Entwurf

Bundesgesetz, mit dem ein Bundesgesetz zur Gewährleistung eines hohen Cybersicherheitsniveaus von Netz- und Informationssystemen (Netz- und Informationssystemsicherheitsgesetz 2024 – NISG 2024) erlassen wird und das Telekommunikationsgesetz 2021 und das Gesundheitstelematikgesetz 2012 geändert werden

Der Nationalrat hat beschlossen:

Inhaltsverzeichnis

Artikel 2
Änderung des Telekommunikationsgesetzes 2021

Artikel 3
Änderung des Gesundheitstelematikgesetzes 2012

1. Hauptstück
Allgemeine Bestimmungen

Verfassungsbestimmung

§ 1. (Verfassungsbestimmung) (1) Die Erlassung, Aufhebung, Änderung sowie Vollziehung von Vorschriften, wie sie in diesem Bundesgesetz enthalten sind, sind auch in den Belangen Bundessache, hinsichtlich derer das Bundes-Verfassungsgesetz (B-VG), BGBl. Nr. 1/1930, etwas anderes bestimmt. Die in diesem Bundesgesetz geregelten Angelegenheiten können unmittelbar von Bundesbehörden besorgt werden.

(2) Soweit in diesem Bundesgesetz nicht anders bestimmt ist, übt der Bundesminister für Inneres seine Befugnisse nach diesem Bundesgesetz auch gegenüber den in Art. 19 B-VG bezeichneten obersten Organen der Vollziehung aus.

(3) Änderungen des § 45 Abs. 5 sowie § 46 dürfen, sofern sie sich auf Behörden und sonstige Stellen der öffentlichen Verwaltung der Länder, wie insbesondere in Formen des öffentlichen Rechts sowie des Privatrechts eingerichtete Stellen, beziehen, nur mit Zustimmung der Länder kundgemacht werden.

Gegenstand und Ziel des Gesetzes

§ 2. Mit diesem Bundesgesetz werden Maßnahmen festgelegt, mit denen ein hohes Cybersicherheitsniveau, insbesondere von wesentlichen und wichtigen Einrichtungen in den Sektoren

1. Energie,
2. Verkehr,
3. Bankwesen,
4. Finanzmarktinfrastrukturen,
5. Gesundheitswesen,
6. Trinkwasser,
7. Abwasser,
8. Digitale Infrastruktur,
9. Verwaltung von IKT-Diensten (Business-to-Business),
10. öffentliche Verwaltung,
11. Weltraum,
12. Post- und Kurierdienste,
13. Abfallbewirtschaftung,
14. Produktion, Herstellung und Handel mit chemischen Stoffen,
15. Produktion, Verarbeitung und Vertrieb von Lebensmitteln,
16. Verarbeitendes Gewerbe/Herstellung von Waren,
17. Anbieter digitaler Dienste,
18. Forschung,

und den zugehörigen Teilsektoren nach den Anlagen 1 und 2 erreicht werden soll.

Begriffsbestimmungen

§ 3. Im Sinne dieses Bundesgesetzes bedeutet

1. „Netz- und Informationssystem“
   a) ein Kommunikationsnetz im Sinne des § 4 Z 1 des Telekommunikationsgesetzes 2021 (TKG 2021), BGBl. I Nr. 190/2021,
   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
   c) digitale Daten, die von den in den Buchstaben a und b genannten Elementen zum Zwecke ihres Betriebs, ihrer Nutzung, ihres Schutzes und ihrer Pflege gespeichert, verarbeitet, abgerufen oder übertragen werden;

2. „Sicherheit von Netz- und Informationssystemen“ die Fähigkeit von Netz- und Informationssystemen, auf einem bestimmten Vertrauensniveau alle Ereignisse abzuwehren, die die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit gespeicherter oder 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. „öffentliches Kommunikationsnetz“ ein öffentliches elektronisches Kommunikationsnetz im Sinne des § 4 Z 9 TKG 2021;
5. „Kommunikationsdienst“ ein elektronischer Kommunikationsdienst des § 4 Z 4 TKG 2021;
6. „IKT-Produkt“ ein Element oder eine Gruppe von Elementen eines Netz- oder Informationssystems;
7. „IKT-Dienst“ ein Dienst, der vollständig oder überwiegend aus der Übertragung, Speicherung, Abfrage oder Verarbeitung von Informationen mittels Netz- und Informationssystemen besteht;
8. „IKT-Prozess“ jegliche Tätigkeiten, mit denen ein IKT-Produkt oder -Dienst konzipiert, entwickelt, bereitgestellt oder gepflegt werden soll;
9. „Schwachstelle“ eine Schwäche, Anfälligkeit oder Fehlfunktion von IKT-Produkten oder IKT-Diensten, die bei einer Cyberbedrohung ausgenutzt werden kann;
10. „Einrichtung“ eine natürliche Person oder nach dem an ihrem Sitz geltenden nationalen Recht geschaffene und anerkannte juristische Person oder eingetragene Personengesellschaft, die in eigenem Namen Rechte ausüben und Pflichten unterliegen kann;
11. „Leitungsorgan“ eine oder mehrere natürliche Personen oder Verwaltungsorgane, die nach Gesetz, Satzung oder Vertrag zur Führung der Geschäfte einer Einrichtung oder innerhalb der Einrichtung zur Überwachung der Geschäftsführung berufen sind;
12. „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;
13. „Namenregister der Domäne oberster Stufe“ oder „TLD-Namenregister“ eine Einrichtung, der eine bestimmte Domäne oberster Stufe (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;
14. „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;
15. „Anbieter digitaler Dienste“ eine juristische Person oder eingetragene Personengesellschaft, die einen digitalen Dienst im Sinne des § 3 Z 1 E-Commerce-Gesetz (ECG), BGBl. I Nr. 152/2001, bei dem es sich um einen Online-Marktplatz, eine Online-Suchmaschine oder einen Cloud-Computing-Dienst handelt, erbringt;
16. „Vertrauensdienst“ ein Vertrauensdienst gemäß Art. 3 Nr. 16 der Verordnung (EU) 910/2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG, ABl. Nr. L 257 vom 28.08.2014 S. 73, in der Fassung der Berichtigung ABl. Nr. L 23 vom 29.01.2015 S. 19 (Verordnung (EU) 910/2014);
17. „Vertrauensdiensteanbieter“ ein Vertrauensdiensteanbieter gemäß Art. 3 Nr. 16 Verordnung (EU) 910/2014;
18. „qualifizierter Vertrauensdiensteanbieter“ ein qualifizierter Vertrauensdiensteanbieter gemäß Art. 3 Nr. 20 Verordnung (EU) 910/2014;
19. „qualifizierte elektronische Signaturerstellungseinheit“ eine qualifizierte elektronische Signaturerstellungseinheit gemäß Art. 3 Nr. 23 c;
20. „qualifizierte elektronische Siegelerstellungseinheit“ eine qualifizierte elektronische Siegelerstellungseinheit gemäß Art. 3 Nr. 32 Verordnung (EU) 910/2014;

