission den Wortlaut der wichtigsten nationalen Rechtsvorschriften mit, die sie auf dem unter diese Richtlinie fallenden Gebiet erlassen.

Artikel 26

Inkrafttreten

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

Artikel 27

Adressaten

Diese Richtlinie ist an die Mitgliedstaaten gerichtet.

Geschehen zu Straßburg am 6. Juli 2016.

Im Namen des Europäischen Parlaments	*Im Namen des Rates*
Der Präsident	*Der Präsident*
M. SCHULZ	I. KORČOK

ANHANG I

COMPUTER SECURITY INCIDENT RESPONSE TEAMS (CSIRTs) — ANFORDERUNGEN UND AUFGABEN

Die Anforderungen an CSIRTs und ihre Aufgaben werden angemessen und genau festgelegt und durch nationale Strategien und/oder Vorschriften gestützt. Sie müssen Folgendes umfassen:

1. Anforderungen an CSIRTs

   a) CSIRTs sorgen für einen hohen Grad der Verfügbarkeit ihrer Kommunikationsdienste, indem sie punktuellen Ausfällen vorbeugen und mehrere Kanäle bereitstellen, damit sie jederzeit erreichbar bleiben und selbst Kontakt aufnehmen können. Die Kommunikationskanäle müssen zudem genau spezifiziert und den CSIRT-Nutzern („Constituency“) und den Kooperationspartnern wohlbekannt sein.

   b) Die Räumlichkeiten der CSIRTs und die unterstützenden Informationssysteme werden an sicheren Standorten eingerichtet.

   c) Betriebskontinuität:

      i) CSIRTs müssen über ein geeignetes System zur Verwaltung und Weiterleitung von Anfragen verfügen, um Übergaben zu erleichtern.

      ii) CSIRTs müssen personell so ausgestattet sein, dass sie eine ständige Bereitschaft gewährleisten können.

      iii) CSIRTs müssen auf eine Infrastruktur gestützt sein, deren Verfügbarkeit sichergestellt ist. Zu diesem Zweck müssen Redundanzsysteme und Ausweicharbeitsräume zur Verfügung stehen.

   d) CSIRTs müssen die Möglichkeit haben, sich an internationalen Kooperationsnetzen zu beteiligen, wenn sie es wünschen.

2. Aufgaben der CSIRTs

   a) Die Aufgaben der CSIRTs umfassen mindestens Folgendes:

      i) Überwachung von Sicherheitsvorfällen auf nationaler Ebene;

      ii) Ausgabe von Frühwarnungen und Alarmmeldungen sowie Bekanntmachung und Verbreitung von Informationen über Risiken und Vorfälle unter den einschlägigen Interessenträgern;

      iii) Reaktion auf Sicherheitsvorfälle;

      iv) dynamische Analyse von Risiken und Vorfällen und Lagebeurteilung;

      v) Beteiligung am CSIRTs-Netzwerk.

   b) CSIRTs bauen Kooperationsbeziehungen zum Privatsektor auf.

   c) Zur Erleichterung der Zusammenarbeit fördern CSIRTs die Annahme und Anwendung gemeinsamer oder standardisierter Verfahren für:

      i) Abläufe zur Bewältigung von Sicherheitsvorfällen und Risiken;

      ii) Systeme zur Klassifizierung von Sicherheitsvorfällen, Risiken und Informationen.

ANHANG II

ARTEN VON EINRICHTUNGEN FÜR DIE ZWECKE DES ARTIKELS 4 NUMMER 4

Sektor	Teilsektor	Art der Einrichtung
1. Energie	a) Elektrizität	— Elektrizitätsunternehmen im Sinne des Artikels 2 Nummer 35 der Richtlinie 2009/72/EG des Europäischen Parlaments und des Rates ([1]), die die Funktion „Versorgung" im Sinne des Artikels 2 Nummer 19 jener Richtlinie wahrnehmen
		— Verteilernetzbetreiber im Sinne des Artikels 2 Nummer 6 der Richtlinie 2009/72/EG
		— Übertragungsnetzbetreiber im Sinne des Artikels 2 Nummer 4 der Richtlinie 2009/72/EG
	b) Erdöl	— Betreiber von Erdöl-Fernleitungen
		— Betreiber von Anlagen zur Produktion, Raffination und Aufbereitung von Erdöl sowie Betreiber von Erdöllagern und Erdöl-Fernleitungen
	c) Erdgas	— Versorgungsunternehmen im Sinne des Artikels 2 Nummer 8 der Richtlinie 2009/73/EG des Europäischen Parlaments und des Rates ([2]);
		— Verteilernetzbetreiber im Sinne des Artikels 2 Nummer 6 der Richtlinie 2009/73/EG
		— Fernleitungsnetzbetreiber im Sinne des Artikels 2 Nummer 4 der Richtlinie 2009/73/EG
		— Betreiber einer Speicheranlage im Sinne des Artikels 2 Nummer 10 der Richtlinie 2009/73/EG
		— Betreiber einer LNG-Anlage im Sinne des Artikels 2 Nummer 12 der Richtlinie 2009/73/EG
		— Erdgasunternehmen im Sinne des Artikels 2 Nummer 1 der Richtlinie 2009/73/EG
		— Betreiber von Anlagen zur Raffination und Aufbereitung von Erdgas
2. Verkehr	a) Luftverkehr	— Luftfahrtunternehmen im Sinne des Artikels 3 Nummer 4 der Verordnung (EG) Nr. 300/2008 des Europäischen Parlaments und des Rates ([3])
		— Flughafenleitungsorgane im Sinne des Artikels 2 Nummer 2 der Richtlinie 2009/12/EG des Europäischen Parlaments und des Rates ([4]), Flughäfen im Sinne des Artikels 2 Nummer 1 jener Richtlinie, einschließlich der in Anhang II Abschnitt 2 der Verordnung (EU) Nr. 1315/2013 des Europäischen Parlaments und des Rates ([5]) aufgeführten Flughäfen des Kernnetzes, und Einrichtungen, die innerhalb von Flughäfen befindliche zugehörige Einrichtungen betreiben

Sektor	Teilsektor	Art der Einrichtung
		— Betreiber von Verkehrsmanagement- und Verkehrssteuerungssystemen, die Flugverkehrskontrolldienste im Sinne des Artikels 2 Nummer 1 der Verordnung (EG) Nr. 549/2004 des Europäischen Parlaments und des Rates ([6]) bereitstellen
	b) Schienenverkehr	— Infrastrukturbetreiber im Sinne des Artikels 3 Nummer 2 der Richtlinie 2012/34/EU des Europäischen Parlaments und des Rates ([7])
		— Eisenbahnunternehmen im Sinne des Artikels 3 Nummer 1 der Richtlinie 2012/34/EU, einschließlich Betreiber einer Serviceeinrichtung im Sinne des Artikels 3 Nummer 12 der Richtlinie 2012/34/EU
	c) Schifffahrt	— Passagier- und Frachtbeförderungsunternehmen der Binnen-, See- und Küstenschifffahrt, wie sie in Anhang I der Verordnung (EG) Nr. 725/2004 des Europäischen Parlaments und des Rates ([8]) für die Schifffahrt definiert sind, ausschließlich der einzelnen von diesen Unternehmen betriebenen Schiffe
		— Leitungsorgane von Häfen im Sinne des Artikels 3 Nummer 1 der Richtlinie 2005/65/EG des Europäischen Parlaments und des Rates ([9]), einschließlich ihrer Hafenanlagen im Sinne des Artikels 2 Nummer 11 der Verordnung (EG) Nr. 725/2004, sowie Einrichtungen, die innerhalb von Häfen befindliche Anlagen und Ausrüstung betreiben
		— Betreiber von Schiffsverkehrsdiensten im Sinne des Artikels 3 Buchstabe o der Richtlinie 2002/59/EG des Europäischen Parlaments und des Rates ([10])
	d) Straßenverkehr	— Straßenverkehrsbehörden im Sinne des Artikels 2 Nummer 12 der Delegierten Verordnung (EU) 2015/962 der Kommission ([11]), die für Verkehrsmanagement- und Verkehrssteuerung verantwortlich sind
		— Betreiber intelligenter Verkehrssysteme im Sinne des Artikels 4 Nummer 1 der Richtlinie 2010/40/EU des Europäischen Parlaments und des Rates ([12])
3. Bankwesen		Kreditinstitute im Sinne des Artikels 4 Nummer 1 der Verordnung (EU) Nr. 575/2013 des Europäischen Parlaments und des Rates ([13])
4. Finanzmarktinfrastrukturen		— Betreiber von Handelsplätzen im Sinne des Artikels 4 Nummer 24 der Richtlinie 2014/65/EU des Europäischen Parlaments und des Rates ([14])
		— zentrale Gegenparteien im Sinne des Artikels 2 Nummer 1 der Verordnung (EU) Nr. 648/2012 des Europäischen Parlaments und des Rates ([15])
5. Gesundheitswesen	Einrichtungen der medizinischen Versorgung (einschließlich Krankenhäuser und Privatkliniken)	Gesundheitsdienstleister im Sinne des Artikels 3 Buchstabe g der Richtlinie 2011/24/EU des Europäischen Parlaments und des Rates ([16])

Sektor	Teilsektor	Art der Einrichtung
6. Trinkwasserlieferung und -versorgung		Lieferanten von und Unternehmen der Versorgung mit „Wasser für den menschlichen Gebrauch“ im Sinne des Artikels 2 Nummer 1 Buchstabe a der Richtlinie 98/83/EG des Rates ([17]), jedoch unter Ausschluss der Lieferanten, für die die Lieferung von Wasser für den menschlichen Gebrauch nur ein Teil ihrer allgemeinen Tätigkeit der Lieferung anderer Rohstoffe und Güter ist, die nicht als wesentliche Dienste eingestuft werden
7. Digitale Infrastruktur		— IXPs
		— DNS-Diensteanbieter
		— TLS-Name-Registries

([1]) Richtlinie 2009/72/EG des Europäischen Parlaments und des Rates vom 13. Juli 2009 über gemeinsame Vorschriften für den Elektrizitätsbinnenmarkt und zur Aufhebung der Richtlinie 2003/54/EG (ABl. L 211 vom 14.8.2009, S. 55).
([2]) Richtlinie 2009/73/EG des Europäischen Parlaments und des Rates vom 13. Juli 2009 über gemeinsame Vorschriften für den Erdgasbinnenmarkt und zur Aufhebung der Richtlinie 2003/55/EG (ABl. L 211 vom 14.8.2009, S. 94).
([3]) Verordnung (EG) Nr. 300/2008 des Europäischen Parlaments und des Rates vom 11. März 2008 über gemeinsame Vorschriften für die Sicherheit in der Zivilluftfahrt und zur Aufhebung der Verordnung (EG) Nr. 2320/2002 (ABl. L 97 vom 9.4.2008, S. 72).
([4]) Richtlinie 2009/12/EG des Europäischen Parlaments und des Rates vom 11. März 2009 über Flughafenentgelte (ABl. L 70 vom 14.3.2009, S. 11).
([5]) Verordnung (EU) Nr. 1315/2013 des Europäischen Parlaments und des Rates vom 11. Dezember 2013 über Leitlinien der Union für den Aufbau eines transeuropäischen Verkehrsnetzes und zur Aufhebung des Beschlusses Nr. 661/2010/EU (ABl. L 348 vom 20.12.2013, S. 1).
([6]) Verordnung (EG) Nr. 549/2004 des Europäischen Parlaments und des Rates vom 10. März 2004 zur Festlegung des Rahmens für die Schaffung eines einheitlichen europäischen Luftraums („Rahmenverordnung“) (ABl. L 96 vom 31.3.2004, S. 1).
([7]) Richtlinie 2012/34/EU des Europäischen Parlaments und des Rates vom 21. November 2012 zur Schaffung eines einheitlichen europäischen Eisenbahnraums (ABl. L 343 vom 14.12.2012, S. 32).
([8]) Verordnung (EG) Nr. 725/2004 des Europäischen Parlaments und des Rates vom 31. März 2004 zur Erhöhung der Gefahrenabwehr auf Schiffen und in Hafenanlagen (ABl. L 129 vom 29.4.2004, S. 6).
([9]) Richtlinie 2005/65/EG des Europäischen Parlaments und des Rates vom 26. Oktober 2005 zur Erhöhung der Gefahrenabwehr in Häfen (ABl. L 310 vom 25.11.2005, S. 28).
([10]) Richtlinie 2002/59/EG des Europäischen Parlaments und des Rates vom 27. Juni 2002 über die Einrichtung eines gemeinschaftlichen Überwachungs- und Informationssystems für den Schiffsverkehr und zur Aufhebung der Richtlinie 93/75/EWG des Rates (ABl. L 208 vom 5.8.2002, S. 10).
([11]) Delegierte Verordnung (EU) 2015/962 der Kommission vom 18. Dezember 2014 zur Ergänzung der Richtlinie 2010/40/EU des Europäischen Parlaments und des Rates hinsichtlich der Bereitstellung EU-weiter Echtzeit-Verkehrsinformationsdienste (ABl. L 157 vom 23.6.2015, S. 21).
([12]) Richtlinie 2010/40/EU des Europäischen Parlaments und des Rates vom 7. Juli 2010 zum Rahmen für die Einführung intelligenter Verkehrssysteme im Straßenverkehr und für deren Schnittstellen zu anderen Verkehrsträgern (ABl. L 207 vom 6.8.2010, S. 1).
([13]) Verordnung (EU) Nr. 575/2013 des Europäischen Parlaments und des Rates vom 26. Juni 2013 über Aufsichtsanforderungen an Kreditinstitute und Wertpapierfirmen und zur Änderung der Verordnung (EU) Nr. 648/2012 (ABl. L 176 vom 27.6.2013, S. 1).
([14]) Richtlinie 2014/65/EU des Europäischen Parlaments und des Rates vom 15. Mai 2014 über Märkte für Finanzinstrumente sowie zur Änderung der Richtlinien 2002/92/EG und 2011/61/EU (ABl. L 173 vom 12.6.2014, S. 349).
([15]) Verordnung (EU) Nr. 648/2012 des Europäischen Parlaments und des Rates vom 4. Juli 2012 über OTC-Derivate, zentrale Gegenparteien und Transaktionsregister (ABl. L 201 vom 27.7.2012, S. 1).
([16]) Richtlinie 2011/24/EU des Europäischen Parlaments und des Rates vom 9. März 2011 über die Ausübung der Patientenrechte in der grenzüberschreitenden Gesundheitsversorgung (ABl. L 88 vom 4.4.2011, S. 45).
([17]) Richtlinie 98/83/EG des Rates vom 3. November 1998 über die Qualität von Wasser für den menschlichen Gebrauch (ABl. L 330 vom 5.12.1998, S. 32).

ANHANG III

ARTEN DIGITALER DIENSTE IM SINNE DES ARTIKELS 4 NUMMER 5

1. Online-Marktplatz
2. Online-Suchmaschine
3. Cloud-Computing-Dienst

VERORDNUNG (EU) 2019/881 DES EUROPÄISCHEN PARLAMENTS UND DES RATES

vom 17. April 2019

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

(Text von Bedeutung für den EWR)

DAS EUROPÄISCHE PARLAMENT UND DER RAT DER EUROPÄISCHEN UNION —

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

auf Vorschlag der Europäischen Kommission,

nach Zuleitung des Entwurfs des Gesetzgebungsakts an die nationalen Parlamente,

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

nach Stellungnahme des Ausschusses der Regionen ([2]),

gemäß dem ordentlichen Gesetzgebungsverfahren ([3]),

in Erwägung nachstehender Gründe:

(1) Netz- und Informationssysteme sowie elektronische Kommunikationsnetze und -dienste spielen eine lebenswichtige Rolle in der Gesellschaft und sind mittlerweile zum Hauptmotor des Wirtschaftswachstums geworden. Die Informations- und Kommunikationstechnologien (IKT) bilden das Rückgrat der komplexen Systeme, die alltägliche 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, Organisationen und Unternehmen 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 eine extrem hohe Zahl 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. In diesem Zusammenhang führt das geringe Maß an Zertifizierung dazu, dass Personen, Organisationen und Unternehmen die IKT-Produkte, -Dienste und -prozesse nutzen, nur unzureichend über deren Cybersicherheitsmerkmale informiert werden, wodurch das Vertrauen in digitale Lösungen untergraben wird. Netz- und Informationssysteme können uns das Leben in jeder Hinsicht erleichtern und das Wirtschaftswachstum der Union anzukurbeln. Sie spielen eine tragende Rolle bei der Verwirklichung des digitalen Binnenmarkts.

(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 Personen wie Kinder ausgesetzt sind. Um diesen Gefahren zu begegnen, gilt es, alle für die Erhöhung der Cybersicherheit in der Union notwendigen Maßnahmen zu ergreifen, damit die Netz- und Informationssysteme, die Kommunikationsnetze und die digitalen Produkte, Dienste und Geräte, die von Bürgern, Organisationen und Unternehmen — von kleinen und mittleren Unternehmen (KMU) im Sinne der Empfehlung 2003/361/EG der Kommission ([4]) bis zu Betreibern kritischer Infrastrukturen — genutzt werden, besser vor Cyberbedrohungen geschützt sind.

([1]) ABl. C 227 vom 28.6.2018, S. 86.
([2]) ABl. C 176 vom 23.5.2018, S. 29.
([3]) Stellungnahme des Europäischen Parlaments vom 12. März 2019 (noch nicht im Amtsblatt veröffentlicht) und Beschluss des Rates vom 9. April 2019.
([4]) Empfehlung der Kommission vom 6. Mai 2003 betreffend die Definition der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen (ABl. L 124 vom 20.5.2003, S. 36).

(4) Durch das Zurverfügungstellung einschlägiger Informationen für die Öffentlichkeit trägt die mit der Verordnung (EU) Nr. 526/2013 des Europäischen Parlaments und des Rates ([5]) errichtete Agentur der Europäischen Union für Netz- und Informationssicherheit (im Folgenden „ENISA") zur Entwicklung der Cybersicherheitsbranche in der Union, insbesondere von KMU und Start-ups, bei. Die ENISA sollte sich um eine engere Zusammenarbeit mit Universitäten und Forschungseinrichtungen bemühen, um einen Beitrag zur Verringerung der Abhängigkeit von Cybersicherheitsprodukten und -diensten von außerhalb der Union zu leisten und die Lieferketten innerhalb der Union zu stärken.

(5) Cyberangriffe nehmen zu und eine Wirtschaft und Gesellschaft, die durch ihre Vernetzung anfälliger für Cyberbedrohungen und -angriffe ist, benötigt daher einen stärkeren Schutz. Obwohl jedoch die Cyberangriffe häufig grenzüberschreitend sind, sind die Zuständigkeiten und Reaktionen der für die Cybersicherheit und für die Strafverfolgung zuständigen Behörden vor allem national. Sicherheitsvorfälle großen Ausmaßes könnten die Bereitstellung wesentlicher Dienste in der gesamten Union empfindlich stören. Notwendig sind daher effektive und koordinierte Maßnahmen sowie ein Krisenmanagement auf Unionsebene, gestützt auf gezielte Strategien, sowie ein breiter angelegtes Instrumentarium für europäische Solidarität und gegenseitige Hilfe. Zudem sind daher eine auf zuverlässigen Daten der Union basierende regelmäßige Überprüfung des Stands der Cybersicherheit und der Abwehrfähigkeit in der Union sowie eine systematische Prognose künftiger Entwicklungen, Herausforderungen und Bedrohungen — auf Unionsebene und auf globaler Ebene — für die Entscheidungsträger, die Branche und die Nutzer gleichermaßen wichtig.

(6) 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 aufbauen und sich wechselseitig verstärkende Ziele unterstützen würde. Diese Ziele beinhalten eine weitere Stärkung der Fähigkeiten und der Abwehrbereitschaft der Mitgliedstaaten und Unternehmen sowie eine bessere Zusammenarbeit, einen besseren Informationsaustausch und Koordinierung zwischen den Mitgliedstaaten und den Organen, Einrichtungen und sonstigen Stellen der Union. Da Cyberbedrohungen an keinen Grenzen Halt machen, gilt es zudem, die Fähigkeiten auf Unionsebene zu stärken, die Maßnahmen der Mitgliedstaaten vor allem dann ergänzen könnten, wenn es zu grenzüberschreitenden Sicherheitsvorfällen und -krisen von großem Ausmaß kommt, unter Berücksichtigung der Bedeutung der Bewahrung und Verbesserung der nationalen Fähigkeiten zur Reaktion auf Cyberbedrohungen jeglichen Umfangs.

(7) Darüber hinaus sind weitere Anstrengungen notwendig, um die Bürger, Organisationen und Unternehmen für Fragen der Cybersicherheit zu sensibilisieren. Da Sicherheitsvorfälle das Vertrauen in Anbieter digitaler Dienste und in den digitalen Binnenmarkt als solchen insbesondere unter den Verbrauchern untergraben, sollte dieses Vertrauen dadurch gestärkt werden, dass auf transparente Art und Weise Informationen über das Niveau der Sicherheit von IKT-Produkten, -Diensten und -Prozessen bereitgestellt werden, wobei betont wird, dass auch eine Cybersicherheitszertifizierung auf hohem Niveau nicht garantieren kann, dass ein IKT-Produkt, -Dienst oder -Prozess völlig sicher ist. Eine Stärkung des Vertrauens kann durch eine unionsweite Zertifizierung erleichtert werden, für die über nationale Märkte und Sektoren hinaus unionsweit einheitliche Anforderungen und Bewertungskriterien für die Cybersicherheit festgelegt werden.

(8) Cybersicherheit ist nicht nur eine Frage der Technologie, sondern eine, bei der das menschliche Verhalten ebenso wichtig ist. Daher sollte die „Cyberhygiene", also einfache Routinemaßnahmen, durch die, wenn sie von Bürgern, Organisationen und Unternehmen regelmäßig umgesetzt und durchgeführt werden, die Risiken von Cyberbedrohungen so gering wie möglich gehalten werden, nachdrücklich gefördert werden.

(9) Um die Cybersicherheitsstrukturen der Union zu stärken, müssen die Fähigkeiten der Mitgliedstaaten, umfassend auf Cyberbedrohungen — einschließlich grenzüberschreitender Sicherheitsvorfälle — zu reagieren, erhalten und ausgebaut werden.

(10) Die Unternehmen und die einzelnen Verbraucher sollten über präzise Informationen darüber verfügen, auf welcher Vertrauenswürdigkeitsstufe die Sicherheit ihrer IKT-Produkte, -Dienste und -Prozesse zertifiziert wurde. Allerdings bietet kein IKT-Produkt oder -dienst hundertprozentige Cybersicherheit weshalb grundlegenden Prinzipien der Cyberhygiene verbreitet werden sollten und ihnen Vorrang eingeräumt werden sollte. Angesichts der zunehmenden Verbreitung von Geräten des Internets der Dinge kann die Privatwirtschaft zahlreiche freiwillige Maßnahmen treffen, um das Vertrauen in die Sicherheit von IKT-Produkten, -Diensten und -Prozessen zu stärken.

(11) Moderne IKT-Produkte und -Systeme weisen oft einen oder mehrere von Dritten entwickelte Technologien und Bestandteile wie Software-Module, Bibliotheken oder Programmierschnittstellen auf und sind von diesen abhängig. Diese „Abhängigkeit" könnte zusätzliche Risiken im Bereich der Cybersicherheit bergen, da sich Sicherheitslücken in Bestandteilen Dritter auch auf die Sicherheit von IKT-Produkten, -Diensten, und -Prozessen auswirken könnten. In vielen Fällen ermöglicht die Aufdeckung und Dokumentierung solcher „Abhängigkeiten" den Endnutzern von IKT-Produkten, -Diensten und -Prozessen die Verbesserung ihres Risikomanagements im Bereich der Cybersicherheit, indem beispielsweise die Behandlung von Sicherheitslücken im Bereich der Cybersicherheit durch die Nutzer und deren Abhilfeverfahren verbessert werden.

([5]) 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).

(12) Organisationen, Hersteller oder Diensteanbieter, die an der Konzeption und Entwicklung von IKT-Produkten, -Diensten und -Prozessen beteiligt sind, sollten dazu angehalten werden, in den ersten Phasen der Konzeption und Entwicklung Maßnahmen durchzuführen, um die Sicherheit dieser Produkte, Dienste und Prozesse möglichst weitgehend zu schützen, in dem sie davon ausgehen, dass Cyberangriffe vorliegen, und deren Folgen vorwegzunehmen und so gering wie möglich zu halten (konzeptionsintegrierte Sicherheit — security by design). Die Sicherheit sollte während der gesamten Lebensdauer des IKT-Produkts, -Dienstes oder -Prozesses berücksichtigt werden, wobei die Konzeptions- und Entwicklungsprozesse ständig weiterentwickelt werden sollten, um das Risiko von Schäden durch eine böswillige Nutzung zu verringern.

(13) Unternehmen, Organisationen und der öffentliche Sektor sollten die von ihnen konzipierten IKT-Produkte, -Dienste oder -Prozesse so konfigurieren, dass ein höheres Maß an Sicherheit gewährleistet ist, das es dem ersten Nutzer ermöglicht, eine Standardkonfiguration mit den sichersten möglichen Einstellungen („security by default“) zu erhalten; somit wären die Nutzer in geringerem Maße der Belastung ausgesetzt, ein IKT-Produkt, -einen IKT-Dienst oder einen IKT-Prozess angemessen konfigurieren zu müssen. Die Sicherheit durch Voreinstellungen („security by default“) sollte weder eine umfangreiche Konfiguration erfordern, noch spezifische technische Kenntnisse oder ein nicht offensichtliches Verhalten seitens des Nutzers, und sie sollte dort, wo sie implementiert wurde, einfach und zuverlässig funktionieren. Wenn im Einzelfall eine Risiko- und Nutzbarkeitsanalyse zu dem Ergebnis führt, dass eine solche vordefinierte Einstellung nicht machbar ist, sollten die Nutzer aufgefordert werden, die sicherste Einstellung zu wählen.

(14) Mit der Verordnung (EG) Nr. 460/2004 des Europäischen Parlaments und des Rates ([6]) wurde die ENISA als Beitrag zu den Zielen errichtet, 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 öffentlicher Verwaltung zugute kommt. Mit der Verordnung (EG) Nr. 1007/2008 des Europäischen Parlaments und des Rates ([7]) wurde das Mandat der ENISA bis März 2012 verlängert. Durch die Verordnung (EU) Nr. 580/2011 des Europäischen Parlaments und des Rates ([8]) wurde das Mandat der ENISA nochmals bis zum 13. September 2013 verlängert. Mit der Verordnung (EU) Nr. 526/2013 des Europäischen Parlaments und des Rates wurde das Mandat der ENISA bis zum 19. Juni 2020 verlängert.

(15) Die Union hat bereits wichtige Maßnahmen ergriffen, um die Cybersicherheit zu gewährleisten und das Vertrauen in die digitale Technik zu stärken. Im Jahr 2013 wurde die EU-Cybersicherheitsstrategie der Europäischen Union verabschiedet, die der Union als Orientierung für strategische Reaktionen auf Cybersicherheitsbedrohungen und -risiken dient. Im Zuge ihrer Bemühung, den Online-Schutz der Bürger zu verbessern, hat die Union im Jahr 2016 mit der Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates ([9]) den ersten Rechtsakt auf dem Gebiet der Cybersicherheit erlassen. Mit der Richtlinie (EU) 2016/1148 wurden Anforderungen an die nationalen Fähigkeiten im Bereich der Cybersicherheit sowie erstmals Mechanismen zur Stärkung der strategischen und operativen Zusammenarbeit zwischen den Mitgliedstaaten festgelegt und ferner Verpflichtungen in Bezug auf die Sicherheitsmaßnahmen und die Meldung von Sicherheitsvorfällen für die Sektoren, die für die Wirtschaft und Gesellschaft lebenswichtig sind, wie Energie, Verkehr, Trinkwasserlieferung und -versorgung, Bankwesen, Finanzmarktinfrastrukturen, Gesundheitswesen, digitale Infrastruktur 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. Andere Rechtsakte wie die Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates ([10]) und die Richtlinie 2002/58/EG ([11]) sowie die Richtlinie (EU) 2018/1972 des Europäischen Parlaments und des Rates ([12]) tragen auch zu einem hohen Maß an Cybersicherheit im digitalen Binnenmarkt bei.

([6]) 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).

([7]) 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).

([8]) Verordnung (EU) 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).

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

([10]) Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (ABl. L 119 vom 4.5.2016, S. 1).

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

([12]) Richtlinie (EU) 2018/1972 des Europäischen Parlaments und des Rates vom 11. Dezember 2018 über den europäischen Kodex für die elektronische Kommunikation (Neufassung) (ABl. L 321 vom 17.12.2018, S. 36).

(16) Seit der Verabschiedung der Cybersicherheitsstrategie der Europäischen Union im Jahr 2013 und der letzten Überarbeitung des Mandats der ENISA hat sich der gesamtpolitische Rahmen deutlich verändert, da das globale Umfeld nun von größeren Unwägbarkeiten und geringerer Sicherheit geprägt ist. Vor diesem Hintergrund und im Kontext der positiven Entwicklung der Rolle der ENISA als ein Bezugspunkt für Beratung und Sachkenntnis und als Vermittlerin in Bezug auf Zusammenarbeit und den Aufbau von Fähigkeiten sowie angesichts der neuen Unionspolitik im Bereich der Cybersicherheit muss das Mandat der ENISA im Hinblick auf ihre neue Rolle im veränderten Cybersicherheitsökosystem überarbeitet werden, damit sie die Union wirksam dabei unterstützen kann, auf die Herausforderungen im Bereich der Cybersicherheit zu reagieren, die sich aus der grundlegend veränderten Cyberbedrohungslandschaft ergeben und für die — wie in der Bewertung der ENISA bestätigt — das laufende Mandat nicht ausreicht.

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

(18) Mit dem Einvernehmlichen Beschluss 2004/97/EG, Euratom der auf Ebene der Staats- und Regierungschefs vereinigten Vertreter der Mitgliedstaaten ([13]), legten die Vertreter der Mitgliedstaaten fest, dass die ENISA ihren Sitz in Griechenland in einer von der griechischen Regierung zu benennenden Stadt haben soll. Der Sitzmitgliedstaat der ENISA sollte die bestmöglichen Voraussetzungen für eine reibungslose und effiziente Tätigkeit der ENISA gewährleisten. Damit die ENISA 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 ENISA bietet. Die erforderlichen Modalitäten sollten in einem Abkommen zwischen der ENISA und dem Sitzmitgliedstaat festgelegt werden, das nach Billigung durch den Verwaltungsrat der ENISA geschlossen wird.

(19) Angesichts der zunehmenden Bedrohungen und Herausforderungen, mit denen die Union im Bereich der Cybersicherheit konfrontiert ist, sollten die Mittelzuweisungen für die ENISA erhöht werden, damit ihre finanzielle und personelle Ausstattung ihrer größeren Rolle und ihren umfangreicheren Aufgaben sowie ihrer wichtigen Stellung im Ökosystem der Organisationen gerecht werden kann, die das digitale Ökosystem der Union verteidigen, sodass die ENISA die ihr mit dieser Verordnung übertragenen Aufgaben wirksam erfüllen kann.

(20) Die ENISA sollte ein hohes Niveau an Sachkenntnis entwickeln und pflegen und als Bezugspunkt fungieren, wobei sie durch ihre Unabhängigkeit, die Qualität ihrer Beratung und der von ihr verbreiteten Informationen, die Transparenz ihrer Verfahren, die Transparenz ihrer Arbeitsmethoden sowie die Sorgfalt, mit der sie ihre Aufgaben erfüllt, Vertrauen in den Binnenmarkt schafft. Die ENISA sollte die Bemühungen der Mitgliedstaaten aktiv 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, wobei Doppelarbeiten vermieden und Synergien gefördert werden sollten. Außerdem sollte sich die ENISA auf die Beiträge des Privatsektors und anderer einschlägiger Interessenträger sowie auf die Zusammenarbeit mit ihnen stützen. Mit einer Reihe von Aufgaben sollte bei gleichzeitiger Wahrung der Flexibilität in ihrer Tätigkeit vorgegeben werden, wie die ENISA ihre Ziele erreichen soll.

(21) Damit sie die operative Zusammenarbeit zwischen den Mitgliedstaaten angemessen unterstützen kann, sollte die ENISA ihre technischen und menschlichen Fähigkeiten und Fertigkeiten weiter ausbauen. Die ENISA sollte ihr Know-how und ihre Fähigkeiten vergrößern. Die ENISA und die Mitgliedstaaten könnten auf freiwilliger Basis Programme für die Entsendung von nationalen Sachverständigen an die ENISA, die Bildung von Pools von Sachverständigen und den Austausch von Personal entwickeln.

(22) Die ENISA 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 den diesbezüglichen sektorenspezifischen Aspekten zusammenhängen, unterstützen, damit die Strategien und Rechtsvorschriften der Union mit einer Cybersicherheitsdimension zweckdienlicher gestaltet werden und die kohärente Umsetzung dieser Strategien und Rechtsvorschriften auf nationaler Ebene ermöglicht wird. Für sektorspezifische Strategien und Rechtsetzungsinitiativen der Union im Zusammenhang mit der Cybersicherheit sollte die ENISA als Bezugspunkt für Beratung und Sachkenntnis dienen. Die ENISA sollte dem Europäischen Parlament regelmäßig über ihre Tätigkeiten Bericht erstatten.

([13]) Einvernehmlicher Beschluss 2004/97/EG, Euratom der auf Ebene der Staats- und Regierungschefs vereinigten Vertreter der Mitgliedstaaten vom 13. Dezember 2003 über die Festlegung der Sitze bestimmter Ämter, Behörden und Agenturen der Europäischen Union (ABl. L 29 vom 3.2.2004, S. 15).

(23) Der öffentliche Kern des offenen Internets, d. h. seine wichtigsten Protokolle und Infrastrukturen, die ein globales öffentliches Gut sind, stellt die wesentlichen Funktionen des Internets als Ganzes bereit und bildet die Grundlage für dessen normalen Betrieb. Die ENISA sollte die Sicherheit und Stabilität dieses öffentlichen Kerns des offenen Internets unterstützen, unter anderem — aber nicht beschränkt auf — die wichtigsten Protokolle (insbesondere DNS, BGP und IPv6), den Betrieb des „Domain Name System" (DNS) (wie den Betrieb aller Domänen der obersten Ebene) und den Betrieb der Root-Zone.

(24) Die ENISA hat grundsätzlich die Aufgabe, die einheitliche Umsetzung des einschlägigen Rechtsrahmens, vor allem die wirksame Umsetzung der Richtlinie (EU) 2016/1148 und anderer maßgeblicher Rechtsakte zu Aspekten der Cybersicherheit, zu unterstützen, was für die Stärkung der Abwehrfähigkeit gegen Cyberangriffe unerlässlich ist. Angesichts der sich rasch weiterentwickelnden Bedrohungen für die Cybersicherheit ist klar, dass die Mitgliedstaaten beim Aufbau der Abwehrfähigkeit gegen Cyberangriffe durch ein umfassenderes und ressortübergreifendes Konzept unterstützt werden müssen.

(25) Die ENISA sollte die Mitgliedstaaten und die Organe, Einrichtungen und sonstigen Stellen der Union in ihrem Bemühen um den Auf- und Ausbau der Fähigkeiten und der Bereitschaft zur Verhütung, Erkennung und Bewältigung von Cyberbedrohungen und von Sicherheitsvorfällen im Zusammenhang mit der Netz- und Informationssicherheit unterstützen. So sollte die ENISA den Auf- und Ausbau der in der Richtlinie (EU) 2016/1148 vorgesehenen Reaktionsteams für Computersicherheitsverletzungen (im Folgenden „CSIRTs") der Mitgliedstaaten und der Union unterstützen, damit sie ein unionsweit hohes Maß an Ausgereiftheit erreichen. Die Tätigkeiten der ENISA im Zusammenhang mit den operativen Kapazitäten der Mitgliedstaaten sollten die Maßnahmen der Mitgliedstaaten zur Erfüllung ihrer Verpflichtungen aus der Richtlinie (EU) 2016/1148 aktiv unterstützen und diese daher nicht ersetzen.

(26) Zudem sollte die ENISA auf Ersuchen die Ausarbeitung und Aktualisierung von Strategien im Bereich der Netz- und Informationssysteme auf Unionsebene und, auf Anfrage, auf Ebene der Mitgliedstaaten, insbesondere der Cybersicherheit, unterstützen und sollte die Verbreitung solcher Strategien fördern und die Fortschritte bei deren Umsetzung verfolgen. Die ENISA sollte auch dazu beitragen, den Bedarf an Ausbildungsmaßnahmen und Ausbildungsmaterial, auch in Bezug auf öffentliche Stellen, zu decken, und gegebenenfalls in großem Umfang auf der Grundlage des Referenzrahmens für digitale Kompetenzen der Bürger Ausbilder weiterbilden, um die Mitgliedstaaten und die Organe, Einrichtungen und sonstigen Stellen der Union darin zu unterstützen, eigene Ausbildungskapazitäten aufzubauen.

(27) Die ENISA sollte die Mitgliedstaaten im Bereich der Sensibilisierung und Ausbildung in Bezug auf die Cybersicherheit unterstützen, indem sie eine engere Koordinierung und den Austausch von bewährten Verfahren zwischen den Mitgliedstaaten fördert. Diese Unterstützung könnte darin bestehen, dass sie ein Netz von nationalen Bildungskontaktstellen und eine Ausbildungsplattform zur Cybersicherheit entwickelt. Das Netz der nationalen Bildungskontaktstellen könnte im Rahmen des Netzes der nationalen Verbindungsbeamten betrieben werden und einen Ausgangspunkt für die zukünftige Koordinierung innerhalb der Mitgliedstaaten bilden.

(28) Die ENISA sollte die durch die Richtlinie (EU) 2016/1148 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, unter anderem was die Ermittlung von Betreibern wesentlicher Dienste durch die Mitgliedstaaten in Bezug auf Risiken und Sicherheitsvorfälle anbelangt, auch mit Blick auf grenzüberschreitende Abhängigkeiten.

(29) Die ENISA sollte als Anreiz für die Zusammenarbeit zwischen dem öffentlichen und privaten Sektor, vor allem als Beitrag zum Schutz kritischer Infrastrukturen, 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 Leitfäden zu den verfügbaren Instrumenten und Verfahren bereitstellt und aufzeigt, wie regulatorische Fragen im Zusammenhang mit der Informationsweitergabe geklärt werden können, wobei dies beispielsweise durch die Erleichterung des Aufbaus sektorbezogener Informationsaustausch- und -analysezentren (Information Sharing and Analysis Centres) erreicht werden soll.

(30) In Anbetracht der Tatsache, dass die möglichen negativen Auswirkungen von Sicherheitslücken bei IKT-Produkten, -Diensten und -Prozessen stetig zunehmen, spielen die Aufdeckung und die Behebung solcher Sicherheitslücken eine wichtige Rolle bei der Verringerung der Gesamtrisiken im Bereich der Cybersicherheit. Es hat sich gezeigt, dass die Zusammenarbeit zwischen Organisationen, Herstellern oder Anbietern besonders gefährdeter IKT-Produkte, -Dienste oder -Prozesse sowie Mitgliedern der Forschungsgemeinschaft im Bereich der Cybersicherheit und Regierungen, die diese Sicherheitslücken aufspüren, sowohl die Aufdeckung als auch die Behebung von Sicherheitslücken bei IKT-Produkten, -Diensten oder -Prozessen erheblich verbessert. Die koordinierte Offenlegung von Sicherheitslücken erfolgt in einem strukturierten Prozess der Zusammenarbeit, in dem Sicherheitslücken dem Eigentümer des Informationssystems gemeldet werden, wodurch die Organisation Gelegenheit zur Diagnose und Behebung der Sicherheitslücke erhält, bevor detaillierte Informationen über die Sicherheitslücke an Dritte oder die Öffentlichkeit weitergegeben werden. Das Verfahren sieht ferner eine Koordinierung zwischen demjenigen, der die Sicherheitslücke aufgespürt hat, und der Organisation im Hinblick auf die Veröffentlichung jener Sicherheitslücke vor. Grundsätze für die koordinierte Offenlegung von Sicherheitslücken könnten eine wichtige Rolle bei den Bemühungen der Mitgliedstaaten um die Verbesserung der Cybersicherheit spielen.

(31) Die ENISA sollte die freiwillig bereitgestellten nationalen Berichte der CSIRTs und des interinstitutionellen IT-Notfallteams für die Organe, Einrichtungen und sonstigen Stellen der Union („CERT-EU"), welche mit der zwischen dem Europäischen Parlament, dem Europäischen Rat, dem Rat der Europäischen Union, der Europäischen Kommission, dem Gerichtshof der Europäischen Union, der Europäischen Zentralbank, dem Europäischen Rechnungshof, dem Europäischen Auswärtigen Dienst, dem Europäischen Wirtschafts- und Sozialausschuss, dem Europäischen Ausschuss der Regionen und der Europäischen Investitionsbank geschlossenen Vereinbarung über die Organisation und die Funktionsweise eines IT-Notfallteams für die Organe, Einrichtungen und sonstigen Stellen der Union (CERT-EU) ([14]) errichtet wurde, zusammenstellen und auswerten, um einen Beitrag zur Aufstellung gemeinsamer Verfahren für den Informationsaustausch, zur Festlegung der Sprache und zu terminologischen Vereinbarungen zu leisten. In diesem Zusammenhang sollte die ENISA im Rahmen der Richtlinie (EU) 2016/1148, die die Grundlage für den freiwilligen Austausch technischer Informationen auf operativer Ebene innerhalb des Netzwerks von Computer-Notfallteams (im Folgenden „CSIRTs-Netz") gemäß der genannten Richtlinie geschaffen hat, auch den Privatsektor einbeziehen.

(32) Die ENISA sollte dazu beitragen, dass bei massiven grenzüberschreitenden Vorfällen und -krisen in Bezug auf Cybersicherheit eine Reaktion auf Unionsebene erfolgt. Diese Aufgabe sollte ENISA entsprechend ihrem Mandat gemäß dieser Verordnung und einem Ansatz ausführen, der von den Mitgliedstaaten im Zusammenhang mit der Empfehlung (EU) 2017/1584 ([15]) der Kommission und den Schlussfolgerungen des Rates vom 26. Juni 2018 zu einer koordinierten Reaktion auf große Cybersicherheitsvorfälle und -krisen festzulegen ist. Zu dieser Aufgabe 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 sollte die ENISA die operative Zusammenarbeit zwischen den Mitgliedstaaten auf Ersuchen eines oder mehrerer Mitgliedstaaten unterstützen, indem sie die Bewältigung der Sicherheitsvorfälle aus technischer Sicht übernimmt, indem sie den Austausch entsprechender technischer Lösungen zwischen den Mitgliedstaaten erleichtert und Beiträge für die Öffentlichkeitsarbeit liefert. Die ENISA sollte die operative Zusammenarbeit unterstützen, indem sie die Modalitäten einer solchen Zusammenarbeit im Rahmen regelmäßig stattfindender Cybersicherheitsübungen testet.

(33) Zur Unterstützung der operativen Zusammenarbeit sollte die ENISA im Wege einer strukturierten Zusammenarbeit auf den bei der CERT-EU vorhandenen technischen und operativen Sachverstand zurückgreifen. Eine solche strukturierte Zusammenarbeit könnte auf der Sachkenntnis der ENISA aufbauen. Für die Festlegung der praktischen Aspekte einer solchen Kooperation und zur Vermeidung von Doppelarbeit sollten gegebenenfalls zwischen den beiden Stellen die hierfür notwendigen Modalitäten festgelegt werden.

(34) Entsprechend ihrer Aufgabe, die operative Zusammenarbeit im Rahmen des CSIRTs-Netzes zu unterstützen, sollte die ENISA in der Lage sein, die Mitgliedstaaten auf deren Ersuchen hin zu unterstützen, indem sie diese beispielsweise 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 sicherstellt, dass Cyberbedrohungen und Sicherheitsvorfälle analysiert werden. Die ENISA sollte die technische Bewältigung von Sicherheitsvorfällen mit beträchtlichen oder erheblichen Auswirkungen insbesondere dadurch erleichtern, dass sie 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 (EU) 2017/1584 zufolge sollten die Mitgliedstaaten in gutem Glauben untereinander sowie mit der ENISA Informationen über massive Vorfälle und -krisen in Bezug auf Cybersicherheit unverzüglich austauschen. Diese Informationen würden zudem der ENISA helfen, ihre Aufgabe wahrzunehmen, die operative Zusammenarbeit zu unterstützen.

(35) Als Teil der regulären Zusammenarbeit auf technischer Ebene zur Unterstützung der EU-Lageeinschätzung sollte die ENISA auf der Grundlage öffentlich verfügbarer Informationen, ihrer eigenen Analysen und anhand von Berichten, die sie von den CSIRTs der Mitgliedstaaten oder den nationalen Anlaufstellen für die Sicherheit von Netz- und Informationssystemen gemäß der Richtlinie (EU) 2016/1148, 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 (EU INTCEN) des Europäischen Auswärtigen Dienstes erhalten hat, regelmäßig und in enger Zusammenarbeit mit den Mitgliedstaaten eingehende EU-Cybersicherheitslageberichte über Sicherheitsvorfälle und Bedrohungen erstellen. Dieser Bericht sollte dem Rat, der Kommission, der Hohen Vertreterin der Union für die Gemeinsame Außen- und Sicherheitspolitik und dem CSIRTs-Netz zur Verfügung gestellt werden.

(36) Die ENISA sollte sich bei der Unterstützung von nachträglichen technischen Untersuchungen von Sicherheitsvorfällen mit beträchtlichen oder erheblichen Auswirkungen, die sie auf Ersuchen der betreffenden Mitgliedstaaten leistet, auf die Verhütung künftiger Sicherheitsvorfälle konzentrieren. Die betreffenden Mitgliedstaaten sollten die notwendigen Informationen und die erforderliche Hilfe bereitstellen, damit die ENISA die nachträgliche technische Untersuchung wirksam unterstützen kann.

([14]) ABl. C 12 vom 13.1.2018, S. 1.
([15]) Empfehlung (EU) 2017/1584 der Kommission vom 13. September 2017 für eine koordinierte Reaktion auf große Cybersicherheitsvorfälle und -krisen (ABl. L 239 vom 19.9.2017, S. 36).

