

BERICHT UND ANTRAG
DER REGIERUNG
AN DEN
LANDTAG DES FÜRSTENTUMS LIECHTENSTEIN
BETREFFEND
**DIE SCHAFFUNG EINES GESETZES ÜBER CYBERSICHERHEIT (CYBER-
SICHERHEITSGESETZ; CSG) SOWIE ABÄNDERUNG DES**
BESCHWERDEKOMMISSIONSGESETZES

(Umsetzung der 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 sowie Durchführung der 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)

<i>Behandlung im Landtag</i>	
	<i>Datum</i>
1. Lesung	
2. Lesung	
Schlussabstimmung	

Nr. 9/2023

INHALTSVERZEICHNIS

	Seite
Zusammenfassung	5
Zuständiges Ministerium.....	5
Betroffene Stellen	6
I. BERICHT DER REGIERUNG	7
1. Ausgangslage	7
2. Begründung der Vorlage.....	9
3. Schwerpunkte der Vorlage	10
3.1 Umsetzung der Richtlinie (EU) 2016/1148.....	10
3.2 Durchführung der Durchführungsverordnung (EU) 2018/151	12
3.3 Durchführung der Verordnung (EU) 2021/887	13
4. Vernehmlassung	13
4.1 Allgemeines	13
4.2 Ergebnisse der Vernehmlassung.....	15
4.2.1 NIS-2-Richtlinie.....	15
4.2.2 Lex specialis im Bereich Cybersicherheit	18
5. Erläuterungen zu den einzelnen Bestimmungen unter Berücksichtigung der Vernehmlassung	25
5.1 Gesetz über Cybersicherheit (Cyber-Sicherheitsgesetz; CSG)	25
5.2 Gesetz über die Abänderung des Beschwerdekommmissionsgesetzes	118
6. Verfassungsmässigkeit / Rechtliches.....	119
7. Auswirkungen auf Verwaltungstätigkeit und Ressourceneinsatz	119
7.1 Neue und veränderte Kernaufgaben	119
7.2 Personelle, finanzielle, organisatorische und räumliche Auswirkungen.....	119
7.3 Betroffene UNO-Nachhaltigkeitsziele und Auswirkungen auf deren Umsetzung	120
7.4 Evaluation.....	123

II. ANTRAG DER REGIERUNG	123
---------------------------------------	------------

III. REGIERUNGSVORLAGE	125
-------------------------------------	------------

Beilagen:

- 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);
- 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);
- 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);
- TOC – Umsetzung der Richtlinie (EU) 2016/1148.

ZUSAMMENFASSUNG

Mit der gegenständlichen Vorlage soll 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 – die sogenannte «NIS-Richtlinie» – ins liechtensteinische Recht umgesetzt werden. 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.

Ebenso werden mit der gegenständlichen Vorlage einzelne Bestimmungen der 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 durchgeführt.

Damit wird in Liechtenstein die Grundlage für das Nationale 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.

ZUSTÄNDIGES MINISTERIUM

Ministerium für Präsidiales und Finanzen

BETROFFENE STELLEN

Stabsstelle Cyber-Sicherheit

Amt für Kommunikation

Datenschutzstelle

Finanzmarktaufsicht Liechtenstein

Landespolizei

Staatsanwaltschaft

Stabsstelle FIU

Gemeinden

Öffentlich-rechtliche Stiftungen und Anstalten

Andere juristische Personen des öffentlichen und privaten Rechts, die überwiegend vom Staat, den Gemeinden oder von anderen Einrichtungen des öffentlichen Rechts finanziert werden oder deren Aufsicht unterliegen.

Vaduz, 31. Januar 2023

LNR 2023-97

P

Sehr geehrter Herr Landtagspräsident,
Sehr geehrte Frauen und Herren Abgeordnete

Die Regierung gestattet sich, dem Hohen Landtag nachstehenden Bericht und Antrag betreffend die Schaffung eines Gesetzes über Cybersicherheit zu unterbreiten.

I. **BERICHT DER REGIERUNG**

1. **AUSGANGSLAGE**

Mit der 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 – die sogenannte «NIS-Richtlinie» – werden Massnahmen festgelegt, mit denen ein hohes gemeinsames Sicherheitsniveau von Netz- und Informationssystemen im EWR erreicht werden soll, um so das Funktionieren des Binnenmarkts zu verbessern. Zu diesem Zweck sieht die Richtlinie (EU) 2016/1148 Folgendes vor:

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

- die Schaffung einer Kooperationsgruppe, um die strategische Zusammenarbeit und den Informationsaustausch zwischen den EWR-Mitgliedstaaten zu erleichtern und den Aufbau von Vertrauen zwischen ihnen zu unterstützen;
- die Schaffung eines Netzwerks von Computer-Notfallteams (CSIRTs-Netzwerk — Computer Security Incident Response Teams Network), um zum Aufbau von Vertrauen zwischen den EWR-Mitgliedstaaten beizutragen und eine rasche und wirksame operative Zusammenarbeit zu fördern;
- Sicherheitsanforderungen und Meldepflichten für die Betreiber wesentlicher Dienste und für Anbieter digitaler Dienste;
- die Pflicht der EWR-Mitgliedstaaten, nationale zuständige Behörden, zentrale Anlaufstellen und sogenannte Computer-Notfallteams (CSIRTs) mit Aufgaben im Zusammenhang mit der Sicherheit von Netz- und Informationssystemen zu betrauen.

Die Verantwortung für die Gewährleistung der Sicherheit von Netz- und Informationssystemen liegt in erheblichem Masse bei den Betreibern wesentlicher Dienste und den Anbietern digitaler Dienste. Durch geeignete rechtliche Anforderungen soll eine Risikomanagementkultur gefördert und entwickelt werden, die unter anderem die Risikobewertung und die Anwendung von Sicherheitsmassnahmen, die den jeweiligen Risiken angemessen sind, umfasst.

Mit der Durchführung der 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 wird in Liechtenstein die rechtliche Grundlage für das Nationale Koordinierungszentrum Cybersicherheit geschaffen, welches als Teil des EWR-weiten Netzwerks

nationaler Koordinierungszentren zusammen mit dem Europäischen Kompetenzzentrum für Cybersicherheit (ECCC) den neuen Rahmen im EWR zur Unterstützung der Innovations- und Industriepolitik im Bereich der Cybersicherheit bildet. Das nationale Koordinierungszentrum muss auf dem Gebiet der Cybersicherheit entweder über Fachwissen in Forschung und Technologie verfügen oder direkten Zugang dazu haben. Die nationalen Koordinierungszentren sollen hinreichende Kapazitäten und Verbindungen zu bestehenden Initiativen und nationalen Cyberkreisen aufbauen. Sie sind in der Lage, sich wirksam mit der Industrie, Wissenschaft und Forschung, den Einwohnerinnen und Einwohnern, dem öffentlichen Sektor sowie den zuständigen Stellen und Behörden auszutauschen und abzustimmen und können direkte EU-Finanzhilfen erhalten.

2. BEGRÜNDUNG DER VORLAGE

Die gegenständliche Vorlage dient der Umsetzung der Richtlinie (EU) 2016/1148 (NIS-Richtlinie) ins liechtensteinische Recht. 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. Mit der gegenständlichen Vorlage kommt Liechtenstein seiner Verpflichtung aus dem EWR-Abkommen nach.

Die Richtlinie (EU) 2016/1148 befindet sich derzeit noch im Übernahmeverfahren ins EWR-Abkommen. Die Unterzeichnung des entsprechenden EWR-Übernahmebeschlusses ist für 3. Februar 2023 vorgesehen.

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 die Verordnung (EU) 2021/887 Bestimmungen, die sich unmittelbar an die EWR-Mitgliedstaaten richten und daher eine Durchführung im nationalen Recht erfordern.

Das durch die Verordnung (EU) 2021/887 eingesetzte Europäische Kompetenzzentrum nimmt eine tragende Rolle bei der Umsetzung der Cybersicherheitskomponente des Programms «Digitales Europa», insbesondere im Hinblick auf Massnahmen im Zusammenhang mit Art. 6 der Verordnung (EU) 2021/694, ein. Liechtenstein nimmt am Programm «Digitales Europa» in der Programmperiode 2021-2027 teil. Durch die zeitnahe Übernahme der Verordnung (EU) 2021/887 ins EWR-Abkommen und deren Durchführung im liechtensteinischen Recht erhält Liechtenstein die Möglichkeit, am Europäischen Kompetenzzentrum für Industrie, Technologie und Forschung im Bereich der Cybersicherheit (ECCC), dem Netzwerk nationaler Koordinierungszentren sowie an Ausschreibungen für Fördermittel, teilzunehmen.

3. SCHWERPUNKTE DER VORLAGE

Zur Umsetzung der Richtlinie (EU) 2016/1148 und der Durchführung der Verordnung (EU) 2021/887 wird die Schaffung eines neuen Gesetzes, konkret des Cyber-Sicherheitsgesetzes (kurz «CSG»), vorgeschlagen.

3.1 Umsetzung der Richtlinie (EU) 2016/1148

Die gegenständliche Vorlage orientiert sich hinsichtlich des Aufbaus und der Wortwahl weitgehend an der Richtlinie (EU) 2016/1148.

Die Vorlage enthält in Kapitel I. zunächst allgemeine Bestimmungen und Begriffsbestimmungen, welche sich unmittelbar an der Richtlinie (EU) 2016/1148 orientieren.

Im Kapitel II. finden sich die Sicherheitsanforderungen und Meldepflichten. So haben Betreiber wesentlicher Dienste als auch Anbieter digitaler Dienste geeignete und verhältnismässige technische und organisatorische Massnahmen zu 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, welches dem bestehenden Risiko angemessen ist. Sicherheitsvorfälle sind durch die Betreiber wesentlicher Dienste und Anbieter digitaler Dienste in bestimmten Situationen und Umständen zu melden.

In Kapitel III. werden in Abschnitt A (Allgemeines) unter anderem die Zuständigkeiten geregelt. Im selben Abschnitt finden sich weiters Bestimmungen zur Verarbeitung personenbezogener Daten (Datenschutzbestimmungen). In Abschnitt B wird die Stabsstelle Cyber-Sicherheit als zuständige nationale Behörde gemäss Art. 8 Abs. 1 der Richtlinie (EU) 2016/1148 sowie als zuständige zentrale Anlaufstelle gemäss Art. 8 Abs. 3 der Richtlinie (EU) 2016/1148 bestimmt. Ebenso werden im erwähnten Abschnitt die Aufgaben und Befugnisse als auch der Betrieb von Informations- und Kommunikationstechnik-Lösungen (IKT-Lösungen) geregelt. So obliegt der Stabsstelle Cyber-Sicherheit unter anderem die Aufsicht und der Vollzug dieses Gesetzes. Ebenso ist die Stabsstelle Cyber-Sicherheit die Verbindungsstelle zur Gewährleistung der grenzüberschreitenden Zusammenarbeit mit internationalen Gremien und Gruppen, wie insbesondere den zuständigen Stellen in den EWR-Mitgliedstaaten sowie der Kooperationsgruppe und dem CSIRT-Netzwerk. Der Stabsstelle Cyber-Sicherheit

werden zur Erfüllung ihrer Aufgaben entsprechende Befugnisse eingeräumt. So kann die Stabsstelle Cyber-Sicherheit beispielsweise Kontrollen zur Einhaltung der Anforderungen an die Cybersicherheit durchführen oder von beauftragten qualifizierten Dritten durchführen lassen.

Wie im Abschnitt C geregelt, wird bei der Stabsstelle Cyber-Sicherheit zur Gewährleistung der Sicherheit von Netz- und Informationssystemen ein Computer-Notfallteam (CSIRT) eingerichtet.

Im Abschnitt D zu Kapitel III. wird schliesslich die sogenannte NIS-Strategie geregelt.

Abschliessend enthält die Vorlage in Kapitel IV. und Kapitel V. noch Regelungen zu Rechtsmitteln sowie die Strafbestimmungen.

Die Schlussbestimmung über das Inkrafttreten findet sich schliesslich in Kapitel VI.

3.2 Durchführung der Durchführungsverordnung (EU) 2018/151

Gemäss der Richtlinie (EU) 2016/1148 steht es den Anbietern digitaler Dienste frei, technische und organisatorische Massnahmen zu ergreifen, die sie zur Bewältigung der Risiken für die Sicherheit ihrer Netz- und Informationssysteme für angemessen und verhältnismässig halten, sofern diese Massnahmen ein angemessenes Sicherheitsniveau gewährleisten und den in der Richtlinie vorgesehenen Elementen Rechnung tragen.

In der Durchführungsverordnung (EU) 2018/151 werden die Elemente näher festgelegt, die die Anbieter digitaler Dienste zu berücksichtigen haben, wenn sie Massnahmen ermitteln und ergreifen, die ein bestimmtes Sicherheitsniveau der Netz- und Informationssysteme gewährleisten, die sie im Rahmen der Bereitstellung der in Anhang III der Richtlinie (EU) 2016/1148 genannten Dienste nutzen. Ferner werden die Parameter näher festgelegt, die bei der Feststellung

zugrunde zu legen sind, ob ein Sicherheitsvorfall erhebliche Auswirkungen auf die Bereitstellung dieser Dienste hat.

3.3 Durchführung der Verordnung (EU) 2021/887

Mit der Verordnung (EU) 2021/887 werden das Europäische Kompetenzzentrum für Industrie, Technologie und Forschung im Bereich der Cybersicherheit (ECCC) sowie das Netzwerk nationaler Koordinierungszentren (NCC) eingerichtet. Die Verordnung (EU) 2021/887 legt Bestimmungen für die Benennung nationaler Koordinierungszentren sowie Bestimmungen für die Einrichtung der Kompetenzgemeinschaft für Cybersicherheit fest.

Das Kompetenzzentrum nimmt eine tragende Rolle bei der Umsetzung der Cybersicherheitskomponente des Programms «Digitales Europa» ein. Liechtenstein nimmt am Programm Digitales Europa (2021-2027) teil (BuA 124/2020, S. 47 ff.). Der Landtag hat die Teilnahme Liechtensteins in seiner Sitzung am 2. Dezember 2020 beschlossen.

4. VERNEHMLASSUNG

4.1 Allgemeines

Mit Entscheidung vom 12. Juli 2022 hat die Regierung den Vernehmlassungsbericht betreffend die Schaffung eines Gesetzes über Cybersicherheit (Cyber-Sicherheitsgesetz; CSG) an nachfolgende Vernehmlassungsteilnehmer zur Stellungnahme bis zum 28. September 2022 übermittelt:

- alle Gemeinden
- Crypto Country Association
- Finanzmarktaufsicht Liechtenstein

- FL 1 (Telecom Liechtenstein AG)
- Gruppenwasserversorgung Liechtensteiner Oberland
- Landesspital Liechtenstein
- Liechtensteinische Alters- und Krankenhilfe
- Liechtensteinischer Anlagefondsverband
- Liechtensteinischer Bankenverband
- Liechtensteinische Industrie- und Handelskammer
- Liechtensteinische Kraftwerke
- Liechtensteinische Rechtsanwaltskammer
- Liechtensteinische Treuhandkammer
- Liechtensteiner Versicherungsverband
- Liechtenstein Wärme
- Verein unabhängiger Vermögensverwalter
- Wasserversorgung Liechtensteiner Unterland
- Wirtschaftskammer Liechtenstein

Auf eine Stellungnahme ausdrücklich verzichtet haben die FL 1 (Telecom Liechtenstein AG), die Gemeinden Balzers, Eschen-Nendeln, Gamprin, Mauren, Planken, Ruggell, Schaan, Triesen und Vaduz, die Liechtensteinische Treuhandkammer, Liechtenstein Wärme sowie die Wirtschaftskammer Liechtenstein.

Zum Vernehmlassungsbericht konkret geäußert haben sich die Beschwerdekommision für Verwaltungsangelegenheiten, die Finanzmarktaufsicht Liechtenstein, der Liechtensteinische Anlagefondsverband, die Liechtensteinische Alters- und Krankenhilfe, der Liechtensteinischer

Bankenverband, die Liechtensteinischen Kraftwerke, die Liechtensteinische Rechtsanwaltskammer, die NetSec.co AG sowie der Verein unabhängiger Vermögensverwalter.

4.2 Ergebnisse der Vernehmlassung

Im Allgemeinen wurde die Vernehmlassungsvorlage positiv aufgenommen und die Vorlage generell begrüsst. Nachfolgend werden die wesentlichen Anmerkungen der Vernehmlassungsteilnehmer kurz dargelegt.

4.2.1 NIS-2-Richtlinie

Der **Liechtensteinische Bankenverband** und die **Finanzmarktaufsicht Liechtenstein** fragen sich, weshalb nach Jahren der Nicht-Umsetzung der Richtlinie (EU) 2016/1148 («NIS-1-Richtlinie») nunmehr dieser Standard übernommen und umgesetzt wird. Bereits seit Dezember 2020 sei der Entwurf der sogenannten NIS-2-Richtlinie verfügbar. Dies sei umso mehr fraglich, als die NIS-2-Richtlinie keine reine Änderungsrichtlinie darstellt, sondern die Richtlinie (EU) 2016/1148 vollständig ersetzt und aufhebt.

Dies gelte für den Sektor Bankwesen auch im Hinblick auf die Verordnung über die Betriebsstabilität digitaler Systeme des Finanzsektors (Digital Operational Resilience Act; «DORA») bzw. zur Regelung der digitalen Betriebsstabilität im Finanzbereich¹, der in weiten Teilen der NIS/NIS-2-Richtlinie für den Bankenbereich als Lex specialis vorgehen wird.

¹ Die Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über die digitale operationale Resilienz im Finanzsektor und zur Änderung der Verordnungen (EG) Nr. 1060/2009, (EU) Nr. 648/2012, (EU) Nr. 600/2014, (EU) Nr. 909/2014 und (EU) 2016/1011 («DORA») wurde am 27. Dezember 2022 im Amtsblatt der Europäischen Union publiziert (ABl. L 333 vom 27.12.2022, S. 1). Die Verordnung (EU) 2022/2554 wird in den EU-Staaten ab dem 17. Januar 2025 gelten.

Die Regierung führt dazu aus, dass das EWR-Übernahmeverfahren zur Richtlinie (EU) 2016/1148 bereits seit dem Jahr 2016 anhängig ist. Aus unterschiedlichen Gründen hat sich die Übernahme der Richtlinie (EU) 2016/1148 in das EWR-Abkommen immer wieder verzögert. Erst am 3. Februar 2023 soll der entsprechende EWR-Übernahmebeschluss vom Gemeinsamen EWR-Ausschuss unterzeichnet werden. Die Richtlinie (EU) 2016/1148 ist EWR-relevant. Liechtenstein ist daher zur Umsetzung der Richtlinie (EU) 2016/1148 aufgrund seiner EWR-Mitgliedschaft verpflichtet.

Die Richtlinie (EU) 2016/1148 war in den EU-Mitgliedstaaten bis zum 9. Mai 2018 umzusetzen. In den EWR/EFTA-Staaten gilt das Inkrafttreten des entsprechenden EWR-Übernahmebeschlusses als Umsetzungsfrist für die Richtlinie (EU) 2016/1148.

Die Richtlinie (EU) 2022/2555 («NIS-2-Richtlinie»)² sowie die Verordnung (EU) 2022/2554 («DORA») wurden zwar mittlerweile im Amtsblatt der Europäischen Union publiziert. Die Richtlinie (EU) 2022/2555 ist in den EU-Mitgliedstaaten bis zum 17. Oktober 2024 umzusetzen, die Verordnung (EU) 2022/2554 wird in den EU-Staaten ab dem 17. Januar 2025 gelten.

Bis wann die Richtlinie (EU) 2022/2555 sowie die Verordnung (EU) 2554 in das EWR-Abkommen übernommen werden können und damit in den EWR/EFTA-Staaten in Kraft treten, ist derzeit nicht absehbar.

Folglich erachtet es die Regierung für erforderlich, zum jetzigen Zeitpunkt mit der Umsetzung der NIS-1-Richtlinie durch den Erlass eines Gesetzes über die

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

Cybersicherheit die erforderlichen rechtlichen Grundlagen in Liechtenstein zu schaffen. So sollen mit der gegenständlichen Vorlage insbesondere die Rechtsgrundlagen für den Betrieb der mit der nationalen Strategie für Liechtenstein zum Schutz vor Cyber-Risiken neu geschaffenen Stabsstelle Cyber-Sicherheit geschaffen werden.

Die Umsetzung der Richtlinie (EU) 2016/1148 eröffnet der Stabsstelle Cyber-Sicherheit zudem den wichtigen und zeitnahen Zugang zum CSIRT-Netzwerk und der NIS-Kooperationsgruppe sowie anderen einschlägigen Gremien in der EU.

Zum Zeitpunkt der Vernehmlassung (Juli bis September 2022) bzw. zum Zeitpunkt der Entscheidung in Bezug auf die Übernahme der Richtlinie im April 2022 war der finale Text der NIS-2-Richtlinie noch nicht verfügbar und es war auch nicht absehbar, bis wann diese im Gesetzgebungsverfahren der EU endgültig beschlossen werden wird. Gerade die Erfahrungen von europäischen Gesetzgebungsverfahren in vergleichbaren Gebieten zeigen deutlich, dass sich kurz vor der Veröffentlichung geglaubte Rechtsakte über Jahre verzögern können.

Hätte Liechtenstein mit der Umsetzung auf die NIS-2-Richtlinie gewartet, wäre die Rechtsgrundlage für die Stabsstelle Cyber-Sicherheit nicht vor Jahresende 2024 zu erwarten. Der zur Aufgabenerfüllung wichtige Zugang zu den erwähnten Gremien der EU bliebe der Stabsstelle Cyber-Sicherheit bis dahin verwehrt.

Mit der Umsetzung der Richtlinie (EU) 2016/1148 wird deshalb wertvolle Zeit gewonnen, in der die Stabsstelle Cyber-Sicherheit ihre Aufgaben wahrnehmen kann, nämlich insbesondere den betroffenen Stellen in Liechtenstein im konkreten Anlassfall als Anlaufstelle zur Verfügung zu stehen und Liechtenstein im Bereich der Cyber-Sicherheit gegenüber den Institutionen der EU sowie des EWR zu vertreten.

Gerade die jüngsten Entwicklungen im Bereich Cyber-Sicherheit haben gezeigt, dass dieses Thema sowohl national als auch international von höchster Brisanz ist und daher eine rasche Schaffung der entsprechenden Rechtsgrundlagen dringend geboten ist.

4.2.2 Lex specialis im Bereich Cybersicherheit

Gerade in den Stellungnahmen des **Liechtensteinischen Bankenverbands** sowie der **Finanzmarktaufsicht Liechtenstein** finden sich mehrere Hinweise auf die Berücksichtigung und Anwendung von Spezialgesetzen im Bereich der Cybersicherheit für die Sektoren Bankenwesen und Finanzmarktinfrastrukturen sowie damit verbundene Ersuchen um weitere Ausführungen dazu.

So führt der **Liechtensteinische Bankenverband** beispielsweise in seiner Stellungnahme zur Vernehmlassung aus, dass der Finanzsektor ein stark regulierter Sektor mit strengen Sicherheitsstandards in verschiedenen Bereichen sei, vor allem in Bezug auf Cybersicherheit und Widerstandsfähigkeit. Es wird seitens des Liechtensteinische Bankenverband dringend angeregt, die Wechselwirkung der verschiedenen Vorgaben im Hinblick auf den Charakter der gegenständlichen Vorlage als Rahmengesetz nochmals zu prüfen, um Duplizitäten oder abweichende Pflichten zu vermeiden. Dazu verweist der Liechtensteinische Bankenverband unter anderem auf die Zahlungsdiensterichtlinie (Payment Services Directive 2, PSD2) sowie auf die zugehörigen technischen Regulierungsstandards zur Strong Customer Authentication (SCA), welche Vorgaben betreffend wirksame Verfahren zur Aufdeckung, Klassifizierung und Handhabung von Vorfällen einschliesslich schwerer Betriebs- und Sicherheitsvorfälle im Zahlungsverkehr sowie deren Meldung an die Finanzmarktaufsicht Liechtenstein vorsehen.

Ebenso weist die **Finanzmarktaufsicht Liechtenstein** in ihrer Stellungnahme auf die Leitlinien der Europäischen Bankenaufsichtsbehörde (EBA) zum IKT- und Sicherheitsrisikomanagement (EBA/GL/2019/04) sowie die entsprechende FMA-Richtlinie 2021/03 hin, welche die Banken einzuhalten haben. Zudem gäbe es bereits Mindestanforderungen an das Risikomanagement und die aufsichtsrechtlichen Anforderungen an die IT, welche ebenfalls Sicherheitsanforderungen an die Banken, die gleichzeitig Betreiber wesentlicher Dienste i.S.d. gegenständlichen Gesetzesentwurfs seien, regeln. Darüber hinaus würden für digitale Zahlungsprodukte, insbesondere für Kartenzahlungen von Kreditkartenunternehmen, internationale Standards wie der Payment Card Industry Data Security Standard (PCI DSS) gelten.

Betreffend die Meldepflicht geht der **Liechtensteinische Bankenverband** in seiner Stellungnahme davon aus, dass schwere Sicherheitsvorfälle i.S.d. Art. 101 f. Zahlungsdienstegesetz (ZDG) in der Regel auch meldepflichtige Sicherheitsvorfälle nach Art. 5 an die Stabsstelle Cyber-Sicherheit begründen.

Die **Finanzmarktaufsicht Liechtenstein** sieht gemäss eigener IKT-Richtlinie zwar eine Meldepflicht für sämtliche von der Finanzmarktaufsicht Liechtenstein beaufsichtigten Finanzintermediäre vor, allerdings nur im Hinblick auf schwerwiegende oder betriebsstörende Cyber-Attacken. Das Cyber-Sicherheitsgesetz gehe hier laut Finanzmarktaufsicht Liechtenstein weiter als die FMA-Richtlinie.

Zusammengefasst kann aus den Stellungnahmen des **Liechtensteinischen Bankenverbandes** und der **Finanzmarktaufsicht Liechtenstein** festgehalten werden, dass es von zentraler Bedeutung ist, dass die Sicherheitsanforderungen sowie die Anforderungen an die Meldepflichten nach Sicherheitsvorfällen derart geregelt sind, dass es keine Widersprüche gibt und unnötige Mehraufwände vermieden werden. Ebenso sei eine einheitliche Aufsicht bzw. Koordination der

zuständigen Behörden, Finanzmarktaufsicht Liechtenstein und Stabsstelle Cyber-Sicherheit aus Sicht des Liechtensteinischen Bankenverbandes sicherzustellen.

Die Regierung führt dazu aus, dass die Lex specialis Bestimmung gemäss Art. 1 Abs. 7 der Richtlinie (EU) 2016/1148 in der gegenständlichen Vorlage entsprechend berücksichtigt wurde. So bestimmt die gegenständliche Gesetzesvorlage beispielsweise in Art. 4 Abs. 4 und Art. 5 Abs. 6, dass wenn eine spezialgesetzliche Bestimmung den Betreibern wesentlicher Dienste Sicherheitsanforderungen und/oder Meldepflichten auferlegt, die in ihrer Wirkung den in diesem Gesetz respektive der Richtlinie (EU) 2016/1148 enthaltenen Pflichten mindestens gleichwertig sind, die Verpflichtungen nach Massgabe des besonderen Rechtsakts gelten.

Bei der Bewertung der Gleichwertigkeit sektorspezifischer Rechtsvorschriften mit den einschlägigen Bestimmungen sollte der Frage, ob die Sicherheitsanforderungen in den sektorspezifischen Rechtsvorschriften Massnahmen zur Gewährleistung der Sicherheit von Netz- und Informationssystemen gemäss Art. 4 Abs. 1 bis 3 umfassen, besondere Bedeutung beigemessen werden.

Im Hinblick auf die Meldepflichten ist in Art. 5 Abs. 1 vorgesehen, dass Betreiber wesentlicher Dienste der Stabsstelle Cyber-Sicherheit Sicherheitsvorfälle, die erhebliche Auswirkungen auf die Bereitstellung ihrer Dienste haben, unverzüglich melden.

Wie vom Liechtensteinischen Bankenverband und der Finanzmarktaufsicht Liechtenstein in deren Stellungnahme zur Vernehmlassung ausgeführt, ergeben sich im Hinblick auf die Betreiber wesentlicher Dienste in den Sektoren Bankwesen und Finanzmarktinfrastrukturen Sicherheitsanforderungen und/oder Meldepflichten aus sektorspezifischen (EU-)Rechtsvorschriften.

In Bezug auf den Sektor Bankwesen, insbesondere was die Bereitstellung von Zahlungsdiensten durch Kreditinstitute im Sinne von Art. 4 Nr. 1 der Verordnung (EU) Nr. 575/2013 betrifft, enthält die so genannte zweite Zahlungsdiensterichtlinie (PSD2) in den Art. 95 und 96 Sicherheitsanforderungen und Meldepflichten.

Genauer gesagt müssen Zahlungsdienstleister – wie auch vom Liechtensteinischen Bankenverband in deren Stellungnahme ausgeführt – gemäss Art. 95 Abs. 1 PSD2 angemessene Risikominderungsmaßnahmen und Kontrollmechanismen zur Beherrschung der operationellen und der sicherheitsrelevanten Risiken im Zusammenhang mit den von ihnen erbrachten Zahlungsdiensten ergreifen. Diese Massnahmen umfassen die Festlegung und Anwendung wirksamer Verfahren für das Management von Vorfällen – auch zur Aufdeckung und Klassifizierung schwerer Betriebs- und Sicherheitsvorfälle. Die Art dieser Sicherheitsmassnahmen wird in den Erwägungsgründen 95 und 96 der PSD2 weiter präzisiert. Aus diesen Bestimmungen geht hervor, dass die vorgeschriebenen Massnahmen auf die Beherrschung der Risiken im Zusammenhang mit den zur Bereitstellung von Zahlungsdiensten verwendeten Netz- und Informationssystemen ausgerichtet sind. Diese Sicherheitsanforderungen können daher als in ihrer Wirkung den entsprechenden Vorgaben von Art. 4 Abs. 1 bis 3 der gegenständlichen Gesetzesvorlage mindestens gleichwertig betrachtet werden.

In Bezug auf die Meldepflichten ist in Art. 96 Abs. 1 PSD2 vorgesehen, dass die Zahlungsdienstleister im Falle eines schwerwiegenden Sicherheitsvorfalls unverzüglich die zuständige Behörde unterrichten. Diese Verpflichtung bedeutet gleichzeitig, dass die Meldung des Sicherheitsvorfalls bestimmte Informationen umfassen muss, die es der zuständigen Behörde gestatten, beispielsweise die grenzüberschreitenden Auswirkungen eines Vorfalls zu beurteilen. Gemäss Art. 96 Abs. 3 Bst. a PSD2 ist die Europäische Bankenaufsichtsbehörde (EBA) in

Zusammenarbeit mit der Europäischen Zentralbank (EZB) in diesem Zusammenhang ermächtigt, Leitlinien über den genauen Inhalt und das Format der Meldung herauszugeben.

Daraus folgt, dass gemäss Art. 5 Abs. 6 für die Bereitstellung von Zahlungsdiensten durch Kreditinstitute die Sicherheitsanforderungen sowie Meldepflichten gemäss den Art. 95 und Art. 96 PSD2 anstelle der entsprechenden Vorschriften der Art. 4 und Art. 5 der gegenständlichen Vorlage gelten.

Die **Finanzmarktaufsicht Liechtenstein** würde in ihrer Stellungnahme die enge Zusammenarbeit und den engen Austausch zwischen der Finanzmarktaufsicht Liechtenstein und der Stabsstelle Cyber-Sicherheit begrüssen. Gleichzeitig lasse die Vorlage jedoch Details und klare Vorgaben zur Kompetenzverteilung offen, sodass nicht nachvollziehbar sei, wie dies konkret geplant ist. Dies beziehe sich auf den Informations- und Datenaustausch ebenso, wie auf die Frage der Befugnisse gegenüber den Betreibern und der Durchführung von Kontrollen – sei es durch die Finanzmarktaufsicht Liechtenstein selbst oder durch die von ihr beauftragten Revisionsstellen.

Dem **Liechtensteinischen Bankenverband** erscheint die weitgehende Kontrollkompetenz der Stabsstelle neben der aufsichtsrechtlichen Prüfkompetenz der Finanzmarktaufsicht Liechtenstein fraglich. Die Kontroll- und Einsichtskompetenz kann laut Liechtensteinischem Bankenverband nur soweit reichen, als im stark regulierten Finanzdienstleistungsbereich überhaupt noch ein Anwendungsbereich des Cyber-Sicherheitsgesetzes verbleibt. Eine Überwachungs- und Überprüfungskompetenz für die Einhaltung des Cyber-Sicherheitsgesetzes durch Betreiber wesentlicher Dienste mache jedoch nur dort Sinn, wo nicht bereits aufgrund der spezialgesetzlichen Zuständigkeit der Aufsichtsbehörden oder anderer zuständiger Behörden entsprechende Kontrollen durchgeführt werden. Der Liechtensteinische Bankenverband bittet um Prüfung,

inwieweit nicht die Kompetenz zur Überwachung der regulatorischen Anforderungen im Bereich Netz- und Informationssystemsicherheit für Banken zentral bei der Finanzmarktaufsicht Liechtenstein liegen sollte.

Dazu wird ausgeführt, dass mit den Kontrollen gemäss Art. 18 vor allem die Einhaltung der Sicherheitsanforderungen nach Art. 4 sowie der Meldepflichten nach Art. 5 für Betreiber wesentlicher Dienste sowie Art. 6 und Art. 7 für die Anbieter digitaler Dienste überprüft werden sollen. Da jedoch – wie zuvor ausgeführt – in Bezug auf die Sicherheitsanforderungen sowie die Meldepflichten für die Sektoren Bankwesen und Finanzmarktinfrastrukturen nach Art. 4 Abs. 4 und Art. 5 Abs. 6 der gegenständlichen Gesetzesvorlage nicht anwendbar sind (Lex specialis), besteht nach Auffassung der Regierung für die Stabsstelle Cyber-Sicherheit auch keine Befugnis zur Durchführung von Kontrollen nach Art. 18 im erwähnten Sektor.

Der **Liechtensteinische Bankenverband** regt in seiner Stellungnahme zur Vernehmlassung an, seitens der Stabsstelle Cyber-Sicherheit gemeinsam mit der Finanzmarktaufsicht Liechtenstein und der Datenschutzstelle vor Einführung des Gesetzes für den Sektor Bankwesen eine Auslegeordnung hinsichtlich der Überschneidungen mit der PSD2 (ZDG), eIDAS-VO (SigVG), DSGVO (DSG), anerkannten (internationalen) Standards (z.B. ISO 27001/27002, NIST, MaRisk/BIAT etc.), den aufsichtsrechtlichen Vorgaben der europäischen Bankenaufsichtsbehörde EBA bzw. der Finanzmarktaufsicht Liechtenstein im Bereich IKT-Sicherheit und Cybersicherheit sowie inskünftig NIS-2, DORA und der Critical Entities Resilience Directive (CER), welche die Resilienz kritischer Infrastrukturen gegenüber nicht-cyberbedingten Bedrohungen regelt, vorzunehmen.

Die Zusammenarbeit zwischen der Stabsstelle Cyber-Sicherheit, der Finanzmarktaufsicht Liechtenstein und der Datenschutzstelle wird mit Art. 13 Abs.

1 Bst. i der Gesetzesvorlage adressiert. Die entsprechenden Grundlagen für die Zusammenarbeit zwischen diesen Stellen werden unter Federführung der Stabsstelle Cyber-Sicherheit erarbeitet werden. Die Grundlagen können in Form von Vereinbarungen zwischen den beteiligten Stellen ausgestaltet sein als auch – wo erforderlich oder zweckmässig – in die Verordnung zur gegenständlichen Gesetzesvorlage mit aufgenommen werden. Die Verordnungskompetenz findet sich in Art. 13 Abs. 3.

Die Regierung erachtet den Austausch mit der Finanzmarktaufsicht Liechtenstein sowie der Datenschutzstelle für essentiell, um eine umfassende Aufsicht im Bereich der Cyber-Sicherheit garantieren zu können.

Überdies ist es der Regierung ein Anliegen, den Aufwand für die Banken sowie alle übrigen von der gegenständlichen Gesetzesvorlage umfassten Stellen so gering als möglich zu halten.

Der **Liechtensteinische Bankenverband** führt weiters aus, dass ein Anschluss einzelner oder aller liechtensteinischer Banken an den Verein «Swiss Financial Sector Cyber Security Centre» (Swiss FS-CSC) mit dem Ziel des Informationsaustausches und der Zusammenarbeit unter seinen Mitgliedern und Affiliates zur Verbesserung der Cyberresilienz im Hinblick auf die datenschutz- und strafrechtliche Konformität zu prüfen wäre.

