Liechtensteinisches Landesgesetzblatt
Jahrgang 2024 **Nr. ...** **ausgegeben am ... 2024**

Cyber-Sicherheitsgesetz (CSG)

vom 5. Dezember 2024

Dem nachstehenden vom Landtag gefassten Beschluss erteile Ich Meine Zustimmung:[1]

I. Allgemeine Bestimmungen

Art. 1

Gegenstand und Geltungsbereich

1) Dieses Gesetz legt die Massnahmen fest, mit denen ein hohes Cybersicherheitsniveau der öffentlichen und privaten Einrichtungen nach den Anhängen 1 und 2 erreicht werden soll, die:

a) nach Art. 1064 Abs. 2 oder 3 des Personen- und Gesellschaftsrechts als mittelgrosse oder grosse Gesellschaften gelten; und

b) ihre Dienste oder Tätigkeiten in Liechtenstein erbringen bzw. ausüben.

2) Es gilt zudem, unabhängig der Grösse der Einrichtungen, für:

a) Einrichtungen nach den Anhängen 1 und 2, wenn:

1. die Dienste erbracht werden von:

aa) Anbietern von öffentlichen elektronischen Kommunikationsnetzen oder von öffentlich zugänglichen elektronischen Kommunikationsdiensten;

bb) Vertrauensdiensteanbietern;

cc) Namenregistern der Domäne der ersten Ebene (TLD-Namenregistern) und DNS-Diensteanbietern;

1 Bericht und Antrag sowie Stellungnahme der Regierung Nr. 93/2024 und 133/2024

2. es sich bei der Einrichtung um den einzigen Anbieter handelt, der einen Dienst erbringt, der für die Aufrechterhaltung kritischer gesellschaftlicher oder wirtschaftlicher Tätigkeiten unerlässlich ist;
3. sich eine Störung des von der Einrichtung erbrachten Dienstes wesentlich auf die öffentliche Ordnung, die öffentliche Sicherheit oder die öffentliche Gesundheit auswirken könnte;
4. eine Störung des von der Einrichtung erbrachten Dienstes zu einem wesentlichen Systemrisiko führen könnte, insbesondere in Sektoren, in denen eine solche Störung grenzübergreifende Auswirkungen haben könnte;
5. die Einrichtung aufgrund der besonderen Bedeutung, die sie auf nationaler oder regionaler Ebene für den betreffenden Sektor, die betreffende Art des Dienstes oder für andere voneinander abhängige Sektoren hat, kritisch ist; oder
6. die Einrichtung eine Einrichtung der öffentlichen Verwaltung des Landes ist;

b) Einrichtungen:

1. die nach der Richtlinie (EU) 2022/2557[2] als kritische Einrichtungen eingestuft wurden;
2. die Domänennamen-Registrierungsdienste erbringen.

3) Die in diesem Gesetz vorgesehenen Risikomanagementmassnahmen und Berichtspflichten nach Art. 4 und 6 gelten nicht für Einrichtungen der öffentlichen Verwaltung des Landes, die ihre Tätigkeiten in den Bereichen nationale Sicherheit, öffentliche Sicherheit, Verteidigung oder Strafverfolgung ausüben, einschliesslich der Verhütung, Ermittlung, Aufdeckung und Verfolgung von Straftaten.

Art. 2

Umsetzung und Durchführung von EWR-Rechtsvorschriften

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

2 Richtlinie (EU) 2022/2557 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über die Resilienz kritischer Einrichtungen und zur Aufhebung der Richtlinie 2008/114/EG des Rates (ABl. L 333 vom 27.12.2022, S. 164)

a) Richtlinie (EU) 2022/2555 über Massnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union[3];

b) Verordnung (EU) 2021/887 zur Einrichtung des Europäischen Kompetenzzentrums für Industrie, Technologie und Forschung im Bereich der Cybersicherheit und des Netzwerks nationaler Koordinierungszentren[4];

c) Verordnung (EU) 2019/881 über die ENISA (Agentur der Europäischen Union für Cybersicherheit) und über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik[5].

2) 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.

Art. 3

Begriffsbestimmungen und Bezeichnungen

1) Im Sinne dieses Gesetzes gelten als:

1. "Netz- und Informationssystem":
   a) ein elektronisches Kommunikationsnetz nach Art. 3 Abs. 1 Ziff. 5 des Kommunikationsgesetzes;
   b) ein Gerät oder eine Gruppe miteinander verbundener oder zusammenhängender Geräte, die einzeln oder zu mehreren auf der Grundlage eines Programms die automatische Verarbeitung digitaler Daten durchführen; oder

---

3 Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Massnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS-2-Richtlinie) (ABl. L 333 vom 27.12.2022, S. 80)

4 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)

5 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)

c) digitale Daten, die von den in Bst. 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 Ereignisse abzuwehren, die die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit gespeicherter, übermittelter oder verarbeiteter Daten oder der Dienste, die über diese Netz- und Informationssysteme angeboten werden bzw. zugänglich sind, beeinträchtigen können;
3. "Cybersicherheit": alle Tätigkeiten, die notwendig sind, um Netz- und Informationssysteme, die Nutzer solcher Systeme und andere von Cyberbedrohungen betroffene Personen zu schützen;
4. "NIS-Strategie" (Nationale Cybersicherheitsstrategie): ein kohärenter Rahmen mit strategischen Zielen und Prioritäten im Bereich der Cybersicherheit und der zu ihrer Verwirklichung erforderlichen Governance;
5. "Beinahe-Vorfall": jedes Ereignis, das die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit gespeicherter, übermittelter oder verarbeiteter Daten oder der Dienste, die über Netz- und Informationssysteme angeboten werden oder zugänglich sind, beeinträchtigt haben könnte, dessen Eintritt jedoch erfolgreich verhindert wurde oder das nicht eingetreten ist;
6. "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;
7. "erheblicher Sicherheitsvorfall": ein Sicherheitsvorfall, wenn er:
   a) schwerwiegende Betriebsstörungen der Dienste oder finanzielle Verluste für die betreffende Einrichtung verursacht hat oder verursachen kann;
   b) andere natürliche oder juristische Personen durch erhebliche materielle oder immaterielle Schäden beeinträchtigt hat oder beeinträchtigen kann;
8. "Cybersicherheitsvorfall grossen Ausmasses": ein Sicherheitsvorfall, der eine Störung verursacht, deren Ausmass die Reaktionsfähigkeit eines EWR-Mitgliedstaats übersteigt, oder der beträchtliche Auswirkungen auf mindestens zwei EWR-Mitgliedstaaten hat;

9. "Bewältigung von Sicherheitsvorfällen": alle Massnahmen und Verfahren zur Verhütung, Erkennung, Analyse und Eindämmung von Sicherheitsvorfällen oder die Reaktion darauf und die Erholung davon;
10. "Risiko": das Potenzial für Verluste oder Störungen, die durch einen Sicherheitsvorfall verursacht werden, das als eine Kombination des Ausmasses eines solchen Verlusts oder einer solchen Störung und der Wahrscheinlichkeit des Eintretens des Sicherheitsvorfalls zum Ausdruck gebracht wird;
11. "Cyberbedrohung": ein möglicher 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. "erhebliche Cyberbedrohung": eine Cyberbedrohung, die das Potenzial besitzt, die Netz- und Informationssysteme einer Einrichtung oder der Nutzer solcher Systeme aufgrund ihrer technischen Merkmale erheblich zu beeinträchtigen, indem sie erheblichen materiellen oder immateriellen Schaden verursacht;
13. "IKT-Produkt": ein Element oder eine Gruppe von Elementen eines Netz- oder Informationssystems;
14. "IKT-Dienst": ein Dienst, der vollständig oder überwiegend aus der Übertragung, Speicherung, Abfrage oder Verarbeitung von Informationen mittels Netz- und Informationssystemen besteht;
15. "IKT-Prozess": jegliche Tätigkeiten, mit denen ein IKT-Produkt oder -Dienst konzipiert, entwickelt, bereitgestellt oder gepflegt werden soll;
16. "Schwachstelle": eine Schwäche, Anfälligkeit oder Fehlfunktion von IKT-Produkten oder IKT-Diensten, die bei einer Cyberbedrohung ausgenutzt werden kann;
17. "Norm": eine Norm nach Art. 2 Ziff. 1 der Verordnung (EU) Nr. 1025/2012[6];
18. "technische Spezifikation": eine technische Spezifikation nach Art. 2 Ziff. 4 der Verordnung (EU) Nr. 1025/2012;

---

6 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)