(37) Die Mitgliedstaaten können die von dem Sicherheitsvorfall betroffenen Unternehmen auffordern, mit der ENISA zusammenzuarbeiten und dieser — unbeschadet ihres Rechts, sensible Geschäftsinformationen und Informationen, die für die öffentliche Sicherheit von Bedeutung sind, zu schützen — die notwendigen Informationen und Hilfen zur Verfügung stellen.

(38) Um die Herausforderungen im Bereich der Cybersicherheit besser verstehen und den Mitgliedstaaten und den Organen, Einrichtungen und sonstigen Stellen der Union langfristige strategische Beratung anbieten zu können, muss die ENISA aktuelle und neu auftretende Cybersicherheitsrisiken analysieren. Hierzu sollte die ENISA 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 für die Netz- und Informationssicherheit, insbesondere die Cybersicherheit, haben. Die ENISA sollte die Mitgliedstaaten sowie die Organe, Einrichtungen und sonstigen Stellen der Union darüber hinaus bei der Ermittlung sich abzeichnender Cybersicherheitsrisiken und bei der Vermeidung von Vorfällen unterstützen, indem sie Analysen der Cyberbedrohungen, Sicherheitslücken und Sicherheitsvorfälle durchführt.

(39) Um die Abwehrfähigkeit der Union zu stärken, sollte die ENISA Fachwissen im Bereich der Cybersicherheit der Infrastrukturen, insbesondere zur Unterstützung der in Anhang II der Richtlinie (EU) 2016/1148 aufgeführten Sektoren und der Infrastrukturen, die von den in Anhang III jener Richtlinie aufgeführten Anbietern digitaler Dienste genutzt werden, aufbauen, indem Beratung, Leitlinien zur Verfügung gestellt und bewährte Verfahren ausgetauscht werden. Um den Zugang zu besser strukturierten Informationen über Cybersicherheitsrisiken und mögliche Abhilfemaßnahmen zu erleichtern, sollte die ENISA das Informationsportal der Union aufbauen und pflegen, über das der Öffentlichkeit Informationen der Organe, Einrichtungen und sonstigen Stellen der Union und der Mitgliedstaaten zur Cybersicherheit bereitgestellt werden. Ein leichterer Zugang zu besser strukturierten Informationen über Cybersicherheitsrisiken und mögliche Abhilfemaßnahmen könnte den Mitgliedstaaten auch dabei helfen, ihre Kapazitäten auszubauen und ihre Verfahren aufeinander abzustimmen, sodass die Abwehrfähigkeit gegenüber Cyberangriffen insgesamt gestärkt wird.

(40) Die ENISA sollte dabei mitwirken, die Öffentlichkeit für Cybersicherheitsrisiken zu sensibilisieren, unter anderem durch eine unionsweite Sensibilisierungskampagne, die Förderung von Schulungen, und Leitlinien für bewährte Verfahren, die sich an Bürger, Organisationen und Unternehmen richten. Darüber hinaus sollte die ENISA einen Beitrag dazu leisten, bewährte Verfahren und Lösungen, einschließlich Cyberhygiene und Cyberkompetenz, auf der Ebene von Bürgern, Organisationen und Unternehmen zu fördern, indem sie öffentlich verfügbare Informationen über erhebliche Sicherheitsvorfälle sammelt und analysiert und Berichte und Leitlinien hierüber erstellt und veröffentlicht, die das Niveau der Abwehrbereitschaft und Abwehrfähigkeit von Bürgern, Organisationen und Unternehmen insgesamt erhöhen. Die ENISA sollte sich außerdem bemühen, Verbrauchern relevante Informationen über anwendbare Zertifizierungsschemata an die Hand zu geben, indem sie beispielsweise Leitlinien und Empfehlungen bereitstellt. Ferner sollte die ENISA gemäß dem mit der Mitteilung der Kommission vom 17. Januar 2018 aufgestellten Aktionsplan für digitale Bildung in Zusammenarbeit mit den Mitgliedstaaten und den Organen, Einrichtungen und sonstigen Stellen der Union regelmäßige öffentliche Aufklärungskampagnen durchführen, die sich an die Endnutzer richten, um sicherere Verhaltensweisen der Nutzer im Internet und digitale Kompetenz zu fördern, die Nutzer stärker für potenzielle Bedrohungen im Internet — auch für die Internetkriminalität wie das Abgreifen von Daten (Phishing), Botnets, Finanz- und Bankenbetrug sowie Datenbetrug — zu sensibilisieren und einfache Empfehlungen in Bezug auf mehrstufige Authentifizierung, Patching, Verschlüsselung, Anonymisierung und Datenschutz zu geben.

(41) Die ENISA sollte eine zentrale Rolle dabei spielen, die Sensibilisierung der Endnutzer für die Sicherheit von Geräten und die sichere Nutzung von Diensten zu forcieren und auf Unionsebene konzeptionsintegrierte Sicherheit und konzeptionsintegrierten Schutz der Privatsphäre (privacy by design) zu fördern. Dabei sollte die ENISA die verfügbaren bewährten Verfahren und die vorhandene Erfahrung insbesondere von Forschungseinrichtungen und Wissenschaftlern im Bereich IT-Sicherheit optimal nutzen.

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

(43) Die ENISA sollte einen Beitrag zu den Bemühungen der Union um eine Zusammenarbeit mit internationalen Organisationen sowie innerhalb der einschlägigen internationalen Gremien für die Zusammenarbeit im Bereich der Cybersicherheit leisten. Insbesondere sollte die ENISA gegebenenfalls an der Zusammenarbeit mit Organisationen wie der OECD, der OSZE und der NATO mitwirken. Diese Zusammenarbeit könnte gemeinsame Cybersicherheitsübungen und eine gemeinsame Koordinierung der Reaktion auf Sicherheitsvorfälle umfassen. Diese Aktivitäten müssen unter uneingeschränkter Achtung der Grundsätze der Inklusivität, der Gegenseitigkeit und der Beschlussfassungsautonomie der Union — unbeschadet der spezifischen Merkmale der Sicherheits- und Verteidigungspolitik der einzelnen Mitgliedstaaten — erfolgen.

(44) Damit die ENISA ihre Ziele in vollem Umfang verwirklichen kann, sollte sie zu den einschlägigen Aufsichtsbehörden und anderen zuständigen Behörden in der Union und anderen zuständigen Behörden, Einrichtungen und sonstigen Stellen der Union Kontakt halten — etwa zum CERT-EU, EC3, zur Europäischen Verteidigungsagentur (EDA), zur Agentur für das Europäische zivile Satellitennavigationssystem (Europäische GNSS Agentur — GSA), zum Gremium Europäischer Regulierungsstellen für elektronische Kommunikation (GEREK), zur Europäischen Agentur für das Betriebsmanagement von IT-Großsystemen im Raum der Freiheit, der Sicherheit und des Rechts (eu-LISA), zur Europäischen Zentralbank (EZB), zur Europäischen Bankenaufsichtsbehörde (EBA), zum Europäischen Datenschutzausschuss, zur Agentur für die Zusammenarbeit der Energieregulierungsbehörden (ACER), zur Europäischen Agentur für Flugsicherheit (EASA) und zu sonstigen Agenturen der Union, die sich mit Fragen der Cybersicherheit beschäftigen. Für den Austausch von Know-how und bewährten Verfahren und für die Beratung zu Fragen der Cybersicherheit, die sich auf die Arbeit von Datenschutzbehörden auswirken können, sollte die ENISA 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 ENISA-Beratungsgruppe in Frage kommen. Bei ihren Kontakten mit Strafverfolgungsbehörden in Bezug auf Netz- und Informationssicherheitsfragen, die sich möglicherweise auf deren Arbeit auswirken, sollte die ENISA vorhandene Informationskanäle und bestehende Netze beachten.

(45) Es könnten Partnerschaften mit Hochschulen eingerichtet werden, die in den einschlägigen Bereichen Forschungsinitiativen betreiben, und es sollten geeignete Kanäle für Beiträge von Verbraucherschutzverbänden und anderen Organisationen, die berücksichtigt werden sollten, zur Verfügung stehen.

(46) Die ENISA sollte in ihrer Rolle als Sekretariat des CSIRTs-Netzes bezüglich der in der Richtlinie (EU) 2016/1148 festgelegten einschlägigen Aufgaben des CSIRTs-Netzes die CSIRTs der Mitgliedstaaten und das CERT-EU bei der operativen Zusammenarbeit unterstützen. Zudem sollte die ENISA 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 CSIRTs betreffen oder betreffen können, fördern und unterstützen.

(47) Zur Erhöhung der Abwehrbereitschaft der Union bei Cybersicherheitsvorfällen sollte die ENISA auf Unionsebene regelmäßige Cybersicherheitsübungen organisieren und die Mitgliedstaaten sowie die Organe, Einrichtungen und sonstigen Stellen der Union auf deren Ersuchen hin bei der Organisation solcher Übungen unterstützen. Eine Großübung sollte alle zwei Jahre veranstaltet werden, die technische, operative und strategische Elemente umfasst. Darüber hinaus sollte die ENISA regelmäßig weniger umfassende Übungen organisieren können, mit denen dasselbe Ziel verfolgt wird, nämlich die Abwehrbereitschaft der Union bei Sicherheitsvorfällen zu stärken.

(48) Die ENISA sollte ihre Sachkenntnis im Bereich der Cybersicherheitszertifizierung weiter ausbauen und pflegen, damit sie die Unionspolitik auf diesem Gebiet unterstützen kann. Die ENISA sollte auf bestehenden bewährten Verfahren aufbauen und die Nutzung der Cybersicherheitszertifizierung in der Union fördern, auch indem sie zum Aufbau und zur Pflege eines Rahmens für die Cybersicherheitszertifizierung auf Unionsebene (europäischer Rahmen für die Cybersicherheitszertifizierung) beiträgt, um so die Transparenz der Vertrauenswürdigkeit der Cybersicherheit von IKT-Produkten, -Diensten und -Prozessen zu erhöhen und damit das Vertrauen in den digitalen Binnenmarkt und in seine Wettbewerbsfähigkeit zu stärken.

(49) 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 ENISA 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.

(50) Die ENISA sollte die Mitgliedstaaten, die Hersteller oder die Anbieter von IKT-Produkten, -Diensten oder -Prozessen dazu anspornen, ihre allgemeinen Sicherheitsstandards zu heben, damit alle Internetnutzer die erforderlichen Vorkehrungen für ihre persönliche Cybersicherheit treffen können und sie sollte Anreize dazu geben. So sollten Hersteller und Anbieter von IKT-Produkten, -Diensten oder -Prozessen jegliche notwendigen Aktualisierungen bereitstellen und diese IKT-Produkte, -Dienste und -Prozesse zurückrufen, vom Markt nehmen oder umrüsten, wenn sie den Cybersicherheitsstandards nicht genügen, während Einführer und Händler sicherstellen sollten, dass IKT-Produkte, -Dienste und -Prozesse, die sie in der Union vermarkten, den geltenden Anforderungen genügen und kein Risiko für die Verbraucher in der Union darstellen.

(51) In Zusammenarbeit mit den zuständigen Behörden sollte die ENISA Informationen über das Niveau der Cybersicherheit von IKT-Produkten, -Diensten oder -Prozessen verbreiten, die auf dem Binnenmarkt angeboten werden, und sollte Hersteller oder Anbieter von IKT-Produkten, -Diensten oder -Prozessen verwarnen und sie auffordern, die Sicherheit, auch die Cybersicherheit, ihrer IKT-Produkte, -Dienste oder -Prozesse zu verbessern.

(52) Die ENISA 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 und die Prioritäten im Bereich der Cybersicherheit zu beraten. Um den Bedarf und die Prioritäten im Forschungsbereich zu ermitteln, sollte die ENISA auch die einschlägigen Nutzergruppen konsultieren. Insbesondere könnte eine Zusammenarbeit mit dem Europäischen Forschungsrat und dem Europäischen Innovations- und Technologieinstitut sowie mit dem Institut der Europäischen Union für Sicherheitsstudien eingerichtet werden.

(53) Die ENISA sollte die Normungsgremien, insbesondere die europäischen Normungsgremien, bei der Ausarbeitung von europäischen Schemata für die Cybersicherheitszertifizierung regelmäßig konsultieren.

(54) Cyberbedrohungen bestehen weltweit. Um die Cybersicherheitsstandards, einschließlich der Notwendigkeit der Festlegung gemeinsamer Verhaltensnormen und der Annahme von Verhaltenskodizes, der Verwendung internationaler Normen und des Informationsaustauschs 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 ENISA 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.

(55) Die ENISA sollte in der Lage sein, auf Ersuchen der Mitgliedstaaten und der Organe, Einrichtungen und sonstigen Stellen der Union um Rat und Hilfestellung zu Angelegenheiten, die durch das Mandat der ENISA abgedeckt sind, ad hoc zu reagieren.

(56) In Bezug auf die Führung der ENISA ist es vernünftig und wird empfohlen bestimmte Prinzipien umzusetzen, 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 dezentralen Agenturen dynamischer zu gestalten und ihre Leistung zu verbessern. Die in der Gemeinsamen Erklärung und dem Gemeinsamen Konzept enthaltenen Empfehlungen sollten gegebenenfalls auch in den Arbeitsprogrammen, den Bewertungen und den Berichterstattungs- und Verwaltungsverfahren der ENISA zur Geltung kommen.

(57) Der Verwaltungsrat, der sich aus Vertretern der Mitgliedstaaten und der Kommission zusammensetzt, sollte die allgemeine Ausrichtung der Tätigkeit der ENISA 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 die Ausführung des Haushaltsplans zu überprüfen, angemessene Finanzvorschriften und transparente Verfahren für die Entscheidungsfindung der ENISA festzulegen, das einheitliche Programmplanungsdokument der ENISA anzunehmen, sich eine Geschäftsordnung zu geben, den Exekutivdirektor zu ernennen und über die Verlängerung sowie die Beendigung der Amtszeit des Exekutivdirektors zu beschließen.

(58) Damit die ENISA 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 geeignete Erfahrung 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.

(59) Damit die ENISA reibungslos funktioniert, ist es erforderlich, dass ihr Exekutivdirektor aufgrund seiner Verdienste und nachgewiesenen Verwaltungs- und Managementfähigkeiten ernannt wird und über einschlägige Sachkenntnis und Erfahrungen auf dem Gebiet der Cybersicherheit verfügt. Die Aufgaben des Exekutivdirektors sollten in völliger Unabhängigkeit wahrgenommen werden. Der Exekutivdirektor sollte nach Anhörung der Kommission einen Vorschlag für das jährliche Arbeitsprogramm der ENISA 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 ENISA behandelt wird, ausarbeiten, einen Entwurf eines Voranschlags für die Einnahmen und Ausgaben der ENISA erstellen und den Haushaltsplan ausführen. Der Exekutivdirektor sollte zudem die Möglichkeit haben, Ad-hoc-Arbeitsgruppen einzusetzen, die sich mit wissenschaftlichen, technischen, rechtlichen oder sozioökonomischen Einzelfragen befassen. Insbesondere im Zusammenhang mit der Ausarbeitung eines möglichen europäischen Schemas für die Cybersicherheitszertifizierung (im Folgenden „mögliches Schema“) wird die Einrichtung einer Ad-hoc-Arbeitsgruppe für notwendig

erachtet. Der Exekutivdirektor sollte dafür sorgen, dass die Mitglieder der Ad-hoc-Arbeitsgruppen höchsten fachlichen Ansprüchen genügen, ein ausgewogenes Verhältnis von Frauen und Männern besteht und dass je nach behandelter Einzelfrage gegebenenfalls ein angemessenes Gleichgewicht zwischen öffentlichen Verwaltungen der Mitgliedstaaten, den Organen, Einrichtungen und sonstigen Stellen der Union und dem Privatsektor einschließlich der Wirtschaft, der Nutzer und wissenschaftlicher Sachverständiger für Netz- und Informationssicherheit gewahrt wird.

(60) Der Exekutivrat sollte dazu beitragen, dass der Verwaltungsrat effektiv arbeiten kann. Im Rahmen seiner vorbereitenden Arbeiten für die Beschlüsse des Verwaltungsrats sollte der Exekutivrat 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.

(61) Die ENISA sollte über eine ENISA-Beratungsgruppe als Beratungsgremium verfügen, um einen regelmäßigen Dialog mit dem Privatsektor, den Verbraucherorganisationen und sonstigen relevanten Interessenträgern sicherzustellen. Die vom Verwaltungsrat auf Vorschlag des Exekutivdirektors eingesetzte ENISA-Beratungsgruppe sollte hauptsächlich Fragen behandeln, die die Beteiligten betreffen, und diese der ENISA zur Kenntnis bringen. Die ENISA-Beratungsgruppe sollte vor allem im Hinblick auf den Entwurf des jährlichen Arbeitsprogramms der ENISA hinzugezogen werden. Die Zusammensetzung der ENISA-Beratungsgruppe und die dieser Gruppe übertragenen Aufgaben, sollten gewährleisten, dass die Interessenträger bei der Tätigkeit der ENISA ausreichend vertreten sind.

(62) Die Gruppe der Interessenträger für die Cybersicherheitszertifizierung sollte eingesetzt werden, um der ENISA und der Kommission die Konsultation der maßgeblichen Interessenträger zu erleichtern. Die Gruppe der Interessenträger für die Cybersicherheitszertifizierung sollte sich in ausgewogenem Verhältnis aus Branchenvertretern sowohl der Nachfrage- als auch der Angebotsseite in Bezug auf IKT-Produkte und -Dienste zusammensetzen; insbesondere sollten KMU, Anbieter digitaler Dienste, europäische und internationale Normungsgremien, nationale Akkreditierungsstellen, Datenschutz-Aufsichtsbehörden, Konformitätsbewertungsstellen gemäß der Verordnung (EG) Nr. 765/2008 des Europäischen Parlaments und des Rates ([16]) und die Wissenschaft sowie Verbraucherorganisationen vertreten sein.

(63) Die ENISA sollte über Vorschriften zur Vermeidung und Handhabung von Interessenkonflikten verfügen. Die ENISA 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 ([17]) anwenden. Die Verarbeitung personenbezogener Daten durch die ENISA sollte nach der Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates ([18]) erfolgen. Die ENISA sollte die für die Organe, Einrichtungen und sonstigen Stellen der Union geltenden Bestimmungen über den Umgang mit Informationen, insbesondere mit sensiblen Informationen und Verschlusssachen der Europäischen Union (EUCI), sowie die entsprechenden nationalen Rechtsvorschriften befolgen.

(64) Damit die volle Autonomie und Unabhängigkeit der ENISA gewährleistet ist und sie zusätzliche Aufgaben — auch nicht vorhergesehene Aufgaben in Notfällen — erfüllen kann, sollte die ENISA 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 ENISA beteiligen, finanziert werden sollte. Ein angemessen ausgestatteter Haushaltsplan ist von entscheidender Bedeutung dafür, dass die ENISA ausreichende Kapazitäten hat, um ihren wachsenden Aufgaben zu erfüllen und ihre Ziele zu erreichen. Die Mehrheit der Agenturbediensteten sollte unmittelbar mit der operativen Umsetzung des Mandats der ENISA befasst sein. Dem Sitzmitgliedstaat und anderen Mitgliedstaaten sollte es erlaubt sein, freiwillige Beiträge zum Haushaltsplan der ENISA zu leisten. Sämtliche Zuschüsse aus dem Gesamthaushaltsplan der Europäischen Union sollten dem Haushaltsverfahren der Union unterliegen. Ferner sollte die Rechnungsführung der ENISA durch den Rechnungshof geprüft werden, um Transparenz und Rechenschaftspflicht sicherzustellen.

(65) Die Cybersicherheitszertifizierung spielt eine große Rolle, wenn es darum geht, das Vertrauen in IKT-Produkte, -Dienste und -Prozesse 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, Dienste und Prozesse ein gewisses Maß an Cybersicherheit gewährleisten. Vernetzte und automatisierte Fahrzeuge, elektronische medizinische Geräte, die automatischen Steuerungssysteme der Industrie und intelligente Netze sind, sind nur einige Beispiele von Sektoren, in denen die Zertifizierung bereits breiten Einsatz findet oder in naher Zukunft eingesetzt werden soll. Die unter die Richtlinie (EU) 2016/1148 fallenden Sektoren sind zudem Sektoren, in denen die Cybersicherheitszertifizierung ein maßgeblicher Faktor ist.

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

([17]) 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).

([18]) Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates vom 23. Oktober 2018 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen und sonstigen Stellen der Union, zum freien Datenverkehr und zur Aufhebung der Verordnung (EG) Nr. 45/2001 und des Beschlusses Nr. 1247/2002/EG ABl. L 295 vom 21.11.2018, S. 39).

(66) In ihrer Mitteilung aus dem Jahr 2016 mit dem Titel „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, -Diensten und -Prozessen 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 unionsweiten Zertifizierungsmechanismen zu den Defiziten, die den Binnenmarkt im Bereich der Cybersicherheit beeinträchtigen. Dies macht es für europäische Unternehmen schwerer, im nationalen, unionsweiten und weltweiten Wettbewerb zu bestehen. Es verringert sich dadurch auch das Angebot an tragfähiger und einsetzbarer Cybersicherheitstechnik, auf die Privatpersonen und Unternehmen zugreifen können. Auch in der Mitteilung des Jahres 2017 zur Halbzeitbewertung der Umsetzung der Strategie für den digitalen Binnenmarkt — Ein vernetzter digitaler Binnenmarkt für alle — 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 Binnenmarkts eingedämmt wird.

(67) Derzeit werden IKT-Produkte, -Dienste und -Prozesse, 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 Behörde für die Cybersicherheitszertifizierung ausgestelltes Zertifikat nicht grundsätzlich auch in anderen Mitgliedstaaten anerkannt. Unternehmen müssen somit ihre IKT-Produkte, -Dienste und -Prozesse möglicherweise in mehreren Mitgliedstaaten, in denen sie tätig sind, zertifizieren lassen, um beispielsweise an einer nationalen Ausschreibung teilzunehmen, was ihre Kosten erhöht. 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, was die Verfahren zur gegenseitigen Anerkennung in der Union behindert.

(68) Einige Anstrengungen wurden bereits unternommen, um eine gegenseitige Anerkennung der Zertifikate in der Union zu gewährleisten. 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 SOG-IS nur einige der Mitgliedstaaten. Dies hat aus Binnenmarktsicht zur Folge, dass die Vereinbarungen der Gruppe nur begrenzt wirksam sind.

(69) Daher ist es notwendig, einen gemeinsamen Ansatz zu verfolgen und einen europäischen Rahmen für die Cybersicherheitszertifizierung aufzubauen, auf dessen Grundlage die Anforderungen an die zu entwickelnden europäischen Schemata für die Cybersicherheitszertifizierung festgelegt werden, damit die europäischen Cybersicherheitszertifikate und EU-Konformitätserklärungen für IKT-Produkte, -Dienste oder -Prozesse in allen Mitgliedstaaten anerkannt und verwendet werden können. Dabei ist es wichtig, auf vorhandenen nationalen und internationalen Schemata sowie auf Systemen der gegenseitigen Anerkennung, insbesondere der SOG-IS, aufzubauen und einen reibungslosen Übergang von vorhandenen Schemata im Rahmen solcher Systeme zu Schemata auf der Grundlage des neuen europäischen Rahmens für die Cybersicherheitszertifizierung zu ermöglichen. Mit einem europäischen Rahmen für die Cybersicherheitszertifizierung sollten zwei Ziele verfolgt werden: erstens sollte er dazu beitragen, das Vertrauen in IKT-Produkte, -Dienste und -Prozesse zu erhöhen, die nach Schemata für die europäische Cybersicherheitszertifizierung zertifiziert wurden. Zweitens sollte er dazu beitragen, dass sich vielfältige, sich widersprechende oder überlappende nationale Schemata für die Cybersicherheitszertifizierung vermeiden lassen, und so die Kosten für auf dem digitalen Binnenmarkt tätige Unternehmen senken. Die europäischen Schemata für die Cybersicherheitszertifizierung sollten nichtdiskriminierend sein und sich auf europäische oder internationale Normen stützen, sofern diese Normen nicht unwirksam oder unangemessen im Hinblick auf die Erreichung der legitimen Ziele der Union in diesem Bereich sind.

(70) Der europäische Rahmen für die Cybersicherheitszertifizierung sollte in einheitlicher Weise in allen Mitgliedstaaten eingeführt werden, damit es nicht aufgrund unterschiedlicher Anforderungsniveaus zwischen den Mitgliedstaaten zu einem „Zertifizierungsshopping“ kommt.

(71) Europäische Schemata für die Cybersicherheitszertifizierung sollten auf dem auf internationaler und nationaler Ebene bereits Vorhandenen und erforderlichenfalls auf den von Gremien und Konsortien erstellten technischen Spezifikationen aufbauen, wobei die derzeitigen Stärken genutzt und Schwachstellen bewertet und behoben werden sollten.

(72) Es bedarf flexibler Cybersicherheitslösungen, damit die Branche den Cyberbedrohungen immer einen Schritt voraus ist und daher sollte jedes Zertifizierungsschema so gestaltet werden, dass das Risiko eines schnellen Veraltens vermieden wird.

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

(74) Die Rechtsvorschriften der Union, in denen bestimmte Vorschriften zur Zertifizierung von IKT-Produkten, -Diensten und -Prozessen festgelegt sind, bleiben von den Bestimmungen dieser Verordnung unberührt. Insbesondere enthält die Verordnung (EU) 2016/679 Bestimmungen zur Einführung von Zertifizierungsverfahren sowie von Datenschutzsiegeln und -prüfzeichen, die dem Nachweis dienen, dass die für die Datenverarbeitung Verantwortlichen und die Auftragsverarbeiter bei der Verarbeitung von Daten die Bestimmungen der genannten Verordnung einhalten. Solche Zertifizierungsverfahren sowie Datenschutzsiegel und -prüfzeichen sollten den betroffenen Personen einen raschen Überblick über das Datenschutzniveau einschlägiger IKT-Produkte, -Dienste und -Prozesse ermöglichen. Die Zertifizierung von Datenverarbeitungsvorgängen, die unter die Verordnung (EU) 2016/679 fallen, auch wenn solche Vorgänge in IKT-Produkte, -Dienste und -Prozesse eingebettet sind, bleibt von der vorliegenden Verordnung unberührt.

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

(76) Die in europäischen Schemata für die Cybersicherheitszertifizierung zu verwendenden technischen Spezifikationen sollten unter Beachtung der in Anhang II der Verordnung (EU) Nr. 1025/2012 des Europäischen Parlaments und des Rates ([19]) festgelegten Anforderungen bestimmt werden. Gewisse Abweichungen von diesen Anforderungen könnten jedoch in hinreichend begründeten Fällen als notwendig erachtet werden, wenn diese technischen Spezifikationen in einem europäischen Schema für die Cybersicherheitszertifizierung in der Vertrauenswürdigkeitsstufe „hoch" verwendet werden sollen. Die Gründe für solche Abweichungen sollten öffentlich zugänglich gemacht werden.

(77) Eine Konformitätsbewertung ist ein Verfahren, mit dem bewertet wird, ob bestimmte Anforderungen an ein IKT-Produkt, einen IKT-Dienst oder einen IKT-Prozess erfüllt werden. Dieses Verfahren wird von einem unabhängigen Dritten, bei dem es sich nicht um den Hersteller oder den Anbieter der IKT-Produkte, -Dienste oder -Prozesse, welche bewertet werden, handelt, durchgeführt. Ein europäisches Cybersicherheitszertifikat sollte nach der erfolgreichen Bewertung eines IKT-Produkts, -Dienstes oder -Prozesses ausgestellt werden. Ein europäisches Cybersicherheitszertifikat sollte als Bestätigung gelten, dass die Bewertung ordnungsgemäß durchgeführt wurde. Je nach Vertrauenswürdigkeitsstufe sollte im europäischen Schema für die Cybersicherheitszertifizierung angegeben werden, ob ein europäisches Cybersicherheitszertifikat von einer privaten oder einer öffentlichen Stelle auszustellen ist. Die Konformitätsbewertung und die Zertifizierung an sich können nicht garantieren, dass die zertifizierten IKT-Produkte, -Dienste und -Prozesse cybersicher sind. Es handelt sich vielmehr um Verfahren und technische Methoden, um zu bescheinigen, dass die IKT-Produkte, -Dienste und -Prozesse geprüft wurden und bestimmte Anforderungen an die Cybersicherheit erfüllen, wie sie anderweitig, beispielsweise in technischen Normen, festgelegt sind.

(78) Die Auswahl der angemessenen Zertifizierung und der dazugehörigen Sicherheitsanforderungen durch die Nutzer der europäischen Cybersicherheitszertifizierung sollte auf der Grundlage einer Risikoanalyse der Verwendung des IKT-Produkts, -Dienstes oder -Prozesses erfolgen. Dementsprechend sollte die Vertrauenswürdigkeitsstufe das mit der beabsichtigten Verwendung eines IKT-Produkts, -Dienstes oder -Prozesses verbundene Risiko widerspiegeln.

([19]) Verordnung (EU) Nr. 1025/2012 des Europäischen Parlaments und des Rates vom 25. Oktober 2012 zur europäischen Normung, zur Änderung der Richtlinien 89/686/EWG und 93/15/EWG des Rates sowie der Richtlinien 94/9/EG, 94/25/EG, 95/16/EG, 97/23/EG, 98/34/EG, 2004/22/EG, 2007/23/EG, 2009/23/EG und 2009/105/EG des Europäischen Parlaments und des Rates und zur Aufhebung des Beschlusses 87/95/EWG des Rates und des Beschlusses Nr. 1673/2006/EG des Europäischen Parlaments und des Rates (ABl. L 316 vom 14.11.2012, S. 12).

(79) Europäische Schemata für die Cybersicherheitszertifizierung könnten eine Konformitätsbewertung vorsehen, die unter der alleinigen Verantwortung des Herstellers oder Anbieters von IKT-Produkten, -Diensten und -Prozessen durchzuführen wäre (im Folgenden „Selbstbewertung der Konformität"). In diesen Fällen sollte es ausreichen, dass der Hersteller oder Anbieter von IKT-Produkten, -Diensten oder -Prozessen selbst alle Überprüfungen vornimmt, um sicherzustellen, dass die IKT-Produkte, -Dienste oder -Prozesse mit dem europäischen Schema für die Cybersicherheitszertifizierung konform sind. Die Selbstbewertung der Konformität sollte für IKT-Produkte, -Dienste oder -Prozesse von geringer Komplexität, die ein geringes Risiko für die Öffentlichkeit darstellen, wie bei einfacher Konzeption und einfachem Herstellungsmechanismus, als angemessen angesehen werden. Zudem sollte die Selbstbewertung der Konformität nur dann für IKT-Produkte, IKT-Dienste oder IKT-Prozesse erlaubt sein, wenn sie der Vertrauenswürdigkeitsstufe „niedrig" entsprechen.

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

(81) Ein Hersteller oder Anbieter von IKT-Produkten, -Diensten oder -Prozessen, der eine Selbstbewertung der Konformität durchführt, sollte die EU-Konformitätserklärung im Rahmen des Konformitätsbewertungsverfahrens abfassen und unterzeichnen können. Eine EU-Konformitätserklärung ist ein Dokument, welches bestätigt, dass das betreffende IKT-Produkt, der betreffende IKT-Dienst oder der betreffende IKT-Prozess die Anforderungen des Schemas erfüllt. Durch die Abfassung und Unterzeichnung der EU-Konformitätserklärung übernimmt der Hersteller oder Anbieter die Verantwortung dafür, dass das IKT-Produkt, der IKT-Dienst oder der IKT-Prozess die rechtlichen Anforderungen des europäischen Schemas für die Cybersicherheitszertifizierung erfüllt. Eine Kopie der EU-Konformitätserklärung sollte der nationalen Behörde für die Cybersicherheitszertifizierung und der ENISA vorgelegt werden.

(82) Hersteller oder Anbieter von IKT-Produkten, -Diensten und -Prozessen sollten die EU-Konformitätserklärung, die technische Dokumentation und alle weiteren einschlägigen Informationen in Bezug auf die Konformität der IKT-Produkte, -Dienste oder -Prozesse mit einem System während eines Zeitraums, der im einschlägigen europäischen Schema für die Cybersicherheitszertifizierung festgelegt ist, für die zuständige nationale Behörde für die Cybersicherheitszertifizierung bereithalten. In der technischen Dokumentation sollten die in diesem System geltenden Anforderungen aufgeführt werden und die Konzeption, Herstellung und Funktionsweise des IKT-Produkts, -Dienstes oder -Prozesses erfasst werden. Die technische Dokumentation sollte so erstellt werden, dass es möglich ist, die Konformität eines IKT-Produkts oder -Dienstes mit den in diesem System geltenden Anforderungen zu bewerten.

(83) Bei der Gestaltung des Rahmens des europäischen Schemas für die Cybersicherheitszertifizierung sollte die Einbeziehung der Mitgliedstaaten sowie eine angemessene Einbeziehung der Interessenträger berücksichtigt werden; ferner sollte die Rolle der Kommission während der Planung und Vorlage eines europäischen Schemas für die Cybersicherheitszertifizierung, der Erteilung des entsprechenden Auftrags sowie der Ausarbeitung, der Annahme und der Überprüfung eines europäischen Schemas für die Cybersicherheitszertifizierung festgelegt werden.

(84) Die Kommission sollte mit Unterstützung der Europäischen Gruppe für die Cybersicherheitszertifizierung und der Gruppe der Interessenträger für die Cybersicherheitszertifizierung im Anschluss an eine offene und umfassende Konsultation ein fortlaufendes Arbeitsprogramm der Union für europäische Schemata für die Cybersicherheitszertifizierung ausarbeiten und in Form eines nicht verbindlichen Instruments veröffentlichen. Das fortlaufende Arbeitsprogramm der Union sollte ein strategisches Dokument sein und insbesondere der Branche, den nationalen Behörden und den Normungsgremien ermöglichen, sich auf die künftigen Europäischen Schemata für die Cybersicherheitszertifizierung vorzubereiten. Das fortlaufende Arbeitsprogramm der Union sollte eine mehrjährige Übersicht über die Aufträge für die Ausarbeitung möglicher Systeme umfassen, die die Kommission der ENISA aus bestimmten Gründen zu erteilen beabsichtigt. Die Kommission sollte dieses fortlaufende Arbeitsprogramm der Union im Rahmen des fortlaufenden Plans für die IKT-Normung und bei der Erstellung ihrer Normungsaufträge an die europäischen Normungsorganisationen berücksichtigen. Wegen der raschen Einführung und Übernahme neuer Technologien sowie die Entstehung bislang unbekannter Cybersicherheitsrisiken und Gesetzgebungs- und Marktentwicklungen sollte die Kommission oder die Europäische Gruppe für die Cybersicherheitszertifizierung befugt sein, die ENISA mit der Ausarbeitung möglicher Zertifizierungsschemata, die nicht im fortlaufenden Arbeitsprogramm der Union enthalten waren, zu beauftragen. In solchen Fällen sollten die Kommission und die Europäische Gruppe für die Cybersicherheitszertifizierung auch die Notwendigkeit eines solchen Auftrags bewerten, wobei die allgemeinen Zielsetzungen und Vorgaben dieser Verordnung und die Notwendigkeit der Kontinuität bei der Planung der ENISA und der Nutzung der Ressourcen durch die ENISA zu berücksichtigen sind.

Im Anschluss an einen solchen Auftrag sollte die ENISA ohne ungebührliche Verzögerung mögliche Zertifizierungsschemata für bestimmte IKT- Produkte -Dienste und -Prozesse, ausarbeiten. Die Kommission sollte die positiven und negativen Auswirkungen ihres Auftrags auf den spezifischen Markt und insbesondere auf KMU, Innovation, die Schranken für den Eintritt in diesen Markt und die Kosten für die Endverbraucher bewerten. Die Kommission sollte befugt sein, auf der Grundlage des von der ENISA vorbereiteten möglichen Schemas das europäische Schema für die Cybersicherheitszertifizierung mittels eines Durchführungsrechtsakts anzunehmen. Unter Berücksichtigung des allgemeinen Zwecks dieser Verordnung und der in ihr festgelegten Sicherheitsziele sollten in den von der Kommission angenommenen europäischen Schemata für die Cybersicherheitszertifizierung Mindestbestimmungen in Bezug auf den Gegenstand, den Anwendungsbereich und die Funktionsweise des einzelnen Schemas festgelegt werden. Unter diese Bestimmungen sollte unter anderem Folgendes fallen: Anwendungsbereich und Ziel der Cybersicherheitszertifizierung, darunter auch die Kategorien von IKT-Produkten, -Diensten und -Prozessen, 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“ oder „hoch“) sowie gegebenenfalls die Bewertungsniveaus. Die ENISA sollte einen Auftrag der Europäischen Gruppe für die Cybersicherheitszertifizierung ablehnen können. Solche Entscheidungen sollten gebührend begründet und vom Verwaltungsrat getroffen werden.

(85) Die ENISA sollte eine eigene Website unterhalten, auf der sie über die europäischen Schemata für die Cybersicherheitszertifizierung informiert und für diese wirbt und auf der unter anderem die Aufträge für die Ausarbeitung eines möglichen Schemas und die Rückmeldungen im Rahmen des Konsultationsverfahrens, das von der ENISA in der Ausarbeitungsphase durchgeführt wird, zur Verfügung stehen. Auf der Website sollten auch Informationen über die europäischen Cybersicherheitszertifikate und die nach dieser Verordnung ausgestellten EU-Konformitätserklärungen einschließlich Informationen zum Widerruf und Ablauf solcher europäischen Cybersicherheitszertifikate und EU-Konformitätserklärungen bereitgestellt werden. Auf der Website sollten auch diejenigen nationalen Schemata für die Cybersicherheitszertifizierung angegeben werden, die durch ein europäisches Schema für die Cybersicherheitszertifizierung ersetzt wurden.

(86) Die Vertrauenswürdigkeit eines europäischen Zertifizierungsschemas ist die Grundlage für das Vertrauen, dass ein IKT-Produkt, -Dienst oder -Prozess den Sicherheitsanforderungen eines spezifischen europäischen Schemas für die Cybersicherheitszertifizierung genügt. Um die Kohärenz des Rahmens für ein europäisches Schema für die Cybersicherheitszertifizierung zu gewährleisten, sollte ein europäisches Schema für die Cybersicherheitszertifizierung die Vertrauenswürdigkeitsstufen für europäische Cybersicherheitszertifikate und EU-Konformitätserklärungen, die im Rahmen dieses Schemas ausgestellt werden, angeben können. Jedes europäische Cybersicherheitszertifikat könnte sich auf eine der Vertrauenswürdigkeitsstufen „niedrig“, „mittel“ oder „hoch“ beziehen, wohingegen sich die EU-Konformitätserklärung nur auf die Vertrauenswürdigkeitsstufe „niedrig“ beziehen könnte. Die Vertrauenswürdigkeitsstufen würden die entsprechende Strenge und Gründlichkeit für die Bewertung des IKT-Produkts, -Dienstes oder -Prozesses vorgeben und durch Bezugnahme auf die diesbezüglichen technischen Spezifikationen, Normen und Verfahren einschließlich technischer Prüfungen, deren Zweck in der Minderung oder Prävention der Gefahr von Vorfällen besteht, gekennzeichnet sein. Jede Vertrauenswürdigkeitsstufe sollte in den verschiedenen Bereichen der Sektoren, in denen die Zertifizierung angewandt wird, einheitlich sein.

(87) In einem europäischen Schema für die Cybersicherheitszertifizierung können je nach Strenge und Gründlichkeit der verwendeten Evaluierungsmethode mehrere Bewertungsniveaus angegeben werden. Die Evaluierungsstufen sollten jeweils einer der Vertrauenswürdigkeitsstufen entsprechen und mit einer entsprechenden Kombination von Vertrauenswürdigkeitskomponenten verknüpft sein sollten. Für alle Vertrauenswürdigkeitsstufen sollte das IKT-Produkt, der IKT-Dienst oder der IKT-Prozess eine Reihe sicherer Funktionen enthalten, die im jeweiligen System festgelegt sind, so unter anderem eine voreingestellte sichere Konfiguration, einen signierten Code, ein sicheres Aktualisierungsverfahren und die Reduzierung von Exploits sowie eine vollständige Absicherung von Stapelspeicher (Stack) oder dynamischem Speicher (Heap). Diese Funktionen sollten weiterentwickelt und gepflegt werden, wobei sicherheitsorientierte Entwicklungskonzepte und dazugehörige Instrumente zu verwenden sind, um sicherzustellen, dass wirksame Software- und Hardware-Mechanismen zuverlässig integriert werden.

(88) 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-Produkts -Dienstes oder -Prozesses durch die Konformitätsbewertungsstelle umfassen. Schließt die Zertifizierung IKT-Prozesse ein, sollte auch das Verfahren zur Konzipierung, Entwicklung und Pflege eines IKT-Produkts oder -Dienstes einer technischen Überprüfung unterzogen werden. Ist in einem europäischen Schema für die Cybersicherheitszertifizierung eine Selbstbewertung der Konformität vorgesehen, so sollte es genügen, wenn der Hersteller oder Anbieter von IKT- Produkten, Diensten oder Prozessen eine Selbstbewertung der Konformität des IKT-Produkts, -Dienstes oder -Prozesses, mit dem Zertifizierungsschema vornimmt.

(89) Bei der Vertrauenswürdigkeitsstufe „mittel“ sollte sich die Bewertung — zusätzlich zu den Anforderungen bei der Vertrauenswürdigkeitsstufe „niedrig“ — mindestens auf eine Überprüfung der Konformität der Sicherheitsfunktionen des IKT-Produkts, -Dienstes oder -Prozesses mit seiner technischen Dokumentation stützen.

(90) Bei der Vertrauenswürdigkeitsstufe „hoch“ sollte sich die Bewertung — zusätzlich zu den Anforderungen bei der Vertrauenswürdigkeitsstufe „mittel“ — mindestens auf einen Wirksamkeitstest stützen, bei dem die Widerstandsfähigkeit der Sicherheitsfunktionen des IKT-Produkts, -Dienstes oder -Prozesses gegen gründlich vorbereitete Cyberattacken bewertet wird, die von Akteuren mit umfangreichen Fähigkeiten und Ressourcen durchgeführt wird.

(91) Der Rückgriff auf eine europäische Cybersicherheitszertifizierung und eine EU-Konformitätserklärung sollte freiwillig bleiben, sofern im Unionsrecht oder in entsprechend dem Unionsrecht erlassenen Rechtsvorschriften der Mitgliedstaaten nichts anderes festgelegt ist. Falls es keine harmonisierten Unionsrechtsvorschriften gibt, können die Mitgliedstaaten nationale technische Vorschriften gemäß der Richtlinie (EU) 2015/1535 des Europäischen Parlaments und des Rates ([20]) erlassen. Die Mitgliedstaaten können auch im Zusammenhang mit öffentlichen Ausschreibungen und der Richtlinie 2014/24/EU des Europäischen Parlaments und des Rates ([21]) auf eine europäische Cybersicherheitszertifizierung zurückgreifen.

(92) In einigen Bereichen könnte es künftig notwendig werden, bestimmte Anforderungen an die Cybersicherheit und die entsprechende Zertifizierung für bestimmte IKT-Produkte, -Dienste oder -Prozesse verbindlich vorzuschreiben, um das Niveau der Cybersicherheit in der Union zu erhöhen. Die Kommission sollte die Auswirkungen der angenommenen europäischen Schemata für die Cybersicherheitszertifizierung auf die Verfügbarkeit sicherer IKT-Produkte, -Dienste und -Prozesse im Binnenmarkt regelmäßig überwachen und sollte regelmäßig bewerten, inwieweit die Zertifizierungsschemata durch die Hersteller oder Anbieter von IKT-Produkten, -Diensten oder -Prozessen in der Union genutzt werden. Die Effizienz der europäischen Schemata für die Cybersicherheitszertifizierung und die Frage, ob bestimmte Systeme verbindlich vorgeschrieben werden sollten, sollte anhand der Rechtsvorschriften der Union im Bereich der Cybersicherheit, insbesondere der Richtlinie (EU) 2016/1148, unter Berücksichtigung der Sicherheit der von Betreibern wesentlicher Dienste genutzten Netz- und Informationssysteme bewertet werden.

(93) Die europäischen Cybersicherheitszertifikate und die EU-Konformitätserklärung sollten den Endnutzern dabei helfen, kundige Entscheidungen zu treffen. Daher sollten IKT-Produkte, -Dienste und -Prozesse, die zertifiziert wurden oder für die eine EU-Konformitätserklärung ausgestellt wurde, strukturierte Informationen beigegeben werden, die an das erwartete technische Niveau des vorgesehenen Endnutzers angepasst sind. Alle diese Informationen sollten online verfügbar sein, und gegebenenfalls physisch bereitgestellt werden. Der Endnutzer sollte Zugang zu Informationen über die Kennnummer des Zertifizierungsschemas, die Vertrauenswürdigkeitsstufe, die Beschreibung der Cybersicherheitsrisiken in Verbindung mit dem IKT-Produkt, -Dienst oder -Prozess sowie die ausstellende Stelle haben oder eine Kopie des europäischen Cybersicherheitszertifikats erhalten können. Darüber hinaus sollten die Endnutzer über die Politik des Herstellers oder Anbieters von IKT-Produkten, -Diensten oder -Prozessen zur Förderung der Cybersicherheit, d. h. darüber, wie lange ein Endnutzer Aktualisierungen oder Patches im Bereich der Cybersicherheit erwarten kann, informiert sein. Gegebenenfalls sollten Leitlinien über Maßnahmen oder Einstellungen, die der Endnutzer von IKT-Produkten oder -Diensten zur Aufrechterhaltung oder Verbesserung der Cybersicherheit vornehmen kann, und Kontaktinformationen einer zentralen Anlaufstelle zur Meldung von Cyberangriffen und zur Unterstützung im Fall von Cyberangriffen (neben der automatischen Berichterstattung) zur Verfügung gestellt werden. Diese Informationen sollten regelmäßig auf den neuesten Stand gebracht werden und auf einer Website, die Informationen über das europäische Schema für die Cybersicherheitszertifizierung bereitstellt, zur Verfügung stehen.