Die Regierung unterstützt die Bestrebungen seitens des Liechtensteinischen Bankenverbands im Hinblick auf eine Zusammenarbeit mit dem Verein Swiss FS-CSC. Das damit verfolgte Ziel einer funktionierenden grenzüberschreitenden Zusammenarbeit wird ebenfalls begrüsst. Welche Anforderungen an eine Mitgliedschaft der Banken im Swiss FS-CSC bestehen und welche allfälligen rechtlichen Hürden dabei auftreten könnten, soll von der Stabsstelle Cyber-

Sicherheit gemeinsam mit dem Liechtensteinischen Bankenverband analysiert werden.

5. ERLÄUTERUNGEN ZU DEN EINZELNEN BESTIMMUNGEN UNTER BERÜCKSICHTIGUNG DER VERNEHMLASSUNG

5.1 Gesetz über Cybersicherheit (Cyber-Sicherheitsgesetz; CSG)

I. Allgemeine Bestimmungen

Zu Art. 1 – Gegenstand und Geltungsbereich

In Art. 1 werden der Gegenstand und der Geltungsbereich des Gesetzes festgelegt. Netz- und Informationssysteme spielen eine zentrale Rolle für das Funktionieren des staatlichen Gemeinwesens. Die Sicherstellung ihrer Verlässlichkeit und Sicherheit ist deshalb von grosser Bedeutung und mit entsprechenden Massnahmen soll ein hohes, dem Risiko angemessenes Sicherheitsniveau von Netz- und Informationssystemen erreicht werden.

Der Anwendungsbereich des Gesetzes umfasst gemäss **Abs. 1** neben Betreibern wesentlicher Dienste (Art. 3 Abs. 1 Bst. e) ebenso Anbieter digitaler Dienste (Art. 3 Abs. 1 Bst. g). Die Art. 1 und 2 der Gesetzesvorlage wurden seit der Vernehmlassung redaktionell angepasst und umgestellt, bleiben inhaltlich jedoch unverändert.

Bei den Betreibern wesentlicher Dienste wird der Anwendungsbereich gemäss **Abs. 1 Bst. a** auf die Sektoren gemäss Anhang II der Richtlinie (EU) 2016/1148 in Spalte 1 eingeschränkt, sprich auf die Sektoren Energie, Verkehr, Bankwesen, Finanzmarktinfrastrukturen, Gesundheitswesen, Trinkwasserlieferung und -versorgung und Digitale Infrastruktur. Das gegenständliche Gesetz verfolgt somit einen eingeschränkten Ansatz und verlangt nur von Betreibern wesentlicher

Dienste in den zuvor erwähnten Sektoren ein hohes, dem Risiko angemessenes Sicherheitsniveau von Netz- und Informationssystemen.

Der **Verein unabhängiger Vermögensverwalter in Liechtenstein** merkt in seiner Stellungnahme zur Vernehmlassungsvorlage an, dass das Thema Cyber-Sicherheit auch für Vermögensverwaltungsgesellschaften relevant sei. Diese hätten insbesondere die FMA-Richtlinie 2021/3 (Richtlinie IKT-Sicherheit) umzusetzen und dabei ähnliche Pflichten zu erfüllen, wie dies das Cyber-Sicherheitsgesetz vorsieht. Jedoch erachtet der Verein unabhängiger Vermögensverwalter in Liechtenstein eine Klarstellung in der gegenständlichen Gesetzesvorlage für erforderlich, dass Vermögensverwaltungsgesellschaften nicht in dessen Anwendungsbereich fallen.

Inwieweit dieses Gesetz zur Anwendung kommt, ist im konkreten Einzelfall zu prüfen. Gleichzeitig wird auf den Geltungsbereich dieses Gesetzes verwiesen. So gilt dieses Gesetz für Betreiber wesentlicher Dienste in den in Abs. 1 Bst. a aufgeführten Sektoren sowie für Anbieter digitaler Dienste. Was wesentliche Dienste und digitale Dienste im Sinne dieses Gesetzes sind, wird in Art. 3 Abs. 1 Bst. d bzw. Bst. f legal definiert.

Die Regierung kann die Vermögensverwaltungsgesellschaften daher zum jetzigen Zeitpunkt nicht pauschal vom Anwendungsbereich dieses Gesetzes ausschliessen. Vielmehr wird in Abstimmung mit der Stabsstelle Cyber-Sicherheit im konkreten Einzelfall zu prüfen sein, ob ein Anwendungsfall des gegenständlichen Gesetzes vorliegt oder nicht.

Das Unternehmen **NetSec.co AG** führt in seiner Stellungnahme zur Vernehmlassungsvorlage aus, dass geprüft werden sollte, ob Medienhäuser, die die Bevölkerung mit Informationen versorgen, nicht auch zu den wesentlichen Diensten gezählt werden sollten. In Krisenfällen seien sie ein wichtiges Standbein

der Krisenbewältigung und sollten daher vor möglicher Manipulation ausreichend geschützt sein.

Dazu führt die Regierung einleitend aus, dass es sich bei den in Abs. 1 genannten sieben Sektoren Energie, Verkehr, Bankwesen, Finanzmarktinfrastrukturen, Gesundheitswesen, Trinkwasserlieferung und -versorgung sowie Digitale Infrastruktur, um jene handelt, welche im Anhang II der Richtlinie (EU) 2016/1148 gelistet sind. Die Richtlinie (EU) 2017/1148 beschränkt sich auf eine Mindestharmonisierung.

Der Bereich Medien und Rundfunk ist sowohl im Gesetz über den Liechtensteinischen Rundfunk (LRFG) als auch im MedienG bzw. der MedienV geregelt. Ein Versorgungsauftrag ergibt sich aus Art. 6 LRFG sowie aus Art. 80 MedienG. Weiter regelt Art. 8 LRFG, dass der Liechtensteinischen Rundfunk zu jeder Zeit die notwendige und zweckentsprechende Sendezeit [...] zur Verfügung zu stellen hat: a) Landes- und Gemeindebehörden für Aufrufe in Krisen- und Katastrophenfällen und andere wichtige Meldungen an die Allgemeinheit sowie b) Privaten für Aufrufe in begründeten und dringenden Notfällen zur Vermeidung von erheblichen Gefahren für Gesundheit und Leben von Menschen.

Die Funktionsfähigkeit öffentlicher Informations- und Kommunikationstechnologie ist, soweit sie sich auf digitale Infrastrukturen stützt, vom bestehenden Gesetzesentwurf umfasst. (vgl. Art. 1 Abs. 1 Bst. a iVm Art. 3 Abs. 1 Bst. d CSG)

Neben Betreibern wesentlicher Dienste verlassen sich auch zahlreiche Unternehmen bei der Bereitstellung ihrer Dienste auf Dienste von Drittanbietern. Da manche dieser Anbieter digitaler Dienste für ihre Nutzer eine wichtige Ressource darstellen und da derartigen Nutzern möglicherweise nicht in allen Fällen Alternativen zur Verfügung stehen, gilt dieses Gesetz gemäss **Abs. 1 Bst. b** ebenso für die Anbieter derartiger Dienste. Die Sicherheit, Verfügbarkeit und

Verlässlichkeit digitaler Dienste gemäss dieser Gesetzesvorlage sind für das reibungslose Funktionieren vieler Unternehmen von wesentlicher Bedeutung (z. B. Cloud-Computing-Dienst oder Online-Marktplätze). Eine Störung eines solchen digitalen Dienstes könnte die Bereitstellung anderer, von ihnen abhängiger Dienste verhindern und somit wesentliche wirtschaftliche und gesellschaftliche Tätigkeiten in Liechtenstein beeinträchtigen.

Für die Liechtensteinische Landesverwaltung (LLV) ist dieses Gesetz nur in jenen Bereichen anwendbar, in welchen die LLV als Betreiberin wesentlicher Dienste auftritt. Ungeachtet dessen sind auch von der öffentlichen Verwaltung zur Gewährleistung der Sicherheit von Netz- und Informationssystemen nicht zuletzt aufgrund anderer Bestimmungen, wie z. B. dem Datenschutzgesetz (DSG) und der Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung; DSGVO), entsprechende Massnahmen zur Sicherstellung eines angemessenen Sicherheitsniveaus einzuhalten.

Das Gesetz konzentriert sich somit auf besonders kritische Einrichtungen und Infrastrukturen, weshalb es kein «allgemeines Cyber-Sicherheitsgesetz» darstellt.

Gemäss **Abs. 2** gelten die den Betreibern wesentlicher Dienste und den Anbietern digitaler Dienste auferlegten Sicherheitsanforderungen und Meldepflichten nicht für Unternehmen, die den Anforderungen nach Art. 40 und 41 der Richtlinie (EU) 2018/1972 unterliegen (**Bst. a**) sowie für Vertrauensdiensteanbieter, die den Anforderungen nach Art. 19 der Verordnung (EU) Nr. 910/2014 unterliegen (**Bst. b**).

Zu Art. 2

In **Abs. 1** werden jene EWR-Rechtsvorschriften aufgezählt, welche mit der gegenständlichen Vorlage umgesetzt bzw. durchgeführt werden. Dies sind die Richtlinie (EU) 2016/1148 (**Bst. a**) sowie die Verordnung (EU) 2021/887 (**Bst. b**).

Seit dem 1. Februar 2021 erfolgt die Kundmachung des verbindlichen Wortlauts von EWR-Rechtsvorschriften durch eine vereinfachte Publikation und einen direkten Verweis auf das Amtsblatt der Europäischen Union (ABl.). Die Bezugnahme auf die genannten EU-Rechtsakte erfolgt deshalb neu in verkürzter Form. Der Volltitel der Richtlinie sowie deren Fundstelle im ABl. finden sich in der entsprechenden Fussnote.

Die gültige Fassung der EWR-Rechtsvorschriften, auf die in diesem Gesetz Bezug genommen wird, ergibt sich aus der Kundmachung der Beschlüsse des Gemeinsamen EWR-Ausschusses im Liechtensteinischen Landesgesetzblatt nach Art. 3 Bst. k des Kundmachungsgesetzes (**Abs. 2**).

Zu Art. 3

In **Abs. 1** finden sich die Begriffsbestimmungen. Wo es keiner für Liechtenstein spezifischen Legaldefinition bedarf, wurden die in Art. 4 der Richtlinie (EU) 2016/1148 geregelten Definitionen wortgleich in die Vorlage übernommen.

«Netz- und Informationssysteme» (**Bst. a**) sind elektronische Kommunikationsnetze, wie sie auch in Art. 3 Abs. 1 Ziff. 5 des Gesetzes über die elektronische Kommunikation (Kommunikationsgesetz; KomG) definiert werden. Darüber hinaus versteht man darunter auch räumlich verteilte, digitale Verarbeitungsvorrichtungen zur technischen Unterstützung der Erhebung, Verarbeitung, Speicherung, Wartung, Nutzung, Weitergabe, Verbreitung oder Disposition von Informationen. Auch die Daten, die in einem solchen elektronischen Kommunikationsnetz oder einer solchen Vorrichtung verarbeitet werden, sind von dem Begriff umfasst. Diese Begriffsdefinition wurde aus der Richtlinie (EU) 2016/1148 übernommen.

Der Begriff der «Sicherheit von Netz- und Informationssystemen» (**Bst. b**) umfasst nicht nur die Fähigkeit, Sicherheitsvorfälle abzuwehren, sondern auch die

Fähigkeit, Sicherheitsvorfällen präventiv vorzubeugen, eine bereits entstandene Störung zu erkennen, zu beseitigen und möglichst rasch den Normalbetrieb wiederherzustellen. Die Sicherheit der Netz- und Informationssysteme trägt dazu bei, Gefährdungen zu erkennen, zu bewerten und zu verfolgen, Störungen zu bewältigen, die damit verbundenen Folgen zu mindern sowie die Handlungs- und Funktionsfähigkeit der davon betroffenen Akteure, Infrastrukturen und Dienste wiederherzustellen. Die Begriffsdefinition wurde aus der Richtlinie (EU) 2016/1148 übernommen.

Der **Liechtensteinische Bankenverband** führt zur Sicherheit von Netz- und Informationssystemen in seiner Stellungnahme zur Vernehmlassung aus, dass gemäss der gegenständlichen Gesetzesvorlage die Betreiber wesentlicher Dienste in der Lage sein müssen, «auf einem bestimmten Vertrauensniveau alle Angriffe abzuwehren[...]». Auch wenn die Definition dem Wortlaut der Richtlinie entnommen ist, bittet der Liechtensteinische Bankenverband im Hinblick auf das Prinzip der Verhältnismässigkeit um Klarstellung – in der Definition oder zumindest in den Erläuterungen –, dass durch Betreiber wesentlicher Dienste die Sicherheit der Netz- und Informationssysteme derart sicherzustellen ist, dass Angriffe im Bereich des Zumutbaren und dem jeweiligen Stand der Technik abgewehrt werden.

Mit der Sicherheit von Netz- und Informationssystemen wird die Fähigkeit von Netz- und Informationssystemen verstanden, auf einem bestimmten Vertrauensniveau alle Angriffe abzuwehren. Im besten Fall werden alle Angriffe abgewehrt, um die Sicherheit von Netz- und Informationssystemen für ein bestimmtes Vertrauensniveau zu garantieren. In diesem Zusammenhang regelt Art. 4 Abs. 1, dass Betreiber wesentlicher Dienste bzw. Art. 6 Abs. 1, dass Anbieter digitaler Dienste geeignete und verhältnismässige technische und organisatorische Massnahmen ergreifen müssen, um die Risiken für die Sicherheit der Netz- und

Informationssysteme zu bewältigen. Diese Massnahmen müssen unter Berücksichtigung des Stands der Technik ein Sicherheitsniveau der Netz- und Informationssysteme gewährleisten, welches dem bestehenden Risiko angemessen ist. Daraus folgt, dass in allen Fällen ein bestimmtes Risiko besteht, dass die Sicherheit von Netz- und Informationssystemen nicht abschliessend garantiert werden kann (oder anders, nicht alle Angriffe abgewehrt werden können). Diese Risiken sind durch die Betreiber wesentlicher Dienste und Anbieter digitaler Dienste zu identifizieren und mit Massnahmen zu adressieren.

Die sogenannte NIS-Strategie (Nationale Strategie für die Sicherheit von Netz- und Informationssystemen) gemäss **Bst. c** stellt einen Rahmen mit strategischen Zielen und Prioritäten für die Sicherheit von Netz- und Informationssystemen auf nationaler Ebene dar. Diese Begriffsdefinition wurde ebenfalls wörtlich aus der Richtlinie (EU) 2016/1148 übernommen.

Ein «wesentlicher Dienst» (**Bst. d**) wird in einem der in Art. 1 Abs. 1 Bst. a genannten Sektoren erbracht (**Ziff. 1**). Er zeichnet sich dadurch aus, dass er von wesentlicher Bedeutung für die Aufrechterhaltung kritischer gesellschaftlicher und/oder wirtschaftlicher Tätigkeiten ist. Dies umfasst insbesondere die Aufrechterhaltung des öffentlichen Gesundheitsdienstes, der öffentlichen Versorgung mit Wasser, Energie sowie lebenswichtigen Gütern, des öffentlichen Verkehrs oder die Funktionsfähigkeit öffentlicher Informations- und Kommunikationstechnologie. Die Begriffsdefinition entspricht im Kern der Definition einer kritischen Infrastruktur gemäss dem § 74 Abs. 1 Ziff. 10 StGB (**Ziff. 2**). Zudem muss die Verfügbarkeit des Dienstes abhängig von Netz- und Informationssystemen sein (**Ziff. 3**), was dann der Fall ist, wenn bei seiner Bereitstellung oder Erbringung Netz- und Informationssysteme eingesetzt werden. Ebenso ist es Bedingung, dass im Falle eines Sicherheitsvorfalls mit tatsächlichen Auswirkungen auf die Sicherheit von Netz- und

Informationssystemen eine erhebliche Störung bei der Bereitstellung dieses Dienstes auftritt (**Ziff. 4**). Bei der Bestimmung des Ausmasses einer Störung werden zumindest die folgenden sektorübergreifenden Faktoren berücksichtigt: die Zahl der Nutzer, die den von der jeweiligen Einrichtung angebotenen Dienst in Anspruch nehmen; Abhängigkeit anderer Sektoren vom angebotenen Dienst; mögliche Auswirkungen — hinsichtlich Ausmass und Dauer — auf wirtschaftliche und gesellschaftliche Tätigkeiten oder die öffentliche Sicherheit; Marktanteil der betroffenen Einrichtung; geografische Ausbreitung des Gebiets, das von einer Störung betroffen sein könnte; Bedeutung der Einrichtung für die Aufrechterhaltung des wesentlichen Dienstes in ausreichendem Umfang, unter Berücksichtigung der Verfügbarkeit von alternativen Mitteln.

Der **Liechtensteinische Bankenverband** führt in seiner Stellungnahme zur Vernehmlassung aus, dass Bst. d zwar den Begriff des wesentlichen Dienstes definiert, jedoch sei es für die betroffenen Unternehmen in den relevanten Sektoren von zentraler Bedeutung, eine einheitliche Methodik sowie handhabbare, objektive Kriterien zur Bestimmung kritischer Infrastrukturen zur Verfügung zu haben. Ausschlaggebend sei stets die Bedeutung für das Funktionieren des Gemeinwesens. Als Beispiel werden vom Liechtensteinischen Bankenverband verschiedene Dienste bzw. Dienstleistungen im Bankensektor aufgeführt. So sei im Bereich Banken sicherlich die Bargeldversorgung sowie der kartengestützte und konventionelle Zahlungsverkehr von Bedeutung. Inwieweit auch die reibungslose Abwicklung von Wertpapier- und Derivategeschäften einen wesentlichen Dienst i.S.d. Gesetzes darstellt, wäre laut dem Liechtensteinischen Bankenverband zu evaluieren. Der Bankenverband regt daher an, dringend mit den einzelnen Sektoren und in Abstimmung mit der Finanzmarktaufsicht Liechtenstein, welche u.a. die bankenaufsichtsrechtlichen Anforderungen an die Funktionsfähigkeit kritischer Infrastrukturen und deren Sicherheitsanforderungen

definiert und überwacht, bzw. den anderen zuständigen Aufsichtsbehörden, im Rahmen von Wegleitungen die Vorgaben aus dem CSG zu konkretisieren.

Dazu führt die Regierung aus, dass seitens der Stabsstelle Cyber-Sicherheit für jeden in Art. 1 Abs. 1 Bst. a genannten Sektor im Einzelfall zu prüfen sein wird, ob es sich um einen wesentlichen Dienst im Sinne der Legaldefinition handelt (Art. 13 Abs. 1 Bst. e). Die Stabsstelle wird sich bei der Identifikation der wesentlichen Dienste vor allem an den bisherigen Erkenntnissen und Erfahrungen aus anderen Ländern orientieren. Daher erachtet die Regierung eine Auslegung im Rahmen einer Wegleitung, ob ein konkreter Dienst einen wesentlichen Dienst im Sinne der Legaldefinition dieses Gesetzes darstellt, im Regelfall nicht für möglich. Vielmehr müssen in diese Entscheidung die konkreten Umstände im Einzelfall miteinbezogen und gewürdigt werden.

Die Stabsstelle Cyber-Sicherheit ist bemüht, sämtliche anderen betroffenen Stellen, so u.a. die Finanzmarktaufsicht, in die Prüfung sowie den Entscheidungsprozess so weit als möglich zu involvieren.

Der **Liechtensteinische Bankenverband** führt in seiner Stellungnahme weiter aus, dass aufgrund ihres Marktanteils am Retailgeschäft sowie den gesicherten Einlagen nach erster Einschätzung lediglich die drei grössten Banken, LGT, LLB sowie VP Bank, als besonders kritische Einrichtungen zu definieren seien.

Ebenso wie das Führen einer Liste mit den wesentlichen Diensten, wird es auch gemäss Art. 13 Abs. 1 Bst. e Aufgabe der Stabsstelle Cyber-Sicherheit sein, die Betreiber dieser wesentlichen Dienste zu ermitteln. Dabei ist vorgesehen, dass die Stabsstelle Cyber-Sicherheit die Kriterien und Schwellenwerte gemeinsam mit den einzelnen Sektoren erarbeitet, wobei etwaige auf europäischer Ebene bereits vorhandene einschlägige Dokumente zu berücksichtigen sind. Ebenso sollen allfällige Aufsichtsbehörden, denen ein Betreiber oder Anbieter unterliegt,

entsprechend eingebunden werden. Die Stabsstelle Cyber-Sicherheit wird hier den direkten Kontakt mit den Betreibern und Anbietern suchen.

Zur Einschätzung des Liechtensteinischen Bankenverbandes, wonach es sich lediglich bei den drei grössten Banken um besonders kritische Einrichtungen handelt, kann daher zum jetzigen Zeitpunkt noch keine Stellungnahme abgegeben werden.

«Betreiber wesentlicher Dienste» (**Bst. e**) sind öffentliche oder private Einrichtungen mit Sitz in Liechtenstein, die einen wesentlichen Dienst in einem der in Art. 1 Abs. 1 Bst. a genannten Sektoren erbringen. Gemäss Erwägungsgrund 21 der Richtlinie (EU) 2016/1148 setzt ein Sitz die 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.

Der **Liechtensteinische Bankenverband** weist im Hinblick auf Art. 3 Abs. 1 Bst. e darauf hin, dass gerade im Finanzdienstleistungsbereich häufig Dienstleistungen, so auch kritische IT-Dienstleistungen, ausgelagert würden. Aus Sicht des Liechtensteinischen Bankenverbandes dürfe im Falle einer Auslagerung kritischer IT-Dienstleistungen von Banken und Finanzmarktinfrastrukturen unter Gesamtschau der Umstände lediglich der jeweilige IT-Dienstleister als «Betreiber» des wesentlichen Dienstes anzusehen sein, obwohl die Bank aufsichtsrechtlich für die Einhaltung der Sicherheitsanforderungen verantwortlich bliebe.

Ebenso ersucht der **Liechtensteinische Anlagefondsverband** in seiner Stellungnahme um Ausführungen, wer im Falle einer Auslagerung von IT-Dienstleistungen als «Betreiber wesentlicher Dienste» qualifiziert wird.

Grundsätzlich bleibt der Betreiber wesentlicher Dienste alleine in der Verantwortung. Es wird hier auf Erwägungsgrund 52 der Richtlinie (EU) 2016/1148

verwiesen. Demnach gewährleisten Betreiber wesentlicher Dienste und die Anbieter digitaler Dienste die Sicherheit der von ihnen verwendeten Netz- und Informationssysteme. Die Sicherheitsanforderungen und die Meldepflicht sollen nach Erwägungsgrund 52 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. Daraus ergibt sich für externe IT-Dienstleister, die einen Betreiber wesentlicher Dienste servizieren, dass sie nicht selbst zum Betreiber dieses wesentlichen Dienstes werden. Vielmehr wären die Pflichten aus diesem Gesetz vom Betreiber wesentlicher Dienste, abhängig vom Einzelfall, im Wege der Lieferantenverträge auf den Dienstleister zu «überbinden».

Die **Finanzmarktaufsicht Liechtenstein** empfiehlt klarzustellen, dass die Betreiber die Einhaltung der in der Vorlage vorgesehenen Anforderungen auch für den Fall der Liquidation und/oder Abwicklung nach dem Gesetz über die Sanierung und Abwicklung von Banken und Wertpapierfirmen (SAG) sicherzustellen haben, etwa über spezifische Vertragsklauseln. Jüngste Erfahrungen im EWR hätten gezeigt, dass in einem solchen Szenario externe IT-Anbieter ihre Dienstleistungsverträge unverzüglich kündigen und eine angemessene IT-Infrastruktur nicht mehr gewährleistet werden könne.

Die Regierung bedankt sich für den Hinweis. Sie wird dieses Thema mit der Finanzmarktaufsicht aufnehmen. Eine Gewährleistung von angemessener IT-Leistung auch im Falle der Liquidation und/oder Abwicklung wird für unbedingt erforderlich erachtet.

Ein «Digitaler Dienst» (**Bst. f**) ist ein Dienst der Informationsgesellschaft, also in der Regel ein gegen Entgelt elektronisch im Fernabsatz und auf individuellen Abruf eines Empfängers bereitgestellter Dienst (Art. 3 Abs. 1 Bst. e des EWR-Notifikationsgesetzes), wie insbesondere der Online-Vertrieb von Waren und

Dienstleistungen, Online-Informationsangebote, die Online-Werbung, elektronische Suchmaschinen und Datenabfragemöglichkeiten sowie Dienste, die Informationen über ein elektronisches Netz übermitteln, die den Zugang zu einem solchen vermitteln oder die Informationen eines Nutzers speichern. Die Richtlinie (EU) 2016/1148 beschränkt den Anwendungsbereich auf drei digitale Dienste: 1. Online-Marktplätze (Bst. o), 2. Online-Suchmaschinen (Bst. p) und 3. Cloud-Computing-Dienste (Bst. q).

«Anbieter digitaler Dienste» (**Bst. g**) sind juristische Personen, die einen digitalen Dienst anbieten und die keine kleine Gesellschaft oder Kleinstgesellschaft im Sinne des Art. 1064 Abs. 1 und 1a des Personen- und Gesellschaftsrechts sind, die einen Sitz in Liechtenstein haben (**Ziff. 1**) oder die einen Vertreter nach Bst. h namhaft gemacht haben, wenn sie ihren Sitz ausserhalb des Europäischen Wirtschaftsraums (EWR) haben (**Ziff. 2**).

Anbieter digitaler Dienste ohne Sitz im EWR sind verpflichtet, einen Vertreter nach Bst. h in einem EWR-Mitgliedstaat namhaft zu machen. Der Vertreter handelt im Auftrag des Anbieters digitaler Dienste, und es muss für die zuständigen Behörden oder die CSIRTs möglich sein, mit ihm Kontakt aufzunehmen (**Bst. h**).

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 Tätigkeit, unterscheidet diese Vorlage diese beiden Gruppen und verfolgt – wie von der Richtlinie (EU) 2016/1148 vorgesehen – jeweils einen unterschiedlichen Ansatz. So sind beispielsweise Betreiber wesentlicher Dienste durch die Stabsstelle Cyber-Sicherheit zu erheben (Art. 13 Abs. 1 Bst. e) und es wird ein anderer Massstab an die Aufsicht gestellt als dies bei Anbietern digitaler Dienste der Fall ist (Vgl. Art. 14 und 15).

Ein «Sicherheitsvorfall» (**Bst. i**) liegt vor, wenn ein Ereignis die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit gespeicherter, übermittelter oder verarbeiteter Daten oder entsprechender Dienste, die über Netz- und Informationssysteme angeboten werden bzw. zugänglich sind, beeinträchtigt. Eine solche Beeinträchtigung kann beispielsweise neben Cyberangriffen oder Einwirkungen Dritter auch durch physische Ereignisse wie etwa Naturereignisse, aber auch durch Ereignisse wie z. B. Stromausfälle oder das Verhalten eigener Mitarbeiter verursacht werden. Damit ein Sicherheitsvorfall im Sinne dieser Begriffsdefinition vorliegt, genügt es bereits, wenn der Dienst in qualitativer Hinsicht beeinträchtigt ist. Es ist somit nicht notwendig, dass ein Dienst vollständig ausfällt oder das Ereignis eine Störung mit erheblichen Auswirkungen zur Folge hat.

Der **Liechtensteinische Bankenverband** ersucht in seiner Stellungnahme zur Vernehmlassung um eine weitere Präzisierung des Begriffs des Sicherheitsvorfalls. Unter anderem bleibe in der Vernehmlassungsvorlage unklar, ab wann tatsächlich von einer Beeinträchtigung des wesentlichen Dienstes auszugehen sei.

Auch die **Liechtensteinische Alters- und Krankenhilfe** ersucht in ihrer Stellungnahme um eine Präzisierung der Definition von Sicherheitsvorfällen. Dies ermögliche es Betreibern von wesentlichen Diensten, ihrer Meldepflicht betreffend relevanter Sicherheitsvorfällen nachzukommen.

Dasselbe Anliegen äusserten auch die **Liechtensteinischen Kraftwerke** in ihrer Stellungnahme zur Vernehmlassungsvorlage. Die Liechtensteinischen Kraftwerke ersuchten zudem um Anpassung und Ergänzung der Legaldefinition wie folgt: «...; sofern nur einzelne Systeme (Endnutzengeräte, Nutzerkonten) von geringer Kritikalität betroffen sind und/oder der Angriff unter Anwendung geeigneter Schutzmassnahmen erfolgreich abgewehrt werden konnte, handelt es sich nicht um einen Sicherheitsvorfall im Sinne dieses Gesetzes.».

Die Regierung hält in diesem Zusammenhang fest, dass sich die Begriffsdefinition des Sicherheitsvorfalls unmittelbar an der Richtlinie (EU) 2016/1148 orientiert. Demnach sind sämtliche Ereignisse, welche die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit verarbeiteter Daten oder entsprechender Dienste beeinträchtigen, als Sicherheitsvorfall zu qualifizieren. Diese Definition soll beibehalten werden.

Unabhängig vom Sicherheitsvorfall ist die Meldepflicht nach Art. 5 und Art. 7 zu sehen. Hier wurde – abweichend der Vernehmlassungsvorlage und aufgrund zahlreicher Rückmeldungen zu diesem Punkt – ein entsprechender höherer Schwellenwert für die Meldepflicht eingeführt.

So stellen beispielsweise ein sogenannter Port Scan oder eine Phishing E-Mail noch keine Sicherheitsvorfälle im Sinne der Legaldefinition nach Bst. i dar, solange die Schutzziele nicht beeinträchtigt sind. Dagegen stellen ein Stromausfall sowie der Ausfall einer Netzwerkinfrastruktur, der die Verfügbarkeit beeinträchtigt, oder auch die erfolgreiche Kompromittierung eines Systems mit Schadsoftware Sicherheitsvorfälle im Sinne dieser Bestimmung dar.

In Bezug auf die Meldepflicht von Sicherheitsvorfällen wird auf die Erläuterungen in Art. 5, Art. 7 und Art. 8 verwiesen. Mit der Anpassung des Schwellenwertes der Meldepflicht in den erwähnten Artikel wird den Bedenken des Liechtensteinischen Bankenverbands, der Liechtensteinischen Alters- und Krankenhilfe sowie der Liechtensteinischen Kraftwerke dahingehend entsprochen, dass nicht jeder Sicherheitsvorfall eine Meldepflicht nach sich zieht. Die Legaldefinition des Sicherheitsvorfall soll jedoch unverändert bleiben.

Die «Bewältigung von Sicherheitsvorfällen» (**Bst. k**) umfasst sämtliche Verfahren zur Unterstützung der Erkennung, Analyse und Eindämmung von Sicherheitsvorfällen sowie die Reaktion darauf. Dies können unter anderem sein:

Die Aufrechterhaltung und Erprobung von Erkennungsprozessen und Verfahren zur Gewährleistung einer rechtzeitigen und angemessenen Lageerfassung bei ungewöhnlichen Ereignissen, Prozesse und Vorgaben für die Meldung von Vorfällen und die Feststellung von Schwachstellen und Anfälligkeiten in Informationssystemen, die Reaktion gemäss den festgelegten Verfahren und Berichterstattung über die Ergebnisse der ergriffenen Massnahmen, die Bewertung der Schwere des Sicherheitsvorfalls mit einer Dokumentation der Erkenntnisse aus der Vorfallanalyse und einer Sammlung relevanter Informationen, die als Nachweis dienen können und einen kontinuierlichen Verbesserungsprozess fördern.

Im Rahmen der gegenständlichen Vorlage stellt ein «Risiko» (**Bst. l**) einen mit vernünftigem Aufwand feststellbaren Umstand oder ein Ereignis dar, welche potenziell nachteilige Auswirkungen auf die Sicherheit von Netz- und Informationssystemen haben können. Risiken sind beispielsweise Schwachstellen in Netz- und Informationssystemen. Die Begriffsdefinition wurde wortgleich der Richtlinie (EU) 2016/1148 entnommen.

Die Begriffe «Kooperationsgruppe» (**Bst. m**) und «CSIRTs-Netzwerk» (**Bst. n**) entsprechen wortgleich den Art. 11 und Art. 12 der Richtlinie (EU) 2016/1148.

Im Hinblick auf die besondere Situation Liechtensteins und die Anbindung an das Nationale Zentrum für Cybersicherheit (NCSC) Schweiz regt der **Liechtensteinische Bankenverband** in seiner Stellungnahme zur Vernehmlassungsvorlage die Ergänzung der Legaldefinition dahingehend an, dass neben den bereits benannten Vertretern ebenfalls «Vertreter weiterer vertrauenswürdiger Drittstaaten» berücksichtigt werden.

Dem CSIRTs-Netzwerk gemäss Art. 12 Abs. 2 der Richtlinie (EU) 2016/1148 setzt sich aus Vertretern der CSIRTs der Mitgliedstaaten und des CERT-EU zusammen.

Die Vernetzung der Stabsstelle Cyber-Sicherheit mit dem Nationalen Zentrum für Cybersicherheit der Schweiz (NCSC) stützt sich unmittelbar auf Art. 13 Abs. 1 Bst. l. Aus diesem Grund bedarf es nach Ansicht der Regierung keiner Anpassung des Art. 3 Abs. 1 Bst. n.

Ein «Online-Marktplatz» (**Bst. o**) ermöglicht es Verbrauchern und Unternehmern, Online-Kaufverträge oder Online-Dienstleistungsverträge mit Unternehmern abzuschliessen, und ist der endgültige Bestimmungsort für den Abschluss dieser Verträge. Der Begriff des «Online-Marktplatzes» erstreckt sich nicht auf Online-Dienste, die lediglich als Vermittler für Drittdienste fungieren, durch die letztlich ein Vertrag geschlossen werden kann. Online-Dienste, 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, sind daher nicht erfasst. Die von dem Online-Marktplatz bereitgestellten IT-Dienste können die Verarbeitung von Transaktionen, die Aggregation von Daten oder die Erstellung von Nutzerprofilen einschliessen.

Eine «Online-Suchmaschine» (**Bst. p**) ermöglicht es dem Nutzer, Suchen grundsätzlich auf allen Internetseiten anhand einer Abfrage zu einem beliebigen Thema vorzunehmen. Sie kann alternativ dazu auf Internetseiten in einer bestimmten Sprache beschränkt sein. Die Definition des Begriffs «Online-Suchmaschine» in diesem Gesetz erstreckt sich nicht auf Suchfunktionen, die auf den Inhalt einer bestimmten Internetseite beschränkt sind, unabhängig davon, ob diese Suchfunktionen durch eine externe Suchmaschine bereitgestellt werden. Sie erstreckt sich auch nicht auf Online-Dienste, 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.

«Cloud-Computing-Dienste» (**Bst. q**) umfassen eine breite Palette von Tätigkeiten, die auf unterschiedliche Weise erbracht werden können. Gemäss diesem Gesetz 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 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.

Abs. 2 enthält den Standardhinweis betreffend die Geschlechtsneutralität der verwendeten Personenbezeichnungen.

II. Sicherheitsanforderungen und Meldepflichten

A. Betreiber wesentlicher Dienste

Zu Art. 4

In Umsetzung von Art. 14 Abs. 1 der Richtlinie (EU) 2016/1148 müssen Betreiber wesentlicher Dienste die Sicherheit der von ihnen verwendeten Netz- und Informationssysteme gewährleisten. So wird in **Abs. 1** bestimmt, dass 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. Die Massnahmen zur Sicherheit von Netz- und Informationssystemen adressieren die Sicherheit gespeicherter, übermittelter und verarbeiteter Daten. Damit keine unverhältnismässige finanzielle und administrative Belastung für Betreiber wesentlicher Dienste entsteht, sollen die Massnahmen in einem angemessenen Verhältnis zu den Risiken stehen, denen das betreffende Netz- und Informationssystem ausgesetzt ist.

Sowohl die **Wasserversorgung Liechtensteiner Unterland e. G.** als auch der **Liechtensteinische Bankenverband** ersuchen in ihren Stellungnahmen zur Vernehmlassungsvorlage um eine Einbeziehung in die Ausarbeitung näherer Sicherheitsanforderungen.

Die Regierung wird die Vernehmlassungsteilnehmer in die Ausarbeitung der entsprechenden Grundlagen für die Sicherheitsmassnahmen bestmöglich miteinbeziehen.