21. „Konformitätsbewertungsbericht“ ein Konformitätsbewertungsbericht gemäß Art. 20 Abs. 1 Verordnung (EU) 910/2014;
22. „vertrauenswürdige Systeme eines Vertrauensdiensteanbieters“ Systeme und Produkte, die den Erfordernissen gemäß Art. 24 Abs. 2 Buchstabe e und f Verordnung (EU) 910/2014 entsprechen;
23. „Anbieter verwalteter Dienste“ (Managed Service Provider) 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, dies entweder in den Räumlichkeiten der Kunden oder aus der Ferne;
24. „Anbieter verwalteter Sicherheitsdienste“ ein Anbieter verwalteter Dienste, der Unterstützung für Tätigkeiten im Zusammenhang mit dem Risikomanagement im Bereich der Cybersicherheit durchführt oder erbringt;
25. „Vertreter“ eine in der Europäischen Union 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 in der Europäischen Union 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 Bundesgesetzes wenden kann;
26. „Risiko“ das Potenzial für Verluste oder Störungen, die durch einen Cybersicherheitsvorfall verursacht werden, das als eine Kombination des Ausmaßes eines solchen Verlusts oder einer solchen Störung und der Wahrscheinlichkeit des Eintretens des Cybersicherheitsvorfalls zum Ausdruck gebracht wird;
27. „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;
28. „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;
29. „Beinahe-Cybersicherheitsvorfall“ (Near Miss) ein Ereignis, das die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit gespeicherter, übermittelter oder verarbeiteter Daten oder der Dienste, die über Netz- und Informationssysteme angeboten werden bzw. zugänglich sind, beeinträchtigt haben könnte, dessen Eintritt jedoch erfolgreich verhindert wurde bzw. das nicht eingetreten ist;
30. „Cybersicherheitsvorfall“ ein Ereignis, das die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit gespeicherter, übermittelter oder verarbeiteter Daten oder der Dienste, die über Netz- und Informationssysteme angeboten werden bzw. zugänglich sind, beeinträchtigt;
31. „Cybersicherheitsvorfall großen Ausmaßes“ ein Cybersicherheitsvorfall, der eine Störung verursacht, deren Ausmaß die Reaktionsfähigkeit eines Mitgliedstaats der Europäischen Union übersteigt, oder der beträchtliche Auswirkungen auf mindestens zwei Mitgliedstaaten hat;
32. „Innerer Kreis der Operativen Koordinierungsstruktur (IKDOK)“ eine Struktur zur Koordination auf der operativen Ebene im Bereich der Cybersicherheit bestehend aus Vertretern des Bundeskanzlers, des Bundesministers für Inneres, des Bundesministers für Landesverteidigung, des Bundesministers für europäische und internationale Angelegenheiten;
33. „Operative Koordinierungsstruktur (OpKoord)“ eine Struktur zur Koordination auf der operativen Ebene im Bereich der Cybersicherheit bestehend aus dem IKDOK und den Computer-Notfallteams (CSIRTs), die anlassbezogen um zusätzliche Teilnehmer erweitert werden kann;
34. „Kooperationsgruppe“ ein gemäß Art. 14 der 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) 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS-2-Richtlinie), ABl. Nr. 19 vom 27.12.2022 S. 80, eingesetztes Gremium zur Unterstützung und Erleichterung der strategischen Zusammenarbeit und des Informationsaustauschs zwischen den Mitgliedstaaten der Europäischen Union und zur Stärkung des Vertrauens;

35. „CSIRTs-Netzwerk“ ein gemäß Art. 15 NIS-2-Richtlinie errichtetes Gremium zum Aufbau von Vertrauen zwischen den Mitgliedstaaten der Europäischen Union und zur Förderung einer raschen und wirksamen operativen Zusammenarbeit zwischen ihnen;
36. „EU-CyCLONe“ das gemäß Art. 16 NIS-2-Richtlinie zur Unterstützung des koordinierten Managements von Cybersicherheitsvorfällen großen Ausmaßes und Krisen auf operativer Ebene und zur Gewährleistung eines regelmäßigen Austauschs relevanter Informationen zwischen den Mitgliedstaaten und den Organen, Einrichtungen und sonstigen Stellen der Europäischen Union eingerichtete Europäische Netzwerk der Verbindungsorganisationen für Cyberkrisen (European Cyber Crisis Liaison Organisation Network, kurz: EU-CyCLONe);
37. „Überwachungsbeauftragter“ ein Mitarbeiter der Cybersicherheitsbehörde, der für den gemäß § 39 Abs. 3 festgelegten Zeitraum die Einhaltung der Risikomanagementmaßnahmen (§ 32) und der Berichtspflichten (§ 34) einer wesentlichen Einrichtung überprüft.

2. Hauptstück
Strukturen und Aufgaben

1. Abschnitt
Zuständige Behörde

Cybersicherheitsbehörde

§ 4. (1) Der Bundesminister für Inneres hat als zuständige Behörde für die Gewährleistung eines hohen Cybersicherheitsniveaus von Netz- und Informationssystemen (Cybersicherheitsbehörde) folgende Aufgaben wahrzunehmen:

1. Koordination der Erstellung der Österreichischen Strategie für Cybersicherheit (ÖSCS) gemäß § 15;
2. Leitung der Koordinierungsstrukturen (CSS, IKDOK und OpKoord) gemäß §§ 12 bis 14;
3. Regelmäßige Erstellung und Weiterleitung von Lagebildern und zusätzlich relevanter Informationen gemäß §§ 12 bis 14;
4. Erstellung und Weitergabe von zur Gewährleistung der Sicherheit von Netz- und Informationssystemen relevanten Informationen zur Vorbeugung von Cybersicherheitsvorfällen gemäß §§ 20 und 21;
5. Ausübung der Funktion der nationalen Behörde für das Management von Cybersicherheitsvorfällen großen Ausmaßes gemäß § 16;
6. Ausübung der Funktion des Nationalen Koordinierungszentrums für Cybersicherheit gemäß § 6;
7. Vertretung von Österreich in EU-weiten und internationalen Gremien betreffend die Gewährleistung eines hohen Cybersicherheitsniveaus von Netz- und Informationssystemen, insbesondere der Kooperationsgruppe, EU-CyCLONe sowie dem Europäischen Kompetenznetz und Zentrum für Cybersicherheit (ECCC), sofern nicht der Wirkungsbereich anderer Bundesminister betroffen ist;
8. Konsultation und Zusammenarbeit mit den zuständigen Behörden anderer Mitgliedstaaten der Europäischen Union gemäß § 22;
9. Betrieb der zentralen Anlaufstelle gemäß § 5;
10. Betrieb des GovCERT gemäß § 8 Abs. 4;
11. Ermächtigung sowie Beaufsichtigung von CSIRTs gemäß § 8 Abs. 2 und § 10;
12. Zulassung sowie Kontrolle der Einhaltung der Erfordernisse unabhängiger Stellen und unabhängiger Prüfer gemäß § 7;
13. Ausübung der Aufsichts- und Durchsetzungsmaßnahmen gegenüber wesentlichen und wichtigen Einrichtungen gemäß §§ 38 und 39;
14. Entgegennahme, Analyse und Weiterleitung von Meldungen gemäß § 34, § 37 sowie gemäß § 8 Abs. 1 Z 7.

(2) Angelegenheiten die unter die Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates und vom 14. Dezember 2022 über die digitale operationale Resilienz im Finanzsektor und zur Änderung der Verordnungen (EG) 1060/2009, (EU) 648/2012, (EU) 600/2014, (EU) 909/2014 und (EU) 2016/1011 vom 14. Dezember 2022 über die digitale operationale Resilienz im Finanzsektor und zur Änderung der Verordnungen (EG) 1060/2009, (EU) 648/2012, (EU) 600/2014, (EU)909/2014 und (EU) 2016/1011, ABl. 333 vom 27.12.2022 S 1 (im Folgenden: Verordnung (EU) 2022/2554) fallen, bleiben von diesem Bundesgesetz unberührt.

(3) Der Bundesminister für Inneres hat den jährlichen Bericht zur Cybersicherheit gemeinsam mit einer Übersicht über die eingelangten Meldungen gemäß §§ 34 und 37 sowie die Höhe der gemäß § 8 Abs. 6 ersetzten Aufwendungen dem Nationalrat und dem Bundesrat vorzulegen.

Zentrale Anlaufstelle der Cybersicherheitsbehörde

§ 5. (1) Die Cybersicherheitsbehörde hat eine zentrale Anlaufstelle zu betreiben, die als operative Verbindungsstelle der Gewährleistung der Sicherheit von Netz- und Informationssystemen, der grenzüberschreitenden Zusammenarbeit und Kommunikation mit den zuständigen Stellen in den anderen Mitgliedstaaten der Europäischen Union sowie der Kooperationsgruppe, EU-CyCLONe und dem CSIRTs-Netzwerk dient.

(2) Die zentrale Anlaufstelle hat

1. eingehende Meldungen und Anfragen unmittelbar an die Mitglieder des IKDOK und die CSIRTs weiterzuleiten, soweit dies zur Erfüllung einer gesetzlich übertragenen Aufgabe des jeweiligen Mitglieds des IKDOK oder des CSIRTs erforderlich ist;
2. einen Auszug aus dem Register der Einrichtungen gemäß § 29 Abs. 6 an die ENISA weiterzuleiten;
3. die zentralen Anlaufstellen in anderen Mitgliedstaaten der Europäischen Union zu unterrichten, wenn ein Cybersicherheitsvorfall einen oder mehrere andere Mitgliedstaaten betrifft (§ 34 Abs. 5).