(94) Mit Blick auf die Ziele dieser Verordnung und zur Vermeidung einer Fragmentierung des Binnenmarkts sollten nationale Schemata oder Verfahren für die Cybersicherheitszertifizierung für die IKT-Produkte, -Dienste oder -Prozesse, die unter ein europäisches Schema für die Cybersicherheitszertifizierung fallen, ab einem Zeitpunkt unwirksam werden, den die Kommission in Durchführungsrechtsakten festlegt. Zudem sollten die Mitgliedstaaten keine neuen nationalen Schemata für die Cybersicherheitszertifizierung der IKT-Produkte, -Dienste oder -Prozesse einführen, die bereits unter ein geltendes europäisches Schema für die Cybersicherheitszertifizierung fallen. Allerdings sollte es den Mitgliedstaaten freistehen, aus Gründen der nationalen Cybersicherheit nationale Cyberzertifizierungsschemata einzuführen oder beizubehalten. Die Mitgliedstaaten sollten die Kommission und die Europäische Gruppe für die Cybersicherheitszertifizierung über ihre Absicht unterrichten, neue nationale Schemata für die Cybersicherheitszertifizierung auszuarbeiten. Die Kommission und die Europäische Gruppe für die Cybersicherheitszertifizierung sollten die Auswirkungen des neuen nationalen Schemas für die Cybersicherheitszertifizierung auf das ordnungsgemäße Funktionieren des Binnenmarkts und im Hinblick auf das strategische Interesse bewerten, stattdessen einen Auftrag für ein europäisches Schema für die Cybersicherheitszertifizierung zu erteilen.

(95) Die europäischen Schemata für die Cybersicherheitszertifizierung sollen dabei helfen, die Cybersicherheitsverfahren in der Union zu harmonisieren. Sie müssen dazu beitragen, das Niveau der Cybersicherheit in der Union zu erhöhen. Das Design der europäischen Schemata für die Cybersicherheitszertifizierung sollte weitere Innovationen im Bereich der Cybersicherheit berücksichtigen und ermöglichen werden.

([20]) Richtlinie (EU) 2015/1535 des Europäischen Parlaments und des Rates vom 9. September 2015 über ein Informationsverfahren auf dem Gebiet der technischen Vorschriften und der Vorschriften für die Dienste der Informationsgesellschaft (ABl. L 241 vom 17.9.2015, S. 1.)

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

(96) Die europäischen Schemata für die Cybersicherheitszertifizierung sollten die derzeitigen Methoden der Software- und Hardware-Entwicklung und insbesondere die Auswirkungen häufiger Software- oder Firmware-Aktualisierungen zu einzelnen europäischen Cybersicherheitszertifikaten berücksichtigen. Bei den europäischen Schemata für die Cybersicherheitszertifizierung sollten die Bedingungen angegeben werden, unter denen eine Aktualisierung erfordern kann, dass ein IKT-Produkt, ein IKT-Dienst oder ein IKT-Prozess neu zertifiziert werden muss oder dass der Umfang des spezifischen europäische Cybersicherheitszertifikats eingeschränkt werden muss, wobei die möglichen nachteiligen Auswirkungen der Aktualisierung auf die Einhaltung der Sicherheitsanforderungen des Zertifikats zu berücksichtigen sind.

(97) Sobald ein europäisches Schema für die Cybersicherheitszertifizierung eingeführt worden ist, sollten die Hersteller oder die Anbieter von IKT-Produkten, -Diensten oder -Prozessen die Zertifizierung ihrer IKT-Produkte, -Dienste oder -Prozesse bei einer nationalen Konformitätsbewertungsstelle ihrer Wahl an einem beliebigen Ort in der Union beantragen können. Die Konformitätsbewertungsstellen sollten, sofern sie bestimmten in dieser Verordnung festgelegten Anforderungen genügen, von einer nationalen 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 weiterhin erfüllt. Die nationalen Akkreditierungsstellen sollten die einer Konformitätsbewertungsstelle erteilte Akkreditierung beschränken, aussetzen oder widerrufen, wenn die Voraussetzungen für die Akkreditierung nicht erfüllt wurden oder nicht mehr erfüllt werden oder wenn die Konformitätsbewertungsstelle gegen diese Verordnung verstößt.

(98) Verweise im nationalen Recht, die sich auf nationale Normen beziehen, die aufgrund des Inkrafttretens eines europäischen Schemas für die Cybersicherheitszertifizierung keine Rechtswirkung mehr haben, können zu Verwirrung führen. Daher sollten die Mitgliedstaaten der Annahme eines europäischen Schemas für die Cybersicherheitszertifizierung in ihren nationalen Rechtsvorschriften Rechnung zu tragen.

(99) Zur Erreichung gleichwertiger Standards in der gesamten Union, zur Erleichterung der gegenseitigen Anerkennung und zur Förderung der allgemeinen Akzeptanz der Europäischen Cybersicherheitszertifikate und EU-Konformitätserklärungen bedarf es eines Systems der gegenseitigen Begutachtung der nationalen Behörden für die Cybersicherheitszertifizierung. Die gegenseitige Begutachtung sollte Verfahren für Folgendes umfassen: Überwachung der Übereinstimmung der IKT-Produkte, -Dienste und -Prozesse mit den europäischen Cybersicherheitszertifikaten, Überwachung der Verpflichtungen der Hersteller oder Anbieter von IKT-Produkten, -Diensten und -Prozessen, die eine Selbstbewertung der Konformität vornehmen, Überwachung der Konformitätsbewertungsstellen sowie Angemessenheit des Fachwissens des Personals der Einrichtungen, die Zertifikate für die Vertrauenswürdigkeitsstufe „hoch“ ausstellen. Die Kommission sollte im Wege von Durchführungsrechtsakten mindestens einen Fünfjahresplan für gegenseitige Begutachtungen sowie Kriterien und Methoden für die Abwicklung der gegenseitigen Begutachtungen festlegen können.

(100) Unbeschadet des allgemeinen Systems der gegenseitigen Begutachtung, das zwischen allen nationalen Behörden für die Cybersicherheitszertifizierung im Rahmen der europäischen Cybersicherheitszertifizierung eingerichtet werden soll, können bestimmte Schemata für die europäische Cybersicherheit ein Verfahren zur gegenseitigen Begutachtung der Stellen für die Ausstellung europäischer Cybersicherheitszertifikate für IKT-Produkte, -Dienste und -Prozesse auf der Vertrauenswürdigkeitsstufe „hoch“ im Rahmen solcher Schemata umfassen. Die Gruppe für die Cybersicherheitszertifizierung sollte die Umsetzung der Verfahren der gegenseitigen Begutachtung unterstützen. Bei solchen gegenseitigen Begutachtungen sollte insbesondere bewertet werden, ob die betreffenden Stellen ihre Aufgaben einheitlich ausführen; zudem können sie Einspruchsmöglichkeiten umfassen. Die Ergebnisse der gegenseitigen Begutachtungen sollten veröffentlicht werden. Die betreffenden Stellen können entsprechend geeignete Maßnahmen ergreifen, um ihre Verfahren und Sachkenntnisse anzupassen.

(101) Die Mitgliedstaaten sollten eine oder mehrere nationale Behörden für die Cybersicherheitszertifizierung benennen, die die Einhaltung der sich aus dieser Verordnung ergebenden Verpflichtungen beaufsichtigen. Eine nationale Behörde für die Cybersicherheitszertifizierung kann eine bereits bestehende oder eine neue Behörde sein. Ein Mitgliedstaat sollte im gegenseitigen Einvernehmen mit einem anderen Mitgliedstaat auch eine oder mehrere nationale Behörden für die Cybersicherheitszertifizierung im Hoheitsgebiet dieses anderen Mitgliedstaats benennen können.

(102) Die nationalen Behörden für die Cybersicherheitszertifizierung sollten insbesondere die Verpflichtungen der in ihrem jeweiligen Hoheitsgebiet niedergelassenen Hersteller oder Anbieter von IKT-Produkten, -Diensten oder -Prozessen 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 diese in einem europäischen Schema für die Cybersicherheitszertifizierung festgelegte zusätzliche Anforderungen erfüllen, und einschlägige Entwicklungen auf dem Gebiet der Cybersicherheitszertifizierung verfolgen. Die nationalen Behörden für die Cybersicherheitszertifizierung sollten auch Beschwerden bearbeiten, die von natürlichen oder juristischen Personen in Bezug auf die von diesen Behörden ausgestellten europäischen Cybersicherheitszertifikate oder die in Verbindung mit den europäischen Cybersicherheitszertifikaten 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 die nationalen Behörden für die Cybersicherheitszertifizierung mit anderen nationalen Behörden für die Cybersicherheitszertifizierung und anderen öffentlichen Stellen zusammenarbeiten, auch indem sie Informationen über die etwaige Nichtkonformität von IKT-Produkten, -Diensten und -Prozessen mit den Anforderungen dieser Verordnung oder bestimmten europäischen Schemata für die Cybersicherheitszertifizierung austauschen. Die Kommission sollte diesen Informationsaustausch erleichtern, indem sie ein allgemeines elektronisches Informationssystem zur Unterstützung bereitstellt, zum Beispiel das internetgestützte Informations- und Kommunikationssystem zur europaweiten Marktüberwachung (Information and Communication System on Market Surveillance — ICSMS) und das gemeinschaftliche System zum raschen Austausch von Informationen über die Gefahren bei der Verwendung von Konsumgütern (Community system for the rapid exchange of information on dangers arising from the use of consumer products — RAPEX), die in Übereinstimmung mit der Verordnung (EG) Nr. 765/2008 bereits von Marktüberwachungsbehörden genutzt werden.

(103) Für eine einheitliche Anwendung des europäischen Rahmens für die Cybersicherheitszertifizierung sollte eine europäische Gruppe für die Cybersicherheitszertifizierung eingesetzt werden, die sich aus Vertretern der nationalen Behörden für die Cybersicherheitszertifizierung oder anderer zuständiger nationaler Behörden zusammensetzt. Die Gruppe für die Cybersicherheitszertifizierung 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 ENISA bei der Ausarbeitung der möglichen Cybersicherheitszertifizierungsschemata unterstützen und mit ihr eng zusammenarbeiten, in entsprechend begründeten Fällen die ENISA mit der Ausarbeitung eines möglichen Schemas beauftragen, an die ENISA gerichtete Stellungnahmen zu möglichen Schemata annehmen, und an die Kommission gerichtete Stellungnahmen zur Pflege und Überprüfung vorhandener europäischer Schemata für die Cybersicherheitszertifizierung annehmen. Die Gruppe für die Cybersicherheitszertifizierung sollte den Austausch von bewährten Verfahren und Sachkenntnissen zwischen den verschiedenen nationalen Behörden für die Cybersicherheitszertifizierung, die für die Ermächtigung der Konformitätsbewertungsstellen und die Ausstellung von Europäischen Cybersicherheitszertifikaten zuständig sind, erleichtern.

(104) Zur Sensibilisierung und um die Akzeptanz künftiger europäischer Schemata für die Cybersicherheitssicherheit zu erhöhen, kann die 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, -Dienste und -Prozesse hervorheben.

(105) Da die IKT-Lieferketten weltumspannend sind, kann die Union zur weiteren Erleichterung des Handels gemäß Artikel 218 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV) Abkommen über die gegenseitige Anerkennung von europäischen Cybersicherheitszertifikaten schließen. Die Kommission kann unter Berücksichtigung der Ratschläge der ENISA und der europäischen Gruppe für die Cybersicherheitszertifizierung die Aufnahme entsprechender Verhandlungen empfehlen. In jedem europäischen Schema für die Cybersicherheitszertifizierung sollten spezifische Bedingungen für diese Abkommen über die gegenseitige Anerkennung bei Drittländern vorgesehen werden.

(106) Zur Gewährleistung einheitlicher Bedingungen für die Durchführung dieser Verordnung sollten der Kommission Durchführungsbefugnisse übertragen werden. Diese Befugnisse sollten nach Maßgabe der Verordnung (EU) Nr. 182/2011 des Europäischen Parlaments und des Rates ([22]) ausgeübt werden.

(107) Das Prüfverfahren sollte für die Annahme der Durchführungsrechtsakte über die europäischen Schemata für die Cybersicherheitszertifizierung von IKT-Produkten, -Diensten oder -Prozessen, für die Annahme von Durchführungsrechtsakten über die Modalitäten für die Durchführung von Umfragen durch die ENISA, für die Annahme von Durchführungsrechtsakten über einen Plan für die gegenseitige Begutachtung der nationalen Behörden für die Cybersicherheitszertifizierung sowie für die Annahme von Durchführungsrechtsakten über die Umstände, Formate und Verfahren der Notifikation akkreditierter Konformitätsbewertungsstellen durch die nationalen Behörden für die Cybersicherheitszertifizierung bei der Kommission verwendet werden.

(108) Die Tätigkeit der ENISA sollte regelmäßig und unabhängig bewertet werden. Diese Bewertung sollte sich darauf beziehen, inwieweit die ENISA ihre Ziele erreicht, wie sie arbeitet und inwieweit ihre Aufgaben relevant sind, insbesondere ihre Aufgaben bezüglich der operativen Zusammenarbeit auf Unionsebene. Zudem sollten Wirkung, Wirksamkeit und Effizienz des europäischen Rahmens für Cybersicherheitszertifizierung bewertet werden. Im Falle einer Überprüfung sollte die Kommission bewerten, wie die Rolle der ENISA als Bezugspunkt für Beratung und Sachkenntnis verstärkt werden kann und sollte ebenfalls die Möglichkeit einer Rolle der ENISA bei der Unterstützung der Bewertung von IKT-Produkten, -Diensten und -Prozessen aus Drittländern, die auf den Unionsmarkt gelangen und gegen die Unionsvorschriften verstoßen, bewerten.

([22]) Verordnung (EU) Nr. 182/2011 des Europäischen Parlaments und des Rates vom 16. Februar 2011 zur Festlegung der allgemeinen Regeln und Grundsätze, nach denen die Mitgliedstaaten die Wahrnehmung der Durchführungsbefugnisse durch die Kommission kontrollieren (ABl. L 55 vom 28.2.2011, S. 13).

(109) Da die Ziele dieser Verordnung von den Mitgliedstaaten nicht ausreichend verwirklicht werden können, sondern vielmehr wegen ihres Umfangs und ihrer Wirkungen auf Unionsebene besser zu verwirklichen sind, kann die Union im Einklang mit dem in Artikel 5 des Vertrags über die Europäische Union (EUV) 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.

(110) Die Verordnung (EU) Nr. 526/2013 sollte aufgehoben werden —

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 ENISA (Agentur der Europäischen Union für Cybersicherheit) und

b) ein Rahmen für die Festlegung europäischer Schemata für die Cybersicherheitszertifizierung, mit dem Ziel, für IKT-Produkte und -Dienste und -Prozesse in der Union ein angemessenes Maß an Cybersicherheit zu gewährleisten und mit dem Ziel, eine Fragmentierung des Binnenmarkts bei Zertifizierungsschemata, in der Union zu verhindern.

Der Rahmen nach Unterabsatz 1 Buchstabe b 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 für 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“ bezeichnet alle Tätigkeiten, die notwendig sind, um Netz- und Informationssysteme, die Nutzer solcher Systeme und andere von Cyberbedrohungen betroffene Personen zu schützen;

2. „Netz- und Informationssystem“ bezeichnet ein Netz- und Informationssystem im Sinne des Artikels 4 Nummer 1 der Richtlinie (EU) 2016/1148;

3. „nationale Strategie für die Sicherheit von Netz- und Informationssystemen“ bezeichnet eine nationale Strategie für die Sicherheit von Netz- und Informationssystemen im Sinne des Artikels 4 Nummer 3 der Richtlinie (EU) 2016/1148;

4. „Betreiber wesentlicher Dienste“ bezeichnet einen Betreiber wesentlicher Dienste im Sinne des Artikels 4 Nummer 4 der Richtlinie (EU) 2016/1148;

5. „Anbieter digitaler Dienste“ bezeichnet einen Anbieter digitaler Dienste im Sinne des Artikels 4 Nummer 6 der Richtlinie (EU) 2016/1148;

6. „Sicherheitsvorfall“ bezeichnet einen Sicherheitsvorfall im Sinne des Artikels 4 Nummer 7 der Richtlinie (EU) 2016/1148;

7. „Bewältigung von Sicherheitsvorfällen“ bezeichnet die Bewältigung von Sicherheitsvorfällen im Sinne des Artikels 4 Nummer 8 der Richtlinie (EU) 2016/1148;

8. „Cyberbedrohung“ bezeichnet einen möglichen Umstand, ein mögliches Ereignis oder eine mögliche Handlung, der/das/die Netz- und Informationssysteme, die Nutzer dieser Systeme und andere Personen schädigen, stören oder anderweitig beeinträchtigen könnte;

9. „europäisches Schema für die Cybersicherheitszertifizierung“ bezeichnet ein umfassendes Paket von Vorschriften, technischen Anforderungen, Normen und Verfahren, die auf Unionsebene festgelegt werden und für die Zertifizierung oder Konformitätsbewertung von bestimmten IKT-Produkten, -Diensten und -Prozessen gelten;

10. „nationales Schema für die Cybersicherheitszertifizierung“ bezeichnet ein umfassendes, von einer nationalen Behörde ausgearbeitetes und erlassenes Paket von Vorschriften, technischen Anforderungen, Normen und Verfahren, die für die Zertifizierung oder Konformitätsbewertung von IKT-Produkten, -Diensten und -Prozessen gelten, die von diesem Schema erfasst werden;

11. „europäisches Cybersicherheitszertifikat“ bezeichnet ein von der maßgeblichen Stelle ausgestelltes Dokument, in dem bescheinigt wird, dass ein bestimmtes IKT-Produkt, ein bestimmter IKT-Dienst oder ein bestimmter IKT-Prozess im Hinblick auf die Erfüllung besonderer Sicherheitsanforderungen, die in einem europäischen Schema für die Cybersicherheitszertifizierung festgelegt sind, bewertet wurde;

12. „IKT-Produkt“ bezeichnet ein Element oder eine Gruppe von Elementen eines Netz- oder Informationssystems;

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

14. „IKT-Prozess“ bezeichnet jegliche Tätigkeiten, mit denen ein ITK-Produkt oder -Dienst konzipiert, entwickelt, bereitgestellt oder gepflegt werden soll;

15. „Akkreditierung“ bezeichnet die Akkreditierung im Sinne des Artikels 2 Nummer 10 der Verordnung (EG) Nr. 765/2008;

16. „nationale Akkreditierungsstelle“ bezeichnet eine nationale Akkreditierungsstelle im Sinne des Artikels 2 Nummer 11 der Verordnung (EG) Nr. 765/2008;

17. „Konformitätsbewertung“ bezeichnet eine Konformitätsbewertung im Sinne des Artikels 2 Nummer 12 der Verordnung (EG) Nr. 765/2008;

18. „Konformitätsbewertungsstelle“ bezeichnet eine Konformitätsbewertungsstelle im Sinne des Artikels 2 Nummer 13 der Verordnung (EG) Nr. 765/2008;

19. „Norm“ bezeichnet eine Norm im Sinne des Artikels 2 Nummer 1 der Verordnung (EU) Nr. 1025/2012;

20. „technische Spezifikation“ bezeichnet ein Dokument, in dem die technischen Anforderungen, denen ein IKT-Prozess, -Produkt oder -Dienst genügen muss oder ein diesbezügliches Konformitätsbewertungsverfahren vorgeschrieben sind;

21. „Vertrauenswürdigkeitsstufe“ bezeichnet die Grundlage für das Vertrauen darin, dass ein IKT-Produkt, -Dienst oder -Prozess den Sicherheitsanforderungen eines spezifischen europäischen Schemas für die Cybersicherheitszertifizierung genügt, gibt an, auf welchem Niveau das IKT-Produkt, der IKT-Dienst oder der IKT-Prozess, bei der Bewertung eingestuft wurde, misst jedoch als solche nicht die Sicherheit des IKT-Produkts, -Dienstes oder -Prozesses;

22. „Selbstbewertung der Konformität“ bezeichnet eine Maßnahme eines Herstellers oder Anbieters von IKT-Produkten, -Diensten oder -Prozessen zur Bewertung, ob diese IKT- Produkte, -Dienste oder -Prozesse die Anforderungen, die in einem spezifischen europäischen Schema für die Cybersicherheitszertifizierung festgelegt sind, erfüllen.

TITEL II

ENISA (AGENTUR DER EUROPÄISCHEN UNION FÜR CYBERSICHERHEIT)

KAPITEL I

Mandat und Ziele

Artikel 3

Mandat

(1) Die ENISA nimmt die ihr mit dieser Verordnung zugewiesenen Aufgaben mit dem Ziel wahr, ein hohes gemeinsames Maß an Cybersicherheit in der gesamten Union zu erreichen, unter anderem indem sie die Mitgliedstaaten und die Organe, Einrichtungen und sonstigen Stellen der Union bei der Verbesserung der Cybersicherheit unterstützt. Die ENISA dient den Organen, Einrichtungen und sonstigen Stellen der Union sowie anderen maßgeblichen Interessenträgern der Union als Bezugspunkt für Beratung und Sachkenntnis im Bereich Cybersicherheit.

Die ENISA trägt durch die Wahrnehmung der ihr mit dieser Verordnung zugewiesenen Aufgaben zur Verringerung der Fragmentierung im Binnenmarkt bei.

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

(3) Die ENISA handelt bei der Wahrnehmung ihrer Aufgaben unabhängig, vermeidet Überschneidungen mit den Tätigkeiten der Mitgliedstaaten und berücksichtigt die bereits vorhandene Sachkenntnis der Mitgliedstaaten.

(4) Die ENISA entwickelt ihre eigenen Ressourcen, einschließlich technischer und menschlicher Fähigkeiten und Fertigkeiten, die erforderlich sind, um die ihr mit dieser Verordnung zugewiesenen Aufgaben wahrzunehmen.

Artikel 4

Ziele

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

(2) Die ENISA 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 sektorbezogene Strategien zur Cybersicherheit gehören.

(3) Die ENISA 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 ENISA fördert auf Unionsebene die Zusammenarbeit einschließlich des Informationsaustauschs und die Koordinierung zwischen den Mitgliedstaaten, den Organen, Einrichtungen und sonstigen Stellen der Union sowie den einschlägigen privaten und öffentlichen Interessenträgern in Fragen, die im Zusammenhang mit der Cybersicherheit stehen.

(5) Die ENISA trägt zum Ausbau der Cybersicherheitskapazitäten auf Unionsebene bei, um — insbesondere bei grenzüberschreitenden Sicherheitsvorfällen — die Maßnahmen zu unterstützen, die die Mitgliedstaaten zur Vermeidung von Cyberbedrohungen oder als Reaktion darauf ergreifen.

(6) Die ENISA fördert die Nutzung der europäischen Cybersicherheits-Zertifizierung, um der Fragmentierung des Binnenmarkts vorzubeugen. Die ENISA trägt zum Aufbau und zur Pflege eines Cybersicherheitszertifizierungsrahmens im Sinne des Titels III dieser Verordnung bei, um die auf mehr Transparenz gestützte Vertrauenswürdigkeit der Cybersicherheit von IKT-Produkten, -Diensten und -Prozessen zu erhöhen und damit das Vertrauen in den digitalen Binnenmarkt sowie dessen Wettbewerbsfähigkeit zu stärken.

(7) Die ENISA fördert ein hohes Maß der Sensibilisierung für die Cybersicherheit, einschließlich der Cyberhygiene und der Cyberkompetenz von Bürgern, Organisationen und Unternehmen.

KAPITEL II

Aufgaben

Artikel 5

Entwicklung und Umsetzung der Unionspolitik und des Unionsrechts

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

1. insbesondere durch unabhängige Stellungnahmen und Analysen sowie 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 die Abgabe von Stellungnahmen, Herausgabe von Leitlinien, Anbieten von Beratung und bewährten 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. die Mitgliedstaaten und die Organe, Einrichtungen und sonstigen Stellen der Union bei der Entwicklung und Förderung von Strategien im Zusammenhang mit der Cybersicherheit unterstützt, die die allgemeine Verfügbarkeit oder Integrität des öffentlichen Kerns des offenen Internets bewahren;

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

5. Folgendes unterstützt:

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

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

   c) die Mitgliedstaaten bei der Umsetzung bestimmter auf die Cybersicherheit bezogener Aspekte der Politik und des Rechts der Union im Bereich des Datenschutzes und des Schutzes der Privatsphäre, was — auf dessen Ersuchen die Beratung des Europäischen Datenschutzausschusses einschließt;

6. die regelmäßige Überprüfung der Unionspolitik unterstützt und dazu einen Jahresbericht über den Stand der Umsetzung des jeweiligen Rechtsrahmens in Bezug auf Folgendes erstellt:

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

   b) Zusammenfassungen von Meldungen von Sicherheitsverletzungen oder Integritätsverlusten von Vertrauensdiensteanbietern, die der ENISA auf der Grundlage des Artikels 19 Absatz 3 der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates ([23]) von den Aufsichtsstellen übermittelt werden;

   c) die Meldungen von Sicherheitsvorfällen durch Anbieter öffentlicher elektronischer Kommunikationsnetze oder öffentlich zugängliche elektronische Kommunikationsdienste, die der ENISA von den zuständigen Behörden auf der Grundlage des Artikels 40 der Richtlinie (EU) 2018/1972 übermittelt werden.

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

Artikel 6

Kapazitätsaufbau

(1) Die ENISA unterstützt

a) die Mitgliedstaaten bei ihren Bemühungen zur Verhütung, Erkennung und Analyse und zur Stärkung ihrer Fähigkeiten bei der Bewältigung von Cyberbedrohungen und Cybersicherheitsvorfällen, indem sie ihnen Wissen und Sachkenntnisse zur Verfügung stellt;

b) die Mitgliedstaaten und die Organe, Einrichtungen und sonstigen Stellen der Union bei der Aufstellung und Umsetzung von Strategien für eine Offenlegung von Sicherheitslücken auf freiwilliger Basis;

c) die Organe, Einrichtungen und sonstigen Stellen der Union bei ihren Bemühungen zur Verhütung, Erkennung und Analyse von Cyberbedrohungen und Cybersicherheitsvorfällen und zur Verbesserung ihrer Fähigkeiten bei der Bewältigung derartiger Cyberbedrohungen und Cybersicherheitsvorfällen, indem sie insbesondere das CERT-EU angemessen unterstützt;

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

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

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

g) 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 Bestand an Minimalfähigkeiten hat und entsprechend der bewährten Praxis arbeitet;

h) die Mitgliedstaaten durch die regelmäßige Veranstaltung der mindestens alle zwei Jahre stattfindenden Cybersicherheitsübungen auf Unionsebene nach Artikel 7 Absatz 5 und durch die Abgabe von Empfehlungen, die sie aus der Auswertung der Übungen und der bei diesen gemachten Erfahrungen ableitet;

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

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

(2) Die ENISA unterstützt den Informationsaustausch in und zwischen den 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 ENISA unterstützt die operative Zusammenarbeit zwischen den Mitgliedstaaten und Organen, Einrichtungen und sonstigen Stellen der Union untereinander und zwischen den Interessenträgern.

(2) Die ENISA 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 die Veröffentlichung von Leitlinien zu einschlägigen Fragen im Zusammenhang mit der Cybersicherheit;

c) die Festlegung praktischer Modalitäten für die Wahrnehmung besonderer Aufgaben nach Konsultation der Kommission.

(3) Die ENISA führt die Sekretariatsgeschäfte des CSIRTs-Netzes nach Artikel 12 Absatz 2 der Richtlinie (EU) 2016/1148 und unterstützt in dieser Eigenschaft aktiv den Informationsaustausch und die Zusammenarbeit zwischen den Mitgliedern des CSIRTs-Netzes.

(4) Die ENISA unterstützt die Mitgliedstaaten bei der operativen Zusammenarbeit innerhalb des CSIRTs-Netzes, indem sie

a) diese berät, wie sie ihre Fähigkeiten zur Verhütung, Erkennung und Bewältigung von Sicherheitsvorfällen verbessern können, und auf Ersuchen eines oder mehrerer Mitgliedstaaten Beratung in Bezug auf eine spezifische Cyberbedrohung leistet;

b) auf Ersuchen eines oder mehrerer Mitgliedstaaten bei der Bewertung von Sicherheitsvorfällen mit beträchtlichen oder erheblichen Auswirkungen Hilfe leistet, indem sie Sachkenntnisse bereitstellt und die technische Bewältigung solcher Vorfälle erleichtert, insbesondere auch durch die Unterstützung der freiwilligen Weitergabe maßgeblicher Informationen und technischer Lösungen zwischen den Mitgliedstaaten;

c) Sicherheitslücken und Sicherheitsvorfälle auf der Grundlage von öffentlich verfügbaren Informationen oder freiwillig von den Mitgliedstaaten zu diesem Zweck bereitgestellten Informationen analysiert und

d) auf Ersuchen eines oder mehrerer Mitgliedstaaten die nachträglichen technischen Untersuchungen von Sicherheitsvorfällen mit beträchtlichen oder erheblichen Auswirkungen im Sinne der Richtlinie (EU) 2016/1148 unterstützt.

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

(5) Die ENISA veranstaltet auf Unionsebene regelmäßig Cybersicherheitsübungen und unterstützt die Mitgliedstaaten und die Organe, Einrichtungen und sonstigen Stellen der Union auf deren Ersuchen hin bei der Organisation solcher Cybersicherheitsübungen. Diese Cybersicherheitsübungen auf Unionsebene können technische, operative oder strategische Elemente umfassen. Alle zwei Jahre veranstaltet die ENISA eine umfassende Großübung.

Die ENISA unterstützt gemeinsam mit den betreffenden Organisationen gegebenenfalls auch die Organisation sektorspezifischer Cybersicherheitsübungen, zu denen sie beiträgt, wobei diese Organisationen an den Cybersicherheitsübungen auf Unionsebene teilnehmen können.

(6) Die ENISA erstellt in enger Zusammenarbeit mit den Mitgliedstaaten regelmäßig einen eingehenden technischen EU-Cybersicherheitslagebericht über Sicherheitsvorfälle und Bedrohungen auf der Grundlage von öffentlich zugänglichen Informationen, eigenen Analysen und Berichten, die ihr unter anderem von den CSIRTs der Mitgliedstaaten () oder den zentralen Anlaufstellen im Sinne der Richtlinie (EU) 2016/1148 (in beiden Fällen auf freiwilliger Basis) sowie dem EC3 und dem CERT-EU übermittelt werden.

(7) Die ENISA 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) öffentlich verfügbare oder auf freiwilliger Grundlage bereitgestellte Berichte aus nationalen Quellen als Beitrag zu einer gemeinsamen Lageerfassung zusammenstellt und analysiert;

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 die technische Bewältigung dieser Sicherheitsvorfälle oder Krisen erleichtert, insbesondere auch durch die Unterstützung der freiwilligen Weitergabe technischer Lösungen zwischen den Mitgliedstaaten;

d) die Organe, Einrichtungen und sonstigen Stellen der Union und auf deren Ersuchen die Mitgliedstaaten bei der öffentlichen Kommunikation im Umfeld solcher Sicherheitsvorfälle oder der Krisen unterstützt;

e) die Kooperationspläne für die Reaktion auf solche Sicherheitsvorfälle oder Krisen auf Ebene der Union testet und auf deren Ersuchen die Mitgliedstaaten bei der Erprobung solcher Pläne auf nationaler Ebene unterstützt.

Artikel 8

Markt, Cybersicherheitszertifizierung und Normung

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

a) die Entwicklungen in damit zusammenhängenden Normungsbereichen fortlaufend überwacht und in Fällen, in denen keine Normen zur Verfügung stehen, geeignete technische Spezifikationen für die Entwicklung europäischer Schemata für die Cybersicherheitszertifizierung nach Artikel 54 Absatz 1 Buchstabe c empfiehlt;

b) mögliche europäische Schemata für die Cybersicherheitszertifizierung (im Folgenden „mögliche Schemata“) von IKT-Produkten, -Diensten und -Prozessen nach Artikel 49 ausarbeitet;

c) angenommene europäische Schemata für die Cybersicherheitszertifizierung nach Artikel 49 Absatz 8 evaluiert;

d) sich an gegenseitigen Begutachtungen nach Artikel 59 Absatz 4 beteiligt;

e) die Kommission bei der Wahrnehmung der Sekretariatsgeschäfte der nach Artikel 62 Absatz 5 eingesetzten Europäischen Gruppe für die Cybersicherheitszertifizierung unterstützt.

(2) Die ENISA nimmt die Sekretariatsgeschäfte der nach Artikel 22 Absatz 4 eingesetzten Gruppe der Interessenträger für die Cybersicherheitszertifizierung wahr.

(3) Die ENISA stellt in Zusammenarbeit mit den nationalen Behörden für die Cybersicherheitszertifizierung und der Branche auf formelle, strukturierte und transparente Art und Weise Leitlinien zusammen und veröffentlicht diese und entwickelt bewährte Verfahren im Zusammenhang mit den Anforderungen an die Cybersicherheit von IKT-Produkten, -Diensten und -Prozessen.

(4) Die ENISA trägt zu einem hinreichenden Kapazitätsaufbau im Zusammenhang mit den Bewertungs- und Zertifizierungsverfahren bei, indem sie Leitlinien erstellt und veröffentlicht und die Mitgliedstaaten auf deren Ersuchen hin unterstützt.

(5) Die ENISA erleichtert die Ausarbeitung und Übernahme europäischer und internationaler Normen für das Risikomanagement und die Sicherheit von IKT-Produkten, -Diensten und -Prozessen.

(6) Die ENISA bietet nach Artikel 19 Absatz 2 der Richtlinie (EU) 2016/1148 in Zusammenarbeit mit den Mitgliedstaaten und der Branche Beratung an und erstellt 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.

(7) Die ENISA 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 ENISA

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 Cyberbedrohungen und Sicherheitsvorfälle durch, um neu auftretende Trends erkennen und dazu beitragen zu können, Sicherheitsvorfälle zu vermeiden;

c) stellt in Zusammenarbeit mit den Sachverständigen der Behörden der Mitgliedstaaten und den maßgeblichen Interessenträgern 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 Anbietern der in Anhang III der genannten Richtlinie aufgeführten digitaler Dienste genutzt werden;

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

e) erhebt und analysiert öffentlich verfügbare Informationen über signifikante Sicherheitsvorfälle und stellt Berichte mit dem Ziel zusammen, den Bürgern, Organisationen und Unternehmen unionsweite Leitlinien bereitzustellen.

Artikel 10

Sensibilisierung und Ausbildung

Die ENISA

a) sensibilisiert die Öffentlichkeit für Cybersicherheitsrisiken und stellt Leitlinien für bewährte Verfahren für einzelne Nutzer zur Verfügung, die sich an Bürger, Organisationen und Unternehmen richten und auch Cyberhygiene und Cyberkompetenz umfassen;

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 und eine umfassende öffentliche Debatte anzuregen;

c) unterstützt die Mitgliedstaaten bei ihren Anstrengungen zur Sensibilisierung in Bezug auf Cybersicherheit und zur Förderung der Ausbildung im Bereich Cybersicherheit;

d) unterstützt die engere Koordinierung und den Austausch bewährter Verfahren zwischen den Mitgliedstaaten in Bezug auf Sensibilisierung und Ausbildung im Bereich Cybersicherheit.

Artikel 11

Forschung und Innovation

Die ENISA, in Zusammenhang mit der Forschung und Innovation,

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

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

c) trägt im Bereich der Cybersicherheit zur strategischen Forschungs- und Innovationsagenda auf Unionsebene bei.

Artikel 12

Internationale Zusammenarbeit

Die ENISA unterstützt die Bemühungen der Union um Zusammenarbeit mit Drittländern und internationalen Organisationen sowie innerhalb der einschlägigen Rahmen für internationale Zusammenarbeit, 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) auf Ersuchen der Kommission den Austausch bewährter Verfahren erleichtert;

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

d) die Kommission in Zusammenarbeit mit der nach Artikel 62 eingesetzten Europäischen Gruppe für die Cybersicherheitszertifizierung bei Fragen zu Abkommen über die gegenseitige Anerkennung von Cybersicherheitszertifikaten mit Drittländern berät und unterstützt.

KAPITEL III

Organisation der ENISA

Artikel 13

Struktur der ENISA

Die Verwaltungs- und Leitungsstruktur der ENISA besteht aus

a) einem Verwaltungsrat;

b) einem Exekutivrat;

c) einem Exekutivdirektor;

d) einer EINSA-Beratungsgruppe; und

e) einem Netz der nationalen Verbindungsbeamten.

Abschnitt 1

Verwaltungsrat

Artikel 14

Zusammensetzung des Verwaltungsrats

(1) Dem Verwaltungsrat gehören je ein von jedem Mitgliedstaat ernanntes Mitglied und zwei von der Kommission ernannte Mitglieder an. Alle Mitglieder haben Stimmrecht.

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

(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 ein ausgewogenes Geschlechterverhältnis im Verwaltungsrat ein.

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

Artikel 15

Aufgaben des Verwaltungsrats

(1) Der Verwaltungsrat

a) legt die allgemeine Ausrichtung der Tätigkeit der ENISA fest und sorgt auch dafür, dass die ENISA ihre Geschäfte gemäß der in dieser Verordnung festgelegten Vorschriften und Grundsätze führt. Er sorgt zudem für die Abstimmung der Arbeit der ENISA mit den Tätigkeiten, die von den Mitgliedstaaten und auf Unionsebene durchgeführt werden;

b) nimmt den Entwurf des in Artikel 24 genannten einheitlichen Programmplanungsdokuments der ENISA an, bevor dieser der Kommission zur Stellungnahme vorgelegt wird;

c) nimmt — unter Berücksichtigung der Stellungnahme der Kommission — das einheitliche Programmplanungsdokument der ENISA an;

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

e) stellt den jährlichen Haushaltsplan der Agentur fest und übt andere Funktionen in Bezug auf den Haushalt der ENISA gemäß Kapitel IV aus;

f) bewertet und genehmigt den konsolidierten Jahresbericht über die Tätigkeiten der ENISA einschließlich des Jahresabschlusses und der Ausführungen darüber, inwiefern die ENISA die vorgegebenen Leistungsindikatoren erfüllt hat, 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, und macht ihn der Öffentlichkeit zugänglich;

g) erlässt nach Artikel 32 die für die ENISA geltende Finanzregelung;

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

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

j) 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;

k) gibt sich eine Geschäftsordnung einschließlich Regelungen zu den vorläufigen Beschlüssen zur Übertragung bestimmter Aufgaben gemäß Artikel 19 Absatz 7;

l) nimmt gemäß Absatz 2 des vorliegenden Artikels in Bezug auf das Personal der ENISA die Befugnisse wahr, die der Anstellungsbehörde durch das Statut der Beamten der Europäischen Union (im Folgenden „Statut der Beamten") bzw. der Stelle, die zum Abschluss der Dienstverträge ermächtigt ist, durch die Beschäftigungsbedingungen für die sonstigen Bediensteten der Europäischen Union (im Folgenden „Beschäftigungsbedingungen für die sonstigen Bediensteten der Europäischen Union") nach der Verordnung (EWG, Euratom, EGKS) Nr. 259/68 des Rates ([24]) übertragen wurden (im Folgenden „Befugnisse der Anstellungsbehörde");

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

n) ernennt den Exekutivdirektor und verlängert gegebenenfalls dessen Amtszeit oder enthebt ihn nach Artikel 36 seines Amtes;

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

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

q) genehmigt das Treffen von Arbeitsvereinbarungen bezüglich Artikel 7;

r) genehmigt das Treffen oder den Abschluss von Arbeitsvereinbarungen nach Artikel 42.

(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 der Anstellungsbehörde dem Exekutivdirektor überträgt und die Bedingungen festlegt, unter denen die Befugnisübertragung ausgesetzt werden kann. Der Exekutivdirektor kann diese Befugnisse einer nachgeordneten Ebene übertragen.

([24]) Verordnung (EWG, Euratom, EGKS) Nr. 259/68 des Rates vom 29. Februar 1968 zur Festlegung des Statuts der Beamten der Europäischen Gemeinschaften und der Beschäftigungsbedingungen für die sonstigen Bediensteten dieser Gemeinschaften sowie zur Einführung von Sondermaßnahmen, die vorübergehend auf die Beamten der Kommission anwendbar sind (ABl. L 56 vom 4.3.1968, S. 1).

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

Artikel 16

Vorsitz des Verwaltungsrats

Der Verwaltungsrat wählt aus dem Kreis seiner Mitglieder mit der Zweidrittelmehrheit seiner Mitglieder einen Vorsitzenden und einen stellvertretenden Vorsitzenden. Ihre Amtszeit beträgt vier Jahre, 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 17

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 teil, hat jedoch kein Stimmrecht.

(4) Die Mitglieder der ENISA-Beratungsgruppe können auf Einladung des Vorsitzes an den Sitzungen des Verwaltungsrats teilnehmen, haben jedoch kein Stimmrecht.

(5) Die Mitglieder des Verwaltungsrats und ihre Stellvertreter können sich nach Maßgabe der Geschäftsordnung des Verwaltungsrats von Beratern oder Sachverständigen bei den Sitzungen des Verwaltungsrats unterstützen lassen.

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

Artikel 18

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 der Mitglieder des Verwaltungsrats erforderlich.

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

(4) Der Vorsitzende des Verwaltungsrats nimmt an den Abstimmungen teil.

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

(6) Die näheren Einzelheiten der Abstimmungsregeln, 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 19

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 20 den Exekutivdirektor bei der Umsetzung der verwaltungs- und haushaltsbezogenen Beschlüsse des Verwaltungsrats nach Artikel 20.

(3) Der Exekutivrat besteht aus fünf Mitgliedern. Die Mitglieder des Exekutivrats werden aus den Reihen der Mitglieder des Verwaltungsrats ernannt. Eines der Mitglieder ist der Vorsitzende des Verwaltungsrats, der zugleich auch Vorsitzender des Exekutivrats sein kann, und ein weiteres ist einer der Vertreter der Kommission. Bei den Ernennungen der Mitglieder des Exekutivrats wird die Sicherstellung eines ausgewogenen Geschlechterverhältnisses im Exekutivrat angestrebt. Der Exekutivdirektor nimmt an den Sitzungen des Exekutivrats, hat jedoch kein Stimmrecht.

(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) Ist dies aufgrund der Dringlichkeit notwendig, so kann der Exekutivrat im Namen des Verwaltungsrats bestimmte vorläufige Beschlüsse fassen, vor allem in Verwaltungsangelegenheiten, einschließlich der Aussetzung der Übertragung der Befugnisse der Anstellungsbehörde, und in Haushaltsangelegenheiten. über Diese vorläufigen Beschlüsse werden dem Verwaltungsrat unverzüglich mitgeteilt. Der Verwaltungsrat entscheidet sodann spätestens drei Monate, nachdem der Beschluss gefasst wurde, ob er den vorläufigen Beschluss genehmigt oder ob er ihn nicht genehmigt. Der Exekutivrat fasst keine Beschlüsse im Namen des Verwaltungsrats, die mit einer Mehrheit von zwei Dritteln der Mitglieder des Verwaltungsrats angenommen werden müssen.

Abschnitt 3

Exekutivdirektor

Artikel 20

Pflichten des Exekutivdirektors

(1) Die ENISA 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 ENISA 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 ENISA, einschließlich der Umsetzung des jährlichen Arbeitsprogramms der ENISA, 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 OLAF auszuarbeiten und der Kommission zweimal jährlich und dem Verwaltungsrat regelmäßig über die erzielten Fortschritte Bericht zu erstatten;

h) den Entwurf der für die ENISA geltenden Finanzregelung nach Artikel 32 auszuarbeiten;

i) den Entwurf des Voranschlags der Einnahmen und Ausgaben der ENISA 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 ENISA 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;

m) einen regelmäßigen Gedanken- und Informationsaustausch 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 Unionspolitik sicherzustellen;

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

(4) Soweit erforderlich sowie entsprechend den Zielen und Aufgaben der ENISA kann der Exekutivdirektor der ENISA Ad-hoc-Arbeitsgruppen aus Sachverständigen — auch von den zuständigen Behörden der Mitgliedstaaten — einsetzen. Der Exekutivdirektor unterrichtet den Verwaltungsrat hiervon vorab. 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 ENISA 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 ENISA 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 ENISA 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. Die Gesamtzahl der Mitarbeiter in allen Außenstellen ist möglichst gering zu halten und darf insgesamt nicht 40 % der Gesamtzahl der Mitarbeiter der ENISA ii dem Mitgliedstaat, in dem die ENISA ihren Sitz hat, überschreiten. Die Anzahl der Mitarbeiter in jeder Außenstelle darf nicht 10 % der Gesamtzahl der Mitarbeiter der Agentur im Mitgliedstaat, in dem die ENISA ihren Sitz hat, überschreiten.

In dem Beschluss zur Einrichtung einer Außenstelle wird der Umfang der in der Außenstelle auszuübenden Tätigkeiten so festgelegt, dass unnötige Kosten und eine Überschneidung der Verwaltungsfunktionen mit denen der ENISA vermieden werden.

Abschnitt 4

ENISA-Beratungsgruppe, Gruppe der Interessenträger für die Cybersicherheitszertifizierung und Netz der nationalen Verbindungsbeamten

Artikel 21

ENISA-Beratungsgruppe

(1) Der Verwaltungsrat setzt auf Vorschlag des Exekutivdirektors auf transparente Art und Weise eine ENISA-Beratungsgruppe ein, die sich aus anerkannten Sachverständigen als Vertreter der einschlägigen Interessenträger zusammensetzt, darunter die IKT-Branche, Anbieter öffentlich zugänglicher elektronischer Kommunikationsnetze oder -dienste, KMU, Betreiber wesentlicher Dienste, Verbrauchergruppen, wissenschaftliche Sachverständige aus dem Bereich der Cybersicherheit sowie Vertreter der zuständigen Behörden, die nach der Richtlinie (EU) 2018/1972 notifiziert wurden, europäische Normungsorganisationen sowie Strafverfolgungsbehörden und Datenschutz-Aufsichtsbehörden. Der Verwaltungsrat strebt ein angemessenes Gleichgewicht zwischen den Geschlechtern, ein angemessenes geographisches Gleichgewicht und ein angemessenes Gleichgewicht zwischen den verschiedenen Interessengruppen an.

