Liechtensteinisches Landesgesetzblatt
Jahrgang 2023 Nr. 269 ausgegeben am 30. Juni 2023

Cyber-Sicherheitsgesetz (CSG)

vom 4. Mai 2023

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 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) 2018/1972[2] unterliegen; und

1 Bericht und Antrag sowie Stellungnahme der Regierung Nr. 9/2023 und 35/2023

2 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)

b) Vertrauensdiensteanbieter, die den Anforderungen nach Art. 19 der Verordnung (EU) Nr. 910/2014[3] 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 Union[4];

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

a) "Netz- und Informationssystem":

1. ein elektronisches Kommunikationsnetz im Sinne von Art. 3 Abs. 1 Ziff. 5 des Kommunikationsgesetzes;

---

3 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)

4 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)

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. L 202 vom 8.6.2021, S. 1)

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 Unternehmern ermöglicht, Online-Kaufverträge oder Online-Dienstleistungsverträge mit Unternehmern 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 ihres Geschlechts 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.

3) Art. 4 Abs. 4 findet sinngemäss Anwendung.

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.

3) Art. 5 Abs. 6 findet sinngemäss Anwendung.

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) 2016/679[6] zu verarbeiten.

6 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)

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

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 Informatik, 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)

2018/151[7], einschliesslich der nachweislichen Sicherheitsmassahmen, unverzüglich zur Verfügung stellen.

Art. 16

Befugnisse bei Verstössen

1) Hat die Stabstelle 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.

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 Betrei-

7 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)

bers 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 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. 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. Sie wird nach der Genehmigung auf der Internetseite der Stabsstelle Cyber-Sicherheit veröffentlicht.

IV. Rechtsmittel

Art. 21

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. 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 Sicherheitsmassahmen, 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. Schlussbestimmungen

Art. 24

Durchführungsverordnungen

Die Regierung erlässt die zur Durchführung dieses Gesetzes notwendigen Verordnungen.

Art. 25

Anwendbarkeit von EU-Rechtsvorschriften

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

a) die Richtlinie (EU) 2016/1148 über Massnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union;

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

c) die Durchführungsrechtsakte zu den EU-Rechtsvorschriften nach Bst. a und b.

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. 26

Inkrafttreten

1) Dieses Gesetz tritt unter Vorbehalt des ungenutzten Ablaufs der Referendumsfrist am 1. Juli 2023 in Kraft, andernfalls am Tag nach der Kundmachung.

2) Art. 2 Abs. 1 Bst. a tritt gleichzeitig mit dem Beschluss des Gemeinsamen EWR-Ausschusses Nr. 21/2023 vom 3. Februar 2023 zur Änderung von Anhang XI (Elektronische Kommunikation, audiovisuelle Dienste und Informationsgesellschaft) des EWR-Abkommens in Kraft.

3) Art. 2 Abs. 1 Bst. b tritt gleichzeitig mit dem Beschluss des Gemeinsamen EWR-Ausschusses Nr. 27/2023 vom 3. Februar 2023 zur Änderung von Protokoll 31 (Zusammenarbeit in bestimmten Bereichen ausserhalb der vier Freiheiten) des EWR-Abkommens in Kraft.

In Stellvertretung des Landesfürsten:
gez. *Alois*
Erbprinz

gez. *Dr. Daniel Risch*
Fürstlicher Regierungschef