19. "Internet-Knoten": eine Netzeinrichtung, die die Zusammenschaltung von mehr als zwei unabhängigen Netzen (autonomen Systemen) ermöglicht, in erster Linie zur Erleichterung des Austauschs von Internet-Datenverkehr, der nur der Zusammenschaltung autonomer Systeme dient und weder voraussetzt, dass der Internet-Datenverkehr zwischen zwei beliebigen teilnehmenden autonomen Systemen über ein drittes autonomes System läuft; noch den betreffenden Datenverkehr verändert oder anderweitig beeinträchtigt;
20. "DNS-Diensteanbieter": eine Einrichtung, die:
    a) für Internet-Endnutzer öffentlich verfügbare rekursive Dienste zur Auflösung von Domänennamen anbietet; oder
    b) autoritative Dienste zur Auflösung von Domänennamen zur Nutzung durch Dritte, mit Ausnahme von Root-Namenservern, anbietet;
21. "Namenregister der Domäne der ersten Ebene" oder "TLD-Namenregister": eine Einrichtung, der eine bestimmte Domäne der ersten Ebene (Top Level Domain, TLD) übertragen wurde und die für die Verwaltung der TLD, einschliesslich der Registrierung von Domänennamen unterhalb der TLD, sowie für den technischen Betrieb der TLD, einschliesslich des Betriebs ihrer Namenserver, der Pflege ihrer Datenbanken und der Verteilung von TLD-Zonendateien über die Namenserver, zuständig ist, unabhängig davon, ob der Betrieb durch die Einrichtung selbst erfolgt oder ausgelagert wird, jedoch mit Ausnahme von Situationen, in denen TLD-Namen von einem Register nur für seine eigenen Zwecke verwendet werden;
22. "Einrichtung, die Domänennamen-Registrierungsdienste erbringt": ein Registrar oder eine Stelle, die im Namen von Registraren tätig ist, wie etwa ein Anbieter oder Wiederverkäufer von Datenschutz- oder Proxy-Registrierungsdiensten;
23. "digitaler Dienst": ein Dienst nach Art. 3 Abs. 1 Bst. e des EWR-Notifikationsgesetzes;
24. "Vertrauensdienst": ein Vertrauensdienst nach Art. 3 Ziff. 16 der Verordnung (EU) Nr. 910/2014[7];
25. "Vertrauensdiensteanbieter": ein Vertrauensdiensteanbieter nach Art. 3 Ziff. 19 der Verordnung (EU) Nr. 910/2014;

---

7 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)

26. "qualifizierter Vertrauensdienst": ein qualifizierter Vertrauensdienst nach Art. 3 Ziff. 17 der Verordnung (EU) Nr. 910/2014;
27. "qualifizierter Vertrauensdiensteanbieter": ein qualifizierter Vertrauensdiensteanbieter nach Art. 3 Ziff. 20 der Verordnung (EU) Nr. 910/2014;
28. "Online-Marktplatz": ein Dienst, der es Verbrauchern durch die Verwendung von Software, einschliesslich einer Internetseite, eines Teils einer Internetseite oder einer Anwendung, die vom oder im Namen des Gewerbetreibenden betrieben wird, ermöglicht, Fernabsatzverträge mit anderen Gewerbetreibenden oder Verbrauchern, abzuschliessen;
29. "Online-Suchmaschine": ein digitaler Dienst, der es Nutzern ermöglicht, in Form eines Stichworts, einer Spracheingabe, einer Wortgruppe oder einer anderen Eingabe Anfragen einzugeben, um prinzipiell auf allen Internetseiten oder auf allen Internetseiten in einer bestimmten Sprache eine Suche zu einem beliebigen Thema vorzunehmen und Ergebnisse in einem beliebigen Format angezeigt zu bekommen, über die sie Informationen im Zusammenhang mit dem angeforderten Inhalt finden können;
30. "Cloud-Computing-Dienst": ein digitaler Dienst, der auf Abruf die Verwaltung und den umfassenden Fernzugang zu einem skalierbaren und elastischen Pool gemeinsam nutzbarer Rechenressourcen ermöglicht, auch wenn diese Ressourcen auf mehrere Standorte verteilt sind;
31. "Rechenzentrumsdienst": ein Dienst, mit dem spezielle Strukturen oder Gruppen von Strukturen für die zentrale Unterbringung, die Verbindung und den Betrieb von IT- und Netzausrüstungen zur Erbringung von Datenspeicher-, Datenverarbeitungs- und Datentransportdiensten sowie alle Anlagen und Infrastrukturen für die Leistungsverteilung und die Umgebungskontrolle bereitgestellt werden;
32. "Inhaltszustellnetz": ein Netz dezentraler Server zur Gewährleistung einer hohen Verfügbarkeit, Zugänglichkeit oder schnellen Zustellung digitaler Inhalte und Dienste für Internetnutzer im Auftrag von Inhalte- und Diensteanbietern;
33. "Plattform für Dienste sozialer Netzwerke": eine Plattform, auf der Endnutzer mit unterschiedlichen Geräten insbesondere durch Chats, Posts, Videos und Empfehlungen miteinander in Kontakt treten und kommunizieren sowie Inhalte teilen und entdecken können;
34. "Vertreter": eine im EWR niedergelassene natürliche oder juristische Person, die ausdrücklich benannt wurde, um im Auftrag eines DNS-Diensteanbieters, einer Einrichtung, die Domänennamen-Registrierungsdienste erbringt, eines TLD-Namenregisters, eines Anbieters von Cloud-Computing-Diensten, eines Anbieters von Rechenzentrumsdiensten, eines Betreibers von Inhaltszustellnetzen, eines Anbieters

verwalteter Dienste, eines Anbieters verwalteter Sicherheitsdienste oder eines Anbieters von einem Online-Marktplatz, von einer Online-Suchmaschine oder von einer Plattform für Dienste sozialer Netzwerke, der bzw. die nicht im EWR niedergelassen ist, zu handeln, und an die sich eine nationale zuständige Behörde oder ein CSIRT - statt an die Einrichtung - hinsichtlich der Pflichten dieser Einrichtung gemäss dieses Gesetzes wenden kann;

35. "öffentliches elektronisches Kommunikationsnetz": ein öffentliches elektronisches Kommunikationsnetz nach Art. 3 Abs. 1 Ziff. 16 des Kommunikationsgesetzes;
36. "elektronischer Kommunikationsdienst": ein elektronischer Kommunikationsdienst nach Art. 3 Abs. 1 Ziff. 9 des Kommunikationsgesetzes;
37. "Einrichtung": eine natürliche Person oder nach dem an ihrem Sitz geltenden nationalen Recht geschaffene und anerkannte juristische Person, die in eigenem Namen Rechte ausüben und Pflichten unterliegen kann;
38. "Anbieter verwalteter Dienste": eine Einrichtung, die Dienste im Zusammenhang mit der Installation, der Verwaltung, dem Betrieb oder der Wartung von IKT-Produkten, Netzen, Infrastruktur, Anwendungen oder jeglicher anderer Netz- und Informationssysteme durch Unterstützung oder aktive Verwaltung erbringt, die entweder in den Räumlichkeiten der Kunden oder aus der Ferne erbringt;
39. "Anbieter verwalteter Sicherheitsdienste": ein Anbieter verwalteter Dienste, der Unterstützung für Tätigkeiten im Zusammenhang mit dem Risikomanagement im Bereich der Cybersicherheit durchführt oder erbringt;
40. "Forschungseinrichtung": eine Einrichtung, deren primäres Ziel es ist, angewandte Forschung oder experimentelle Entwicklung im Hinblick auf die Nutzung der Ergebnisse dieser Forschung für kommerzielle Zwecke durchzuführen, die jedoch Bildungseinrichtungen nicht einschliesst;
41. "Kooperationsgruppe": ein nach Art. 14 der Richtlinie (EU) 2022/2555 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 Cybersicherheitsniveaus im EWR dient;

42. "CSIRTs-Netzwerk": ein nach Art. 15 der Richtlinie (EU) 2022/2555 eingerichtetes Gremium, das sich aus Vertretern der Computer-Notfallteams der EWR-Mitgliedstaaten und des IT-Notfallteams für die Organe, Einrichtungen und sonstigen Stellen der Europäischen Union (CERT-EU) zusammensetzt und zum Aufbau von Vertrauen zwischen den EWR-Mitgliedstaaten beitragen sowie eine rasche und wirksame operative Zusammenarbeit fördern soll;
43. "EU-CyCLONe" (European Cyber Crises Liaison Organisation Network): ein nach Art. 16 der Richtlinie (EU) 2022/2555 eingerichtetes Gremium, das sich aus Vertretern der Behörden für das Cyberkrisenmanagement der EWR-Mitgliedstaaten und der Europäischen Kommission zusammensetzt und bei der koordinierten Bewältigung von Cybersicherheitsvorfällen grossen Ausmasses und Krisen auf operativer Ebene sowie bei der Gewährleistung eines regelmässigen Austauschs relevanter Informationen zwischen den EWR-Mitgliedstaaten und den Organen, Einrichtungen und sonstigen Stellen unterstützen soll.