Jedenfalls müssen die Massnahmen gemäss **Abs. 2** unter Berücksichtigung des Stands der Technik ein Sicherheitsniveau der Netz- und Informationssysteme gewährleisten, welches dem bestehenden Risiko, das mit vernünftigem Aufwand feststellbar ist, angemessen ist. Dadurch soll insbesondere der im Bereich der Netz- und Informationssicherheit praktizierte «risikobasierte Ansatz» abgebildet werden. Die Sicherheitsanforderungen und die Meldepflicht (Art. 5) gelten für die einschlägigen Betreiber wesentlicher Dienste unabhängig davon, ob sie ihre Netz- und Informationssysteme selbst warten oder diese Aufgabe an Dritte ausgelagert haben.

Gegenständlich wird unter dem Begriff «Stand der Technik» verstanden, dass die Massnahmen insbesondere einschlägige – sofern vorhanden – internationale und

branchenspezifische Standards berücksichtigen, eine gewisse Marktreife besitzen und im Einsatz erprobt sind.

Um Duplizitäten zu vermeiden, ersucht der **Liechtensteinische Bankenverband** um einen Abgleich mit den sektorspezifischen, insbesondere aufsichtsrechtlichen, Vorgaben betreffend Sicherheitsvorgaben für Betreiber wesentlicher Dienste sowie dem Incident Reporting. Die Vorgaben in Art. 4 Abs. 1 und Abs. 2 seien für den Banksektor durch die EBA/GL/2019/04 bzw. die FMA-Richtlinie 2021/3 und die FMA-Mitteilung 2018/03 bereits aufsichtsrechtlich abgedeckt. Ebenfalls bestünden mit der DSGVO bereits Vorgaben zur Verarbeitung von besonders schützenswerten personenbezogenen Daten.

Den Anregungen des Liechtensteinischen Bankenverbands sollen dahingehend Rechnung getragen werden, als dass bei der Ausarbeitung der Verordnung zur Präzisierung der Sicherheitsmassnahmen gemäss Abs. 5 der Liechtensteinische Bankenverband sowie die Finanzmarktaufsicht Liechtenstein so weit als möglich abgeholt werden. Hinsichtlich der Sektoren Bankenwesen und Finanzmarktinfrastrukturen wird auf die entsprechenden Ausführungen zu Abs. 4 (Lex specialis) verwiesen.

Die **NetSec.co AG** stellt in ihrer Stellungnahme fest, dass in Art. 4 und Art. 6 die Sicherheitsanforderungen für Betreiber wesentlicher Dienste sowie für Anbieter digitaler Dienste aufgeführt werden. Die Anforderungen seien nahezu identisch, wobei in Art. 6 konkrete Aspekte aufgeführt seien, welche in Art. 4 fehlen würden. Die NetSec.co AG schlägt vor, zu prüfen, ob die beiden Artikel zusammengelegt werden können.

Dazu führt die Regierung aus, dass die Richtlinie (EU) 2016/1148 in Bezug auf die Sicherheitsanforderungen bewusst zwischen den Betreibern wesentlicher Dienste und den Anbietern digitaler Dienste unterscheidet. Im Erwägungsgrund 57 hält die

Richtlinie (EU) 2016/1148 beispielsweise fest, dass wegen der grundlegenden Unterschiede zwischen Betreibern wesentlicher Dienste, insbesondere wegen deren unmittelbarer Verbindung mit einer physischen Infrastruktur, und Anbietern digitaler Dienste, insbesondere wegen deren grenzüberschreitenden Tätigkeit, in Bezug auf das Mass der Harmonisierung im Hinblick auf diese beiden Gruppen jeweils einen unterschiedlichen Ansatz verfolgt werden soll.

Aus Sicht der Regierung ist die Unterscheidung zwischen Betreibern wesentlicher Dienste und Anbietern digitaler Dienste somit erforderlich und soll beibehalten werden.

Gemäss **Abs. 3** ergreifen die Betreiber wesentlicher Dienste geeignete (präventive) Massnahmen, um den Auswirkungen von Sicherheitsvorfällen, die die Sicherheit der von ihnen für die Bereitstellung von Diensten genutzten Netz- und Informationssysteme beeinträchtigen, vorzubeugen beziehungsweise diese so gering wie möglich zu halten, damit die Verfügbarkeit dieser Dienste gewährleistet wird. Hiervon sind Massnahmen umfasst, welche zur Ermittlung von Gefahren und Schwachstellen dienen. Ebenso sollen Sicherheitsvorfälle verhindert, aufgedeckt und bewältigt werden, sodass die Folgen gemindert werden. Ziel ist insbesondere, die Verfügbarkeit des wesentlichen Dienstes sicherzustellen.

Mit **Abs. 4** wird Art. 1 Abs. 7 der Richtlinie (EU) 2016/1148 entsprochen. Dieser enthält eine Lex specialis Bestimmung, wonach unter anderem die Bestimmungen über die Sicherheitsanforderungen für Betreiber wesentlicher Dienste nach der Richtlinie (EU) 2016/1148 keine Anwendung finden, wenn sie bereits unter den Anwendungsbereich sektorenspezifischer EWR-Rechtsvorschriften für Sicherheitsanforderungen fallen, die in ihrer Wirkung den in der Richtlinie (EU) 2016/1148 enthaltenen Pflichten mindestens gleichwertig sind. Art. 1 Abs. 7 der Richtlinie (EU) 2016/1148 ist von den EWR-Mitgliedstaaten bei der Umsetzung zu berücksichtigen (vgl. auch ErwGr. 9 der Richtlinie (EU) 2016/1148). Ebendies wird

durch Abs. 4 gewährleistet. Trotz der Anwendbarkeit von Lex specialis-Bestimmungen wird die betreffende Einrichtung als Betreiber wesentlicher Dienste gemäss Art. 10 Abs. 1 Bst. f ermittelt.

Die **Finanzmarktaufsicht Liechtenstein** führte in ihrer Stellungnahme zur Vernehmlassung aus, dass sie es als notwendig erachtet, den Wortlaut des Abs. 4 anzupassen. Die Bestimmung könne so verstanden werden, dass das gegenständliche Gesetz und spezialgesetzliche Bestimmungen nebeneinander zur Anwendung kommen. Die Richtlinie (EU) 2016/1148 statuiere hingegen in Art. 1 Abs. 7 einen klaren Vorrang sektorspezifischer Bestimmungen.

Abs. 4 wurde auf Grund dieses Hinweises redaktionell angepasst und damit eindeutig klargestellt, dass die Pflichten nach den Abs. 1 bis 3 keine Anwendung finden, sofern spezialgesetzliche Bestimmungen über Sicherheitsanforderungen, die zumindest ein gleichwertiges Sicherheitsniveau für Netz- und Informationssysteme vorsehen, bestehen. Im Zusammenhang mit der Anwendung von spezialgesetzlichen Bestimmungen im Bereich Bankenwesen und Finanzmarktinfrastrukturen wird auf die Ausführungen unter dem Abschnitt 4.2.2 verwiesen.

Abs. 5 gibt der Regierung die Kompetenz, Näheres betreffend die Sicherheitsanforderungen für Betreiber wesentlicher Dienste mittels Verordnung zu regeln.

Zu Art. 5

Die Tragweite, Häufigkeit und Auswirkungen von Sicherheitsvorfällen nehmen zu und stellen eine erhebliche Bedrohung für den störungsfreien Betrieb von Netz- und Informationssystemen dar. Die 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 grossen Schaden zufügen.

In Umsetzung des Art. 14 Abs. 3 Richtlinie (EU) 2016/1148 wird daher in **Abs. 1** vorgesehen, dass Betreiber wesentlicher Dienste unter bestimmten Umständen Sicherheitsvorfälle, die den wesentlichen Dienst betreffen, unverzüglich an die Stabsstelle Cyber-Sicherheit zu melden haben.

In der ursprünglichen Bestimmung der Vernehmlassungsvorlage war es für die Meldepflicht unerheblich, ob es durch den Sicherheitsvorfall zu einem Schaden oder zu einer anderweitigen Störung gekommen ist. Aufgrund mehrerer Stellungnahmen zu Art. 5 Abs. 1 wurde diese Bestimmung entsprechend abgeändert und ein Schwellenwert eingeführt. Somit ist es gemäss aktuellem Gesetzesvorschlag notwendig, dass es durch den Sicherheitsvorfall zu erheblichen Auswirkungen auf die Verfügbarkeit eines von einem Betreiber wesentlicher Dienste bereitgestellten Dienstes gekommen ist oder der Sicherheitsvorfall zumindest geeignet ist, sich erheblich auf die Verfügbarkeit eines bereitgestellten Dienstes auszuwirken.

Die Meldepflicht soll anhand des Beispiels Ransomware erörtert werden. Ransomware, sogenannte Erpressungstrojaner, Erpressungssoftware oder auch Verschlüsselungstrojaner, sind Schadprogramme, mit deren Hilfe ein Angreifer den Zugriff des Inhabers auf seine Daten, deren Nutzung oder auf das ganze Computersystem verhindern kann. Dabei werden die Daten auf den Computern verschlüsselt oder der Zugriff auf sie verhindert, um für die Entschlüsselung oder Freigabe ein Lösegeld zu fordern.

Ein erfolgreicher Angriff mit Ransomware ist offensichtlich geeignet, die Verfügbarkeit eines bereitgestellten Dienstes, welcher auf Grundlage der nicht

mehr verfügbaren Daten erbracht wird, erheblich zu beeinträchtigen. Dies war beispielsweise im Mai 2021 bei der Colonial Pipeline in den USA der Fall. Ein erfolgreicher Angriff mit Ransomware begründet somit eine Meldepflicht an die Stabsstelle Cyber-Sicherheit. Doch selbst wenn bei einem Angriff mittels Ransomware ein kritisches System bzw. der wesentliche Dienst aufgrund implementierter Sicherheitsmassnahmen nicht unmittelbar betroffen sein sollte, kann sich für den Betreiber wesentlicher Dienste eine Meldepflicht an die Stabsstelle Cyber-Sicherheit ergeben. Dies unter anderem, weil ein erfolgreicher Angriff mittels Ransomware – selbst, wenn er die kritischen Systeme (noch) nicht betrifft – grundsätzlich geeignet ist, sich erheblich auf die Verfügbarkeit eines bereitgestellten Dienstes auszuwirken.

Der **Liechtensteinische Bankenverband** führte in seiner Stellungnahme zu Art. 5 Abs. 1 aus, dass Betreiber jegliche Sicherheitsvorfälle, die einen wesentlichen Dienst betreffen, an die Stabsstelle zu melden haben. Die Meldeschwelle sei damit jedoch deutlich niedriger als die Vorgaben des Art. 14 Abs. 3 der Richtlinie (EU) 2016/1148, welche Meldungen von Sicherheitsvorfällen vorsehe, die erhebliche Auswirkungen auf die Verfügbarkeit der von ihnen bereitgestellten wesentlichen Dienste haben. Der Liechtensteinische Bankenverband führt aus, dass ein Sicherheitsvorfall von einer Cyberbedrohung oder einem Beinahe-Vorfall zu unterscheiden sei. Von Interesse seien wesentliche Sicherheits- oder Cybervorfälle, nicht aber operative Störungen oder einfache Vorfälle des Tagesgeschäfts. So verlange auch die Richtlinie (EU) 2016/1148 nicht, dass durch den Sicherheitsvorfall eine Störung oder ein Schaden eingetreten sein muss, sondern nur, dass die Auswirkungen auf die Verfügbarkeit des bereitgestellten wesentlichen Dienstes erheblich gewesen sind. Wann eine derartige Erheblichkeit gegeben ist, wäre durch weitergehende Verwaltungsanweisung zu konkretisieren. Es bedürfe klarer Leitlinien, ab wann ein Vorfall relevant und wie dieser zu klassifizieren ist (Fraud Incident, Cyber Angriff, Data Breach, etc.). Der

Liechtensteinische Bankenverband regt daher an, die Formulierung des Art. 5 Abs. 1 im Lichte der Richtlinie zu schärfen.

Eine ähnliche Anregung betreffend den Schwellenwert der Meldepflicht findet sich in der Stellungnahme zur Vernehmlassung der **Liechtensteinischen Kraftwerke**.

Dem Anliegen des Liechtensteinischen Bankenverbands sowie den Liechtensteinischen Kraftwerken wurde entsprochen, indem der Schwellwert der Meldepflicht angepasst wurde. Eine Meldepflicht nach Art. 5 Abs. 1 ist nunmehr in jenen Fällen jedenfalls gegeben, wenn durch einen Sicherheitsvorfall eine erhebliche Auswirkung auf die Verfügbarkeit eines wesentlichen Dienstes eingetreten ist. Jedoch sind auch solche Sicherheitsvorfälle der Stabsstelle Cyber-Sicherheit zu melden, die geeignet sind, sich erheblich auf die Verfügbarkeit eines von ihnen bereitgestellten wesentlichen Dienstes auszuwirken, selbst wenn es noch zu keiner erheblichen Auswirkung gekommen ist. Damit wird vor allem der Kleinheit des Landes Rechnung getragen.

Anders als in anderen EWR-Mitgliedstaaten ist in der Regel bei einer Beeinträchtigung der Verfügbarkeit eines wesentlichen Dienstes das ganze Land unmittelbar betroffen und ein alternativer Dienst steht zumeist nicht oder jedenfalls nicht zeitnah zur Verfügung.

Was unter einer erheblichen Auswirkung verstanden wird und welche Parameter dabei zu berücksichtigen sind, soll in der entsprechenden Verordnung geregelt werden.

Auf konkrete Leitlinien seitens der Stabsstelle Cyber-Sicherheit soll so weit als möglich verzichtet werden. Vielmehr sollen sämtliche Betreiber wesentlicher Dienste eingeladen werden, an der Ausarbeitung eines gemeinsamen Verständnisses für die Schwellenwerte der Meldepflicht mitzuwirken.

Sowohl der **Liechtensteinische Bankenverband**, als auch der **Liechtensteinische Anlagefondsverband** und die **Liechtensteinischen Kraftwerke** weisen in ihren Stellungnahmen zur Vernehmlassungsvorlage darauf hin, dass eine Konkretisierung des Begriffs «unverzüglich» wünschenswert wäre. Dabei könnte nach Auffassung der Liechtensteinischen Kraftwerke auf die Meldefrist im Rahmen der DSGVO (72 Stunden) oder aber nach Meinung des Liechtensteinischen Bankenverbands auf die FMA-Mitteilung 2018/3 (innert 14 Tagen ab Kenntniserlangung über schwerwiegende und betriebsstörende Cyber-Attacken) abgestellt werden.

Der **Liechtensteinische Bankenverband** ersucht weiter um Aufnahme einer Legaldefinition in Art. 3 derart, dass unverzüglich nicht die – bereits rein faktisch nicht mögliche – sofortige Vornahme der geforderten Handlung, bspw. Meldung eines Sicherheitsvorfalls, vorausgesetzt wird, sondern dass nach einer Erstanalyse so rasch als möglich, d.h. ohne schuldhaftes Zögern innerhalb einer nach vernünftigem Ermessen festzulegenden Frist, die geforderte Handlung vorzunehmen ist.

Dazu führt die Regierung aus, dass es gemäss Art. 13 Abs. 1 Bst. b eine Aufgabe der Stabstelle Cyber-Sicherheit sein wird, ein Computer-Notfallteam (CSIRT) nach Art. 19 einzurichten und zu koordinieren. Das CSIRT kann den Betroffenen bei Bedarf gemäss Art. 19 Abs. 1 Bst. c eine erste allgemeine Unterstützung bei der Reaktion auf Sicherheitsvorfälle leisten. Ebenso kann das CSIRT im Rahmen seiner Möglichkeiten zur Bewältigung eines Sicherheitsvorfalls nützliche Informationen gemäss Art. 19 Abs. 1 Bst. a zur Verfügung stellen.

Damit das CSIRT den Betreiber wesentlicher Dienste bei Sicherheitsvorfällen unterstützen kann, bedarf es einer zeitnahen Meldung. Daher sollte eine Meldung eben «unverzüglich» erfolgen, um den zuvor genannten Aufgaben auch entsprechen zu können.

Eine Frist von 72 Stunden gemäss der DSGVO oder auch von 14 Tagen wird dem oben genannte Zweck der Meldepflicht nicht gerecht.

Gegenständlich ist unter dem Begriff «unverzüglich» das Erfordernis einer Meldung ohne schuldhaftes Zögern zu verstehen. Die Auslegung dieses Begriffs ist jeweils von den etwaigen Umständen des Einzelfalls abhängig und ist deshalb im Einzelfall zu beurteilen. Eine pauschale oder generelle Aussage, wann eine Meldung «ohne schuldhaftes Zögern» erfolgt, ist daher nicht möglich.

Die zuständige Meldestelle ist nach Art. 5 Abs. 1 die Stabsstelle Cyber-Sicherheit. Eine allgemeine Unterstützung der meldenden Stelle nach Sicherheitsvorfällen findet in weiterer Folge gemäss Art. 19 Abs. 1 Bst. a und c durch das CSIRT statt, welches gemäss Art. 19 Abs. 1 1. Satz bei der Stabsstelle Cyber-Sicherheit eingerichtet wird. Das CSIRT kann sich zur Erfüllung seiner Aufgaben gemäss Art. 9 Abs. 2 qualifizierten Dritten bedienen.

Der **Liechtensteinische Bankenverband** führt in seiner Stellungnahme aus, dass mehrere Banken als kritische Infrastrukturen bereits beim NCSC in der Schweiz angegliedert sind. Wenn nun das neue nationale CSIRT Mitglied im CSIRT-Netzwerk nach Art. 3 Abs. 1 Bst. n ist, sei es für die Banken von grundlegender Bedeutung, dass auch in Zukunft Cyber-Vorfälle bzw. sonstige Sicherheitsvorfälle in Bezug auf Netz- und Informationssysteme – im internationalen Kontext – nur an eine Stelle zentral gemeldet werden müssen.

Sofern eine Meldepflicht nach einem Sicherheitsvorfall gemäss diesem Gesetz besteht, ist dieser Sicherheitsvorfall gemäss Art. 5 unverzüglich an die Stabsstelle Cyber-Sicherheit zu melden. Für Meldungen im Bankenwesen und der Finanzplatzinfrastrukturen sind dem gegenständlichen Gesetz vorgehende spezialgesetzliche Bestimmungen zu berücksichtigen, sprich eine Meldung hat an

die Finanzmarktaufsicht hat zu erfolgen. Dazu wird auf die entsprechenden Ausführungen in Abschnitt 4.2.2 verwiesen.

Das Nationale Zentrum für Cybersicherheit in der Schweiz (NCSC) befindet sich aktuell im organisatorischen Umbau. Die Stabsstelle Cyber-Sicherheit ist im ständigen Austausch mit den entsprechenden Stellen in der Schweiz. Dabei wird sich die Regierung und die Stabsstelle Cyber-Sicherheit dafür einsetzen, dass die bisherige bewährte Zusammenarbeit mit der Schweiz in einer solchen Art und Weise weiter bestehen bleibt, dass Unternehmen durch die Umorganisation in der Schweiz sowie den Aufbau der Stabsstelle Cyber-Sicherheit in Liechtenstein keine Nachteile erfahren. Jeglicher unnötige Aufwand für die von der gegenständlichen Gesetzesvorlage betroffenen Stellen soll so weit als möglich vermieden werden.

Der **Liechtensteinische Bankenverband** führt in seiner Stellungnahme zur Vernehmlassung aus, dass durch den Betreiber wesentlicher Dienste mithin mehrere Meldungen an verschiedene nationale Behörden/Stellen abgesetzt werden müssen, so etwa beispielsweise eine Meldung an die Datenschutzstelle (Data Breach), an die Finanzmarktaufsicht Liechtenstein (Operational Incident oder auf spezialgesetzlicher Grundlage, bspw. Art. 102 ZOG oder Cyber Incident) oder auch an die Stabstelle Cyber-Sicherheit (Cyber Incident). In Bezug auf die Resilienz wäre eine zentrale nationale Meldestelle (Hub) für alle Arten von Sicherheitsvorfällen und alle betroffenen Marktteilnehmer wünschenswert. Sollte dies nicht umsetzbar sein, sei laut Liechtensteinischem Bankenverband gerade für stark regulierte Sektoren wie den Finanzbereich jedenfalls eine klare Struktur der Zuständigkeiten zu schaffen. Es erscheine angezeigt, auch die Zusammenarbeit der Behörden untereinander zu intensivieren und daher näher zu regeln, beispielsweise in einer Art Verständigungsverfahren. Es sei bisher unklar, welche der zuständigen Behörden federführend ist und wie der allenfalls notwendige

grenzüberschreitende Informationsaustausch der verschiedenen Behörden organisiert wird.

Die Regierung betont in diesem Zusammenhang, dass die Meldepflichten in den unterschiedlichen nationalen Regelungen unterschiedliche Zwecke verfolgen.

Im Bereich Bankwesen und Finanzmarktinfrastrukturen melden die Betreiber wesentlicher Dienste an die Finanzmarktaufsicht (s. Abschnitt 4.2.2). Eine Weiterleitung der Meldungen an die Stabsstelle Cyber-Sicherheit wird mit Art. 5 Abs. 6 2. Satz geregelt.

Jedenfalls aber soll die Stabsstelle Cyber-Sicherheit als vertrauenswürdige und zentrale Anlaufstelle für sämtliche Belange im Bereich Cyber-Sicherheit sowie im Umgang mit Cyber-Risiken etabliert werden. Sie soll als Drehscheibe, Vermittlungs- und Verbindungsstelle für die Bevölkerung, die Wirtschaft, der kritischen Infrastrukturen sowie die Behörden fungieren. Meldungen an die Stabsstelle Cyber-Sicherheit dienen der Lagebeurteilung und vor allem der Unterstützung der meldenden Stelle, indem im Rahmen der Möglichkeiten der Stabsstelle Cyber-Sicherheit eine allgemeine Unterstützung nach Sicherheitsvorfällen bereitgestellt wird.

Meldungen nach Art. 33 DSGVO an die Datenschutzstelle verfolgen einen anderen Zweck.

Bevor eine zentrale Meldestelle geschaffen wird, muss sichergestellt werden, dass damit den Anforderungen sämtlicher Meldungsempfänger entsprochen werden kann.

Die Zusammenarbeit zwischen der Stabsstelle Cyber-Sicherheit, der Datenschutzstelle, der Finanzmarktaufsicht Liechtenstein sowie weiterer inländischer Behörden und Stellen ist in Art. 13 Abs. 1 Bst. i explizit normiert.

Es ist hier jedoch anzumerken, dass die Stabsstelle Cyber-Sicherheit keine an sie erstattete Meldungen – weder basierend auf einer Pflicht nach Art. 5 oder Art. 7 noch freiwillig nach Art. 8 – ungefiltert an andere Stellen weiterleiten wird. Die Interessen der meldenden Stelle sind in allen Fällen zu wahren. Daher hat im Zweifel eine Weiterleitung, sei es auch in Auszügen und gekürzt, zu unterbleiben.

Die Regierung erachtet eine Zusammenarbeit der Stabsstelle Cyber-Sicherheit mit anderen betroffenen inländischen Behörden, allen voran mit der Finanzmarktaufsicht Liechtenstein sowie mit der Datenschutzstelle, für erforderlich. Diese soll im Einzelfall so weit als möglich sichergestellt werden, um die meldenden Stellen zu entlasten und eine umfassende Abdeckung aller Risiken im Bereich Cyber-Sicherheit zu gewährleisten.

Da die eingegangenen Meldungen an die Stabsstelle Cyber-Sicherheit vor allem dazu dienen, die Lage der betroffenen Einrichtung, die Erheblichkeit des Sicherheitsvorfalls generell und allfällige Auswirkungen auf andere Sektoren oder die Öffentlichkeit bewerten zu können, legt **Abs. 2** dementsprechend den Inhalt der jeweiligen verpflichtenden Meldung fest. So muss die Meldung an die Stabsstelle Cyber-Sicherheit bestimmte Angaben enthalten, namentlich sind dies sämtliche relevante Angaben zum Sicherheitsvorfall und zu den technischen Rahmenbedingungen, die im Zeitpunkt der Erstmeldung bekannt sind, insbesondere die vermutete oder tatsächliche Ursache, die betroffene Informationstechnik, die Art der betroffenen Einrichtung oder Anlage. Zur Erfüllung der Meldepflicht ist es erforderlich, sämtliche Umstände darzulegen, die zum Zeitpunkt der Meldung bekannt sind.

Angaben über später bekanntgewordene Umstände zum Sicherheitsvorfall sind in Nachmeldungen und letztendlich in einer Abschlussmeldung unverzüglich nach Feststellung der Umstände der Stabsstelle Cyber-Sicherheit mitzuteilen. Durch diese Regelung wird zum Ausdruck gebracht, dass einer möglichst frühzeitigen

Meldung Vorrang gegenüber einer vollständigen Meldung eingeräumt wird. Die Pflicht, später bekanntgewordene Angaben zu melden, soll die Bewältigung eines Sicherheitsvorfalls nicht beeinträchtigen.

Der **Liechtensteinische Bankenverband** ersucht in seiner Stellungnahme im Hinblick auf Art. 22 Abs. 1 Bst. b um Klarstellung, unter welchen Umständen eine bussgeldbewährte unvollständige Meldung vorliegt.

Die Regierung hält fest, dass ein Betreiber eines wesentlichen Dienstes nach Kenntniserlangung eines Sicherheitsvorfalles durchaus Erstabklärungen und Analysen durchführen kann, ohne sich mit einem potentiellen Verstoss gegen Art. 5 Abs. 2 CSG konfrontiert zu sehen. Denn wie der Liechtensteinische Bankenverband in seiner Stellungnahme ausführt, wird sich die Schwere eines Sicherheitsvorfalles zum Zeitpunkt seines Eintrittes oftmals noch gar nicht unmittelbar bewerten lassen. Da zum Zeitpunkt des Sicherheitsvorfalles in vielen Fällen noch nicht alle Begleitumstände oder die nach Art. 5 Abs. 2 erforderlichen Mindestangaben bekannt sind, ist in Abs. 2 auch die Möglichkeit von Nachmeldungen und einer Abschlussmeldung vorgesehen.

Doch je früher gemeldet wird, desto schneller kann die Stabsstelle Cyber-Sicherheit bei einem Sicherheitsvorfall unterstützen oder über qualifizierte Dritte den Betroffenen die notwendige Unterstützung zukommen lassen bzw. diese vermitteln.

Die Meldeplattform wird dabei so einfach und unbürokratisch wie möglich aufgebaut sein, sodass die betroffenen Stellen einen Sicherheitsvorfall mit wenigen Schritten der Stabsstelle Cyber-Sicherheit mitteilen können.

Eine unvollständige Meldung liegt vor allem dann vor, wenn ein Betreiber wesentlicher Dienste zu einem meldepflichtigen Sicherheitsvorfall keine Angaben

zum betroffenen System (Informationstechnik) und der Art der betroffenen Einrichtung macht sowie trotz Kenntnis der Ursache diese nicht bekannt gibt.

Bei der Anwendung des Art. 22 Abs. 1 Bst. b und d werden die Umstände zum Zeitpunkt des Sicherheitsvorfalls besonders gewichtet und im Sinne der betroffenen Stelle auch gewürdigt werden.

Meldungen sind in einem gesicherten und soweit als möglich standardisierten elektronischen Format zu übermitteln (**Abs. 3**). Dazu wird die Stabsstelle Cyber-Sicherheit entsprechende Meldeformulare auf ihrer Internetseite sowie abweichend der ursprünglichen Vernehmlassungsvorlage ebenso alternative Meldewege zur Verfügung stellen.

Die **Liechtensteinischen Kraftwerke** begrüßen in ihrer Stellungnahme zur Vernehmlassung die Meldung über ein standardisiertes Verfahren. Sie ersuchen jedoch um Aufnahme des Begriffs «gesichert», sodass die Vertraulichkeit der Übermittlung der Meldung garantiert wird.

Der **Liechtensteinische Bankenverband** regt zu Abs. 3 an, neben dem elektronischen Meldeformat alternative Kanäle zu erwägen. Dies beispielsweise in solchen Fällen, in denen die Internetseite der Stabsstelle Cyber-Sicherheit oder das elektronische Meldeformular im Falle einer Störung nicht erreichbar oder verfügbar ist (z. B. DDoS Angriff oder Ausfall des Internet Service Providers).

Der Anregung der Liechtensteinischen Kraftwerke zu Abs. 3 wurde dahingehend Rechnung getragen, dass die sichere Übermittlung explizit und als Grundsatz in der gegenständlichen Gesetzesvorlage normiert wird.

Gleichzeitig wurde Abs. 3 dahingehend angepasst, dass weiterhin die elektronische Übermittlung als Grundsatz gilt und falls möglich gefordert wird. Dennoch sind nun

Ausnahmen zulässig, falls eine elektronische Übermittlung nicht möglich ist, etwa weil die Infrastruktur für die Meldungen nicht verfügbar ist.

Mit **Abs. 4** wird die Meldepflicht für jene Fälle geregelt, in denen ein Betreiber wesentlicher Dienste für die Bereitstellung seines wesentlichen Dienstes die Dienste eines Dritten als Anbieter digitaler Dienste in Anspruch nimmt. In der Vernehmlassung fand sich dieser Absatz noch bei den Anbietern digitaler Dienste in Art. 7, er wurde jedoch aufgrund der Stellungnahme des **Liechtensteinischen Bankenverbands** aus systematischen Gründen in Art. 5 neu verortet.

Hat ein Sicherheitsvorfall bei einem Anbieter digitaler Dienste erhebliche Auswirkungen auf die Bereitstellung des wesentlichen Dienstes, den ein Betreiber wesentlicher Dienste erbringt, weil dieser sich des Anbieters digitaler Dienste als Dienstleister bedient, so trifft den Betreiber wesentlicher Dienste eine Meldepflicht gegenüber der Stabsstelle Cyber-Sicherheit.

Der **Liechtensteinische Bankenverband** regte in seiner Stellungnahme weiters an, dass nur eine Meldepflicht für relevante/erhebliche Auswirkungen auf die Verfügbarkeit dieser Dienste bestehen sollte.

Dazu führt die Regierung aus, dass der Begriff «erheblich» – vergleiche dazu Abs. 1 – in der Gesetzesvorlage ergänzt wurde und Abs. 4 nun wortgleich mit Art. 16 Abs. 5 der Richtlinie (EU) 2016/1148 ist.

Die **Liechtensteinischen Kraftwerke** führen an, dass es ein konkretes Beispiel gäbe, in dem die ausländischen Strafverfolgungsbehörden dem betroffenen Unternehmen (Dritten) ausdrücklich untersagt hätten, die Beeinträchtigung ihrer Systeme im Rahmen eines Cybervorfalles an andere Unternehmen und Partner weiterzugeben, sprich diese wurden erst Tage später über den Sicherheitsvorfall informiert. Die Liechtensteinischen Kraftwerke bitten zu prüfen, ob die Rechtslage

in den verschiedenen Ländern dies zulässt und inwieweit sich bei Nichteinhaltung der Meldefristen auf den/die Dritten überwälzen lassen.

Mit Abs. 4 wird Art. 16 Abs. 5 der Richtlinie (EU) 2016/1148 von der Regierung mit gegenständlicher Vorlage wortgleich umgesetzt. Der Stabsstelle Cyber-Sicherheit ist der Sicherheitsvorfall durch den Betreiber wesentlicher Dienste unverzüglich zu melden. Inwieweit im konkreten Fall ein Verstoß gegen die Meldepflicht vorliegt, muss im Einzelfall geprüft werden. Eine pauschale oder allgemeine Beurteilung ist hier nicht möglich.. Dies insbesondere vor dem Hintergrund, dass sämtliche EWR-Mitgliedstaaten die Bestimmungen der Richtlinie (EU) 2016/1148 gleichermassen und vollumfänglich umzusetzen haben.

Abs. 5 entspricht Art. 14 Abs. 6 der Richtlinie (EU) 2016/1148 und eröffnet der Stabsstelle Cyber-Sicherheit in bestimmten Fällen die Möglichkeit, im Falle eines Sicherheitsvorfalls die Öffentlichkeit zwecks Verhütung weiterer Sicherheitsvorfälle entsprechend zu sensibilisieren. Voraussetzung ist dabei jedoch die Anhörung des meldenden Betreibers wesentlicher Dienste sowie der Umstand, dass die Sensibilisierung der Öffentlichkeit zur Verhütung von Sicherheitsvorfällen oder zur Bewältigung aktueller Sicherheitsvorfälle erforderlich ist.

Bei der Bekanntmachung von Sicherheitsvorfällen ist das Interesse der Öffentlichkeit über Bedrohungen informiert zu werden, sorgfältig gegen einen möglichen wirtschaftlichen Schaden oder einen Imageschaden abzuwiegen, der den Betreibern wesentlicher Dienste, die solche Vorfälle melden, entstehen kann.

Die **Liechtensteinischen Kraftwerke** weisen in ihrer Stellungnahme zur Vernehmlassung darauf hin, dass es zwingend notwendig sei eine Anhörung durchzuführen und die Kommunikation mit dem jeweiligen Krisenkommunikationskonzept des betroffenen Unternehmens abzustimmen, um

Desinformation, einen wirtschaftlichen Schaden, Panik oder ähnliches in der Bevölkerung beziehungsweise bei den Unternehmen zu vermeiden.

Eine Anhörung und Abstimmung mit dem Betreiber wesentlicher Dienste sind gemäss Abs. 5 zwingend vorgesehen. Diese Anhörung ist unabhängig von den individuellen Umständen des Sicherheitsvorfalles in jedem Fall vorzunehmen. Ein Einbezug der konkret betroffenen Betreiber wird damit sichergestellt.

Allgemeine Informationen und Warnungen an die Bevölkerung ohne Bezug zu einem konkreten Betreiber kann die Stabsstelle Cyber-Sicherheit nach Art. 13 Abs. 1 Bst. h jederzeit ohne vorherige Anhörung versenden. In diesem Fall erachtet die Regierung die Gefahr von Nachteilen für den konkret betroffenen Betreiber nicht für gegeben.

Der **Liechtensteinische Bankenverband** führt in seiner Stellungnahme zur Vernehmlassung aus, dass im Einzelfall nach Art. 5 Abs. 5 bzw. Art. 7 Abs. 2 eine Information der Öffentlichkeit über konkrete Sicherheitsvorfälle erfolgen könne. Nach Art. 7 Abs. 2 könne die Stabsstelle Cyber-Sicherheit neben der Eigeninformation sogar «verlangen, dass der Anbieter digitaler Dienste dies unternimmt». Offen bleibe in beiden Fällen, auf welcher Grundlage letztlich die Stabsstelle Cyber-Sicherheit entscheidet, ob und durch wen die Öffentlichkeit zu informieren ist.

Offen sind auch die Art und Weise der Information, über die Internetseite der Stabsstelle oder des Anbieters digitaler Dienste, Printmedien, Radio usw. Der Liechtensteinische Bankenverband bittet um weitere Ergänzung der Materialien.

Mit Art. 5 Abs. 5 und Art. 7 Abs. 2 werden Art. 14 Abs. 6 bzw. Art. 16 Abs. 7 der Richtlinie (EU) 2016/1148 national umgesetzt. Der Zweck der Information über einen Sicherheitsvorfall an die Öffentlichkeit ist die Sensibilisierung zur Verhütung von Sicherheitsvorfällen oder zur Bewältigung aktueller Sicherheitsvorfälle.

Die Entscheidung, ob nach einem Sicherheitsvorfall die Öffentlichkeit informiert wird, erfolgt nach Anhörung des betroffenen Betreibers wesentlicher Dienste. Vor der Unterrichtung der Öffentlichkeit über Sicherheitsvorfälle, ist das Interesse der Öffentlichkeit, über Bedrohungen informiert zu werden, sorgfältig gegen einen möglichen wirtschaftlichen Schaden bzw. einen Imageschaden abzuwiegen. Diese Interessensabwägung ist im Einzelfall durchzuführen.

Im Zusammenhang mit Betreibern wesentlicher Dienste erfolgt die Information in allen Fällen durch die Stabsstelle Cyber-Sicherheit.

Bei den Anbietern digitaler Dienste handelt es sich gemäss Legaldefinition um Online Suchmaschinen, Cloud-Computing-Dienste und Online-Marktplätze. In diesen Fällen kann es daher durchaus sinnvoll sein, dass die Stabsstelle Cyber-Sicherheit vom Anbieter digitaler Dienste verlangt, dass dieser die Öffentlichkeit entsprechend unterrichtet. Doch auch hier wird die Entscheidung von der konkreten Situation im Einzelfall abhängen.

Die Wahl des geeignetsten Mediums für die Information hängt ebenso vom Einzelfall ab und kann sowohl digitale Dienste wie Newsletter als auch Printmedien sowie in dringenden Fällen auch das Radio umfassen.