Nationales Koordinierungszentrum für Cybersicherheit

§ 6. (1) Die Cybersicherheitsbehörde nimmt die Aufgaben eines nationalen Koordinierungszentrums für Cybersicherheit wahr. Dies umfasst insbesondere die nachstehenden Tätigkeiten:

1. den Betrieb eines nationalen Koordinierungszentrums gemäß der Verordnung (EU) 2021/887 zur Einrichtung des Europäischen Kompetenzzentrums für Industrie, Technologie und Forschung im Bereich der Cybersicherheit und des Netzwerks nationaler Koordinierungszentren, ABl. Nr. L 202 vom 08.06.2021 S. 1;
2. die Koordination der öffentlich-privaten Zusammenarbeit im Bereich der Cybersicherheit;
3. die Koordination der Erstellung eines jährlichen Berichts zur Cybersicherheit;
4. die Dokumentation und Bereitstellung von Informationen zum Thema Cybersicherheit für die Öffentlichkeit;
5. die Organisation und Durchführung von Kampagnen zur Bewusstseinsbildung und Sensibilisierung der Öffentlichkeit, insbesondere für Cyberbedrohungen sowie zur Stärkung und Erweiterung von Fähigkeiten und Kenntnissen im Bereich der Cybersicherheit;
6. die Bereitstellung von generellen Empfehlungen und Leitlinien zur Prävention von Cybersicherheitsvorfällen und Reduktion von Risiken;
7. die regelmäßige Veranstaltung von und Mitwirkung an Cybersicherheitsübungen;
8. die Durchführung und Unterstützung von Risikobewertungen, insbesondere in den in § 2 genannten Sektoren und bei EU-weit koordinierten Risikobewertungen, gegebenenfalls in Zusammenarbeit mit den maßgeblichen Interessenträgern;
9. die Durchführung von Analysen über Informations- und Kommunikationstechnik und themenspezifische Bewertung der von technischen Innovationen zu erwartenden gesellschaftlichen, rechtlichen, wirtschaftlichen und regulatorischen Auswirkungen auf die Cybersicherheit;
10. die Durchführung von langfristigen strategischen Analysen von Cyberbedrohungen und Cybersicherheitsvorfällen, gegebenenfalls in Zusammenarbeit mit maßgeblichen Interessenträgern;
11. die Beratung der zuständigen Bundesminister und öffentlichen Einrichtungen zum Forschungs- und Förderbedarf und zu den Forschungs- und Förderprioritäten im Bereich Cybersicherheit;
12. die Verfolgung von Entwicklungen und gegebenenfalls Mitarbeit an der Er- oder Überarbeitung von Normen mit Bezug auf Cybersicherheit;
13. die Mitwirkung und Teilnahme an nationalen, europäischen und internationalen Forschungs- und Förderprojekten und -programmen auf dem Gebiet der Cybersicherheit.

(2) Der Bundesminister für Inneres kann mittels Verordnung die Verwendung von Formularen zur Antragstellung von Einrichtungen zur Aufnahme in die Europäische Kompetenzgemeinschaft gemäß Art. 7 Abs. 1 Buchstabe i und Abs. 4 der Verordnung (EU) 2021/887 des Europäischen Parlaments und des Rates vom 20. Mai 2021 zur Einrichtung des Europäischen Kompetenzzentrums für Industrie,

Technologie und Forschung im Bereich der Cybersicherheit und des Netzwerks nationaler Koordinierungszentren, ABl. Nr. 202 vom 8.6.2021 S. 1, festlegen.

2. Abschnitt
Unabhängige Stellen und unabhängige Prüfer

Unabhängige Stellen und unabhängige Prüfer

§ 7. (1) Eine unabhängige Stelle ist eine juristische Person oder eingetragene Personengesellschaft mit Niederlassung in Österreich, die zur Prüfung der Umsetzung der Risikomanagementmaßnahmen wesentlicher und wichtiger Einrichtungen gemäß § 33 Abs. 2 und 3 zumindest einen unabhängigen Prüfer gemäß Abs. 5 einzusetzen hat.

(2) Die Zulassung als unabhängige Stelle hat durch die Cybersicherheitsbehörde bei Erfüllung der Voraussetzungen gemäß Abs. 13 Z 1 auf begründeten schriftlichen Antrag mit Bescheid zu erfolgen.

(3) Zur Kontrolle der Einhaltung der Anforderungen, die unabhängige Stellen gemäß Abs. 13 Z 1 erfüllen müssen, kann die Cybersicherheitsbehörde Aufsichtsmaßnahmen nach Maßgabe des § 38 Abs. 1 vornehmen.

(4) Bei Nichteinhaltung der Anforderungen gemäß Abs. 13 Z 1 hat die Cybersicherheitsbehörde die Zulassung gemäß Abs. 2 zu widerrufen, außer die Nichteinhaltung ist auf ein von der unabhängigen Stelle nicht beeinflussbares Ereignis zurückführbar. Nach einem Widerruf ihrer Zulassung kann die betroffene Einrichtung erst nach Ablauf eines Jahres ab Rechtskraft des Widerrufs einen neuerlichen Antrag auf Zulassung als unabhängige Stelle stellen.

(5) Ein unabhängiger Prüfer ist eine natürliche Person, die von einer unabhängigen Stelle zur Beurteilung der Umsetzung von Risikomanagementmaßnahmen wesentlicher und wichtiger Einrichtungen gemäß § 33 Abs. 2 und 3 eingesetzt werden kann.

(6) Die Zulassung als unabhängiger Prüfer hat durch die Cybersicherheitsbehörde auf begründeten schriftlichen Antrag mit Bescheid zu erfolgen, wenn der Antragsteller über

1. eine vor nicht länger als drei Jahren durchgeführte Sicherheitsüberprüfung auf begründetes Ersuchen einer unabhängigen Stelle oder sonstigen Einrichtung nach §§ 55 ff des Sicherheitspolizeigesetzes (SPG), BGBl. Nr. 566/1991, für den Zugang zu geheimer Information verfügt sowie
2. gegenüber der Cybersicherheitsbehörde seine Eignung zur Beurteilung der Umsetzung von Risikomanagementmaßnahmen durch die positive Absolvierung einer Fachprüfung gemäß Abs. 8 nachgewiesen hat.

(7) Zur Fachprüfung gemäß Abs. 8 ist zuzulassen, wer über

1. ein österreichisches Reifeprüfungszeugnis, ein österreichisches Reife- und Diplomprüfungszeugnis oder ein österreichisches Zeugnis über die Berufsreifeprüfung, sowie diesen durch völkerrechtliche Vereinbarung gleichwertige Zeugnisse, sowie
2. facheinschlägige und durchgängige Berufserfahrung von mindestens drei Jahren im Ausmaß von zumindest zwanzig Wochenstunden im Bereich der Cybersicherheit, welche anhand von Zeugnissen gemäß § 39 des Angestelltengesetzes, BGBl. Nr. 292/1921 oder in gleichwertiger Form nachzuweisen sind, verfügt.

(8) Im Rahmen der Fachprüfung hat der Prüfungskandidat ausreichende theoretische Fachkenntnisse über die Risikomanagementmaßnahmen gemäß § 32 und ausreichende praktische Fähigkeiten zur Beurteilung der Umsetzung von Risikomanagementmaßnahmen gemäß § 32 in organisatorischer oder technischer Hinsicht nachzuweisen.

(9) Der Nachweis gemäß Abs. 6 Z 2 gilt als nicht mehr vorhanden, wenn

1. der jeweilige unabhängige Prüfer in einem Zeitraum von fünf Jahren nicht zumindest bei zwei Prüfungen von wesentlichen oder wichtigen Einrichtungen gemäß Abs. 1 zur Beurteilung der Umsetzung von Risikomanagementmaßnahmen durch eine unabhängige Stelle eingesetzt wurde oder
2. für die Cybersicherheitsbehörde im Zuge von Aufsichtsmaßnahmen erkennbar wird, dass bei dem jeweiligen unabhängigen Prüfer die benötigten Fachkenntnisse und Fähigkeiten gemäß Abs. 8 nicht mehr vorliegen, insbesondere aufgrund wiederholter mangelhafter Beurteilung der Umsetzung von Risikomanagementmaßnahmen wesentlicher oder wichtiger Einrichtungen.