(2) Die Verfahren für die ENISA-Beratungsgruppe, die insbesondere ihre Zusammensetzung, den Vorschlag des in Absatz 1 genannten Exekutivdirektors, die Anzahl und die Ernennung der Mitglieder und die Arbeitsweise der ENISA-Beratungsgruppe betreffen, werden in den internen Verfahrensvorschriften der ENISA festgelegt und öffentlich bekannt gemacht.

(3) Den Vorsitz der ENISA-Beratungsgruppe führt der Exekutivdirektor oder eine jeweils vom Exekutivdirektor ernannte Person.

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

(5) Die ENISA-Beratungsgruppe berät die ENISA bei der Durchführung ihrer Aufgaben, ausgenommen der Anwendung der Bestimmungen des Titels III dieser Verordnung. Sie berät insbesondere den Exekutivdirektor bei der Ausarbeitung eines Vorschlags für das Jahresarbeitsprogramms der ENISA und bei der Sicherstellung der Kommunikation mit den einschlägigen Interessenträgern bezüglich Fragen im Zusammenhang mit dem Jahresarbeitsprogramm.

(6) Die ENISA-Beratungsgruppe unterrichtet den Verwaltungsrat regelmäßig über ihre Tätigkeiten.

Artikel 22

Gruppe der Interessenträger für die Cybersicherheitszertifizierung

(1) Es wird eine Gruppe der Interessenträger für die Cybersicherheitszertifizierung eingesetzt.

(2) Die Mitglieder der Gruppe der Interessenträger für die Cybersicherheitszertifizierung werden unter anerkannten Sachverständigen als Vertreter der einschlägigen Interessenträger ausgewählt. Die Kommission wählt die Mitglieder der Gruppe der Interessenträger für die Cybersicherheitszertifizierung auf Vorschlag der ENISA im Wege eines transparenten und offenen Auswahlverfahrens aus, durch das ein Gleichgewicht zwischen den verschiedenen Interessengruppen sowie ein angemessenes Gleichgewicht zwischen den Geschlechtern und ein angemessenes geographisches Gleichgewicht sichergestellt wird.

(3) Die Gruppe der Interessenträger für die Cybersicherheitszertifizierung:

a) berät die Kommission in strategischen Fragen im Zusammenhang mit dem europäischen Rahmen für die Cybersicherheitszertifizierung;

b) berät auf Ersuchen die ENISA in allgemeinen und strategischen Fragen im Zusammenhang mit den Aufgaben der ENISA in Bezug auf den Markt, die Cybersicherheitszertifizierung und die Normung;

c) unterstützt die Kommission bei der Ausarbeitung des in Artikel 47 genannten fortlaufenden Arbeitsprogramms der Union;

d) nimmt zum fortlaufenden Arbeitsprogramm der Union gemäß Artikel 47 Absatz 4 Stellung und

e) berät in dringenden Fällen die Kommission und die Europäische Gruppe für die Cybersicherheitszertifizierung in Bezug auf die Notwendigkeit zusätzlicher Zertifizierungsschemata, die nicht Teil des fortlaufenden Arbeitsprogramms der Union sind, wie in Artikel 47 und 48 beschrieben.

(4) Den Vorsitz der Gruppe der Interessenträger für die Cybersicherheitszertifizierung führen die Vertreter der Kommission und der ENISA gemeinsam, und die Sekretariatsgeschäfte werden von der ENISA wahrgenommen.

Artikel 23

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 (im Folgenden „nationale Verbindungsbeamten"). Jeder Mitgliedstaat ernennt einen Vertreter im Netz der nationalen Verbindungsbeamten. Die Sitzungen des Netzes der nationalen Verbindungsbeamten können in verschiedenen Sachverständigenzusammensetzungen abgehalten werden.

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

(3) Die nationalen Verbindungsbeamten dienen als Kontaktstelle auf nationaler Ebene, um die Zusammenarbeit zwischen der ENISA und den nationalen Sachverständigen im Rahmen der Durchführung des Jahresarbeitsprogramms der ENISA zu erleichtern.

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

(5) Die Funktionen und Verfahren des Netzes der nationalen Verbindungsbeamten werden in den internen Verfahrensvorschriften der ENISA festgelegt und der Öffentlichkeit zugänglich gemacht.

Abschnitt 5

Arbeitsweise

Artikel 24

Einheitliches Programmplanungsdokument

(1) Die ENISA führt ihre Geschäfte 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 Finanz- und Personalplanung nach Artikel 32 der Delegierten Verordnung (EU) Nr. 1271/2013 der Kommission ([25]) 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 übermittelt es bis zum 31. Januar des Folgejahres dem Europäischen Parlament, dem Rat und der Kommission, sowie jede spätere Aktualisierung dieses Dokuments.

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

([25]) 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).

(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.

(6) Der Verwaltungsrat ändert das angenommene Jahresarbeitsprogramm, wenn der ENISA 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 67 genannten Bewertung Rechnung zu tragen.

Artikel 25

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 ENISA legt in ihren internen Verfahrensvorschriften die praktischen Einzelheiten der Vorschriften über Interessenerklärungen nach den Absätzen 1 und 2 fest.

Artikel 26

Transparenz

(1) Die ENISA übt ihre Tätigkeiten mit einem hohen Maß an Transparenz und im Einklang mit Artikel 28 aus.

(2) Die ENISA 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 25 abgegebenen Interessenerklärungen.

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

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

Artikel 27

Vertraulichkeit

(1) Unbeschadet des Artikels 28 gibt die Agentur Informationen, die bei ihr eingehen oder von ihr verarbeitet werden und die auf begründetes Ersuchen vertraulich behandelt werden sollen, nicht an Dritte weiter.

(2) Die Mitglieder des Verwaltungsrats, der Exekutivdirektor, die Mitglieder der ENISA-Beratungsgruppe, die externen Sachverständigen der Ad-hoc-Arbeitsgruppen sowie das Personal der ENISA, einschließlich der von den Mitgliedstaaten auf Zeit abgeordneten Beamten, unterliegen auch nach Beendigung ihrer Tätigkeit den Vertraulichkeitsbestimmungen des Artikels 339 AEUV.

(3) Die ENISA 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 ENISA erforderlich ist, beschließt der Verwaltungsrat, die ENISA zum Umgang mit Verschlusssachen zu ermächtigen. In diesem Fall nimmt die ENISA im Einvernehmen mit den Dienststellen der Kommission Sicherheitsvorschriften zur Anwendung der Sicherheitsgrundsätze an, die in den Beschlüssen (EU, Euratom) 2015/443 ([26]) und (EU, Euratom) 2015/444 ([27]) der Kommission festgelegt sind. Diese Sicherheitsvorschriften betreffen unter anderem die Bestimmungen über den Austausch, die Verarbeitung und die Speicherung von Verschlusssachen.

Artikel 28

Zugang zu Dokumenten

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

(2) Der Verwaltungsrat legt bis zum 28. Dezember 2019 Maßnahmen zur Durchführung der Verordnung (EG) Nr. 1049/2001 fest.

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

KAPITEL IV

Aufstellung und Gliederung des Haushaltsplans der ENISA

Artikel 29

Aufstellung des Haushaltsplans der ENISA

(1) Der Exekutivdirektor erstellt jedes Jahr den Entwurf des Voranschlags der Einnahmen und Ausgaben der ENISA für das folgende Haushaltsjahr und übermittelt 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 Entwurfs des Voranschlags einen Voranschlag der Einnahmen und Ausgaben der ENISA 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 42 Absatz 2 geschlossen hat, den 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 der Union in den Haushaltsplanentwurf der Union ein, den sie nach Artikel 314 AEUV dem Europäischen Parlament und dem Rat vorlegt.

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

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

([26]) 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).

([27]) 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).

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

Artikel 30

Gliederung des Haushaltsplans der ENISA

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

a) ein Beitrag aus dem Gesamthaushalt der Union;

b) Einnahmen, die konkreten Ausgabenpositionen im Einklang mit der in Artikel 32 genannten Finanzregelung zugewiesen werden;

c) Unionsmittel in Form von Übertragungsvereinbarungen oder Ad-hoc-Finanzhilfen im Einklang mit der in Artikel 32 genannten Finanzregelung der Agentur und den Bestimmungen der einschlägigen Instrumente zur Unterstützung der Unionspolitik;

d) Beiträge von Drittländern, die sich nach Artikel 42 an der Arbeit der ENISA beteiligen;

e) freiwillige Zahlungen oder Sachleistungen von Mitgliedstaaten.

Mitgliedstaaten, die einen freiwilligen Beitrag nach Unterabsatz 1 Buchstabe e leisten, können aufgrund dessen keine bestimmten Rechte oder Dienstleistungen beanspruchen.

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

Artikel 31

Ausführung des Haushaltsplans der ENISA

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

(2) Der interne Rechnungsprüfer der Kommission übt gegenüber der ENISA 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 für das Haushaltsjahr (Jahr n).

(4) Nach Eingang der Bemerkungen des Rechnungshofes zum vorläufigen Jahresabschluss der ENISA gemäß Artikel 246 der Verordnung (EU, Euratom) 2018/1046 des Europäischen Parlaments und des Rates ([28]), erstellt der Rechnungsführer in eigener Verantwortung den endgültigen Jahresabschluss der ENISA und legt ihn dem Verwaltungsrat zur Stellungnahme vor.

(5) Der Verwaltungsrat gibt eine Stellungnahme zu den endgültigen Jahresabschlüssen der ENISA ab.

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

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

([28]) Verordnung (EU, Euratom) 2018/1046 des Europäischen Parlaments und des Rates vom 18. Juli 2018 über die Haushaltsordnung für den Gesamthaushaltsplan der Union, zur Änderung der Verordnungen (EU) Nr. 1296/2013, (EU) Nr. 1301/2013, (EU) Nr. 1303/2013, (EU) Nr. 1304/2013, (EU) Nr. 1309/2013, (EU) Nr. 1316/2013, (EU) Nr. 223/2014, (EU) Nr. 283/2014 und des Beschlusses Nr. 541/2014/EU sowie zur Aufhebung der Verordnung (EU, Euratom) Nr. 966/2012 (ABl. L 193 vom 30.7.2018, S. 1).

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

(9) Bis zum 15. November des Jahres n+1 veröffentlicht der Exekutivdirektor den endgültigen Jahresabschluss im *Amtsblatt der Europäischen Union*.

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

(11) Der Exekutivdirektor unterbreitet dem Europäischen Parlament auf dessen Ersuchen nach Artikel 261 Absatz 3 der Verordnung (EU, Euratom) 2018/1046 alle für ein reibungsloses Entlastungsverfahren für das betreffende Haushaltsjahr notwendigen Informationen.

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

Artikel 32

Finanzregelung

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

Artikel 33

Betrugsbekämpfung

(1) Zur Erleichterung der Bekämpfung von Betrug, Korruption und sonstigen rechtswidrigen Handlungen gemäß der Verordnung (EU, Euratom) Nr. 883/2013 des Europäischen Parlaments und des Rates [29] tritt die ENISA bis zum 28. Dezember 2019 der Interinstitutionellen Vereinbarung vom 25. Mai 1999 zwischen dem Europäischen Parlament, dem Rat der Europäischen Union und der Kommission der Europäischen Gemeinschaften über die internen Untersuchungen des Europäischen Amtes für Betrugsbekämpfung (OLAF) [30] bei. Die ENISA erlässt die einschlägigen Vorschriften, die für sämtliche Mitarbeiter der ENISA 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 ENISA erhalten haben, Rechnungsprüfungen anhand von Belegkontrollen und Kontrollen vor Ort durchzuführen.

(3) Das OLAF kann gemäß den Bestimmungen und Verfahren der Verordnung (EU, Euratom) Nr. 883/2013 und der Verordnung (Euratom, EG) Nr. 2185/96 des Rates [31] Untersuchungen, einschließlich Kontrollen und Überprüfungen vor Ort, durchführen, um festzustellen, ob im Zusammenhang mit von der ENISA 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 oder internationalen Organisationen, Verträge, Finanzhilfevereinbarungen und Finanzhilfebeschlüsse der ENISA Bestimmungen enthalten, die den Rechnungshof und das OLAF ausdrücklich ermächtigen, derartige Rechnungsprüfungen und Untersuchungen im Rahmen ihrer jeweiligen Zuständigkeiten durchzuführen.

---

[29] 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).

[30] ABl. L 136 vom 31.5.1999, S. 15.

[31] 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).

KAPITEL V

Personal

Artikel 34

Allgemeine Bestimmungen

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

Artikel 35

Vorrechte und Befreiungen

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

Artikel 36

Exekutivdirektor

(1) Der Exekutivdirektor wird als Zeitbediensteter der ENISA 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 Arbeitsvertrags des Exekutivdirektors wird die ENISA 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 fünf Jahre. Zum Ende dieses Zeitraums nimmt die Kommission eine Bewertung der Leistung des Exekutivdirektors und der künftigen Aufgaben und Herausforderungen der ENISA vor.

(6) Der Verwaltungsrat beschließt über die Ernennung, die Verlängerung der Amtszeit oder die Abberufung des Exekutivdirektors gemäß Artikel 18 Absatz 2.

(7) Der Verwaltungsrat kann auf Vorschlag der Kommission unter Berücksichtigung der Bewertung nach Absatz 5 die Amtszeit des Exekutivdirektors einmal um fünf 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, nimmt nicht an einem anderen Auswahlverfahren für dieselbe Stelle teil.

(10) Der Exekutivdirektor kann nur durch einen Beschluss des Verwaltungsrats auf Vorschlag der Kommission seines Amtes enthoben werden.

Artikel 37

Abgeordnete nationale Sachverständige und sonstiges Personal

(1) Die ENISA kann auf abgeordnete nationale Sachverständige oder sonstiges Personal zurückgreifen, das nicht von der ENISA 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 ENISA abgeordnete nationale Sachverständige.

KAPITEL VI

Allgemeine Bestimmungen für die ENISA

Artikel 38

Rechtsform der ENISA

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

(2) Die ENISA besitzt in jedem Mitgliedstaat die weitestgehende Rechts- und Geschäftsfähigkeit, die juristischen Personen nach nationalem Recht zuerkannt ist. Sie kann insbesondere bewegliches und unbewegliches Vermögen erwerben oder veräußern und ist vor Gericht parteifähig.

(3) Die ENISA wird vom Exekutivdirektor vertreten.

Artikel 39

Haftung der ENISA

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

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

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

(4) In Streitsachen über den Schadensersatz gemäß Absatz 3 ist der Gerichtshof der Europäischen Union zuständig.

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

Artikel 40

Sprachenregelung

(1) Für die ENISA gilt die Verordnung Nr. 1 des Rates ([32]). Die Mitgliedstaaten und die anderen von den Mitgliedstaaten benannten Einrichtungen können sich in einer der Amtssprachen der Organe der Union ihrer Wahl an die ENISA wenden und erhalten eine Antwort in dieser Sprache.

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

Artikel 41

Schutz personenbezogener Daten

(1) Die Verarbeitung personenbezogener Daten durch die ENISA unterliegt der Verordnung (EU) 2018/1725.

(2) Der Verwaltungsrat beschließt die Durchführungsvorschriften gemäß Artikel 45 Absatz 3 der Verordnung (EU) 2018/1725. Der Verwaltungsrat kann zusätzliche Maßnahmen, die für die Anwendung der Verordnung (EU) 2018/1725 durch die ENISA erforderlich sind, festlegen.

([32]) Verordnung Nr. 1 zur Regelung der Sprachenfrage für die Europäische Wirtschaftsgemeinschaft (ABl. 17 vom 6.10.1958, S. 385/58).

Artikel 42

Zusammenarbeit mit Drittländern und internationalen Organisationen

(1) Die ENISA 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 ENISA, nach vorheriger Genehmigung durch die Kommission, Arbeitsvereinbarungen mit den Behörden von Drittländern und internationalen Organisationen treffen. Diese Arbeitsvereinbarungen begründen keine rechtlichen Verpflichtungen für die Union und ihre Mitgliedstaaten.

(2) Die ENISA steht der Beteiligung von Drittländern offen, die entsprechende Übereinkünfte mit der Europäischen Union geschlossen haben. Gemäß den einschlägigen Bestimmungen dieser Übereinkünfte werden Arbeitsvereinbarungen getroffen, die insbesondere Art, Umfang und Form einer Beteiligung dieser Drittländer an der Tätigkeit der ENISA festlegen; hierzu zählen auch Bestimmungen über die Beteiligung an den von der ENISA durchgeführten Initiativen, finanzielle Beiträge und Personal. In Personalfragen müssen derartige Arbeitsvereinbarungen in jedem Fall mit dem Statut der Beamten und den Beschäftigungsbedingungen für die sonstigen Bediensteten vereinbar sein.

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

Artikel 43

Sicherheitsvorschriften für den Schutz von vertraulichen Informationen, die nicht zu den Verschlusssachen zählen und von Verschlusssachen

Nach Konsultation der Kommission legt die ENISA die Sicherheitsvorschriften fest, mit denen die in den Sicherheitsvorschriften der Kommission für den Schutz von vertraulichen Informationen, die nicht zu den Verschlusssachen zählen und von Verschlusssachen der Europäischen Union enthaltenen Sicherheitsgrundsätze angewandt werden, die in den Beschlüssen (EU, Euratom) 2015/443 und 2015/444 festgelegt sind. Die Sicherheitsvorschriften der ENISA enthalten Bestimmungen über den Austausch, die Verarbeitung und die Speicherung derartiger Informationen.

Artikel 44

Sitzabkommen und Arbeitsbedingungen

(1) Die notwendigen Regelungen über die Unterbringung der ENISA 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 ENISA für den Exekutivdirektor, die Mitglieder des Verwaltungsrats, das Personal der ENISA und für Familienangehörige dieser Personen gelten, werden in einem Sitzabkommen festgelegt, das nach Billigung durch den Verwaltungsrat zwischen der ENISA und dem Sitzmitgliedstaat geschlossen wird.

(2) Der Sitzmitgliedstaat der ENISA gewährleistet die bestmöglichen Voraussetzungen für das reibungslose Funktionieren der ENISA, unter Berücksichtigung 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 der Mitglieder des Personals.

Artikel 45

Verwaltungskontrolle

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

TITEL III

ZERTIFIZIERUNGSRAHMEN FÜR DIE CYBERSICHERHEIT

Artikel 46

Europäischer 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 Union erhöht wird und indem im Hinblick auf die Schaffung eines digitalen Binnenmarkts für IKT-Produkte, -Dienste und -Prozesse ein harmonisierter Ansatz auf Unionsebene für europäische Schemata für die Cybersicherheitszertifizierung ermöglicht wird.

(2) Der europäische Zertifizierungsrahmen für die Cybersicherheit legt einen Mechanismus fest, mit dem europäische Schemata für die Cybersicherheitszertifizierung geschaffen werden und mit dem bescheinigt wird, dass die nach einem solchen Schema bewerteten IKT-Produkte, -Dienste und -Prozesse den festgelegten Sicherheitsanforderungen genügen, um die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit von gespeicherten, übermittelten oder verarbeiteten Daten, Funktionen oder Diensten, die von diesen Produkten, Diensten und Prozessen angeboten oder über diese zugänglich gemacht werden, während deren gesamten Lebenszyklus zu schützen.

Artikel 47

Das fortlaufende Arbeitsprogramm der Union für die europäische Cybersicherheitszertifizierung

(1) Die Kommission veröffentlicht ein fortlaufendes Arbeitsprogramm der Union für die europäische Cybersicherheitszertifizierung (im Folgenden „fortlaufendes Arbeitsprogramm der Union"), in dessen Rahmen die strategischen Prioritäten für künftige europäische Schemata für die Cybersicherheitszertifizierung festgelegt werden sollen.

(2) Das fortlaufende Arbeitsprogramm der Union umfasst insbesondere eine Liste der IKT-Produkte, -Dienste und -Prozesse oder Kategorien davon, die von der Aufnahme in ein europäisches Schema für die Cybersicherheitszertifizierung profitieren können.

(3) Die Aufnahme bestimmter IKT-Produkte, -Dienste und -Prozesse oder bestimmter Kategorien davon in das fortlaufende Arbeitsprogramm der Union muss aus einem oder mehreren der folgenden Gründe gerechtfertigt sein:

a) Verfügbarkeit und Entwicklung nationaler Schemata für die Cybersicherheitszertifizierung für bestimmte Kategorien von IKT-Produkten, -Diensten oder -Prozessen, insbesondere im Hinblick auf das Risiko der Fragmentierung;

b) einschlägige Politik oder einschlägiges Recht der Union oder der Mitgliedstaaten;

c) Nachfrage auf dem Markt;

d) Entwicklungen in der Cyberbedrohungslandschaft;

e) Beauftragung mit der Ausarbeitung eines bestimmten möglichen Schemas durch die Europäische Gruppe für die Cybersicherheitszertifizierung.

(4) Die Kommission trägt den Stellungnahmen der Europäischen Gruppe für die Cybersicherheitszertifizierung und der Gruppe der Interessenträger für die Cybersicherheitszertifizierung zum Entwurf des fortlaufenden Arbeitsprogramm der Union gebührend Rechnung.

(5) Das erste fortlaufende Arbeitsprogramm der Union wird spätestens am 28. Juni 2020 vorgelegt. Das fortlaufende Arbeitsprogramm der Union mindestens alle drei Jahre, und bei Bedarf öfter aktualisiert.

Artikel 48

Auftrag für ein europäisches Schema für die Cybersicherheitszertifizierung

(1) Die Kommission kann die ENISA damit beauftragen, ein mögliches Schema auszuarbeiten oder ein bestehendes europäisches Schema für die Cybersicherheitszertifizierung auf der Grundlage des fortlaufenden Arbeitsprogramm der Union zu überarbeiten.

(2) In entsprechend begründeten Fällen kann die Kommission oder die Europäische Gruppe für die Cybersicherheitszertifizierung die ENISA damit beauftragen, ein mögliches Schema auszuarbeiten oder ein bestehendes europäisches Schema für die Cybersicherheitszertifizierung, das nicht im fortlaufenden Arbeitsprogramm der Union enthalten ist, zu überarbeiten. Das fortlaufende Arbeitsprogramm der Union wird entsprechend aktualisiert.

Artikel 49

Ausarbeitung, Annahme und Überarbeitung der europäischen Schemata für die Cybersicherheitszertifizierung

(1) Auf Auftrag der Kommission arbeitet die ENISA gemäß Artikel 48 ein mögliches Schema aus, das den in den Artikeln 51, 52und 54 festgelegten Anforderungen genügt.

(2) nach einem Auftrag der Europäischen Gruppe für die Cybersicherheitszertifizierung gemäß Artikel 48 Absatz 2 kann die ENISA ein mögliches Schema ausarbeiten, das den in den Artikeln 51, 52und 54 festgelegten Anforderungen genügt. Lehnt die ENISA einen solchen Auftrag ab, so muss sie dies begründen. Jede Entscheidung, einen Auftrag abzulehnen, wird vom Verwaltungsrat getroffen.

(3) Bei der Ausarbeitung der möglichen Schemata konsultiert die ENISA alle in Frage kommenden Interessenträger im Wege eines förmlichen, offenen, transparenten und inklusiven Konsultationsprozesses.

(4) Für jedes mögliche Schema setzt die ENISA eine Ad-hoc-Arbeitsgruppe nach Artikel 20 Absatz 4 ein, damit sie der ENISA spezifische Beratung und Sachkenntnis bereitstellt.

(5) Die ENISA arbeitet eng mit der Europäischen Gruppe für die Cybersicherheitszertifizierung zusammen. Die Europäische Gruppe für die Cybersicherheitszertifizierung leistet der ENISA Unterstützung und fachliche Beratung bei der Ausarbeitung des möglichen Schemas und gibt eine Stellungnahme zu dem möglichen Schema ab.

(6) Die ENISA berücksichtigt die Stellungnahme der Europäischen Gruppe für die Cybersicherheitszertifizierung weitestgehend, bevor sie der Kommission das nach den Absätzen 3, 4 und 5 ausgearbeitete mögliche Schema vorlegt. Diese Stellungnahme der Europäischen Gruppe für die Cybersicherheitszertifizierung ist weder bindend, noch hindert das Fehlen einer solchen Stellungnahme die ENISA daran, das mögliche Schema der Kommission vorzulegen.

(7) Auf der Grundlage des von der ENISA ausgearbeiteten möglichen Schemas kann die Kommission Durchführungsrechtsakte erlassen, in denen für IKT-Produkte, -Dienste und -Prozesse, die die Anforderungen der Artikel 51, 52 und 54 erfüllen, ein europäisches Schema für die Cybersicherheitszertifizierung festgelegt wird. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 66 Absatz 2 genannten Prüfverfahren erlassen.

(8) Die ENISA bewertet mindestens alle fünf Jahre jedes angenommene europäische Schema für die Cybersicherheitszertifizierung, wobei sie die Rückmeldungen seitens der Interessenträger berücksichtigt. Erforderlichenfalls kann die Kommission oder die Europäische Gruppe für die Cybersicherheitszertifizierung die ENISA damit beauftragen, den Prozess der Ausarbeitung eines überarbeiteten möglichen Schemas nach Artikel 48 und nach dem vorliegenden Artikel einzuleiten.

Artikel 50

Website zu europäischen Schemata für die Cybersicherheitszertifizierung

(1) Die ENISA unterhält eine eigene Website, auf der sie über die europäischen Schemata für die Cybersicherheitszertifizierung, die europäischen Cybersicherheitszertifikate und EU-Konformitätserklärungen — was Information in Bezug auf nicht mehr gültige Schemata für die Cybersicherheitszertifizierung und widerrufene und abgelaufene europäische Cybersicherheitszertifikate und EU-Konformitätserklärungen einschließt — und die Ablage für Links zu den Informationen zur Cybersicherheit gemäß Artikel 55 informiert und für diese wirbt.

(2) Gegebenenfalls sollten auf der Website gemäß Absatz 1 auch die nationalen Cybersicherheitszertifizierungsschemata angegeben werden, die durch ein europäisches Schema für die Cybersicherheitszertifizierung ersetzt wurden.

Artikel 51

Sicherheitsziele der europäischen Schemata für die Cybersicherheitszertifizierung

Es wird ein europäisches Schema für die Cybersicherheitszertifizierung konzipiert, um — soweit zutreffend — mindestens die folgenden Sicherheitsziele zu verwirklichen:

a) Gespeicherte, übermittelte oder anderweitig verarbeitete Daten werden während des gesamten Lebenszyklus des IKT-Produkts, -Dienstes oder -Prozesses 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 IKT-Produkts, -Dienstes oder -Prozesses vor Zerstörung, Verlust, Änderung oder Nichtverfügbarkeit — gleich, ob sie zufällig oder unbefugt erfolgt sind — geschützt.

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

d) Bekannte Abhängigkeiten und Sicherheitslücken werden ermittelt und dokumentiert.

e) Es wird protokolliert, auf welche Daten, Dienste oder Funktionen zu welchem Zeitpunkt von wem zugegriffen wurde und welche Daten, Funktionen oder Dienste zu welchem Zeitpunkt von wem genutzt oder anderweitig verarbeitet worden sind.

f) 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.

g) Es wird nachgeprüft, dass IKT-Produkte, -Dienste und -Prozesse keine bekannten Sicherheitslücken aufweisen.

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

i) Es wird nachgeprüft, dass IKT-Produkte, -Dienste und -Prozesse sind durch Voreinstellungen und Technikgestaltung sicher sind.

j) IKT-Produkte, -Dienste und -Prozesse werden mit aktueller Software und Hardware, die keine allgemein bekannten Sicherheitslücken aufweisen, bereitgestellt und mit Mechanismen für sichere Updates ausgestattet.

Artikel 52

Vertrauenswürdigkeitsstufen der europäischen Schemata für die Cybersicherheitszertifizierung

(1) Ein europäisches Schema für die Cybersicherheitszertifizierung kann für IKT-Produkte, -Dienste und -Prozesse eine oder mehrere der Vertrauenswürdigkeitsstufen „niedrig“, „mittel“ und/oder „hoch“ angeben. Die Vertrauenswürdigkeitsstufe muss in einem angemessenen Verhältnis zu dem mit der beabsichtigten Verwendung eines IKT-Produkts, -Dienstes oder -Prozesses verbundenen Risiko im Hinblick auf die Wahrscheinlichkeit und die Auswirkungen eines Sicherheitsvorfalls stehen.

(2) Europäische Cybersicherheitszertifikate und EU-Konformitätserklärungen beziehen sich auf die jeweilige Vertrauenswürdigkeitsstufe, die im europäischen Schema für die Cybersicherheitszertifizierung angegeben ist, nach dem das europäische Cybersicherheitszertifikat oder die EU-Konformitätserklärung ausgestellt wurde.

(3) Die jeder Vertrauenswürdigkeitsstufe entsprechenden Sicherheitsanforderungen, einschließlich der entsprechenden Sicherheitsfunktionen und der entsprechenden Strenge und Gründlichkeit für die Bewertung, die das IKT-Produkt, der IKT-Dienst oder der IKT-Prozess durchlaufen muss, werden in dem jeweiligen europäischen Schema für die Cybersicherheitszertifizierung festgelegt.

(4) Das Zertifikat oder die EU-Konformitätserklärung nimmt Bezug auf die diesbezüglichen technischen Spezifikationen, Normen und Verfahren einschließlich technischer Prüfungen, deren Zweck in der Minderung oder Prävention der Gefahr von Cybersicherheitsvorfällen besteht.

(5) Ein europäisches Cybersicherheitszertifikat oder eine EU-Konformitätserklärung für die Vertrauenswürdigkeitsstufe „niedrig“ bietet die Gewissheit, dass die IKT-Produkte, -Dienste und -Prozesse, für welche dieses Zertifikat oder diese EU-Konformitätserklärung ausgestellt wird, die entsprechenden Sicherheitsanforderungen einschließlich der Sicherheitsfunktionen erfüllen und einer Bewertung unterzogen wurden, die darauf ausgerichtet ist, die bekannten grundlegenden Risiken für Sicherheitsvorfälle und Cyberangriffe möglichst gering zu halten. Die durchzuführende Bewertung beinhaltet mindestens eine Überprüfung der technischen Dokumentation. Ist eine solche Prüfung nicht geeignet, werden alternative Prüfungen mit gleicher Wirkung durchgeführt;

(6) Ein europäisches Cybersicherheitszertifikat für die Vertrauenswürdigkeitsstufe „mittel“ bietet die Gewissheit, dass die IKT-Produkte, -Dienste und -Prozesse, für welche dieses Zertifikat ausgestellt wird, die entsprechenden Sicherheitsanforderungen einschließlich der Sicherheitsfunktionen erfüllen und einer Bewertung unterzogen wurden, die darauf ausgerichtet ist, bekannte Cybersicherheitsrisiken und das Risiko von Cybersicherheitsvorfällen und Cyberangriffen seitens Akteuren mit begrenzten Fähigkeiten und Ressourcen möglichst gering zu halten. Die durchzuführende Bewertung beinhaltet mindestens Folgendes: eine Überprüfung, die zeigt, dass keine allgemein bekannten Sicherheitslücken vorliegen, und die Prüfung, dass die IKT-Produkte, -Dienste und -Prozesse die erforderlichen Sicherheitsfunktionen korrekt durchführen. Falls diese Bewertungstätigkeiten nicht geeignet sind, werden alternative Tätigkeiten mit gleicher Wirkung durchgeführt;

(7) Ein europäisches Cybersicherheitszertifikat für die Vertrauenswürdigkeitsstufe „hoch“ bietet die Gewissheit, dass die IKT-Produkte, -Dienste und -Prozesse, für welche dieses Zertifikat ausgestellt wird, die entsprechenden Sicherheitsanforderungen einschließlich der Sicherheitsfunktionen erfüllen und dass sie einer Bewertung unterzogen wurden, die darauf ausgerichtet ist, das Risiko von dem neuesten Stand der Technik entsprechenden Cyberangriffen durch Akteure mit umfangreichen Fähigkeiten und Ressourcen möglichst gering zu halten. Die durchzuführenden Bewertungstätigkeiten beinhaltet das Folgende; eine Nachprüfung, die zeigt, dass keine allgemein bekannten Sicherheitslücken vorliegen; eine Prüfung, die zeigt, dass die IKT-Produkte, -Dienste und -Prozesse die erforderlichen Sicherheitsfunktionen entsprechend dem neuesten Stand der Technik ordnungsgemäß durchführen, und eine Beurteilung ihrer Widerstandsfähigkeit gegen kompetente Angreifer mittels Penetrationstests Falls diese Bewertungstätigkeiten nicht geeignet sind, alternative Tätigkeiten durchgeführt.

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

Artikel 53

Selbstbewertung der Konformität

(1) Ein europäisches Schema für die Cybersicherheitszertifizierung kann die Durchführung einer Selbstbewertung der Konformität unter der alleinigen Verantwortung des Herstellers oder Anbieters von IKT-Produkten, -Diensten und -Prozessen zulassen. Die Selbstbewertung der Konformität ist nur für IKT-Produkte, -Dienste und -Prozesse mit niedrigem Risiko erlaubt, die der Vertrauenswürdigkeitsstufe „niedrig“ entsprechen.

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

(3) Der Hersteller oder Anbieter von IKT-Produkten, -Diensten oder -Prozessen hält die EU-Konformitätserklärung, die technische Dokumentation und alle weiteren einschlägigen Informationen in Bezug auf die Konformität der IKT-Produkte oder -Dienste mit dem Schema während eines Zeitraums, der im entsprechenden europäischen Schema für die Cybersicherheitszertifizierung festgelegt ist, für die in Artikel 58 genannte nationale Behörde für die Cybersicherheitszertifizierung bereit. Eine Kopie der EU-Konformitätserklärung ist der nationalen Behörde für die Cybersicherheitszertifizierung und der ENISA vorzulegen.

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

(5) Die ausgestellte EU-Konformitätserklärung wird in allen Mitgliedstaaten anerkannt.

Artikel 54

Elemente der europäischen Schemata für die Cybersicherheitszertifizierung

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

a) den Gegenstand und Umfang des Zertifizierungsschemas, einschließlich der Art oder Kategorie der erfassten IKT-Produkte, -Dienste und -Prozesse;

b) eine eindeutige Beschreibung des Zwecks des Schemas und der Art und Weise, wie die ausgewählten Normen, Bewertungsmethoden und Vertrauenswürdigkeitsstufen mit den Erfordernissen der vorgesehenen Nutzer des Schemas in Einklang gebracht wurden;

c) eine Bezugnahme auf die für die Bewertung maßgeblichen internationalen, europäischen oder nationalen Normen oder, wenn keine solchen Normen verfügbar oder geeignet sind, auf technische Spezifikationen, die die Auflagen des Anhangs II der Verordnung (EU) Nr. 1025/2012 erfüllen, oder — wenn solche Spezifikationen nicht verfügbar sind — auf die im europäischen Schema für die Cybersicherheitszertifizierung festgelegten technischen Spezifikationen oder Cybersicherheitsanforderungen;

d) gegebenenfalls eine oder mehrere Vertrauenswürdigkeitsstufen;

e) die Angabe, ob eine Selbstbewertung der Konformität im Rahmen des Schemas zulässig ist;

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

g) besondere Bewertungskriterien und -methoden — wie auch Bewertungsarten — für den Nachweis, dass die in Artikel 51 festgelegten Sicherheitsziele eingehalten werden;

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

i) Bedingungen für die Verwendung von Siegeln oder Kennzeichen, sofern das Schema solche vorsieht;

j) Vorschriften für die Überwachung der Einhaltung der mit dem europäischen Cybersicherheitszertifikat oder der EU-Konformitätserklärung verbundenen Anforderungen an IKT-Produkte, -Dienste und -Prozesse, einschließlich der Mechanismen für den Nachweis der beständigen Einhaltung der festgelegten Cybersicherheitsanforderungen;

k) falls anwendbar, Bedingungen für die Ausstellung, Aufrechterhaltung, Fortführung und Verlängerung eines europäischen Cybersicherheitszertifikats sowie Bedingungen für die Ausweitung oder Verringerung des Zertifizierungsumfangs;

l) Vorschriften, wie mit IKT-Produkten, -Diensten und -Prozessen zu verfahren ist, die zertifiziert wurden oder für die eine EU-Konformitätserklärung ausgestellt wurde, die aber den Anforderungen des Schemas nicht genügen;

m) Vorschriften für die Meldung und Behandlung bislang nicht erkannter Cybersicherheitslücken von IKT-Produkten und -Diensten und -Prozessen;

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

o) Angabe nationaler oder internationaler Schemata für die Cybersicherheitszertifizierung für dieselbe Art oder Kategorie von IKT-Produkten, -Diensten und -Prozessen, Sicherheitsanforderungen, Evaluierungskriterien und -methoden und Vertrauenswürdigkeitsstufen;

p) Inhalt und Format des europäischen Cybersicherheitszertifikats oder der EU-Konformitätserklärungen, die auszustellen sind;

q) die Dauer der Verfügbarkeit der EU-Konformitätserklärung, der technischen Dokumentation und aller weiteren bereitzuhaltenden Informationen des Herstellers oder Anbieters von IKT-Produkten, -Diensten und -Prozessen;

r) die maximale Gültigkeitsdauer der nach diesem Schema ausgestellten europäischen Cybersicherheitszertifikate;

s) eine Offenlegungspolitik für nach diesem Schema ausgestellte, geänderte oder entzogene europäische Cybersicherheitszertifikate;

t) Bedingungen für die auf Gegenseitigkeit beruhende Anerkennung von Zertifizierungsschemata von Drittländern;

u) falls anwendbar, Regeln für etwaige im Schema vorgesehene Verfahren zur gegenseitigen Begutachtung für die Behörden oder Stellen, die im Einklang mit Artikel 56 Absatz 6 europäische Cybersicherheitszertifikate für die Vertrauenswürdigkeitsstufe „hoch“ ausstellen. Diese Verfahren gelten unbeschadet der gegenseitigen Begutachtung gemäß Artikel 59;

v) Format und Verfahren, die von den Herstellern oder Anbietern von IKT-Produkten, -Diensten und -Prozessen bei der Bereitstellung und Aktualisierung der ergänzenden Informationen zur Cybersicherheit gemäß Artikel 55 zu befolgen sind.

(2) Die für das europäische Schema für die Cybersicherheitszertifizierung festgelegten Anforderungen stehen in Einklang mit allen geltenden rechtlichen Anforderungen, vor allem jenen, die sich aus dem harmonisierten Unionsrecht ergeben.

(3) Soweit dies in einem bestimmten Rechtsakt der Union so festgelegt ist, kann eine Zertifizierung oder eine EU-Konformitätserklärung, die auf der Grundlage eines europäischen Schemas für die Cybersicherheitszertifizierung ausgestellt wurde, dafür verwendet werden kann, die Vermutung zu begründen, dass eine Übereinstimmung mit den Anforderungen jenes Rechtsakts gegeben ist.

(4) Fehlt harmonisiertes Unionsrecht, so kann das Recht der Mitgliedstaaten auch festlegen, dass ein europäisches Schema für die Cybersicherheitszertifizierung dafür verwendet werden kann, die Vermutung zu begründen, dass eine Übereinstimmung mit den gesetzlichen Anforderungen gegeben ist.

Artikel 55

Ergänzende Informationen über die Cybersicherheit von zertifizierten IKT-Produkten, -Diensten und -Prozessen

(1) Hersteller oder Anbieter von zertifizierten IKT-Produkten, -Diensten oder -Prozessen oder von IKT-Produkten, -Diensten und -Prozessen, für die eine EU-Konformitätserklärung ausgestellt wurde, machen folgende ergänzende Cybersicherheitsangaben der Öffentlichkeit zugänglich:

a) Leitlinien und Empfehlungen zur Unterstützung der Endnutzer bei der sicheren Konfiguration, der Installation, der Bereitstellung, dem Betrieb und der Wartung der IKT-Produkte oder -Dienste;

b) Zeitraum, während dessen den Endnutzern eine Sicherheitsunterstützung angeboten wird, insbesondere in Bezug auf die Verfügbarkeit von cybersicherheitsbezogenen Aktualisierungen;

c) Kontaktangaben des Herstellers oder Anbieters und zulässige Verfahren für den Erhalt von Informationen über Sicherheitslücken von Endnutzern und im Bereich der IT-Sicherheit tätigen Wissenschaftlern;

d) Verweis auf Online-Register mit öffentlich offengelegten Sicherheitslücken in Bezug auf das IKT-Produkt, den IKT-Dienst oder den IKT-Prozess und gegebenenfalls relevante Cybersicherheitsratgeber.

(2) Die in Absatz 1 aufgeführten Angaben werden in elektronischer Form bereitgestellt und bleiben mindestens bis zum Ablauf des jeweiligen EU-Cybersicherheitszertifikats oder der EU-Konformitätserklärung verfügbar und werden bei Bedarf aktualisiert.

Artikel 56

Cybersicherheitszertifizierung

(1) Für IKT-Produkte, -Dienste, und -Prozesse die auf der Grundlage eines nach Artikel 49 angenommenen europäischen Schemas für die Cybersicherheitszertifizierung zertifiziert wurden, gilt die Vermutung der Einhaltung der Anforderungen dieses Schemas.

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

(3) Die Kommission bewertet regelmäßig die Effizienz und Nutzung der angenommenen europäischen Cybersicherheitszertifizierungsschemata sowie die Frage, ob ein bestimmtes europäisches Cybersicherheitszertifizierungsschema durch das einschlägige Unionsrecht verbindlich vorgeschrieben werden soll, um ein angemessenes Maß an Cybersicherheit von IKT-Produkten, -Diensten und -Prozessen in der Union sicherzustellen und das Funktionieren des Binnenmarktes zu verbessern. Die erste Bewertung findet bis zum 31. Dezember 2023 statt und danach nachfolgende Bewertungen finden mindestens alle zwei Jahre statt.

Die Kommission stellt auf der Grundlage der Ergebnisse der Bewertung fest, welche IKT-Produkte, -Dienste und -Prozesse, die unter ein bestehendes Zertifizierungsschema fallen, unter ein verpflichtendes Zertifizierungsschema fallen müssen.

Die Kommission konzentriert sich dabei vorrangig auf die Sektoren, die in Anhang II der Richtlinie (EU) 2016/1148 aufgeführt sind und die spätestens zwei Jahre nach der Annahme des ersten europäischen Cybersicherheitszertifizierungsschemas bewertet werden.

Bei der Vorbereitung der Bewertung verfährt die Kommission wie folgt:

a) Sie berücksichtigt die Auswirkungen der Maßnahmen auf die Hersteller oder Anbieter solcher IKT-Produkte, -Dienste und -Prozesse und auf die Nutzer hinsichtlich der Kosten dieser Maßnahmen und des gesellschaftlichen oder wirtschaftlichen Nutzens, der sich aus dem erwarteten höheren Maß an Sicherheit für die betreffenden IKT-Produkte, -Dienste und -Prozesse ergibt;

b) sie berücksichtigt das Bestehen und die Umsetzung von Rechtsvorschriften der Mitgliedstaaten und von Drittländern;

c) sie führt eine offene, transparente und inklusive Konsultation mit allen relevanten Interessenträgern und mit den Mitgliedstaaten durch;

d) sie berücksichtigt die Umsetzungsfristen sowie die Übergangsmaßnahmen oder -zeiträume und insbesondere in Hinblick auf die möglichen Auswirkungen der Maßnahme auf die Anbieter oder Hersteller von IKT-Produkten, -Diensten und -Prozessen, einschließlich KMU;

e) sie schlägt die schnellste und effizienteste Art und Weise für die Durchführung des Übergangs von freiwilligen zu obligatorischen Zertifizierungsschemata vor.

(4) Die in Artikel 60 genannten Konformitätsbewertungsstellen stellen ein europäisches Cybersicherheitszertifikat nach diesem Artikel mit der Vertrauenswürdigkeitsstufe „niedrig“ oder „mittel“ auf der Grundlage der Kriterien des nach Artikel 49 durch die Kommission angenommenen europäischen Schemas für die Cybersicherheitszertifizierung aus.

(5) Abweichend von Absatz 4 kann in hinreichend begründeten Fällen ein europäisches Schema für die Cybersicherheitszertifizierung vorsehen, dass ein im Rahmen dieses Schemas erteiltes europäisches Cybersicherheitszertifikat nur von einer öffentlichen Stelle auszustellen ist. Bei einer solchen Stelle muss es sich um eine der folgenden Stellen handeln:

a) eine nationale Behörde für die Cybersicherheitszertifizierung nach Artikel 58 Absatz 1;

b) eine als Konformitätsbewertungsstelle akkreditierte öffentliche Stelle nach Artikel 60 Absatz 1.

(6) Ist im Rahmen eines europäischen Schemas für die Cybersicherheitszertifizierung nach Artikel 49 die Vertrauenswürdigkeitsstufe „hoch“ erforderlich, so kann das europäische Cybersicherheitszertifikat nach diesem Schema nur von einer nationalen Behörde für die Cybersicherheitszertifizierung oder in den folgenden Fällen von einer Konformitätsbewertungsstelle ausgestellt werden:

a) wenn die nationale Behörde für die Cybersicherheitszertifizierung zuvor für jedes einzelne, von einer Konformitätsbewertungsstelle ausgestellte europäische Cybersicherheitszertifikat ihre Zustimmung erteilt hat oder

b) wenn die nationale Behörde für die Cybersicherheitszertifizierung die Aufgabe der Ausstellung solcher europäischen Cybersicherheitszertifikate zuvor allgemein einer Konformitätsbewertungsstelle übertragen hat.

(7) Die natürliche oder juristische Person, die ihre IKT-Produkte, -Dienste oder -Prozesse zur Zertifizierung einreicht, hat der in Artikel 58 genannten nationalen Behörde für die Cybersicherheitszertifizierung — sofern diese Behörde die Stelle ist, die das europäische Cybersicherheitszertifikat erteilt — oder der in Artikel 60 genannten Konformitätsbewertungsstelle alle für das Zertifizierungsverfahren notwendigen Informationen vorzulegen.