Jedenfalls wird in allen Fällen so entschieden werden, dass – sofern die Voraussetzungen für die Information an die Öffentlichkeit vorliegen und mit der betroffenen Stelle abgestimmt sind – mit der Information der damit verfolgte Zweck, nämlich die Sensibilisierung zur Verhütung von Sicherheitsvorfällen oder zur Bewältigung aktueller Sicherheitsvorfälle, bestmöglich erreicht werden kann.

Der **Liechtensteinische Bankenverband** begrüsst in seiner Stellungnahme den Lex specialis Vorbehalt bei den Sicherheitsanforderungen des Art. 4 Abs. 4 für Betreiber wesentlicher Dienste. Er führt darin jedoch weiter aus, dass in der Vernehmlassungsvorlage lediglich die Bestimmungen über

Sicherheitsanforderungen berücksichtigt sind, nicht jedoch die ebenfalls spezifischen Meldepflichten. Der Liechtensteinische Bankenverband verweist in seiner Stellungnahme in weiterer Folge auf den Lex specialis Vorbehalt des Art. 1 Abs. 7 der Richtlinie (EU) 2016/1148, welcher explizit auch im Bereich der Meldepflicht greife und in der Vernehmlassung in Art. 5 oder Art. 7 nicht nachvollzogen sei. Selbiger Hinweis findet sich ebenso in der Stellungnahme der **Finanzmarktaufsicht Liechtenstein**.

Die vom Liechtensteinischen Bankenverband und der Finanzmarktaufsicht Liechtenstein aufgezeigte fehlende Lex specialis Regelung für Meldepflichten von Betreibern wesentlicher Dienste wurden von der Regierung in der gegenständlichen Vorlage mit Art. 5 Abs. 6 eingeführt.

Gemäss **Abs. 6** finden die Pflichten nach den Abs. 1 bis 5 (Meldepflichten für die Betreiber wesentlicher Dienste) keine Anwendung, wenn spezialgesetzliche Bestimmungen über die Meldepflicht bestehen und die Kriterien für die Meldepflicht mindestens gleichwertig sind. Dieser Absatz wurde nach der Vernehmlassung ergänzt, da dieser Lex specialis Vorbehalt für die Meldepflicht in der Vernehmlassung fehlte, worauf insbesondere durch den **Liechtensteinischen Bankenverband** und die **Finanzmarktaufsicht Liechtenstein** hingewiesen wurde.

Ob eine spezialgesetzliche Meldepflicht gleichwertig ist, muss im Einzelfall geprüft werden. Kriterien dafür sind unter anderem der Schwellenwert der Meldung sowie die Frist für die Meldung nach Art. 5 Abs. 1.

In diesen Fällen haben die Meldungsempfänger, wie unter Umständen die Finanzmarktaufsicht Liechtenstein, jedoch gemäss Abs. 6 2. Satz die bei ihnen aufgrund einer spezialgesetzlichen Bestimmung eingegangenen Meldungen zu Sicherheitsvorfällen unverzüglich an die Stabsstelle Cyber-Sicherheit weiterzuleiten.

Durch die unverzügliche Weiterleitung wird sichergestellt, dass die Stabsstelle Cyber-Sicherheit sowie das CSIRT über die für die Erstellung von Lagebildern gemäss Art. 13 Abs. 1 Bst. c notwendigen Informationen verfügen bzw. nach Art. 19 Abs. 1 entsprechende allgemeine Unterstützung leisten können.

Der **Liechtensteinische Bankenverband** bittet in seiner Stellungnahme um Abstimmung betreffend die aufsichtsrechtlichen Erfordernisse. Banken sollten nur eine Meldung (an die und gemäss den Vorgaben der Finanzmarktaufsicht Liechtenstein) absetzen müssen. Der Informationsfluss an weitere zuständige Stellen solle über die behördliche Zusammenarbeit sichergestellt werden. Es sei daher zwingend vorzusehen, dass die Verwendung von aufgrund sektorspezifischer aufsichtsrechtlicher Vorgaben erstellter Meldungen und Meldeformulare auch für Zwecke der Meldung nach Art. 5 an die Stabsstelle Cyber-Sicherheit zulässig ist, sofern der Mindestinhalt der Meldung nach Art. 5 Abs. 2 abgedeckt ist.

Dazu führt die Regierung aus, dass mit Abs. 6 2. Satz sichergestellt wird, dass in jenen Fällen, in denen Meldungen über Sicherheitsvorfälle aufgrund von spezialgesetzlichen Bestimmungen an andere zuständige Stellen (z. B. die Finanzmarktaufsicht Liechtenstein) gemeldet werden, die Meldungsempfänger die bei ihnen eingegangenen Meldungen unverzüglich an die Stabsstelle Cyber-Sicherheit weiterzuleiten haben. Damit werden der Informationsfluss und die behördliche Zusammenarbeit sichergestellt.

Die **Finanzmarktaufsicht Liechtenstein** führt in ihrer Stellungnahme zur Vernehmlassung aus, dass sich unter Umständen Doppelspurigkeiten für solche Intermediäre ergeben könnten, die sowohl unter die IKT-Richtlinie als auch unter das künftige Cyber-Sicherheitsgesetz fallen, soweit es um schwerwiegende oder betriebsstörende Sicherheitsvorfälle geht. Im Hinblick auf die Meldepflicht und das Meldeformular für solche Fälle wäre es aus Sicht der Finanzmarktaufsicht

Liechtenstein jedenfalls wünschenswert, Doppelspurigkeiten so weit wie möglich zu vermeiden bzw. im günstigsten Fall eine zentrale Meldepflicht bzw. -stelle sowie ein Meldeformat zu schaffen. Dies sei auch im Sinne der künftig geltenden DORA, welche zum Ziel hat, Meldungen IKT-bezogener Vorfälle zu straffen und überschneidende Meldepflichten zu beseitigen. In Erwägungsgrund 42 der DORA werde dazu explizit angeführt, dass die Meldung IKT-bezogener Vorfälle für alle Finanzunternehmen harmonisiert werden sollte, indem sie verpflichtet werden, nur ihren zuständigen Behörden Bericht zu erstatten. Die Finanzaufsichtsbehörden sollen diese Informationen sodann an Nicht-Finanzbehörden (u.a. für Netz- und Informationssicherheit zuständige Behörde, nationale Datenschutzbehörde und Strafverfolgungsbehörden im Fall strafrechtlicher Vorfälle) weiterleiten.

Bei der erwähnten «DORA» handelt es sich um den Vorschlag für eine Verordnung über die Betriebsstabilität digitaler Systeme des Finanzsektors. Mit dem aktuellen Entwurf zu Abs. 6 werden Doppelspurigkeiten vermieden, da geregelt wird, dass soweit spezialgesetzliche Bestimmungen über die Meldepflicht bestehen, die (direkte) Meldepflicht an die Stabsstelle Cyber-Sicherheit keine Anwendung findet. Inwieweit die spezialgesetzlichen Regelungen gleichwertig sind, wird im Einzelfall zu prüfen sein.

In Bezug auf die europäische Richtlinie PSD2 hat bereits die EU-Kommission festgestellt, dass für die Bereitstellung von Zahlungsdiensten durch Kreditinstitute die Sicherheitsanforderungen und Meldepflichten gemäss den Art. 95 und Art. 96 PSD2 anstelle der entsprechenden Vorschriften der Art. 4 und Art. 5 gelten sollen. Diese sind damit nach Auffassung der EU-Kommission als gleichwertig einzustufen. Weitere Erläuterungen dazu finden sich im Abschnitt 4.2.2.

Die Regierung hat gemäss **Abs. 7** eine Verordnungskompetenz, um die Meldepflicht sowie insbesondere die Schwellenwerte für eine allfällige Meldung

an die Stabsstelle Cyber-Sicherheit für Betreiber wesentlicher Dienste näher zu präzisieren und auszugestalten.

B. Anbieter digitaler Dienste

Zu Art. 6

Angesichts der Bedeutung ihrer Dienste für die Tätigkeit anderer Unternehmen haben ebenso Anbieter digitaler Dienste ein Sicherheitsniveau zu gewährleisten, das der Höhe des Risikos für die Sicherheit der von ihnen gebotenen Dienste angemessen ist. In der Praxis ist das Risiko für die Betreiber wesentlicher Dienste, die für die Aufrechterhaltung kritischer gesellschaftlicher und wirtschaftlicher Tätigkeiten von wesentlicher Bedeutung sind, höher als das Risiko für den Anbieter digitaler Dienste.

Ungeachtet dessen haben die Anbieter digitaler Dienste gemäss **Abs. 1** geeignete und verhältnismässige technische und organisatorische Massnahmen zu ergreifen, um die Risiken für die Sicherheit der Netz- und Informationssysteme, die sie im Rahmen der Bereitstellung des digitalen Dienstes nutzen, zu bewältigen.

Anbietern digitaler Dienste ist es freigestellt, 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 unterliegen die Anbieter digitaler Dienste jedoch einem im EWR stark harmonisierten Konzept. In diesem Sinne bestimmt die Durchführungsverordnung (EU) 2018/151³ die Spezifikation und die Umsetzung derartiger Massnahmen.

³ 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).

Die von Anbietern digitaler Dienste zu treffenden Sicherheitsvorkehrungen können sowohl technischer als auch organisatorischer Art sein und sollen im Hinblick auf die betriebenen digitalen Dienste dazu dienen, die Sicherheit der Netz- und Informationssysteme zu gewährleisten. Nach **Abs. 2** müssen diese Massnahmen unter Berücksichtigung des Stands der Technik ein Sicherheitsniveau gewährleisten, welches dem bestehenden Risiko angemessen ist. Dabei ist folgenden Aspekten Rechnung zu tragen: der Sicherheit der Systeme und Anlagen (**Bst. a**), der Bewältigung von Sicherheitsvorfällen (**Bst. b**), dem Betriebskontinuitätsmanagement (**Bst. c**), der Überwachung, der Überprüfung und Erprobung (**Bst. d**) sowie der Einhaltung internationaler Normen (**Bst. e**).

In der Durchführungsverordnung (EU) 2018/151 werden jene Elemente näher festgelegt, die die Anbieter digitaler Dienste zu berücksichtigen haben, wenn sie Massnahmen ermitteln und ergreifen, damit ein bestimmtes Sicherheitsniveau der Netz- und Informationssysteme gewährleistet wird. Ferner werden die Parameter näher festgelegt, die bei der Feststellung, ob ein Sicherheitsvorfall erhebliche Auswirkungen auf die Bereitstellung dieser Dienste hat, zugrunde zu legen sind.

In Bezug auf die Einhaltung internationaler Normen (Bst. e) bittet der **Liechtensteinische Bankenverband** in seiner Stellungnahme zur Vernehmlassung angesichts der Vielzahl an internationalen Standards und Normen um Präzisierung in den Erläuterungen oder im Gesetzestext dahingehend, dass Anbieter digitaler Dienste lediglich die für sie geltenden oder relevanten internationalen Normen und Standards einzuhalten haben.

Betreffend die Anbieter digitaler Dienste wird im Grundsatz auf die Durchführungsverordnung (EU) 2018/151 verwiesen. Internationale Normen im Sinne des Bst. e sind demnach Normen, die von einer internationalen Normungsorganisation im Sinne des Art. 2 Abs. 1 Bst. a der Verordnung (EU)

1025/2012 des Europäischen Parlaments und des Rates angenommen wurden. Gemäss Artikel 19 der Richtlinie (EU) 2016/1148 können auch europäische oder international anerkannte Normen und Spezifikationen für die Sicherheit von Netz- und Informationssystemen sowie bestehende nationale Normen verwendet werden.

In der Praxis werden die Anbieter in Bezug auf die Sicherheitsmassnahmen branchenspezifische anerkannte Standards und Normen, die sich vielfach an den einschlägigen ISO-Standards oder auch dem BSI-Grundschutzkatalog orientieren, berücksichtigen. Je nach Einsatzbereich existieren verschiedene Standards und Normen. Wesentlich ist, dass sie für den konkreten Einsatz anerkannt und auf dem aktuellen Stand sind. Die Anwendung veralteter oder nicht anerkannter oder für die konkrete Schutzmassnahme nicht geeigneter Standards entspricht jedenfalls nicht den Anforderungen nach Bst. e. Konkrete Vorgaben zur Verwendung eines bestimmten Standards oder einer bestimmten Norm bestehen nicht.

Zu Art. 7

Nach **Abs. 1** melden die Anbieter digitaler Dienste der Stabsstelle Cyber-Sicherheit unverzüglich jeden Sicherheitsvorfall, der erhebliche Auswirkungen auf die Bereitstellung eines von ihnen innerhalb des EWR erbrachten Dienstes hat. Für die Beurteilung, ob ein Sicherheitsvorfall als ein solcher mit erheblichen Auswirkungen gilt, sind die Kriterien nach Art. 4 Abs. 1 Bst. a bis d der Durchführungsverordnung (EU) 2018/151 heranzuziehen. Eine Meldepflicht besteht beispielsweise in jenen Fällen, wenn ein Sicherheitsvorfall zu einem Verlust der Integrität, Authentizität oder Vertraulichkeit gespeicherter oder übermittelter oder verarbeiteter Daten oder der entsprechenden Dienste, die über ein Netz- und Informationssystem des Anbieters digitaler Dienste angeboten werden bzw. zugänglich sind, geführt hat, von dem mehr als 100 000 Nutzer im EWR betroffen sind.

Die Meldepflicht gilt allerdings nur dann, wenn die Anbieter Zugang zu Informationen haben, die benötigt werden, um die Auswirkung eines Sicherheitsvorfalls zu bewerten. Dabei handelt es sich insbesondere um Informationen über die Zahl der vom Sicherheitsvorfall betroffenen Nutzer, der Dauer des Sicherheitsvorfalls, die geografische Ausbreitung in Bezug auf das von dem Sicherheitsvorfall betroffene Gebiet, das Ausmass der Unterbrechung der Bereitstellung des digitalen Dienstes und das Ausmass der Auswirkungen auf wirtschaftliche und gesellschaftliche Tätigkeiten.

Analog zu Art. 5 Abs. 5 wird mit **Abs. 2** für die Stabsstelle Cyber-Sicherheit die Möglichkeit eröffnet, im Falle eines Sicherheitsvorfalls die Öffentlichkeit zwecks Verhütung weiterer Sicherheitsvorfälle entsprechend zu sensibilisieren. Voraussetzung ist jedoch die Anhörung des betreffenden Anbieters digitaler Dienste durch die Stabsstelle Cyber-Sicherheit. Ebenso kann die Stabsstelle Cyber-Sicherheit von Anbietern digitaler Dienste verlangen, dass diese die Information an die Öffentlichkeit vornehmen. Voraussetzung ist jedoch in beiden Fällen, dass die Sensibilisierung der Öffentlichkeit zur Verhütung von Sicherheitsvorfällen oder zur Bewältigung aktueller Sicherheitsvorfälle erforderlich ist (**Bst. a**). Abweichend zu Art. 5 Abs. 5 genügt es hier jedoch auch, dass die Offenlegung des Sicherheitsvorfalls auf sonstige Weise im öffentlichen Interesse liegt (**Bst. b**).

Bei der Bekanntmachung von Sicherheitsvorfällen ist das Interesse der Öffentlichkeit, über Bedrohungen informiert zu werden, sorgfältig gegen einen möglichen wirtschaftlichen Schaden bzw. einen Imageschaden abzuwiegen, der den Anbietern digitaler Dienste, die solche Vorfälle melden, entstehen kann.

Mit dieser Bestimmung wird der Art. 16 Abs. 7 der Richtlinie (EU) 2016/1148 umgesetzt.

C. Andere Einrichtungen

Zu Art. 8

Andere Einrichtungen, die nicht in den Geltungsbereich dieses Gesetzes fallen, können ebenso 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 oder auch im eigenen Interesse liegt, das Auftreten derartiger Sicherheitsvorfälle zu melden, können sie dies nach **Abs. 1** auf freiwilliger Basis tun.

Solche Meldungen werden von der Stabsstelle Cyber-Sicherheit im Rahmen der verfügbaren Ressourcen und Möglichkeiten bearbeitet und sofern diese Bearbeitung keinen unverhältnismässigen oder ungebührlichen Aufwand darstellt.

Abs. 2 bestimmt, dass die freiwilligen Meldungen weder die Identität der Einrichtung noch Informationen, die auf diese schliessen lassen, enthalten müssen.

Zudem führt eine freiwillige Meldung nicht dazu, dass der meldenden Einrichtung Pflichten auferlegt werden, die nicht für sie gegolten hätten, wenn sie den Sicherheitsvorfall nicht bei der Stabsstelle Cyber-Sicherheit gemeldet hätte. Anderweitige Meldepflichten bleiben davon jedoch unberührt.

III. Organisation und Durchführung

A. Allgemeines

Zu Art. 9

Der gegenständliche Artikel wurde nach der Vernehmlassung neu eingefügt. Inhaltlich finden sich darin die Art. 10 Abs. 1 Bst. a sowie Art. 15 Abs. 4 und 5 der

Vernehmlassungsvorlage betreffend die Zuständigkeit der Durchführung dieses Gesetzes sowie qualifizierte Dritte im Zusammenhang mit dem CSIRT.

Abs. 1 bestimmt, dass mit der Durchführung dieses Gesetzes einerseits die Stabsstelle Cyber-Sicherheit (**Bst. a**) als auch das Computer-Notfallteam (**Bst. b**) betraut sind.

Die Stabsstelle Cyber-Sicherheit und das Computer-Notfallteam (CSIRT) können zur Erfüllung ihrer Aufgaben gemäss **Abs. 2** qualifizierte Dritte beauftragen. Gerade für den laufenden Betrieb des CSIRT wird eine entsprechende Kooperation mit Dritten notwendig sein.

Denn die Richtlinie (EU) 2016/1148 verlangt, dass jeder Mitgliedsstaat über angemessene technische und organisatorische Fähigkeiten zur Prävention, Erkennung, Reaktion und Abschwächung von Sicherheitsvorfällen und Risiken bei Netz- und Informationssystemen verfügen muss. Ein Element dazu stellen funktionierende Computer-Notfallteams (CSIRTs) gemäss Art. 19 dar, die die grundlegenden Anforderungen zur Gewährleistung wirksamer und kompatibler Fähigkeiten zur Bewältigung von Vorfällen und Risiken erfüllen.

Die Anforderungen an qualifizierte Dritte im Bereich des CSIRT ergeben sich vor allem aus Anhang I der Richtlinie (EU) 2016/1148. Dieser gibt unter anderem vor, dass für einen hohen Grad der Verfügbarkeit der Kommunikationsdienste gesorgt sein muss, indem beispielsweise punktuellen Ausfällen vorgebeugt und mehrere Kanäle bereitgestellt werden, damit die Stelle jederzeit erreichbar bleibt und selbst Kontakt aufnehmen kann. Die Kommunikationskanäle müssen zudem genau spezifiziert und den Nutzern sowie den Kooperationspartnern wohlbekannt sein. Die Räumlichkeiten der qualifizierten Dritten und die unterstützenden Informationssysteme werden an sicheren Standorten eingerichtet.

Ebenso müssen qualifizierte Dritte im Zusammenhang mit den CSIRT über ein geeignetes System zur Verwaltung und Weiterleitung von Anfragen verfügen, um Übergaben zu erleichtern und müssen personell so ausgestattet sein, dass sie eine ständige Bereitschaft gewährleisten können. Schliesslich müssen sie sich auf eine Infrastruktur stützen, deren Verfügbarkeit sichergestellt ist. Zu diesem Zweck müssen Redundanzsysteme und Ausweicharbeitsräume zur Verfügung stehen.

Zu den Anforderungen betreffend die qualifizierten Dritten besteht mit **Abs. 3** sowie im Zusammenhang mit CSIRT ergänzend mit Art. 19 Abs. 3 eine entsprechende Verordnungskompetenz für die Regierung.

Zu Art. 10

Diese Bestimmung entspricht inhaltlich Art. 20 der Vernehmlassungsvorlage. Mit dieser Bestimmung wird geregelt, dass die mit der Durchführung dieses Gesetzes betrauten Organe sowie allfällig durch diese beauftragte qualifizierte Dritte dem Amtsgeheimnis unterliegen und gegenüber anderen Amtsstellen und Personen über die in Ausübung dieser Tätigkeit gemachten Wahrnehmungen Stillschweigen zu bewahren sowie Einsicht in verarbeitete Daten und amtliche Akten zu verweigern haben. Die Befugnisse gegenüber Betreibern wesentlicher Dienste gemäss Art. 14 bleiben vorbehalten.

Zu Art. 11

In Art. 11 finden sich die Regelungen betreffend die Verarbeitung und Offenlegung personenbezogener Daten. In der Vernehmlassungsvorlage fand sich diese Bestimmung in Art. 16 (Datenschutz) und wurde in der gegenständlichen Vorlage redaktionell überarbeitet.

Die Stabsstelle Cyber-Sicherheit ist gemäss **Abs. 1** berechtigt, zur Gewährleistung eines hohen Sicherheitsniveaus von Netz- und Informationssystemen bei der Wahrnehmung ihrer – insbesondere die in Art. 13 Abs. 1 Bst. a bis n sowie Art. 19

Abs. 1 Bst. a bis e aufgeführten – Aufgaben nach diesem Gesetz, die erforderlichen personenbezogenen Daten nach Art. 4 Ziff. 1 Datenschutz-Grundverordnung (DSGVO)⁴ zu verarbeiten (Art. 4 Ziff. 2 DSGVO).

Die Stabsstelle Cyber-Sicherheit wird bei der Wahrnehmung ihrer Aufgaben vor allem personenbezogene Daten verarbeiten, welche nicht direkt einer natürlichen Person zugeordnet werden können. Als Beispiel werden hier IP-Adressen, Nicknamen im Internet oder andere technische Kennnummern genannt, die insbesondere bei der Meldung und Analyse von Sicherheitsvorfällen verarbeitet werden.

Im Zuge einer Verarbeitung im engeren Sinn, kann die Stabsstelle Cyber-Sicherheit personenbezogene Daten nach Abs. 1 gemäss **Abs. 2**, die ihr aufgrund der Wahrnehmung ihrer Aufgaben nach diesem Gesetz bekannt sind, in- und ausländischen Behörden sowohl in EWR-Mitgliedstaaten als auch in vertrauenswürdigen Drittstaaten wie der Schweiz, und anderen öffentlichen wie nicht öffentlichen Stellen offenlegen. Die Zulässigkeit der Offenlegung ist jedoch an Bedingungen geknüpft.

So muss die Offenlegung zur Erfüllung der Aufgaben der Stabsstelle Cyber-Sicherheit erforderlich (**Bst. a**) sowie die Vertraulichkeit der Daten gewährleistet sein (**Bst. b**) und die Sicherheit sowie die geschäftlichen Interessen der Betreiber wesentlicher Dienste und der Anbieter digitaler Dienste müssen geschützt sein (**Bst c**).

Die auszutauschenden Informationen werden im Einzelfall auf jenen Umfang beschränkt, der im Hinblick auf das verfolgte Ziel relevant und angemessen ist. Bei

⁴ 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 (ABl. L 119 vom 4.5.2016, S. 1).

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. Mit diesem Absatz wird Art. 8 Abs. 6 der Richtlinie (EU) 2016/1148 entsprechend umgesetzt.

Die gegenständliche Bestimmung wurde eng mit der Datenschutzstelle abgestimmt. Im Zuge des Vernehmlassungsverfahrens wies die Datenschutzstelle in ihrer Stellungnahme lediglich auf die Notwendigkeit einer Anpassung eines Verweises auf die DSGVO hin, welcher in der gegenständlichen Bestimmung entsprechend korrigiert wurde.

B. Stabsstelle Cyber-Sicherheit

Zu Art. 12

Die gegenständliche Bestimmung entspricht inhaltlich Art. 9 der Vernehmlassungsvorlage.

Abs. 1 bestimmt die Stabsstelle Cyber-Sicherheit als die für die Sicherheit von Netz- und Informationssystemen zuständige nationale Behörde gemäss Art. 8 Abs. 1 der Richtlinie (EU) 2016/1148. Ihr obliegt somit die Aufsicht und der Vollzug dieses Gesetzes.

Der **Liechtensteinische Bankenverband** ersucht in seiner Stellungnahme zur Vernehmlassungsvorlage um eine Klarstellung in den Materialien dahingehend, dass die Stabsstelle Cyber-Sicherheit als NCC-FL beziehungsweise im Hinblick auf das CSIRT selbst auch als kritische Infrastruktur zu werten ist.

Die Stabsstelle Cyber-Sicherheit gilt in jenen Bereichen als kritische Infrastruktur, in welchen sie wesentliche Dienste gemäss Legaldefinition erbringt. Welche Dienste dies im Konkreten sind, wird im Einzelfall zu prüfen sein. Die Anforderungen an das CSIRT sind insbesondere im Anhang I zur Richtlinie (EU) 2016/1148

festgelegt. Demnach sorgen CSIRTs 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. Ungeachtet der Anwendbarkeit des Cyber-Sicherheitsgesetzes wird die Stabsstelle Cyber-Sicherheit jedenfalls geeignete und verhältnismässige technische und organisatorische Massnahmen implementieren, um die Risiken für die Sicherheit der Netz- und Informationssysteme entsprechend zu adressieren.

Mit **Abs. 2** wird festgelegt, dass die Stabsstelle Cyber-Sicherheit ebenso die für die Sicherheit von Netz- und Informationssystemen zuständige zentrale Anlaufstelle gemäss Art. 8 Abs. 3 der Richtlinie (EU) 2016/1148 in Liechtenstein ist. Als solche ist sie die Verbindungsstelle zur Gewährleistung der grenzüberschreitenden Zusammenarbeit mit internationalen Gremien und Gruppen, wie insbesondere den zuständigen Stellen in den EWR-Mitgliedstaaten sowie der Kooperationsgruppe und dem CSIRTs-Netzwerk. Die Benennung der Stabsstelle Cyber-Sicherheit als zentrale Anlaufstelle dient insbesondere der Erleichterung der grenzüberschreitenden Zusammenarbeit und Kommunikation und soll die effektive Umsetzung der Richtlinie (EU) 2016/1148 ermöglichen.

Die Stabsstelle Cyber-Sicherheit wird mit angemessenen technischen, finanziellen und personellen Ressourcen ausgestattet, um die ihr übertragenen Aufgaben nach Art. 12 wirksam und effizient erfüllen und somit die Ziele dieses Gesetzes erreichen zu können. Sie verfügt über entsprechende Strukturen und kann wirksam mit den Wirtschaftsteilnehmern zusammenarbeiten.

Die **Liechtensteinischen Kraftwerke** weisen in ihrer Stellungnahme zur Vernehmlassung darauf hin, dass das Sicherheitsniveau der Stabsstelle Cyber-Sicherheit als zentrale Anlaufstelle und konzentrierter «Datenhub» entsprechend den sich stetig steigenden Risiken angemessen hochzuhalten ist. Insbesondere in technischen Belangen (hochprofessionelles Equipment, Schutz der erlangten

Informationen usw.), die personellen Ressourcen betreffend (hochqualifiziertes spezialisiertes Personal, gilt auch für Dritte), aber auch in finanzieller Hinsicht müssen nicht unerhebliche Mittel bereitgestellt werden, um keine zusätzliche Angriffsfläche zu bieten und um die Cyber-Sicherheit im Land Liechtenstein gewährleisten zu können.

Der **Liechtensteinische Bankenverband** merkt in seiner Stellungnahme zur Vernehmlassung ebenso an, dass die Problemstellungen rund um das Thema Cybersicherheit immer mehr an Bedeutung gewinnen werden. In Liechtenstein sei nunmehr mit der Stabsstelle Cyber-Sicherheit eine entsprechende zentrale Stelle im Zusammenhang mit Sicherheitsvorfällen und Cyberattacken etabliert worden. Zwecks wirkungsvoller Wahrnehmung der gesetzlich verankerten Aufgaben und Kompetenzen sei es grundlegend Voraussetzung, dass der Stabsstelle auch ausreichend Ressourcen zur Verfügung stehen.

Die Regierung ist der Ansicht, dass der aktuelle Entwurf den Hinweisen der Liechtensteinischen Kraftwerke und des Liechtensteinischen Bankenverbands gerecht wird. Die Stabsstelle Cyber-Sicherheit ist, insbesondere was die administrativen Aufgaben betrifft, in die IT-Infrastruktur der Liechtensteinischen Landesverwaltung eingebettet. Hier zeichnet das Amt für Informatik für die Informationssicherheit verantwortlich. Die Stabsstelle hat einen nur sehr eingeschränkten Einfluss auf die technische Ausgestaltung der Arbeitsplätze. Generell weisen aber alle staatlichen Stellen ein sehr hohes Sicherheitsniveau auf. Die Stabsstelle Cyber-Sicherheit steht zudem im ständigen Kontakt mit dem Amt für Informatik (Abteilung Information Security) und tauscht sich dabei in regelmässigen Sitzungen über aktuelle Bedrohungen aus.

Vertrauliche Informationen als auch entsprechend kritische Daten werden zukünftig in eigenen Systemen des CSIRT verarbeitet werden. Die detaillierte Architektur steht noch nicht fest. Doch es wird sichergestellt werden, dass die von

der Stabsstelle selbst betriebenen Systeme höchsten Sicherheitsstandards entsprechen.

Das Personal bei der Stabsstelle wird gemäss den Anforderungen dieses Gesetzes rekrutiert und nimmt regelmässig an Fortbildungen teil. So wird sichergestellt, dass die notwendigen Qualifikationen für die Wahrnehmung der Aufgaben vorhanden sind. Aufgrund des Zugangs zu klassifizierten Informationen unterzieht sich sämtliches Personal gemäss der Verordnung über den Schutz von Informationen des Landes (Informationsschutzverordnung; ISchV) einer Personensicherheitsprüfung.

Beim Zugriff auf qualifizierte Dritte gemäss Art. 9 Abs. 2 wird die Stabsstelle Cyber-Sicherheit sicherstellen, dass diese den jeweiligen Anforderungen genügen. Die finanziellen Mittel zur Aufgabenerfüllen sind vorhanden.

Die Regierung nutzt die Gelegenheit darauf hinzuweisen und eine allfällige überhöhte Erwartungshaltung dahingehend zu berichtigen, dass es nicht Aufgabe der Stabsstelle Cyber-Sicherheit ist, die Cybersicherheit im weitesten Sinn im Land Liechtenstein zu gewährleisten. Eine einzelne Stelle könnte dies auch gar nicht leisten. Vielmehr etabliert sich die Stabsstelle als zentrale Anlaufstelle für sämtliche Belange im Umgang mit Cyberrisiken, als Drehscheibe, Vermittlungs- und Verbindungsstelle für die Bevölkerung, die Wirtschaft, der kritischen Infrastrukturen sowie der Behörden. Die wesentlichen Aufgaben finden sich in Art. 13 und Art. 19.

Die Stabsstelle Cybersicherheit unterstützt insbesondere die Betreiber wesentlicher Dienste, die Wirtschaft sowie die Behörden dahingehend, dass sie etwa relevante Informationen zur Gewährleistung der Sicherheit von Netz- und Informationssystemen oder zur Vorbeugung von Sicherheitsvorfällen erstellt und an betroffene Stellen weitergibt.

Cybersicherheit verlangt eigenverantwortliches Handeln und Massnahmen jedes einzelnen Betreibers von Netz- und Informationssystemen sowie von Anbietern digitaler Dienste und aller sonstigen Stellen.

Ebenso merkt der Liechtensteinische Bankenverband an, dass die Vernetzung und Zusammenarbeit mit dem Nationalen Zentrum für Cybersicherheit in der Schweiz (NCSC) sowie den europäischen CSIRTs weiter vorangetrieben werden solle.

Die Regierung teilt die Einschätzung des Bankenverbandes und sieht die Vernetzung als ein wesentliches Element, um die Stabsstelle Cyber-Sicherheit auch als zentrale Anlaufstelle für sämtliche Belange im Umgang mit Cyber-Risiken zu positionieren. Sie wird als Drehscheibe, Vermittlungs- und Verbindungsstelle für die Bevölkerung, die Wirtschaft, der kritischen Infrastrukturen sowie der Behörden fungieren. Die Stabsstelle Cyber-Sicherheit steht bereits im engen Kontakt mit dem Nationalen Zentrum für Cybersicherheit in der Schweiz. Mit der raschen Übernahme der Richtlinie (EU) 2016/1148 eröffnet sich in weiterer Folge die Möglichkeit der Mitarbeit im CSIRT-Netzwerk. Wie einleitend unter Abschnitt 4.2.1 beschrieben, ist dies ebenso ein Grund dafür, dass die Richtlinie (EU) 2016/1148 so rasch als möglich umgesetzt werden soll.

Zu Art. 13

Die gegenständliche Bestimmung entspricht inhaltlich Art. 10 der Vernehmlassungsvorlage und hat entsprechende redaktionelle Anpassungen erfahren. Der Abs. 1 Bst. a des Vernehmlassungsentwurfs wurde in Art. 9 Abs. 1 aufgenommen.

Die Aufgaben der Stabsstelle Cyber-Sicherheit gemäss **Abs. 1** sind sowohl strategischer als auch operativer Natur und umfassen Tätigkeiten von der Überprüfung der Sicherheitsanforderungen sowie die Einhaltung der Meldepflichten (Bst. a), über die Koordination einer NIS-Strategie (Bst. m), bis zur

Vertretung Liechtensteins in Gremien im EWR und in internationalen Gremien (Bst. n).

Bst. a hebt einen wesentlichen Teil der Überwachung hervor, welche die Überprüfung von Sicherheitsvorkehrungen (Art. 4 und 6) und die Einhaltung der Meldepflichten bei Betreibern wesentlicher Dienste und Anbieter digitaler Dienste (Art. 5 und 7) betrifft. Bei Kontrollen nach Art. 18 werden insbesondere die Überprüfungen der implementierten Sicherheitsmassnahmen als auch die Einhaltung der Meldepflicht in der Praxis den Schwerpunkt der Kontrolltätigkeit der Stabsstelle Cyber-Sicherheit darstellen. Es sind jedoch keine periodischen Kontrollen seitens der Stabsstelle Cyber-Sicherheit vorgegeben. Die Betreiber wesentlicher Dienste sowie die Anbieter digitaler Dienste sollen mit der Stabsstelle Cyber-Sicherheit vielmehr im engen regelmässigen Austausch in Bezug auf die Einhaltung der entsprechenden Bestimmungen stehen. Im Falle einer Kontrolle werden durch die Stabsstelle Cyber-Sicherheit einschlägige Normen und Standards in Bezug auf die Kontrolltätigkeit eingehalten. So wird der Ablauf bei einer angekündigten Kontrolle beispielsweise jedenfalls vorsehen, dass mit der zu kontrollierenden Stelle eine Vorbesprechung durchgeführt wird, in welchem der Umfang sowie der detaillierte Ablauf der Kontrolle besprochen werden. Auf eine Dokumentenprüfung folgt nicht in allen Fällen zwingend eine Prüfung und Abklärungen vor Ort. Die Notwendigkeit wird im Einzelfall in Absprache mit der kontrollierten Stelle entschieden. Weitere Ausführungen zur Kontrolltätigkeit finden sich in den Erläuterungen zu Art. 18.

Bst. b legt fest, dass die Einrichtung und Koordination des Computer-Notfallteams (CSIRT) nach Art. 19 zur Gewährleistung der Sicherheit von Netz- und Informationssystemen eine weitere Aufgabe der Stabsstelle Cyber-Sicherheit darstellt.

*Auf Vorschlag des **Liechtensteinischen Bankenverbands** wird in Art. 13 Abs. 1 Bst. b vorgesehen, dass die Stabsstelle Cyber-Sicherheit – anstelle des «Betriebs», wie in der Vernehmlassungsvorlage – für die Einrichtung und die Koordination des Computer-Notfallteams gemäss Art. 19 zuständig ist.*

Insbesondere zwecks der Erstellung von Lagebildern und zur Durchführung von Analysen ist es die Aufgabe der Stabsstelle Cyber-Sicherheit gemäss **Bst. c**, Meldungen über Risiken oder Sicherheitsvorfälle entgegenzunehmen und zu analysieren. Bei Bedarf können diese Meldungen sowie das erstellte Lagebild mitsamt allfälligen zusätzlichen relevanten Informationen in weiterer Folge an inländische Behörden oder auch andere betroffene (öffentliche als auch nicht öffentliche) Stellen weitergeleitet werden.