2) Im Sinne dieses Gesetzes gelten zudem als:

a) wesentliche Einrichtungen:
   1. Einrichtungen nach Anhang 1, die die in Art. 1064 Abs. 2 des Personen- und Gesellschaftsrechts genannten Schwellenwerte für mittelgrosse Gesellschaften überschreiten;
   2. qualifizierte Vertrauensdiensteanbieter und TLD-Namenregister sowie DNS-Diensteanbieter, unabhängig von ihrer Grösse;
   3. Anbieter öffentlicher elektronischer Kommunikationsnetze oder öffentlich zugänglicher elektronischer Kommunikationsdienste, die nach Art. 1064 Abs. 2 des Personen- und Gesellschaftsrechts als mittelgrosse Gesellschaften gelten;
   4. Einrichtungen der öffentlichen Verwaltung des Landes;
   5. sonstige Einrichtungen nach Anhang 1 oder 2, die von der Regierung mit Verordnung nach Massgabe der Kriterien von Art. 1 Abs. 2 Bst. a Ziff. 2 bis 6 als wesentliche Einrichtungen eingestuft werden;
   6. Einrichtungen, die gemäss der Richtlinie (EU) 2022/2557 als kritische Einrichtungen eingestuft wurden;
b) wichtige Einrichtungen:
   1. Einrichtungen nach Anhang 1 oder 2, die nicht als wesentliche Einrichtungen nach Abs. 2 gelten;
   2. sonstige Einrichtungen nach Anhang 1 oder 2, die von der Regierung mit Verordnung nach Massgabe der Kriterien von Art. 1 Abs. 2 Bst. a Ziff. 2 bis 6 als wichtige Einrichtungen eingestuft wurden.

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

II. Risikomanagement-, Berichts-, Registrierungs- und Informationspflichten

A. Wesentliche und wichtige Einrichtungen

Art. 4

Risikomanagementmassnahmen

1) Wesentliche und wichtige Einrichtungen ergreifen geeignete und verhältnismässige technische, operative und organisatorische Massnahmen, um die Risiken für die Sicherheit der Netz- und Informationssysteme, die sie für ihren Betrieb oder für die Erbringung ihrer Dienste nutzen, zu beherrschen und die Auswirkungen von Sicherheitsvorfällen auf die Empfänger ihrer Dienste und auf andere Dienste zu verhindern oder möglichst gering zu halten.

2) Die Massnahmen nach Abs. 1 müssen unter Berücksichtigung des Stands der Technik und gegebenenfalls der einschlägigen europäischen und internationalen Normen sowie der Kosten der Umsetzung ein Sicherheitsniveau der Netz- und Informationssysteme gewährleisten, welches dem bestehenden Risiko angemessen ist. Bei der Bewertung der Verhältnismässigkeit dieser Massnahmen sind gebührend zu berücksichtigen:

a) das Ausmass der Risikoexposition der Einrichtung;

b) die Grösse der Einrichtung; und

c) die Wahrscheinlichkeit des Eintretens von Sicherheitsvorfällen und deren Schwere, einschliesslich ihrer gesellschaftlichen und wirtschaftlichen Auswirkungen.

3) Die Massnahmen nach Abs. 1 müssen auf einem gefahrenübergreifenden Ansatz beruhen, der darauf abzielt, die Netz- und Informationssysteme und die physische Umwelt dieser Systeme vor Sicherheitsvorfällen zu schützen, und zumindest Folgendes umfassen:

a) Konzepte in Bezug auf die Risikoanalyse und Sicherheit für Informationssysteme;

b) Bewältigung von Sicherheitsvorfällen;

c) Aufrechterhaltung des Betriebs, wie Backup-Management und Wiederherstellung nach einem Notfall, und Krisenmanagement;

d) Sicherheit der Lieferkette, einschliesslich sicherheitsbezogener Aspekte der Beziehungen zwischen den einzelnen Einrichtungen und ihren unmittelbaren Anbietern oder Diensteanbietern;

e) Sicherheitsmassnahmen bei Erwerb, Entwicklung und Wartung von Netz- und Informationssystemen, einschliesslich Management und Offenlegung von Schwachstellen;

f) Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmassnahmen im Bereich der Cybersicherheit;

g) grundlegende Verfahren im Bereich der Cyberhygiene und Schulungen im Bereich der Cybersicherheit;

h) Konzepte und Verfahren für den Einsatz von Kryptografie und gegebenenfalls Verschlüsselung;

i) Sicherheit des Personals, Konzepte für die Zugriffskontrolle und Management von Anlagen;

k) Verwendung von Lösungen zur Multi-Faktor-Authentifizierung oder kontinuierlichen Authentifizierung, gesicherte Sprach-, Video- und Textkommunikation sowie gegebenenfalls gesicherte Notfallkommunikationssysteme innerhalb der Einrichtung.

4) Die Einrichtungen berücksichtigen bei der Erwägung geeigneter Massnahmen nach Abs. 3 Bst. d bei den einzelnen unmittelbaren Anbietern und Diensteanbietern:

a) die spezifischen Schwachstellen;

b) die Gesamtqualität der Produkte;

c) die Cybersicherheitspraxis, einschliesslich die Sicherheit der Entwicklungsprozesse.

5) Stellt eine Einrichtung fest, dass sie den Massnahmen nach Abs. 3 nicht nachkommt, ergreift sie unverzüglich alle erforderlichen, angemessenen und verhältnismässigen Korrekturmassnahmen.

6) Die Pflichten nach diesem Artikel finden keine Anwendung, wenn spezialgesetzliche Bestimmungen über Risikomanagementmassnahmen bestehen, die zumindest ein gleichwertiges Cybersicherheitsniveau vorsehen.

7) Die Regierung kann das Nähere über die Risikomanagementmassnahmen mit Verordnung regeln.

Art. 5

Besondere Verantwortlichkeit der Leitungsorgane und der vertretungsbefugten Personen

1) Leitungsorgane wesentlicher und wichtiger Einrichtungen sind verpflichtet:

a) die von diesen Einrichtungen zur Einhaltung von Art. 4 ergriffenen Risikomanagementmassnahmen im Bereich der Cybersicherheit zu billigen und ihre Umsetzung zu überwachen;

b) an Schulungen teilzunehmen und allen Mitarbeitern regelmässig entsprechende Schulungen anzubieten, um ausreichende Kenntnisse und Fähigkeiten zur Erkennung und Bewertung von Risiken sowie Managementpraktiken im Bereich der Cybersicherheit und deren Auswirkungen auf die von der Einrichtung erbrachten Dienste zu erwerben.

2) Natürliche Personen, die für eine wesentliche Einrichtung verantwortlich sind oder auf der Grundlage ihrer Vertretungsbefugnis, der Befugnis, im Namen der Einrichtung Entscheidungen zu treffen, oder ihrer Kontrollbefugnis über die Einrichtung als Vertreter der wesentlichen Einrichtung handeln, haben zu gewährleisten, dass die Einrichtung die Bestimmungen dieses Gesetzes erfüllt.

Art. 6

Berichtspflichten

1) Wesentliche und wichtige Einrichtungen haben erhebliche Sicherheitsvorfälle der Stabsstelle Cyber-Sicherheit unverzüglich zu melden.

2) Für die Zwecke der Meldung nach Abs. 1 haben die betroffenen Einrichtungen der Stabsstelle Cyber-Sicherheit Folgendes zu übermitteln:

a) unverzüglich, in jedem Fall aber innerhalb von 24 Stunden nach Kenntnisnahme des erheblichen Sicherheitsvorfalls, eine Frühwarnung, in der gegebenenfalls angegeben wird, ob der Verdacht besteht, dass der erhebliche Sicherheitsvorfall auf rechtswidrige oder böswillige Handlungen zurückzuführen ist oder grenzüberschreitende Auswirkungen haben könnte;

b) unverzüglich, in jedem Fall aber innerhalb von 72 Stunden nach Kenntnisnahme des erheblichen Sicherheitsvorfalls, eine Meldung über den Sicherheitsvorfall, in der gegebenenfalls die unter Bst. a genannten Informationen aktualisiert werden und eine erste Bewertung des erheblichen Sicherheitsvorfalls, einschliesslich seines Schweregrads und seiner

Auswirkungen, sowie gegebenenfalls die Kompromittierungsindikatoren angegeben werden;

c) auf Ersuchen der Stabsstelle Cyber-Sicherheit einen Zwischenbericht über relevante Statusaktualisierungen;

d) spätestens einen Monat nach Übermittlung der Meldung des Sicherheitsvorfalls nach Bst. b einen Abschlussbericht, der insbesondere Folgendes enthält:

   1. eine ausführliche Beschreibung des Sicherheitsvorfalls, einschliesslich seines Schweregrads und seiner Auswirkungen;
   2. Angaben zur Art der Bedrohung bzw. der dieser zugrunde liegenden Ursache, die wahrscheinlich den Sicherheitsvorfall ausgelöst hat;
   3. Angaben zu den getroffenen und laufenden Abhilfemassnahmen;
   4. gegebenenfalls die grenzüberschreitenden Auswirkungen des Sicherheitsvorfalls;

e) im Falle eines andauernden Sicherheitsvorfalls zum Zeitpunkt der Vorlage des Abschlussberichts nach Bst. d einen Fortschrittsbericht und einen Abschlussbericht innerhalb eines Monats nach Behandlung des Sicherheitsvorfalls.