(8) Der Inhaber eines europäischen Cybersicherheitszertifikats informiert die in Absatz 7 genannte Behörde oder Stelle über etwaige später festgestellte Sicherheitslücken oder Unregelmäßigkeiten hinsichtlich der Sicherheit des zertifizierten IKT-Produkts, -Dienstes oder -Prozesses, die sich auf die mit der Zertifizierung verbundenen Anforderungen auswirken könnten. Die Behörde oder Stelle leitet diese Informationen unverzüglich an die betreffende nationale Behörde für die Cybersicherheitszertifizierung weiter.

(9) Ein europäisches Cybersicherheitszertifikat wird für die im jeweiligen europäischen Zertifizierungsschema für Cybersicherheit festgelegte Dauer erteilt und kann verlängert werden, sofern die einschlägigen Voraussetzungen weiterhin erfüllt sind.

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

Artikel 57

Nationale Cybersicherheitszertifizierungsschemata und Cybersicherheitszertifikate

(1) Unbeschadet des Absatzes 3 dieses Artikels werden nationale Schemata für die Cybersicherheitszertifizierung und die zugehörigen Verfahren für die IKT-Produkte, -Dienste und -Prozesse, die unter ein europäisches Schema für die Cybersicherheitszertifizierung fallen, ab dem Zeitpunkt unwirksam, der in dem nach Artikel 49 Absatz 7 erlassenen Durchführungsrechtsakt festgelegt ist. Nationale Schemata für die Cybersicherheitszertifizierung und die zugehörigen Verfahren für die IKT-Produkte, -Dienste und-Prozesse, die nicht unter ein europäisches Schema für die Cybersicherheitszertifizierung fallen, bleiben bestehen.

(2) Die Mitgliedstaaten führen keine neuen nationalen Schemata für die Cybersicherheitszertifizierung von IKT-Produkten, -Diensten und -Prozessen ein, die unter ein geltendes europäisches Schema für die Cybersicherheitszertifizierung fallen.

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

(4) Um die Fragmentierung des Binnenmarkts zu vermeiden, unterrichten die Mitgliedstaaten die Kommission und die Europäische Gruppe für die Cybersicherheitszertifizierung über die Absicht zur Ausarbeitung neuer nationaler Schemata für die Cybersicherheitszertifizierung.

Artikel 58

Nationale Behörden für die Cybersicherheitszertifizierung

(1) Jeder Mitgliedstaat benennt eine oder mehrere nationale Behörden für die Cybersicherheitszertifizierung in seinem Hoheitsgebiet oder im Einverständnis mit einem anderen Mitgliedstaat eine oder mehrere nationale Behörden für die Cybersicherheitszertifizierung mit Sitz in diesem anderen Mitgliedstaat, als für die Aufsichtsaufgaben im benennenden Mitgliedstaat zuständig.

(2) Jeder Mitgliedstaat teilt der Kommission den Namen der benannten nationalen Behörden für Cybersicherheitszertifizierung mit. Sofern ein Mitgliedstaat mehr als eine Behörde benennt, teilt er der Kommission auch die Aufgaben mit, die diesen Behörden jeweils zugewiesen wurden.

(3) Unbeschadet des Artikels 56 Absatz 5 Buchstabe a und Absatz 6 ist jede nationale Behörde für die Cybersicherheitszertifizierung im Hinblick auf ihre Organisation, Finanzierungsentscheidungen, Rechtsform und Entscheidungsfindung unabhängig von den Stellen, die sie beaufsichtigt.

(4) Die Mitgliedstaaten stellen sicher, dass die Tätigkeiten der nationalen Behörden für die europäische Cybersicherheitszertifizierung im Zusammenhang mit der Ausstellung von Zertifikaten nach Artikel 56 Absatz 5 Buchstabe a und Absatz 6 von den Aufsichtstätigkeiten nach diesem Artikel streng getrennt sind und dass diese Tätigkeiten unabhängig voneinander durchgeführt werden.

(5) Die Mitgliedstaaten stellen sicher, dass die nationalen Behörden für die Cybersicherheitszertifizierung eine angemessene Ausstattung zur Ausübung ihrer Befugnisse und zur wirksamen und effizienten Wahrnehmung ihrer Aufgaben besitzen.

(6) Im Hinblick auf eine wirksame Durchführung dieser Verordnung ist es angemessen, dass die nationalen Behörden für die Cybersicherheitszertifizierung in der Europäischen Gruppe für die Cybersicherheitszertifizierung in aktiver, wirksamer, effizienter und sicherer Weise mitarbeiten.

(7) Die nationalen Behörden für die Cybersicherheitszertifizierung haben folgende Aufgaben:

a) Überwachung und Durchsetzung der Vorschriften im Rahmen der europäischen Schemata für die Cybersicherheitszertifizierung gemäß Artikel 54 Absatz 1 Buchstabe j im Hinblick auf die Beobachtung der Übereinstimmung der IKT-Produkte, -Dienste und -Prozesse mit den Anforderungen der in ihrem jeweiligen Hoheitsgebiet ausgestellten europäischen Cybersicherheitszertifikate in Zusammenarbeit mit anderen zuständigen Marktüberwachungsbehörden;

b) Überwachung und Durchsetzung der Verpflichtungen der in ihrem jeweiligen Hoheitsgebiet niedergelassenen Hersteller oder Anbieter von IKT-Produkten, -Diensten oder -Prozessen, die eine Selbstbewertung der Konformität durchführen, insbesondere Überwachung und Durchsetzung der Verpflichtungen dieser Hersteller oder Anbieter nach Artikel 53 Absätze 2 und 3 und nach dem entsprechenden europäischen Schema für die Cybersicherheitszertifizierung;

c) unbeschadet des Artikels 60 Absatz 3 aktive Unterstützung der nationalen Akkreditierungsstellen bei der Überwachung und Beaufsichtigung der Tätigkeiten der Konformitätsbewertungsstellen für die Zwecke dieser Verordnung;

d) Überwachung und Beaufsichtigung der Tätigkeiten der in Artikel 56 Absatz 5 genannten öffentlichen Stellen;

e) gegebenenfalls Ermächtigung der Konformitätsbewertungsstellen nach Artikel 60 Absatz 3 und Beschränkung, Aussetzung oder Widerruf bestehender Ermächtigungen, wenn die Konformitätsbewertungsstellen gegen die Anforderungen dieser Verordnung verstoßen;

f) Bearbeitung von Beschwerden, die von natürlichen oder juristischen Personen in Bezug auf europäische Cybersicherheitszertifikate, die von der nationalen Behörde für die Cybersicherheitszertifizierung ausgestellt wurden, oder in Bezug auf europäische Cybersicherheitszertifikate, die nach Artikel 56 Absatz 6 von Konformitätsbewertungsstellen ausgestellt wurden, oder in Bezug auf EU-Konformitätserklärungen nach Artikel 53 eingereicht werden, und Untersuchung des Beschwerdegegenstands in angemessenem Umfang, und Unterrichtung des Beschwerdeführers über die Fortschritte und das Ergebnis der Untersuchung innerhalb einer angemessenen Frist;

g) Vorlage eines zusammenfassenden Jahresberichts über die ausgeführten Tätigkeiten gemäß den Buchstaben b, c und d dieses Absatzes oder gemäß Absatz 8 an die ENISA und die Europäische Gruppe für die Cybersicherheitszertifizierung;

h) Zusammenarbeit mit anderen nationalen Behörden für die Cybersicherheitszertifizierung und anderen öffentlichen Stellen; dies beinhaltet auch den Informationsaustausch über die etwaige Nichtkonformität von IKT-Produkten, -Diensten und -Prozessen mit den Anforderungen dieser Verordnung oder mit den Anforderungen bestimmter europäischer Schemata für die Cybersicherheitszertifizierung; und

i) Verfolgung einschlägiger Entwicklungen auf dem Gebiet der Cybersicherheitszertifizierung.

(8) Jede nationale Behörde für die Cybersicherheitszertifizierung 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 deren Einhaltung der Bestimmungen dieses Titels zu überprüfen;

c) sie kann im Einklang mit dem nationalen Recht geeignete Maßnahmen ergreifen, um sicherzustellen, dass die Konformitätsbewertungsstellen, die Inhaber von europäischen Cybersicherheitszertifikaten und die Aussteller von EU-Konformitätserklärungen den Anforderungen dieser Verordnung oder eines europäischen Schemas 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 dem nationalen Recht europäische Cybersicherheitszertifikate widerrufen, die von den nationalen Behörden für die Cybersicherheitszertifizierung oder europäische Cybersicherheitszertifikate, die nach Artikel 56 Absatz 6 von den Konformitätsbewertungsstellen ausgestellt wurden, wenn diese Zertifikate den Anforderungen dieser Verordnung oder eines europäischen Schemas für die Cybersicherheitszertifizierung nicht genügen;

f) sie kann im Einklang mit dem nationalen Recht Sanktionen nach Artikel 65 verhängen und die unverzügliche Beendigung von Verstößen gegen die in dieser Verordnung festgelegten Verpflichtungen anordnen.

(9) Die nationalen Behörden für die Cybersicherheitszertifizierung arbeiten untereinander und mit der Kommission zusammen, indem sie insbesondere Informationen, Erfahrungen und bewährte Verfahren im Zusammenhang mit der Cybersicherheitszertifizierung und technischen Fragen in Bezug auf die Cybersicherheit von IKT-Produkten -Diensten und -Prozessen austauschen.

Artikel 59

Gegenseitige Begutachtung

(1) Um in der gesamten Union gleichwertige Standards in Bezug auf die europäischen Cybersicherheitszertifikate und EU-Konformitätserklärungen zu erreichen, unterliegen die nationalen Behörden für die Cybersicherheitszertifizierung einer gegenseitigen Begutachtung.

(2) Die gegenseitige Begutachtung erfolgt auf der Grundlage fundierter und transparenter Bewertungskriterien und -verfahren und erstreckt sich insbesondere auf die Strukturen, Personalressourcen und Verfahren betreffenden Anforderungen sowie auf Vertraulichkeit und Beschwerden.

(3) Die gegenseitige Begutachtung umfasst die Bewertung folgender Aspekte:

a) gegebenenfalls die Frage, ob bei den Tätigkeiten der nationalen Behörden für die europäische Cybersicherheitszertifizierung im Zusammenhang mit der Ausstellung von Zertifikaten nach Artikel 56 Absatz 5 Buchstabe a und Absatz 6 eine strenge Trennung der Aufgaben und Zuständigkeiten von den Aufsichtstätigkeiten nach Artikel 58 gewahrt wird und beide Tätigkeiten unabhängig voneinander durchgeführt werden;

b) die Verfahren für die Überwachung und Durchsetzung der Vorschriften für die Beobachtung der Übereinstimmung von IKT-Produkten, -Diensten und -Prozessen mit den europäischen Cybersicherheitszertifikaten nach Artikel 58 Absatz 7 Buchstabe a;

c) die Verfahren für die Überwachung und Durchsetzung der Verpflichtungen der Hersteller und Anbieter von IKT-Produkten -Diensten oder -Prozessen nach Artikel 58 Absatz 7 Buchstabe b;

d) die Verfahren für die Überwachung, Genehmigung und Beaufsichtigung der Tätigkeiten der Konformitätsbewertungsstellen;

e) gegebenenfalls die Frage, ob das Personal von Behörden oder Stellen, die gemäß Artikel 56 Absatz 6 Zertifikate für die Vertrauenswürdigkeitsstufe „hoch“ ausstellen, über die erforderlichen Sachkenntnisse verfügt.

(4) Die gegenseitige Begutachtung erfolgt durch mindestens zwei nationale Behörden für die Cybersicherheitszertifizierung anderer Mitgliedstaaten und die Kommission, und sie wird mindestens einmal alle fünf Jahre durchgeführt. Die ENISA kann sich an der gegenseitigen Begutachtung beteiligen.

(5) Die Kommission kann Durchführungsrechtsakte erlassen, um einen Plan für die gegenseitige Begutachtung festzulegen, der sich auf einen Zeitraum von mindestens fünf Jahren erstreckt, und darin die Kriterien für die Zusammensetzung des die gegenseitige Begutachtung durchführenden Teams, die Methode für die gegenseitige Begutachtung und den Zeitplan, die Häufigkeit und die übrigen damit verbundenen Aufgaben vorzugeben. Beim Erlass dieser Durchführungsrechtsakte trägt die Kommission den Erwägungen der Europäischen Gruppe für die Cybersicherheitszertifizierung angemessen Rechnung. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 66 Absatz 2 genannten Prüfverfahren erlassen.

(6) Die Europäische Gruppe für die Cybersicherheitszertifizierung prüft die Ergebnisse der gegenseitigen Begutachtung, erstellt eine Zusammenfassung, die der Öffentlichkeit zugänglich gemacht werden kann, und erlässt erforderlichenfalls Leitlinien oder Empfehlungen zu den von den betreffenden Stellen zu ergreifenden Maßnahmen.

Artikel 60

Konformitätsbewertungsstellen

(1) Die Konformitätsbewertungsstellen werden von den nach der Verordnung (EG) Nr. 765/2008 benannten nationalen Akkreditierungsstellen akkreditiert. Diese Akkreditierung wird nur ausgestellt, wenn die Konformitätsbewertungsstelle die im Anhang der vorliegenden Verordnung aufgeführten Anforderungen erfüllt.

(2) Hat eine nationale Behörde für die Cybersicherheitszertifizierung nach Artikel 56 Absatz 5 Buchstabe a und Absatz 6 ein europäisches Cybersicherheitszertifikat ausstellt, so wird die Zertifizierungsstelle der nationalen Behörde für die Cybersicherheitszertifizierung nach Absatz 1 des vorliegenden Artikels als Konformitätsbewertungsstelle akkreditiert.

(3) Sind in einem europäischen Schema für die Cybersicherheitszertifizierung spezifische oder zusätzliche Anforderungen gemäß Artikel 54 Absatz 1 Buchstabe f festgelegt, so darf nur solchen Konformitätsbewertungsstellen von der nationalen Behörde für die Cybersicherheitszertifizierung die Befugnis erteilt werden, Aufgaben im Rahmen dieses Schemas wahrzunehmen, die diese Anforderungen einhalten.

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

Artikel 61

Notifikation

(1) Für jedes europäische Schema für die Cybersicherheitszertifizierung notifizieren die nationalen Behörden für die Cybersicherheitszertifizierung der Kommission die Konformitätsbewertungsstellen, die für die Erteilung von Zertifikaten entsprechend den in Artikel 52 genannten Vertrauenswürdigkeitsstufen akkreditiert und gegebenenfalls nach Artikel 60 Absatz 3 ermächtigt wurden. Die nationalen Behörden für die Cybersicherheitszertifizierung teilt der Kommission etwaige diesbezügliche Änderungen unverzüglich mit.

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

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

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

(5) Die Kommission kann im Wege von Durchführungsrechtsakten Einzelheiten, Form und Verfahren für die Notifikationen nach Absatz 1 festlegen. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 66 Absatz 2 genannten Prüfverfahren erlassen.

Artikel 62

Europäische Gruppe für die Cybersicherheitszertifizierung

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

(2) Die Europäische Gruppe für die Cybersicherheitszertifizierung setzt sich aus Vertretern der nationalen Behörden für die Cybersicherheitszertifizierung oder Vertretern anderer einschlägiger nationaler Behörden zusammen. Ein Mitglied der Europäischen Gruppe für die Cybersicherheitszertifizierung darf nicht mehr als zwei Mitgliedstaat vertreten.

(3) Interessenträger und maßgebliche Dritte können zur Teilnahme an den Sitzungen der Europäischen Gruppe für die Cybersicherheitszertifizierung und zur Beteiligung an ihrer Arbeit eingeladen werden.

(4) Die Europäische Gruppe für die Cybersicherheitszertifizierung hat folgende Aufgaben:

a) Sie berät und unterstützt die Kommission bei ihren Tätigkeiten zur Gewährleistung einer einheitlichen Umsetzung und Anwendung dieses Titels — insbesondere in Bezug auf das fortlaufende Arbeitsprogramm der Union — in politischen Fragen der Cybersicherheitszertifizierung, bei der Koordinierung von Politikkonzepten und bei der Ausarbeitung europäischer Schemata für die Cybersicherheitszertifizierung;

b) sie unterstützt und berät die ENISA bei der Ausarbeitung eines möglichen Schemas nach Artikel 49 und arbeitet hierbei mit der ENISA zusammen;

c) sie gibt nach Artikel 49 eine Stellungnahme zu den von der ENISA vorbereiteten möglichen Schemata ab;

d) sie beauftragt die ENISA mit der Ausarbeitung von möglichen Schemata nach Artikel 48 Absatz 2;

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

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

g) sie erleichtert die Zusammenarbeit zwischen den nationalen Behörden für die Cybersicherheitszertifizierung nach diesem Titel im Wege des Kapazitätsaufbaus und des Informationsaustauschs, insbesondere durch die Festlegung von Methoden für einen effizienten Austausch von Informationen über Fragen der Cybersicherheitszertifizierung;

h) sie leistet Unterstützung bei der Anwendung des Mechanismus der gegenseitigen Begutachtung gemäß den Regeln, die in einem europäischen Cybersicherheitszertifizierungsschema nach Artikel 54 Absatz 1 Buchstabe u festgelegt wurden;

i) sie erleichtert die Anpassung europäischer Schemata für die Cybersicherheitszertifizierung an international anerkannte Normen, indem sie unter anderem bestehende europäische Schemata für die Cybersicherheitszertifizierung überprüft und der ENISA erforderlichenfalls Empfehlungen unterbreitet, sich mit den einschlägigen internationalen Normungsorganisationen in Verbindung zu setzen, um Unzulänglichkeiten oder Lücken in verfügbaren international anerkannten Normen anzugehen.

(5) Die Kommission nimmt gemäß Artikel 8 Absatz 1 Buchstabe e die Sekretariatsgeschäfte der Europäischen Gruppe für die Cybersicherheitszertifizierung wahr, und führt mit Unterstützung der ENISA ihren Vorsitz.

Artikel 63

Beschwerderecht

(1) Natürliche und juristische Personen haben das Recht, bei dem Aussteller eines europäischen Cybersicherheitszertifikats oder — wenn sich die Beschwerde gegen ein von einer Konformitätsbewertungsstelle nach Artikel 56 Absatz 6 ausgestelltes europäischen Cybersicherheitszertifikat richtet — bei der zuständigen nationalen Behörde für die Cybersicherheitszertifizierung eine Beschwerde einzulegen.

(2) Die Behörde oder Stelle, bei der die Beschwerde eingelegt wurde, unterrichtet den Beschwerdeführer über den Stand des Verfahrens und die getroffene Entscheidung und informiert den Beschwerdeführer über die Möglichkeit eines wirksamen gerichtlichen Rechtsbehelfs nach Artikel 64.

Artikel 64

Recht auf einen wirksamen gerichtlichen Rechtsbehelf

(1) Jede natürliche oder juristische Person hat unbeschadet eines anderweitigen verwaltungsrechtlichen oder außergerichtlichen Rechtsbehelfs das Recht auf einen wirksamen gerichtlichen Rechtsbehelf in Bezug auf

a) Entscheidungen einer Behörde oder einer Stelle gemäß Artikel 63 Absatz 1, gegebenenfalls auch in Bezug auf die mangelnde Erteilung, Verweigerung der Erteilung oder Anerkennung eines europäischen Cybersicherheitszertifikats, das diese natürliche oder juristische Person innehat bzw. beantragt hat;

b) Untätigkeit im Anschluss an eine Beschwerde bei einer Behörde oder Stelle gemäß Artikel 63 Absatz 1.

(2) Verfahren nach diesem Artikel werden bei den Gerichten des Mitgliedstaats eingeleitet, in dem die Behörde oder Stelle, gegen die der Rechtsbehelf gerichtet ist, ihren Sitz hat.

Artikel 65

Sanktionen

Die Mitgliedstaaten erlassen Vorschriften über Sanktionen, die bei Verstößen gegen diesen Titel und bei Verstößen gegen die europäischen Schemata 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 unverzüglich mit und melden ihr etwaige spätere Änderungen.

TITEL IV

SCHLUSSBESTIMMUNGEN

Artikel 66

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 67

Bewertung und Überarbeitung

(1) Bis zum 28. Juni 2024 und danach alle fünf Jahre bewertet die Kommission die Wirkung, Wirksamkeit und Effizienz der ENISA und ihrer Arbeitsmethoden und prüft, ob das Mandat der ENISA möglicherweise geändert werden muss und welche finanziellen Auswirkungen eine solche Änderung hätte. In der Bewertung werden alle Rückmeldungen an die ENISA in Bezug auf ihre Tätigkeiten berücksichtigt. Gelangt die Kommission zu der Auffassung, dass Ziele, Mandat und Aufgaben der ENISA deren Tätigkeit nicht länger rechtfertigen können, kann sie eine Änderung dieser Verordnung im Hinblick auf die für die ENISA geltenden Bestimmungen vorschlagen.

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

(3) Bei der Bewertung wird beurteilt, ob wesentliche Anforderungen an die Cybersicherheit für den Zugang zum Binnenmarkt erforderlich sind, damit keine IKT-Produkte, -Dienste und -Prozesse auf den Unionsmarkt gelangen, die den grundlegenden Anforderungen an die Cybersicherheit nicht entsprechen.

(4) Die Kommission übermittelt bis zum 28. Juni 2024 und danach alle fünf Jahre den Bericht über die Bewertung zusammen mit ihren Schlussfolgerungen dem Europäischen Parlament, dem Rat und dem Verwaltungsrat. Die Ergebnisse des Berichts werden öffentlich bekannt gemacht.

Artikel 68

Aufhebung und Rechtsnachfolge

(1) Die Verordnung (EU) Nr. 526/2013 wird mit Wirkung vom 27. Juni 2019 aufgehoben.

(2) Bezugnahmen auf die Verordnung (EU) Nr. 526/2013 und auf die durch jene Verordnung errichtete ENISA gelten als Bezugnahmen auf die vorliegende Verordnung und auf die durch die vorliegende Verordnung errichtete ENISA.

(3) Die durch die vorliegende Verordnung errichtete ENISA ist in Bezug auf das Eigentum und alle Abkommen, rechtlichen Verpflichtungen, Beschäftigungsverträge, finanziellen Verpflichtungen und Verbindlichkeiten die Rechtsnachfolgerin der durch die Verordnung (EU) Nr. 526/2013 errichteten ENISA. Alle vom Verwaltungsrat und vom Exekutivrat gemäß der Verordnung (EU) Nr. 526/2013 getroffenen Entscheidungen bleiben gültig, sofern sie der vorliegenden Verordnung nicht zuwiderlaufen.

(4) Die ENISA wird zum 27. Juni 2019 für unbegrenzte Zeit errichtet.

(5) Der nach Artikel 24 Absatz 4 der Verordnung (EU) Nr. 526/2013 ernannte Exekutivdirektor bleibt im Amt und übt die Funktion des Exekutivdirektors nach Artikel 20 der vorliegenden Verordnung für die restliche Dauer seiner Amtszeit aus. Die übrigen Bestimmungen seines Vertrags bleiben unverändert.

(6) Die nach Artikel 6 der Verordnung (EU) Nr. 526/2013 ernannten Mitglieder des Verwaltungsrats und ihre Stellvertreter bleiben im Amt und üben die Funktion des Verwaltungsrats nach Artikel 15 der vorliegenden Verordnung für die restliche Dauer ihrer Amtszeit aus.

Artikel 69

Inkrafttreten

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

(2) Die Artikel 58, 60, 61, 63, 64und 65, gelten ab dem 28. Juni 2021.

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

Geschehen zu Straßburg am 17. April 2019.

Im Namen des Europäischen Parlaments	*Im Namen des Rates*
Der Präsident	*Der Präsident*
A. TAJANI	G. CIAMBA

ANHANG

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, -Diensten oder -Prozessen, die er bewertet, in keinerlei Verbindung steht.

3. Eine Stelle, die einem Wirtschaftsverband oder einem Fachverband angehört und die IKT-Produkte, -Dienste oder -Prozesse 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 die Abwesenheit jedweder Interessenkonflikte nachgewiesen sind.

4. Die Konformitätsbewertungsstellen, ihre oberste Leitungsebene und die für die Erfüllung der Konformitätsbewertungsaufgaben zuständigen Mitarbeiter dürfen weder Konstrukteur, Hersteller, Lieferant, Installateur, Käufer, Eigentümer, Verwender oder Wartungsbetrieb des zu bewertenden IKT-Produkts, -Dienstes oder -Prozesses noch Bevollmächtigter einer dieser Parteien sein. Dieses Verbot schließt nicht die Verwendung von bereits einer Konformitätsbewertung unterzogenen IKT-Produkten, die für die Tätigkeit der Konformitätsbewertungsstelle nötig sind, oder die Verwendung solcher IKT-Produkte zum persönlichen Gebrauch aus.

5. Die Konformitätsbewertungsstellen, 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, -Dienste oder -Prozesse beteiligt sein, noch die an diesen Tätigkeiten beteiligten Parteien vertreten. Die Konformitätsbewertungsstellen, ihre oberste Leitungsebene und die für die Erfüllung der Konformitätsbewertungsaufgaben zuständigen Mitarbeiter dürfen sich nicht mit Tätigkeiten befassen, die ihre Unabhängigkeit bei der Beurteilung oder ihre Integrität im Zusammenhang mit ihren Konformitätsbewertungstätigkeiten, beeinträchtigen können. Dieses Verbot gilt besonders für Beratungsdienste.

6. Falls eine Konformitätsbewertungsstelle Eigentum einer öffentlichen Stelle oder Einrichtung ist oder von dieser betrieben wird, sind die Unabhängigkeit und die Abwesenheit von Interessenkonflikten zwischen der nationalen Behörde für die Cybersicherheitszertifizierung und der Konformitätsbewertungsstelle sicherzustellen und zu dokumentieren.

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

8. 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 durch Druck oder Vergünstigungen, auch finanzieller Art, ausgesetzt sein, die sich auf ihre Beurteilung oder die Ergebnisse ihrer Konformitätsbewertungsarbeit auswirken könnte, insbesondere keinem Druck und keiner Einflussnahme durch Personen oder Personengruppen, die ein Interesse am Ergebnis dieser Tätigkeiten haben.

9. 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. Jegliche Unterauftragsvergabe oder die Inanspruchnahme von externem Personal sind angemessen zu dokumentieren, dürfen nicht über Vermittler erfolgen und bedürfen einer schriftlichen Vereinbarung, in der unter anderem Vertraulichkeitsaspekte und Interessenkonflikte geklärt werden. Die betreffende Konformitätsbewertungsstelle übernimmt die volle Verantwortung für die durchgeführten Aufgaben.

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

    a) das erforderliche Personal mit Fachkenntnis und ausreichender einschlägiger Erfahrung, um die bei der Konformitätsbewertung anfallenden Aufgaben zu erfüllen;

    b) Beschreibungen von Verfahren, nach denen die Konformitätsbewertung durchgeführt 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 nach Artikel 61 notifizierte Stelle wahrnimmt, und ihren 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, -Dienste oder -Prozesse und der Umstand, dass es sich um Massenfertigung oder Serienproduktion handelt, gebührend berücksichtigt werden.

11. 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.

12. Die Personen, die für die Durchführung der Konformitätsbewertungstätigkeiten zuständig sind, müssen Folgendes besitzen:

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

b) eine ausreichende Kenntnis der Anforderungen, die mit den durchzuführenden Konformitätsbewertungen 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 Konformitätsbewertungen.

13. Die Unparteilichkeit der Konformitätsbewertungsstellen, ihrer obersten Führungsebene, des für Bewertungen zuständigen Personals der Konformitätsbewertungsstelle und ihrer Unterauftragnehmer muss gewährleistet sein.

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

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

16. Die Konformitätsbewertungsstelle und ihre Mitarbeiter, Gremien, Tochterunternehmen, Unterauftragnehmer und alle verbundenen Stellen oder Mitarbeiter externer Gremien einer Konformitätsbewertungsstelle müssen die Vertraulichkeit wahren, und die Informationen, die sie bei der Durchführung ihrer Konformitätsbewertungsaufgaben nach dieser Verordnung oder nach einer nationalen Vorschrift zur Durchführung dieser Verordnung erhalten, fallen unter die berufliche Schweigepflicht, außer wenn eine Offenlegung aufgrund von Rechtsvorschriften der Union oder des Mitgliedstaats, denen diese Personen unterliegen, erforderlich ist und außer gegenüber den zuständigen Behörden der Mitgliedstaaten, in denen sie ihre Tätigkeiten ausüben. Die Rechte des geistigen Eigentums sind zu schützen. Die Konformitätsbewertungsstelle muss über dokumentierte Verfahren in Bezug auf die Anforderungen dieser Nummer verfügen.

17. Abgesehen von Nummer 16 schließen die Anforderungen dieses Anhangs in keiner Weise der Austausch von technischen Informationen und regulatorischen Leitlinien zwischen einer Konformitätsbewertungsstelle und einer Person, die eine Zertifizierung beantragt oder deren Beantragung in Erwägung zieht, aus.

18. Konformitätsbewertungsstellen müssen ihre Tätigkeiten im Einklang mit einer Reihe kohärenter, gerechter und angemessener Geschäftsbedingungen ausüben, wobei sie in Bezug auf Gebühren die Interessen der KMU berücksichtigen.

19. Die Konformitätsbewertungsstellen müssen die Anforderungen der einschlägigen Norm erfüllen, die gemäß der Verordnung (EG) Nr. 765/2008 für die Akkreditierung der Konformitätsbewertungsstellen, die die Zertifizierung von IKT-Produkten, -Diensten oder -Prozessen vornehmen, harmonisiert ist.

20. Die Konformitätsbewertungsstellen müssen sicherstellen, dass die für die Konformitätsbewertung eingesetzten Prüflabors den Anforderungen der einschlägigen Norm entsprechen, die gemäß der Verordnung (EG) Nr. 765/2008 für die Akkreditierung der Labors, die Tests durchführen, harmonisiert ist.

I

(Gesetzgebungsakte)

VERORDNUNGEN

VERORDNUNG (EU) 2021/887 DES EUROPÄISCHEN PARLAMENTS UND DES RATES

vom 20. Mai 2021

zur Einrichtung des Europäischen Kompetenzzentrums für Industrie, Technologie und Forschung im Bereich der Cybersicherheit und des Netzwerks nationaler Koordinierungszentren

DAS EUROPÄISCHE PARLAMENT UND DER RAT DER EUROPÄISCHEN UNION —

gestützt auf den Vertrag über die Arbeitsweise der Europäischen Union, insbesondere auf Artikel 173 Absatz 3 und Artikel 188 Absatz 1,

auf Vorschlag der Europäischen Kommission,

nach Zuleitung des Entwurfs des Gesetzgebungsakts an die nationalen Parlamente,

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

gemäß dem ordentlichen Gesetzgebungsverfahren ([2]),

in Erwägung nachstehender Gründe:

(1) Die Mehrheit der Bevölkerung der Union verfügt über einen Internetanschluss. Das tägliche Leben der Menschen und die Wirtschaft werden in zunehmendem Maße von digitalen Technologien bestimmt. Bürger und Unternehmen werden zunehmend der Gefahr schwerwiegender Cybersicherheitsvorfälle ausgesetzt und viele europäische Unternehmen verzeichnen jährlich mindestens einen Cybersicherheitsvorfall. Dies verdeutlicht, dass Abwehrfähigkeit geboten ist, die technischen und industriellen Fähigkeiten verbessert und hohe Cybersicherheitsstandards angewendet und ganzheitliche Lösungen für die Cybersicherheit, die sowohl Menschen als auch Erzeugnisse, Prozesse und Technologie in der Union einbinden, eingesetzt werden müssen sowie die Notwendigkeit, dass die Union auf dem Gebiet der Cybersicherheit und der digitalen Autonomie eine Führungsrolle übernimmt. Die Cybersicherheit kann auch verbessert werden, indem das Bewusstsein für Bedrohungen im Bereich der Cybersicherheit geschärft wird und Kompetenzen, Kapazitäten und Fähigkeiten in der gesamten Union entwickelt werden, wobei die gesellschaftlichen und ethischen Begleiterscheinungen und Bedenken konsequent zu berücksichtigen sind.

(2) Die Union hat ihre Maßnahmen zur Bewältigung der wachsenden Herausforderungen im Bereich der Cybersicherheit nach Vorlage der Cybersicherheitsstrategie durch die Kommission und die Hohe Vertreterin der Union für Außen- und Sicherheitspolitik (im Folgenden „Hohe Vertreterin") in ihrer Gemeinsamen Mitteilung an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen vom 7. Februar 2013 mit dem Titel „Cybersicherheitsstrategie der Europäischen Union — ein offener, sicherer und geschützter Cyberraum" (im Folgenden „Cybersicherheitsstrategie von 2013") kontinuierlich ausgebaut. Mit der Cybersicherheitsstrategie von 2013 sollte ein zuverlässiges, sicheres und offenes Cyberökosystem gefördert werden. Im Jahr 2016 erließ die Union mit der Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates ([3]) über die Sicherheit von Netz- und Informationssystemen die ersten Maßnahmen im Bereich der Cybersicherheit.

([1]) ABl. C 159 vom 10.5.2019, S. 63.
([2]) Standpunkt des Europäischen Parlaments vom 17. April 2019 (noch nicht im Amtsblatt veröffentlicht) und Standpunkt des Rates nach erster Lesung vom 20. April 2021 (noch nicht im Amtsblatt veröffentlicht). Standpunkt des Europäischen Parlaments vom 19. Mai 2021 (noch nicht im Amtsblatt veröffentlicht).
([3]) Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union (ABl. L 194 vom 19.7.2016, S. 1).

(3) Im September 2017 legten die Kommission und die Hohe Vertreterin dem Europäischen Parlament und dem Rat eine Gemeinsame Mitteilung mit dem Titel „Abwehrfähigkeit, Abschreckung und Abwehr: die Cybersicherheit in der EU wirksam erhöhen“ vor, um die Abwehrfähigkeit, Abschreckung und Abwehr der Union im Bereich der Cyberangriffe weiter zu stärken.

(4) Auf dem Digitalgipfel im September 2017 in Tallinn forderten die Staats- und Regierungschefs, dass die Union bis zum Jahr 2025 weltweit zum Vorreiter in Sachen Cybersicherheit werden müsse, um das Vertrauen, die Zuversicht und den Schutz der Bürger, Verbraucher und Unternehmen online zu sichern und ein freies, von mehr Sicherheit getragenes und durch Gesetze gesichertes Internet zu ermöglichen, und erklärten ihre Absicht, dass zur (Neu-)Entwicklung von Systemen und Lösungen im Bereich Informations- und Kommunikationstechnologie (IKT) verstärkt Open-Source-Lösungen und offene Standards, auch durch Interoperabilitäts- und Standardisierungsprogramme der Union (wie ISA[2]) entwickelte bzw. geförderte Lösungen und Standards, herangezogen würden, insbesondere, um eine Herstellerabhängigkeit (Lock-in-Effekt) zu vermeiden.

(5) Mit dem durch diese Verordnung eingerichteten Europäischen Kompetenzzentrum für Industrie, Technologie und Forschung im Bereich der Cybersicherheit (im Folgenden „Kompetenzzentrum“) sollte dazu beigetragen werden, die Sicherheit von Netz- und Informationssystemen, darunter das Internet und andere für das Funktionieren der Gesellschaft wichtige Infrastrukturen wie Verkehrs-, Gesundheits-, Energie- und Digitalinfrastruktur, Wasserversorgung, die Finanzmärkte und die Bankensysteme, zu erhöhen.

(6) Schwere Störungen von Netz- und Informationssystemen können einzelne Mitgliedstaaten und die Union als Ganzes beeinträchtigen. Daher ist für die Gesellschaft ebenso wie für die Wirtschaft ein hohes Maß an Sicherheit bei Netz- und Informationssystemen in der gesamten Union unerlässlich. Derzeit ist die Union von nichteuropäischen Cybersicherheitsanbietern abhängig. Es liegt jedoch im strategischen Interesse der Union, dass sie sicherstellt, dass wesentliche Forschungs- und Technologiekapazitäten im Bereich der Cybersicherheit gewahrt und weiterentwickelt werden, um die Netz- und Informationssysteme von Bürgern und Unternehmen und insbesondere kritische Netz- und Informationssysteme zu sichern, und dass sie zentrale Cybersicherheitsdienste bereitstellt.

(7) In der Union gibt es eine Fülle von Fachwissen und Erfahrungen bezüglich Forschung, Technologie und industrieller Entwicklung im Bereich der Cybersicherheit, jedoch sind die Anstrengungen in Forschung und Industrie fragmentiert — es mangelt an Einheitlichkeit und einer gemeinsamen Zugrichtung —, worunter die Wettbewerbsfähigkeit und der wirksame Schutz von Netzen und Systemen in diesem Bereich leidet. Solche Anstrengungen und solches Fachwissen müssen in effizienter Weise gebündelt, vernetzt und genutzt werden, um die vorhandenen Forschungs-, Technologie- und Industriekapazitäten sowie die vorhandenen Qualifikationen auf Unionsebene und nationaler Ebene zu stärken und zu ergänzen. Wenngleich die IKT-Branche vor großen Herausforderungen steht, etwa der Befriedigung der Nachfrage nach qualifizierten Arbeitskräften, kann sie doch Nutzen daraus ziehen, wenn sie die Vielfalt der Gesellschaft insgesamt vertritt, eine ausgewogene Vertretung der Geschlechter und der ethnischen Vielfalt und die Gleichbehandlung von Menschen mit Behinderungen erreicht und künftigen Sachverständigen im Bereich Cybersicherheit den Zugang zu Wissen und Fortbildung erleichtert, auch im Rahmen der nichtformalen Bildung solcher Sachverständiger, wie etwa bei Free- und Open-Source-Software-Projekten, Civic-Technology-Projekten, Start-up-Unternehmen und Kleinstunternehmen.

(8) Kleine und mittlere Unternehmen (KMU) sind wichtige Interessenträger in der Cybersicherheitsbranche der Union und können dank ihrer schnellen Reaktionsfähigkeit Spitzenlösungen bereitstellen. Nicht auf Cybersicherheit spezialisierte KMU sind jedoch tendenziell auch stärker durch Cybersicherheitsvorfälle gefährdet, da wirksame Cybersicherheitslösungen hohe Investitionen und umfangreiche Sachkenntnis erfordern. Das Kompetenzzentrum und das Netzwerk nationaler Koordinierungszentren (im Folgenden „Netzwerk“) müssen KMU daher durch einen leichteren Zugang der KMU zu Wissen und einen maßgeschneiderten Zugang zu den Ergebnissen von Forschung und Entwicklung unterstützen, damit die KMU sich hinreichend schützen können und damit im Bereich der Cybersicherheit tätige KMU ihre Wettbewerbsfähigkeit aufrechterhalten und ihren Beitrag zur Führungsrolle der Union auf dem Gebiet der Cybersicherheit leisten können.

(9) Sachverstand ist nicht nur in der Branche selbst und in Forschungskontexten zu finden. Bei den als „Civic-Tech-Projekte“ bezeichneten nichtkommerziellen und vorkommerziellen Projekten werden im Interesse der Gesellschaft und des Gemeinwohls offene Standards, offene Daten und freie und quelloffene Software genutzt.

(10) Der Bereich Cybersicherheit ist vielfältig. Die einschlägigen Interessenträger umfassen Interessenträger von öffentlichen Einrichtungen, der Mitgliedstaaten und der Union, sowie der Industrie, der Zivilgesellschaft, z. B. von Gewerkschaften, von Verbraucherverbänden oder aus der Free- und Open-Source-Software-Gemeinschaft, aus Wissenschaft und Forschung, und anderen Organisationen.

(11) In den im November 2017 angenommenen Schlussfolgerungen des Rates wurde die Kommission aufgefordert, rasch eine Folgenabschätzung der möglichen Optionen für die Einrichtung eines Netzwerks von Cybersicherheitskompetenzzentren und eines Europäischen Forschungs- und Kompetenzzentrums für Cybersicherheit vorzunehmen und bis Mitte 2018 ein einschlägiges Rechtsinstrument für die Einrichtung eines solchen Netzwerks und eines solchen Zentrums vorzuschlagen.

(12) Die Union verfügt nach wie vor nicht über ausreichende technologische und industrielle Kapazitäten und Fähigkeiten, um ihre Wirtschaft und ihre kritischen Infrastrukturen autonom zu sichern und zu einem weltweit führenden Akteur im Bereich der Cybersicherheit zu werden. Das Niveau der strategischen und nachhaltigen Abstimmung und Zusammenarbeit zwischen Branchen, Forschungsgemeinschaften im Bereich der Cybersicherheit und Regierungen ist unzureichend. Die Union leidet unter unzulänglichen Investitionen in und einem eingeschränkten Zugang zu Know-how, Kompetenzen und Einrichtungen im Bereich der Cybersicherheit, und nur wenige Ergebnisse von Forschung und Innovation im Bereich Cybersicherheit der Union werden in marktfähige Lösungen umgesetzt oder in der Wirtschaft großflächig eingesetzt.

(13) Die Errichtung des Kompetenzzentrums sowie des Netzwerks, das über das Mandat verfügt, zur Unterstützung industrieller Technologien und im Bereich Forschung und Innovation Maßnahmen zu ergreifen, ist der beste Weg, die Ziele der vorliegenden Verordnung zu verwirklichen und gleichzeitig die größtmögliche wirtschaftliche, soziale und ökologische Wirkung zu erzielen und die Interessen der Union zu wahren.

(14) Das Kompetenzzentrum sollte das wichtigste Instrument der Union sein, um Investitionen in Forschung, Technologie und industrielle Entwicklung im Bereich der Cybersicherheit zu bündeln sowie einschlägige Projekte und Initiativen zusammen mit dem Netzwerk durchzuführen. Das Kompetenzzentrum sollte aus dem mit der Verordnung (EU) 2021/695 des Europäischen Parlaments und des Rates ([4]) festgelegten Rahmenprogramm für Forschung und Innovation (im Folgenden „„Horizont Europa"") und dem mit der Verordnung (EU) 2021/694 des Europäischen Parlaments und des Rates ([5]) aufgestellten Programm „Digitales Europa" finanzielle Unterstützung für den Bereich der Cybersicherheit verwalten und gegebenenfalls auch für andere Programme offenstehen. Dieser Ansatz sollte dazu beitragen, Synergien zu schaffen und die finanzielle Unterstützung im Zusammenhang mit Initiativen der Union auf dem Gebiet der Forschung und Entwicklung, Innovation, Technologie und industriellen Entwicklung im Bereich der Cybersicherheit zu koordinieren und sollte unnötige Doppelarbeit vermeiden.

(15) Es ist wichtig, dass bei Forschungsprojekten im Bereich der Cybersicherheit, die durch das Kompetenzzentrum unterstützt werden, die Achtung der Grundrechte und ethisches Verhalten gewährleistet werden.

(16) Das Kompetenzzentrum sollte keine operativen Cybersicherheitsaufgaben wie Aufgaben im Zusammenhang mit Reaktionsteams für Computersicherheitsverletzungen (CSIRT), einschließlich der Überwachung und Bewältigung von Cybersicherheitsvorfällen, wahrnehmen. Das Kompetenzzentrum sollte jedoch in der Lage sein, im Einklang mit dem Auftrag und den Zielen dieser Verordnung die Entwicklung von IKT-Infrastrukturen im Dienste der Wirtschaftszweige, insbesondere von KMU, der Forschungsgemeinschaften, der Zivilgesellschaft und des öffentlichen Sektors zu erleichtern. Wenn die CSIRT und andere Interessenträger versuchen, die Meldung und Offenlegung von Schwachstellen zu fördern, sollten das Kompetenzzentrum und die Mitglieder der Kompetenzgemeinschaft für Cybersicherheit (im Folgenden „Gemeinschaft") in der Lage sein, diese Interessenträger auf deren Ersuchen im Rahmen ihrer jeweiligen Aufgaben zu unterstützen, und dabei Überschneidungen mit der durch die Verordnung (EU) 2019/881 des Europäischen Parlaments und des Rates ([6]) eingerichteten Agentur der Europäischen Union für Cybersicherheit (ENISA) vermeiden.

(17) Das Kompetenzzentrum, die Gemeinschaft und das Netzwerk sollen — was das Management der Gemeinschaft und die Vertretung der Gemeinschaft im Zentrum betrifft — von der Erfahrung und der breiten Vertretung der einschlägigen Interessenträger, die während der Laufzeit von Horizont 2020 — des mit der Verordnung (EU) Nr. 1291/2013 des Europäischen Parlaments und des Rates ([7]) eingerichteten Rahmenprogramms für Forschung und Innovation (2014-2020) — in der vertraglichen öffentlich-privaten Partnerschaft für Cybersicherheit zwischen der Kommission und der Europäischen Cybersicherheitsorganisation (ECSO) aufgebaut wurde, von den Erfahrungen, die im Zuge der Anfang 2019 im Rahmen von Horizont 2020 eingeleiteten vier Pilotprojekte — nämlich CONCORDIA, ECHO, SPARTA und CyberSec4Europe — sowie vom Pilotprojekt und von den vorbereitenden Maßnahmen im Rahmen der Prüfung freier und quelloffener Software (EU-FOSSA) gesammelt wurden, profitieren.

(18) Angesichts des Umfangs der mit der Cybersicherheit verbundenen Herausforderungen und der in anderen Teilen der Welt getätigten Investitionen in Cybersicherheitskapazitäten und -fähigkeiten sollten die Union und die Mitgliedstaaten ermutigt werden, ihre finanzielle Unterstützung für Forschung, Entwicklung und Realisierung in diesem Bereich aufzustocken. Um Skaleneffekte zu erzielen und in der gesamten Union ein vergleichbares Schutzniveau zu erreichen, sollten die Bemühungen der Mitgliedstaaten in einen Unionsrahmen fließen, indem sie aktiv zur Arbeit des Kompetenzzentrums und des Netzwerks beitragen.

([4]) Verordnung (EU) 2021/695 des Europäischen Parlaments und des Rates vom 28. April 2021 über das Rahmenprogramm für Forschung und Innovation „Horizont Europa" sowie über die Regeln für die Beteiligung und die Verbreitung der Ergebnisse und zur Aufhebung der Verordnungen (EU) Nr. 1290/2013 und (EU) Nr. 1291/2013 (ABl. L 170 vom 12.5.2021, S. 1).