(10) Bei Wegfall oder Nichteinhaltung der Erfordernisse gemäß Abs. 6 sowie für den Fall, dass jeweils nach Ablauf von drei Jahren seit der letztmaligen Durchführung keine Wiederholung der

Sicherheitsüberprüfung gemäß Abs. 6 Z 1 erfolgt, hat die Cybersicherheitsbehörde die Zulassung als unabhängiger Prüfer zu widerrufen. Nach einem Widerruf der Zulassung kann die betroffene natürliche Person erst nach Ablauf eines Jahres ab Rechtskraft des Widerrufs einen neuerlichen Antrag auf Zulassung als unabhängiger Prüfer stellen.

(11) Die Cybersicherheitsbehörde hat eine Liste mit den zugelassenen unabhängigen Stellen und unabhängigen Prüfern zu führen und wesentlichen und wichtigen Einrichtungen sowie unabhängigen Stellen in Bezug auf unabhängige Prüfer in geeigneter Weise zur Verfügung zu stellen.

(12) Unabhängige Prüfer sind über bekanntgewordene Tatsachen und Erkenntnisse, die im Rahmen der Prüfung und Beurteilung der Umsetzung von Risikomanagementmaßnahmen auftreten und deren Geheimhaltung im Interesse der jeweiligen geprüften Einrichtungen geboten ist, zur Verschwiegenheit verpflichtet. Dies gilt auch für Personen, denen im Zuge ihrer Tätigkeit bei einer unabhängigen Stelle solche Tatsachen und Erkenntnisse bekanntwerden.

(13) Der Bundesminister für Inneres hat mit Verordnung Folgendes festzulegen:

1. das Verfahren zur Zulassung einer unabhängigen Stelle und die Anforderungen, die eine unabhängige Stelle erfüllen muss, insbesondere hinsichtlich der nötigen Vorkehrungen und Strukturen, mit denen die fachliche Qualität und ein systematischer Verfahrensablauf der Prüfungen gemäß § 33 Abs. 2 und 3 sicherzustellen ist;
2. nähere Regelungen zum Verfahren und zu den Inhalten einer Fachprüfung gemäß Abs. 8;
3. Pauschalsätze für die Zulassung als unabhängige Stelle, als unabhängiger Prüfer sowie zur Ablegung einer Fachprüfung zu bestimmen, die dem durchschnittlichen Aufwand der jeweiligen Zulassung entsprechen.

3. Abschnitt
Computer-Notfallteams

Zweck und Aufgaben der Computer-Notfallteams

§ 8. (1) Computer-Notfallteams (CSIRTs) haben zur Gewährleistung der Sicherheit von Netz- und Informationssystemen folgende Aufgaben wahrzunehmen:

1. die Überwachung und die Analyse von Cyberbedrohungen, Schwachstellen und Cybersicherheitsvorfällen auf nationaler Ebene und gegebenenfalls die Unterstützung betreffender wesentlicher und wichtiger Einrichtungen hinsichtlich der Überwachung ihrer Netz- und Informationssysteme in Echtzeit oder nahezu in Echtzeit;
2. die Ausgabe von Frühwarnungen und Alarmmeldungen sowie die Bekanntmachung und die Weitergabe von Informationen über Cyberbedrohungen, Schwachstellen und Cybersicherheitsvorfälle an wesentliche und wichtige Einrichtungen sowie an zuständige Behörden und andere einschlägige Interessenträger in Echtzeit oder nahezu in Echtzeit;
3. die Reaktion auf Cybersicherheitsvorfälle und gegebenenfalls die Unterstützung betreffender wesentlicher und wichtiger Einrichtungen bei deren Bewältigung;
4. die Erhebung und die Analyse forensischer Daten sowie die dynamische Analyse von Risiken und Cybersicherheitsvorfällen sowie die Lagebeurteilung im Hinblick auf die Cybersicherheit;
5. die Vornahme einer proaktiven Überprüfung der Netz- und Informationssysteme einer ersuchenden wesentlichen oder wichtigen Einrichtung im Hinblick auf Schwachstellen mit potentiell signifikanten Auswirkungen (Schwachstellenscan);
6. die Beteiligung am CSIRTs-Netzwerk (§ 3 Z 35) und die auf Gegenseitigkeit beruhende Unterstützung anderer Mitglieder des CSIRTs-Netzwerks;
7. die Entgegennahme von Meldungen gemäß §§ 34 und 37;
8. die Teilnahme an Peer Reviews gemäß § 23.

(2) Der Bundesminister für Inneres hat bei Erfüllung der Voraussetzungen gemäß § 9 eine Einrichtung zur Wahrnehmung der Aufgaben gemäß Abs. 1 zu ermächtigen (nationales CSIRT). Das nationale CSIRT ist zur proaktiven nicht intrusiven Überprüfung öffentlich zugänglicher Netz- und Informationssysteme berechtigt. Eine solche Überprüfung darf keine nachteiligen Auswirkungen auf das Funktionieren der Dienste der betroffenen wesentlichen oder wichtigen Einrichtungen haben. Werden bei einer solchen Überprüfung anfällige oder unsicher konfigurierte Netz- und Informationssysteme ermittelt, sind die jeweiligen Einrichtungen darüber zu unterrichten.

(3) Der Bundesminister für Inneres kann bei Erfüllung der Voraussetzungen gemäß § 9 für jeden Sektor (§ 2) eine Einrichtung zur Wahrnehmung der Aufgaben gemäß Abs. 1 ermächtigen (sektorspezifisches CSIRT). Solange kein sektorspezifisches CSIRT besteht, hat das nationale CSIRT

(Abs. 2) die Aufgaben des jeweiligen sektorspezifischen CSIRTs für den jeweiligen Sektor wahrzunehmen.

(4) Das beim Bundesminister für Inneres eingerichtete GovCERT hat als sektorspezifisches CSIRT (Abs. 3) die Aufgaben gemäß Abs. 1 für die Einrichtungen im Sektor der öffentlichen Verwaltung (§ 24 Abs. 3) wahrzunehmen. Solange kein nationales CSIRT besteht, hat das GovCERT die Aufgaben des nationalen CSIRTs (Abs. 2) wahrzunehmen.

(5) Der Bundesminister für Inneres hat die Entscheidung über die Ermächtigung des nationalen CSIRTs (Abs. 2) sowie sektorspezifischer CSIRTs (Abs. 3) in einer Weise kundzumachen, die geeignet scheint, einen möglichst weiten Adressatenkreis zu erreichen.

(6) Dem nationalen CSIRT gebührt vom Bund ein pauschalierter Ersatz für die bei Erfüllung ihrer Aufgaben gemäß Abs. 1 entstandenen Aufwendungen.

(7) Sektorspezifische CSIRTs (Abs. 3 und 4) sind ermächtigt, für Zwecke des Abs. 1 Z 2 und 4 auf Ersuchen einer wesentlichen oder wichtigen Einrichtung Daten gemäß § 17 Abs. 2 zweiter Satz, die durch eine bei dieser Einrichtung eingerichtete IKT-Lösung gemäß § 17 Abs. 2 erster Satz gewonnen wurden, zu analysieren.

(8) Die CSIRTs haben mit sektorspezifischen oder sektorübergreifenden Zusammenschlüssen wesentlicher und wichtiger Einrichtungen zusammenzuarbeiten und mit diesen gemäß § 36 gegebenenfalls einschlägige Informationen auszutauschen.

(9) Die CSIRTs sind ermächtigt, Kooperationsbeziehungen mit CSIRTs und gleichwertigen Stellen oder Sicherheitsdienstleistern in Drittländern aufzunehmen. Es sind einschlägige Regeln und Verfahren für den wirksamen, effizienten und sicheren Informationsaustausch, einschließlich des Traffic Light Protocol, zu verwenden.