Die Stabsstelle Cyber-Sicherheit trägt dafür Sorge, dass vertrauenswürdige Kanäle für den Informationsaustausch vorhanden sind und genutzt werden. Bei der Erfüllung der Meldepflichten achtet die Stabsstelle Cyber-Sicherheit besonders darauf, dass Informationen über die Anfälligkeit von Produkten bis zur Veröffentlichung der entsprechenden Sicherheitsupdates und -fixes vertraulich bleiben.

Bst. d ergänzt die zuvor erwähnte Aufgabe mit jener, dass die Erstellung und Weitergabe von relevanten Informationen, die beispielsweise nicht auf Meldungen nach Art. 5, Art. 7 und Art. 8 basieren, zur Gewährleistung der Sicherheit von Netz- und Informationssystemen oder zur Vorbeugung von Sicherheitsvorfällen ebenso eine Aufgabe der Stabsstelle Cyber-Sicherheit darstellt.

Bst. e legt fest, dass die Stabsstelle Cyber-Sicherheit die Betreiber wesentlicher Dienste ermittelt sowie die wesentlichen Dienste in einer Liste festhält. Regelmässig, jedoch mindestens alle zwei Jahre wird diese Liste der wesentlichen

Dienste durch die Stabsstelle überprüft und bei Bedarf aktualisiert. Mit dieser Aufgabe wird Art. 5 Abs. 3 und 5 der Richtlinie (EU) 2016/1148 umgesetzt.

Bei der Beurteilung, ob eine Einrichtung oder eine Stelle Dienste erbringen, die für die Aufrechterhaltung kritischer gesellschaftlicher oder wirtschaftlicher Tätigkeiten wesentlich sind, arbeitet die Stabsstelle Cyber-Sicherheit mit dem Amt für Bevölkerungsschutz zusammen.

Voraussetzung für die Ermittlung eines Betreibers wesentlicher Dienste ist, dass ein Sitz in Liechtenstein und die effektive und tatsächliche Ausübung einer Tätigkeit durch eine ständige Einrichtung im Land besteht. Die Rechtsform einer solchen Einrichtung, gleich, ob es sich um eine Zweigstelle oder eine Tochtergesellschaft mit eigener Rechtspersönlichkeit handelt, ist dabei unerheblich.

Es ist durchaus möglich, dass Einrichtungen in den in Art. 1 Abs. 1 Bst. a aufgeführten Sektoren sowohl wesentliche als auch nicht wesentliche Dienste erbringen. Betreiber wesentlicher Dienste sollten den spezifischen Sicherheitsanforderungen nur in Bezug auf die als wesentlich geltenden Dienste unterworfen sein.

Nach **Bst. f** sind die Unterrichtung und Weiterleitung von durch den Betreiber wesentlicher Dienste bereitgestellten Informationen an den bzw. die anderen betroffenen EWR-Mitgliedstaaten eine weitere Aufgabe der Stabsstelle Cyber-Sicherheit. Die Unterrichtung und Weiterleitung erfolgt jedoch lediglich in jenen Fällen, in denen ein Sicherheitsvorfall erhebliche Auswirkungen auf die Verfügbarkeit wesentlicher Dienste in einem oder mehreren anderen EWR-Mitgliedstaaten hat.

Der Stabsstelle Cyber-Sicherheit obliegt nach **Bst. g** die Koordination der öffentlich-privaten Zusammenarbeit im Bereich der Sicherheit von Netz- und

Informationssystemen. Diese zentrale Schnittstellenfunktion des Landes zu Gesellschaft, Wirtschaft und Wissenschaft im Bereich der Netz- und Informationssystemsicherheit nimmt die Stabsstelle Cyber-Sicherheit beispielsweise in Form des Nationalen Koordinierungszentrums Cybersicherheit (NCC-LIE) im Sinne der Verordnung (EU) 2021/887⁵ wahr. Als Nationales Koordinierungszentrum Cybersicherheit für Liechtenstein bemüht sich die Stabsstelle Cyber-Sicherheit um Kooperationen, beispielsweise mit der Universität Liechtenstein, mit dem Amt für Volkswirtschaft (AVW) sowie der Stabsstelle Finanzplatzinnovation und Digitalisierung (SFID) und bildet als Teil des EWR-weiten Netzwerks nationaler Koordinierungszentren zusammen mit dem Europäischen Kompetenzzentrum für Cybersicherheit (ECCC) den neuen europäischen Rahmen zur Unterstützung der Innovations- und Industriepolitik im Bereich der Cybersicherheit.

Mit dieser Bestimmung wird die Verordnung (EU) 2021/887 entsprechend durchgeführt.

Die **NetSec.co AG** schlägt vor, die Förderung der allgemeinen Cyber-Sicherheit als zusätzliche Aufgabe zu definieren.

Die Förderung der Cybersicherheit wird mit der Durchführung der Verordnung (EU) 2021/887 bereits entsprechend adressiert. So wird die Stabsstelle Cyber-Sicherheit federführend das Nationale Koordinierungszentrums für Cybersicherheit in Liechtenstein (NCC-LIE) koordinieren.

Die Nationalen Koordinierungszentren im EWR stellen Fachwissen für die strategischen Aufgaben bereit und unterstützen aktiv bei diesen Aufgaben, unter

⁵ 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. 202 vom 8.6.2021, S. 1).

Berücksichtigung der einschlägigen nationalen und regionalen Herausforderungen für die Cybersicherheit in verschiedenen Sektoren. 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 EU finanziert werden, und ermutigen diese zur Teilnahme. 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.

Dem Anliegen der NetSec.co AG wird mit der gegenständlichen Aufgabe bereits entsprochen und die Regierung sieht die Aufnahme einer zusätzlichen Aufgabe nicht als notwendig.

*Auf Ersuchen des **Liechtensteinischen Bankenverbands** führt die Regierung weiter aus, dass der Stabsstelle Cyber-Sicherheit nach Bst. g die Gesamtkoordination und Schnittstellenfunktion gemäss der Verordnung (EU) 2021/887 obliegt. Als NCC-LIE ist derzeit eine Zusammenarbeit zwischen verschiedenen bereits bestehenden öffentlichen Stellen geplant. Aktuell wird eine Kooperation zwischen der Stabsstelle Cyber-Sicherheit, der Universität Liechtenstein, konkret der Hilti-Professur für Daten und Anwendungssicherheit (vormals Institut für Wirtschaftsinformatik, Hilti Lehrstuhl für Daten- und Anwendungssicherheit), dem Amt für Volkswirtschaft (AVW), konkret der Abteilung Technologie/Innovation und Energie bzw. der Nationalen Kontaktstelle für Forschung und technologische Entwicklung, sowie der Stabsstelle für Finanzplatzinnovation und Digitalisierung (SFID), als bevorzugte Variante für die Ausgestaltung des NCC geprüft.*

Zudem wird zwecks Aufgabenerfüllung in Abs. 2 eine entsprechende Bestimmung zur Ermöglichung von Public Private Partnerships (PPP) im Bereich Cybersicherheit geschaffen.

Da sämtliche Aufgaben zentral bei der Stabsstelle Cyber-Sicherheit konzentriert sind, können Synergieeffekte – auch in Bezug auf die Aufgaben des CSIRT – genutzt werden.

Bst. h legt fest, dass die Unterrichtung sowie die Sensibilisierung der Öffentlichkeit über Sicherheitsvorfälle sowie die Veröffentlichung allgemeiner Informationen im Zusammenhang mit der Sicherheit von Netz- und Informationssystemen weitere Aufgaben der Stabsstelle Cyber-Sicherheit sind. Für die Öffentlichkeitsarbeit bedient sich die Stabsstelle Cyber-Sicherheit verschiedenster Kanäle, wie beispielsweise der eigenen Internetseite oder auch Newslettern.

Informationen über Sicherheitsvorfälle sind für die Öffentlichkeit und Unternehmen, insbesondere für kleine und mittlere Unternehmen, zunehmend von Bedeutung. Daher ist es das Ziel der Stabsstelle Cyber-Sicherheit, dass sie regelmässig derartige Informationen mit besonderem Schwerpunkt auf Sicherheitsvorfälle und Sicherheitsereignisse mit nationalem Bezug bereitstellt.

Die **Wasserversorgung Liechtensteiner Unterland e. G.** führt in ihrer Stellungnahme zur Vernehmlassung aus, dass die Sensibilisierung als Aufgabe nicht erwähnt wird, die bei der Cybersicherheit auf Grund der rasanten Entwicklung und der zunehmenden Bedeutung der Cybersicherheit absolut zentral sei. Aus Sicht der Wasserversorgung Liechtensteiner Unterland e. G. sei es angezeigt, dass auch die präventive Aufgabe der Sensibilisierung der Betreiber wahrgenommen werden solle. Eine solche Aufgabe der Sensibilisierung der Stabsstelle sollte explizit aufgenommen werden.

Um der Sensibilisierung einen entsprechenden Stellenwert zu geben, wurde die Aufgabe unter Bst. h entsprechend erweitert und dem Anliegen der Wasserversorgung Liechtensteiner Unterland e. G. damit entsprochen.

Die **Liechtensteinische Alters- und Krankenhilfe** führt in ihrer Stellungnahme zur Vernehmlassung zu Bst. h aus, dass es zu begrüssen wäre, wenn im Gesetz auch berücksichtigt würde, dass zu den Aufgaben der Stabsstelle Cyber-Sicherheit gehören sollte, Betreiber wesentlicher Dienste in allen Fällen über gemeldete Sicherheitsvorfälle vollumfänglich zu informieren. Dies könne dazu beitragen, eigene Sicherheitsvorkehrungen zu prüfen und gegebenenfalls anzupassen, um ausschliessen zu können, dass genau derselbe Sicherheitsvorfall bei den anderen Betreibern wesentlicher Dienste eintritt. Ziel sei dabei, aus Fehlern zu lernen und entsprechende Massnahmen einzuleiten.

Dazu führt die Regierung aus, dass es gemäss Art. 13 Abs. 1 Bst. d sowie Art. 19 Abs. 1 Bst. b Aufgaben der Stabsstelle Cyber-Sicherheit sind, Betreiber wesentlicher Dienste über Gefahren zu informieren oder vor konkreten Bedrohungen zu warnen.

So ist es unter anderem eine Aufgabe des CSIRT, Frühwarnungen und Alarmmeldungen auszugeben sowie Informationen über Risiken und Sicherheitsvorfälle unter den einschlägigen Interessenträgern bekanntzumachen und zu verbreiten.

Eine Information in allen Fällen, wie dies von der Liechtensteinische Alters- und Krankenhilfe vorgeschlagen wird, würde einen erheblichen Aufwand für die Stabsstelle Cyber-Sicherheit bedeuten.

Zudem hat die Stabsstelle – vergleichbar mit einer Information der Öffentlichkeit nach Art. 5 Abs. 5 und Art. 7 Abs. 2 – die meldende Stelle entsprechend anzuhören und die Interessen der Betroffenen abzuwägen.

Sicherheitsvorfälle könnten jedoch in regelmässigen Treffen in einem geschlossenen und vertrauensvollen Rahmen mit den Betreibern wesentlicher Dienste diskutiert werden.

Die Stabsstelle Cyber-Sicherheit arbeitet mit öffentlichen Stellen, insbesondere der Landespolizei, der Staatsanwaltschaft, der Datenschutzstelle, dem Amt für Kommunikation, der Stabsstelle FIU und der Finanzmarktaufsicht Liechtenstein zusammen und tauscht zum Zweck des Schutzes der Netz- und Informationssysteme relevante Informationen aus (**Bst. i**). Häufig ist bei Sicherheitsvorfällen vor allem der Schutz personenbezogener Daten nicht mehr gewährleistet. Aus diesem Grund ist eine enge Zusammenarbeit mit der Datenschutzstelle besonders wichtig. Dabei werden beispielsweise Informationen zu einschlägigen Fragen ausgetauscht, um etwa allfälligen Verletzungen des Schutzes personenbezogener Daten aufgrund von Sicherheitsvorfällen vorzubeugen.

Ebenso profitiert die Stabsstelle Cyber-Sicherheit von der Weiterleitung von Meldungen nach Verletzungen des Schutzes personenbezogener Daten gemäss Art. 33 DSGVO an die Datenschutzstelle in Bezug auf die Erstellung eines Lagebildes (vgl. Bst. c). Mit dieser Zusammenarbeit und der Weiterleitung von Meldungen der Datenschutzstelle an die Stabsstelle Cyber-Sicherheit wird auch Art. 15 Abs. 4 der Richtlinie (EU) 2016/1148 entsprochen.

Beim Informationsaustausch mit den öffentlichen Stellen wird die Stabsstelle Cyber-Sicherheit jedoch darauf achten, dass die Interessen der Betreiber wesentlicher Dienste, der Anbieter digitaler Dienste oder ebenso der meldenden Stelle bei freiwilligen Meldungen geschützt sind. Daher wird die Informationsweitergabe seitens der Stabsstelle Cyber-Sicherheit lediglich solche Informationen enthalten, die weder die Identität einer möglicherweise

betroffenen oder meldenden Einrichtung noch Informationen, die auf diese schliessen lassen, beinhalten.

Wie die Europäische Zentralbank bereits in ihrer Stellungnahme vom 25. Juli 2014⁶ erklärt hat, berührt die Richtlinie (EU) 2016/1148 nicht die bestehenden EWR-rechtlichen Bestimmungen zur Überwachung von Zahlungsverkehrs- und Abwicklungssystemen. Die für eine derartige Überwachung verantwortliche Behörde, sprich die Finanzmarktaufsicht Liechtenstein, soll jedoch ihre Erfahrungen in Angelegenheiten der Sicherheit von Netz- und Informationssystemen mit der Stabsstelle Cyber-Sicherheit austauschen.

Die Stabsstelle Cyber-Sicherheit ist die zentrale Ansprechstelle für die Sicherheit von Netz- und Informationssystemen in Liechtenstein. Eine Aufgabe nach **Bst. k** ist die grenzüberschreitende Zusammenarbeit und der Informationsaustausch mit den zuständigen Stellen und entsprechenden Behörden in anderen EWR-Mitgliedstaaten, wie insbesondere mit der Agentur der Europäischen Union für Cybersicherheit (ENISA), der Kooperationsgruppe und dem CSIRTs-Netzwerk. Angesichts des globalen Charakters von Sicherheitsproblemen, die Netz- und Informationssysteme beeinträchtigen, bedarf es einer engen internationalen Zusammenarbeit, damit die Sicherheitsstandards und der Informationsaustausch verbessert und ein gemeinsames umfassendes Konzept für Sicherheitsfragen gefördert wird.

Der **Liechtensteinische Bankenverband** führt in seiner Stellungnahme aus, dass die Banken teilweise direkt beim Schweizer Nationalen Zentrum für Cybersicherheit (NCSC) oder dem CERT Österreich akkreditiert seien. Neben den Kompetenzen und Befugnissen der Stabsstelle sei daher auch zu regeln, wie die

⁶ Siehe unter <https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:52014AB0058>.

Reaktionszeiten der Stabsstelle und die Support-Dienstleistungen und Pflichten aussehen und ob bzw. wann eine Weitergabe der Informationen durch die Stabsstelle Cyber-Sicherheit an das Schweizer Nationale Zentrum für Cybersicherheit oder an europäische CERT zu erfolgen hat. Das Verhältnis der Stellen und Behörden untereinander, sowohl international als auch national, müsse klar und abschliessend geregelt sein.

Die Regierung führt dazu aus, dass die Reaktionszeiten oder konkrete «Dienstleistungen» der Stabsstelle Cybersicherheit gegenüber Interessensgruppen nicht auf Gesetzesstufe geregelt werden sollen. Betreffend die Präzisierungen zu den verschiedenen Aufgaben findet sich im Abs. 3 eine Verordnungskompetenz.

Betreffend das Verhältnis der Stellen und Behörden untereinander wird ausgeführt, dass die Stabsstelle Cyber-Sicherheit gemäss Art. 12 Abs. 1 und 2 die zuständige nationale Behörde nach Art. 8 Abs. 1 der Richtlinie (EU) 2016/1148 sowie die zuständige zentrale Anlaufstelle nach Art. 8 Abs. 3 der Richtlinie (EU) 2016/1148 sein wird. Sie wird die Verbindungsstelle zur Gewährleistung der grenzüberschreitenden Zusammenarbeit mit internationalen Gremien und Gruppen, wie insbesondere den zuständigen Stellen in anderen EWR-Mitgliedstaaten, der Kooperationsgruppe und dem CSIRTs-Netzwerk sein. Das Verhältnis zwischen der Stabsstelle Cyber-Sicherheit in Bezug auf die entsprechenden Stellen im EWR wird durch die die erwähnten Bestimmungen klar geregelt. Die Stabsstelle Cyber-Sicherheit wird Mitglied des CSIRTs-Netzwerks. Eine Vernetzung der CSIRTs bzw. CERTs findet neben dem erwähnten Netzwerk ebenso in anderen Zusammenschlüssen statt, wo auch eine Beteiligung von Drittstaaten, wie bspw. der Schweiz, möglich ist. Der Fluss von sicherheitsrelevanten Informationen zwischen den Ländern wird auf diese Weise sicherstellt. Wo es weiterer Regelungen bedarf, können diese gemäss Abs. 3 in eine Verordnung aufgenommen werden.

Im Zuge der Erarbeitung der Verordnung sollen die Interessensgruppen und vor allem die Betreiber wesentlicher Dienste gehört und deren Anliegen wo möglich entsprechend berücksichtigt werden.

Neben den EWR-Mitgliedstaaten pflegt die Stabsstelle Cyber-Sicherheit auch Kontakte mit vertrauenswürdigen Drittstaaten, insbesondere mit der Schweiz. Gemäss **Bst. I** ist die grenzüberschreitende Zusammenarbeit und der Informationsaustausch im Bereich der Sicherheit von Netz- und Informationssystemen mit öffentlichen und nicht öffentlichen Stellen sowie Behörden in Drittstaaten eine weitere Aufgabe der Stabsstelle.

Überdies merkt der **Liechtensteinische Bankenverband** an, dass mit dem gegenständlichen Gesetz nunmehr für den behördlichen Austausch in Art. 13 Abs. 1 Bst. k und l CSG eine Rechtsgrundlage geschaffen werde. Der Liechtensteinische Bankenverband erachtet jedoch eine ergänzende Regelung des grenzüberschreitenden Austausches sicherheitsrelevanter Informationen und Informationen zu Sicherheitsvorfällen zwischen den Betreibern wesentlicher Dienste bzw. Anbietern digitaler Dienste und privatrechtlich organisierten Branchenvereinigungen (bspw. FS-ISAC) bzw. eine Klarstellung in den Materialien, dass ein derartiger Austausch zulässig ist, für erforderlich.

Die gegenständliche Vorlage dient der Umsetzung und Durchführung der Richtlinie (EU) 2016/1148 bzw. der Verordnung (EU) 2021/887. Damit verbunden sind auch Regelungen betreffend die Aufgaben und Befugnisse der durchführenden Stellen, der Stabsstelle Cyber-Sicherheit und dem CSIRT (vgl. Art. 9 Abs. 1 Bst. a und b). Die gegenständliche Vorlage kann hier nach Ansicht der Regierung keine Regelungen betreffend den Informationsaustausch zwischen zwei privatrechtlich organisierten juristischen Personen betreffen. Doch die Stabsstelle Cyber-Sicherheit kann als durchführende Stelle nach Rücksprache mit dem zuständigen Regierungsmitglied gemäss Abs. 2 zur Aufgabenerfüllung mit Privaten im Rahmen von öffentlich-

privaten Partnerschaften zusammenarbeiten. Dieser Umstand wurde entsprechend berücksichtigt.

Bst. m adressiert die nationale Strategie zur Sicherheit von Netz- und Informationssystemen (Art. 20). Um ein hohes Sicherheitsniveau von Netz- und Informationssystemen zu erreichen und aufrechtzuerhalten, muss Liechtenstein gemäss Art. 1 Abs. 2 Bst a der Richtlinie (EU) 2016/1148 über eine nationale Strategie zur Sicherheit von Netz- und Informationssystemen verfügen, in der die strategischen Ziele sowie konkrete politische Massnahmen vorgesehen sind. Es ist Aufgabe der Stabsstelle Cyber-Sicherheit, die Erstellung einer solchen nationalen Strategie für die Sicherheit von Netz- und Informationssystemen zu koordinieren.

Die Stabsstelle Cyber-Sicherheit ist nach **Bst. n** die Vertretung von Liechtenstein in der Kooperationsgruppe, dem CSIRTs-Netzwerk sowie in anderen EWR-weiten und internationalen Gremien für die Sicherheit von Netz- und Informationssystemen.

Unter anderem vom **Liechtensteinischen Bankenverband** wurde angeregt, der Stabsstelle Cyber-Sicherheit die Kompetenz zum Abschluss von Vereinbarungen für die Zusammenarbeit (z. B. in Form eines Memorandum of Understanding, MoU) mit Partnern zu übertragen.

*Mit **Abs. 2** wird dieser Anregung Rechnung getragen. Abs. 2 erlaubt es der Stabsstelle Cyber-Sicherheit nach Rücksprache mit dem zuständigen Regierungsmitglied mit anderen in- und ausländischen Behörden Vereinbarungen über die Modalitäten der Zusammenarbeit abzuschliessen sowie zur Aufgabenerfüllung mit Privaten im Rahmen von öffentlich-privaten Partnerschaften zusammenzuarbeiten.*

Mit **Abs. 3** bekommt die Regierung eine Verordnungskompetenz und kann das Nähere über die Aufgaben der Stabsstelle Cyber-Sicherheit mit Verordnung regeln.

Zu Art. 14

Neben den Aufgaben nach Art. 13 wird die Stabsstelle Cyber-Sicherheit mit den zur Erfüllung ihrer Aufgaben erforderlichen Befugnissen gegenüber Betreibern wesentlicher Dienste ausgestattet. Mit **Abs. 1** wird Art. 15 Abs. 1 und 2 der Richtlinie (EU) 2016/1148 umgesetzt.

Die Stabsstelle Cyber-Sicherheit kann bei der Wahrnehmung ihrer Aufgaben nach diesem Gesetz von den Betreibern wesentlicher Dienste verlangen, dass sie ihr die zur Bewertung der Sicherheit ihrer Netz- und Informationssysteme erforderlichen Informationen, einschliesslich der dokumentierten Sicherheitsmassnahmen, zur Verfügung stellen (**Bst. a**), Nachweise für die wirksame Umsetzung der Sicherheitsmassnahmen erbringen (**Bst. b**) sowie Informationen, insbesondere technische und statistische Daten, zu statistischen Zwecken oder für die Erstellung konkreter Lagebilder unentgeltlich offenlegen (**Bst. c**).

Der Art. 14 entspricht im Kern Art. 11 der Vernehmlassung, welcher jedoch in der gegenständlichen Vorlage redaktionell angepasst wurde.

Die **Liechtensteinischen Kraftwerke** regen in ihrer Stellungnahme an, dass sich die Überprüfungen auf ein definiertes und kalkulierbares Zeitfenster beschränken sollen und schlägt daher vor, eine Anpassung der Bst. a und b wie folgt vorzunehmen: «a) die zur Bewertung der Sicherheit ihrer Netz- und Informationssysteme erforderlichen Informationen im Rahmen eines zeitlich befristeten Audits, einschliesslich der dokumentierten Sicherheitsmassnahmen, zur Verfügung stellen, welche von der Stabsstelle Cyber-Sicherheit und

beauftragten Dritten, innert einer Frist von 4 Wochen wieder vollständig vernichtet werden» Der Bst. b könne auf Grundlage des neuen Artikels gestrichen werden, da ein Audit auch die Erbringung von Nachweisen umfasse.

Die Regierung führt hierzu aus, dass im Hinblick auf die Stellungnahme der Liechtensteinischen Kraftwerke Art. 14 nach der Vernehmlassung redaktionell angepasst wurde. Mit Art. 14 Abs. 1 Bst. a und b wird etwa Art. 15 Abs. 2 Bst. a und b der Richtlinie (EU) 2016/1148 umgesetzt.

Informationen über Sicherheitsmassnahmen zur Verfügung zu stellen kann nicht mit dem Nachweis der wirksamen Umsetzung gleichgestellt werden. So wäre es beispielsweise durchaus möglich, dass es dokumentierte Sicherheitsmassnahmen in einem Unternehmen gibt, welche jedoch in der Praxis nicht korrekt oder unwirksam implementiert wurden. Aus diesem Grund bedarf es durchaus der Unterscheidung von Bst. a und b in der aktuellen Vorlage.

Was die zeitlichen Befristungen betrifft, ist die Regierung der Auffassung, dass Art. 14 nicht die passende Bestimmung ist, um diesen Punkt zu adressieren. Vielmehr werden in Art. 14 die Befugnisse der Stabsstelle Cyber-Sicherheit gegenüber Betreibern wesentlicher Dienste geregelt. Für die Audits bzw. die Kontrollen im Allgemeinen finden sich die entsprechenden Regelungen in Art. 18. An dieser Stelle sieht die aktuelle Vorlage zudem eine Verordnungskompetenz in Abs. 3 vor, wonach die Regierung das Nähere über die Durchführung von Kontrollen mit Verordnung regeln kann. Weitere Ausführungen zu den Kontrollen finden sich unter den Erläuterungen zu Art. 18.

Die **NetSec.co AG** schlägt in ihrer Stellungnahme vor, dass die Betreiber ihre Risikoanalyse, die die Bewertung der Risiken und die risikoreduzierenden Massnahmen enthält, ebenfalls offenlegen müssen. Nach Ansicht der NetSec.co

AG könne nur damit beurteilt werden, ob die Risiken realistisch beurteilt wurden und die getroffenen Sicherheitsmassnahmen zweckmässig und ausreichend sind.

Sämtliche für die «Bewertung der Sicherheit ihrer Netz- und Informationssysteme erforderlichen Informationen» sind von Art. 14 Abs. 1 umfasst. Die Regierung ist daher der Meinung, dass es keiner expliziten Nennung einer Risikoanalyse oder anderer, unter Umständen ebenfalls relevanter, Dokumente bedarf. Vielmehr werden nach Ansicht der Regierung die für die Bewertung der Sicherheit der Netz- und Informationssysteme erforderlichen Informationen jeweils vom Einzelfall abhängen. Diese Informationen können im Einzelfall jedenfalls auch eine Risikoanalyse umfassen.

Der **Liechtensteinische Bankenverband** erachtet es in seiner Stellungnahme als kritisch, dass durch Art. 14 und 18 faktisch eine weitere Aufsichtsbehörde für den Finanzbereich geschaffen wird. Die alleinige Aufsichtsbehörde für Banken solle weiterhin die Finanzmarktaufsicht Liechtenstein bleiben. Der Lex specialis Vorbehalt des Art. 1 Abs. 7 der Richtlinie (EU) 2016/1148 müsse generell nicht nur betreffend Sicherheitsanforderungen allgemein und Meldepflichten gelten, sondern auch betreffend Überwachung und Kontrolle.

Die Regierung verweist hier auf die Ausführungen und Erläuterungen unter Art. 18. Die Regierung betont in diesem Zusammenhang explizit, dass der Lex specialis Vorbehalt nicht nur Sicherheitsanforderungen und Meldepflichten, sondern auch die Überwachung sowie die Kontrolle umfasst.

Gestützt auf **Bst. c** kann die Stabsstelle Cyber-Sicherheit von Betreibern wesentlicher Dienste Informationen zu allgemeinen Fragen betreffend die Sicherheit der Netz- und Informationssysteme oder auch statistische Daten in Bezug auf die Sicherheit der Netz- und Informationssysteme erheben, um

beispielsweise ein Lagebild nach Art. 13 Abs. 1 Bst. c zu erstellen. Die Offenlegung gegenüber der Stabsstelle Cyber-Sicherheit hat unentgeltlich zu erfolgen.

Der Bst. c entspricht im Kern Art. 11 Abs. 2 der Vernehmlassung, wobei der Zweck der Bestimmung dahingehend erweitert wurde, dass nun neben den statistischen Zwecken auch der Zweck «Erstellung konkreter Lagebilder» mit aufgenommen wurde.

Die **Liechtensteinischen Kraftwerke** führen in ihrer Stellungnahme aus, dass es sich gegenständlich bei anonymisierten oder nicht anonymisierten Daten in jedem Fall stets um hoch vertrauliche Informationen handle und diese sollten nicht uneingeschränkt aufbewahrt werden dürfen. Es wird daher eine Anpassung der Bestimmung wie folgt vorgeschlagen: «Sofern zu statistischen Zwecken Originaldaten zur Verfügung gestellt werden müssen, müssen diese von der Stabsstelle Cyber-Sicherheit innert 6 Monate vollständig und unwiederbringlich vernichtet werden. Können die Daten anonymisiert zur Verfügung gestellt werden, sind diese innert einem Jahr vollständig und unwiederbringlich zu vernichten.»

Die Regierung ist der Ansicht, dass es zur Erkennung aktueller Entwicklungen und Trends im Bereich der Cybersicherheit, beispielsweise für die Analyse von Risiken sowie für die allgemeine Lagebeurteilung im Sinne des Art. 19 Abs. 1 Bst. d, es neben tagesaktueller auch historischer Daten bedarf.

Der Stabsstelle Cyber-Sicherheit stehen dabei verschiedenste Datenquellen zur Verfügung. Dies sind unter anderem Meldungen gemäss Art. 5 und Art. 7 als auch Informationen aus der nationalen wie internationalen Zusammenarbeit gemäss Art. 13 Abs. 1 Bst. i bis l. Sämtliche erhobenen Informationen werden bei der Stabsstelle Cyber-Sicherheit der Schutzstufe entsprechend verarbeitet und aufbewahrt. Die erhobenen Daten sollen bei Stabsstelle solange aufbewahrt

werden, wie sie für die Zweckerreichung, sprich zu statistischen Zwecken oder für die Erstellung konkreter Lagebilder, erforderlich sind. Die Aufnahme einer konkreten Aufbewahrungsfrist in das gegenständliche Gesetz erachtet die Regierung als dem Ziel der Zweckerreichung entgegenwirkend.

Ebenso sehen die Richtlinie (EU) 2016/1148 sowie die Durchführungsverordnung 2018/151 keine Aufbewahrungsfrist vor.

Weiters führen die **Liechtensteinischen Kraftwerke** in ihrer Stellungnahme aus, dass nicht ausgeführt sei, wem und in welcher Form die Stabsstelle Cyber-Sicherheit über die von ihr oder beauftragten Dritten erlangten, aus Sicht der Liechtensteinischen Kraftwerke auch auf Landesebene gegebenenfalls hoch vertraulichen Informationen und Erkenntnisse, öffentlich oder auch nichtöffentlich Bericht erstattet. Ebenso sei nicht ausgeführt, wie in diesem Zusammenhang einerseits die Informationswege (Thema: hoch verschlüsselte Datenübertragung) als auch die Geheimhaltung geregelt sei, um einen unbefugten Zugriff zu verhindern.

Dazu führt die Regierung aus, dass mit dem gegenständlichen Gesetz ein hohes Sicherheitsniveau von jenen Netz- und Informationssystemen erreicht werden soll, die von Betreibern wesentlicher Dienste in den bestimmten Sektoren sowie von Anbietern digitaler Dienste betrieben werden (vgl. Art. 1). Die gegenständliche Vorlage sieht keine explizite Berichterstattungspflicht für die Stabsstelle Cyber-Sicherheit vor, gemäss derer vertrauliche Informationen und Erkenntnisse weitergegeben werden. Vielmehr baut die Stabsstelle Cyber-Sicherheit auf Vertrauen, um ihre Aufgaben ordnungsgemäss erfüllen zu können.

Jegliche Weitergabe von Informationen, sei es an konkrete Empfänger oder auch an die Öffentlichkeit, berücksichtigt jeweils die Interessen der Informationsquelle. Der Art. 5 Abs. 5 oder der Art. 7 Abs. 2 sind dabei analog anzuwenden.

Erkenntnisse werden vor ihrer Weitergabe oder Veröffentlichung in allen Fällen derart bearbeitet, dass dem Schutzziel der Vertraulichkeit entsprochen wird.

Schon jetzt nimmt die SCS freiwillig Meldungen über Sicherheitsvorfälle entgegen, auch aus sehr sensiblen Bereichen. Doch gerade aus diesen sensiblen Meldungen generiert die Stabsstelle Cyber-Sicherheit wichtige Erkenntnisse über die Cyberlage in Liechtenstein, die in weiterer Folge den betroffenen Betreibern wesentlicher Dienste aufbereitet und auf eine solche Art und Weise und verallgemeinert zur Verfügung gestellt werden, dass auch tatsächlich ein Mehrwert entsteht.

Die Kenntnis über die aktuellen Bedrohungen und laufende Angriffe ist auch im internationalen Austausch für die SCS von zentraler Bedeutung, damit dort gezielt nach Unterstützung und Werkzeugen angefragt werden kann.

Der Austausch und die Analyse von Informationen – auch über einen längeren Zeitraum hinweg – ist eines der wichtigsten Elemente, um die (Cyber-)Sicherheit zu erhöhen.

Zur Sicherstellung der Vertraulichkeit bedient sich die Stabsstelle Cyber-Sicherheit im täglichen Betrieb der Werkzeuge der Liechtensteinischen Landesverwaltung, wobei für Datenübermittlungen mit einem besonderen Schutzbedarf eigene Endgeräte mit entsprechender Ende-zu-Ende-Verschlüsselung verwendet werden.

Im Einzelfall wird es der Stabsstelle Cyber-Sicherheit auch möglich sein, mit der Gegenstelle einen sicheren Kommunikationskanal zu vereinbaren und diesen aufzusetzen.

Die **NetSec.co AG** schlägt in ihrer Stellungnahme weiter vor, dass diese Daten der Stabsstelle Cyber-Sicherheit in einem automatisch verarbeitbaren digitalen Format offengelegt werden müssen. Zudem wird seitens der NetSec.co AG vorgeschlagen, diesen Artikel so zu ergänzen, dass die Betreiber auch verpflichtet

sind, Log-Daten für eine bestimmte Zeit (z.B. 18 Monate) aufzubewahren, so dass diese bei Bedarf für forensische Analysen verwendet werden können.

Es wird davon ausgegangen, dass es sich bei Informationen in Netz- und Informationssystemen per Definition gemäss Art. 3 Abs. 1 Bst. a Ziff. 3 um digitale Daten handelt. Demnach können diese digital oder in einem anderen maschinenlesbaren Format vorhanden Informationen ohne grossen Aufwand der Stabsstelle Cyber-Sicherheit gegenüber offengelegt werden.

Betreffend die Aufbewahrung hält die Regierung fest, dass die Protokollierung Teil der Sicherheitsanforderungen nach Art. 4 ist, welche einen Betreiber wesentlicher Dienste jeweils verpflichten, geeignete und verhältnismässige technische und organisatorische Massnahmen zu implementieren. Je nach Netz- und Informationssystem werden unterschiedliche Protokolldaten generiert, welche unterschiedlichen Zwecken dienen. Die Aufnahme einer konkreten Aufbewahrungsfrist in das gegenständliche Gesetz scheint der Regierung nicht sinnvoll.

So sehen etwa die Richtlinie (EU) 2016/1148 sowie die Durchführungsverordnung 2018/151 ebenso keine Aufbewahrungsfrist vor.

Der **Liechtensteinische Bankenverband** merkt in seiner Stellungnahme zur Vernehmlassung an, dass es nicht verständlich sei, weshalb allfällige zusätzliche Aufwände der Banken, welche durch die Erhebung/Aufbereitung der Daten, gegebenenfalls sogar unter Einbezug externer Stellen/Dienstleister, entstehen, nicht abgegolten werden. Der Liechtensteinische Bankenverband bittet um Ergänzung des Wortlauts derart, dass «Die Offenlegung [...] unentgeltlich zu erfolgen [hat], sofern dadurch dem Betreiber kein unverhältnismässiger Mehraufwand entsteht.»

Die Regierung erklärt dazu, dass diese Bestimmung der Stabsstelle Cyber-Sicherheit die Möglichkeit gibt, die bei den Betreibern wesentlicher Dienste in vielen Fällen ohnehin vorliegenden (technischen und statistischen) Informationen für statistische Zwecke oder einer ersten Lagebeurteilung heraus zu verlangen.

Bei der Einholung der technischen und statistischen Daten wird die Stabsstelle Cyber-Sicherheit darauf achten, dass es sich jeweils um solche technische oder statistische Informationen handelt, die ohne unverhältnismässigen Mehraufwand durch die Betreiber wesentlicher Dienste zur Verfügung gestellt werden können. Beispielsweise, weil die Daten ohnehin verfügbar sein sollten, da sie durch technische oder organisatorische Sicherheitsmassnahmen generiert werden, die als Teil der Sicherheitsanforderungen gemäss Art. 4 implementiert sein müssten. Die Regierung bleibt deshalb bei der ursprünglichen Formulierung.