3) Wesentliche und wichtige Einrichtungen informieren gegebenenfalls jene Empfänger ihrer Dienste unverzüglich über den erheblichen Sicherheitsvorfall, die die Erbringung des jeweiligen Dienstes beeinträchtigen könnten, und teilen ihnen unverzüglich Massnahmen oder Abhilfemassnahmen mit, die diese Empfänger als Reaktion auf diese Bedrohung ergreifen können.

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

5) Die Pflichten nach Abs. 1 bis 3 finden keine Anwendung, wenn spezialgesetzliche Bestimmungen über eine Meldepflicht bestehen und die Kriterien für diese Meldepflicht mindestens gleichwertig sind. In diesen Fällen haben die Meldungsempfänger die bei ihnen eingegangenen Meldungen unverzüglich an die Stabsstelle Cyber-Sicherheit weiterzuleiten.

6) Die Regierung kann das Nähere über die Berichtspflicht für wesentliche und wichtige Einrichtungen mit Verordnung regeln.

Art. 7

Registrierungspflicht

1) Wesentliche und wichtige Einrichtungen übermitteln der Stabsstelle Cyber-Sicherheit zwecks Registrierung unverzüglich folgende Angaben:

a) den Namen der Einrichtung;

b) den Sektor, Teilsektor und die Art der Einrichtung nach Anhang 1 oder 2;

c) die Anschrift der Hauptniederlassung der Einrichtung und ihrer sonstigen Niederlassungen im EWR oder, falls sie nicht im EWR niedergelassen ist, die Anschrift ihres Vertreters oder Zustellungsbevollmächtigten;

d) die aktuellen Kontaktdaten, einschliesslich E-Mail-Adressen und Telefonnummern der Einrichtung und gegebenenfalls ihres Vertreters;

e) die EWR-Mitgliedstaaten, in denen die Einrichtung Dienste erbringt;

f) die IP-Adressbereiche der Einrichtung.

2) Sie informieren die Stabsstelle Cyber-Sicherheit unverzüglich über jede Änderung der Angaben nach Abs. 1, in jedem Fall aber innerhalb von zwei Wochen ab dem Tag der Änderung.

Art. 8

Information der Öffentlichkeit

Nach Eingang einer Meldung nach Art. 6 Abs. 2 Bst. b und nach Anhörung der betreffenden Einrichtung kann die Stabsstelle Cyber-Sicherheit die Öffentlichkeit über konkrete Sicherheitsvorfälle informieren oder verlangen, dass die Einrichtung 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.

B. Andere Einrichtungen

Art. 9

Freiwillige Meldung

1) Jede Einrichtung kann Sicherheitsvorfälle, Cyberbedrohungen oder Beinahe-Vorfälle der Stabsstelle Cyber-Sicherheit melden.

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

Art. 10

Informationsaustausch

1) Jede Einrichtung kann auf freiwilliger Basis Informationen betreffend die Cybersicherheit, einschliesslich personenbezogener Daten, untereinander austauschen, insbesondere über:

a) Cyberbedrohungen;
b) Schwachstellen;
c) Taktiken, Techniken und Verfahren;
d) Kompromittierungsindikatoren;
e) Empfehlungen für die Konfiguration von Cybersicherheitsinstrumenten zur Aufdeckung von Cyberangriffen;
f) Beinahe-Vorfälle.

2) Der Informationsaustausch nach Abs. 1 ist zulässig, sofern:

a) der Informationsaustausch darauf abzielt, Sicherheitsvorfälle zu verhindern, aufzudecken, darauf zu reagieren oder sich von ihnen zu erholen oder ihre Folgen einzudämmen;
b) durch diesen Informationsaustausch das Cybersicherheitsniveau erhöht wird, insbesondere indem:
   1. Aufklärungsarbeit über Cyberbedrohungen geleistet wird;
   2. die Fähigkeit solcher Bedrohungen, sich zu verbreiten eingedämmt bzw. verhindert wird;
   3. Abwehrkapazitäten, die Beseitigung und Offenlegung von Schwachstellen, Techniken zur Erkennung, Eindämmung und Verhütung von Bedrohungen, Eindämmungsstrategien, Reaktions- und Wiederherstellungsphasen unterstützt werden; oder

4. die gemeinsame Forschung im Bereich Cyberbedrohung zwischen öffentlichen und privaten Einrichtungen gefördert wird.

III. Organisation und Durchführung

A. Allgemeines

Art. 11

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. 12

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. 16 bleibt vorbehalten.

Art. 13

Verarbeitung und Offenlegung personenbezogener Daten

1) Die Stabsstelle Cyber-Sicherheit ist berechtigt, personenbezogene Daten, einschliesslich besonderer Kategorien personenbezogener Daten, zu verarbeiten oder verarbeiten zu lassen, soweit dies zur Erfüllung ihrer Aufgaben nach diesem Gesetz erforderlich ist.

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

a) dies zur Erfüllung ihrer Aufgaben nach diesem Gesetz oder der Richtlinie (EU) 2022/2555 erforderlich ist;

b) die Vertraulichkeit der Daten gewährleistet ist; sowie

c) die Sicherheit und die geschäftlichen Interessen der wesentlichen und wichtigen Einrichtungen geschützt sind.

3) Bei Übermittlungen personenbezogener Daten an Drittstaaten oder internationale Organisationen hat die Stabsstelle Cyber-Sicherheit neben den Anforderungen nach Abs. 2 zusätzlich die datenschutzrechtlichen Voraussetzungen nach Kapitel V der Verordnung (EU) 2016/679[8] entsprechend zu berücksichtigen.

B. Stabsstelle Cyber-Sicherheit

Art. 14

Zuständigkeit

Die Stabsstelle Cyber-Sicherheit gilt als:

a) national zuständige Behörde für Cybersicherheit nach Art. 8 Abs. 1 der Richtlinie (EU) 2022/2555; ihr obliegt die Aufsicht und der Vollzug dieses Gesetzes;

b) zentrale Anlaufstelle für Cybersicherheit nach Art. 8 Abs. 3 der Richtlinie (EU) 2022/2555; 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;

c) zuständige Behörde für das Management von Cybersicherheitsvorfällen grossen Ausmasses und Krisen nach Art. 9 Abs. 1 der Richtlinie (EU) 2022/2555;

8 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)

d) zuständige Behörde für Cybersicherheitszertifizierungen nach Art. 58 Abs. 1 der Verordnung (EU) 2019/881; sie nimmt die Aufgaben und Befugnisse nach Art. 58 Abs. 7 und 8 der genannten Verordnung wahr.

Art. 15

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 Risikomanagementmassnahmen nach Art. 4 sowie die Einhaltung der Berichtspflichten nach Art. 6;

b) die Einrichtung und Koordination des CSIRT nach Art. 20;

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 Cybersicherheit oder zur Vorbeugung von Sicherheitsvorfällen;

e) die Führung eines Registers mit Daten zu den wesentlichen und wichtigen Einrichtungen und zu Einrichtungen, die Domänennamen-Registrierungsdienste erbringen, sowie die regelmässige, mindestens jedoch einmal alle zwei Jahre, Überprüfung und Aktualisierung der Registerinhalte;

f) die Entgegennahme von Nennungen und das Führen einer Liste der Vertreter nach Art. 3 Abs. 1 Ziff. 34;

g) die Förderung der Anwendung europäischer und internationaler Normen und technischer Spezifikationen für die Sicherheit von Netz- und Informationssystemen;

h) die Unterrichtung und Weiterleitung von durch wesentliche und wichtige Einrichtungen bereitgestellten Informationen an die zentrale Anlaufstelle der betroffenen EWR-Mitgliedstaaten, wenn ein Sicherheitsvorfall eine grenzüberschreitende Auswirkung in diesen EWR-Mitgliedstaaten hat;

i) die Koordination und die Förderung der öffentlich-privaten Zusammenarbeit im Bereich der Cybersicherheit;

k) 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 Cybersicherheit;

l) die Zusammenarbeit und der Informationsaustausch mit anderen inländischen Behörden und Stellen, insbesondere der Landespolizei, der Staatsanwaltschaft, der Datenschutzstelle, dem Amt für Informatik, dem Amt für Kommunikation, dem Amt für Bevölkerungsschutz, dem Amt für Hochbau und Raumplanung, dem Amt für Tiefbau und Geoinformation, der Stabsstelle FIU und der Finanzmarktaufsicht Liechtenstein;