(10) Die Cybersicherheitsbehörde hat der Europäischen Kommission unverzüglich die Identität der CSIRTs gemäß Abs. 2 bis 4 und des als Koordinator gemäß § 11 Abs. 1 benannten CSIRTs, ihre jeweiligen Aufgaben in Bezug auf wesentliche und wichtige Einrichtungen sowie allfällige Änderungen dieser Angaben mitzuteilen.

(11) CSIRTs können die Aufgaben gemäß Abs. 1 Z 2 bis 4 auch gegenüber sonstigen Einrichtungen oder Personen wahrnehmen, sofern diese von einem Risiko oder einem Cybersicherheitsvorfall betroffen sind.

Anforderungen und Eignung von CSIRTs

§ 9. (1) Die CSIRTs (§ 8 Abs. 2 bis 4) haben die zur Erfüllung der Aufgaben gemäß § 8 Abs. 1 erforderlichen technischen und organisatorischen Fähigkeiten aufzuweisen und müssen zur Gewährleistung einer angemessenen Personalausstattung über ausreichende Ressourcen und geeignetes Personal verfügen. Die Ermächtigung darf nur vertrauenswürdigen Personen verliehen werden. Die CSIRTs haben jedenfalls folgende Anforderungen zu erfüllen:

1. ihre Kommunikationskanäle weisen einen hohen Grad an Sicherheit, Belastbarkeit und Verfügbarkeit auf, indem punktuellen Ausfällen vorgebeugt und mehrere Kanäle bereitgestellt werden, damit sie jederzeit erreichbar bleiben und die Möglichkeit besteht, proaktiv mit anderen Kontakt aufzunehmen; sie legen die Kommunikationskanäle genau fest und machen sie den wesentlichen und wichtigen Einrichtungen, sonstigen Einrichtungen sowie den Kooperationspartnern bekannt;
2. sie verfügen über ein geeignetes System zur Verwaltung und Weiterleitung von Anfragen, insbesondere über ein für den effizienten Informationsaustausch geeignetes System;
3. sie stellen die Vertraulichkeit und Vertrauenswürdigkeit ihrer Tätigkeiten sicher;
4. sie verfügen über entsprechend geschultes Personal und können hinsichtlich der Ausstattung eine ständige Bereitschaft ihrer Dienste gewährleisten;
5. sie verfügen über Redundanzsysteme und Ausweicharbeitsräume, um die Kontinuität ihrer Dienste sicherzustellen;
6. sie setzen Risikomanagementmaßnahmen nach § 32 um und melden erhebliche Cybersicherheitsvorfälle gemäß § 34 der Cybersicherheitsbehörde;
7. ihre Mitarbeiter müssen sich einer Sicherheitsüberprüfung nach §§ 55 ff SPG für den Zugang zu geheimer Information unterzogen haben. Die Sicherheitsüberprüfung ist alle fünf Jahre zu wiederholen.

(2) CSIRTs gemäß § 8 Abs. 2 und 3 haben Änderungen hinsichtlich jener Umstände, die Voraussetzung für die Erteilung der Ermächtigung waren, unverzüglich dem Bundesminister für Inneres anzuzeigen.

(3) Zur Wahrnehmung ihrer gesetzlichen Aufgaben sind die CSIRTs verpflichtet, Kooperationsbeziehungen mit einschlägigen Interessenträgern des Privatsektors zu pflegen. Zur Erleichterung dieser Zusammenarbeit haben die CSIRTs die Annahme und Anwendung gemeinsamer oder standardisierter Vorgehensweisen, Klassifizierungssysteme und Taxonomien für

1. die Verfahren zur Bewältigung von Cybersicherheitsvorfällen,
2. das Krisenmanagement und
3. die koordinierte Offenlegung von Schwachstellen nach § 11 Abs. 1

zu fördern.

(4) Mitarbeiter von CSIRTs sind über bekanntgewordene Tatsachen und Erkenntnisse, die im Rahmen der Wahrnehmung ihrer Aufgaben nach § 8 auftreten und deren Geheimhaltung im Interesse der jeweiligen geprüften Einrichtungen geboten ist, zur Verschwiegenheit verpflichtet.

Aufsicht

§ 10. (1) CSIRTs gemäß § 8 Abs. 2 und 3 unterliegen hinsichtlich ihrer Tätigkeit der Aufsicht des Bundesministers für Inneres.

(2) Der Bundesminister für Inneres kann in Ausübung seines Aufsichtsrechts, insbesondere zur Wahrung sicherheitspolitischer Interessen, den CSIRTs allgemeine Weisungen oder Weisungen im Einzelfall erteilen.

(3) Weisungen an die CSIRTs sind schriftlich zu erteilen und zu begründen. Eine aus besonderen Gründen, insbesondere wegen Gefahr im Verzug, vorerst mündlich erteilte Weisung ist unverzüglich schriftlich nachzureichen.

(4) Die CSIRTs haben dem Bundesminister für Inneres alle zur Ausübung seines Aufsichtsrechts erforderlichen Auskünfte zu erteilen und die hiefür notwendigen Unterlagen zu übermitteln.

(5) Die CSIRTs haben dem Bundesminister für Inneres einen jährlichen Bericht über die gemäß § 8 Abs. 1 wahrgenommenen Aufgaben bis zum Ablauf des auf das Berichtsjahr folgenden Kalendermonats zu erstatten. Dieser Bericht ist ebenfalls dem Nationalrat zu übermitteln.

(6) Der Bundesminister für Inneres ist ermächtigt, jederzeit zu überprüfen, ob die Voraussetzungen für die Erteilung der Ermächtigung gemäß § 8 Abs. 2 und 3 noch gegeben sind und die Verpflichtungen gemäß § 9 eingehalten werden. Der Bundesminister für Inneres kann Anordnungen zur Behebung von Mängeln treffen, wobei diesen Anordnungen unverzüglich zu entsprechen ist. Werden die Aufgaben gemäß § 8 Abs. 1 nicht ordnungsgemäß besorgt oder wird gegen die Verpflichtungen gemäß § 9 verstoßen, kann der Bundesminister für Inneres den Ausschluss bestimmter Personen von dieser Tätigkeit anordnen.

(7) Der Bundesminister für Inneres kann zudem die Ermächtigung gemäß § 8 Abs. 2 und 3 widerrufen, wenn ein CSIRT eine Weisung gemäß Abs. 2 nicht befolgt oder eine Auskunft gemäß Abs. 4 nicht erteilt. Er ist zudem verpflichtet, die Ermächtigung zu widerrufen, wenn eine für die Erteilung der Ermächtigung erforderliche Voraussetzung gemäß § 9 Abs. 1 nicht mehr gegeben ist.

Koordinierte Offenlegung von Schwachstellen

§ 11. (1) Das nationale CSIRT (§ 8 Abs. 2) koordiniert die Offenlegung von Schwachstellen. Es fungiert dabei als vertrauenswürdiger Vermittler und erleichtert erforderlichenfalls die Interaktion zwischen der eine Schwachstelle meldenden natürlichen oder juristischen Person und dem Hersteller oder Anbieter der potentiell gefährdeten IKT-Produkte oder IKT-Dienste auf Ersuchen einer der beiden Seiten. Zu den Aufgaben des als Koordinator benannten nationalen CSIRT gehört es insbesondere,

1. die betreffenden Einrichtungen zu ermitteln und zu kontaktieren,
2. die natürlichen oder juristischen Personen, die eine Schwachstelle melden, zu unterstützen,
3. die Zeitpläne für die Offenlegung auszuhandeln und das Vorgehen bei Schwachstellen zu koordinieren, die mehrere Einrichtungen betreffen sowie
4. gegebenenfalls die sektorspezifischen CSIRTs zu informieren.

(2) Natürliche oder juristische Personen können dem nationalen CSIRT eine Schwachstelle auf Wunsch anonym melden. Das nationale CSIRT stellt sicher, dass in Bezug auf die gemeldete Schwachstelle sorgfältige Folgemaßnahmen durchgeführt werden können. Die Anonymität der die Schwachstelle meldenden natürlichen oder juristischen Person ist zu wahren.