([5]) Verordnung (EU) 2021/694 des Europäischen Parlaments und des Rates vom 29. April 2021 zur Aufstellung des Programms „Digitales Europa" und zur Aufhebung des Beschlusses (EU) 2015/2240 (ABl. L 166 vom 11.5.2021, S. 1).

([6]) Verordnung (EU) 2019/881 des Europäischen Parlaments und des Rates vom 17. April 2019 über die ENISA (Agentur der Europäischen Union für Cybersicherheit) und über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik und zur Aufhebung der Verordnung (EU) Nr. 526/2013 (Rechtsakt zur Cybersicherheit) (ABl. L 151 vom 7.6.2019, S. 15).

([7]) Verordnung (EU) Nr. 1291/2013 des Europäischen Parlaments und des Rates vom 11. Dezember 2013 über das Rahmenprogramm für Forschung und Innovation Horizont 2020 (2014-2020) und zur Aufhebung des Beschlusses Nr. 1982/2006/EG (ABl. L 347 vom 20.12.2013, S. 104).

(19) Soweit das für den Auftrag, die Ziele und die Aufgaben des Kompetenzzentrums von Bedeutung ist, sollten das Kompetenzzentrum und die Gemeinschaft zur Förderung der Wettbewerbsfähigkeit der Union und hoher Cybersicherheitsnormen auf internationaler Ebene einen Austausch mit der internationalen Gemeinschaft über Entwicklungen im Bereich Cybersicherheit, einschließlich Produkte und Verfahren, und im Bereich Normen und technische Normen, anstreben. Zu den einschlägigen technischen Normen könnte für die Zwecke dieser Verordnung auch die Erstellung von Referenzimplementierungen gehören, einschließlich Implementierungen, die im Rahmen von auf offenen Standards beruhenden Lizenzen veröffentlicht wurden.

(20) Das Kompetenzzentrum hat seinen Sitz in Bukarest.

(21) Das Kompetenzzentrum sollte bei der Ausarbeitung seines jährlichen Arbeitsprogramms (im Folgenden „jährliches Arbeitsprogramm") die Kommission über seinen Kofinanzierungsbedarf, den es auf der Grundlage der von Mitgliedstaaten geplanten Kofinanzierungsbeiträge für gemeinsame Maßnahmen ermittelt, informieren, damit die Kommission bei der Aufstellung des Entwurfs des Gesamthaushaltsplans der Union für das folgende Jahr einen entsprechenden Unionsbeitrag einstellen kann.

(22) Die Kommission sollte bei der Ausarbeitung des Arbeitsprogramms für „Horizont Europa" bei die Cybersicherheit betreffenden Fragen, auch im Kontext des Verfahrens zur Konsultation der Interessenträger und insbesondere vor der Verabschiedung dieses Arbeitsprogramms, die Beiträge des Kompetenzzentrums berücksichtigen und diese Beiträge auch dem Programmausschuss von „Horizont Europa" zur Verfügung stellen.

(23) Das Kompetenzzentrum sollte als eine mit Rechtspersönlichkeit ausgestattete Einrichtung der Union errichtet werden, auf die die Delegierte Verordnung (EU) 2019/715 der Kommission ([8]) Anwendung findet, um es ihm zu ermöglichen, seine Rolle im Bereich der Cybersicherheit auszuüben, die Einbeziehung des Netzwerks zu unterstützen und die Leitungsrolle der Mitgliedstaaten zu stärken. Das Kompetenzzentrum sollte eine doppelte Funktion wahrnehmen und sowohl spezifische Aufgaben in Bezug auf Industrie, Technologie und Forschung im Bereich der Cybersicherheit gemäß der vorliegenden Verordnung ausführen als auch cybersicherheitsbezogene Finanzierungsmittel aus mehreren Programmen, insbesondere aus „Horizont Europa" und dem Programm „Digitales Europa" sowie gegebenenfalls auch aus weiteren Unionsprogrammen, verwalten. Diese Verwaltung müsste im Einklang mit den für diese Programme geltenden Vorschriften erfolgen. Da die Finanzierungsmittel für den Betrieb des Kompetenzzentrums überwiegend aus „Horizont Europa" und aus dem Programm „Digitales Europa" stammen würden, muss das Kompetenzzentrum dennoch für die Zwecke des Haushaltsvollzugs, einschließlich in der Programmplanungsphase, als Partnerschaft betrachtet werden.

(24) Infolge des Beitrags der Union muss der Zugang zu den Ergebnissen der Tätigkeiten des Kompetenzzentrums und den Projekten so offen wie möglich und so beschränkt wie nötig gestaltet werden und eine Wiederverwendung hat möglich zu sein, soweit das angemessen ist.

(25) Das Kompetenzzentrum sollte die Arbeit des Netzwerks erleichtern und koordinieren. Das Netzwerk sollte aus einem nationalen Koordinierungszentren je Mitgliedstaat bestehen. Die nationalen Koordinierungszentren, die von der Kommission als Einrichtungen anerkannt wurden, die über die notwendigen Kapazitäten zur Mittelverwaltung verfügen, um den Auftrag und die Ziele nach dieser Verordnung zu erfüllen, sollten eine direkte finanzielle Unterstützung durch die Union erhalten, einschließlich Finanzhilfen, die ohne Aufforderung zur Einreichung von Vorschlägen vergeben werden, um ihre Tätigkeiten im Zusammenhang mit dieser Verordnung durchzuführen.

(26) Bei den nationalen Koordinierungszentren sollte es sich um öffentliche Einrichtungen oder Einrichtungen mit mehrheitlich staatlicher Beteiligung handeln, die nach nationalem Recht, einschließlich durch Befugnisübertragung, Aufgaben der öffentlichen Verwaltung wahrnehmen, und sie sollten von den Mitgliedstaaten ausgewählt werden. Die Funktionen eines nationalen Koordinierungszentrums in einem Mitgliedstaat sollten von einer Einrichtung wahrgenommen werden können, die andere nach Unionsrecht vorgesehene Funktionen wahrnimmt, beispielsweise die einer zuständigen nationalen Behörde, einer zentralen Anlaufstelle im Sinne der Richtlinie (EU) 2016/1148 oder anderer Verordnungen der Union oder die eines Digitalen Innovationszentrums im Sinne der Verordnung (EU) 2021/694. Andere Einrichtungen des öffentlichen Sektors oder Einrichtungen, die in einem Mitgliedstaat Aufgaben der öffentlichen Verwaltung wahrnehmen, sollten das nationale Koordinierungszentrum in diesem Mitgliedstaat bei der Wahrnehmung seiner Funktionen unterstützen können.

(27) Die nationalen Koordinierungszentren sollten die erforderlichen Verwaltungskapazitäten haben, über Fachwissen in Bezug auf Industrie, Technologie und Forschung im Bereich der Cybersicherheit verfügen oder Zugang dazu haben sowie in der Lage sein, sich wirksam mit den Fachkreisen der Industrie, des öffentlichen Sektors und der Forschung auszutauschen und abzustimmen.

(28) Die Bedeutung eines angemessenen Bewusstseins für Cybersicherheit und entsprechender Kompetenzen sollte sich in den Bildungssystemen der Mitgliedstaaten niederschlagen. Zu diesem Zweck und unter Berücksichtigung der Rolle der ENISA sowie unbeschadet der Zuständigkeiten der Mitgliedstaaten für Bildung sollten neben den einschlägigen Behörden und Interessenträgern auch die nationalen Koordinierungszentren zur Förderung und Verbreitung von Bildungsprogrammen im Bereich der Cybersicherheit beitragen.

([8]) Delegierte Verordnung (EU) 2019/715 der Kommission vom 18. Dezember 2018 über die Rahmenfinanzregelung für gemäß dem AEUV und dem Euratom-Vertrag geschaffene Einrichtungen nach Artikel 70 der Verordnung (EU, Euratom) 2018/1046 des Europäischen Parlaments und des Rates (ABl. L 122 vom 10.5.2019, S. 1).

(29) Die nationalen Koordinierungszentren sollten vom Kompetenzzentrum Finanzhilfen erhalten können, um Dritten in Form von Finanzhilfen finanzielle Unterstützung zu leisten. Die direkten Kosten, die den nationalen Koordinierungszentren für die Bereitstellung und Verwaltung von finanzieller Unterstützung für Dritte entstehen, sollten unter den entsprechenden Programmen förderfähig sein.

(30) Das Kompetenzzentrum, das Netzwerk und die Gemeinschaft sollten helfen, die neuesten Cybersicherheitsprodukte, -dienste und -verfahren voranzubringen und zu verbreiten. Gleichzeitig sollten das Kompetenzzentrum und das Netzwerk die Cybersicherheitsfähigkeiten der nachfrageseitigen Industrie fördern, indem sie insbesondere Entwicklern und Betreibern in Bereichen wie Verkehr, Energie, Gesundheit, Finanzen, Regierung, Telekommunikation, Fertigung und Raumfahrt Unterstützung leisten, um solchen Entwicklern und Betreibern bei der Bewältigung ihrer Herausforderungen im Bereich der Cybersicherheit, beispielsweise durch die Umsetzung konzeptionsintegrierter Sicherheit („security by design"), zu helfen. Das Kompetenzzentrum und das Netzwerk sollten außerdem die Normung und Realisierung von Cybersicherheitsprodukten, -diensten und -verfahren unterstützen und gleichzeitig, soweit möglich, die Umsetzung des in der Verordnung (EU) 2019/881 festgelegten europäischen Rahmens für die Cybersicherheitszertifizierung fördern.

(31) Da Cyberbedrohungen und Cybersicherheit von schnellen Veränderungen gekennzeichnet sind, muss die Union in der Lage sein, sich schnell und kontinuierlich an neue Entwicklungen in diesem Bereich anzupassen. Daher sollten das Kompetenzzentrum, das Netzwerk und die Gemeinschaft hinreichend flexibel sein, damit die erforderliche Fähigkeit, auf solche Entwicklungen zu reagieren, vorhanden ist. Sie sollten Projekte unterstützen, mit denen Einrichtungen ermöglicht wird, ihre Fähigkeiten stetig auszubauen und damit sowohl die eigene Abwehrfähigkeit als auch die der Union zu stärken.

(32) Das Kompetenzzentrum sollte die Gemeinschaft unterstützen. Das Kompetenzzentrum sollte die für Cybersicherheit relevanten Teile von „Horizont Europa" und des Programms „Digitales Europa" in Übereinstimmung mit dem mehrjährigen Arbeitsprogramm des Kompetenzzentrums (im Folgenden „mehrjähriges Arbeitsprogramm"), dem jährlichen Arbeitsprogramm sowie dem Strategieplanungsprozess im Rahmen von „Horizont Europa" umsetzen, indem Finanzhilfen und andere Formen von Finanzierungen vergeben werden, vor allem nach einer wettbewerbsorientierten Aufforderung zur Einreichung von Vorschlägen. Das Kompetenzzentrum sollte auch die Weitergabe von Fachwissen im Netzwerk und in der Gemeinschaft erleichtern und sollte gemeinsame Investitionen der Union, der Mitgliedstaaten oder der Industrie unterstützen. Besonderes Augenmerk sollte auf die Unterstützung von KMU im Bereich der Cybersicherheit und Maßnahmen zur Schließung von Qualifikationslücken gerichtet werden.

(33) Die für die Projektvorbereitung geleistete technische Hilfe sollte in uneingeschränkt objektiver und transparenter Weise erfolgen, mit der sichergestellt wird, dass alle potenziellen Begünstigten die gleichen Informationen erhalten und mit der Interessenkonflikte vermieden werden.

(34) Das Kompetenzzentrum sollte die langfristige strategische Zusammenarbeit und Koordinierung der Tätigkeiten der Gemeinschaft anregen und unterstützen, was eine große, offene, interdisziplinäre und vielfältige Gruppe von im Bereich Cybersicherheitstechnologie tätigen europäischen Interessenträger einbeziehen würde. Die Gemeinschaft sollte Forschungseinrichtungen, Branchen sowie den öffentlichen Sektor umfassen. Die Gemeinschaft sollte — insbesondere über die strategische Beratungsgruppe — einen Beitrag zu den Tätigkeiten des Kompetenzzentrums, dem mehrjährigen Arbeitsprogramm und dem jährlichen Arbeitsprogramm leisten. Die Gemeinschaft sollte auch von den Tätigkeiten des Kompetenzzentrums und des Netzwerks zum Aufbau von Gemeinschaften profitieren; darüber hinaus sollte sie aber im Hinblick auf Aufforderungen zur Einreichung von Vorschlägen oder Ausschreibungen nicht bevorzugt werden. Die Gemeinschaft sollte sich aus kollektiven Einrichtungen und Organisationen zusammensetzen. Damit das gesamte Fachwissen auf dem Gebiet der Cybersicherheit in der Union genutzt werden kann, sollten das Kompetenzzentrum und seine Gremien in der Lage sein, gleichzeitig auch auf das Fachwissen natürlicher Personen als Ad-hoc-Sachverständige zurückzugreifen.

(35) Das Kompetenzzentrum sollte mit der ENISA zusammenarbeiten und Synergien mit dieser Agentur sicherstellen und dem Kompetenzzentrum sachdienliche Hinweise von der ENISA geben, wenn es um die Festlegung der Finanzierungsprioritäten geht.

(36) Um den Erfordernissen sowohl der Anbieter- als auch der Nachfrageseite im Bereich Cybersicherheit gerecht zu werden, sollte sich die Aufgabe des Kompetenzzentrums, Branchen Fachwissen und technische Hilfe im Bereich der Cybersicherheit bereitzustellen, auf IKT-Produkte, -Prozesse und -Dienste sowie auf alle anderen technischen Produkte und Prozesse beziehen, in die Cybersicherheit einzubinden ist. Auf Antrag sollte auch der öffentliche Sektor vom Kompetenzzentrum unterstützt werden können.

(37) Um ein tragfähiges Cybersicherheitsumfeld zu etablieren, muss bei der Entwicklung, der Wartung, dem Betrieb und der Aktualisierung von Infrastrukturen, Produkten und Diensten grundsätzlich die konzeptionsintegrierte Sicherheit greifen, indem insbesondere modernste sichere Entwicklungsmethoden, angemessene Sicherheitstests und Sicherheitsprüfungen unterstützt, unverzüglich Aktualisierungen zur Behebung bekannter Schwachstellen oder Gefahren bereitgestellt und, soweit möglich, Dritte dazu befähigt werden, über das jeweilige Wartungsende des Produkts hinaus Aktualisierungen zu erstellen und bereitzustellen. Die konzeptionsintegrierte Sicherheit des IKT-Produkts, -Dienstes oder -Prozesses sollte während seiner gesamten Lebensdauer über dessen Konzeption und durch Entwicklungsprozesse sichergestellt werden, die ständig weiterentwickelt werden, um das Risiko von Schäden durch eine böswillige Nutzung zu verringern.

(38) Während das Kompetenzzentrum und das Netzwerk sich um stärkere Synergien und Abstimmung zwischen dem zivilen und dem Verteidigungssektor im Bereich der Cybersicherheit bemühen sollten, sollten die unter diese Verordnung fallenden, im Rahmen von „Horizont Europa" finanzierten Projekte im Einklang mit der Verordnung (EU) 2021/695 durchgeführt werden, in der festgelegt ist, dass der Schwerpunkt bei Forschungs- und Innovationstätigkeiten im Rahmen von „Horizont Europa" ausschließlich auf zivilen Anwendungen liegen muss.

(39) Diese Verordnung findet in erster Linie auf zivile Angelegenheiten Anwendung, jedoch können die Tätigkeiten der Mitgliedstaaten im Rahmen dieser Verordnung den Besonderheiten der Mitgliedstaaten Rechnung tragen, wenn die Cybersicherheitspolitik durch Behörden verfolgt wird, die sowohl zivile als auch militärische Aufgaben wahrnehmen und sollten darauf ausgerichtet sein, Komplementarität zu erreichen und Überschneidungen mit verteidigungsbezogenen Finanzierungsinstrumenten zu vermeiden.

(40) Diese Verordnung sollte die Haftung und die Transparenz des Kompetenzzentrums und jener Unternehmen, die Finanzmittel erhalten, im Einklang mit den einschlägigen Programmverordnungen gewährleisten.

(41) Die Umsetzung von Realisierungsprojekten, die insbesondere auf Unionsebene oder über gemeinsame Auftragsvergabe realisierte Infrastrukturen und Fähigkeiten betreffen, könnte in verschiedene Umsetzungsphasen unterteilt werden, etwa in getrennte Ausschreibungen für Hardware-Design und Software-Architektur, ihre Einrichtung sowie ihren Betrieb und ihre Wartung, wobei Unternehmen jeweils nur an einer der Phasen teilnehmen dürften und gegebenenfalls verlangen könnte, dass die Begünstigten, die an einer oder mehreren dieser Phasen beteiligt sind, bestimmte für Europa geltende Anforderungen in Bezug auf Eigentum oder Kontrolle erfüllen.

(42) Angesichts ihres Fachwissens im Bereich der Cybersicherheit und ihres Mandats als Bezugspunkt der Organe, Einrichtungen und sonstigen Stellen der Union sowie anderen maßgeblichen Interessenträgern der Union für Beratung und Fachwissen auf dem Gebiet der Cybersicherheit und angesichts der von ihr im Zusammenhang mit ihren Aufgaben gesammelten Beiträge sollte sich die ENISA aktiv an den Tätigkeiten des Kompetenzzentrums, einschließlich der Entwicklung der Agenda, beteiligen, wobei jedoch — insbesondere durch die Mitwirkung der ENISA als ständige Beobachterin im Verwaltungsrat des Kompetenzzentrums — Doppelarbeit vermieden werden sollte. Bezüglich der Aufstellung der Agenda, des jährlichen Arbeitsprogramms und des mehrjährigen Arbeitsprogramms sollten der Exekutivdirektor des Kompetenzzentrums und der Verwaltungsrat sämtliche von der ENISA durchgeführten strategischen Beratungen und bereitgestellten Beiträge im Einklang mit der vom Verwaltungsrat festgelegten Geschäftsordnung berücksichtigen.

(43) Erhalten die nationalen Koordinierungszentren und die Einrichtungen, die Teil der Gemeinschaft sind, einen Finanzbeitrag aus dem Unionshaushalt, so sollten sie öffentlich machen, dass ihre jeweiligen Tätigkeiten im Rahmen der vorliegenden Verordnung durchgeführt werden.

(44) Die Kosten für die Einrichtung des Kompetenzzentrums sowie für die Verwaltungs- und Koordinierungstätigkeiten des Kompetenzzentrums sollten von der Union sowie — im Verhältnis zum freiwilligen Beitrag der Mitgliedstaaten zu gemeinsamen Maßnahmen — von den Mitgliedstaaten finanziert werden. Um eine Doppelfinanzierung zu vermeiden, sollten in diese Tätigkeiten nicht gleichzeitig auch Mittel aus anderen Unionsprogrammen fließen.

(45) Der Verwaltungsrat, der sich aus Vertretern der Mitgliedstaaten und der Kommission zusammensetzen sollte, sollte die allgemeine Ausrichtung der Tätigkeit des Kompetenzzentrums festlegen und dafür sorgen, dass das Kompetenzzentrums seine Aufgaben im Einklang mit dieser Verordnung wahrnimmt. Der Verwaltungsrat sollte die Agenda annehmen.

(46) Dem Verwaltungsrat sollten über die erforderlichen Befugnisse übertragen werden, um den Haushaltsplan des Kompetenzzentrums zu erstellen. Er sollte die Ausführung des Haushaltsplans überprüfen, eine angemessene Finanzordnung annehmen sowie transparente Verfahren für die Entscheidungsfindung des Kompetenzzentrums festlegen, einschließlich für die Annahme des jährlichen Arbeitsprogramm und des mehrjährigen Arbeitsprogramms, die die Agenda widerspiegeln. Der Verwaltungsrat sollte sich auch eine Geschäftsordnung geben, den Exekutivdirektor ernennen und über die Verlängerung oder die Beendigung der Amtszeit des Exekutivdirektors beschließen.

(47) Der Verwaltungsrat sollte die strategischen Tätigkeiten und Umsetzungstätigkeiten des Kompetenzzentrums beaufsichtigen und dafür sorgen, dass diese Tätigkeiten aufeinander abgestimmt sind. Das Kompetenzzentrum sollte in seinem jährlichen Bericht einen besonderen Schwerpunkt auf die strategischen Ziele legen, die es verwirklicht hat, und erforderlichenfalls Maßnahmen vorschlagen, um die Verwirklichung dieser strategischen Ziele weiter zu verbessern.

(48) Damit das Kompetenzzentrum seine 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 den 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.

(49) Angesichts des besonderen Status und der Zuständigkeit des Kompetenzzentrums für die Ausführung der Unionsmittel, insbesondere der Mittel aus „Horizont Europa“ und dem Programm „Digitales Europa“, sollte die Kommission im Verwaltungsrat bei Beschlüssen im Zusammenhang mit Unionsmitteln über 26 % aller Stimmen verfügen, um den Unionsmehrwert dieser Beschlüsse zu maximieren und gleichzeitig die Rechtmäßigkeit dieser Beschlüsse und deren Übereinstimmung mit den Prioritäten der Union zu gewährleisten.

(50) Damit das Kompetenzzentrum reibungslos funktioniert, ist es erforderlich, dass sein Exekutivdirektor in transparenter Weise aufgrund seiner Verdienste, seiner nachgewiesenen Verwaltungs- und Managementfähigkeiten und seiner einschlägigen Sachkenntnis und Erfahrungen auf dem Gebiet der Cybersicherheit ernannt wird und seine Aufgaben völlig unabhängig wahrnimmt.

(51) Das Kompetenzzentrum sollte über eine strategische Beratungsgruppe als Beratungsgremium verfügen. Die strategische Beratungsgruppe sollte auf der Grundlage eines regelmäßigen Dialogs zwischen dem Kompetenzzentrum und der Gemeinschaft, die aus Vertretern von Privatsektor, Verbraucherorganisationen, Wissenschaft und sonstigen Interessenträgern bestehen sollte, Empfehlungen abgeben. Die strategische Beratungsgruppe sollte sich auf für die Interessenträger relevante Fragen konzentrieren und sie dem Verwaltungsrat und dem Exekutivdirektor zur Kenntnis bringen. Die Aufgaben der strategischen Beratungsgruppe sollten Empfehlungen zur Agenda, zum jährlichen Arbeitsprogramm und zum mehrjährigen Arbeitsprogramm einschließen. Die Vertretung der verschiedenen Interessenträger in der strategischen Beratungsgruppe sollte ausgewogen sein, unter besonderer Berücksichtigung von Vertretern von KMU, damit eine angemessene Vertretung der Interessenträger in der Arbeit des Kompetenzzentrums gewährleistet ist.

(52) Bei den Beiträgen der Mitgliedstaaten zu den Ressourcen des Kompetenzzentrums könnte es sich um Finanzbeiträge oder Beiträge in Form von Sachleistungen handeln. Finanzbeiträge könnten beispielsweise aus einer Finanzhilfe bestehen, die ein Mitgliedstaat einem Begünstigten in diesem Mitgliedstaat gewährt und die die finanzielle Unterstützung der Union für ein Projekt im Rahmen des jährlichen Arbeitsprogramms ergänzt. Allerdings würden Beiträge in Form von Sachleistungen typischerweise geleistet werden, wenn eine Einrichtung eines Mitgliedstaats selbst Begünstigte einer finanziellen Unterstützung durch die Union ist. Wenn zum Beispiel die Union die Tätigkeit eines nationalen Koordinierungszentrums zu 50 % subventioniert, würden die verbleibenden Kosten der Tätigkeit als Beitrag in Form von Sachleistungen verbucht. Ein anderes Beispiel wäre wie folgt: Wenn eine Einrichtung eines Mitgliedstaats finanzielle Unterstützung der Union für die Schaffung oder die Aufrüstung einer Infrastruktur erhält, die im Einklang mit dem jährlichen Arbeitsprogramm von den Interessenträgern gemeinsam genutzt werden soll, würden die damit verbundenen nicht subventionierten Kosten als Beiträge in Form von Sachleistungen verbucht.

(53) Gemäß den einschlägigen Bestimmungen der Delegierten Verordnung (EU) 2019/715 über Interessenkonflikte sollte das Kompetenzzentrum Vorschriften zur Vermeidung, Ermittlung und Beseitigung sowie zur Handhabung von Interessenkonflikten bezüglich seiner Mitglieder, Gremien und Mitarbeiter, des Verwaltungsrates sowie der strategischen Beratungsgruppe und der Gemeinschaft haben. Die Mitgliedstaaten sollten dafür Sorge tragen, dass Interessenkonflikte mit Blick auf die nationalen Koordinierungszentren im Einklang mit dem nationalen Recht vermieden, ermittelt und beseitigt werden. Das Kompetenzzentrum sollte das einschlägige Unionsrecht in Bezug auf den Zugang der Öffentlichkeit zu Dokumenten gemäß der Verordnung (EG) Nr. 1049/2001 des Europäischen Parlaments und des Rates ([9]) anwenden. Die Verarbeitung personenbezogener Daten durch das Kompetenzzentrum sollte der Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates ([10]) unterliegen. Das Kompetenzzentrum sollte die für die Unionsorgane geltenden Bestimmungen des Unionsrechts über den Umgang mit Informationen, insbesondere den Umgang mit sensiblen Informationen und Verschlusssachen der EU, sowie die entsprechenden nationalen Rechtsvorschriften befolgen.

(54) Die finanziellen Interessen der Union und der Mitgliedstaaten sollten während des gesamten Ausgabenzyklus durch angemessene Maßnahmen geschützt werden; dazu gehören unter anderem Maßnahmen zur Prävention, Aufdeckung und Untersuchung von Unregelmäßigkeiten, die Rückforderung entgangener, zu Unrecht gezahlter oder nicht widmungsgemäß verwendeter Mittel und gegebenenfalls verwaltungsrechtliche und finanzielle Sanktionen gemäß der Verordnung (EU, Euratom) 2018/1046 des Europäischen Parlaments und des Rates ([11]) (im Folgenden „Haushaltsordnung“).

(55) Das Kompetenzzentrum sollte seine Geschäftstätigkeit in offener und transparenter Weise ausüben. Es sollte alle relevanten Informationen fristgerecht übermitteln und seine Tätigkeiten bekannt machen, unter anderem auch durch an die Öffentlichkeit gerichtete Informations- und Verbreitungsmaßnahmen. Die Geschäftsordnungen des Verwaltungsrats des Kompetenzzentrums und der strategischen Beratungsgruppe sollten öffentlich zugänglich gemacht werden.

([9]) 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).

([10]) Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates vom 23. Oktober 2018 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen und sonstigen Stellen der Union, zum freien Datenverkehr und zur Aufhebung der Verordnung (EG) Nr. 45/2001 und des Beschlusses Nr. 1247/2002/EG (ABl. L 295 vom 21.11.2018, S. 39).

([11]) Verordnung (EU, Euratom) 2018/1046 des Europäischen Parlaments und des Rates vom 18. Juli 2018 über die Haushaltsordnung für den Gesamthaushaltsplan der Union, zur Änderung der Verordnungen (EU) Nr. 1296/2013, (EU) Nr. 1301/2013, (EU) Nr. 1303/2013, (EU) Nr. 1304/2013, (EU) Nr. 1309/2013, (EU) Nr. 1316/2013, (EU) Nr. 223/2014, (EU) Nr. 283/2014 und des Beschlusses Nr. 541/2014/EU sowie zur Aufhebung der Verordnung (EU, Euratom) Nr. 966/2012 (ABl. L 193 vom 30.7.2018, S. 1).

(56) Der Interne Prüfer der Kommission sollte gegenüber dem Kompetenzzentrum die gleichen Befugnisse ausüben wie gegenüber der Kommission.

(57) Die Kommission, der Rechnungshof und das Europäische Amt für Betrugsbekämpfung sollten Zugang zu allen Informationen und Räumlichkeiten des Kompetenzzentrums erhalten, die für die Durchführung von Rechnungsprüfungen und Untersuchungen in Bezug auf die vom Kompetenzzentrum unterzeichneten Finanzhilfen, Aufträge und Vereinbarungen erforderlich sind.

(58) Da die Ziele dieser Verordnung — nämlich die Stärkung der Wettbewerbsfähigkeit und der Kapazitäten der Union, die Wahrung und Weiterentwicklung der technischen und industriellen Kapazitäten der Union im Bereich der Cybersicherheitsforschung, die Steigerung der Wettbewerbsfähigkeit der Cybersicherheitsbranche der Union und die Verwandlung der Cybersicherheit in einen Wettbewerbsvorteil für andere Branchen der Union — von den Mitgliedstaaten allein nicht ausreichend verwirklicht werden können, da die vorhandenen begrenzten Ressourcen weit verstreut und umfangreiche Investitionen erforderlich sind, sondern vielmehr besser auf Unionsebene zu verwirklichen sind, da es darum geht, unnötige Doppelarbeit bei diesen Anstrengungen zu vermeiden, die kritische Investitionsmasse zu erreichen und sicherzustellen, dass die öffentlichen Mittel optimal genutzt werden und ein hohes Maß an Cybersicherheit in allen Mitgliedstaaten gefördert wird, kann die Union im Einklang mit dem in Artikel 5 des Vertrags über die Europäische Union (EUV) 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:

KAPITEL I

Allgemeine Bestimmungen und Grundsätze des Kompetenzzentrums und des Netzwerks

Artikel 1

Gegenstand und Anwendungsbereich

(1) Mit dieser Verordnung werden das Europäische Kompetenzzentrum für Industrie, Technologie und Forschung im Bereich der Cybersicherheit (im Folgenden „Kompetenzzentrum“) sowie das Netzwerk nationaler Koordinierungszentren (im Folgenden „Netzwerk“) eingerichtet. Diese Verordnung legt Bestimmungen für die Benennung nationaler Koordinierungszentren sowie Bestimmungen für die Einrichtung der Kompetenzgemeinschaft für Cybersicherheit (im Folgenden „Gemeinschaft“) fest.

(2) Das Kompetenzzentrum nimmt eine tragende Rolle bei der Umsetzung der Cybersicherheitskomponente des Programms „Digitales Europa“, insbesondere im Hinblick auf Maßnahmen im Zusammenhang mit Artikel 6 der Verordnung (EU) 2021/694, ein und trägt zur Umsetzung von „Horizont Europa“, insbesondere in Bezug auf Anhang I Pfeiler II Abschnitt 3.1.3 des Beschlusses (EU) 2021/764 des Rates ([12]) bei.

(3) Die Mitgliedstaaten tragen gemeinsam zur Arbeit des Kompetenzzentrums und des Netzwerks bei.

(4) Von dieser Verordnung unberührt bleiben die Zuständigkeiten der Mitgliedstaaten in Bezug auf die öffentliche Sicherheit, die Verteidigung, die nationale Sicherheit und das staatliche Handeln im strafrechtlichen Bereich.

Artikel 2

Begriffsbestimmungen

Für die Zwecke dieser Verordnung bezeichnet der Ausdruck

1. „Cybersicherheit“ alle Tätigkeiten, die notwendig sind, um Netz- und Informationssysteme, die Nutzer solcher Systeme und andere von Cyberbedrohungen betroffene Personen zu schützen;

2. „Netz- und Informationssystem“ ein Netz- und Informationssystem im Sinne des Artikels 4 Nummer 1 der Richtlinie (EU) 2016/1148;

3. „Cybersicherheitsprodukte, -dienste und -prozesse“ kommerzielle und nicht kommerzielle IKT-Produkte, -Dienste oder -Prozesse, die dem besonderen Zweck dienen, Netz- und Informationssysteme zu schützen oder die Vertraulichkeit, Integrität und Zugänglichkeit von Daten, die in Netz- und Informationssystemen verarbeitet oder gespeichert werden, sowie die Cybersicherheit der Nutzer solcher Systeme und anderer von Cyberbedrohungen betroffener Personen zu gewährleisten;

4. „Cyberbedrohung“ einen möglichen Umstand, ein mögliches Ereignis oder eine mögliche Handlung, der/das/die Netz- und Informationssysteme, die Nutzer dieser Systeme und andere Personen schädigen, stören oder anderweitig beeinträchtigen könnte;

([12]) Beschluss (EU) 2021/764 des Rates vom 10. Mai 2021 zur Einrichtung des spezifischen Programms zur Durchführung von „Horizont Europa“, dem Rahmenprogramm für Forschung und Innovation, und zur Aufhebung des Beschlusses 2013/743/EU (ABl. L 167 I vom 12.5.2021, S. 1).

5. „gemeinsame Maßnahme“ eine im jährlichen Arbeitsprogramm enthaltene Maßnahme, die finanzielle Unterstützung von „Horizont Europa“, dem Programm „Digitales Europa“ oder anderen Programmen der Union sowie finanzielle Unterstützung oder Unterstützung in Form von Sachleistungen von einem oder mehreren Mitgliedstaaten erhält und die im Wege von Projekten durchgeführt wird, an denen Begünstigte beteiligt sind, die in den Mitgliedstaaten niedergelassen sind und die finanzielle Unterstützung oder Unterstützung in Form von Sachleistungen von diesen Mitgliedstaaten erhalten;

6. „Beitrag in Form von Sachleistungen“ den nationalen Koordinierungszentren und anderen öffentlichen Einrichtungen bei der Beteiligung an im Rahmen dieser Verordnung finanzierten Projekten entstehende förderfähige Kosten, die nicht durch einen Beitrag der Union oder durch Finanzbeiträge der Mitgliedstaaten finanziert werden;

7. „Europäisches Digitales Innovationszentrum“ ein Europäisches Digitales Innovationszentrum im Sinne des Artikels 2 Buchstabe e der Verordnung (EU) 2021/694;

8. „Agenda“ eine umfassende und nachhaltige Strategie für Industrie, Technologie und Forschung im Bereich der Cybersicherheit, in der strategische Empfehlungen für die Entwicklung und das Wachstum des europäischen Sektors für Industrie, Technologie und Forschung im Bereich der Cybersicherheit sowie strategische Prioritäten für die Tätigkeiten des Kompetenzzentrums dargelegt sind und die hinsichtlich der Beschlüsse über die jährlichen Arbeitsprogramme nicht verbindlich ist;

9. „technische Hilfe“ die Unterstützung durch das Kompetenzzentrum für die nationalen Koordinierungszentren oder für die Gemeinschaft bei der Wahrnehmung ihrer Aufgaben durch Bereitstellung von Wissen oder Erleichterung des Zugangs zu Fachwissen in Bezug auf Industrie, Technologie und Forschung im Bereich der Cybersicherheit, Ermöglichung der Vernetzung, Sensibilisierung und Förderung der Zusammenarbeit, oder die Unterstützung durch das Kompetenzzentrum gemeinsam mit den nationalen Koordinierungszentren für die Interessenträger in Bezug auf die Vorbereitung von Projekten im Zusammenhang mit dem Auftrag des Kompetenzzentrums und des Netzwerks sowie den Zielen des Kompetenzzentrums.

Artikel 3

Auftrag des Kompetenzzentrums und des Netzwerks

(1) Der Auftrag des Kompetenzzentrums und des Netzwerks ist es, die Union zu unterstützen bei

a) der Stärkung ihrer Führungsrolle und strategischen Autonomie im Bereich der Cybersicherheit durch die Wahrung und Weiterentwicklung der forschungsbezogenen, wissenschaftlichen, gesellschaftsbezogenen, technologischen und industriellen Kapazitäten und Fähigkeiten der Union im Bereich der Cybersicherheit, die nötig sind, um das Vertrauen und die Sicherheit, einschließlich der Vertraulichkeit, Integrität und Zugänglichkeit von Daten, in den digitalen Binnenmarkt und auf diesem Markt zu steigern;

b) der Förderung der technologischen Kapazitäten, Fähigkeiten und Kompetenzen in der Union im Zusammenhang mit der Abwehrfähigkeit und Zuverlässigkeit der Infrastruktur der Netz- und Informationssysteme, darunter der kritischen Infrastruktur und der in der Union gängigen Hard- und Software; und

c) der Steigerung der globalen Wettbewerbsfähigkeit der Cybersicherheitsbranche der Union, der Gewährleistung hoher Cybersicherheitsstandards in der gesamten Union und der Verwandlung der Cybersicherheit in einen Wettbewerbsvorteil für andere Wirtschaftszweige der Union.

(2) Das Kompetenzzentrum und das Netzwerk nehmen ihre Aufgaben in Zusammenarbeit mit der ENISA und der Gemeinschaft, je nachdem, was angemessen ist, wahr.

(3) Das Kompetenzzentrum verwendet, im Einklang mit den Gesetzgebungsakten zur Einrichtung der betreffenden Programme, insbesondere „Horizont Europa“ und dem Programm „Digitales Europa“, die einschlägigen Finanzmittel der Union in einer Weise, dass ein Beitrag zu dem in Absatz 1 dargelegten Auftrag geleistet wird.

Artikel 4

Ziele des Kompetenzzentrums

(1) Das Kompetenzzentrum hat das allgemeine Ziel, die Forschung, Innovation und Realisierung im Bereich der Cybersicherheit zu fördern, um den in Artikel 3 festgelegten Auftrag zu erfüllen.

(2) Das Kompetenzzentrum hat folgende spezifische Ziele:

a) die Kapazitäten, die Fähigkeiten, das Wissen und die Infrastruktur im Bereich der Cybersicherheit zugunsten der Wirtschaft, insbesondere von KMU, der Forschungsgemeinschaften, des öffentlichen Sektors und der Zivilgesellschaft, zu verbessern, sofern angemessen,

b) die Abwehrfähigkeit im Bereich der Cybersicherheit, die Übernahme bewährter Verfahren im Bereich der Cybersicherheit, den Grundsatz der konzeptionsintegrierten Sicherheit und die Zertifizierung der Sicherheit digitaler Produkte und Dienste auf eine Art zu fördern, die die Maßnahmen anderer öffentlicher Einrichtungen ergänzt,

c) zu einem starken europäischen Cybersicherheitsökosystem, in dem alle einschlägigen Interessenträger zusammengeführt werden, beizutragen.

(3) Das Kompetenzzentrum verwirklicht die in Absatz 2 genannten spezifischen Ziele, indem es:

a) strategische Empfehlungen für Forschung, Innovation und Realisierung im Bereich der Cybersicherheit im Einklang mit dem Unionsrecht ausarbeitet und strategische Prioritäten für die Tätigkeiten des Kompetenzzentrums festlegt;

b) Maßnahmen im Rahmen der einschlägigen Finanzierungsprogramme der Union im Einklang mit den einschlägigen Arbeitsprogrammen und der Gesetzgebungsakte der Union zur Einrichtung dieser Finanzierungsprogramme durchführt;

c) die Zusammenarbeit und die Abstimmung zwischen den nationalen Koordinierungszentren sowie mit und innerhalb der Gemeinschaft fördert und

d) soweit dies sachdienlich und angemessen ist, IKT-Infrastrukturen und -Dienste entsprechend den in Artikel 5 Absatz 3 Buchstabe b aufgeführten jeweiligen Arbeitsprogrammen zu erwerben, wenn dies zur Erfüllung der in Artikel 5 genannten Aufgaben erforderlich ist.

Artikel 5

Aufgaben des Kompetenzzentrums

(1) Zur Erfüllung seines Auftrags und seiner Ziele übernimmt das Kompetenzzentrum folgende Aufgaben:

a) strategische Aufgaben und

b) Umsetzungsaufgaben.

(2) Die in Absatz 1 Buchstabe a genannten strategischen Aufgaben bestehen aus:

a) der Erarbeitung der Agenda und der Überwachung ihrer Umsetzung;

b) über die Agenda und das mehrjährige Arbeitsprogramm, unter Vermeidung von Überschneidungen mit den Tätigkeiten der ENISA und unter Berücksichtigung der Notwendigkeit von Synergien zwischen Cybersicherheit und anderen Teilen von „Horizont Europa“ und des Programms „Digitales Europa“:

   i) die Festlegung von Prioritäten für die Arbeit des Kompetenzzentrums in folgenden Bereichen:

      1. auf den gesamten Innovationszyklus ausgerichtete Ausweitung der Forschung und Innovation im Bereich der Cybersicherheit und die Realisierung dieser Forschung und Innovation;

      2. Entwicklung von Kapazitäten, Fähigkeiten und Infrastrukturen für Industrie, Technologie und Forschung im Bereich der Cybersicherheit;

      3. Verbesserung von Cybersicherheits- und Technologiekenntnissen und -kompetenzen in Industrie, Technologie und Forschung und auf allen relevanten Bildungsebenen bei gleichzeitiger Förderung eines ausgewogenen Geschlechterverhältnisses;

      4. Realisierung von Cybersicherheitsprodukten, -diensten und -verfahren;

      5. Unterstützung der Aufnahme von Cybersicherheitsprodukten, -diensten und -verfahren, die zur Erfüllung der Aufgaben gemäß Artikel 3 beitragen, am Markt;

      6. Unterstützung der Einführung und Integration modernster Cybersicherheitsprodukte, -dienste und -verfahren durch Behörden auf deren Ersuchen, durch nachfragende Branchen und durch andere Nutzer;

   ii) die Unterstützung der Cybersicherheitsbranche, insbesondere von KMU, um die Exzellenz, Kapazität und Wettbewerbsfähigkeit der Union im Hinblick auf Cybersicherheit zu stärken, auch durch Erschließung potenzieller Märkte und Realisierungsmöglichkeiten, und um Investoren zu gewinnen; und

   iii) Unterstützung und technische Hilfe für im Bereich der Cybersicherheit tätige Start-up-Unternehmen, KMU, Kleinstunternehmen, Verbände, Sachverständige und Civic-Technologie-Projekte;

c) die Gewährleistung von Synergien zwischen und Zusammenarbeit mit einschlägigen Organen, Einrichtungen und sonstigen Stellen der Union, insbesondere der ENISA, unter Vermeidung jeglicher Doppelarbeit in Bezug auf die Tätigkeiten dieser Organe, Einrichtungen und sonstigen Stellen der Union;

d) die Koordinierung der nationalen Koordinierungszentren durch das Netzwerk und die Gewährleistung eines regelmäßigen Austauschs von Fachwissen;

e) die fachkundige Beratung von Mitgliedstaaten, auf deren Ersuchen, zu Industrie, Technologie und Forschung im Bereich der Cybersicherheit, einschließlich der Vergabe öffentlicher Aufträge und der Realisierung von Technologien;

f) die Förderung der Zusammenarbeit und des Austauschs von Fachwissen zwischen allen einschlägigen Interessenträgern, insbesondere den Mitgliedern der Gemeinschaft;

g) die Teilnahme an Unions-, nationalen und internationalen Konferenzen, Messen und Foren, die einen Bezug zu dem Auftrag, den Zielen und den Aufgaben des Kompetenzzentrums haben, um Ansichten und einschlägige bewährte Verfahren mit anderen Teilnehmern auszutauschen;

h) die Ermöglichung der Nutzung der Ergebnisse von Forschungs- und Innovationsprojekten bei Maßnahmen im Zusammenhang mit der Entwicklung von Cybersicherheitsprodukten, -diensten und -verfahren, wobei angestrebt wird, Fragmentierung und Doppelarbeit zu vermeiden und bewährte Verfahren in Bezug auf Cybersicherheitsprodukte, -dienste und -verfahren nachzubilden, insbesondere solche, die von KMU entwickelt wurden, und solche, die auf quelloffener Software beruhen;

(3) Die Umsetzungsaufgaben gemäß Absatz 1 Buchstabe b bestehen aus:

a) der Koordinierung und Verwaltung der Arbeit des Netzwerks und der Gemeinschaft zur Erfüllung des in Artikel 3 festgelegten Auftrags, insbesondere durch Unterstützung von im Bereich der Cybersicherheit tätigen Start-up-Unternehmen, KMU, Kleinstunternehmen, Verbänden und Civic-Technology-Projekten in der Union und der Erleichterung ihres Zugangs zu Fachwissen, Finanzierung, Investitionen und Märkten;

b) der Aufstellung und Durchführung des jährlichen Arbeitsprogramms im Einklang mit der Agenda und dem mehrjährigen Arbeitsprogramm in Bezug auf die die Cybersicherheit betreffenden Teile:

   i) des Programms „Digitales Europa“, insbesondere den Maßnahmen im Zusammenhang mit Artikel 6 der Verordnung (EU) 2021/694,

   ii) gemeinsamer Maßnahmen, die gemäß den die Cybersicherheit betreffenden Bestimmungen von „Horizont Europa“, insbesondere in Bezug auf Anhang I Pfeiler II Abschnitt 3.1.3 des Beschlusses (EU) 2021/764 Unterstützung erhalten, im Einklang mit dem mehrjährigen Arbeitsprogramm und dem strategischen Planungsprozess im Rahmen von „Horizont Europa“, und

   iii) anderer Programme, wenn diese in Gesetzgebungsakten der Union vorgesehen sind;

c) gegebenenfalls Unterstützung der Verwirklichung des spezifischen Ziels 4 „fortgeschrittene digitale Kompetenzen“ gemäß Artikel 7 der Verordnung (EU) 2021/694 in Zusammenarbeit mit den Europäischen Digitalen Innovationszentren;

d) fachkundiger Beratung der Kommission zu Industrie, Technologie und Forschung im Bereich der Cybersicherheit, wenn die Kommission die Entwürfe der Arbeitsprogramme gemäß Artikel 13 des Beschlusses (EU) 2021/764 erstellt;

e) der Durchführung oder Ermöglichung der Realisierung von IKT-Infrastrukturen sowie der Erleichterung der Beschaffung einer solchen Infrastruktur im Dienst der Gesellschaft, der Wirtschaft und des öffentlichen Sektors auf Ersuchen der Mitgliedstaaten, der Forschungsgemeinschaften und der Betreiber wesentlicher Dienste unter anderem durch Beiträge der Mitgliedstaaten und Finanzierungsmittel der Union für gemeinsame Maßnahmen im Einklang mit der Agenda, dem jährlichen Arbeitsprogramm und dem mehrjährigen Arbeitsprogramm.;

f) der Aufklärung über den Auftrag des Kompetenzzentrums und des Netzwerks sowie über die Ziele und Aufgaben des Kompetenzzentrums;

g) unbeschadet des zivilen Charakters der über „Horizont Europa“ zu finanzierenden Projekte und im Einklang mit den Verordnungen (EU) 2021/695 und (EU) 2021/694 die Verstärkung der Synergien und der Koordinierung zwischen dem zivilen und dem Verteidigungssektor im Bereich der Cybersicherheit, durch die Förderung des Austauschs von:

   i) Wissen und Informationen über Technologien und Anwendungen mit doppeltem Verwendungszweck,

   ii) Ergebnissen, Anforderungen und bewährten Verfahren, und

   iii) Informationen über die Prioritäten der einschlägigen Programme der Union.