Die Offenlegung von Informationen gegenüber der Stabsstelle Cyber-Sicherheit betreffend die Sicherheit der Netz- und Informationssysteme, einschliesslich der dokumentierten Sicherheitsmassnahmen oder auch technische und statistische Daten gemäss Abs. 1 Bst. c können gemäss **Abs. 2** von Betreibern wesentlicher Dienste nicht wegen Berufs-, Geschäfts- oder Betriebsgeheimnissen verweigert werden.

Zu Art. 15

In der Vernehmlassung fanden sich die Befugnisse gegenüber Anbietern digitaler Dienste in zwei Absätzen des Art. 12. Die beiden Absätze wurden in der gegenständlichen Gesetzesvorlage zusammengefasst.

Im Vergleich zu Betreibern wesentlicher Dienste unterliegen Anbieter digitaler Dienste weniger strikten reaktiven Aufsichtstätigkeiten (ex-post), die durch die Art ihrer Dienste und Tätigkeiten gerechtfertigt sind. Die Stabsstelle Cyber-Sicherheit wird daher nur dann tätig, wenn ihr z. B. durch den Anbieter digitaler Dienste

selbst, durch eine andere zuständige Behörde – auch der eines anderen EWR-Vertragsstaates – oder durch einen Nutzer des digitalen Dienstes Nachweise dafür vorgelegt werden, dass ein Anbieter digitaler Dienste die Anforderungen dieses Gesetzes nicht erfüllt. Dies ist vor allem nach einem Sicherheitsvorfall relevant. Die Stabsstelle Cyber-Sicherheit hat daher keine generelle, sondern bloss eine anlassbezogene Befugnis und Verpflichtung zur Beaufsichtigung der Anbieter digitaler Dienste.

Die Stabsstelle Cyber-Sicherheit kann von den Anbietern digitaler Dienste verlangen, dass diese die zur Beurteilung der Sicherheit ihrer Netz- und Informationssysteme erforderlichen Informationen (Dokumentation) unverzüglich zur Verfügung stellen. Art. 2 Abs. 2 der Durchführungsverordnung (EU) 2018/151 verpflichtet die Anbieter digitaler Dienste zur Führung angemessener Dokumentationen, anhand derer die zuständige Behörde, sprich die Stabsstelle Cyber-Sicherheit, die Einhaltung der Sicherheitselemente bei Bedarf überprüfen kann.

Der **Liechtensteinische Bankenverband** führt in seiner Stellungnahme erneut aus, dass er die Kontrollbefugnisse aufgrund von Lex specialis gegenüber Banken eingeschränkt sieht.

Die Regierung verweist in diesem Zusammenhang auf die ausführlichen Erläuterungen zu Lex specialis im Bereich Bankwesen und Finanzmarktinfrastruktur in Abschnitt 4.2.2.

Die Offenlegungspflicht könne sich laut **Liechtensteinischem Bankenverband** zudem nur auf jene Netz- und Informationssysteme beziehen, die zur Bereitstellung digitaler Dienste genutzt werden. Ebenso dürfe die Pflicht zur unverzüglichen Offenlegung den operativen Betrieb einer kritischen Infrastruktur nicht beeinträchtigen. Hier erscheine laut Liechtensteinischem Bankenverband

Augenmass wichtig sowie angemessene Fristen, um eine Bereitstellung der Informationen in guter Qualität zu ermöglichen.

Gegenständlich ist zu berücksichtigen, dass die Stabsstelle Cyber-Sicherheit gegenüber Anbietern digitaler Dienste, im Unterschied zu Betreibern wesentlicher Dienste, lediglich eingeschränkte Befugnisse besitzt. So ist das Herausverlangen von Informationen nur in jenen Fällen möglich, wenn bereits ein Nachweis vorliegt, dass der betreffende Anbieter etwa die Sicherheitsanforderungen nach Art. 6 nicht einhält. Lediglich ein Verdacht genügt hier nicht. Dieser Faktor muss bei der Auslegung des Begriffs «unverzüglich» berücksichtigt werden. So kann es durchaus geboten sein, hier rasch zu handeln und die Sicherheit der Netz- und Informationssysteme eines Anbieters digitaler Dienste zeitnah und ohne unnötigen Aufschub zu beurteilen.

Kontrollen der Stabsstelle Cyber-Sicherheit sind grundsätzlich unter möglicher Schonung von Betrieb und Ressourcen der kontrollierten Stelle durchzuführen. Weitere Ausführungen dazu finden sich in den Erläuterungen zu Art. 18.

Zu Art. 16

Mit dieser Bestimmung werden die Art. 15 und 17 der Richtlinie (EU) 2016/1148 (Durchsetzung) umgesetzt.

Inhaltlich enthält Art. 16 die Bestimmungen des Art. 18 (Aufforderungen seitens der Stabsstelle Cyber-Sicherheit) der Vernehmlassungsvorlage.

Abs. 1 entspricht Art. 18 Abs. 1 der Vernehmlassungsvorlage und legt fest, dass sofern die Stabsstelle Cyber-Sicherheit Anhaltspunkte dafür hat, dass ein Betreiber wesentlicher Dienste oder Anbieter digitaler Dienste gegen Vorschriften dieses Gesetzes, der dazu erlassenen Verordnungen oder gegen darauf gestützte Entscheidungen oder Verfügungen verstösst, sie dem Betreiber wesentlicher Dienste oder dem Anbieter digitaler Dienste eine angemessene Frist setzt und

diesen formlos auffordert, eine entsprechende Stellungnahme abzugeben (**Bst. a**) oder aber den geforderten rechtmässigen Zustand herzustellen (**Bst. b**).

Anhaltspunkte nach Abs. 1 können sich vor allem aufgrund von Meldungen oder durch Nachweise von Dritten als auch aufgrund von durchgeführten Kontrollen nach Art. 18 ergeben.

Die Frist nach Abs. 1 Bst. b kann gemäss **Abs. 2** von der Stabsstelle Cyber-Sicherheit in begründeten Fällen auf Antrag des Betreibers wesentlicher Dienste und Anbieter digitaler Dienste angemessen verlängert werden. Dies vor allem, wenn der Betreiber wesentlicher Dienste oder Anbieter digitaler Dienste dadurch voraussichtlich den rechtmässigen Zustand herstellt. Abs. 2 entspricht inhaltlich Art. 18 Abs. 2 der Vernehmlassungsvorlage.

Handelt es sich bei dem Betreiber wesentlicher Dienste oder dem Anbieter digitaler Dienste um eine öffentliche Stelle oder um eine nicht öffentliche Stelle, soweit sie in Erfüllung einer übertragenen öffentlichen Aufgaben tätig ist, so informiert die Stabsstelle Cyber-Sicherheit gemäss **Abs. 3** zusätzlich die Regierung über eine Mitteilung beziehungsweise Aufforderung nach Abs. 1.

Unter öffentlichen Stellen werden Organe des Staates, der Gemeinden und von Körperschaften, Stiftungen und Anstalten sowie andere juristische Personen des öffentlichen Rechts verstanden sowie auch jene natürlichen und juristischen Personen sowie rechtsfähige Personengesellschaften, die dem Privatrecht unterstehen, soweit ihnen öffentliche Aufgaben übertragen wurden.

Abs. 4 soll insbesondere die Zusammenarbeit der unterschiedlichen nationalen Aufsichtsbehörden mit der Stabsstelle Cyber-Sicherheit regeln. Eine solche Zusammenarbeit kann sich insbesondere dann ergeben, wenn die Anhaltspunkte für Verstösse gegen dieses Gesetz ebenso einen möglichen Verstoß gegen andere Bestimmungen, welche im Wirkungsbereich einer anderen Aufsichtsbehörde

liegen, darstellen. So wäre es beispielsweise denkbar, dass ein Verstoß gegen Sicherheitsanforderungen oder Meldepflichten eines Unternehmens in einem der in Art. 1 Abs. 1 Bst. a genannten Sektoren eine Aufsichtstätigkeit einer Aufsichtsbehörde nach sich zieht. Durch Abs. 4 wird sichergestellt, dass von der Stabsstelle Cyber-Sicherheit bei Anhaltspunkten für mögliche Verstöße gegen die Vorschriften dieses Gesetzes die jeweils zuständige Aufsichtsbehörde informiert wird und diese unter Setzung einer angemessenen Frist Gelegenheit zur Stellungnahme erhält.

Sollte durch den Betreiber wesentlicher Dienste oder dem Anbieter digitaler Dienste der Aufforderung nach Abs. 1 nicht fristgerecht nachgekommen werden, erlässt die Stabsstelle Cyber-Sicherheit gemäss **Abs. 5** eine Entscheidung mittels rechtmittelfähiger Verfügung.

Abweichend der Vernehmlassungsvorlage wurde in Abs. 5 ergänzt, dass in dringenden oder begründeten Fällen auch ohne Aufforderung nach Abs. 1 eine Verfügung erfolgen kann. Ebenso ergänzt wurde, dass die Stabsstelle Cyber-Sicherheit eine allfällige zuständige Aufsichtsbehörde des Betreibers wesentlicher Dienste oder des Anbieters digitaler Dienste über ihre Entscheidung informiert.

Ungeachtet der Reaktion auf die Aufforderung gemäss Abs. 1 steht es der Stabsstelle Cyber-Sicherheit gemäss **Abs. 6** offen, eine Busse nach Art. 22 gegenüber dem Betreiber wesentlicher Dienste und dem Anbieter digitaler Dienste zu verhängen.

Zu Art. 17 – Betrieb von IKT-Lösungen

Der gegenständliche Artikel entspricht Art. 17 der Vernehmlassungsvorlage, die ursprünglichen zwei Absätze wurden jedoch redaktionell und legislatisch überarbeitet.

Bst. a stellt sicher, dass die Stabsstelle Cyber-Sicherheit die zur Erfüllung ihrer Aufgaben notwendigen Informations- und Kommunikationstechnik-Lösungen («IKT-Lösungen») betreiben oder durch Dritte betreiben lassen kann, welche Risiken oder Sicherheitsvorfälle von Netz- und Informationssystemen frühzeitig erkennen. In der Praxis sind dies beispielsweise sogenannte «Honeypots», mit denen Angreifer gezielt angelockt werden, indem Server, Datenbanken oder andere potenzielle Angriffsziele mit definierten Schwachstellen vorgetäuscht werden. Honeypots sind in der Regel so konfiguriert, dass ein erfolgreicher Angriff zwar möglich ist, jedoch im Idealfall der Angreifer nicht bemerkt, dass er sich in einer «Falle» befindet. Auf diese Weise können Cyberangriffe und die Vorgehensweise der Angreifer nachvollzogen und in einem gesicherten Umfeld analysiert werden.

Der **Bst. b** gibt der Stabsstelle Cyber-Sicherheit jedoch die Möglichkeit, neben dem Betrieb eigener IKT-Lösungen, mit Einwilligung der betroffenen Einrichtung eine dort bereits vorhandene IKT-Lösung zu nutzen, um die Muster von Angriffen auf Netz- und Informationssysteme zu erkennen. Darunter sind vor allem Sensoren zu verstehen, die gezielt an einem Netz- und Informationssystem angebracht werden. Im Gegensatz dazu werden unter Bst. a IKT-Lösungen verstanden, die allgemein mit dem Internet verbunden sind und kein konkretes Netz- und Informationssystem betreffen.

Der **Liechtensteinische Bankenverband** ersucht in seiner Stellungnahme um Klarstellung, inwieweit IKT-Lösungen durch die Stabsstelle Cyber-Sicherheit bei den Banken bzw. Betreibern wesentlicher Dienste platziert bzw. betrieben werden dürfen. Die gewählte Formulierung sei unklar und liesse offen, ob die Stabsstelle die IKT-Lösungen selbst einsetzt oder den Betreibern wesentlicher Dienste auferlegen kann, von der Stabsstelle vorgegebene IKT-Lösungen in ihren Netz- und

Informationssystemen zu implementieren bzw. der Stabsstelle Zugang zu eigenen IKT-Lösungen zu gewähren.

Die Regierung stellt hier klar, dass die Stabsstelle Cyber-Sicherheit gemäss Art. 17 von keiner Stelle verlangen kann, bestimmte IKT-Lösungen der Stabsstelle in deren Netz- und Informationssystemen zu betreiben. Die Stabsstelle Cyber-Sicherheit erhält gestützt auf Art. 17 auch keinen Zugang zu IKT-Lösungen, die nicht von ihr selbst betrieben werden.

Zu Art. 18 – Kontrolle

In der Vernehmlassungsvorlage waren Kontrollen in Art. 13 geregelt.

Abs. 1 legt fest, dass die Stabsstelle Cyber-Sicherheit Kontrollen zur Einhaltung der Anforderungen nach diesem Gesetz selbst durchführen oder durch von ihr beauftragte qualifizierte Dritte durchführen lassen kann.

Die gegenständlichen Kontrollen dienen insbesondere dazu, bei Bedarf oder auch aus einem bestimmten Anlass, wie etwa ein Sicherheitsvorfall, festzustellen, ob durch Betreiber wesentlicher Dienste als auch durch Anbieter digitaler Dienste die Anforderungen an die Sicherheitsmassnahmen sowie Meldepflichten nach diesem Gesetz eingehalten werden bzw. wurden.

Die Kontrolle kann auch durch einen von der Stabsstelle Cyber-Sicherheit beauftragten qualifizierte Dritten durchgeführt werden. Bei den qualifizierten Dritten handelt es sich um eine gemäss Art. 15 Abs. 2 Bst. b der Richtlinie (EU) 2016/1148 qualifizierte Stelle. Diese Möglichkeit der Beauftragung ist dahingehend sinnvoll, als im Bereich der Auditierung bereits entsprechendes Potential am Markt verfügbar ist und der innerbehördliche Aufbau entsprechender Ressourcen bei der Stabsstelle Cyber-Sicherheit für sämtliche Betreiber wesentlicher Dienste und Anbieter digitaler Dienste zeit- und vor allem kostenintensiv wäre.

Die Kriterien, die ein qualifizierter Dritter zu erfüllen hat, richten sich nach den Erfordernissen im Einzelfall. Es ist durchaus zulässig, auch nur für einzelne Sicherheitsmassnahmen (eingeschränkter Aufgabenbereich) als qualifiziert zu gelten. Ein qualifizierter Dritter hat gegenüber der Stabsstelle Cyber-Sicherheit vor der Ausübung einer Kontrolle nach Art. 18 für den jeweiligen Einzelfall entsprechende Befähigungen nachzuweisen. Dies können etwa die Darstellung der verwendeten Methodik und Kontrollprozesse als auch die verwendeten Werkzeuge sein. Ein wesentliches Merkmal für einen qualifizierten Dritten ist die Verfügbarkeit von qualifiziertem Personal, das für die jeweilige Kontrolle eingesetzt wird. Die Voraussetzungen für eine Qualifikation sind z. B. nur dann erfüllt, wenn die Personen für den kontrollierten Bereich einschlägige Ausbildungen und mehrjährige Berufserfahrung in diesem Bereich nachweisen können. Darüber hinaus müssen sämtliche Mitarbeiter des qualifizierten Dritten, die Kontrollen bei Betreibern wesentlicher Dienste durchführen, eine Sicherheitsüberprüfung angelehnt an die Informationsschutzverordnung (LGBI. 2009 Nr. 315) vorweisen.

Gemäss Art. 9 Abs. 3 kann die Regierung das Nähere über die Anforderungen an qualifizierte Dritte mit Verordnung regeln.

Der **Liechtensteinische Bankenverband** fragt in seiner Stellungnahme zur Vernehmlassung, wer bei Kontrollen die Kosten der qualifizierten Dritten trägt und bittet um entsprechende Ergänzung.

Betreffend die Kosten für die qualifizierten Dritten hält die Regierung fest, dass diese durch die Stabsstelle Cyber-Sicherheit zu tragen sind, wenn der qualifizierte Dritte durch die Stabsstelle Cyber-Sicherheit für eine bestimmte Kontrolle beigezogen wird.

Die **Liechtensteinischen Kraftwerke** führen in ihrer Stellungnahme zur Vernehmlassung aus, dass die abgegebenen Informationen von der Stabsstelle höchst vertraulich behandelt sowie gegen Angriffe gesichert übermittelt und aufbewahrt werden sollten. Dies gilt auch für qualifizierte Dritte, die im Auftrag der Stabsstelle Cyber-Sicherheit Kontrollen durchführen. Wenn die Informationen aller Kontrollen kritischer Infrastrukturen zentral an einem Ort aufbewahrt werden, gibt es laut den Liechtensteinischen Kraftwerken kaum ein Angriffsziel welches interessanter sein könne. Die betroffenen Betreiber wesentlicher Dienste, als auch die Anbieter digitaler Dienste, sollten die Möglichkeit erhalten, sich über die getroffenen Sicherheitsvorkehrungen, Vertraulichkeitserklärungen etc. zu informieren.

Der **Liechtensteinische Bankenverband** regt in seiner Stellungnahme in der Vernehmlassung an, in Abs. 1 vorzusehen, dass nach Abschluss der Kontrollen sämtliche Unterlagen mit Ausnahme der Abschlussberichte wieder zu vernichten sind.

Die Regierung führt dazu aus, dass die Stabsstelle Cyber-Sicherheit in Bezug auf die Kontrollen ein Reglement ausarbeiten wird, welches unter anderem die Datenverarbeitung unter Einhaltung von Sicherheitsstandards, die dem Stand der Technik entsprechen, regeln wird. Dadurch entsteht Transparenz über den Ablauf und die Modalitäten, welche auch regelmässig überprüft und bei Bedarf angepasst werden können. Überdies wird dadurch eine einheitliche Handhabung seitens der Stabsstelle Cyber-Sicherheit gewährleistet.

Gerade bei Kontrollen in sensiblen Bereichen ist es üblich, dass wo vermeidbar und geboten, keine vertraulichen Informationen durch die kontrollierende Stelle herausverlangt oder gar zentral gespeichert werden.

So können beispielsweise Dokumente zum Nachweis der Einhaltung von Sicherheitsanforderungen ebenso vor Ort eingesehen sowie in einer sicheren und vom Betreiber zur Verfügung gestellten Räumlichkeit geprüft werden. Somit erfolgt keine Speicherung bei der Stabsstelle Cyber-Sicherheit.

Wo eine Speicherung und Verarbeitung direkt durch die Stabsstelle Cyber-Sicherheit erfolgt, sind die Grundlagen der Prüfung zum Zwecke der Nachvollziehbarkeit aufzubewahren. Dies ist vergleichbar mit einer entsprechenden Bestimmung im Bereich der Wirtschaftsprüfungen, wo die begleitenden Dokumente einer Prüfung (Prüfungsdokumentation) gemäss Art. 43 Wirtschaftsprüfungsgesetz für 10 Jahre aufbewahrt werden. Als Bedingung könnte hier vorgesehen werden, dass die Aufbewahrung in Liechtenstein zu erfolgen hat.

Jedenfalls wird die Stabsstelle Cyber-Sicherheit bei der Datenverarbeitung die geltenden Grundsätze der Informationssicherheit einhalten.

Zudem bitten die **Liechtensteinischen Kraftwerke** zu prüfen, inwieweit die Stabsstelle Cyber-Sicherheit bzw. das Land Liechtenstein und/oder von ihr beauftragte Dritte betreffend Schadenersatz belangt bzw. haftbar gemacht werden können, sollte durch unzureichende Schutzmassnahmen etc. einem auditierten Unternehmen nachweislich Schaden entstehen.

Die Regierung verweist an dieser Stelle auf das Gesetz über die Amtshaftung, da die Stabsstelle Cyber-Sicherheit als Behörde handelt. Dies gilt ebenso für qualifizierte Dritte, falls diese durch die Stabsstelle Cyber-Sicherheit beauftragt sind.

Der **Liechtensteinische Bankenverband** erklärt in seiner Stellungnahme, dass die Überwachungs- und Überprüfungscompetenz der Stabsstelle Cyber-Sicherheit nur dort Sinn mache, wo nicht bereits aufgrund der spezialgesetzlichen Zuständigkeit der Aufsichtsbehörden oder anderer zuständiger Behörden entsprechende

Kontrollen durchgeführt werden. Der Liechtensteinische Bankenverband bittet in seiner Stellungnahme um Ergänzung des Art. 18 wie folgt: «Werden durch sektorspezifische Rechtsakte anderen Behörden bzw. Stellen Befugnisse für die Überwachung und Kontrolle der Sicherheit von Netz- und Informationssystemen eingeräumt, die zur Erbringung bzw. Bereitstellung wesentlicher Dienste nach diesem Gesetz oder durch Anbieter digitaler Dienste genutzt werden, so gelten auch für die Überwachung und Kontrolle die einschlägigen Bestimmungen jenes sektorspezifischen Rechtsakts. Die zuständige Behörde/Stelle hat die Stabsstelle Cyber-Sicherheit über die durchgeführten Kontrollen zu unterrichten.»

Die Regierung führt dazu aus, dass das Cyber-Sicherheitsgesetz gegenüber den Lex specialis Regelungen zurücktritt. Die Finanzmarktaufsicht Liechtenstein ist die zuständige Aufsichtsbehörde für die Sektoren Bankwesen und Finanzmarktinfrastrukturen und nimmt daher in diesen Sektoren die entsprechenden Befugnisse wahr. Daher hat die Stabsstelle Cyber-Sicherheit nach Ansicht der Regierung keine Kontrollbefugnisse, sofern es sich um Bestimmungen handelt, welche vom Lex specialis abgedeckt sind. An dieser Stelle wird auf die diesbezüglichen Ausführungen in Abschnitt 4.2.2 verwiesen.

Nach **Abs. 2** können die Stabsstelle Cyber-Sicherheit oder eben von ihr beauftragte qualifizierte Dritte zum Zweck der Kontrolle Einsicht in die Netz- und Informationssysteme, die für die Bereitstellung wesentlicher Dienste und Anbieter digitaler Dienste genutzt werden, und diesbezügliche Unterlagen nehmen.

Zum Zweck der Einsicht sind die Stabsstelle Cyber-Sicherheit oder von ihr beauftragte Dritte weiters berechtigt, Örtlichkeiten, in welchen Netz- und Informationssysteme gelegen sind, zu betreten. Die Ausübung der Einsicht hat verhältnismässig zu erfolgen und ist unter möglichster Schonung der Rechte der betroffenen Einrichtung und Dritter sowie des Betriebs auszuüben.

Eine durchgeführte Kontrolle nach Art. 18 stellt in allen Fällen eine Momentaufnahme des geprüften Sicherheitsniveaus eines auf den Prüfungsgegenstand eingeschränkten Bereich der Sicherheit der Netz- und Informationssysteme dar. Allein der Umstand, dass eine Kontrolle durchgeführt wurde oder dass allenfalls keine wesentlichen Mängel beim Betreiber wesentlicher Dienste oder Anbieter digitaler Dienste festgestellt wurden, lässt keine verbindliche Aussage betreffend möglicher zukünftiger Sicherheitsvorfälle zu.

Die Betreiber wesentlicher Dienste und Anbieter digitaler Dienste haben ihre Sicherheitsmassnahmen regelmässig selbst zu überprüfen und sie handeln stets in Eigenverantwortung.

Gegenständlich wird mit **Abs. 3** der Regierung – abweichend zum Art. 13 der Vernehmlassungsvorlage – die Möglichkeit gegeben, das Nähere über die Durchführung von Kontrollen mit Verordnung zu regeln.

C. Computer-Notfallteam (CSIRT)

Zu Art. 19 – Zweck und Aufgaben

Mit Art. 19 wird Art. 9 der Richtlinie (EU) 2016/1148 umgesetzt und entspricht inhaltlich Art. 15 der Vernehmlassungsvorlage.

Das Computer-Notfallteam (CSIRT) zur Gewährleistung der Sicherheit von Netz- und Informationssystemen wird gemäss **Abs. 1** bei der Stabsstelle Cyber-Sicherheit eingerichtet. Dem CSIRT kommen insbesondere die in Bst. a bis e aufgeführten Aufgaben zu, welche in der Vernehmlassungsvorlage in Abs. 2 aufgelistet waren.

Dies sind insbesondere die Entgegennahme von Meldungen über Risiken oder Sicherheitsvorfälle gemäss Art. 5, 7 und 8 sowie – falls verfügbar oder erhebbar –

die zur Verfügungstellung von zur Bewältigung eines Sicherheitsvorfalls nützlichen Informationen (**Bst. a**).

Weitere Aufgaben sind die Ausgabe von Frühwarnungen und Alarmmeldungen sowie Bekanntmachung und Verbreitung von Informationen über Risiken und Sicherheitsvorfälle unter den einschlägigen Interessenträgern (**Bst. b**) sowie eine erste allgemeine Unterstützung bei der Reaktion auf einen Sicherheitsvorfall (**Bst. c**). Zur allgemeinen Unterstützung wird ergänzt, dass das CSIRT bei der Stabsstelle Cyber-Sicherheit keine dahingehende Unterstützung anbieten wird können, als dass Mitarbeitende der Stabsstelle nach einem Sicherheitsvorfall vor Ort beim betroffenen Unternehmen eine aktive Rolle zur Schadenseindämmung oder Schadensminderung vornehmen. Die Unterstützung kann sich lediglich auf eine beratende Funktion beschränken, wobei das CSIRT sein entsprechendes Netzwerk, wie z. B. das CSIRT-Netzwerk gemäss Art. 12 der Richtlinie (EU) 2016/1148 nutzen wird, um die von einem Sicherheitsvorfall betroffenen Stellen bestmöglich allgemein zu unterstützen.

Der **Liechtensteinische Bankenverband** hält in seiner Stellungnahme zur Vernehmlassung fest, dass eine reine Berichterstattung an die Stabsstelle Cyber-Sicherheit den Banken bei der Bewältigung einer Cyberkrise nicht weiterhelfe. Vielmehr würden die wenigen verfügbaren Ressourcen der Spezialisten gebunden. Auch sei unklar, welche Stelle den Banken anlässlich eines Sicherheitsvorfalls Unterstützung leistet.

Die Regierung führt dazu aus, dass es gemäss Art. 13 Abs. 1 Bst. b eine nicht unwesentliche Aufgabe der Stabsstelle Cyber-Sicherheit ist, das Computer-Notfallteam (CSIRT) gemäss Art. 19 einzurichten und zu koordinieren. Das CSIRT seinerseits kann sich gemäss Art. 9 Abs. 2 für bestimmte Aufgaben sowie auch insbesondere im Anlassfall qualifizierter Dritter bedienen.

Dadurch wird sichergestellt, dass auch entsprechende Unterstützung bei Bedarf bereitsteht. Die Art der Unterstützung, die das CSIRT leisten kann, hängt vom konkreten Einzelfall ab.

Ungeachtet dessen haben Betreiber wesentlicher Dienste und auch Anbieter digitaler Dienste gemäss Art. 4 Abs. 3 bzw. Art. 6 Abs. 2 Bst. b eigenverantwortlich sicherzustellen, dass geeignete Massnahmen zur Minimierung der Auswirkungen nach Sicherheitsvorfällen implementiert sind. Dazu gehören beispielsweise auch die Erstellung und Anwendung von Notfallplänen, die Aufrechterhaltung und Erprobung von Erkennungsprozessen und -verfahren zur Gewährleistung einer rechtzeitigen und angemessenen Lageerfassung bei ungewöhnlichen Ereignissen sowie die Reaktion gemäss den festgelegten Verfahren.

Der **Liechtensteinische Bankenverband** regt in seiner Stellungnahme an, dass die bestehenden Kanäle – wie zum Beispiel zum Schweizer Nationalen Zentrum für Cybersicherheit (NCSC) – unter keinen Umständen unterbrochen oder vervielfältigt werden sollten oder parallele Strukturen aufgebaut werden, die redundant und mit anderer Periodizität der Berichterstattung bedient werden müssen. Dies sei soweit erforderlich auf zwischenstaatlicher Ebene sicherzustellen.

Die Regierung führt dazu aus, dass der Kontakt der Stabsstelle Cyber-Sicherheit zum Nationalen Zentrum für Cybersicherheit in der Schweiz (NCSC) bereits besteht. Die Stabsstelle Cyber-Sicherheit ist hier ebenso im regelmässigen Austausch mit anderen entsprechenden Stellen in der Schweiz.

Doch um aktuelle massgeschneiderte Informationen betreffend die Cybersicherheit in Liechtenstein auch Unternehmen und Banken, die bisher keinen Zugang zu solchen Informationen hatten oder diese nicht in Anspruch genommen

haben, niederschwellig zugänglich zu machen, wird sich die Stabsstelle Cyber-Sicherheit als Verbindungstelle und zentrale Drehscheibe positionieren.

Ebenso ist die Beobachtung und Analyse von Risiken und Sicherheitsvorfällen sowie eine entsprechende Lagebeurteilung (**Bst. d**) als auch die Teilnahme am CSIRTs-Netzwerk gemäss Art. 12 der Richtlinie (EU) 2016/1148 (**Bst. e**) Aufgabe des CSIRT bei der Stabsstelle Cyber-Sicherheit.

Die **NetSec.co AG** äussert in ihrer Stellungnahme zur Vernehmlassungsvorlage die Auffassung, Liechtenstein sei zu klein, um ein eigenes CSIRT zu betreiben. Daher solle seitens der Regierung geprüft werden, ob die Muss-Vorgabe in eine Kann-Vorgabe umformuliert und die Option, sich an ein bestehendes CSIRT eines anderen (idealerweise deutschsprachigen) Staates anzuschliessen, geschaffen werden sollte. Auch der **Liechtensteinische Bankenverband** weist darauf hin, dass Personalressourcen nötig sein werden, um ein funktionierendes nationales CSIRT zu etablieren. Der Mehrwert eines CSIRT Liechtenstein sei dabei schwierig abzuschätzen und es stelle sich die Frage, inwieweit eine Auslagerung mit den für den Finanzbereich geltenden hohen regulatorischen Anforderungen zu Bankgeheimnis und Datenschutz vereinbar ist sowie ob ein Anschluss an bestehende Netzwerke (Schweiz, EU) nicht zielführender und realistischer sei.

Die Regierung führt einleitend dazu aus, dass das CSIRT Liechtenstein eine direkte Vorgabe aus der Richtlinie (EU) 2016/1148 ist und es in diesem Punkt keinen Spielraum bei der Umsetzung gibt.

Den Mehrwert sieht die Regierung insbesondere darin, dass für Unternehmen in Liechtenstein die Erkenntnisse und Dienstleistungen aus einem eigenen CSIRT niederschwelliger zugänglich sind. Die Formulierung der Aufgabe der Stabsstelle Cyber-Sicherheit in Art. 13 Abs. 1 Bst. b wurde aufgrund von Rückmeldungen zur Vernehmlassung auch dahingehend geändert, dass das CSIRT nicht wie

ursprünglich bei der Stabsstelle betrieben wird, sondern dass sich die Stabsstelle Cyber-Sicherheit für die Einrichtung und Koordination des CSIRT verantwortlich zeichnet.

Dadurch ergibt sich in diesem Punkt mehr Spielraum bei der Ausgestaltung des CSIRT. Die konkrete Ausgestaltung ist aktuell noch nicht entschieden. Verschiedene Varianten sollen evaluiert und die Vereinbarkeit mit dem geltenden als auch dem zukünftigen Rechtsrahmen (beispielsweise die Richtlinie (EU) 2022/2555) geprüft werden.

Wie bereits oben erwähnt, kann das CSIRT sich gemäss Art. 9 Abs. 2 für bestimmte Aufgaben, was auch die Erreichbarkeit zur Meldung von Vorfällen betrifft, sowie auch insbesondere im Anlassfall qualifizierten Dritten bedienen. Schon die von einem CSIRT geforderte ständige Bereitschaft gemäss Punkt 1 Bst. c Ziff. ii des Anhangs I zur Richtlinie (EU) 2016/1148 wird eine Kooperation mit einem externen Partner notwendig machen.

*Bezugnehmend auf die Frage des **Liechtensteinische Bankenverband** betreffend die Vereinbarkeit der Auslagerung des CSIRT mit den regulatorischen Anforderungen zu Bankgeheimnis und Datenschutz führt die Regierung aus, dass es einen Anschluss an bestehende CSIRTs geben wird und die geltenden regulatorischen Anforderungen eingehalten werden. So ist beispielsweise das CSIRT-Netzwerk nach Art. 3 Abs. 1 Bst. n bzw. Art. 12 der Richtlinie (EU) 2016/1148 ein Gremium, das sich aus Vertretern der Computer-Notfallteams der EWR-Mitgliedstaaten zusammensetzt und zum Aufbau von Vertrauen zwischen den EWR-Mitgliedstaaten beitragen und eine rasche und wirksame operative Zusammenarbeit fördern soll. Darüber hinaus wird sich die Stabsstelle Cyber-Sicherheit bzw. das eingerichtete CSIRT Liechtenstein mit den CSIRTs im EWR und der Schweiz entsprechend vernetzen.*

Die Regierung weist ausserdem darauf hin, dass sich Betreiber wesentlicher Dienste auch weiterhin mit anderen CSIRTs vernetzen können, Art. 15 nimmt in dieser Hinsicht keine Einschränkung vor.

Mit **Abs. 2** wird der Stabsstelle Cyber-Sicherheit die Möglichkeit eröffnet, ebenso sonstigen Einrichtungen oder Personen entsprechende Dienstleistungen des CSIRT zukommen zu lassen, sofern diese Einrichtungen oder Personen von einem Risiko oder einem Sicherheitsvorfall ihrer Netz- und Informationssysteme betroffen sind.

Das Nähere über den Zweck und die Aufgaben des CSIRT kann die Regierung mittels Verordnung regeln (**Abs. 3**).

D. NIS-Strategie

Zu Art. 20 – Grundsatz

Mit Art. 20 wird Art. 7 der Richtlinie (EU) 2016/1148 umgesetzt und entspricht Art. 14 der Vernehmlassungsvorlage. Die Bestimmung sieht vor, dass zwecks Erreichung und Aufrechterhaltung eines hohen Sicherheitsniveaus von Netz- und Informationssystemen, jeder EWR-Mitgliedstaat über eine nationale Strategie zur Sicherheit von Netz- und Informationssystemen (NIS-Strategie) zu verfügen hat, in der die strategischen Ziele sowie konkrete politische Massnahmen vorgesehen sind.

Die **Liechtensteinischen Kraftwerke** weisen in ihrer Stellungnahme darauf hin, dass der Begriff «NIS (Netz- und Informationssystem)»-Strategie bzw. Richtlinie für die Liechtensteinischen Kraftwerke irreführend sei, da der Begriff schon im Zusammenhang mit der Thematik «Nichtionisierende Strahlung» belegt sei.

Dazu führt die Regierung aus, dass die Abkürzung NIS für Netz- und Informationssysteme sowie die NIS-Richtlinie offiziell in diesem Zusammenhang

verwendet wird. Die Nachfolgerichtlinie der Richtlinie (EU) 2016/1148, die Richtlinie (EU) 2022/2555 enthält im Titel gar die Bezeichnung «NIS-2-Richtlinie». Daher wird von dieser Abkürzung nicht abgewichen. Eine Verwechslungsgefahr erkennt die Regierung hier nicht, da aus dem jeweiligen Kontext erkennbar sein sollte, ob es sich um Strahlung oder um Informationssysteme handelt.

Die nationale NIS-Strategie behandelt insbesondere die folgenden Aspekte: a) die Ziele und Prioritäten; b) einen Steuerungsrahmen zur Erreichung der Ziele und Prioritäten, 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 NIS-Strategie; e) eine Angabe der Forschungs- und Entwicklungspläne im Zusammenhang mit der nationalen NIS-Strategie; f) einen Risikobewertungsplan zur Bestimmung von Risiken; g) eine Liste der verschiedenen Akteure, die an der Umsetzung der nationalen NIS-Strategie beteiligt sind.

Die Stabsstelle Cyber-Sicherheit zeichnet sich gemäss Art. 13 Abs. 1 Bst. m für die Koordination der Erstellung dieser nationalen Strategie verantwortlich, wobei die Regierung gemäss **Abs. 3** die NIS-Strategie abschliessend genehmigt.

Abs. 3 wurde nach dem Vernehmlassungsverfahren eingefügt. Die geltende nationale Strategie für Liechtenstein zum Schutz vor Cyber-Risiken wurde im Oktober 2020 von der Regierung beschlossen. Die Zuständigkeit und Rolle der Regierung ergaben sich aus Art. 20 nicht explizit. Mit Abs. 3 wird dies nun klar geregelt.

IV. Rechtsmittel

Das Kapitel IV. regelt das Rechtsmittel der Beschwerde.

Zu Art. 21

Art. 21 entspricht inhaltlich, jedoch redaktionell und legislatisch entsprechend angepasst, Art. 19 der Vernehmlassungsvorlage.