m) die Zusammenarbeit mit dem Landesführungsstab und die Koordination der Ausarbeitung eines nationalen Plans für die Reaktion auf Cybersicherheitsvorfälle grossen Ausmasses und Krisen;

n) die grenzüberschreitende Zusammenarbeit und der grenzüberschreitende Informationsaustausch, insbesondere im Falle der Amtshilfe oder eines erheblichen Sicherheitsvorfalls oder bei einem Cybersicherheitsvorfall grossen Ausmasses, von dem zwei oder mehr EWR-Mitgliedstaaten betroffen sind, mit den zuständigen Behörden und Stellen in anderen EWR-Mitgliedstaaten, der ENISA, der Kooperationsgruppe, dem EU-CyCLONe und dem CSIRTs-Netzwerk;

o) die grenzüberschreitende Zusammenarbeit und der grenzüberschreitende Informationsaustausch im Bereich der Cybersicherheit mit den zuständigen Behörden und Stellen in Drittstaaten;

p) die Koordination der Erstellung einer NIS-Strategie nach Art. 21;

q) die Vertretung Liechtensteins in der Kooperationsgruppe, dem CSIRTs-Netzwerk, dem EU-CyCLONe, der Europäischen Gruppe für die Cybersicherheitszertifizierung sowie in anderen grenzüberschreitenden Gremien im EWR und internationalen Gremien für die Cybersicherheit;

r) die Teilnahme an Peer Reviews nach Art. 19 der Richtlinie (EU) 2022/2555.

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. 16

Befugnisse gegenüber wesentlichen und wichtigen Einrichtungen

1) Die Stabsstelle Cyber-Sicherheit kann bei der Wahrnehmung ihrer Aufgaben nach diesem Gesetz von den wesentlichen und wichtigen Einrichtungen verlangen, dass sie ihr:

a) die zur Bewertung der Cybersicherheit erforderlichen Informationen, einschliesslich der ergriffenen Risikomanagementmassnahmen sowie der dokumentierten Cybersicherheitskonzepte, zur Verfügung stellen;

b) Nachweise für die wirksame Umsetzung der Cybersicherheitskonzepte erbringen;

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

2) Sie kann weiters wesentliche oder wichtige Einrichtungen verpflichten:

a) natürliche oder juristische Personen, für die sie Dienste erbringen oder Tätigkeiten ausüben und die potenziell von einer erheblichen Cyberbedrohung betroffen sind, über die Art der Bedrohung und mögliche Abwehr- oder Abhilfemassnahmen zu unterrichten, die von diesen natürlichen oder juristischen Personen als Reaktion auf diese Bedrohung ergriffen werden können;

b) in begründeten Fällen, für einen bestimmten Zeitraum einen mit genau festgelegten Aufgaben betrauten Überwachungsbeauftragten zu benennen, der die Einhaltung der Risikomanagementmassnahmen und Berichtspflichten nach Art. 4 und 6 durch die betreffenden Einrichtungen überwacht;

c) spezielle IKT-Produkte, -Dienste und -Prozesse zu verwenden, die im Rahmen europäischer Schemata für die Cybersicherheitszertifizierung, die nach Art. 49 der Verordnung (EU) 2019/881 angenommen wurden, zertifiziert sind, um die Erfüllung bestimmter Anforderungen nach Art. 4 nachzuweisen.

3) Sie ist befugt, Sicherheitsscans auf der Grundlage objektiver, nichtdiskriminierender, fairer und transparenter Risikobewertungskriterien, erforderlichenfalls in Zusammenarbeit mit der betreffenden Einrichtung, durchzuführen.

4) Wesentliche und wichtige Einrichtungen können die Offenlegung von Informationen nach Abs. 1 Bst. c nicht wegen Berufs-, Geschäfts- oder Betriebsgeheimnissen verweigern.

Art. 17

Befugnisse bei Verstössen

1) Hat die Stabstelle Cyber-Sicherheit Anhaltspunkte dafür, dass eine wesentliche oder wichtige Einrichtung gegen Vorschriften dieses Gesetzes, der dazu erlassenen Verordnungen oder gegen darauf gestützte Entscheidungen oder Verfügungen verstösst, teilt sie dies der wesentlichen oder wichtigen Einrichtung vorbehaltlich Abs. 5 formlos mit und setzt ihr 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 die wesentliche oder wichtige Einrichtung dadurch voraussichtlich den rechtmässigen Zustand herstellt.

3) Handelt es sich bei der wesentlichen oder wichtigen Einrichtung 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.

4) Die Stabsstelle Cyber-Sicherheit informiert bei Anhaltspunkten zu Verstössen gegen Vorschriften dieses Gesetzes oder dazu erlassenen Verordnungen durch wesentliche oder wichtige Einrichtungen die zuständige Aufsichtsbehörde und gibt dieser vor einer Aufforderung nach Abs. 1 Gelegenheit zur Stellungnahme.

5) Kommt eine wesentliche oder wichtige Einrichtung 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 der wesentlichen oder wichtigen Einrichtung über die Entscheidung.

6) Die Verhängung von Bussen nach Art. 23 bleibt vorbehalten.

Art. 18

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;

c) IKT-Lösungen einzusetzen, um Sicherheitsscans auf der Grundlage objektiver, nichtdiskriminierender, fairer und transparenter Risikobewertungskriterien durchzuführen;

d) IKT-Lösungen zu betreiben oder durch Dritte betreiben zu lassen, um Recherchen im Internet durchzuführen, sich dabei auch an Foren oder Internetseiten mit einem geschlossenen Benutzerkreis zu registrieren und anzumelden sowie in weiterer Folge Daten, einschliesslich personenbezogener Daten, aus dem Internet herunterzuladen und zu analysieren.

Art. 19

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 von wesentlichen und wichtigen Einrichtungen 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 möglichster 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. 20

Zweck und Aufgaben

1) Zur Gewährleistung der Cybersicherheit 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 oder Orientierungshilfen für die Durchführung möglicher Abhilfemassnahmen nach Eingang von Meldungen über Risiken oder Sicherheitsvorfälle nach Art. 6 und 9;

b) die Ausgabe von Frühwarnungen und Alarmmeldungen sowie die Bekanntmachung und Verbreitung von Informationen über Cyberbedrohungen, Schwachstellen und Sicherheitsvorfälle unter den einschlägigen Interessensträgern;

c) die erste allgemeine oder technische Unterstützung bei der Reaktion auf einen Sicherheitsvorfall;

d) die Unterstützung wesentlicher und wichtiger Einrichtungen hinsichtlich der Überwachung ihrer Netz- und Informationssysteme auf Anfrage;

e) auf Ersuchen einer wesentlichen oder wichtigen Einrichtung die proaktive Überprüfung der Netz- und Informationssysteme der betreffenden Einrichtung auf Schwachstellen mit potenziell signifikanten Auswirkungen oder die proaktive nicht intrusive Überprüfung öffentlich zugänglicher Netz- und Informationssysteme aus eigenem Antrieb (Schwachstellenscan);

f) die Beobachtung und Analyse, einschliesslich die Analyse forensischer Daten sowie die dynamische Analyse, von Risiken, Cyberbedrohungen, Schwachstellen und Sicherheitsvorfällen sowie die Lagebeurteilung;

g) die Zusammenarbeit mit sektorspezifischen oder sektorübergreifenden Gruppierungen wesentlicher und wichtiger Einrichtungen sowie der Austausch von einschlägigen Informationen;

h) die Förderung der Anwendung gemeinsamer oder standardisierter Vorgehensweisen, Klassifizierungssysteme und Taxonomien für Verfahren zur Bewältigung von Sicherheitsvorfällen, das Krisenmanagement und die koordinierte Offenlegung von Schwachstellen;

i) die Beteiligung am CSIRTs-Netzwerk;

k) die Zusammenarbeit mit nationalen Computer-Notfallteams oder gleichwertigen Stellen von Drittstaaten, insbesondere um Unterstützung im Bereich der Cybersicherheit zu leisten.

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

3) Es fungiert als Koordinator und vertrauenswürdiger Vermittler für die Zwecke einer koordinierten Offenlegung von Schwachstellen nach Art. 12 Abs. 1 der Richtlinie (EU) 2022/2555.

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

D. NIS-Strategie

Art. 21

Grundsatz

1) Die NIS-Strategie bestimmt insbesondere die strategischen Ziele, die zur Erreichung dieser Ziele erforderlichen Ressourcen und die angemessenen Politik- und Regulierungsmassnahmen, mit denen ein hohes Cybersicherheitsniveau erreicht und aufrechterhalten werden soll.