(4) Das Kompetenzzentrum führt die in Absatz 1 genannten Aufgaben in enger Zusammenarbeit mit dem Netzwerk aus.

(5) Gemäß Artikel 6 der Verordnung (EU) 2021/695 und vorbehaltlich einer Beitragsvereinbarung gemäß Artikel 2 Nummer 18 der Haushaltsordnung kann das Kompetenzzentrum mit der Durchführung der die Cybersicherheit betreffenden Teile im Rahmen von „Horizont Europa", die nicht durch die Mitgliedstaaten kofinanzierten werden, insbesondere des Anhangs I Pfeiler II Abschnitt 3.1.3 des Beschlusses (EU) 2021/764, betraut werden.

Artikel 6

Benennung der nationalen Koordinierungszentren

(1) Bis zum 29. Dezember 2021 benennt jeder Mitgliedstaat eine Einrichtung, die die in Absatz 5 festgelegten Kriterien erfüllt, die als nationales Koordinierungszentrum für die Zwecke dieser Verordnung dienen soll. Jeder Mitgliedstaat notifiziert dem Verwaltungsrat diese Einrichtung unverzüglich. Bei dieser Einrichtung kann es sich um eine in dem jeweiligen Mitgliedstaat bereits bestehende Einrichtung handeln.

Die in Unterabsatz 1 dieses Absatzes genannte Frist wird um den Zeitraum verlängert, in dem die Kommission die in Absatz 2 genannte Stellungnahme abzugeben hat.

(2) Ein Mitgliedstaat kann die Kommission jederzeit um eine Stellungnahme dazu ersuchen, ob die Einrichtung, die er als nationales Koordinierungszentrum benannt hat oder zu benennen beabsichtigt, über die notwendigen Kapazitäten zur Mittelverwaltung verfügt, um den Auftrag und die Ziele gemäß dieser Verordnung erfüllen zu können. Die Kommission gibt dem betreffenden Mitgliedstaat ihre Stellungnahme innerhalb von drei Monaten nach dem Ersuchen des Mitgliedstaats ab.

(3) Auf der Grundlage der Notifizierung einer Einrichtung durch einen Mitgliedstaat gemäß Absatz 1 nimmt der Verwaltungsrat diese Einrichtung spätestens drei Monate nach der Notifizierung in die Liste der nationalen Koordinierungszentren auf. Das Kompetenzzentrum veröffentlicht die Liste der ernannten nationalen Koordinierungszentren.

(4) Ein Mitgliedstaat kann jederzeit eine neue Einrichtung als nationales Koordinierungszentrum für die Zwecke dieser Verordnung benennen. Die Absätze 1, 2 und 3 gelten für die Benennung jeder neuen Einrichtung.

(5) Das nationale Koordinierungszentrum muss eine öffentliche Einrichtung oder eine Einrichtung mit mehrheitlicher Beteiligung des Mitgliedstaats sein, die nach nationalem Recht, einschließlich durch Befugnisübertragung, Aufgaben der öffentlichen Verwaltung wahrnimmt und die Kapazität hat, das Kompetenzzentrum und das Netzwerk bei der Erfüllung ihres Auftrags gemäß Artikel 3 dieser Verordnung zu unterstützen. Es muss entweder über Fachwissen in Forschung und Technologie auf dem Gebiet der Cybersicherheit verfügen oder direkten Zugang dazu haben. Es muss die Kapazität haben, sich wirksam mit der Industrie, dem öffentlichen Sektor, Wissenschaft und Forschung, den Bürgern sowie den nach der Richtlinie (EU) 2016/1148 benannten Behörden auszutauschen und abzustimmen.

(6) Ein nationales Koordinierungszentrum können jederzeit seine Anerkennung als eine Einrichtung beantragen, die über die notwendigen Kapazitäten zur Mittelverwaltung verfügt, um den Auftrag und die Ziele gemäß dieser Verordnung im Einklang mit den Verordnungen (EU) 2021/695 und (EU) 2021/694 zu erfüllen. Innerhalb von drei Monaten nach einem solchen Antrags bewertet die Kommission, ob das betreffende nationale Koordinierungszentrum über diese Kapazitäten verfügt, und trifft eine Entscheidung.

Hat die Kommission einem Mitgliedstaat nach dem Verfahren des Absatzes 2 eine befürwortende Stellungnahme übermittelt, so gilt diese Stellungnahme als Entscheidung, mit der anerkannt wird, dass die betreffende Einrichtung über die notwendigen Kapazitäten für die Zwecke des vorliegenden Absatzes verfügt.

Spätestens bis zum 29. August 2021 gibt die Kommission nach Anhörung des Verwaltungsrats Leitlinien in Bezug auf die Bewertung nach Unterabsatz 1 heraus, einschließlich einer Präzisierung der Bedingungen für die Anerkennung und der Modalitäten für die Durchführung von Stellungnahmen und Bewertungen.

Vor Abgabe der Stellungnahme gemäß Absatz 2 und der Entscheidung gemäß Unterabsatz 1 des vorliegenden Absatzes berücksichtigt die Kommission etwaige von dem antragstellenden nationalen Koordinierungszentrum bereitgestellten Informationen und Unterlagen.

Jede Entscheidung, ein nationales Koordinierungszentrum nicht anzuerkennen, weil es nicht über die notwendigen Kapazitäten zur Mittelverwaltung verfügt, um den Auftrag und die Ziele gemäß dieser Verordnung zu erfüllen, muss hinreichend begründet werden, wobei die Anforderungen anzugeben sind, die das antragstellende nationale Koordinierungszentrum noch nicht erfüllt hat, welche die Entscheidung, die Anerkennung abzulehnen, rechtfertigen. Jedes nationale Koordinierungszentrum, dessen Antrag zur Anerkennung abgelehnt wurde, kann seinen Antrag mit zusätzlichen Informationen jederzeit erneut einreichen.

Die Mitgliedstaaten unterrichten die Kommission über Änderungen bei den nationalen Koordinierungszentren, wie beispielsweise der Zusammensetzung des nationalen Koordinierungszentrums, der Rechtsform des nationalen Koordinierungszentrums oder anderen relevanten Aspekten, die sich auf ihre Kapazitäten zur Verwaltung von Mitteln zur Erfüllung des Auftrags und der Ziele gemäß dieser Verordnung auswirken. Erhält die Kommission solche Informationen, kann sie die Entscheidung über die Anerkennung oder Ablehnung der Anerkennung der Tatsache, dass ein nationales Koordinierungszentrum über die notwendigen Kapazitäten zur Mittelverwaltung verfügt, entsprechend überprüfen.

(7) Dem Netzwerk gehören alle nationalen Koordinierungszentren an, die dem Verwaltungsrat von den Mitgliedstaaten notifiziert wurden.

Artikel 7

Aufgaben der nationalen Koordinierungszentren

(1) Die nationalen Koordinierungszentren haben folgende Aufgaben:

a) sie dienen als auf nationaler Ebene angesiedelte Anlaufstellen für die Gemeinschaft zur Unterstützung des Kompetenzzentrums bei der Erfüllung seines Auftrags und seiner Ziele, insbesondere bei der Koordinierung der Gemeinschaft durch Koordinierung der Mitglieder der Gemeinschaft in ihren Mitgliedstaaten;

b) sie stellen Fachwissen für die strategischen Aufgaben gemäß Artikel 5 Absatz 2 bereit und unterstützen aktiv bei diesen Aufgaben, unter Berücksichtigung der einschlägigen nationalen und regionalen Herausforderungen für die Cybersicherheit in verschiedenen Sektoren;

c) sie fördern und erleichtern die Beteiligung der Zivilgesellschaft, der Industrie, insbesondere von Start-up-Unternehmen und KMU, von Wissenschaft und Forschung und anderer Interessenträger auf der nationalen Ebene an grenzübergreifenden Projekten und Cybersicherheitsmaßnahmen, die im Rahmen der einschlägigen Programme der Union finanziert werden, und ermutigen diese zur Teilnahme;

d) sie stellen technische Hilfe für Interessenträger bereit, indem sie diese in der Antragsphase bei Projekten, die das Kompetenzzentrum im Rahmen seines Auftrags und seiner Ziele verwaltet, unterstützen, wobei die Regeln der wirtschaftlichen Haushaltsführung, insbesondere in Bezug auf Interessenkonflikte, uneingeschränkt einzuhalten sind;

e) sie bemühen sich um die Schaffung von Synergien mit einschlägigen Tätigkeiten auf nationaler, regionaler und lokaler Ebene, wie etwa der nationalen Forschungs-, Entwicklungs- und Innovationspolitik im Bereich der Cybersicherheit, insbesondere der Politikbereiche, die in den nationalen Cybersicherheitsstrategien aufgeführt sind;

f) sie führen spezifische Maßnahmen durch, für die das Kompetenzzentrum Finanzhilfen gewährt hat, unter anderem durch die finanzielle Unterstützung Dritter gemäß Artikel 204 der Haushaltsordnung unter den in den betreffenden Finanzhilfevereinbarungen festgelegten Bedingungen;

g) sie arbeiten mit den Behörden der Mitgliedstaaten im Hinblick auf einen möglichen Beitrag zur Förderung und Verbreitung von Schulungsprogrammen im Bereich Cybersicherheit zusammen, unbeschadet der Zuständigkeiten der Mitgliedstaaten für Bildung und unter Berücksichtigung der einschlägigen Aufgaben der ENISA;

h) sie fördern und verbreiten die einschlägigen Ergebnisse der Arbeit des Netzwerks, der Gemeinschaft und des Kompetenzzentrums auf nationaler, regionaler oder lokaler Ebene;

i) sie prüfen die Anträge von Einrichtungen, die in demselben Mitgliedstaat wie das nationale Koordinierungszentrum niedergelassen sind, auf Aufnahme in die Gemeinschaft;

j) sie unterstützen und fördern die Beteiligung einschlägiger Einrichtungen an den Tätigkeiten des Kompetenzzentrums, des Netzwerks und der Gemeinschaft und überwachen gegebenenfalls den Umfang der Beteiligung an der Forschung, Entwicklung und Realisierung im Bereich der Cybersicherheit und der Höhe der in diesem Zusammenhang gewährten öffentlichen Finanzhilfen.

(2) Für die Zwecke von Absatz 1 Buchstabe f des vorliegenden Artikels kann die finanzielle Unterstützung Dritter in jeder in Artikel 125 der Haushaltsordnung genannten Form des Beitrags der Union, auch in Form von Pauschalbeträgen, gewährt werden.

(3) Die nationalen Koordinierungszentren können auf der Grundlage der Entscheidung gemäß Artikel 6 Absatz 6 der vorliegenden Verordnung im Einklang mit Artikel 195 Absatz 1 Buchstabe d der Haushaltsordnung für die Wahrnehmung der im vorliegenden Artikel festgelegten Aufgaben eine Finanzhilfe der Union erhalten.

(4) Die nationalen Koordinierungszentren arbeiten gegebenenfalls über das Netzwerk zusammen.

Artikel 8

Die Kompetenzgemeinschaft für Cybersicherheit

(1) Die Gemeinschaft leistet einen Beitrag zu dem in Artikel 3 festgelegten Auftrag des Kompetenzzentrums und des Netzwerks und fördert, teilt und verbreitet Fachwissen auf dem Gebiet der Cybersicherheit in der gesamten Union.

(2) Die Gemeinschaft besteht aus Einrichtungen der Industrie, einschließlich KMU, Wissenschafts- und Forschungseinrichtungen, anderen einschlägigen Organisationen der Zivilgesellschaft sowie gegebenenfalls europäischen Normungsorganisationen und öffentlichen und anderen Einrichtungen, die sich mit operativen und technischen Fragen der Cybersicherheit befassen, und gegebenenfalls aus Interessenträgern aus Sektoren, die ein Interesse an Cybersicherheit haben und mit Herausforderungen in Bezug auf die Cybersicherheit konfrontiert sind. Die Gemeinschaft bringt die wichtigsten Interessenträger im Hinblick auf die technologischen, industriellen, forschungsbezogenen und wissenschaftlichen Kapazitäten im Bereich der Cybersicherheit in der Union zusammen. Sie bezieht die nationalen Koordinierungszentren, gegebenenfalls die Europäischen Digitalen Innovationszentren sowie die Organe, Einrichtungen und sonstigen Stellen der Union, die über einschlägiges Fachwissen verfügen, wie etwa die ENISA, in ihre Arbeit ein.

(3) Nur Einrichtungen, die in den Mitgliedstaaten niedergelassen sind, können als Mitglieder der Gemeinschaft registriert werden. Sie müssen nachweisen, dass sie einen Beitrag zum Auftrag leisten können, und müssen über Fachwissen auf dem Gebiet der Cybersicherheit in mindestens einem der folgenden Bereiche verfügen:

a) Wissenschaft, Forschung oder Innovation,

b) industrielle Entwicklung oder Produktentwicklung,

c) Schulung und Bildung,

d) Informationssicherheit oder Maßnahmen zur Reaktion auf Vorfälle,

e) Ethik,

f) formale und technische Normung und entsprechende Spezifikationen.

(4) Das Kompetenzzentrum registriert Einrichtungen auf deren Ersuchen als Mitglieder der Gemeinschaft, nachdem das nationale Koordinierungszentrum des Mitgliedstaats, in dem diese Einrichtungen niedergelassen sind, geprüft hat, ob diese Einrichtungen die Kriterien nach Absatz 3 des vorliegenden Artikels erfüllen. Bei dieser Prüfung werden auch alle einschlägigen nationalen Prüfungen berücksichtigt, die die nationalen zuständigen Behörden aus Sicherheitsgründen vorgenommen haben. Solche Registrierungen gelten unbefristet, können jedoch vom Kompetenzzentrum jederzeit widerrufen werden, wenn das einschlägige nationale Koordinierungszentrum der Auffassung ist, dass die betreffende Einrichtung die Kriterien nach Absatz 3 des vorliegenden Artikels nicht mehr erfüllt oder unter Artikel 136 der Haushaltsordnung fällt, oder wenn dies aus Gründen der Sicherheit gerechtfertigt ist. Wird die Mitgliedschaft in der Gemeinschaft aus Sicherheitsgründen widerrufen, so muss die Widerrufsentscheidung verhältnismäßig und begründet sein. Die nationalen Koordinierungszentren streben eine ausgewogene Vertretung der Interessenträger in der Gemeinschaft an und unterstützen aktiv die Beteiligung, insbesondere von KMU.

(5) Die nationalen Koordinierungszentren sind dazu angehalten, über das Netzwerk zusammenzuarbeiten, damit sie die Kriterien gemäß Absatz 3 und die Verfahren zur Prüfung und Registrierung von Einrichtungen gemäß Absatz 4 einheitlich anwenden.

(6) Das Kompetenzzentrum registriert einschlägige Organe, Einrichtungen und sonstige Stellen der Union als Mitglieder der Gemeinschaft, nachdem es geprüft hat, ob dieses Organ, diese Einrichtung oder sonstige Stelle der Union die Kriterien nach Absatz 3 des vorliegenden Artikels erfüllt. Solche Registrierungen gelten unbefristet, können jedoch vom Kompetenzzentrum jederzeit widerrufen werden, wenn es der Auffassung ist, dass das Organ, die Einrichtung oder sonstige Stelle der Union die Kriterien nach Absatz 3 des vorliegenden Artikels nicht mehr erfüllt oder unter Artikel 136 der Haushaltsordnung fällt.

(7) Die Vertreter der Organe, Einrichtungen und sonstigen Stellen der Union können sich an der Arbeit der Gemeinschaft beteiligen.

(8) Eine Einrichtung, die als Mitglied der Gemeinschaft registriert ist, benennt ihre Vertreter, damit ein effizienter Dialog sichergestellt ist. Diese Vertreter müssen über Fachwissen in Bezug auf Industrie, Technologie oder Forschung im Bereich der Cybersicherheit verfügen. Die Anforderungen können vom Verwaltungsrat weiter präzisiert werden, ohne den Einrichtungen bei der Benennung ihrer Vertreter übermäßige Beschränkungen aufzuerlegen.

(9) Die Gemeinschaft leistet im Einklang mit der Geschäftsordnung des Verwaltungsrats dem Exekutivdirektor und dem Verwaltungsrat durch ihre Arbeitsgruppen und insbesondere die strategische Beratungsgruppe strategische Beratung zu der Agenda, dem jährlichen Arbeitsprogramm und dem mehrjährigen Arbeitsprogramm.

Artikel 9

Aufgaben der Mitglieder der Gemeinschaft

Die Mitglieder der Gemeinschaft

a) unterstützen das Kompetenzzentrum bei der Erfüllung seines Auftrags und seiner Ziele und arbeiten hierzu eng mit dem Kompetenzzentrum und den nationalen Koordinierungszentren zusammen;

b) beteiligen sich gegebenenfalls an formellen oder informellen Tätigkeiten sowie an den in Artikel 13 Absatz 3 Buchstabe n genannten Arbeitsgruppen, um bestimmte, im jährlichen Arbeitsprogramm vorgesehene Tätigkeiten durchzuführen; und

c) unterstützen das Kompetenzzentrum und die nationalen Koordinierungszentren gegebenenfalls bei der Förderung bestimmter Projekte.

Artikel 10

Zusammenarbeit des Kompetenzzentrums mit anderen Organen, Einrichtungen und sonstigen Stellen der Union sowie mit internationalen Organisationen

(1) Um Kohärenz und Komplementarität sicherzustellen und gleichzeitig Doppelarbeit zu vermeiden, arbeitet das Kompetenzzentrum mit den einschlägigen Organen, Einrichtungen und sonstigen Stellen der Union zusammen, einschließlich der ENISA, des Europäischen Auswärtigen Dienstes, der Generaldirektion der Gemeinsamen Forschungsstelle der Kommission, der Europäischen Exekutivagentur für die Forschung, der Exekutivagentur des Europäischen Forschungsrats und der Europäischen Exekutivagentur für Gesundheit und Digitales, die mit dem Durchführungsbeschluss (EU) 2021/173 der Kommission ([13]) eingerichtet wurden, der einschlägigen Europäischen Digitalen Innovationszentren, des Europäischen Zentrums zur Bekämpfung der Cyberkriminalität bei der mit der Verordnung (EU) 2016/794 des Europäischen Parlaments und des Rates ([14]) eingerichteten Agentur der Europäischen Union für die Zusammenarbeit auf dem Gebiet der Strafverfolgung, der Europäischen Verteidigungsagentur im Zusammenhang mit den Aufgaben gemäß Artikel 5 der vorliegenden Verordnung und anderer einschlägiger Einrichtungen der Union. Das Kompetenzzentrum kann gegebenenfalls auch mit internationalen Organisationen zusammenarbeiten.

(2) Die Zusammenarbeit gemäß Absatz 1 des vorliegenden Artikels kann im Rahmen von Arbeitsvereinbarungen stattfinden. Diese Vereinbarungen werden dem Verwaltungsrat zur Genehmigung vorgelegt. Der Austausch von Verschlusssachen erfolgt im Rahmen von gemäß Artikel 36 Absatz 3 geschlossenen Verwaltungsvereinbarungen.

KAPITEL II

Organisation des Kompetenzzentrums

Artikel 11

Zusammensetzung und Struktur

(1) Die Mitglieder des Kompetenzzentrums sind die Union, vertreten durch die Kommission, und die Mitgliedstaaten.

(2) Die Struktur des Kompetenzzentrums muss die Erfüllung der Ziele nach Artikel 4 und der Aufgaben nach Artikel 5 gewährleisten und umfasst

a) einen Verwaltungsrat;

b) einen Exekutivdirektor;

c) eine strategische Beratungsgruppe.

([13]) Durchführungsbeschluss (EU) 2021/173 der Kommission vom 12. Februar 2021 zur Einrichtung der Europäischen Exekutivagentur für Klima, Infrastruktur und Umwelt, der Europäischen Exekutivagentur für Gesundheit und Digitales, der Europäischen Exekutivagentur für die Forschung, der Europäischen Exekutivagentur für den Innovationsrat und für KMU, der Exekutivagentur des Europäischen Forschungsrats sowie der Europäischen Exekutivagentur für Bildung und Kultur und zur Aufhebung der Durchführungsbeschlüsse 2013/801/EU, 2013/771/EU, 2013/778/EU, 2013/779/EU, 2013/776/EU und 2013/770/EU (ABl. L 50 vom 15.2.2021, S. 9).

([14]) Verordnung (EU) 2016/794 des Europäischen Parlaments und des Rates vom 11. Mai 2016 über die Agentur der Europäischen Union für die Zusammenarbeit auf dem Gebiet der Strafverfolgung (Europol) und zur Ersetzung und Aufhebung der Beschlüsse 2009/371/JI, 2009/934/JI, 2009/935/JI, 2009/936/JI und 2009/968/JI des Rates (ABl. L 135 vom 24.5.2016, S. 53).

Abschnitt I

Verwaltungsrat

Artikel 12

Zusammensetzung des Verwaltungsrats

(1) Der Verwaltungsrat besteht aus je einem Vertreter pro Mitgliedstaat und zwei Kommissionsvertretern, die im Namen der Union handeln.

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

(3) Die von den Mitgliedstaaten ernannten Mitglieder des Verwaltungsrats und deren Stellvertreter sind Bedienstete des öffentlichen Sektors ihres jeweiligen Mitgliedstaats und werden aufgrund ihrer Sachkenntnis auf dem Gebiet Forschung, Technologie und Industrie im Bereich Cybersicherheit, ihrer Fähigkeit, zur Gewährleistung der Koordinierung der Maßnahmen und Standpunkte mit ihrem jeweiligen nationalen Koordinierungszentrum oder ihrer einschlägigen Management-, Verwaltungs- und Haushaltsführungskompetenzen ernannt. Die Kommission ernennt ihre Mitglieder des Verwaltungsrats und deren Stellvertreter aufgrund ihrer Sachkenntnis auf dem Gebiet Cybersicherheit und Technologie oder ihrer einschlägigen Management-, Verwaltungs- und Haushaltsführungskompetenzen sowie ihrer Fähigkeit zur Gewährleistung von Koordinierung, Synergien und — soweit möglich — gemeinsamen Initiativen zwischen verschiedenen sektoralen und horizontalen Strategien der Union im Zusammenhang mit Cybersicherheit. 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.

(5) Die Mitglieder des Verwaltungsrats stellen in unabhängiger und transparenter Weise sicher, dass der Auftrag, die Ziele, die Identität und die Eigenständigkeit des Kompetenzzentrums gewahrt werden und dass dessen Maßnahmen mit jenem Auftrag und jenen Zielen übereinstimmen.

(6) Der Verwaltungsrat kann gegebenenfalls Beobachter einladen, die an den Sitzungen des Verwaltungsrats teilnehmen, darunter Vertreter der einschlägigen Organe, Einrichtungen und sonstigen Stellen der Union sowie die Mitglieder der Gemeinschaft.

(7) Ein Vertreter der ENISA ist ständiger Beobachter im Verwaltungsrat. Der Verwaltungsrat kann einen Vertreter der strategischen Beratungsgruppe einladen, an seinen Sitzungen teilzunehmen.

(8) Der Exekutivdirektor nimmt an den Sitzungen des Verwaltungsrats teil, hat jedoch kein Stimmrecht.

Artikel 13

Aufgaben des Verwaltungsrats

(1) Der Verwaltungsrat trägt die Gesamtverantwortung für die strategische Ausrichtung und die Geschäfte des Kompetenzzentrums, beaufsichtigt die Durchführung seiner Tätigkeiten und ist zuständig für alle Aufgaben, die nicht ausdrücklich dem Exekutivdirektor übertragen wurden.

(2) Der Verwaltungsrat gibt sich eine Geschäftsordnung. Diese Geschäftsordnung beinhaltet spezielle Verfahren zur Ermittlung und Vermeidung von Interessenkonflikten und gewährleistet die Vertraulichkeit sensibler Informationen.

(3) Der Verwaltungsrat trifft die erforderlichen strategischen Entscheidungen, insbesondere im Hinblick auf:

a) die Ausarbeitung und Annahme der Agenda und die Überwachung ihrer Durchführung;

b) die Annahme — unter Berücksichtigung der politischen Prioritäten der Union und der Agenda — des mehrjährigen Arbeitsprogramms, in dem die gemeinsamen Prioritäten für Industrie, Technologie und Forschung auf der Grundlage der von den Mitgliedstaaten in Zusammenarbeit mit der Gemeinschaft ermittelten Bedürfnisse enthalten sind, auf die sich die finanzielle Unterstützung seitens der Union konzentrieren muss, einschließlich der Schlüsseltechnologien und -bereiche für die Entwicklung der eigenen Fähigkeiten der Union im Bereich der Cybersicherheit;

c) die Annahme des jährlichen Arbeitsprogramms für die Verwendung der einschlägigen Mittel der Union, insbesondere für die Umsetzung der die Cybersicherheit betreffenden Teile von „Horizont Europa“, soweit sie von den Mitgliedstaaten freiwillig kofinanziert werden, und des Programms „Digitales Europa“ im Einklang mit dem mehrjährigen Arbeitsprogramm des Kompetenzzentrums und dem Strategieplanungsprozess im Rahmen von „Horizont Europa“;

d) die Annahme des Jahresabschlusses und der Bilanz sowie des jährlichen Tätigkeitsberichts des Kompetenzzentrums auf der Grundlage eines Vorschlags des Exekutivdirektors;

e) die Annahme der eigenen Finanzordnung des Kompetenzzentrums gemäß Artikel 70 der Haushaltsordnung;

f) die Zuweisung von Mitteln aus dem Haushaltsplan der Union für Themenbereiche mit gemeinsamen Maßnahmen von Union und Mitgliedstaaten als Teil des jährlichen Arbeitsprogramms;

g) die Beschreibung der in Buchstabe f des vorliegenden Unterabsatzes genannten gemeinsamen Maßnahmen und die Festlegung der Bedingungen für deren Durchführung solcher gemeinsamer Maßnahmen im Rahmen des jährlichen Arbeitsprogramms und im Einklang mit den in Buchstabe f genannten Beschlüssen und gemäß den Verordnungen (EU) 2021/695 und (EU) 2021/694;

h) die Annahme eines Verfahrens zur Ernennung des Exekutivdirektors sowie die Ernennung und Abberufung des Exekutivdirektors, die Verlängerung seiner Amtszeit, die Vorgabe von Leitlinien für den Exekutivdirektor und die Beaufsichtigung der Leistung des Exekutivdirektors;

i) die Annahme von Leitlinien zur Prüfung und Registrierung von Einrichtungen als Mitglieder der Gemeinschaft;

j) die Annahme der in Artikel 10 Absatz 2 genannten Arbeitsvereinbarungen;

k) die Ernennung des Rechnungsführers;

l) die Annahme des jährlichen Haushaltsplans des Kompetenzzentrums, einschließlich des entsprechenden Stellenplans mit Angabe der Zahl der Planstellen auf Zeit nach Funktions- und Besoldungsgruppe, mit der Zahl der Vertragsbediensteten und abgeordneten nationalen Sachverständigen in Vollzeitäquivalenten;

m) die Annahme von Transparenzvorschriften für das Kompetenzzentrum und von Vorschriften zur Vermeidung von und zum Umgang mit Interessenkonflikten — auch in Bezug auf die Mitglieder des Verwaltungsrates — gemäß Artikel 42 der Delegierten Verordnung (EU) 2019/715;

n) die Einrichtung von Arbeitsgruppen innerhalb der Gemeinschaft, gegebenenfalls unter Berücksichtigung der Empfehlungen der strategischen Beratungsgruppe;

o) die Ernennung der Mitglieder der strategischen Beratungsgruppe;

p) die Annahme von Vorschriften über die Kostenerstattung für Mitglieder der strategischen Beratungsgruppe;

q) die Einrichtung eines Überwachungsmechanismus, um sicherzustellen, dass die Verwendung der entsprechenden vom Kompetenzzentrum verwalteten Mittel im Einklang mit der Agenda, dem Auftrag, dem mehrjährigen Arbeitsprogramm sowie den Vorschriften der Programme, aus denen die jeweilige Finanzierung stammt, erfolgt;

r) die Gewährleistung eines regelmäßigen Dialogs und die Einrichtung eines wirksamen Mechanismus für die Zusammenarbeit mit der Gemeinschaft;

s) die Festlegung der Kommunikationspolitik des Kompetenzzentrums auf Grundlage einer Empfehlung des Exekutivdirektors;

t) gegebenenfalls die Festlegung von Durchführungsbestimmungen zum Statut der Beamten der Europäischen Union und die Beschäftigungsbedingungen für die sonstigen Bediensteten der Union gemäß der Verordnung (EWG, Euratom, EGKS) Nr. 259/68 des Rates ([15]) (im Folgenden „Statut der Beamten“ und „Beschäftigungsbedingungen“) nach Artikel 30 Absatz 3 der vorliegenden Verordnung;

u) gegebenenfalls die Festlegung von Bestimmungen über die Abstellung nationaler Sachverständiger zum Kompetenzzentrum und über den Einsatz von Praktikanten nach Artikel 31 Absatz 2;

v) die Annahme von Sicherheitsvorschriften für das Kompetenzzentrum;

w) die Annahme einer Betrugs- und Korruptionsbekämpfungsstrategie, die den diesbezüglichen Betrugs- und Korruptionsrisiken entspricht, sowie die Annahme von umfassenden Maßnahmen — im Einklang mit den geltenden Rechtsvorschriften der Union — zum Schutz von Personen, die Verstöße gegen das Unionsrecht melden, unter Berücksichtigung einer Kosten-Nutzen-Analyse der durchzuführenden Maßnahmen;

x) erforderlichenfalls die Festlegung der Methode zur Berechnung des freiwilligen Finanzbeitrags der beitragenden Mitgliedstaaten und ihres freiwilligen Beitrags in Form von Sachleistungen im Einklang mit den Verordnungen (EU) 2021/695 und (EU) 2021/694 oder anderer anwendbarer Gesetzgebung;

([15]) ABl. L 56 vom 4.3.1968, S. 1.

y) die Gewährleistung von Kohärenz und Synergien mit den nicht vom Kompetenzzentrum verwalteten Teilen der Programme „Digitales Europa“ und von „Horizont Europa“ sowie mit anderen Unionsprogrammen im Zusammenhang mit dem jährlichen Arbeitsprogramm und dem mehrjährigen Arbeitsprogramm;

z) die Annahme des jährlichen Berichts über die Verwirklichung der strategischen Ziele und Prioritäten des Kompetenzzentrums, erforderlichenfalls mit einer Empfehlung für eine bessere Verwirklichung dieser Ziele und Prioritäten.

Sofern im Jahresarbeitsprogramm gemeinsame Maßnahmen vorgesehen sind, enthält es Informationen über die freiwilligen Beiträge der Mitgliedstaaten zu gemeinsamen Maßnahmen. Gegebenenfalls wird in Vorschlägen, insbesondere im Vorschlag für das jährliche Arbeitsprogramm, bewertet, ob es notwendig ist, die Sicherheitsvorschriften gemäß Artikel 33 der vorliegenden Verordnung, einschließlich des Sicherheitsselbstbewertungsverfahrens gemäß Artikel 20 der Verordnung (EU) 2021/695 anzuwenden;

(4) Bezüglich der in Absatz 3 Buchstaben a, b und c festgelegten Entscheidungen haben der Exekutivdirektor und der Verwaltungsrat im Einklang mit der vom Verwaltungsrat festgelegten Geschäftsordnung einschlägige strategische Beratung durch die und Beiträge der ENISA zu berücksichtigen.

(5) Der Verwaltungsrat ist dafür verantwortlich, sicherzustellen, dass adäquate Folgemaßnahmen zu den Empfehlungen, die im Durchführungsbericht und in der Bewertung, die in Artikel 38 Absatz 2 und Absatz 4 genannt sind, durchgeführt werden.

Artikel 14

Vorsitz und Sitzungen des Verwaltungsrats

(1) Der Verwaltungsrat wählt aus dem Kreis seiner Mitglieder einen Vorsitzenden und einen stellvertretenden Vorsitzenden für einen Zeitraum von jeweils drei Jahren. Die Amtszeit des Vorsitzenden und des stellvertretenden Vorsitzenden kann einmal auf Beschluss des Verwaltungsrats verlängert werden. Endet jedoch die Mitgliedschaft des Vorsitzenden oder des stellvertretenden Vorsitzenden im Verwaltungsrat während ihrer Amtszeit, so endet auch ihre Amtszeit automatisch zu diesem Zeitpunkt. Der stellvertretende Vorsitzende tritt im Fall der Verhinderung des Vorsitzenden von Amts wegen an dessen Stelle. Der Vorsitzende nimmt an den Abstimmungen teil.

(2) Der Verwaltungsrat hält mindestens dreimal jährlich ordentliche Sitzungen ab. Außerordentliche Sitzungen können auf Antrag der Kommission, auf Antrag eines Drittels aller Mitglieder des Verwaltungsrats, auf Antrag des Vorsitzenden oder auf Antrag des Exekutivdirektors in Wahrnehmung seiner Aufgaben einberufen werden.

(3) Der Exekutivdirektor beteiligt sich an den Beratungen des Verwaltungsrats, sofern der Verwaltungsrat nichts anderes beschließt, verfügt jedoch über kein Stimmrecht.

(4) Der Verwaltungsrat kann im Einzelfall andere Personen einladen, um an den Sitzungen als Beobachter teilzunehmen.

(5) Der Vorsitzende kann Vertreter der Gemeinschaft einladen, an den Sitzungen des Verwaltungsrats teilzunehmen; sie besitzen jedoch kein Stimmrecht.

(6) Die Mitglieder des Verwaltungsrats und ihre Stellvertreter können sich nach Maßgabe der Geschäftsordnung des Verwaltungsrats in den Sitzungen von Beratern oder Sachverständigen unterstützen lassen.

(7) Die Sekretariatsgeschäfte des Verwaltungsrats werden vom Kompetenzzentrum wahrgenommen.

Artikel 15

Abstimmungsregeln des Verwaltungsrats

(1) Der Verwaltungsrat verfolgt bei seinen Beratungen einen konsensorientierten Ansatz. Eine Abstimmung findet statt, wenn die Mitglieder des Verwaltungsrats keinen Konsens erzielen konnten.

(2) Kann der Verwaltungsrat keinen Konsens bei einer Angelegenheit erzielen, so fasst er seine Beschlüsse mit einer Mehrheit von mindestens 75 % der Stimmen aller Mitglieder, wobei die Vertreter der Kommission zu diesem Zweck ein einziges Mitglied darstellen. Ein abwesendes Mitglied des Verwaltungsrats kann sein Stimmrecht auf seinen Stellvertreter oder — bei Abwesenheit seines Stellvertreters — auf ein anderes Mitglied übertragen. Ein Mitglied des Verwaltungsrats darf höchstens ein anderes Mitglied vertreten.

(3) Beschlüsse des Verwaltungsrats zu den gemeinsamen Maßnahmen und deren Verwaltung gemäß Artikel 13 Absatz 3 Buchstaben f und g werden wie folgt gefasst:

a) Beschlüsse über die Zuweisung von Mitteln aus dem Haushaltsplan der Union für gemeinsame Maßnahmen gemäß Artikel 13 Absatz 3 Buchstabe f sowie Beschlüsse über die Aufnahme der betreffenden gemeinsamen Maßnahmen in das jährliche Arbeitsprogramm werden gemäß Absatz 2 des vorliegenden Artikels gefasst.

b) Beschlüsse im Zusammenhang mit der Beschreibung der gemeinsamen Maßnahmen und zur Festlegung der Bedingungen für deren Durchführung gemäß Artikel 13 Absatz 3 Buchstabe g werden von den teilnehmenden Mitgliedstaaten und der Kommission gefasst, wobei die Stimmrechte der Mitglieder im Verhältnis zu dem entsprechenden Beitrag stehen, den sie gemäß der nach Artikel 13 Absatz 3 Buchstabe x festgelegten Methode zu der betreffenden gemeinsamen Maßnahme geleistet haben.

(4) Bei Beschlüssen, die gemäß Artikel 13 Absatz 3 Buchstaben b, c, d, e, f, k, l, p, q, t, u, w, x und y gefasst werden, verfügt die Kommission über 26 % aller Stimmen im Verwaltungsrat.

(5) Bei anderen als den in Absatz 3 Buchstabe b und in Absatz 4 genannten Beschlüssen verfügen jeder Mitgliedstaat und die Union über jeweils eine Stimme. Die Stimme der Union wird gemeinsam von den beiden Vertretern der Kommission abgegeben.

(6) Der Vorsitzende nimmt an der Abstimmung teil.

Abschnitt II

Exekutivdirektor

Artikel 16

Ernennung und Abberufung des Exekutivdirektors und Verlängerung seiner Amtszeit

(1) Der Exekutivdirektor ist eine Person mit Fachwissen und hohem Ansehen auf den Gebieten, auf denen das Kompetenzzentrum tätig ist.

(2) Der Exekutivdirektor wird als Zeitbediensteter des Kompetenzzentrums nach Artikel 2 Buchstabe a der Beschäftigungsbedingungen eingestellt.

(3) Der Exekutivdirektor wird vom Verwaltungsrat auf der Grundlage einer Liste von Bewerbern ernannt, die die Kommission im Anschluss an ein offenes, transparentes und diskriminierungsfreies Auswahlverfahren vorschlägt.

(4) Für den Abschluss des Vertrags mit dem Exekutivdirektor wird das Kompetenzzentrum durch den Vorsitzenden des Verwaltungsrats vertreten.

(5) Die Amtszeit des Exekutivdirektors beträgt vier Jahre. Vor dem Ende dieses Zeitraums nimmt die Kommission eine Bewertung vor, bei der die Leistung des Exekutivdirektors und die künftigen Aufgaben und Herausforderungen des Kompetenzzentrums berücksichtigt werden.

(6) Der Verwaltungsrat kann auf einen Vorschlag der Kommission, der die Bewertung nach Absatz 5 berücksichtigt, die Amtszeit des Exekutivdirektors einmal um höchstens vier Jahre verlängern.

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

(8) Der Exekutivdirektor kann nur durch einen Beschluss des Verwaltungsrats auf Vorschlag der Kommission oder von mindestens 50 % der Mitgliedstaaten seines Amtes enthoben werden.

Artikel 17

Aufgaben des Exekutivdirektors

(1) Der Exekutivdirektor ist für den Betrieb und die laufende Geschäftsführung des Kompetenzzentrums verantwortlich und ist dessen gesetzlicher Vertreter. Der Exekutivdirektor ist gegenüber dem Verwaltungsrat rechenschaftspflichtig und nimmt seine Aufgaben im Rahmen der ihm übertragenen Befugnisse völlig unabhängig wahr. Der Exekutivdirektor wird vom Personal des Kompetenzzentrums unterstützt.

(2) Der Exekutivdirektor erfüllt mindestens folgende Aufgaben in unabhängiger Weise:

a) Durchführung der vom Verwaltungsrat gefassten Beschlüsse;

b) Unterstützung des Verwaltungsrats bei seiner Arbeit, Wahrnehmung der Sekretariatsgeschäfte für seine Sitzungen und Bereitstellung aller zur Wahrnehmung seiner Aufgaben erforderlichen Informationen;

c) Ausarbeitung und Vorlage des Entwurfs der Agenda sowie — im Einklang mit der Agenda — des Entwurfs des mehrjährigen Arbeitsprogramms und des Entwurfs des jährlichen Arbeitsprogramms des Kompetenzzentrums zur Annahme durch den Verwaltungsrat, einschließlich Angaben zum Umfang der Aufforderungen zur Einreichung von Vorschlägen, der Aufforderungen zur Interessenbekundung und der Ausschreibungen, die für die Durchführung des jährlichen Arbeitsprogramms erforderlich sind, sowie der entsprechenden von den Mitgliedstaaten und der Kommission vorgelegten Ausgabenvoranschläge; dies geschieht nach Anhörung des Verwaltungsrats und der Kommission und unter Berücksichtigung der Beiträge der nationalen Koordinierungszentren und der Gemeinschaft;

d) Ausarbeitung und Vorlage des Entwurfs des jährlichen Haushaltsplans zur Annahme durch den Verwaltungsrat, einschließlich des entsprechenden Stellenplans gemäß Artikel 13 Absatz 3 Buchstabe l mit Angabe der Zahl der Planstellen auf Zeit je Besoldungs- und Funktionsgruppe sowie der Zahl der Vertragsbediensteten und abgeordneten nationalen Sachverständigen, ausgedrückt in Vollzeitäquivalenten;

e) Durchführung des jährlichen Arbeitsprogramms und des mehrjährigen Arbeitsprogramms und Berichterstattung darüber an den Verwaltungsrat;

f) Ausarbeitung des Entwurfs des jährlichen Tätigkeitsberichts des Kompetenzzentrums mit den Angaben über die entsprechenden Ausgaben und die Durchführung der Agenda und des mehrjährigen Arbeitsprogramms; erforderlichenfalls werden diesem Bericht Vorschläge für eine weitere Verbesserung der Verwirklichung oder für die Neuformulierung der strategischen Ziele und Prioritäten beigefügt;

g) Gewährleistung der Durchführung wirksamer Überwachungs- und Bewertungsverfahren in Bezug auf die Leistung des Kompetenzzentrums;

h) Ausarbeitung eines Aktionsplans mit Folgemaßnahmen zu den Schlussfolgerungen des Durchführungsberichts und der Bewertung, die in Artikel 38 Absatz 2 und Absatz 4 genannt sind, und alle zwei Jahre Übermittlung von Fortschrittsberichten an das Europäische Parlament und die Kommission;

i) Ausarbeitung und Abschluss von Vereinbarungen mit den nationalen Koordinierungszentren;

j) Wahrnehmung der Zuständigkeit für Verwaltungs-, Finanz- und Personalangelegenheiten, einschließlich der Ausführung des Haushaltsplans des Kompetenzzentrums, wobei die Beratung durch die einschlägige interne Auditstelle im Einklang mit den Beschlüssen gemäß Artikel 13 Absatz 3 Buchstaben e, l, t, u, v und w gebührend zu berücksichtigen ist;

k) Genehmigung und Verwaltung der Einleitung von Aufforderungen zur Einreichung von Vorschlägen entsprechend dem jährlichen Arbeitsprogramm und Verwaltung der sich daraus ergebenden Finanzhilfevereinbarungen und -beschlüsse;

l) Genehmigung der Liste der Maßnahmen, die auf der Grundlage einer von einer unabhängigen Sachverständigengruppe erstellten Rangliste für eine Finanzierung ausgewählt wurden;

m) Genehmigung und Verwaltung der Einleitung von Ausschreibungen entsprechend dem jährlichen Arbeitsprogramm und Verwaltung der sich daraus ergebenden Verträge;

n) Genehmigung der Angebote, die für eine Finanzierung ausgewählt wurden;

o) Vorlage des Entwurfs des Jahresabschlusses und der Bilanz bei der einschlägigen internen Auditstelle und anschließend beim Verwaltungsrat;

p) Gewährleistung der Durchführung von Risikobewertungen und eines Risikomanagements;

q) Unterzeichnung einzelner Finanzhilfevereinbarungen, Beschlüsse und Verträge;

r) Unterzeichnung der Verträge über öffentliche Aufträge;

s) Ausarbeitung eines Aktionsplans mit Folgemaßnahmen zu den Schlussfolgerungen interner oder externer Prüfberichte sowie der Untersuchungen des mit dem Beschluss 1999/352/EG, EGKS, Euratom der Kommission ([16]) errichteten Europäischen Amtes für Betrugsbekämpfung (OLAF) und alle zwei Jahre Berichterstattung über die erzielten Fortschritte an die Kommission sowie regelmäßig an den Verwaltungsrat;

t) Ausarbeitung des Entwurfs der für das Kompetenzzentrum geltenden Finanzordnung;

u) Einrichtung eines wirksamen und effizienten internen Kontrollsystems und Sicherstellung seines ordnungsgemäßen Funktionierens sowie Meldung bedeutsamer diesbezüglicher Änderungen an den Verwaltungsrat;

([16]) Beschluss 1999/352/EG, EGKS, Euratom der Kommission vom 28. April 1999 zur Errichtung des Europäischen Amtes für Betrugsbekämpfung (OLAF) (ABl. L 136 vom 31.5.1999, S. 20).

v) Gewährleistung einer wirksamen Kommunikation mit den Organen der Union und auf Ersuchen Berichterstattung an das Europäische Parlament und den Rat;

w) Ergreifung sonstiger Maßnahmen, die zur Beurteilung der Erfüllung des Auftrags und der Ziele des Kompetenzzentrums erforderlich sind;

x) Ausführung der ihm vom Verwaltungsrat übertragenen sonstigen Aufgaben.

Abschnitt III

Strategische Beratungsgruppe

Artikel 18

Zusammensetzung der strategischen Beratungsgruppe

(1) Die strategische Beratungsgruppe besteht aus höchstens 20 Mitgliedern. Die Mitglieder werden vom Verwaltungsrat auf Vorschlag des Exekutivdirektors aus dem Kreis der Vertreter der Mitglieder der Gemeinschaft, bei denen es sich nicht um Vertreter von Organen, Einrichtungen und sonstigen Stellen der Union handelt, ernannt. Es kommen nur Vertreter von Mitgliedern infrage, die nicht von einem Drittland oder einer Einrichtung mit Sitz in einem Drittland kontrolliert werden. Die Ernennung erfolgt nach Maßgabe eines offenen, transparenten und diskriminierungsfreien Verfahrens. Der Verwaltungsrat verfolgt bei der Zusammensetzung der strategischen Beratungsgruppe das Ziel, im Hinblick auf die Vertretung in der Gemeinschaft ein ausgewogenes Verhältnis zwischen wissenschaftlichen, wirtschaftlichen und zivilgesellschaftlichen Einrichtungen, nachfrage- und angebotsseitigen Branchen, großen Unternehmen und KMU, sowie ein ausgewogenes Verhältnis in Bezug auf geographische Herkunft und Geschlecht, zu erreichen. Bei der Zusammensetzung der strategischen Beratungsgruppe wird auch das Ziel verfolgt, im Interesse des Zusammenhalts der Union und aller Mitgliedstaaten im Bereich der Cybersicherheit bei Forschung, Industrie und Technologie ein intrasektorales Gleichgewicht zu erreichen. Die strategische Beratungsgruppe setzt sich so zusammen, dass ein umfassender, kontinuierlicher und ständiger Dialog zwischen der Gemeinschaft und dem Kompetenzzentrum ermöglicht wird.