Abs. 1 sieht die Beschwerdekommision für Verwaltungsangelegenheiten als Rechtsmittelinstanz bei Beschwerden gegen Entscheidungen der Stabsstelle Cyber-Sicherheit vor.

Gegen Entscheidungen und Verfügungen der Beschwerdekommision für Verwaltungsangelegenheiten kann wiederum Beschwerde an den Verwaltungsgerichtshof (VGH) erhoben werden (**Abs. 2**).

In der Vernehmlassungsvorlage war in Abs. 3 geregelt, dass das Beschwerderecht sowohl dem Betroffenen als auch der Stabsstelle Cyber-Sicherheit zusteht. Aufgrund der Stellungnahmen zur Vernehmlassungsvorlage von der **Beschwerdekommision für Verwaltungsangelegenheiten** sowie der **Rechtsanwaltskammer** wurde das Beschwerderecht der Stabsstelle Cyber-Sicherheit aus der gegenständlichen Gesetzesvorlage ersatzlos gestrichen.

Im liechtensteinischen Verwaltungsrecht sei es laut Beschwerdekommision für Verwaltungsangelegenheiten und Rechtsanwaltskammer nur in vereinzelt Fällen vorgesehen, dass die Behörde, welche eine Verfügung erlässt, gegen eine Entscheidung der oberen Instanz ein Beschwerderecht erhält. Die Behörden würden im Beschwerdeverfahren zur Stellungnahme eingeladen und haben somit ausreichend Gelegenheit, ihre Position zu vertreten. Sollte eine Entscheidung der Beschwerdeinstanz nach Ansicht der belangten Behörde angefochten werden, da die Notwendigkeit eines Weiterzuges durch die Behörde gesehen wird, so gebe es laut VBK die Möglichkeit der Amtsbeschwerde gemäss Art. 92 LVG.

Abs. 3 – in der Vernehmlassungsvorlage noch Abs. 4 – beschränkt die Kognitionsbefugnis der Rechtsmittelinstanzen in Übereinstimmung mit der einschlägigen Rechtsprechung des VGH. Die Beschwerdekommision für Verwaltungsangelegenheiten sowie der Verwaltungsgerichtshof dürfen in der Beschwerde nur jene Punkte aufgreifen, die in der Beschwerde vorgebracht wurden; der Prüfungsumfang beschränkt sich auf den Inhalt der Beschwerde. Eine Entscheidung über eine Frage, die vom Beschwerdeführer nicht angesprochen wird, überschreitet – so auch die einschlägige Rechtsprechung in Liechtenstein – die Entscheidungskompetenz.

Abs. 4 – in der Vernehmlassungsvorlage noch Abs. 5 – beinhaltet eine Klarstellung betreffend die Anwendbarkeit des LVG.

V. Strafbestimmungen

Mit Kapitel V. werden bestimmte Zuwiderhandlungen unter Strafe gestellt sowie die Verantwortlichkeit geregelt.

Zu Art. 22

Mit dem gegenständlichen Artikel wird Art. 21 der Richtlinie (EU) 2016/1148 umgesetzt. In Vernehmlassungsvorlage fanden sich die Regelungen in Art. 21.

Abs. 1 enthält Vorschriften über Sanktionen für Verstösse gegen die nach diesem Gesetz erlassenen Bestimmungen. Die Sanktionen haben gemäss der Richtlinie (EU) 2016/1148 wirksam, angemessen und abschreckend zu sein.

So wird von der Stabsstelle Cyber-Sicherheit wegen Übertretung mit Busse bis zu 100'000 Franken bestraft, wenn die Tat nicht den Tatbestand einer in die Zuständigkeit der Gerichte fallenden strafbaren Handlung bildet sowie das Tatbild einem nach Bst. a bis k entspricht. Die Strafbestimmungen wurden, ohne den Inhalt zu verändern, nach der Vernehmlassung sowohl redaktionell wie legislatisch überarbeitet.

Der **Liechtensteinische Anlagefondsverband** sowie der **Liechtensteinische Bankenverband** ersuchen in ihren Stellungnahmen um Klarstellung bzw. Sicherstellung, dass die vorgesehenen Sanktionsmöglichkeiten zu keiner Doppelbestrafung führen, wenn beispielsweise wegen desselben Tatbestands auch aus aufsichtsrechtlicher Sicht eine Sanktionierung erfolgt. Der Liechtensteinischer Anlagefondsverband sieht mit der Schaffung des Cyber-Sicherheitsgesetzes eine Doppelspurigkeit zwischen den aufsichtsrechtlichen Anforderungen an Finanzdienstleister einerseits und den Anforderungen aufgrund des Cyber-Sicherheitsgesetzes andererseits, die potenziell zu Unsicherheiten und Unklarheiten führen könne.

Wie in Abschnitt 4.2.2 ausführlich erläutert, bestehen in den Sektoren Bankwesen und Finanzmarktinfrastrukturen mit dem Zahlungsdienstegesetz einschlägige Bestimmungen betreffend die Sicherheitsanforderungen und die Meldepflichten. Somit kommen die materiellen Bestimmungen, welche eine Strafbarkeit nach Art. 22 begründen gar nicht erst zur Anwendung. Falls eine bisher nicht berücksichtigte rechtliche Situation eintreten sollte, bei welcher die Gefahr einer Doppelbestrafung bestehen könnte, wird mit Art. 16 Abs. 4 sichergestellt, dass eine allfällige zuständige Aufsichtsbehörde Gelegenheit zur Stellungnahme bekommt und der Sachverhalt entsprechend geklärt wird. Somit besteht aus Sicht der Regierung keine Gefahr der Doppelbestrafung.

Die **Wasserversorgung Liechtensteiner Unterland e. G.** führt in ihrer Stellungnahme zur Vernehmlassungsvorlage aus, dass der Katalog der Verwaltungsübertretungen (der Bussenkatalog sei etwa zu umfassend) sowie die Höhe der möglichen Bussen überdacht werden solle, da beide nicht als angemessen erscheinen. Bereits heute komme der Cybersicherheit eine zentrale Funktion zu und sei im ureigenen Interesse der Wasserversorgung Liechtensteiner

Unterland e. G. Daher solle vielmehr die Prävention in den Vordergrund gestellt werden.

Betreffend die Höhe der Busse wird ausgeführt, dass diese gemäss Art. 21 der Richtlinie (EU) 2016/1148 wirksam, angemessen und abschreckend sein soll. Die Höhe von 100'000 Franken erachtet die Regierung als diesen Anforderungen gerecht.

Falls Verstösse gegen Vorschriften dieses Gesetzes festgestellt werden, wird die Stabsstelle Cyber-Sicherheit gemäss Art. 16 Abs. 1 dies der betreffenden Stelle in einem ersten Schritt formlos mitteilen, und dem Betreiber wesentlicher Dienste oder dem Anbieter digitaler Dienste eine angemessene Frist setzen, um Stellung zu nehmen oder bestenfalls zeitnah den rechtmässigen Zustand herzustellen. Nur in dringenden Fällen wird die Stabsstelle Cyber-Sicherheit gemäss Art. 16 Abs. 5 ohne Aufforderung eine Verfügung übermitteln und allenfalls eine Busse nach Art. 22 iVm Art. 16 Abs. 6 aussprechen.

Die **Liechtensteinischen Kraftwerke** merken in ihrer Stellungnahme an, dass die Höhe der Bussen trotz der gewählten Formulierung «bis zu» für KMU's zu einer sehr grossen Belastung werden könne und regt daher an, eine Abstufung in Relation zur Unternehmensgrösse vorzunehmen.

Betreffend die Höhe der Busse führt die Regierung aus, dass es bei den 100'000 Franken um den Maximalbetrag handelt. Dieser gibt den maximal möglichen Rahmen der Stabsstelle Cyber-Sicherheit bei der Verhängung von Bussen vor. Die Stabsstelle wird bei der Bemessung dem Umstand der Unternehmensgrösse Rechnung tragen, da die Busse wirksam und vor allem den Umständen entsprechend angemessen sein muss. Von einer Abstufung aufgrund der Unternehmensgrösse wird daher abgesehen.

*Ebenso ist es unüblich, die genauen Kriterien für die Bemessung der Bussen in Form eines Kriterienkatalogs in einem Gesetz aufzunehmen, wie es von der **Wasserversorgung Liechtensteiner Unterland e. G.** in ihrer Stellungnahme angeregt wurde.*

Abs. 2 legt fest, dass die Strafobergrenze nach Abs. 1 bei fahrlässiger Begehung auf die Hälfte herabgesetzt wird sowie im Wiederholungsfall eine Verdoppelung erfährt.

Art. 23 – Verantwortlichkeit

Werden strafbare Handlungen im Geschäftsbetrieb einer juristischen Person, einer Personengesellschaft oder einer Einzelfirma begangen, so finden die Strafbestimmungen auf die Personen Anwendung, die für sie gehandelt haben oder hätten handeln sollen, jedoch unter solidarischer Mithaftung der juristischen Person, der Personengesellschaft oder der Einzelfirma für die Bussen und Kosten.

Die Regelung betreffend die Verantwortlichkeit der juristischen Personen wurde nach der Vernehmlassung und legislatischen Prüfung eingefügt.

VI. Schlussbestimmung

Zu Art. 24 – Inkrafttreten

In der Vernehmlassungsvorlage sollte in Art. 22 angesichts der Dringlichkeit der Umsetzung der Richtlinie (EU) 2016/1148 das gegenständliche Gesetz am Tage der Kundmachung in Kraft treten.

Der **Liechtensteinische Bankenverband** bittet jedoch um Kopplung des Inkrafttretens dieses Gesetzes an den EWR-Übernahmebeschlusses zur Richtlinie (EU) 2016/1148.

*Dieser Bitte wird insofern nachgekommen, dass mit **Abs. 1** des gegenständlichen Vorschlags das Cyber-Sicherheitsgesetz nun gleichzeitig mit dem Beschluss des*

*Gemeinsamen EWR-Ausschusses betreffend die Übernahme der Richtlinie (EU) 2016/1148 in das EWR-Abkommen in Kraft treten soll. Selbiges gilt für die Verordnung (EU) 2021/887 gemäss **Abs. 2**.*

Seitens der Regierung wird jedoch bereits zu diesem Zeitpunkt darauf hingewiesen, dass im Hinblick auf die zweite Lesung und Beschlussfassung im Landtag die gegenständliche Bestimmung dahingehend anpasst werden soll, dass eine Vorabumsetzung vorgesehen wird, sofern erkennbar wird, dass sich die EWR-Übernahme verzögert. Die Regierung steht diesbezüglich im Austausch mit den beiden anderen EWR/EFTA-Staaten Island und Norwegen. Aus Sicht der Regierung ist es unbedingt erforderlich, dass die Richtlinie (EU) 2016/1148 möglichst rasch umgesetzt werden kann. Nur so kann sichergestellt werden, dass Liechtenstein im Bereich der Cyber-Sicherheit denselben Rechtsbestand aufweist wie die EU-Mitgliedstaaten. Ausserdem werden durch die gegenständliche Gesetzesvorlage die rechtlichen Grundlagen für die Tätigkeit der Stabsstelle Cyber-Sicherheit geschaffen und sichergestellt, dass diese Zugang zu allen relevanten EU-Arbeitsgruppen und -gremien erhält. Begründet wird dies insbesondere wie in Abschnitt 4.2.1 ausführlich erläutert.

5.2 Gesetz über die Abänderung des Beschwerdekommissionsgesetzes

Zu Art. 4 Abs. 1 Bst. w

Die Bestimmung ergänzt die Zuständigkeit der Beschwerdekommission für Verwaltungsangelegenheiten für Beschwerden gegen Verfügungen und Entscheidungen der Stabstelle Cyber-Sicherheit im Rahmen des Cyber-Sicherheitsgesetzes sowie der darauf gestützten Verordnungen.

6. VERFASSUNGSMÄSSIGKEIT / RECHTLICHES

Die gegenständliche Gesetzesvorlage wirft keine verfassungsrechtlichen Fragen auf.

7. AUSWIRKUNGEN AUF VERWALTUNGSTÄTIGKEIT UND RESSOURCENEINSATZ

7.1 Neue und veränderte Kernaufgaben

Die Übernahme und Umsetzung der Richtlinie (EU) 2016/1148 sowie die Durchführung der Verordnung (EU) 2021/887 bedingen den Aufbau nationaler Kapazitäten für Cybersicherheit sowie eine stärkere Zusammenarbeit der EWR-Mitgliedstaaten. Gemäss den relevanten EWR-rechtlichen Bestimmungen 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. Zudem ist eine nationale Behörde als zentrale Anlaufstelle und Verbindungsstelle zur Gewährleistung der grenzüberschreitenden Zusammenarbeit mit internationalen Gruppen und Gremien einzurichten. Mit dieser Funktion wird die Stabsstelle Cyber-Sicherheit (SCS) betraut werden.

7.2 Personelle, finanzielle, organisatorische und räumliche Auswirkungen

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

7.3 Betroffene UNO-Nachhaltigkeitsziele und Auswirkungen auf deren Umsetzung

Netz- und Informationssysteme spielen eine zentrale Rolle für das Funktionieren des staatlichen Gemeinwesens. Die Sicherstellung ihrer Verlässlichkeit und Sicherheit ist deshalb von grosser Bedeutung und mit entsprechenden Massnahmen soll ein hohes, dem Risiko angemessenes Sicherheitsniveau von Netz- und Informationssystemen erreicht werden.

Es wird daher erwartet, dass die Regierungsvorlage Auswirkungen auf die folgenden UNO-Nachhaltigkeitsziele (SDGs) haben wird:

Betroffenes Ziel	Relevante Unterziele	Zu erwartende Auswirkungen durch die Regierungsvorlage
SDG 5 Geschlechtergleichheit	5.b, 5.1, 5.5	<p>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.</p> <p>Auch bei der Erstellung der nationalen Strategie von Netz- und Informationssystemen wird der Gender</p>

		<p>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.</p> <p>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.</p>
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	8.2, 8.3, 8.10	Durch hohe Cyber-Standards technologische Modernisierung und Innovation erreichen, die gleichzeitig

Menschenwürdige Arbeit und Wirtschaftswachstum		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. Die Regierung kommt deshalb zum Schluss, dass die Vorlage die Nachhaltigkeit im Sinne der SDGs verbessert.

7.4 Evaluation

Es ist keine Frist für eine Evaluation vorgesehen.

II. ANTRAG DER REGIERUNG

Aufgrund der vorstehenden Ausführungen unterbreitet die Regierung dem Landtag den

Antrag,

der Hohe Landtag wolle diesen Bericht und Antrag zur Kenntnis nehmen und die beiliegende Gesetzesvorlage in Behandlung ziehen.

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

III. REGIERUNGSVORLAGE

Cyber-Sicherheitsgesetz (CSG)

vom ...

Dem nachstehenden vom Landtag gefassten Beschluss erteile Ich Meine Zustimmung:

I. Allgemeine Bestimmungen

Art. 1

Gegenstand und Geltungsbereich

1) Dieses Gesetz legt die Massnahmen fest, mit denen ein hohes Sicherheitsniveau von Netz- und Informationssystemen erreicht werden soll von:

a) Betreibern wesentlicher Dienste in den Sektoren Energie, Verkehr, Bankwesen, Finanzmarktinfrastrukturen, Gesundheitswesen, Trinkwasserlieferung und -versorgung sowie Digitale Infrastruktur; und

b) Anbietern digitaler Dienste.

2) Die in diesem Gesetz vorgesehenen Sicherheitsanforderungen und Meldepflichten gelten nicht für:

- a) Unternehmen, die den Anforderungen nach Art. 40 und 41 der Richtlinie (EU) 2018/1972⁷ unterliegen; und
- b) Vertrauensdiensteanbieter, die den Anforderungen nach Art. 19 der Verordnung (EU) Nr. 910/2014⁸ unterliegen.

Art. 2

Umsetzung und Durchführung von EWR-Rechtsvorschriften

1) Dieses Gesetz dient der Umsetzung bzw. Durchführung folgender EWR-Rechtsvorschriften:

- a) Richtlinie (EU) 2016/1148 über Massnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union⁹;
- b) Verordnung (EU) 2021/887 zur Einrichtung des Europäischen Kompetenzzentrums für Industrie, Technologie und Forschung im Bereich der Cybersicherheit und des Netzwerks nationaler Koordinierungszentren¹⁰.

2) Die gültige Fassung der EWR-Rechtsvorschriften, auf die in diesem Gesetz Bezug genommen wird, ergibt sich aus der Kundmachung der Beschlüsse des

⁷ Richtlinie (EU) 2018/1972 des Europäischen Parlaments und des Rates vom 11. Dezember 2018 über den europäischen Kodex für die elektronische Kommunikation (ABl. L 321 vom 17.12.2018, S. 36)

⁸ 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)

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) 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)

Gemeinsamen EWR-Ausschusses im Liechtensteinischen Landesgesetzblatt nach Art. 3 Bst. k des Kundmachungsgesetzes.

Art. 3

Begriffsbestimmungen und Bezeichnungen

1) Im Sinne dieses Gesetzes gelten als:

- a) "Netz- und Informationssystem":
 - 1. ein elektronisches Kommunikationsnetz im Sinne von Art. 3 Abs. 1 Ziff. 5 des Kommunikationsgesetzes;
 - 2. 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
 - 3. digitale Daten, die von den in Ziff. 1 und 2 genannten Elementen zum Zwecke ihres Betriebs, ihrer Nutzung, ihres Schutzes und ihrer Pflege gespeichert, verarbeitet, abgerufen oder übertragen werden;
- b) "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, übermittelter oder verarbeiteter Daten oder entsprechender Dienste, die über diese Netz- und Informationssysteme angeboten werden oder zugänglich sind, beeinträchtigen;
- c) "NIS-Strategie" (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;

- d) "wesentlicher Dienst": ein Dienst:
1. der in einem der in Art. 1 Abs. 1 Bst. a genannten Sektoren erbracht wird;
 2. der für die Aufrechterhaltung kritischer gesellschaftlicher oder wirtschaftlicher Tätigkeiten von wesentlicher Bedeutung ist, insbesondere für die Aufrechterhaltung des öffentlichen Gesundheitsdienstes, der öffentlichen Versorgung mit Wasser, Energie sowie lebenswichtigen Gütern, des öffentlichen Verkehrs oder die Funktionsfähigkeit öffentlicher Informations- und Kommunikationstechnologien;
 3. dessen Bereitstellung abhängig von Netz- und Informationssystemen ist; und
 4. bei dem ein Sicherheitsvorfall mit tatsächlichen Auswirkungen auf die Sicherheit von Netz- und Informationssystemen eine erhebliche Störung bei der Bereitstellung dieses Dienstes bewirken würde;
- e) "Betreiber wesentlicher Dienste": eine öffentliche oder private Einrichtung mit Sitz in Liechtenstein, die einen wesentlichen Dienst erbringt;
- f) "digitaler Dienst": ein Dienst im Sinne des Art. 3 Abs. 1 Bst. e des EWR-Notifikationsgesetzes, bei dem es sich um einen Online-Marktplatz, eine Online-Suchmaschine oder einen Cloud-Computing-Dienst handelt;
- g) "Anbieter digitaler Dienste": eine juristische Person, die einen digitalen Dienst anbietet und die keine kleine Gesellschaft oder Kleinstgesellschaft im Sinne des Art. 1064 Abs. 1 und 1a des Personen- und Gesellschaftsrechts ist:
1. mit Sitz in Liechtenstein; oder
 2. mit Sitz ausserhalb des Europäischen Wirtschaftsraums (EWR), die einen Vertreter nach Bst. h namhaft gemacht hat;

- h) "Vertreter": eine natürliche oder juristische Person mit Wohnsitz oder Sitz in Liechtenstein, die ausdrücklich benannt wurde, um im Auftrag eines Anbieters digitaler Dienste mit Sitz ausserhalb des EWR zu handeln, und an die sich die Stabsstelle Cyber-Sicherheit – statt an den Anbieter digitaler Dienste – hinsichtlich der Pflichten dieses Anbieters digitaler Dienste gemäss diesem Gesetz wenden kann;
- i) "Sicherheitsvorfall": jedes Ereignis, das die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit gespeicherter, übermittelter oder verarbeiteter Daten oder entsprechender Dienste, die über Netz- und Informationssysteme angeboten werden oder zugänglich sind, beeinträchtigen;
- k) "Bewältigung von Sicherheitsvorfällen": alle Verfahren zur Unterstützung der Erkennung, Analyse und Eindämmung von Sicherheitsvorfällen sowie die Reaktion darauf;
- l) "Risiko": alle mit vernünftigem Aufwand feststellbaren Umstände oder Ereignisse, die potenziell nachteilige Auswirkungen auf die Sicherheit von Netz- und Informationssystemen haben;
- m) "Kooperationsgruppe": ein nach Art. 11 der Richtlinie (EU) 2016/1148 eingerichtetes Gremium, das sich aus Vertretern der EWR-Mitgliedstaaten, der Europäischen Kommission und der Europäischen Agentur für Netz- und Informationssicherheit (ENISA) zusammensetzt und der Unterstützung und Erleichterung der strategischen Zusammenarbeit sowie des Informationsaustausches zwischen den EWR-Mitgliedstaaten zum Aufbau von Vertrauen und zur Erreichung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen im EWR dient;
- n) "CSIRTs-Netzwerk": ein nach Art. 12 der Richtlinie (EU) 2016/1148 eingerichtetes Gremium, das sich aus Vertretern der Computer-

Notfallteams der EWR-Mitgliedstaaten und des europäischen Computer-Notfallteams zusammensetzt und zum Aufbau von Vertrauen zwischen den EWR-Mitgliedstaaten beitragen und eine rasche und wirksame operative Zusammenarbeit fördern soll;

- o) "Online-Marktplatz": ein digitaler Dienst, der es Verbrauchern oder Unternehmen ermöglicht, Online-Kaufverträge oder Online-Dienstleistungsverträge mit Unternehmen entweder auf der Internetseite des Online-Marktplatzes oder auf der Internetseite eines Unternehmers, die von dem Online-Marktplatz bereitgestellte Rechendienste verwendet, abzuschliessen;
- p) "Online-Suchmaschine": ein digitaler Dienst, der es Nutzern ermöglicht, Suchen grundsätzlich auf allen Internetseiten oder auf Internetseiten 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;
- q) "Cloud-Computing-Dienst": ein digitaler Dienst, der den Zugang zu einem skalierbaren und elastischen Pool gemeinsam nutzbarer Rechenressourcen ermöglicht.

2) Unter den in diesem Gesetz verwendeten Personenbezeichnungen sind alle Personen unabhängig von ihrem Geschlecht zu verstehen, sofern sich die Personenbezeichnungen nicht ausdrücklich auf ein bestimmtes Geschlecht beziehen.

II. Sicherheitsanforderungen und Meldepflichten

A. Betreiber wesentlicher Dienste

Art. 4

Sicherheitsanforderungen

1) Betreiber wesentlicher Dienste ergreifen geeignete und verhältnismässige technische und organisatorische Massnahmen, um die Risiken für die Sicherheit der Netz- und Informationssysteme, die sie für ihre Tätigkeiten nutzen, zu bewältigen.

2) Die Massnahmen nach Abs. 1 müssen unter Berücksichtigung des Stands der Technik ein Sicherheitsniveau der Netz- und Informationssysteme gewährleisten, welches dem bestehenden Risiko angemessen ist.

3) Betreiber wesentlicher Dienste ergreifen geeignete Massnahmen, um den Auswirkungen von Sicherheitsvorfällen, welche die Sicherheit der von ihnen für die Bereitstellung von Diensten genutzten Netz- und Informationssysteme beeinträchtigen, vorzubeugen beziehungsweise diese so gering wie möglich zu halten, damit die Verfügbarkeit ihrer Dienste gewährleistet wird.

4) Die Pflichten nach Abs. 1 bis 3 finden keine Anwendung, wenn spezialgesetzliche Bestimmungen über Sicherheitsanforderungen bestehen, die zumindest ein gleichwertiges Sicherheitsniveau für Netz- und Informationssysteme vorsehen.

5) Die Regierung kann das Nähere über die Sicherheitsanforderungen für Betreiber wesentlicher Dienste mit Verordnung regeln.

Art. 5

Meldepflicht

1) Betreiber wesentlicher Dienste haben einen Sicherheitsvorfall, der erhebliche Auswirkungen auf die Verfügbarkeit eines von ihnen bereitgestellten Dienstes hat oder der geeignet ist, sich erheblich auf die Verfügbarkeit eines von ihnen bereitgestellten Dienstes auszuwirken, unverzüglich der Stabsstelle Cyber-Sicherheit zu melden.

2) Die Meldung muss sämtliche relevante Angaben zum Sicherheitsvorfall und zu den technischen Rahmenbedingungen, die im Zeitpunkt der Erstmeldung bekannt sind, enthalten, insbesondere die vermutete oder tatsächliche Ursache, die betroffene Informationstechnik, die Art der betroffenen Einrichtung oder Anlage. Angaben über später bekanntgewordene Umstände zum Sicherheitsvorfall sind in Nachmeldungen und letztendlich in einer Abschlussmeldung unverzüglich nach Feststellung der Umstände mitzuteilen.

3) Meldungen sind in einem gesicherten und soweit möglich standardisierten elektronischen Format zu übermitteln.

4) Nimmt ein Betreiber wesentlicher Dienste für die Bereitstellung eines wesentlichen Dienstes die Dienste eines Dritten als Anbieter digitaler Dienste in Anspruch, so ist jede Auswirkung auf die Verfügbarkeit dieser Dienste im Sinne des Abs. 1, die von einem den Anbieter digitaler Dienste beeinträchtigenden Sicherheitsvorfall verursacht wurde, vom Betreiber wesentlicher Dienste unverzüglich der Stabsstelle Cyber-Sicherheit zu melden.

5) Nach Anhörung des meldenden Betreibers wesentlicher Dienste kann die Stabsstelle Cyber-Sicherheit die Öffentlichkeit über konkrete Sicherheitsvorfälle

unterrichten, wenn die Sensibilisierung der Öffentlichkeit zur Verhütung von Sicherheitsvorfällen oder zur Bewältigung aktueller Sicherheitsvorfälle erforderlich ist.

6) Die Pflichten nach Abs. 1 bis 5 finden keine Anwendung, wenn spezialgesetzliche Bestimmungen über die Meldepflicht bestehen und die Kriterien für die Meldepflicht mindestens gleichwertig sind. In diesen Fällen haben die Meldungsempfänger die bei ihnen eingegangenen Meldungen unverzüglich an die Stabsstelle Cyber-Sicherheit weiterzuleiten.

7) Die Regierung kann das Nähere über die Meldepflicht für Betreiber wesentlicher Dienste mit Verordnung regeln.

B. Anbieter digitaler Dienste

Art. 6

Sicherheitsanforderungen

1) Anbieter digitaler Dienste ergreifen geeignete und verhältnismässige technische und organisatorische Massnahmen, um die Risiken für die Sicherheit der Netz- und Informationssysteme, die sie im Rahmen der Bereitstellung des digitalen Dienstes nutzen, zu bewältigen.

2) Die Massnahmen nach Abs. 1 müssen unter Berücksichtigung des Stands der Technik ein Sicherheitsniveau der Netz- und Informationssysteme gewährleisten, welches dem bestehenden Risiko angemessen ist, wobei Folgendem Rechnung getragen wird:

a) der Sicherheit der Systeme und Anlagen;

- b) der Bewältigung von Sicherheitsvorfällen;
- c) dem Betriebskontinuitätsmanagement;
- d) der Überwachung, Überprüfung und Erprobung;
- e) der Einhaltung internationaler Normen.

Art. 7

Meldepflicht

1) Anbieter digitaler Dienste haben jeden Sicherheitsvorfall, der erhebliche Auswirkungen auf die Bereitstellung eines von ihnen im EWR erbrachten Dienstes hat, unverzüglich der Stabsstelle Cyber-Sicherheit zu melden.

2) Nach Anhörung des betreffenden Anbieters digitaler Dienste kann die Stabsstelle Cyber-Sicherheit die Öffentlichkeit über konkrete Sicherheitsvorfälle unterrichten oder verlangen, dass der Anbieter digitaler Dienste dies unternimmt, wenn:

- a) die Sensibilisierung der Öffentlichkeit zur Verhütung von Sicherheitsvorfällen oder zur Bewältigung aktueller Sicherheitsvorfälle erforderlich ist; oder
- b) die Offenlegung des Sicherheitsvorfalls auf sonstige Weise im öffentlichen Interesse liegt.

C. Andere Einrichtungen

Art. 8

Freiwillige Meldung

1) Einrichtungen, die nicht als Betreiber wesentlicher Dienste ermittelt wurden und keine Anbieter digitaler Dienste sind, können Risiken und Sicherheitsvorfälle der Stabsstelle Cyber-Sicherheit melden.

2) Die freiwillige Meldung muss weder die Identität der Einrichtung noch Informationen, die auf diese schliessen lassen, enthalten.

III. Organisation und Durchführung

A. Allgemeines

Art. 9

Zuständigkeit

1) Mit der Durchführung dieses Gesetzes sind betraut:

- a) die Stabsstelle Cyber-Sicherheit;
- b) das Computer-Notfallteam (CSIRT).

2) Die Stabsstelle Cyber-Sicherheit und das CSIRT können zur Erfüllung ihrer Aufgaben qualifizierte Dritte beauftragen.

3) Die Regierung kann das Nähere über die Anforderungen an qualifizierte Dritte nach Abs. 2 mit Verordnung regeln.

Art. 10

Amtsgeheimnis

Die mit der Durchführung dieses Gesetzes betrauten Organe sowie allfällig durch diese beauftragte qualifizierte Dritte unterliegen dem Amtsgeheimnis und haben gegenüber anderen Amtsstellen und Personen über die in Ausübung dieser Tätigkeit gemachten Wahrnehmungen Stillschweigen zu bewahren und Einsicht in verarbeitete Daten und amtliche Akten zu verweigern. Art. 14 bleibt vorbehalten.

Art. 11

Verarbeitung und Offenlegung personenbezogener Daten

1) Die Stabsstelle Cyber-Sicherheit ist berechtigt, zur Gewährleistung eines hohen Sicherheitsniveaus von Netz- und Informationssystemen bei der Wahrnehmung ihrer Aufgaben nach diesem Gesetz die erforderlichen personenbezogenen Daten nach Art. 4 Ziff. 1 der Verordnung (EU) 2016/679¹¹ zu verarbeiten.

2) Sie kann Daten nach Abs. 1, die ihr aufgrund der Wahrnehmung ihrer Aufgaben nach diesem Gesetz bekannt sind, in- und ausländischen Behörden und Stellen offenlegen, wenn:

- a) dies zur Erfüllung ihrer Aufgaben nach diesem Gesetz oder der Richtlinie (EU) 2016/1148 erforderlich ist;
- b) die Vertraulichkeit der Daten gewährleistet ist; sowie

¹¹ 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)

- c) die Sicherheit und die geschäftlichen Interessen der Betreiber wesentlicher Dienste und der Anbieter digitaler Dienste geschützt sind.

B. Stabsstelle Cyber-Sicherheit

Art. 12

Zuständigkeit

1) Die Stabsstelle Cyber-Sicherheit ist die für die Sicherheit von Netz- und Informationssystemen zuständige nationale Behörde nach Art. 8 Abs. 1 der Richtlinie (EU) 2016/1148. Ihr obliegt die Aufsicht und der Vollzug dieses Gesetzes.

2) Die Stabsstelle Cyber-Sicherheit ist zudem die für die Sicherheit von Netz- und Informationssystemen zuständige zentrale Anlaufstelle nach Art. 8 Abs. 3 der Richtlinie (EU) 2016/1148. Sie ist die Verbindungsstelle zur Gewährleistung der grenzüberschreitenden Zusammenarbeit mit internationalen Gremien und Gruppen, wie insbesondere den zuständigen Stellen in anderen EWR-Mitgliedstaaten, der Kooperationsgruppe und dem CSIRTs-Netzwerk.

Art. 13

Aufgaben

1) Die Stabsstelle Cyber-Sicherheit trifft die im Rahmen ihrer Zuständigkeit erforderlichen Massnahmen, um die Einhaltung dieses Gesetzes sicherzustellen. Ihr obliegen insbesondere:

- a) die Überprüfung der Sicherheitsanforderungen nach Art. 4 und 6 sowie die Einhaltung der Meldepflichten nach Art. 5 und 7;
- b) die Einrichtung und Koordination des CSIRT nach Art. 19;

- c) die Entgegennahme und Analyse von Meldungen über Risiken oder Sicherheitsvorfälle, die Erstellung eines diesbezüglichen Lagebildes und Weiterleitung der Meldungen sowie des Lagebildes und zusätzlicher relevanter Informationen an inländische Behörden oder andere betroffene Stellen bei Bedarf;
- d) die Erstellung und Weitergabe von relevanten Informationen zur Gewährleistung der Sicherheit von Netz- und Informationssystemen oder zur Vorbeugung von Sicherheitsvorfällen;
- e) die Ermittlung der Betreiber wesentlicher Dienste sowie die Erstellung und regelmässige, mindestens jedoch einmal alle zwei Jahre, Überprüfung und Aktualisierung einer Liste mit wesentlichen Diensten;
- f) die Unterrichtung und Weiterleitung von durch den Betreiber wesentlicher Dienste bereitgestellten Informationen an die zentrale Anlaufstelle der betroffenen EWR-Mitgliedstaaten, wenn ein Sicherheitsvorfall erhebliche Auswirkungen auf die Verfügbarkeit wesentlicher Dienste in diesen EWR-Mitgliedsstaaten hat;
- g) die Koordination der öffentlich-privaten Zusammenarbeit im Bereich der Sicherheit von Netz- und Informationssystemen;
- h) die Unterrichtung der Öffentlichkeit über Sicherheitsvorfälle, die Sensibilisierung der Öffentlichkeit zur Verhütung oder Bewältigung von Sicherheitsvorfällen sowie die Veröffentlichung allgemeiner Informationen im Zusammenhang mit der Sicherheit von Netz- und Informationssystemen;
- i) die Zusammenarbeit und der Informationsaustausch mit anderen inländischen Behörden und Stellen, insbesondere der Landespolizei, der Staatsanwaltschaft, der Datenschutzstelle, dem Amt für Kommunikation, der Stabsstelle FIU und der Finanzmarktaufsicht Liechtenstein;

- k) die grenzüberschreitende Zusammenarbeit und der grenzüberschreitende Informationsaustausch mit den zuständigen Behörden und Stellen in anderen EWR-Mitgliedstaaten, der ENISA, der Kooperationsgruppe und dem CSIRTs-Netzwerk;
- l) die grenzüberschreitende Zusammenarbeit und der grenzüberschreitende Informationsaustausch im Bereich der Sicherheit von Netz- und Informationssystemen mit den zuständigen Behörden und Stellen in Drittstaaten;
- m) die Koordination der Erstellung einer NIS-Strategie nach Art. 20;
- n) die Vertretung Liechtensteins in der Kooperationsgruppe, dem CSIRTs-Netzwerk sowie in anderen grenzüberschreitenden Gremien im EWR und internationalen Gremien für die Sicherheit von Netz- und Informationssystemen.

2) Die Stabsstelle Cyber-Sicherheit kann nach Rücksprache mit dem zuständigen Regierungsmitglied mit anderen in- und ausländischen Behörden Vereinbarungen über die Modalitäten der Zusammenarbeit abschliessen sowie zur Aufgabenerfüllung mit Privaten im Rahmen von öffentlich-privaten Partnerschaften zusammenarbeiten.

3) Die Regierung kann das Nähere über die Aufgaben der Stabsstelle Cyber-Sicherheit mit Verordnung regeln.

Art. 14

Befugnisse gegenüber Betreibern wesentlicher Dienste

1) Die Stabsstelle Cyber-Sicherheit kann bei der Wahrnehmung ihrer Aufgaben nach diesem Gesetz von den Betreibern wesentlicher Dienste verlangen, dass sie ihr:

- 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 erbringen;
- c) Informationen, insbesondere technische und statistische Daten, zu statistischen Zwecken oder für die Erstellung konkreter Lagebilder unentgeltlich offenlegen.

2) Betreiber wesentlicher Dienste können die Offenlegung von Informationen nach Abs. 1 Bst. c nicht wegen Berufs-, Geschäfts- oder Betriebsgeheimnissen verweigern.