(3) Wenn die gemeldete Schwachstelle erhebliche Auswirkungen auf Einrichtungen in mehreren Mitgliedstaaten der Europäischen Union haben könnte, hat das nationale CSIRT mit den anderen als Koordinatoren benannten CSIRTs innerhalb des CSIRTs-Netzwerks zusammen zu arbeiten.

(4) Über Schwachstellen, die eine qualifizierte elektronische Signaturerstellungseinheit, eine qualifizierte elektronische Siegelerstellungseinheit oder die vertrauenswürdigen Systeme eines Vertrauensdiensteanbieters betreffen, hat das nationale CSIRT unverzüglich, in jedem Fall aber innerhalb von 24 Stunden nach Kenntnisnahme der Schwachstelle, die Aufsichtsstelle gemäß § 12 des Signatur- und Vertrauensdienstegesetzes (SVG), BGBl. I Nr. 50/2016, zu informieren.

4. Abschnitt
Nationale Koordinierung

Cyber Sicherheit Steuerungsgruppe (CSS)

§ 12. (1) Die Cyber Sicherheit Steuerungsgruppe (CSS) wird als das zentrale strategisch koordinierende Organ der Cybersicherheit in Österreich unter der Leitung des Bundesministers für Inneres eingerichtet.

(2) Der CSS kommen folgende Aufgaben zu:

1. die Mitwirkung bei der Entwicklung und die Koordination der ÖSCS gemäß § 15 Abs. 1;
2. die Beobachtung der Umsetzung der ÖSCS (Monitoring);
3. die Mitwirkung bei der Erstellung eines jährlichen Berichts zur Cybersicherheit;
4. die Erstellung einer eigenen Geschäftsordnung.

(3) Die CSS setzt sich aus fachkundigen Vertretern der im Nationalen Sicherheitsrat vertretenen Bundesminister, denen vom jeweiligen Bundesminister Angelegenheiten zur selbständigen Behandlung übertragen wurden, zusammen. Ferner gehören ihr die für Telekommunikation und Digitalisierung zuständigen Bundesminister an. Themenorientiert kann die CSS um Vertreter zusätzlicher Einrichtungen im Sektor der öffentlichen Verwaltung zur Teilnahme erweitert werden, insbesondere wenn diese selbst oder ihr Wirkungsbereich von Maßnahmen der ÖSCS betroffen sind.

Innerer Kreis der Operativen Koordinierungsstruktur (IKDOK)

§ 13. (1) Zur Erörterung und Aktualisierung des von der Cybersicherheitsbehörde erstellten Lagebildes über Risiken, Cyberbedrohungen und Cybersicherheitsvorfälle sowie zur Erörterung der Erkenntnisse, die gemäß § 17 Abs. 2 und 3 gewonnen wurden, wird der IKDOK eingerichtet.

(2) Im Rahmen des IKDOK können klassifizierte Informationen zwischen den Teilnehmern zur Wahrnehmung der Aufgaben nach Maßgabe ihrer Zuständigkeiten ausgetauscht werden.

Operative Koordinierungsstruktur (OpKoord)

§ 14. (1) Zur Erörterung eines gesamtheitlichen Lagebildes wird eine Operative Koordinierungsstruktur („OpKoord“) eingerichtet. Diese setzt sich aus dem IKDOK und den CSIRTs zusammen.

(2) Die OpKoord kann um Vertreter von wesentlichen und wichtigen Einrichtungen sowie sonstigen Einrichtungen erweitert werden, wenn deren Wirkungsbereich von einem Cybersicherheitsvorfall, einer Cyberbedrohung oder einem Beinahe-Vorfall betroffen ist („erweiterter OpKoord“).

(3) Alle Teilnehmer der OpKoord, soweit es sich nicht um die im IKDOK vertretenen Einrichtungen handelt, sind über die ihnen aufgrund der Teilnahme bekanntgewordenen Informationen zur Verschwiegenheit verpflichtet, sofern dies für eine Sitzung oder einzelne Umstände nicht anders beschlossen wurde.

(4) Die Teilnehmer des IKDOK können einvernehmlich nähere Regelungen über das Zusammenwirken der Teilnehmer des IKDOK und der OpKoord, insbesondere über die Einberufung von Sitzungen und die Zusammensetzung in einer Geschäftsordnung, treffen.

(5) Die an der OpKoord teilnehmenden Einrichtungen dürfen die zum Zweck der Organisation der OpKoord und die zur Wahrnehmung der Aufgaben gemäß Abs. 1 erforderlichen personenbezogenen Daten gemäß § 42 Abs. 2 verarbeiten.

Nationale Cybersicherheitsstrategie

§ 15. (1) Die Cybersicherheitsbehörde hat die Erstellung der Österreichischen Strategie für Cybersicherheit (ÖSCS) unter Einbindung der CSS zu koordinieren. Die ÖSCS wird von der Bundesregierung erlassen.

(2) Die ÖSCS bestimmt insbesondere die strategischen Ziele, die zur Erreichung dieser Ziele erforderlichen Ressourcen sowie angemessene politische und regulatorische Maßnahmen zur Erreichung und Aufrechterhaltung eines hohen Cybersicherheitsniveaus im Bundesgebiet.

(3) Die ÖSCS hat jedenfalls zu enthalten:

1. Ziele und Prioritäten der nationalen Cybersicherheitsstrategie, die insbesondere die in den Anlagen 1 und 2 angeführten Sektoren abdecken;
2. einen Steuerungsrahmen zur Verwirklichung der unter Z 1 dieses Absatzes genannten Ziele und Prioritäten, der die in Abs. 2 genannten Konzepte umfasst;
3. einen Steuerungsrahmen, in dem die Aufgaben und Zuständigkeiten der jeweiligen Interessenträger auf nationaler Ebene klargestellt, die Zusammenarbeit und Koordinierung auf nationaler Ebene zwischen der Cybersicherheitsbehörde, der zentralen Anlaufstelle und der CSIRTs sowie die Koordinierung und Zusammenarbeit zwischen diesen Stellen und nach sektorspezifischen Rechtsakten der Europäischen Union zuständigen Behörden untermauert werden;
4. einen Maßnahmenkatalog zur Förderung der Achtung des Völkerrechts, Stärkung freiwilliger Normen, Regeln und Prinzipien des verantwortungsvollen Staatenverhaltens sowie der Vertrauensbildung im Cyberraum im Wege der Cyberdiplomatie auf bilateraler und multilateraler Ebene;
5. einen Plan zur Umsetzung der Aufgaben des Bundesministers für europäische und internationale Angelegenheiten im Bereich der Cyber-Außenpolitik;
6. einen Mechanismus zur Ermittlung von relevanten Anlagen und eine Bewertung der nationalen Cybersicherheitsrisiken;
7. die Bestimmung von Maßnahmen zur Gewährleistung der Vorsorge, Reaktionsfähigkeit und Wiederherstellung bei Cybersicherheitsvorfällen, einschließlich der Zusammenarbeit zwischen dem öffentlichen und dem privaten Sektor;
8. eine Liste der verschiedenen Behörden und Interessenträger, die an der Umsetzung der nationalen Cybersicherheitsstrategie beteiligt sind;
9. einen politischen Rahmen für eine verstärkte Koordinierung zwischen der Cybersicherheitsbehörde und jener Behörde, die in Umsetzung des Art. 9 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 (im Folgenden: Richtlinie (EU) 2022/2557) national als zuständige Behörde benannt oder eingerichtet wurde, zum Zweck des Informationsaustauschs über Risiken, Cyberbedrohungen und Cybersicherheitsvorfälle sowie über nicht cyberbezogene Risiken, Bedrohungen und Sicherheitsvorfälle und für die Wahrnehmung von Aufsichtsaufgaben;
10. einen Plan, einschließlich erforderlicher Maßnahmen, zur Steigerung des allgemeinen Grads der Sensibilisierung für Cybersicherheit bei Bürgerinnen und Bürgern;
11. einen nationalen Plan für die Reaktion auf Cybersicherheitsvorfälle großen Ausmaßes nach § 16 Abs. 3;
12. einen Plan zum langfristigen Kompetenzaufbau im Bereich der Cybersicherheit unter Berücksichtigung von insbesondere den Aspekten Forschung, Technologie und Innovation;
13. einen Plan für Maßnahmen zur Unterstützung des Kapazitätenaufbaus von Drittstaaten in Schwerpunktregionen im Bereich der Cybersicherheit.