2) Die NIS-Strategie wird regelmässig, mindestens jedoch alle fünf Jahre, auf der Grundlage wesentlicher Leistungsindikatoren bewertet und falls erforderlich aktualisiert.

3) Die NIS-Strategie ist von der Regierung zu genehmigen. Sie wird nach der Genehmigung auf der Internetseite der Stabsstelle Cyber-Sicherheit veröffentlicht.

IV. Rechtsmittel

Art. 22

Beschwerde

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

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

3) Die Überprüfungsbefugnis der Beschwerdekommission 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. 23

Übertretungen

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 nach Abs. 2 bestraft, wer:

a) die vorgeschriebenen Risikomanagementmassnahmen nach Art. 4 nicht ergreift;

b) die Berichtspflichten nach Art. 6 verletzt;

c) der Registrierungspflicht nach Art. 7 Abs. 1 nicht nachkommt;

d) die Stabsstelle Cyber-Sicherheit nicht fristgerecht über Änderungen nach Art. 7 Abs. 2 informiert;

e) die nach Art. 16 Abs. 1 Bst. a erforderlichen Informationen, einschliesslich der dokumentierten Sicherheitsmassnahmen, nicht zur Verfügung stellt;

f) Nachweise nach Art. 16 Abs. 1 Bst. b nicht erbringt;

g) Informationen nach Art. 16 Abs. 1 Bst. c gegenüber der Stabsstelle Cyber-Sicherheit nicht offenlegt;

h) der Verpflichtung nach Art. 16 Abs. 2 Bst. a nicht nachkommt;

i) der Verpflichtung der Benennung eines Überwachungsbeauftragten nach Art. 16 Abs. 2 Bst. b nicht nachkommt;

k) der Verpflichtung spezielle IKT-Produkte, -Dienste und -Prozesse nach Art. 16 Abs. 2 Bst. c zu verwenden nicht nachkommt;

l) die ordnungsgemässe Durchführung einer Kontrolle nach Art. 19 erschwert, behindert oder verunmöglicht;

m) gegen eine rechtskräftige Verfügung oder Entscheidung der Stabsstelle Cyber-Sicherheit verstösst.

2) Die Busse nach Abs. 1 beträgt für:

a) wesentliche Einrichtungen bis zu 10 000 000 Franken oder bis zu 2 % des gesamten weltweiten im vorangegangenen Geschäftsjahr getätigten Umsatzes des Unternehmens, dem die wesentliche Einrichtung angehört, je nachdem, welcher Betrag höher ist;

b) wichtige Einrichtungen bis zu 7 000 000 Franken oder bis zu 1,4 % des gesamten weltweiten im vorangegangenen Geschäftsjahr getätigten Umsatzes des Unternehmens, dem die wesentliche Einrichtung angehört, je nachdem, welcher Betrag höher ist.

3) 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 gegen die Verordnung (EU) 2019/881 verstösst, indem er als:

a) Hersteller oder Anbieter von IKT-Produkten, -Diensten und -Prozessen die Pflichten nach Art. 53 Abs. 2 oder 3 verletzt;

b) Hersteller oder Anbieter von zertifizierten IKT-Produkten, -Diensten oder -Prozessen oder von IKT-Produkten, -Diensten und -Prozessen die Anforderungen nach Art. 55 nicht einhält;

c) Konformitätsbewertungsstelle nach Art. 60 ein europäisches Cybersicherheitszertifikat nach Art. 56 Abs. 4 nicht ordnungsgemäss ausstellt;

d) Inhaber eines europäischen Cybersicherheitszertifikats die Verpflichtungen nach Art. 56 Abs. 8 verletzt; oder

e) Hersteller oder Anbieter von IKT-Produkten, -Diensten oder -Prozessen, die eine Selbstbewertung der Konformität durchführen, oder als Konformitätsbewertungsstelle nach Art. 60 die Überwachung und Beaufsichtigung der Vorschriften der Verordnung (EU) 2019/881

durch die Stabsstelle Cyber-Sicherheit erschwert, behindert oder verunmöglicht.

4) Bei der Verhängung einer Busse nach Abs. 1 bis 3 berücksichtigt die Stabsstelle Cyber-Sicherheit:

a) die Schwere des Verstosses und die Wichtigkeit der Bestimmungen, gegen die verstossen wurde, wobei Folgendes in allen Fällen als schwerer Verstoss anzusehen ist:
   1. wiederholte Verstösse;
   2. eine unterlassene Meldung oder Behebung von erheblichen Sicherheitsvorfällen;
   3. eine Nichtbehebung von Mängeln nach verbindlicher Anweisung der Stabsstelle Cyber-Sicherheit nach Art. 17 Abs. 5;
   4. die Behinderung von Kontrollen nach Art. 19, die nach der Feststellung eines Verstosses von der Stabsstelle Cyber-Sicherheit oder durch von ihr beauftragte qualifizierte Dritte durchgeführt wurden;
   5. die Übermittlung falscher oder grob verfälschender Informationen in Bezug auf Risikomanagementmassnahmen im Bereich der Cybersicherheit oder Berichtspflichten nach Art. 4 und 6;
b) die Dauer des Verstosses;
c) einschlägige frühere Verstösse der betreffenden Einrichtung;
d) der verursachte materielle oder immaterielle Schaden, darunter finanzieller oder wirtschaftlicher Verlust, Auswirkungen auf andere Dienste und die Zahl der betroffenen Nutzer;
e) von der Einrichtung ergriffene Massnahmen zur Verhinderung oder Minderung des materiellen oder immateriellen Schadens;
f) die Einhaltung genehmigter Verhaltensregeln oder genehmigter Zertifizierungsverfahren;
g) den Umfang der Zusammenarbeit der verantwortlichen natürlichen oder juristischen Personen mit den zuständigen Behörden.

5) Bei fahrlässiger Begehung werden die Strafobergrenzen nach Abs. 2 und 3 auf die Hälfte herabgesetzt.

6) Gegen Einrichtungen der öffentlichen Verwaltung des Landes werden keine Bussen verhängt.

Art. 24

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. Übergangs- und Schlussbestimmungen

Art. 25

Durchführungsverordnungen

Die Regierung erlässt die zur Durchführung dieses Gesetzes notwendigen Verordnungen.

Art. 26

Übergangsbestimmung

Wesentliche und wichtige Einrichtungen, die zum Zeitpunkt des Inkrafttretens dieses Gesetzes bestehen, haben der Stabsstelle Cyber-Sicherheit zwecks Registrierung die Angaben nach Art. 7 Abs. 1 innerhalb von vier Wochen ab Inkrafttreten dieses Gesetzes zu übermitteln.

Art. 27

Aufhebung bisherigen Rechts

Das Cyber-Sicherheitsgesetz (CSG) vom 4. Mai 2023, LGBl. 2023 Nr. 269, wird aufgehoben.

Art. 28

Anwendbarkeit von EU-Rechtsvorschriften

1) Bis zu ihrer Übernahme in das EWR-Abkommen gelten als nationale Rechtsvorschriften:

a) die Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Massnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS-2-Richtlinie);

b) die Durchführungsrechtsakte zur Richtlinie (EU) 2022/2555.

2) Der vollständige Wortlaut der in Abs. 1 genannten Rechtsvorschriften ist im Amtsblatt der Europäischen Union unter https://eur-lex.europa.eu veröffentlicht; er kann auf der Internetseite der Stabsstelle Cyber-Sicherheit unter https://scs.llv.li abgerufen werden.

Art. 29

Inkrafttreten

1) Dieses Gesetz tritt unter Vorbehalt des ungenutzten Ablaufs der Referendumsfrist am 1. Februar 2025 in Kraft, andernfalls am Tag nach der Kundmachung.

2) Art. 2 Abs. 1 Bst. a tritt gleichzeitig mit dem Beschluss des Gemeinsamen EWR-Ausschusses betreffend die Übernahme der Richtlinie (EU) 2022/2555 in das EWR-Abkommen in Kraft.