Art. 15

Befugnisse gegenüber Anbietern digitaler Dienste

Die Stabsstelle Cyber-Sicherheit kann, wenn ihr Nachweise vorliegen, dass Anbieter digitaler Dienste die Anforderungen nach diesem Gesetz nicht einhalten, von den Anbietern verlangen, dass sie ihr die zur Beurteilung der Sicherheit ihrer Netz- und Informationssysteme erforderlichen Informationen nach Art. 2 Abs. 2

der Durchführungsverordnung (EU) 2018/151¹², einschliesslich der nachweislichen Sicherheitsmassnahmen, unverzüglich zur Verfügung stellen.

Art. 16

Befugnisse bei Verstössen

1) Hat die Stabsstelle Cyber-Sicherheit Anhaltspunkte dafür, dass ein Betreiber wesentlicher Dienste oder ein Anbieter digitaler Dienste gegen Vorschriften dieses Gesetzes, der dazu erlassenen Verordnungen oder gegen darauf gestützte Entscheidungen oder Verfügungen verstösst, teilt sie dies dem Betreiber wesentlicher Dienste oder dem Anbieter digitaler Dienste vorbehaltlich Abs. 5 formlos mit und setzt ihm eine angemessene Frist, um:

- a) zur Mitteilung Stellung zu nehmen; oder
- b) den rechtmässigen Zustand herzustellen.

2) Die Stabsstelle Cyber-Sicherheit kann die Frist nach Abs. 1 Bst. b in begründeten Fällen auf Antrag angemessen verlängern, wenn der Betreiber wesentlicher Dienste oder der Anbieter digitaler Dienste dadurch voraussichtlich den rechtmässigen Zustand herstellt.

3) Handelt es sich beim Betreiber wesentlicher Dienste oder beim Anbieter digitaler Dienste um eine öffentliche Stelle oder eine Stelle, welche mit öffentlichen Aufgaben betraut ist, informiert die Stabsstelle Cyber-Sicherheit zusätzlich die Regierung über die Aufforderung nach Abs. 1.

¹² 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)

4) Die Stabsstelle Cyber-Sicherheit informiert bei Anhaltspunkten zu Verstößen gegen Vorschriften dieses Gesetzes oder dazu erlassenen Verordnungen durch Betreiber wesentlicher Dienste oder Anbieter digitaler Dienste die zuständige Aufsichtsbehörde und gibt dieser vor einer Aufforderung nach Abs. 1 Gelegenheit zur Stellungnahme.

5) Kommt ein Betreiber wesentlicher Dienste oder ein Anbieter digitaler Dienste der Aufforderung nach Abs. 1 nicht nach, so erlässt die Stabsstelle Cyber-Sicherheit eine entsprechende Verfügung; in dringenden Fällen kann auch ohne Aufforderung eine Verfügung erfolgen. Die Stabsstelle Cyber-Sicherheit informiert die zuständige Aufsichtsbehörde des Betreibers wesentlicher Dienste oder des Anbieters digitaler Dienste über die Entscheidung.

6) Die Verhängung von Bussen nach Art. 22 bleibt vorbehalten.

Art. 17

Betrieb von Informations- und Kommunikationstechnik-Lösungen (IKT-Lösungen)

Die Stabsstelle Cyber-Sicherheit ist zur Erfüllung ihrer Aufgaben berechtigt:

- a) IKT-Lösungen zu betreiben oder durch Dritte betreiben zu lassen, die Risiken oder Sicherheitsvorfälle von Netz- und Informationssystemen frühzeitig erkennen;
- b) IKT-Lösungen zu betreiben oder nach Einwilligung der betroffenen Einrichtung zu nutzen, um die Muster von Angriffen auf Netz- und Informationssysteme zu erkennen.

Art. 18

Kontrolle

1) Die Stabsstelle Cyber-Sicherheit kann Kontrollen zur Einhaltung der Anforderungen nach diesem Gesetz durchführen oder durch von ihr beauftragte qualifizierte Dritte durchführen lassen.

2) Zur Durchführung von Kontrollen können die Stabsstelle Cyber-Sicherheit oder von ihr beauftragte qualifizierte Dritte Einsicht in die Netz- und Informationssysteme, die für die Bereitstellung wesentlicher Dienste und Anbieter digitaler Dienste genutzt werden, und diesbezügliche Unterlagen nehmen. Dabei sind sie berechtigt, Örtlichkeiten, in welchen Netz- und Informationssysteme gelegen sind, zu betreten. Die Ausübung der Einsicht hat verhältnismässig zu erfolgen und ist unter möglicher Schonung der Rechte der betroffenen Einrichtung und Dritter sowie des Betriebs auszuüben.

3) Die Regierung kann das Nähere über die Durchführung von Kontrollen mit Verordnung regeln.

C. Computer-Notfallteam (CSIRT)

Art. 19

Zweck und Aufgaben

1) Zur Gewährleistung der Sicherheit von Netz- und Informationssystemen wird bei der Stabsstelle Cyber-Sicherheit ein CSIRT eingerichtet. Ihm obliegen insbesondere:

- a) gegebenenfalls das zur Verfügung stellen von zur Bewältigung eines Sicherheitsvorfalls nützlichen Informationen nach Eingang von Meldungen über Risiken oder Sicherheitsvorfälle nach Art. 5, 7 und 8;
- b) die Ausgabe von Frühwarnungen und Alarmmeldungen sowie die Bekanntmachung und Verbreitung von Informationen über Risiken und Sicherheitsvorfälle unter den einschlägigen Interessenträgern;
- c) die erste allgemeine Unterstützung bei der Reaktion auf einen Sicherheitsvorfall;
- d) die Beobachtung und Analyse von Risiken und Sicherheitsvorfällen sowie die Lagebeurteilung;
- e) die Beteiligung am CSIRTs-Netzwerk.

2) Das CSIRT kann die Aufgaben nach Abs. 1 Bst. a bis d auch gegenüber sonstigen Einrichtungen oder Personen wahrnehmen, wenn diese von einem Risiko oder einem Sicherheitsvorfall ihrer Netz- und Informationssysteme betroffen sind.

3) Die Regierung kann das Nähere über den Zweck und die Aufgaben des CSIRT mit Verordnung regeln.

D. NIS-Strategie

Art. 20

Grundsatz

1) Die NIS-Strategie bestimmt insbesondere die strategischen Ziele und angemessenen Politik- und Regulierungsmassnahmen, mit denen ein hohes

Sicherheitsniveau von Netz- und Informationssystemen erreicht und aufrechterhalten werden soll.

2) Die Stabsstelle Cyber-Sicherheit teilt die NIS-Strategie der EFTA-Überwachungsbehörde innerhalb von drei Monaten nach ihrer Festlegung mit. Elemente der Strategie, die die nationale Sicherheit berühren, sind nicht mitzuteilen.

3) Die NIS-Strategie ist von der Regierung zu genehmigen.

IV. Rechtsmittel

Art. 21

Beschwerde

1) Gegen Entscheidungen und Verfügungen der Stabsstelle Cyber-Sicherheit kann binnen 14 Tagen ab Zustellung Beschwerde bei der Beschwerdekommision für Verwaltungsangelegenheiten erhoben werden.

2) Gegen Entscheidungen und Verfügungen der Beschwerdekommision für Verwaltungsangelegenheiten kann binnen 14 Tagen ab Zustellung Beschwerde an den Verwaltungsgerichtshof erhoben werden.

3) Die Überprüfungsbefugnis der Beschwerdekommision für Verwaltungsangelegenheiten sowie des Verwaltungsgerichtshofes beschränkt sich auf Rechts- und Sachfragen. Die Ausübung des Ermessens wird ausschliesslich rechtlich überprüft.

4) Im Übrigen finden auf das Verfahren die Bestimmungen des Gesetzes über die allgemeine Landesverwaltungspflege Anwendung.

V. Strafbestimmungen

Art. 22

Verwaltungsübertretungen

1) Von der Stabsstelle Cyber-Sicherheit wird, wenn die Tat nicht den Tatbestand einer in die Zuständigkeit der Gerichte fallenden strafbaren Handlung bildet, wegen Übertretung mit Busse bis zu 100 000 Franken bestraft, wer:

- a) als Betreiber wesentlicher Dienste nicht die vorgeschriebenen Massnahmen nach Art. 4 Abs. 1 bis 3 ergreift;
- b) als Betreiber wesentlicher Dienste die Meldepflicht nach Art. 5 Abs. 1 bis 4 verletzt;
- c) als Anbieter digitaler Dienste nicht die vorgeschriebenen Massnahmen nach Art. 6 Abs. 1 und 2 ergreift;
- d) als Anbieter digitaler Dienste die Meldepflicht nach Art. 7 Abs. 1 verletzt;
- e) als Betreiber wesentlicher Dienste die nach Art. 14 Abs. 1 Bst. a erforderlichen Informationen, einschliesslich der dokumentierten Sicherheitsmassnahmen, nicht zur Verfügung stellt;
- f) als Betreiber wesentlicher Dienste Nachweise nach Art. 14 Abs. 1 Bst. b nicht erbringt;
- g) als Betreiber wesentlicher Dienste Informationen nach Art. 14 Abs. 1 Bst. c gegenüber der Stabsstelle Cyber-Sicherheit nicht offenlegt;

- h) als Anbieter digitaler Dienste die zur Beurteilung der Sicherheit ihrer Netz- und Informationssysteme nach Art. 15 erforderlichen Informationen, einschliesslich der nachweislichen Sicherheitsmassnahmen, nicht unverzüglich zur Verfügung stellt;
- i) als Betreiber wesentlicher Dienste oder Anbieter digitaler Dienste die ordnungsgemässe Durchführung einer Kontrolle nach Art. 18 erschwert, behindert oder verunmöglicht;
- k) als Betreiber wesentlicher Dienste oder als Anbieter digitaler Dienste gegen eine rechtskräftige Verfügung oder Entscheidung der Stabsstelle Cyber-Sicherheit verstösst.

2) Bei fahrlässiger Begehung wird die Strafobergrenze nach Abs. 1 auf die Hälfte herabgesetzt. Im Wiederholungsfall verdoppelt sich die Strafobergrenze.

Art. 23

Verantwortlichkeit

Werden strafbare Handlungen im Geschäftsbetrieb einer juristischen Person, einer Personengesellschaft oder einer Einzelfirma begangen, so finden die Strafbestimmungen auf die Personen Anwendung, die für sie gehandelt haben oder hätten handeln sollen, jedoch unter solidarischer Mithaftung der juristischen Person, der Personengesellschaft oder der Einzelfirma für die Bussen und Kosten.

VI. Schlussbestimmung

Art. 24

Inkrafttreten

1) Dieses Gesetz tritt vorbehaltlich Abs. 2 gleichzeitig mit dem Beschluss des Gemeinsamen EWR-Ausschusses betreffend die Übernahme der Richtlinie (EU) 2016/1148 in das EWR-Abkommen in Kraft.

2) Art. 2 Abs. 1 Bst. b tritt gleichzeitig mit dem Beschluss des Gemeinsamen EWR-Ausschusses betreffend die Übernahme der Verordnung (EU) 2021/887 in das EWR-Abkommen in Kraft.

Gesetz

vom ...

über die Abänderung des Beschwerdekommis­ sionsgesetzes

Dem nachstehenden vom Landtag gefassten Beschluss erteile Ich Meine Zustimmung:

I.

Abänderung bisherigen Rechts

Das Beschwerdekommis­ sionsgesetz vom 25. Oktober 2000, LGBl. 2000 Nr. 248, wird wie folgt abgeändert:

Art. 4 Abs. 1 Bst. w

1) Die Beschwerdekommis­ sion ist zuständig für Beschwerden gegen Verfügungen und Entscheidungen im Bereich:

w) Cyber-Sicherheit:

der Stabsstelle Cyber-Sicherheit aufgrund des Cyber-Sicherheitsgesetzes sowie der darauf gestützten Verordnungen.

II.

Inkrafttreten

Dieses Gesetz tritt gleichzeitig mit dem Cyber-Sicherheitsgesetz vom ... in Kraft.

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 271 vom 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 Seeschiffahrtsorganisation 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 Teilspektoren 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 Teilspektoren 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 Teilspektoren 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 Teilspektoren 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 veröffentlichen 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 vernünftigen 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 Mitgliedsstaaten 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 der 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

Der Präsident

M. SCHULZ

Im Namen des Rates

Der Präsident

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
— 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 Verkehrssteuersystemen, 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 Aufsichtsbedingungen 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
-

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**

DIE EUROPÄISCHE KOMMISSION —

gestützt auf den Vertrag über die Arbeitsweise der Europäischen Union,

gestützt auf 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 ⁽¹⁾, insbesondere auf Artikel 16 Absatz 8,

in Erwägung nachstehender Gründe:

- (1) Gemäß der Richtlinie (EU) 2016/1148 steht es den Anbietern digitaler Dienste frei, technische und organisatorische Maßnahmen zu ergreifen, die sie zur Bewältigung der Risiken für die Sicherheit ihrer Netz- und Informationssysteme für angemessen und verhältnismäßig halten, sofern diese Maßnahmen ein angemessenes Sicherheitsniveau gewährleisten und den in der Richtlinie vorgesehenen Elementen Rechnung tragen.
- (2) Bei der Ermittlung der angemessenen und verhältnismäßigen technischen und organisatorischen Maßnahmen sollten die Anbieter digitaler Dienste die Informationssicherheit systematisch nach einem risikobasierten Ansatz angehen.
- (3) Zur Gewährleistung der Sicherheit der Systeme und Anlagen sollten die Anbieter digitaler Dienste Bewertungs- und Analyseverfahren durchführen. Diese Tätigkeiten sollten das systematische Management der Netz- und Informationssysteme, die physische Sicherheit und die Sicherheit des Umfelds, die Versorgungssicherheit und die Kontrolle des Zugangs umfassen.
- (4) Bei der Durchführung einer Risikoanalyse im Rahmen des systematischen Managements der Netz- und Informationssysteme sollten Anbieter digitaler Dienste dazu angehalten werden, spezifische Risiken zu ermitteln und hinsichtlich ihrer Bedeutung zu quantifizieren, indem sie beispielsweise ermitteln, welche Gefährdungen für unentbehrliche Anlagen oder Wirtschaftsgüter bestehen und wie sich diese auf den Betrieb auswirken können, und indem sie bestimmen, wie diese Gefährdungen unter Berücksichtigung der vorhandenen Fähigkeiten und des Ressourcenbedarfs am besten eingedämmt werden können.
- (5) Maßnahmen im Bereich Humanressourcen könnten das Kompetenzmanagement betreffen, darunter auch Aspekte der sicherheitsrelevanten Kompetenzentwicklung und Bewusstseinsbildung. Bei der Entscheidung über geeignete Maßnahmen für die Betriebssicherheit sollten die Anbieter digitaler Dienste dazu angehalten werden, die Aspekte des Änderungs- und des Schwachstellenmanagements, der Formalisierung betrieblicher und administrativer Verfahren und der Systemerfassung und -abbildung zu berücksichtigen.
- (6) Die Maßnahmen im Bereich Sicherheitsarchitektur könnten insbesondere die Trennung von Netzen und Systemen sowie spezifische Sicherheitsvorkehrungen für unentbehrliche Tätigkeiten, wie beispielsweise administrative Tätigkeiten, umfassen. Die Trennung von Netzen und Systemen könnte die Anbieter digitaler Dienste in die Lage versetzen, zwischen Elementen wie Datenströmen und Rechenressourcen zu unterscheiden, die einem Kunden, einer Gruppe von Kunden, dem Anbieter digitaler Dienste selbst oder Dritten gehören.
- (7) Die mit Blick auf die physische Sicherheit und die Sicherheit des Umfelds getroffenen Maßnahmen sollten die Sicherheit der Netz- und Informationssysteme einer Organisation vor Schäden durch Vorfälle wie Diebstahl, Brand, Überschwemmung oder andere Wettereinflüsse sowie Telekommunikations- oder Stromausfälle gewährleisten.
- (8) Die Sicherheit der Versorgung, z. B. mit elektrischem Strom, Brenn- und Kraftstoffen oder Kühlung, könnte auch die Sicherheit der Lieferkette umfassen, darunter insbesondere die Sicherheit bei Dritten, die Auftragnehmer und Unterauftragnehmer sind, und deren Management. Die Rückverfolgbarkeit unentbehrlicher Güter oder Vorleistungen betrifft die Fähigkeit des Anbieters digitaler Dienste, die Herkunft dieser Güter oder Vorleistungen festzustellen und zu dokumentieren.
- (9) Die Nutzer digitaler Dienste sollten natürliche und juristische Personen umfassen, die Kunden oder Teilnehmer eines Online-Marktplatzes oder eines Cloud-Computing-Dienstes sind, oder die die Website einer Online-Suchmaschine besuchen, um Stichwortsuchen durchzuführen.

⁽¹⁾ ABl. L 194 vom 19.7.2016, S. 1.

- (10) Bei der Definition der Erheblichkeit der Auswirkungen eines Sicherheitsvorfalls sollten die in dieser Verordnung genannten Fälle als nicht erschöpfende Liste erheblicher Sicherheitsvorfälle betrachtet werden. Es sollten Lehren aus der Durchführung dieser Verordnung und aus den Arbeiten der Kooperationsgruppe gemäß Artikel 11 Absatz 3 Buchstaben i und m der Richtlinie (EU) 2016/1148 in Bezug auf die Sammlung von Informationen über bewährte Verfahren bei Risiken und Sicherheitsvorfällen sowie in Bezug auf die Modalitäten für die Berichterstattung über die Meldung von Sicherheitsvorfällen gezogen werden. Hieraus könnten sich umfassende Leitlinien für quantitative Schwellenwerte für Meldungsparameter ergeben, die eine Meldepflicht von Anbietern digitaler Dienste gemäß Artikel 16 Absatz 3 der Richtlinie (EU) 2016/1148 auslösen können. Gegebenenfalls könnte die Kommission auch erwägen, die derzeit in dieser Verordnung festgelegten Schwellenwerte zu überprüfen.
- (11) Damit die zuständigen Behörden über potenzielle neue Risiken auf dem Laufenden bleiben, sollten die Anbieter digitaler Dienste dazu angehalten werden, jeglichen Sicherheitsvorfall freiwillig zu melden, der ihnen zuvor unbekannte Merkmale wie neue Exploits, Angriffsvektoren oder Angreifer, Anfälligkeiten und Gefahren aufweist.
- (12) Diese Verordnung sollte ab dem Tag gelten, der auf den Tag des Ablaufs der Frist für die Umsetzung der Richtlinie (EU) 2016/1148 folgt.
- (13) Die in dieser Verordnung vorgesehenen Maßnahmen entsprechen der Stellungnahme des gemäß Artikel 22 der Richtlinie (EU) 2016/1148 eingesetzten Ausschusses für die Sicherheit von Netz- und Informationssystemen —

HAT FOLGENDE VERORDNUNG ERLASSEN:

Artikel 1

Gegenstand

In dieser Verordnung werden die Elemente näher festgelegt, die die Anbieter digitaler Dienste zu berücksichtigen haben, wenn sie Maßnahmen ermitteln und ergreifen, die ein bestimmtes Sicherheitsniveau der Netz- und Informationssysteme gewährleisten, die sie im Rahmen der Bereitstellung der in Anhang III der Richtlinie (EU) 2016/1148 genannten Dienste nutzen; ferner werden die Parameter näher festgelegt, die bei der Feststellung zugrunde zu legen sind, ob ein Sicherheitsvorfall erhebliche Auswirkungen auf die Bereitstellung dieser Dienste hat.

Artikel 2

Sicherheitselemente

(1) Die Sicherheit der Systeme und Anlagen gemäß Artikel 16 Absatz 1 Buchstabe a der Richtlinie (EU) 2016/1148 bezeichnet die Sicherheit von Netz- und Informationssystemen und ihrer physischen Umgebung und umfasst die folgenden Elemente:

- a) das systematische Management von Netz- und Informationssystemen, d. h. eine Erfassung und Abbildung der Informationssysteme und die Einführung einer Reihe von geeigneten Maßnahmen für das Management der Informationssicherheit, einschließlich Risikoanalyse, Humanressourcen, Betriebssicherheit, Sicherheitsarchitektur, Lebenszyklus-Management gesicherter Daten und Systeme sowie gegebenenfalls Verschlüsselung und Verschlüsselungsmanagement;
- b) die physische Sicherheit und die Sicherheit der Umgebung, d. h. das Vorhandensein einer Reihe von Vorkehrungen zum Schutz der Sicherheit der Netz- und Informationssysteme von Anbietern digitaler Dienste vor Schäden anhand eines risikobasierten Allgefahrenansatzes, der beispielsweise Systemversagen, menschliche Fehler, böswillige Handlungen oder Naturereignisse berücksichtigt;
- c) die Versorgungssicherheit, d. h. die Einführung und Aufrechterhaltung geeigneter Maßnahmen zur Gewährleistung der Zugänglichkeit und gegebenenfalls der Rückverfolgbarkeit unentbehrlicher Güter oder Vorleistungen, die für die Bereitstellung der Dienste genutzt werden;
- d) die Kontrolle des Zugangs zu Netz- und Informationssystemen, d. h. das Vorhandensein einer Reihe von Vorkehrungen, die gewährleisten, dass der physische und logische Zugang zu Netz- und Informationssystemen, einschließlich der administrativen Sicherheit der Netz- und Informationssysteme, auf der Grundlage von Geschäfts- und Sicherheitsanforderungen genehmigt bzw. eingeschränkt wird.

(2) Mit Blick auf die Bewältigung von Sicherheitsvorfällen gemäß Artikel 16 Absatz 1 Buchstabe b der Richtlinie (EU) 2016/1148 umfassen die von dem Anbieter digitaler Dienste getroffenen Vorkehrungen Folgendes:

- a) Aufrechterhaltung und Erprobung von Erkennungsprozessen und -verfahren zur Gewährleistung einer rechtzeitigen und angemessenen Lageerfassung bei ungewöhnlichen Ereignissen;
- b) Prozesse und Vorgaben für die Meldung von Vorfällen und die Feststellung von Schwachstellen und Anfälligkeiten in ihren Informationssystemen;

- c) Reaktion gemäß den festgelegten Verfahren und Berichterstattung über die Ergebnisse der ergriffenen Maßnahme;
- d) Bewertung der Schwere des Sicherheitsvorfalls mit einer Dokumentierung der Erkenntnisse aus der Vorfallaanalyse und einer Sammlung relevanter Informationen, die als Nachweis dienen können und einen kontinuierlichen Verbesserungsprozess fördern.
- (3) Das Betriebskontinuitätsmanagement („*Business continuity management*“) gemäß Artikel 16 Absatz 1 Buchstabe c der Richtlinie (EU) 2016/1148 bezeichnet die Fähigkeit einer Organisation zur Aufrechterhaltung bzw. Wiederherstellung der Erbringung von Diensten auf einem zuvor festgelegten akzeptablen Niveau nach einer Störung und umfasst Folgendes:
- a) die Erstellung und Anwendung von Notfallplänen auf der Grundlage einer Analyse der betrieblichen Auswirkungen zur Gewährleistung der Kontinuität der vom Anbieter digitaler Dienste erbrachten Leistungen, die regelmäßig bewertet und erprobt werden, z. B. anhand von Übungen;
- b) Wiederherstellungskapazitäten, die regelmäßig bewertet und erprobt werden, z. B. anhand von Übungen.
- (4) Die Überwachung, Überprüfung und Erprobung gemäß Artikel 16 Absatz 1 Buchstabe d der Richtlinie (EU) 2016/1148 umfasst die Einführung und Aufrechterhaltung von Maßnahmen in folgenden Bereichen:
- a) Durchführung einer planmäßigen Abfolge von Kontrollen oder Messungen, um zu beurteilen, ob die Netz- und Informationssysteme bestimmungsgemäß funktionieren;
- b) Kontrolle und Überprüfung, um zu ermitteln, ob eine Norm oder ein Leitlinienkatalog befolgt wird, Aufzeichnungen korrekt sind und die Effizienz- und Wirksamkeitsvorgaben erfüllt werden;
- c) Prozess zur Feststellung von Mängeln in den Sicherheitsmechanismen eines Netz- und Informationssystems, die Daten schützen und Funktionen aufrechterhalten sollen. Ein solcher Prozess erstreckt sich auf die technischen Verfahren und das Personal, die in den Betriebsablauf eingebunden sind.
- (5) Internationale Normen im Sinne des Artikels 16 Absatz 1 Buchstabe e der Richtlinie (EU) 2016/1148 sind Normen, die von einer internationalen Normungsorganisation im Sinne des Artikels 2 Absatz 1 Buchstabe a der Verordnung (EU) Nr. 1025/2012 des Europäischen Parlaments und des Rates⁽¹⁾ angenommen wurden. Gemäß Artikel 19 der Richtlinie (EU) 2016/1148 können auch europäische oder international anerkannte Normen und Spezifikationen für die Sicherheit von Netz- und Informationssystemen sowie bestehende nationale Normen verwendet werden.
- (6) Anbieter digitaler Dienste müssen sicherstellen, dass sie über eine angemessene Dokumentation verfügen, anhand derer die zuständige Behörde die Einhaltung der in den Absätzen 1, 2, 3, 4 und 5 genannten Sicherheitselemente überprüfen kann.

Artikel 3

Bei der Feststellung erheblicher Auswirkungen eines Sicherheitsvorfalls zu berücksichtigende Parameter

- (1) Hinsichtlich der in Artikel 16 Absatz 4 Buchstabe a der Richtlinie (EU) 2016/1148 angesprochenen Zahl der von dem Sicherheitsvorfall betroffenen Nutzer, insbesondere der Nutzer, die den Dienst für die Bereitstellung ihrer eigenen Dienste benötigen, muss der Anbieter digitaler Dienste in der Lage sein, eine Schätzung einer der folgenden Zahlen vorzunehmen:
- a) Zahl der betroffenen natürlichen und juristischen Personen, mit denen ein Vertrag über die Bereitstellung des Dienstes abgeschlossen wurde, oder
- b) Zahl der betroffenen Nutzer, die den Dienst genutzt haben, wobei insbesondere frühere Verkehrsdaten zugrunde gelegt werden.
- (2) Die Dauer eines Sicherheitsvorfalls im Sinne des Artikels 16 Absatz 4 Buchstabe b bezeichnet die Zeitspanne von der Unterbrechung der ordnungsgemäßen Bereitstellung des Dienstes in Bezug auf Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit bis zum Zeitpunkt der Wiederherstellung.
- (3) Was die geografische Ausbreitung in Bezug auf das von dem Sicherheitsvorfall betroffene Gebiet im Sinne des Artikels 16 Absatz 4 Buchstabe c der Richtlinie (EU) 2016/1148 betrifft, muss der Anbieter digitaler Dienste in der Lage sein zu ermitteln, ob der Sicherheitsvorfall die Bereitstellung seiner Dienste in bestimmten Mitgliedstaaten beeinträchtigt.
- (4) Das Ausmaß der Unterbrechung der Bereitstellung des Dienstes im Sinne des Artikels 16 Absatz 4 Buchstabe d der Richtlinie (EU) 2016/1148 wird anhand eines oder mehrerer der folgenden Merkmale beurteilt, die durch den Sicherheitsvorfall beeinträchtigt werden: Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit der Daten oder entsprechenden Dienste.

⁽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).

(5) Was das Ausmaß der Auswirkungen auf wirtschaftliche und gesellschaftliche Tätigkeiten im Sinne des Artikels 16 Absatz 4 Buchstabe e der Richtlinie (EU) 2016/1148 anbelangt, muss der Anbieter digitaler Dienste in der Lage sein, auf der Grundlage von Angaben wie der Art der vertraglichen Beziehungen mit dem Kunden oder gegebenenfalls der potenziellen Zahl der Nutzer festzustellen, ob der Sicherheitsvorfall zu erheblichen materiellen oder immateriellen Verlusten für die Nutzer geführt hat, beispielsweise in Bezug auf die Gesundheit, die Sicherheit oder die Beschädigung von Sachen.

(6) Anbieter digitaler Dienste sind nicht verpflichtet, zu den Zwecken der Absätze 1, 2, 3, 4 und 5 zusätzliche Informationen einzuholen, die ihnen nicht zugänglich sind.

Artikel 4

Erhebliche Auswirkungen eines Sicherheitsvorfalls

(1) Ein Sicherheitsvorfall gilt als mit erheblichen Auswirkungen verbunden, wenn mindestens einer der folgenden Fälle eingetreten ist:

- a) der von einem Anbieter digitaler Dienste bereitgestellte Dienst war mehr als 5 000 000 Nutzerstunden lang nicht verfügbar, wobei sich der Begriff Nutzerstunde auf die Zahl der Nutzer in der Union bezieht, die während einer Dauer von sechzig Minuten betroffen waren;
- b) der Sicherheitsvorfall hat zu einem Verlust der Integrität, Authentizität oder Vertraulichkeit gespeicherter oder übermittelter oder verarbeiteter Daten oder der entsprechenden Dienste, die über ein Netz- und Informationssystem des Anbieters digitaler Dienste angeboten werden bzw. zugänglich sind, geführt, von dem mehr als 100 000 Nutzer in der Union betroffen sind;
- c) durch den Sicherheitsvorfall ist eine öffentliche Gefahr oder ein Risiko für die öffentliche Sicherheit entstanden oder es sind Menschen ums Leben gekommen;
- d) der Sicherheitsvorfall hat für mindestens einen Nutzer in der Union zu einem Sachschaden in Höhe von mehr als 1 000 000 EUR geführt.

(2) Auf der Grundlage der bewährten Verfahren, die die Kooperationsgruppe im Rahmen ihrer Aufgaben gemäß Artikel 11 Absatz 3 der Richtlinie (EU) 2016/1148 erarbeitet, und der Erörterungen gemäß Artikel 11 Absatz 3 Buchstabe m kann die Kommission die in Absatz 1 genannten Schwellenwerte überprüfen.

Artikel 5

Inkrafttreten

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

(2) Sie gilt ab dem 10. Mai 2018.

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

Brüssel, den 30. Januar 2018

Für die Kommission
Der Präsident
Jean-Claude JUNCKER

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 ISA²) 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 nicht-formalen 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 (ECISO) 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 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 entwickeln 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 Innovations-tätigkeiten 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 verteidigungs-bezogenen 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 Auftrags-vergabe 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 Arbeits-programms 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 Kompeten-zentrums 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 Arbeits-programms, 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 beauf-sichtigen 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 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, Kleinunternehmen, 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 kofinanziert 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 Verfassungssachen 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 Sicherheitsbewertungsverfahrens 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 Finanzhilfvereinbarungen 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 Finanzhilfvereinbarungen, 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 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 Finanzhilfvereinbarungen 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 Finanzhilfvereinbarungen, 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 Finanzhilfvereinbarung 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 Aufnahmemitgliedstaats**

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

Der Präsident

D.M. SASSOLI

Im Namen des Rates

Die Präsidentin

A.P. ZACARIAS

Table of correspondence

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

umgesetzt in:

Gesetz über Cybersicherheit (Cyber-Sicherheitsgesetz; CSG)

Inkrafttreten der Umsetzungsmassnahme: ...

Richtlinie (EU) 2016/1148:	Nationale Umsetzung (CSG):	Anmerkungen:
Artikel 1		
Art. 1 Abs. 2 Bst. a	Art. 20	
Art. 1 Abs. 2 Bst. e	Art. 12 Art. 19	
Art. 1 Abs. 3	Art. 1 Abs. 2 Bst. a und b	
Art. 1 Abs. 5	Art. 11 Abs. 2	
Art. 1 Abs. 7	Art. 4 Abs. 4 Art. 5 Abs. 6	
Artikel 4		
Art. 4 Ziff. 1	Art. 3 Abs. 1 Bst. a	
Art. 4 Ziff. 2	Art. 3 Abs. 1 Bst. b	
Art. 4 Ziff. 3	Art. 3 Abs. 1 Bst. c	
Art. 4 Ziff. 4	Art. 3 Abs. 1 Bst. e	
Art. 4 Ziff. 5	Art. 3 Abs. 1 Bst. f	
Art. 4 Ziff. 6	Art. 3 Abs. 1 Bst. g	
Art. 4 Ziff. 7	Art. 3 Abs. 1 Bst. i	
Art. 4 Ziff. 8	Art. 3 Abs. 1 Bst. k	
Art. 4 Ziff. 9	Art. 3 Abs. 1 Bst. l	
Art. 4 Ziff. 10	Art. 3 Abs. 1 Bst. h	
Art. 4 Ziff. 17	Art. 3 Abs. 1 Bst. o	
Art. 4 Ziff. 18	Art. 3 Abs. 1 Bst. p	
Art. 4 Ziff. 19	Art. 3 Abs. 1 Bst. q	
Artikel 5		

Art. 5 Abs. 1	Art. 13 Abs. 1 Bst. e	
Art. 5 Abs. 2	Art. 3 Abs. 1 Bst. d	
Art. 5 Abs. 3	Art. 13 Abs. 1 Bst. e	
Art. 5 Abs. 5	Art. 13 Abs. 1 Bst. e	
Artikel 6		
Art. 6	Art. 3 Abs. 1 Bst. d und i (Art. 5 Abs. 1)	
Artikel 7		
Art. 7 Abs. 1	Art. 20 Abs. 1	
Art. 7 Abs. 3	Art. 20 Abs. 2	
Artikel 8		
Art. 8 Abs. 1	Art. 12 Abs. 1	
Art. 8 Abs. 2	Art. 12 Abs. 1	
Art. 8 Abs. 3	Art. 12 Abs. 2	
Art. 8 Abs. 4	Art. 12 Abs. 2	
Art. 8 Abs. 6	Art. 13 Abs. 1 Bst. i	
Artikel 9		
Art. 9 Abs. 1-3	Art. 19	
Artikel 11		
Art. 11 Abs. 2	Art. 13 Abs. 1 Bst. k	
Artikel 12		
Art. 12 Abs. 2	Art. 13 Abs. 1 Bst. k	
Artikel 14		
Art. 14 Abs. 1	Art. 4 Abs. 1 und 2 Art. 13 Abs. 1 Bst. a Art. 18	
Art. 14 Abs. 2	Art. 4 Abs. 3 Art. 13 Abs. 1 Bst. a Art. 18	
Art. 14 Abs. 3	Art. 5 Abs. 1 und 2	
Art. 14 Abs. 4	Art. 3 Abs. 1 Bst. d und i Art. 5 Abs 1 und 2	

Art. 14 Abs. 5 UAbs. 1 Satz 1	Art. 13 Abs. 1 Bst. f	
Art. 14 Abs. 5 UAbs. 1 Satz 2	Art. 11 Abs. 2 und Art. 10	
Art. 14 Abs. 5 UAbs. 2	Art. 19 Abs. 1 Bst. a	
Art. 14 Abs. 5 UAbs. 3	Art. 13 Abs. 1 Bst. k und l	
Art. 14 Abs. 6	Art. 5 Abs. 5	
Artikel 15		
Art. 15 Abs. 1	Art. 13 Abs. 1 Bst. a Art. 14 Art. 18	
Art. 15 Abs. 2	Art. 13 Art. 14 Abs. 1 Art. 18	
Art. 15 Abs. 3	Art. 16 und Art. 21	
Art. 15 Abs. 4	Art. 13 Abs. 1 Bst. i	
Artikel 16		
Art. 16 Abs. 1	Art. 6 Art. 13 Abs. 1 Bst. a Art. 18	
Art. 16 Abs. 2	Art. 6 Art. 13 Abs. 1 Bst. a und d Art. 15 Art. 18	
Art. 16 Abs. 3	Art. 7 Abs. 1 Art. 13 Abs. 1 Bst. f Art. 15 Art. 19	
Art. 16 Abs. 4	Art. 7 Abs. 1	
Art. 16 Abs. 5	Art. 5 Abs. 4	
Art. 16 Abs. 6	Art. 13 Abs. 1 Bst. f Art. 11 Abs. 2	
Art. 16 Abs. 7	Art. 7 Abs. 2	
Art. 16 Abs. 11	Art. 3 Abs. 1 Bst. g	

Artikel 17		
Art. 17 Abs. 1	Art. 15	
Art. 17 Abs. 2 Bst. a	Art. 15	
Art. 17 Abs. 2 Bst. b	Art. 22 Abs. 1 Bst. c, d, h, i und k	
Art. 17 Abs. 3	Art. 13 Abs. 1 Bst. k	
Artikel 18		
Art. 18 Abs. 1	Art. 3 Abs. 1 Bst. g	
Art. 18 Abs. 2	Art. 3 Abs. 1 Bst. g iVm Ziff. h	
Artikel 20		
Art. 20 Abs. 1	Art. 8	
Art. 20 Abs. 2 UAbs. 1	Art. 8	
Art. 20 Abs. 2 UAbs. 2	Art. 8 Abs. 2	
Artikel 21		
Art. 21	Art. 22	
Artikel 25		
Art. 25 Abs. 1 UAbs. 3	Art. 2 Abs. 2	