(4) Im Rahmen der ÖSCS sind insbesondere Konzepte enthalten,

1. für die Cybersicherheit in der Lieferkette für IKT-Produkte und IKT-Dienste, die von Einrichtungen für die Erbringung ihrer Dienste genutzt werden,
2. für die Aufnahme und Spezifikation cybersicherheitsbezogener Anforderungen an IKT-Produkte und IKT-Dienste bei der Vergabe öffentlicher Aufträge, einschließlich hinsichtlich der Zertifizierung der Cybersicherheit, der Verschlüsselung und der Nutzung quelloffener Cybersicherheitsprodukte,
3. für das Vorgehen bei Schwachstellen, das die Förderung und Erleichterung der koordinierten Offenlegung von Schwachstellen nach § 11 Abs. 1 umfasst,
4. im Zusammenhang mit der Aufrechterhaltung der allgemeinen Verfügbarkeit, Integrität und Vertraulichkeit des öffentlichen Kerns des offenen Internets,
5. zur Förderung der Entwicklung und Integration einschlägiger fortgeschrittener Technologien, damit Risikomanagementmaßnahmen im Bereich der Cybersicherheit auf dem neuesten Stand zur Anwendung gelangen,

6. zur Förderung und Entwicklung der allgemeinen und beruflichen Bildung im Bereich der Cybersicherheit, von Kompetenzen, Sensibilisierungsmaßnahmen, Forschungs- und Entwicklungsinitiativen im Bereich der Cybersicherheit sowie der Anleitung zu guten Vorgehensweisen und Kontrollen im Bereich der Cyberhygiene für Bürgerinnen und Bürger, Interessenträger und Einrichtungen,
7. zur Unterstützung von Hochschul- und Forschungseinrichtungen bei der Entwicklung, der Verbesserung des Einsatzes von Cybersicherheitsinstrumenten und sicherer Netzinfrastruktur,
8. mit einschlägigen Verfahren und geeigneten Instrumenten für den Informationsaustausch, um den freiwilligen Austausch von Cybersicherheitsinformationen zwischen Einrichtungen im Einklang mit dem Recht der Europäischen Union zu unterstützen,
9. zur Stärkung des Grundniveaus für Cyberresilienz und Cyberhygiene kleiner und mittlerer Unternehmen (KMU), durch Bereitstellung leicht zugänglicher Orientierungshilfen und Unterstützung für ihre spezifischen Bedürfnisse und
10. zur Förderung eines aktiven Cyberschutzes.

(5) Die Cybersicherheitsbehörde übermittelt der Europäischen Kommission sowie dem Nationalrat die ÖSCS innerhalb von drei Monaten nach ihrem Erlass. Davon sind jedoch jene Bereiche auszunehmen, deren Verbreitung die nationale Sicherheit gefährden könnte.

(6) Die Bundesregierung bewertet die ÖSCS regelmäßig, mindestens aber alle fünf Jahre, auf der Grundlage wesentlicher Leistungsindikatoren und aktualisiert diese erforderlichenfalls.

Management von Cybersicherheitsvorfällen großen Ausmaßes

§ 16. (1) Die Cybersicherheitsbehörde hat die Aufgaben für das Management von Cybersicherheitsvorfällen großen Ausmaßes wahrzunehmen.

(2) Zu diesem Zweck hat die Cybersicherheitsbehörde Kapazitäten, Mittel und Verfahren, die im Fall eines Cybersicherheitsvorfalls großen Ausmaßes eingesetzt werden können, zu ermitteln. Dabei hat sie das Lagebild, welches im Rahmen der Koordinierungsstrukturen (§§ 13 und 14) erstellt und aktualisiert wird zu berücksichtigen.

(3) Die Cybersicherheitsbehörde hat einen nationalen Plan für die Reaktion auf Cybersicherheitsvorfälle großen Ausmaßes zu verabschieden und diesen der CSS zur Berücksichtigung in der zu erstellenden nationalen Cybersicherheitsstrategie nach § 15 Abs. 3 Z 1 zu übermitteln. In diesem Plan wird insbesondere Folgendes beschrieben:

1. die Ziele der nationalen Vorsorgemaßnahmen und -tätigkeiten;
2. die Aufgaben und Zuständigkeiten der Behörden für das Management von Cybersicherheitsvorfällen großen Ausmaßes;
3. die Verfahren für das Management von Cybersicherheitsvorfällen großen Ausmaßes, einschließlich deren Integration in den nationalen Rahmen für das allgemeine Krisenmanagement, und die Kanäle für den Informationsaustausch;
4. die nationalen Vorsorgemaßnahmen, einschließlich Übungen und Ausbildungsmaßnahmen;
5. die einschlägigen öffentlichen und privaten Interessenträger und die betroffene Infrastruktur;
6. die zwischen den einschlägigen nationalen Behörden und Stellen vereinbarten nationalen Verfahren und Regelungen, die gewährleisten sollen, dass sich die Republik Österreich wirksam am koordinierten Management von Cybersicherheitsvorfällen großen Ausmaßes auf Ebene der Europäischen Union beteiligen und dieses unterstützen kann.

(4) Die Cybersicherheitsbehörde übermittelt die einschlägigen Informationen über den gemäß Abs. 3 erstellten Plan für die Reaktion auf Cybersicherheitsvorfälle großen Ausmaßes sowohl an die Europäische Kommission als auch an das EU-CyCLONe. Davon sind jedoch jene Bereiche auszunehmen, deren Verbreitung die nationale Sicherheit gefährden könnte.

5. Abschnitt
IKT-Lösungen

Betrieb von IKT-Lösungen

§ 17. (1) Der Bundesminister für Inneres hat für die Erfüllung seiner behördlichen Aufgaben nach diesem Bundesgesetz IKT-Lösungen zu betreiben.

(2) Der Bundesminister für Inneres ist zur Erfüllung der Aufgabe gemäß § 4 Abs. 1 Z 4 ermächtigt, IKT-Lösungen zu betreiben, die Risiken, Cyberbedrohungen oder Cybersicherheitsvorfälle von Netz- und Informationssystemen frühzeitig erkennen. Wesentliche und wichtige Einrichtungen können an den vom

Bundesminister für Inneres betriebenen IKT-Lösungen teilnehmen und festlegen, welche Daten an den Bundesminister für Inneres übermittelt werden. Für die Teilnahme an den IKT-Lösungen gebührt dem Bund als Ersatz ein Pauschalbetrag, der nach Maßgabe der durchschnittlichen Kosten mit Verordnung des Bundesministers für Inneres festgelegt wird.

(3) Der Bundesminister für Inneres ist zur Erfüllung der Aufgabe gemäß § 4 Abs. 1 Z 4 ermächtigt, IKT-Lösungen zu betreiben oder nach Einwilligung der betroffenen Einrichtung zu nutzen, um die Muster von Angriffen auf Netz- und Informationssysteme zu erkennen. Ebenso ist das GovCERT zum Betrieb solcher IKT-Lösungen zwecks Wahrnehmung der Aufgaben gemäß § 8 Abs. 1 Z 1, 2 und 4 ermächtigt und darf die daraus gewonnenen personenbezogenen technischen Daten als datenschutzrechtlicher Verantwortlicher gemäß Art. 4 Nr. 7 der Verordnung (EU) 2016/679 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (DSGVO), ABl. Nr. L 119 vom 04.05.2016 S. 1, zuletzt berichtigt durch ABl. Nr. L 74 vom 04.03.2021 S. 35, und § 36 Abs. 2 Z 8 des Datenschutzgesetzes (DSG), BGBl. I Nr. 165/1999 verarbeiten.

Meldeanalysesystem

§ 18. (1) Für die Analyse von Meldungen über Risiken, Cyberbedrohungen und Cybersicherheitsvorfälle gemäß §§ 34 und 37 sowie von Erkenntnissen, die gemäß § 17 gewonnen wurden, hat der Bundesminister für Inneres IKT-Lösungen zu betreiben und dem Bundeskanzler und dem Bundesminister für Landesverteidigung bereitzustellen, um die Bewertung von Risiken, Cyberbedrohungen und Cybersicherheitsvorfällen sowie die Erstellung eines Lagebilds mittels strategischer oder operativer Analyse zu unterstützen.