Anhang 1
(Art. 1, 3 und 7)

Sektoren mit hoher Kritikalität

Sektor	Teilsektor	Art der Einrichtung
1. Energie	a) Elektrizität	- Elektrizitätsunternehmen nach Art. 3 Abs. 1 Ziff. 34 des Elektrizitätsmarktgesetzes, die die Funktion "Versorgung" nach Art. 3 Abs. 1 Ziff. 20 des genannten Gesetzes wahrnehmen - Verteilernetzbetreiber nach Art. 3 Abs. 1 Ziff. 19 des Elektrizitätsmarktgesetzes - Übertragungsnetzbetreiber nach Art. 3 Abs. 1 Ziff. 18 des Elektrizitätsmarktgesetzes - Erzeuger nach Art. 3 Abs. 1 Ziff. 2 des Elektrizitätsmarktgesetzes - nominierte Strommarktbetreiber nach Art. 2 Ziff. 8 der Verordnung (EU) 2019/943[9] - Marktteilnehmer nach Art. 2 Ziff. 25 der Verordnung (EU) 2019/943, die Aggregierungs-, Laststeuerungs- oder Energiespeicherungsdienste nach Art. 2 Ziff. 18, 20 und 59 der Richtlinie (EU) 2019/944[10] anbieten - Betreiber von Ladepunkten, die für die Verwaltung und den Betrieb eines Ladepunkts zuständig sind und Endnutzern einen

9 Verordnung (EU) 2019/943 des Europäischen Parlaments und des Rates vom 5. Juni 2019 über den Elektrizitätsbinnenmarkt (ABl. L 158 vom 14.6.2019, S. 54)

10 Richtlinie (EU) 2019/944 des Europäischen Parlaments und des Rates vom 5. Juni 2019 mit gemeinsamen Vorschriften für den Elektrizitätsbinnenmarkt und zur Änderung der Richtlinie 2012/27/EU (ABl. L 158 vom 14.6.2019, S. 125)

Sektor	Teilsektor	Art der Einrichtung
		Aufladedienst erbringen, auch im Namen und Auftrag eines Mobilitätsdienstleisters
	b) Fernwärme und -kälte	- Betreiber von Fernwärme oder Fernkälte nach Art. 2 Ziff. 19 der Richtlinie (EU) 2018/2001[11]
	c) Erdöl	- Betreiber von Erdöl-Fernleitungen - Betreiber von Anlagen zur Produktion, Raffination und Aufbereitung von Erdöl sowie Betreiber von Erdöllagern und Erdöl-Fernleitungen - zentrale Bevorratungsstellen nach Art. 2 Bst. f der Richtlinie 2009/119/EG[12]
	d) Erdgas	- Versorgungsunternehmen nach Art. 4 Abs. 1 Ziff. 10 des Gasmarktgesetzes - Verteilernetzbetreiber nach Art. 4 Abs. 1 Ziff. 8 des Gasmarktgesetzes - Fernleitungsnetzbetreiber nach Art. 4 Abs. 1 Ziff. 6 des Gasmarktgesetzes - Betreiber einer Speicheranlage nach Art. 4 Abs. 1 Ziff. 12 des Gasmarktgesetzes - Betreiber einer LNG-Anlage nach Art. 4 Abs. 1 Ziff. 14 des Gasmarktgesetzes - Erdgasunternehmen nach Art. 4 Abs. 1 Ziff. 4 des Gasmarktgesetzes

11 Richtlinie (EU) 2018/2001 des Europäischen Parlaments und des Rates vom 11. Dezember 2018 zur Förderung der Nutzung von Energie aus erneuerbaren Quellen (ABl. L 328 vom 21.12.2018, S. 82)

12 Richtlinie 2009/119/EG des Rates vom 14. September 2009 zur Verpflichtung der Mitgliedstaaten, Mindestvorräte an Erdöl und/oder Erdölerzeugnissen zu halten (ABl. L 265 vom 9.10.2009, S. 9)

Sektor	Teilsektor	Art der Einrichtung
		- Betreiber von Anlagen zur Raffination und Aufbereitung von Erdgas
	e) Wasserstoff	- Betreiber im Bereich Wasserstofferzeugung, -speicherung und -fernleitung
2. Verkehr	a) Luftverkehr	- Luftfahrtunternehmen nach Art. 3 Ziff. 4 der Verordnung (EG) Nr. 300/2008[13], die für gewerbliche Zwecke genutzt werden - Flughafenleitungsorgane nach Art. 2 Ziff. 2 der Richtlinie 2009/12/EG[14], Flughäfen nach Art. 2 Ziff. 1 der genannten Richtlinie, einschliesslich der in Anhang II der Verordnung (EU) 2024/1679[15] aufgeführten Flughäfen des Kernnetzes, und Einrichtungen, die innerhalb von Flughäfen befindliche zugehörige Einrichtungen betreiben - Betreiber von Verkehrsmanagement- und Verkehrssteuerungssystemen, die Flugverkehrskontrolldienste nach Art. 2 Ziff. 1 der Verordnung (EG) Nr. 549/2004[16] bereitstellen

13 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)

14 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)

15 Verordnung (EU) 2024/1679 des Europäischen Parlaments und des Rates vom 13. Juni 2024 über Leitlinien der Union für den Aufbau des Transeuropäischen Verkehrsnetzes, zur Änderung der Verordnungen (EU) 2021/1153 und (EU) Nr. 913/2010 und zur Aufhebung der Verordnung (EU) Nr. 1315/2013 (ABl. L 2024/1679 vom 28.6.2024)

16 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") - Erklärung der Mitgliedstaaten zu militärischen Aspekten im Zusammenhang mit dem einheitlichen europäischen Luftraum (ABl. L 96 vom 31.3.2004, S. 1)

Sektor	Teilsektor	Art der Einrichtung
	b) Schienenverkehr	- Infrastrukturbetreiber nach Art. 3 Abs. 1 Bst. b des Eisenbahngesetzes - Eisenbahnunternehmen nach Art. 3 Abs. 1 Bst. a des Eisenbahngesetzes, einschliesslich Betreiber einer Serviceeinrichtung nach Art. 3 Ziff. 12 der Richtlinie 2012/34/EU[17]
	c) Schifffahrt	- Passagier- und Frachtbeförderungsunternehmen der Binnen-, See- und Küstenschifffahrt, wie sie in Anhang I der Verordnung (EG) Nr. 725/2004[18] für die Schifffahrt definiert sind, ausschliesslich der einzelnen von diesen Unternehmen betriebenen Schiffe - Leitungsorgane von Häfen nach Art. 3 Ziff. 1 der Richtlinie 2005/65/EG[19], einschliesslich ihrer Hafenanlagen nach Art. 2 Ziff. 11 der Verordnung (EG) Nr. 725/2004, sowie Einrichtungen, die innerhalb von Häfen befindliche Anlagen und Ausrüstung betreiben - Betreiber von Schiffsverkehrsdiensten nach Art. 3 Bst. o der Richtlinie 2002/59/EG[20]

17 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)

18 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)

19 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)

20 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)

Sektor	Teilsektor	Art der Einrichtung
	d) Strassenverkehr	- Strassenverkehrsbehörden nach Art. 2 Ziff. 12 der Delegierten Verordnung (EU) 2015/962[21], die für Verkehrsmanagement und Verkehrssteuerung verantwortlich sind, ausgenommen öffentliche Einrichtungen, für die das Verkehrsmanagement oder der Betrieb intelligenter Verkehrssysteme ein nicht wesentlicher Teil ihrer allgemeinen Tätigkeit ist - Betreiber intelligenter Verkehrssysteme nach Art. 4 Ziff. 1 der Richtlinie 2010/40/EU[22]
3. Bankwesen		Kreditinstitute nach Art. 4 Ziff. 1 der Verordnung (EU) Nr. 575/2013[23]
4. Finanzmarktinfrastrukturen		- Betreiber von Handelsplätzen nach Art. 3 Abs. 1 Ziff. 1 des Handelsplatz- und Börsegesetzes - zentrale Gegenparteien nach Art. 2 Ziff. 1 der Verordnung (EU) Nr. 648/2012[24]

21 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)

22 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)

23 Verordnung (EU) Nr. 575/2013 des Europäischen Parlaments und des Rates vom 26. Juni 2013 über Aufsichtsanforderungen an Kreditinstitute und Wertpapierfirmen und zur Änderung der Verordnung (EU) Nr. 646/2012 (ABl. L 176 vom 27.6.2013, S. 1)

24 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)

Sektor	Teilsektor	Art der Einrichtung
5. Gesundheitswesen		- Gesundheitsdienstleister nach Art. 3 Bst. g der Richtlinie 2011/24/EU[25] - EU-Referenzlaboratorien nach Art. 15 der Verordnung (EU) 2022/2371[26] - Einrichtungen, die Forschungs- und Entwicklungstätigkeiten in Bezug auf Arzneimittel nach Art. 4 Abs. 1 Bst. a des EWR-Arzneimittelgesetzes ausüben - Einrichtungen, die pharmazeutische Erzeugnisse nach Abschnitt C Abteilung 21 der Statistischen Systematik der Wirtschaftszweige in der Europäischen Gemeinschaft (NACE Rev. 2) herstellen - Einrichtungen, die Medizinprodukte herstellen, die während einer Notlage im Bereich der öffentlichen Gesundheit als kritisch nach Art. 22 der Verordnung (EU) 2022/123[27] ("Liste kritischer Medizinprodukte für Notlagen im Bereich der öffentlichen Gesundheit") eingestuft werden

25 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)