(2) Die Mitglieder der strategischen Beratungsgruppe verfügen über Fachwissen in Bezug auf Forschung und industrielle Entwicklung sowie Angebot, Umsetzung bzw. Realisierung gewerblicher Dienstleistungen oder entsprechender Produkte im Bereich der Cybersicherheit. Die Anforderungen in Bezug auf solches Fachwissen werden vom Verwaltungsrat genauer festgelegt.

(3) Die Verfahren für die Ernennung der Mitglieder der strategischen Beratungsgruppe und die Arbeitsweise der strategischen Beratungsgruppe werden in der Geschäftsordnung des Verwaltungsrats festgelegt und veröffentlicht.

(4) Die Amtszeit der Mitglieder der strategischen Beratungsgruppe beträgt zwei Jahre. Sie kann einmal verlängert werden.

(5) Vertreter der Kommission und anderer Organe, Einrichtungen und sonstigen Stellen der Union, insbesondere der ENISA, können von der strategischen Beratungsgruppe dazu eingeladen werden, sich an ihrer Arbeit zu beteiligen und diese zu unterstützen. Die strategische Beratungsgruppe kann im Einzelfall gegebenenfalls zusätzliche Vertreter der Gemeinschaft als Beobachter, Berater oder Sachverständige einladen, um der Entwicklungsdynamik im Bereich der Cybersicherheit Rechnung zu tragen. Die Mitglieder des Verwaltungsrats können als Beobachter an den Sitzungen der strategischen Beratungsgruppe teilnehmen.

Artikel 19

Arbeitsweise der strategischen Beratungsgruppe

(1) Die strategische Beratungsgruppe tritt mindestens dreimal im Jahr zusammen.

(2) Die strategische Beratungsgruppe berät den Verwaltungsrat bei der Einrichtung von Arbeitsgruppen innerhalb der Gemeinschaft gemäß Artikel 13 Absatz 3 Buchstabe n zu bestimmten Fragen, die für die Arbeit des Kompetenzzentrums von Bedeutung sind, sofern diese direkt mit den in Artikel 20 genannten Aufgaben und Zuständigkeiten zusammenhängen. Falls erforderlich unterliegen diese Arbeitsgruppen der Gesamtkoordinierung durch ein Mitglied oder mehrere Mitglieder der strategischen Beratungsgruppe.

(3) Die strategische Beratungsgruppe wählt ihren Vorsitzenden mit einfacher Mehrheit ihrer Mitglieder.

(4) Die Sekretariatsgeschäfte der strategischen Beratungsgruppe werden vom Exekutivdirektor und dem Personal des Kompetenzzentrums unter Verwendung der vorhandenen Ressourcen und unter gebührender Berücksichtigung der Arbeitsbelastung des Kompetenzzentrums wahrgenommen. Die für die Unterstützung der strategischen Beratungsgruppe zugewiesenen Mittel werden im Entwurf des jährlichen Haushaltsplans ausgewiesen.

(5) Die strategische Beratungsgruppe gibt sich mit einfacher Mehrheit ihrer Mitglieder eine Geschäftsordnung.

Artikel 20

Aufgaben der strategischen Beratungsgruppe

Die strategische Beratungsgruppe berät das Kompetenzzentrum regelmäßig bei der Durchführung seiner Tätigkeiten und sorgt für die Kommunikation mit der Gemeinschaft und anderen einschlägigen Interessenträgern. Die strategische Beratungsgruppe

a) unterstützt den Exekutivdirektor und den Verwaltungsrat innerhalb der vom Verwaltungsrat festgelegten Fristen und gegebenenfalls unter Berücksichtigung der Beiträge der Gemeinschaft und der in Artikel 13 Absatz 3 Buchstabe n genannten Arbeitsgruppen durch ständig aktualisierte strategische Beratung und Beiträge zur Agenda, zum jährlichen Arbeitsprogramm und zum mehrjährigen Arbeitsprogramm;

b) berät den Verwaltungsrat bezüglich der Einrichtung von Arbeitsgruppen innerhalb der Gemeinschaft gemäß Artikel 13 Absatz 3 Buchstabe n zu spezifischen Fragen, die für die Arbeit des Kompetenzzentrums von Belang sind;

c) beschließt und organisiert öffentliche Konsultationen, die vom Verwaltungsrat zu genehmigen sind und an denen alle öffentlichen und privaten Akteure teilnehmen können, die ein Interesse im Bereich der Cybersicherheit haben, um Beiträge für die in Buchstabe a genannte strategische Beratung zu sammeln.

KAPITEL III

Finanzbestimmungen

Artikel 21

Finanzbeiträge der Union und der Mitgliedstaaten

(1) Das Kompetenzzentrum wird von der Union und gemeinsame Maßnahmen werden von der Union und durch freiwillige Beiträge der Mitgliedstaaten finanziert.

(2) Die Verwaltungs- und Betriebskosten bei gemeinsamen Maßnahmen werden von der Union und den Mitgliedstaaten, die zu den gemeinsamen Maßnahmen beitragen, im Einklang mit den Verordnungen (EU) 2021/695 und (EU) 2021/694 getragen.

(3) Der Beitrag der Union zur Deckung der Verwaltungs- und Betriebskosten des Kompetenzzentrums besteht aus

a) höchstens 1 649 566 000 EUR aus dem Programm „Digitales Europa", davon höchstens 32 000 000 EUR für Verwaltungskosten;

b) einem Betrag aus „Horizont Europa" — auch für Verwaltungskosten — für gemeinsame Maßnahmen, der dem Betrag der von den Mitgliedstaaten gemäß Absatz 7 des vorliegenden Artikels geleisteten Beiträge entspricht, jedoch nicht den Betrag übersteigt, der in dem gemäß Artikel 6 Absatz 6 der Verordnung (EU) 2021/695 durchzuführenden strategischen Planungsprozess von „Horizont Europa", im jährlichen Arbeitsprogramm oder im mehrjährigen Arbeitsprogramm festgelegt ist;

c) einem Betrag aus den anderen einschlägigen Programmen der Union, sofern er für die Durchführung der Aufgaben oder die Verwirklichung der Ziele des Kompetenzzentrums erforderlich ist, vorbehaltlich der gemäß den Rechtsakten der Union zur Aufstellung dieser Programme gefassten Beschlüsse.

(4) Der Höchstbeitrag der Union wird aus den Mitteln des Gesamthaushaltsplans der Union für das Programm „Digitales Europa", das mit dem Beschluss (EU) 2021/764 festgelegte Spezifische Programm zur Durchführung von „Horizont Europa" und andere Programme und Projekte, die in das Tätigkeitsfeld des Kompetenzzentrums oder des Netzwerks fallen, bereitgestellt.

(5) Das Kompetenzzentrum führt die Cybersicherheitsmaßnahmen im Rahmen des Programms „Digitales Europa" und von „Horizont Europa" im Einklang mit Artikel 62 Absatz 1 Unterabsatz 1 Buchstabe c Ziffer iv der Haushaltsordnung durch.

(6) Beiträge aus anderen als den in den Absätzen 3 und 4 aufgeführten Unionsprogrammen, die Teil der Kofinanzierung seitens der Union für ein von einem der Mitgliedstaaten durchgeführtes Programm sind, werden bei der Berechnung des Höchstbetrags des Finanzbeitrags der Union gemäß den genannten Absätzen nicht angerechnet.

(7) Die Mitgliedstaaten beteiligen sich durch Finanzbeiträge und/oder Beiträge in Form von Sachleistungen freiwillig an gemeinsamen Maßnahmen. Beteiligt sich ein Mitgliedstaat an einer gemeinsamen Maßnahme, so deckt der Finanzbeitrag dieses Mitgliedstaats die Verwaltungskosten im Verhältnis zu seinem Beitrag zu dieser gemeinsamen Maßnahme. Die Verwaltungskosten gemeinsamer Maßnahmen werden durch Finanzbeiträge gedeckt. Die Betriebskosten bei gemeinsamen Maßnahmen können gemäß „Horizont Europa" und dem Programm „Digitales Europa" durch einen Finanzbeitrag oder als Beitrag in Form von Sachleistungen gedeckt werden. Beiträge eines Mitgliedstaats können als Unterstützung erfolgen, die der jeweilige Mitgliedstaat im Rahmen einer gemeinsamen Maßnahme Begünstigten leistet, die in dem betreffenden

Mitgliedstaat niedergelassen sind. Beiträge der Mitgliedstaaten in Form von Sachleistungen bestehen aus den den nationalen Koordinierungszentren und anderen öffentlichen Einrichtungen bei der Beteiligung an im Rahmen dieser Verordnung finanzierten Projekten entstehenden förderfähigen Kosten abzüglich eines etwaigen Beitrags der Union zu diesen Kosten. Bei im Rahmen von „Horizont Europa" finanzierten Projekten werden die förderfähigen Kosten im Einklang mit Artikel 36 der Verordnung (EU) 2021/695 berechnet. Bei im Rahmen des Programms „Digitales Europa" finanzierten Projekten werden die förderfähigen Kosten im Einklang mit der Haushaltsordnung berechnet.

Der veranschlagte Gesamtbetrag der freiwilligen Beiträge der Mitgliedstaaten zu gemeinsamen Maßnahmen im Rahmen von „Horizont Europa" — einschließlich der Finanzbeiträge für Verwaltungskosten — wird im Hinblick auf die Berücksichtigung in dem gemäß Artikel 6 Absatz 6 der Verordnung (EU) 2021/695 durchzuführenden strategischen Planungsprozess unter Mitwirkung des Verwaltungsrats festgelegt. Für Maßnahmen im Rahmen des Programms „Digitales Europa" können die Mitgliedstaaten unbeschadet des Artikels 15 der Verordnung (EU) 2021/694 einen Beitrag zu den über das Programm „Digitales Europa" kofinanzierten Kosten des Kompetenzzentrums leisten, der unter den in Absatz 3 Buchstabe a des vorliegenden Artikels angegebenen Beträgen liegt.

(8) Nationale Kofinanzierungen von durch andere Programme der Union als „Horizont Europa" und dem Programm „Digitales Europa" unterstützten Maßnahmen durch die Mitgliedstaaten gelten als nationale Beiträge der Mitgliedstaaten, soweit diese Beiträge Teil gemeinsamer Maßnahmen sind und in das Arbeitsprogramm des Kompetenzzentrums aufgenommen wurden.

(9) Für die Zwecke der Bewertung der Beiträge nach Absatz 3 des vorliegenden Artikels und Artikel 22 Absatz 2 Buchstabe b werden Kosten nach den üblichen Kostenrechnungsverfahren des betreffenden Mitgliedstaats, den geltenden Rechnungslegungsgrundsätzen des betreffenden Mitgliedstaats und den relevanten internationalen Rechnungslegungsstandards bestimmt. Kosten werden von einem unabhängigen externen Rechnungsprüfer zertifiziert, der von dem betreffenden Mitgliedstaat benannt wird. Die Bewertungsmethode kann vom Kompetenzzentrum überprüft werden, falls hinsichtlich der Zertifizierung Unklarheiten bestehen.

(10) Falls ein Mitgliedstaat seinen Verpflichtungen zur Leistung seiner Finanzbeiträge oder Beiträge in Form von Sachleistungen in Bezug auf gemeinsame Maßnahmen nicht nachgekommen ist, informiert der Exekutivdirektor den betreffenden Mitgliedstaat schriftlich über dessen Versäumnis und setzt ihm eine angemessene Frist für die Beseitigung dieses Versäumnisses. Wird das Versäumnis nicht innerhalb dieser Frist beseitigt, so beruft der Exekutivdirektor eine Sitzung des Verwaltungsrats ein, in der darüber entschieden wird, ob dem säumigen beteiligten Mitgliedstaat das Stimmrecht zu entziehen ist oder ob andere Maßnahmen zu treffen sind, bis dieser Mitgliedstaat seinen Verpflichtungen nachgekommen ist. Das Stimmrecht des säumigen Mitgliedstaats in Bezug auf gemeinsame Maßnahmen wird ausgesetzt, bis er seine Verpflichtungen erfüllt hat.

(11) Die Kommission kann den Finanzbeitrag der Union zu gemeinsamen Maßnahmen aufkündigen, anteilsmäßig kürzen oder aussetzen, wenn die beitragenden Mitgliedstaaten die in Absatz 3 Buchstabe b genannten Beiträge nicht, nur teilweise oder verspätet leisten. Die Kündigung, Kürzung oder Aussetzung des Finanzbeitrags der Union durch die Kommission richtet sich nach dem Betrag und dem Zeitraum, in dem der Mitgliedstaat seine Beiträge nicht, nur zum Teil oder verspätet geleistet hat.

(12) Die beitragenden Mitgliedstaaten melden jährlich bis zum 31. Januar dem Verwaltungsrat die Höhe der in Absatz 7 genannten Beiträge für gemeinsame Maßnahmen mit der Union, die im vorangegangenen Haushaltsjahr geleistet wurden.

Artikel 22

Kosten und Mittelausstattung des Kompetenzzentrums

(1) Die Verwaltungskosten des Kompetenzzentrums werden grundsätzlich durch Finanzbeiträge von der Union gedeckt, die jährlich geleistet werden. Zusätzliche Finanzbeiträge werden von den beitragenden Mitgliedstaaten im Verhältnis zu ihren freiwilligen Beiträgen zu gemeinsamen Maßnahmen geleistet. Wird ein Teil des Beitrags zu den Verwaltungskosten nicht in Anspruch genommen, so kann er zur Deckung von Betriebskosten des Kompetenzzentrums bereitgestellt werden.

(2) Die Betriebskosten des Kompetenzzentrums werden gedeckt durch

a) den Finanzbeitrag der Union,

b) freiwillige Finanzbeiträge oder Beiträge in Form von Sachleistungen der beitragenden Mitgliedstaaten bei gemeinsamen Maßnahmen.

(3) Die in den Haushalt des Kompetenzzentrums eingestellten Mittel setzen sich aus den folgenden Beiträgen zusammen:

a) den Finanzbeiträgen der Union zu Betriebs- und Verwaltungskosten;

b) den freiwilligen Finanzbeiträgen der beitragenden Mitgliedstaaten zu Verwaltungskosten bei gemeinsamen Maßnahmen;

c) den freiwilligen Finanzbeiträgen der beitragenden Mitgliedstaaten zu Betriebskosten bei gemeinsamen Maßnahmen;

d) etwaigen Einnahmen des Kompetenzzentrums;

e) sämtlichen sonstigen Finanzbeiträgen, Mitteln oder Einnahmen.

(4) Zinserträge aus den von den beitragenden Mitgliedstaaten an das Kompetenzzentrum gezahlten Beiträgen gelten als Einnahmen des Kompetenzzentrums.

(5) Alle Mittel des Kompetenzzentrums und seine Tätigkeiten dienen dazu, die festgelegten Ziele zu verwirklichen.

(6) Das Kompetenzzentrum ist Eigentümer aller Vermögenswerte, die es selbst erwirtschaftet hat oder die ihm zum Zweck der Verwirklichung seiner Ziele übertragen wurden. Unbeschadet der geltenden Vorschriften für das jeweilige Förderprogramm wird über das Eigentum an den im Rahmen gemeinsamer Maßnahmen erwirtschafteten oder erworbenen Vermögenswerten gemäß Artikel 15 Absatz 3 Buchstabe b entschieden.

(7) Sofern sich das Kompetenzzentrum nicht in Abwicklung befindet, bleiben etwaige Einnahmeüberschüsse im Eigentum des Kompetenzzentrums und werden nicht an die beitragenden Mitglieder des Kompetenzzentrums ausgezahlt.

(8) Das Kompetenzzentrum arbeitet eng mit anderen Organen, Einrichtungen und sonstigen Stellen der Union zusammen, wobei deren jeweilige Mandate gebührend zu berücksichtigen sind und es nicht zu Überschneidungen mit den bestehenden Kooperationsmechanismen kommen darf, damit Synergien mit diesen genutzt und, sofern möglich und angemessen, damit die Verwaltungskosten gesenkt werden können.

Artikel 23

Finanzielle Verpflichtungen

Die finanziellen Verpflichtungen des Kompetenzzentrums dürfen den Betrag der ihm zur Verfügung stehenden oder seinem Haushalt von seinen Mitgliedern zugewiesenen Finanzmittel nicht übersteigen.

Artikel 24

Haushaltsjahr

Das Haushaltsjahr beginnt am 1. Januar und endet am 31. Dezember.

Artikel 25

Aufstellung des Haushaltsplans

(1) Der Exekutivdirektor erstellt jedes Jahr den Entwurf des Voranschlags der Einnahmen und Ausgaben des Kompetenzzentrums für das folgende Haushaltsjahr und legt ihn dem Verwaltungsrat zusammen mit dem Entwurf des Stellenplans gemäß Artikel 13 Absatz 3 Buchstabe l vor. Einnahmen und Ausgaben müssen ausgeglichen sein. Die Ausgaben des Kompetenzzentrums umfassen die Personal-, Verwaltungs-, Infrastruktur- und Betriebsausgaben. Die Verwaltungsausgaben sind auf ein Mindestmaß zu beschränken, einschließlich durch Umschichtung von Personal oder Planstellen.

(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 des Kompetenzzentrums für das folgende Haushaltsjahr.

(3) Der Verwaltungsrat übermittelt der Kommission jedes Jahr bis zum 31. Januar den in Absatz 2 des vorliegenden Artikels genannten Voranschlag, der Teil des Entwurfs des einheitlichen Programmplanungsdokuments gemäß Artikel 32 Absatz 1 der delegierten Verordnung (EU) 2019/715 ist.

(4) Die Kommission setzt auf der Grundlage des in Absatz 2 des vorliegenden Artikels genannten Voranschlags die von ihr für erforderlich erachteten Mittelansätze für den Stellenplan gemäß Artikel 13 Absatz 3 Buchstabe l der vorliegenden Verordnung und den Betrag des Zuschusses aus dem Gesamthaushaltsplan in den Haushaltsplanentwurf der Union ein, den sie nach den Artikeln 313 und 314 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV) dem Europäischen Parlament und dem Rat vorlegt.

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

(6) Der Stellenplan gemäß Artikel 13 Absatz 3 Buchstabe l wird vom Europäischen Parlament und vom Rat angenommen.

(7) Der Haushaltsplan des Kompetenzzentrums wird zusammen mit dem jährlichen Arbeitsprogramm und dem mehrjährigen Arbeitsprogramm vom Verwaltungsrat angenommen. Er wird endgültig, sobald der Gesamthaushaltsplan der Union endgültig festgestellt ist. Gegebenenfalls nimmt der Verwaltungsrat eine Anpassung des Haushaltsplans des Kompetenzzentrums und des jährlichen Arbeitsprogramms entsprechend dem Gesamthaushaltsplan der Union vor.

Artikel 26

Rechnungslegung des Kompetenzzentrums und Entlastung

Die vorläufige und endgültige Rechnungslegung des Kompetenzzentrums sowie die Entlastung entsprechen den Regeln und dem Zeitplan der Haushaltsordnung und der Finanzordnung des Kompetenzzentrums.

Artikel 27

Tätigkeitsberichte und Finanzberichterstattung

(1) Der Exekutivdirektor erstattet dem Verwaltungsrat jährlich Bericht über die Erfüllung seiner Pflichten gemäß der Finanzordnung des Kompetenzzentrums.

(2) Binnen zwei Monaten nach Ende jedes Haushaltsjahres legt der Exekutivdirektor dem Verwaltungsrat einen jährlichen Tätigkeitsbericht über die Fortschritte des Kompetenzzentrums im vorangegangenen Kalenderjahr zur Billigung vor; darin wird insbesondere auf das für jenes Jahr geltende jährliche Arbeitsprogramm und auf die Verwirklichung seiner strategischen Ziele und Prioritäten Bezug genommen. Dieser Bericht enthält Informationen über folgende Aspekte:

a) durchgeführte operative Maßnahmen mit den entsprechenden Ausgaben;

b) die eingereichten Maßnahmen mit einer Aufschlüsselung nach Art der Teilnehmer — einschließlich KMU — und nach Mitgliedstaat;

c) die für eine Finanzierung ausgewählten Maßnahmen mit einer Aufschlüsselung nach Art der Teilnehmer, einschließlich KMU, und nach Mitgliedstaat unter Angabe des vom Kompetenzzentrum für die einzelnen Teilnehmer und Maßnahmen zur Verfügung gestellten Beitrags;

d) die Erfüllung des Auftrags und der Ziele gemäß dieser Verordnung sowie Vorschläge für weitere Arbeiten, die zur Erfüllung dieses Auftrags und dieser Ziele erforderlich sind;

e) die Kohärenz der Umsetzungsaufgaben mit der Agenda und dem mehrjährigen Arbeitsprogramm.

(3) Der jährliche Tätigkeitsbericht wird nach seiner Genehmigung durch den Verwaltungsrat veröffentlicht.

Artikel 28

Finanzordnung

Das Kompetenzzentrum beschließt eine eigene Finanzordnung gemäß Artikel 70 der Haushaltsordnung.

Artikel 29

Schutz der finanziellen Interessen der Union

(1) Das Kompetenzzentrum gewährleistet bei der Durchführung der nach dieser Verordnung finanzierten Maßnahmen den Schutz der finanziellen Interessen der Union durch geeignete Präventivmaßnahmen gegen Betrug, Korruption und sonstige rechtswidrige Handlungen, durch regelmäßige und wirksame Kontrollen und — bei Feststellung von Unregelmäßigkeiten — durch Rückforderung zu Unrecht gezahlter Beträge sowie gegebenenfalls durch wirksame, verhältnismäßige und abschreckende verwaltungsrechtliche Sanktionen.

(2) Das Kompetenzzentrum gewährt Bediensteten der Kommission und sonstigen von der Kommission ermächtigten Personen sowie dem Europäischen Rechnungshof Zugang zu den Standorten und Räumlichkeiten des Kompetenzzentrums sowie zu allen Informationen, einschließlich Informationen in elektronischer Form, die für die Durchführung der Rechnungsprüfungen erforderlich sind.

(3) Das OLAF kann gemäß den Bestimmungen und Verfahren der Verordnung (Euratom, EG) Nr. 2185/96 des Rates ([17]) und der Verordnung (EU, Euratom) Nr. 883/2013 des Europäischen Parlaments und des Rates ([18]) Untersuchungen, einschließlich Kontrollen und Überprüfungen vor Ort, durchführen, um festzustellen, ob es im Zusammenhang mit Finanzhilfevereinbarungen oder Verträgen, die gemäß dieser Verordnung direkt oder indirekt finanziert werden, zu Betrug, Korruption oder anderen rechtswidrigen Handlungen zum Nachteil der finanziellen Interessen der Union gekommen ist.

(4) Unbeschadet der Absätze 1, 2 und 3 ist in Verträgen und Finanzhilfevereinbarungen, die sich aus der Durchführung dieser Verordnung ergeben, der Kommission, dem Kompetenzzentrum, dem Rechnungshof und OLAF ausdrücklich die Befugnis zu erteilen, entsprechend ihren Zuständigkeiten derartige Rechnungsprüfungen und Untersuchungen durchzuführen. Wenn die Durchführung einer Maßnahme ganz oder teilweise weitervergeben oder weiterdelegiert wird oder wenn sie die Vergabe eines öffentlichen Auftrags oder finanzieller Unterstützung an einen Dritten erfordert, müssen der Vertrag bzw. die Finanzhilfevereinbarung die Pflicht des Auftragnehmers oder des Begünstigten einschließen, von beteiligten Dritten die ausdrückliche Anerkennung dieser Befugnisse der Kommission, des Kompetenzzentrums, des Rechnungshofs und des OLAF zu verlangen.

KAPITEL IV

Personal des Kompetenzzentrums

Artikel 30

Personal

(1) Für das Personal des Kompetenzzentrums gelten das Statut der Beamten und die Beschäftigungsbedingungen sowie die im gegenseitigen Einvernehmen der Organe der Union erlassenen Regelungen zur Durchführung des Statuts der Beamten und der Beschäftigungsbedingungen.

(2) Der Verwaltungsrat übt in Bezug auf das Personal des Kompetenzzentrums die Befugnisse aus, die der Anstellungsbehörde durch das Statut der Beamten und der zum Abschluss von Dienstverträgen befugten Behörde durch die Beschäftigungsbedingungen übertragen wurden (im Folgenden „Befugnisse der Anstellungsbehörde").

(3) Der Verwaltungsrat erlässt gemäß Artikel 110 des Statuts der Beamten einen Beschluss auf der Grundlage von Artikel 2 Absatz 1 des Statuts der Beamten und Artikel 6 der Beschäftigungsbedingungen, durch den dem Exekutivdirektor die entsprechenden Befugnisse der Anstellungsbehörde übertragen und die Bedingungen festgelegt werden, unter denen diese Befugnisübertragung ausgesetzt werden kann. Der Exekutivdirektor kann diese Befugnisse weiterübertragen.

(4) Ist dies in außergewöhnlichen Fällen erforderlich, so kann der Verwaltungsrat die Übertragung der Befugnisse der Anstellungsbehörde auf den Exekutivdirektor sowie jegliche weitere Übertragung durch Letzteren durch einen Beschluss vorübergehend aussetzen. In solchen Fällen übt der Verwaltungsrat die Befugnisse der Anstellungsbehörde selbst aus oder überträgt sie einem seiner Mitglieder oder einem anderen Bediensteten des Kompetenzzentrums als dem Exekutivdirektor.

(5) Der Verwaltungsrat erlässt im Einklang mit Artikel 110 des Statuts der Beamten Durchführungsbestimmungen zum Statut der Beamten und zu den Beschäftigungsbedingungen.

(6) Die Personalstärke wird durch den in Artikel 13 Absatz 3 Buchstabe l genannten Stellenplan unter Angabe der Zahl der Planstellen auf Zeit nach Funktions- und Besoldungsgruppe und der Zahl der Vertragsbediensteten (in Vollzeitäquivalenten) in Übereinstimmung mit dem jährlichen Haushaltsplan des Kompetenzzentrums festgelegt.

(7) Der Personalbedarf des Kompetenzzentrums wird in erster Linie durch eine Umschichtung von Personal oder Planstellen von Organen, Einrichtungen und sonstigen Stellen der Union und durch die Einstellung von zusätzlichem Personal gedeckt. Das Personal des Kompetenzzentrums kann aus Bediensteten auf Zeit und Vertragsbediensteten bestehen.

([17]) 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).

([18]) 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).

(8) Sämtliche Personalausgaben trägt das Kompetenzzentrum.

Artikel 31

Abgeordnete nationale Sachverständige und sonstige Bedienstete

(1) Das Kompetenzzentrum kann auf abgeordnete nationale Sachverständige oder sonstiges Personal zurückgreifen, das nicht vom Kompetenzzentrum selbst beschäftigt wird.

(2) Der Verwaltungsrat beschließt im Einvernehmen mit der Kommission eine Regelung für die Abordnung nationaler Sachverständiger zum Kompetenzzentrum.

Artikel 32

Vorrechte und Befreiungen

Das dem EUV und dem AEUV beigefügte Protokoll Nr. 7 über die Vorrechte und Befreiungen der Europäischen Union findet auf das Kompetenzzentrum und sein Personal Anwendung.

KAPITEL V

Gemeinsame Bestimmungen

Artikel 33

Sicherheitsvorschriften

(1) Artikel 12 der Verordnung (EU) 2021/694 gilt für die Teilnahme an allen vom Kompetenzzentrum finanzierten Maßnahmen.

(2) Für aus „Horizont Europa" finanzierte Maßnahmen gelten die folgenden besonderen Sicherheitsvorschriften:

a) für die Zwecke von Artikel 38 Absatz 1 der Verordnung (EU) 2021/695 kann die Gewährung nicht ausschließlicher Lizenzen, wenn dies im jährlichen Arbeitsprogramm vorgesehen ist, auf Dritte beschränkt werden, die in einem Mitgliedstaat niedergelassen sind oder als niedergelassen gelten und von diesem Mitgliedstaat oder von Staatsangehörigen dieses Mitgliedstaats geführt werden;

b) für die Zwecke von Artikel 40 Absatz 4 Unterabsatz 1 Buchstabe b der Verordnung (EU) 2021/695 kann gegen die Übertragung von Eigentumsrechten an den Ergebnissen oder gegen die Gewährung einer ausschließlichen Lizenz zur Nutzung der Ergebnisse Einspruch erhoben werden, wenn die Übertragung oder Lizenzierung an einen Rechtsträger erfolgen soll, der zwar seinen Sitz in einem assoziierten Land oder in der Union hat, aber aus Drittländern geführt wird;

c) für die Zwecke von Artikel 41 Absatz 7 Unterabsatz 1 Buchstabe a der Verordnung (EU) 2021/695 kann die Gewährung von Zugangsrechten im Sinne von Artikel 2 Nummer 9 der genannten Verordnung, wenn dies im jährlichen Arbeitsprogramm vorgesehen ist, auf Rechtsträger beschränkt werden, die in einem Mitgliedstaat niedergelassen sind oder als niedergelassen gelten und von diesem Mitgliedstaat oder von Staatsangehörigen dieses Mitgliedstaats geführt werden.

Artikel 34

Transparenz

(1) Das Kompetenzzentrum führt seine Tätigkeiten mit einem hohen Maß an Transparenz aus.

(2) Das Kompetenzzentrum stellt sicher, dass die Öffentlichkeit sowie interessierte Kreise rechtzeitig angemessene, objektive, zuverlässige und leicht zugängliche Informationen, insbesondere über die Ergebnisse seiner Arbeit, erhalten. Ferner veröffentlicht es die nach Artikel 43 abgegebenen Interessenerklärungen. Diese Anforderungen gelten auch für die nationalen Koordinierungszentren, die Gemeinschaft und die strategische Beratungsgruppe im Einklang mit einschlägigem Recht.

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

(4) Das Kompetenzzentrum legt in der Geschäftsordnung des Verwaltungsrats des Kompetenzzentrums und der strategischen Beratungsgruppe die praktischen Einzelheiten für die Anwendung der Transparenzvorschriften nach den Absätzen 1 und 2 des vorliegenden Artikels fest. Bei Maßnahmen, die aus „Horizont Europa" finanziert werden, tragen diese Vorschriften und Einzelheiten den Bestimmungen der Verordnung (EU) 2021/695 Rechnung.

Artikel 35

Ausgewogenes Geschlechterverhältnis

Bei der Durchführung dieser Verordnung wählen die Kommission, die Mitgliedstaaten und anderen institutionellen und privatwirtschaftlichen Interessensträger im Zusammenhang mit der Benennung von Kandidaten oder dem Vorschlag von Vertretern nach Möglichkeit aus mehreren Kandidaten Vertreter aus und strebt dabei die Sicherstellung eines ausgewogenen Geschlechterverhältnisses an.

Artikel 36

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

(1) Nach Genehmigung durch die Kommission nimmt der Verwaltungsrat die Sicherheitsvorschriften des Kompetenzzentrums an. Diese Sicherheitsvorschriften wenden dabei die in den Beschlüssen (EU, Euratom) 2015/443 ([19]) und (EU, Euratom) 2015/444 ([20]) der Kommission enthaltenen Grundsätze und Regeln an.

(2) Die Mitglieder des Verwaltungsrats, der Exekutivdirektor, die externen Sachverständigen der Ad-hoc-Arbeitsgruppen sowie das Personal des Kompetenzzentrums unterliegen auch nach Beendigung ihrer Tätigkeit den Vertraulichkeitsbestimmungen des Artikels 339 AEUV.

(3) Das Kompetenzzentrum kann die Maßnahmen treffen, die notwendig sind, um den Austausch von Informationen, die für seine Aufgaben von Belang sind, mit der Kommission und den Mitgliedstaaten sowie gegebenenfalls mit den einschlägigen Organen, Einrichtungen und sonstigen Stellen der Union zu erleichtern. Alle zu diesem Zweck getroffenen Verwaltungsvereinbarungen über den Austausch von EU-Verschlusssachen oder, falls keine solche Vereinbarungen vorliegen, jede Ad-hoc-Weitergabe von EU-Verschlusssachen in Ausnahmefällen bedarf der vorherigen Genehmigung durch die Kommission.

Artikel 37

Zugang zu Unterlagen

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

(2) Der Verwaltungsrat legt bis zum 29. Dezember 2021 Maßnahmen zur Durchführung der Verordnung (EG) Nr. 1049/2001 fest.

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

Artikel 38

Überwachung, Bewertung und Überprüfung

(1) Das Kompetenzzentrum stellt sicher, dass seine Tätigkeiten, einschließlich der über die nationalen Koordinierungszentren und das Netzwerk verwalteten Tätigkeiten, einer kontinuierlichen und systematischen Überwachung und regelmäßigen Bewertung unterzogen werden. Das Kompetenzzentrum stellt sicher, dass die Daten für die Überwachung der Durchführung und der Ergebnisse der in Artikel 4 Absatz 3 Buchstabe b genannten Finanzierungsprogramme der Union effizient, wirksam und zeitnah erhoben werden und erlegt den Empfängern von Unionsmitteln und den Mitgliedstaaten verhältnismäßige Vorgaben für die Berichterstattung auf. Die Schlussfolgerungen dieser Bewertung werden veröffentlicht.

(2) Sobald ausreichende Informationen über die Durchführung dieser Verordnung vorliegen, spätestens jedoch 30 Monate nach dem in Artikel 46 Absatz 4 bestimmten Zeitpunkt, erstellt die Kommission einen Durchführungsbericht zu den Tätigkeiten des Kompetenzzentrums und berücksichtigt dabei die zuvor eingereichten Beiträge des Verwaltungsrats, der nationalen Koordinierungszentren und der Gemeinschaft. Die Kommission übermittelt diesen Durchführungsbericht bis zum 30. Juni 2024 an das Europäische Parlament und den Rat. Das Kompetenzzentrum und die Mitgliedstaaten stellen der Kommission die für die Erstellung des Berichts erforderlichen Informationen zur Verfügung.

(3) Der in Absatz 2 genannte Durchführungsbericht umfasst Bewertungen

a) der Arbeitskapazität des Kompetenzzentrums hinsichtlich seines Auftrags, seiner Ziele, seines Mandats und seiner Aufgaben sowie der Zusammenarbeit und Koordinierung mit anderen Interessenträgern, insbesondere den nationalen Koordinierungszentren, der Gemeinschaft und der ENISA;

([19]) 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).

([20]) 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).

b) der vom Kompetenzzentrum erzielten Ergebnisse im Hinblick auf seinen Auftrag, seine Ziele, sein Mandat und seine Aufgaben, wobei insbesondere die Effizienz des Kompetenzzentrums bei der Koordinierung der Unionsmittel und bei der Bündelung von Fachwissen bewertet werden;

c) der Kohärenz der Umsetzungsaufgaben mit der Agenda und dem mehrjährigen Arbeitsprogramm;

d) der Abstimmung und der Zusammenarbeit des Kompetenzzentrums mit den Programmausschüssen von „Horizont Europa" und des Programms „Digitales Europa", insbesondere im Hinblick auf die Steigerung von Kohärenz und Synergien mit der Agenda, dem jährlichen Arbeitsprogramm, dem mehrjährigen Arbeitsprogramm, „Horizont Europa" und dem Programm „Digitales Europa";

e) der gemeinsamen Maßnahmen.

(4) Nach Übermittlung des in Absatz 2 des vorliegenden Artikels genannten Durchführungsberichts führt die Kommission eine Bewertung des Kompetenzzentrums durch und berücksichtigt dabei die zuvor eingereichten Beiträge des Verwaltungsrats, der nationalen Koordinierungszentren und der Gemeinschaft. Diese Bewertung nimmt Bezug auf oder aktualisiert gegebenenfalls die in Absatz 3 des vorliegenden Artikels genannten Bewertungen und wird vor Ablauf des in Artikel 47 Absatz 1 festgelegten Zeitraums durchgeführt, damit rechtzeitig festgestellt werden kann, ob es angemessen ist, das Mandat des Kompetenzzentrums über diesen Zeitraum hinaus zu verlängern. Bei dieser Bewertung werden rechtliche und administrative Aspekte des Mandats des Kompetenzzentrums sowie das Potenzial, im Hinblick auf andere Organe, Einrichtungen und sonstige Stellen der Union Synergien zu bewirken und Fragmentierung zu vermeiden, beurteilt.

Ist die Kommission der Ansicht, dass das Fortbestehen des Kompetenzzentrums vor dem Hintergrund seines Auftrags, seiner Ziele, seines Mandats und seiner Aufgaben gerechtfertigt ist, so kann sie einen Gesetzgebungsvorschlag zur Verlängerung der in Artikel 47 festgelegten Bestehensdauer des Kompetenzzentrums vorlegen.

(5) Auf der Grundlage der Schlussfolgerungen aus dem Durchführungsbericht nach Absatz 2 kann die Kommission geeignete Maßnahmen ergreifen.

(6) Die Überwachung, Bewertung, stufenweise Beendigung und Erneuerung des Beitrags aus „Horizont Europa" erfolgen nach Maßgabe der Artikel 10, 50 und 52 der Verordnung (EU) 2021/695 und der vereinbarten Durchführungsmodalitäten.

(7) Die Überwachung, Berichterstattung und Bewertung hinsichtlich des Beitrags aus dem Programm „Digitales Europa" erfolgen nach Maßgabe der Artikel 24 und 25 der Verordnung (EU) 2021/694.

(8) Im Falle einer Abwicklung des Kompetenzzentrums nimmt die Kommission innerhalb von sechs Monaten nach der Abwicklung, spätestens jedoch zwei Jahre nach Einleitung des Abwicklungsverfahrens gemäß Artikel 47 eine abschließende Bewertung des Kompetenzzentrums vor. Die Ergebnisse dieser abschließenden Bewertung werden dem Europäischen Parlament und dem Rat übermittelt.

Artikel 39

Rechtspersönlichkeit des Kompetenzzentrums

(1) Das Kompetenzzentrum besitzt Rechtspersönlichkeit.

(2) Das Kompetenzzentrum verfügt in jedem Mitgliedstaat über die weitestgehende Rechts- und Geschäftsfähigkeit, die Rechtspersonen nach dessen Recht zuerkannt wird. Es kann insbesondere bewegliches und unbewegliches Vermögen erwerben und veräußern und ist vor Gericht parteifähig.

Artikel 40

Haftung des Kompetenzzentrums

(1) Die vertragliche Haftung des Kompetenzzentrums bestimmt sich nach dem für die betreffende Vereinbarung bzw. den betreffenden Beschluss oder Vertrag geltenden Recht.

(2) Im Bereich der außervertraglichen Haftung leistet das Kompetenzzentrum für die von seinem Personal in Wahrnehmung seiner Aufgaben verursachten Schäden Schadenersatz nach den allgemeinen Rechtsgrundsätzen, die den Rechtsordnungen der Mitgliedstaaten gemeinsam sind.

(3) Etwaige Schadenersatzzahlungen des Kompetenzzentrums aufgrund der Haftung gemäß den Absätzen 1 und 2 sowie die damit zusammenhängenden Kosten und Ausgaben gelten als Ausgaben des Kompetenzzentrums und werden aus seinen Mitteln geleistet.

(4) Für die Erfüllung seiner Verpflichtungen haftet ausschließlich das Kompetenzzentrum.

Artikel 41

Zuständigkeit des Gerichtshofs der Europäischen Union und anwendbares Recht

(1) Der Gerichtshof der Europäischen Union ist zuständig

a) für Entscheidungen aufgrund von Schiedsklauseln in vom Kompetenzzentrum gefassten Beschlüssen oder in vom Kompetenzzentrum geschlossenen Vereinbarungen oder Verträgen;

b) für Schadenersatzstreitigkeiten aufgrund eines durch das Personal des Kompetenzzentrums in Wahrnehmung seiner Aufgaben verursachten Schadens;

c) für alle Streitsachen zwischen dem Kompetenzzentrum und seinem Personal im Rahmen und unter den Bedingungen des Statuts der Beamten.

(2) In Angelegenheiten, die nicht durch diese Verordnung oder sonstige Rechtsakte der Union geregelt sind, gilt das Recht des Mitgliedstaats, in dem das Kompetenzzentrum seinen Sitz hat.

Artikel 42

Haftung der Union und der Mitgliedstaaten und Versicherung

(1) Die finanzielle Haftung der Union und der Mitgliedstaaten für die Schulden des Kompetenzzentrums ist auf deren bereits zu den Verwaltungsausgaben geleistete Finanzbeiträge beschränkt.

(2) Das Kompetenzzentrum schließt angemessene Versicherungsverträge und erhält diese aufrecht.

Artikel 43

Interessenkonflikt

Der Verwaltungsrat nimmt in Bezug auf seine Mitglieder, seine Gremien und sein Personal, einschließlich des Exekutivdirektors, Regeln zur Vermeidung, Ermittlung und Beseitigung von Interessenkonflikten an. In diesen Regeln sind Bestimmungen vorzusehen, durch die im Einklang mit der Haushaltsordnung Interessenkonflikte bei den Vertretern der Mitglieder, die einen Sitz im Verwaltungsrat sowie in der ständigen Beratungsgruppe haben, vermieden werden, einschließlich Bestimmungen über Interessenerklärungen. Die nationalen Koordinierungszentren unterliegen im Zusammenhang mit Interessenkonflikten dem nationalen Recht.

Artikel 44

Schutz personenbezogener Daten

(1) Die Verarbeitung personenbezogener Daten durch das Kompetenzzentrum unterliegt der Verordnung (EU) 2018/1725.

(2) Der Verwaltungsrat beschließt Durchführungsbestimmungen nach Artikel 45 Absatz 3 der Verordnung (EU) 2018/1725. Der Verwaltungsrat kann zusätzliche Maßnahmen, die für die Anwendung der genannten Verordnung durch das Kompetenzzentrum erforderlich sind, festlegen.

Artikel 45

Unterstützung seitens des Aufnahmemitgliedstaat

Zwischen dem Kompetenzzentrum und dem Aufnahmemitgliedstaat, in dem es seinen Sitz hat, kann eine Verwaltungsvereinbarung über die Vorrechte und Befreiungen und die sonstige Unterstützung des Kompetenzzentrums seitens dieses Mitgliedstaats geschlossen werden.

KAPITEL VI

Schlussbestimmungen

Artikel 46

Erste Maßnahmen

(1) Die Kommission ist für die Einrichtung und die Aufnahme der Tätigkeit des Kompetenzzentrums verantwortlich, bis dieses über die operativen Kapazitäten zur Ausführung seines eigenen Haushaltsplans verfügt. Die Kommission führt im Einklang mit dem Unionsrecht alle notwendigen Maßnahmen unter Einbeziehung der zuständigen Gremien des Kompetenzzentrums durch.

(2) Für die Zwecke von Absatz 1 des vorliegenden Artikels kann die Kommission einen Interims-Exekutivdirektor benennen, bis der Exekutivdirektor nach seiner Ernennung durch den Verwaltungsrat gemäß Artikel 16 die Amtsgeschäfte aufnimmt. Der Interims-Exekutivdirektor nimmt die Aufgaben des Exekutivdirektors wahr und kann von einer begrenzten Zahl von Bediensteten der Kommission unterstützt werden. Die Kommission kann hierzu eine begrenzte Zahl ihrer Bediensteten übergangsweise an das Kompetenzzentrum abordnen.

(3) Der Interims-Exekutivdirektor kann alle Zahlungen genehmigen, für die im Jahreshaushaltsplan des Kompetenzzentrums Mittel zur Verfügung stehen, nachdem Verwaltungsrats ihn beschlossen hat, und Vereinbarungen und Verträge, einschließlich Arbeitsverträge, schließen und Beschlüsse fassen, nachdem der Stellenplan gemäß Artikel 13 Absatz 3 Buchstabe l angenommen wurde.

(4) Der Interims-Exekutivdirektor bestimmt im Einvernehmen mit dem Exekutivdirektor und vorbehaltlich der Genehmigung des Verwaltungsrats den Tag, ab dem das Kompetenzzentrum über die Kapazität zur Ausführung seines eigenen Haushaltsplans verfügen muss. Ab diesem Tag nimmt die Kommission für die Tätigkeiten des Kompetenzzentrums keine Mittelbindungen mehr vor und führt keine Zahlungen mehr aus.

Artikel 47

Bestehensdauer

(1) Das Kompetenzzentrum wird für den Zeitraum vom 28. Juni 2021 bis zum 31. Dezember 2029 eingerichtet.

(2) Wird das Mandat des Kompetenzzentrums nicht gemäß Artikel 38 Absatz 4 verlängert, wird nach Ende des in Absatz 1 des vorliegenden Artikels genannten Zeitraums automatisch das Abwicklungsverfahren eingeleitet.

(3) Zur Abwicklung des Kompetenzzentrums ernennt der Verwaltungsrat einen oder mehrere Abwicklungsbeauftragte, die seinen Beschlüssen nachkommen.

(4) Bei der Abwicklung des Kompetenzzentrums werden seine Vermögenswerte zur Deckung seiner Verbindlichkeiten und der Kosten seiner Abwicklung verwendet. Etwaige Überschüsse werden proportional zu ihren Finanzbeiträgen auf die Union und die beitragenden Mitgliedstaaten umgelegt, die zum Zeitpunkt der Abwicklung am Kompetenzzentrum beteiligt sind. Etwaige auf die Union umgelegte Überschüsse fließen in den Unionshaushalt zurück.

Artikel 48

Inkrafttreten

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

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

Geschehen zu Brüssel am 20. Mai 2021.

Im Namen des Europäischen Parlaments	*Im Namen des Rates*
Der Präsident	*Die Präsidentin*
D.M. SASSOLI	A.P. ZACARIAS