26 Verordnung (EU) 2022/2371 des Europäischen Parlaments und des Rates vom 23. November 2022 zu schwerwiegenden grenzüberschreitenden Gesundheitsgefahren und zur Aufhebung des Beschlusses Nr. 1082/2013/EU (ABl. L 314 vom 6.12.2022, S. 26)

27 Verordnung (EU) 2022/123 des Europäischen Parlaments und des Rates vom 25. Januar 2022 zu einer verstärkten Rolle der Europäischen Arzneimittel-Agentur bei der Krisenvorsorge und -bewältigung in Bezug auf Arzneimittel und Medizinprodukte (ABl. L 20 vom 31.1.2022, S. 1)

Sektor	Teilsektor	Art der Einrichtung
6. Trinkwasser		Lieferanten von und Unternehmen der Versorgung mit "Wasser für den menschlichen Gebrauch" nach Art. 2 Ziff. 1 Bst. a der Richtlinie (EU) 2020/2184[28], jedoch unter Ausschluss der Lieferanten, für die die Lieferung von Wasser für den menschlichen Gebrauch ein nicht wesentlicher Teil ihrer allgemeinen Tätigkeit der Lieferung anderer Rohstoffe und Güter ist
7. Abwasser		Unternehmen, die Abwasser nach Art. 5 Abs. 1 Bst. h des Gewässerschutzgesetzes sammeln, entsorgen oder behandeln, jedoch unter Ausschluss der Unternehmen, für die das Sammeln, die Entsorgung oder die Behandlung solchen Abwassers ein nicht wesentlicher Teil ihrer allgemeinen Tätigkeit ist
8. Digitale Infrastruktur		- Betreiber von Internet-Knoten - DNS-Diensteanbieter, ausgenommen Betreiber von Root-Namenservern - TLD-Namenregister - Anbieter von Cloud-Computing-Diensten - Anbieter von Rechenzentrumsdiensten - Betreiber von Inhaltszustellnetzen - Vertrauensdiensteanbieter - Anbieter öffentlicher elektronischer Kommunikationsnetze oder - Anbieter öffentlich zugänglicher elektronischer Kommunikationsdienste

28 Richtlinie (EU) 2020/2184 des Europäischen Parlaments und des Rates vom 16. Dezember 2020 über die Qualität von Wasser für den menschlichen Gebrauch (ABl. L 435 vom 23.12.2020, S. 1)

Sektor	Teilsektor	Art der Einrichtung
9. Verwaltung von IKT-Diensten (Business-to-Business)		- Anbieter verwalteter Dienste - Anbieter verwalteter Sicherheitsdienste
10. öffentliche Verwaltung		Einrichtungen der öffentlichen Verwaltung des Landes
11. Weltraum		Betreiber von Bodeninfrastrukturen, die sich im Eigentum des Fürstentums Liechtenstein oder privaten Parteien befinden und von diesen verwaltet und betrieben werden und die Erbringung von weltraumgestützten Diensten unterstützen, ausgenommen Anbieter öffentlicher elektronischer Kommunikationsnetze

Anhang 2
(Art. 1, 3 und 7)

Sonstige kritische Sektoren

Sektor	Teilsektor	Art der Einrichtung
1. Post- und Kurierdienste		Anbieter von Postdiensten nach Art. 3 Abs. 1 Bst. k des Postdienste- und Paketzustelldienstegesetzes, einschliesslich Anbieter von Kurierdiensten
2. Abfallbewirtschaftung		Unternehmen der Abfallbewirtschaftung nach Art. 3 Ziff. 9 der Richtlinie 2008/98/EG[29], ausgenommen Unternehmen, für die Abfallbewirtschaftung nicht ihre Hauptwirtschaftstätigkeit ist
3. Produktion, Herstellung und Handel mit chemischen Stoffen		Unternehmen nach Art. 3 Ziff. 9 und 14 der Verordnung (EG) Nr. 1907/2006[30], die Stoffe herstellen und mit Stoffen oder Gemischen handeln, und Unternehmen, die Erzeugnisse nach Art. 3 Ziff. 3 der genannten Verordnung aus Stoffen oder Gemischen produzieren

29 Richtlinie 2008/98/EG des Europäischen Parlaments und des Rates vom 19. November 2008 über Abfälle und zur Aufhebung bestimmter Richtlinien (ABl. L 312 vom 22.11.2008, S. 3)

30 Verordnung (EG) Nr. 1907/2006 des Europäischen Parlaments und des Rates vom 18. Dezember 2006 zur Registrierung, Bewertung, Zulassung und Beschränkung chemischer Stoffe (REACH), zur Schaffung einer Europäischen Agentur für chemische Stoffe, zur Änderung der Richtlinie 1999/45/EG und zur Aufhebung der Verordnung (EWG) Nr. 793/93 des Rates, der Verordnung (EG) Nr. 1488/94 der Kommission, der Richtlinie 76/769/EWG des Rates sowie der Richtlinien 91/155/EWG, 93/67/EWG, 93/105/EG und 2000/21/EG der Kommission (ABl. L 396 vom 30.12.2006, S. 1)

Sektor	Teilsektor	Art der Einrichtung
4. Produktion, Verarbeitung und Vertrieb von Lebensmitteln		Lebensmittelunternehmen nach Art. 3 Ziff. 2 der Verordnung (EG) Nr. 178/2002[31], die im Grosshandel sowie in der industriellen Produktion und Verarbeitung tätig sind
5. Verarbeitendes Gewerbe/Herstellung von Waren	a) Herstellung von Medizinprodukten und In-vitro-Diagnostika	Einrichtungen, die Medizinprodukte nach Art. 2 Ziff. 1 der Verordnung (EU) 2017/745[32] herstellen, und Einrichtungen, die In-vitro-Diagnostika nach Art. 2 Ziff. 2 der Verordnung (EU) 2017/746[33] herstellen, mit Ausnahme der unter Anhang I Ziff. 5 fünfter Gedankenstrich der genannten Richtlinie aufgeführten Einrichtungen, die Medizinprodukte herstellen
	b) Herstellung von Datenverarbeitungsgeräten, elektronischen und optischen Erzeugnissen	Unternehmen, die eine der Wirtschaftstätigkeiten nach Abschnitt C Abteilung 26 der Statistischen Systematik der Wirtschaftszweige in der Europäischen Gemeinschaft (NACE Rev. 2) ausüben
	c) Herstellung von elektrischen Ausrüstungen	Unternehmen, die eine der Wirtschaftstätigkeiten nach Abschnitt C Abteilung 27 der Statistischen Systematik der Wirtschaftszweige in der Europäischen Gemeinschaft (NACE Rev. 2) ausüben

31 Verordnung (EG) Nr. 178/2002 des Europäischen Parlaments und des Rates vom 28. Januar 2002 zur Festlegung der allgemeinen Grundsätze und Anforderungen des Lebensmittelrechts, zur Errichtung der Europäischen Behörde für Lebensmittelsicherheit und zur Festlegung von Verfahren zur Lebensmittelsicherheit (ABl. L 31 vom 1.2.2002, S. 1)

32 Verordnung (EU) 2017/745 des Europäischen Parlaments und des Rates vom 5. April 2017 über Medizinprodukte, zur Änderung der Richtlinie 2001/83/EG, der Verordnung (EG) Nr. 178/2002 und der Verordnung (EG) Nr. 1223/2009 und zur Aufhebung der Richtlinien 90/385/EWG und 93/42/EWG des Rates (ABl. L 117 vom 5.5.2017, S. 1)

33 Verordnung (EU) 2017/746 des Europäischen Parlaments und des Rates vom 5. April 2017 über In-vitro-Diagnostika und zur Aufhebung der Richtlinie 98/79/EG und des Beschlusses 2010/227/EU der Kommission (ABl. L 117 vom 5.5.2017, S. 176)

Sektor	Teilsektor	Art der Einrichtung
	d) Maschinenbau	Unternehmen, die eine der Wirtschaftstätigkeiten nach Abschnitt C Abteilung 28 der Statistischen Systematik der Wirtschaftszweige in der Europäischen Gemeinschaft (NACE Rev. 2) ausüben
	e) Herstellung von Kraftwagen und Kraftwagenteilen	Unternehmen, die eine der Wirtschaftstätigkeiten nach Abschnitt C Abteilung 29 der Statistischen Systematik der Wirtschaftszweige in der Europäischen Gemeinschaft (NACE Rev. 2) ausüben
	f) sonstiger Fahrzeugbau	Unternehmen, die eine der Wirtschaftstätigkeiten nach Abschnitt C Abteilung 30 der Statistischen Systematik der Wirtschaftszweige in der Europäischen Gemeinschaft (NACE Rev. 2) ausüben
6. Anbieter digitaler Dienste		- Anbieter von Online-Marktplätzen - Anbieter von Online-Suchmaschinen - Anbieter von Plattformen für Dienste sozialer Netzwerke
7. Forschung		Forschungseinrichtungen