(2) Für die IKT-Lösungen und IT-Verfahren des Abs. 1 sind der Bundesminister für Inneres, der Bundeskanzler und der Bundesminister für Landesverteidigung gemeinsam datenschutzrechtliche Verantwortliche gemäß Art. 4 Nr. 7 in Verbindung mit Art. 26 DSGVO sowie § 47 DSG.

(3) Macht eine betroffene Person ihre Rechte gemäß den Bestimmungen des Kapitels 3 DSGVO oder §§ 42 bis 45 DSG geltend, so haben die gemeinsam datenschutzrechtlichen Verantwortlichen dies einander unverzüglich mitzuteilen. Jeder der gemeinsam datenschutzrechtlichen Verantwortlichen hat bezüglich der von ihm erhobenen und verarbeiteten Daten die Pflichten in Zusammenhang mit den Rechten betroffener Personen selbstständig wahrzunehmen.

IKDOK-Plattform

§ 19. (1) Der Bundesminister für Inneres kann für die Organisation des IKDOK und zur Wahrnehmung der Aufgaben gemäß § 13 Abs. 1 eine IKT-Lösung betreiben. Im Falle des Betriebs einer solchen ist sie dem Bundeskanzler, dem Bundesminister für Landesverteidigung und dem Bundesminister für europäische und internationale Angelegenheiten bereitzustellen.

(2) Für die IKT-Lösung des Abs. 1 sind der Bundesminister für Inneres, der Bundeskanzler, der Bundesminister für Landesverteidigung und der Bundesminister für europäische und internationale Angelegenheiten gemeinsam datenschutzrechtliche Verantwortliche gemäß Art. 4 Nr. 7 in Verbindung mit Art. 26 DSGVO sowie § 47 DSG.

(3) Macht eine betroffene Person ihre Rechte gemäß den Bestimmungen des Kapitels 3 DSGVO oder §§ 42 bis 45 DSG geltend, so haben die gemeinsam datenschutzrechtlichen Verantwortlichen dies einander unverzüglich mitzuteilen. Jeder der gemeinsam datenschutzrechtlichen Verantwortlichen hat bezüglich der von ihm erhobenen und verarbeiteten Daten die Pflichten in Zusammenhang mit den Rechten betroffener Personen selbstständig wahrzunehmen.

6. Abschnitt
Zusammenarbeit auf nationaler, Unions- und internationaler Ebene

Zusammenarbeit auf nationaler Ebene

§ 20. (1) Die Cybersicherheitsbehörde und die CSIRTs arbeiten bei der Erfüllung ihrer Aufgaben nach diesem Bundesgesetz zusammen.

(2) Die Cybersicherheitsbehörde hat für die Erfüllung ihrer gesetzlichen Aufgaben und Pflichten nach diesem Bundesgesetz insbesondere mit

1. den Strafverfolgungsbehörden,
2. den Behörden, die das Luftfahrtsicherheitsgesetz 2011 (LSG 2011), BGBl. I Nr. 111/2010 vollziehen sowie den Behörden, die als zuständige nationale Aufsichtsbehörde oder zuständige

nationale Behörde im Sinne der Verordnung (EU) 2018/1139 sowie deren delegierte Rechtsakte und Durchführungsrechtsakte benannt sind,

3. den Behörden, welche innerstaatlich die Einhaltung der Verordnung (EU) 2022/2554 sicherstellen,
4. der Aufsichtsstelle gemäß § 12 des Signatur- und Vertrauensdienstegesetzes (SVG), BGBl. I Nr. 50/2016,
5. der nationalen Regulierungsbehörde nach § 194 TKG 2021 sowie
6. der KommAustria nach § 199 TKG 2021

zusammenzuarbeiten und kann in diesem Zusammenhang Informationen über relevante Umstände austauschen, soweit diese im Aufgabenbereich der jeweiligen Behörden liegen und dies der Erhöhung der Cybersicherheit dient.

(3) Die Cybersicherheitsbehörde arbeitet mit der gemäß Richtlinie (EU) 2022/2557 zuständigen Behörde hinsichtlich der Identifizierung kritischer Einrichtungen im Sinne der Richtlinie (EU) 2022/2557, zu Risiken, Cyberbedrohungen und Cybersicherheitsvorfällen sowie zu nicht cyberbezogenen Risiken, Bedrohungen und Sicherheitsvorfällen zusammen und tauschen Informationen zu den als Reaktion ergriffenen Maßnahmen und darüberhinausgehende Informationen aus.

(4) Die Cybersicherheitsbehörde hat vor der Durchführung von Aufsichts- und Durchsetzungsmaßnahmen gegenüber Einrichtungen, die gemäß § 24 Abs. 1 Z 1 lit. f als wesentliche Einrichtungen gelten, jene Behörde, die in Umsetzung von Art. 9 der Richtlinie (EU) 2022/2557 als zuständige Behörde benannt oder eingerichtet wurde, zu unterrichten.

(5) Die Cybersicherheitsbehörde hat auf Ersuchen jener Behörde, die in Umsetzung des Art. 9 Richtlinie (EU) 2022/2557 als zuständige Behörde benannt oder eingerichtet wurde, Aufsichts- und Durchsetzungsmaßnahmen gegenüber Einrichtungen auszuüben, die gemäß der Richtlinie (EU) 2022/2557 als kritische Einrichtungen eingestuft wurden.

(6) Die Cybersicherheitsbehörde hat vor der Durchführung von Aufsichts- und Durchsetzungsmaßnahmen gegenüber wesentlichen und wichtigen Einrichtungen, die als IKT-Drittanbieter gemäß Art. 31 der Verordnung (EU) 2022/2554 benannt wurden, das gemäß Art. 32 Abs. 1 der Verordnung (EU) 2022/2554 eingerichtete Überwachungsforum zu unterrichten.

(7) Ein Informationsaustausch mit der Aufsichtsstelle gemäß Abs. 2 Z 4 hat jedenfalls in Angelegenheiten zu erfolgen, die Risiken, Cyberbedrohungen und Cybersicherheitsvorfälle eines Vertrauensdiensteanbieters oder Schwachstellen einer qualifizierten elektronischen Signaturerstellungseinheit, einer qualifizierten elektronischen Siegelerstellungseinheit oder der vertrauenswürdigen Systeme eines Vertrauensdiensteanbieters betreffen.

(8) Die Cybersicherheitsbehörde hat vor der Durchführung von Aufsichts- und Durchsetzungsmaßnahmen gegenüber Betreibern gemäß § 4 Z 25 TKG 2021 und Anbietern gemäß § 4 Z 36 TKG 2021 die nationale Regulierungsbehörde nach § 194 TKG 2021 und die KommAustria nach § 199 TKG 2021 zu unterrichten.

Zusammenarbeit mit der Datenschutzbehörde

§ 21. (1) Die Cybersicherheitsbehörde und die Datenschutzbehörde, unbeschadet ihrer Zuständigkeiten und Aufgaben nach der DSGVO und dem DSG, arbeiten bei der Bearbeitung und der Anordnung von Abwehr- und Abhilfemaßnahmen von Cybersicherheitsvorfällen, die zur Verletzung des Schutzes personenbezogener Daten im Sinne des Art. 4 Nr. 12 DSGVO und § 36 Abs. 2 Z 1 DSG führen, eng zusammen und tauschen relevante Informationen aus. Der Bundesminister für Inneres gewährt der Datenschutzbehörde zu diesem Zweck Zugang zum Register gemäß § 29.

(2) Besteht Grund zur Annahme, dass ein Verstoß einer wesentlichen oder wichtigen Einrichtung gegen die in den §§ 32 und 34 festgelegten Verpflichtungen eine Verletzung des Schutzes personenbezogener Daten zur Folge hat, die gemäß Art. 33 DSGVO zu melden ist, hat die Cybersicherheitsbehörde unverzüglich, möglichst innerhalb von 72 Stunden, die Datenschutzbehörde zu unterrichten. Betrifft die Verletzung des Schutzes personenbezogener Daten Betroffene in einem anderen Mitgliedstaat der Europäischen Union, hat die Cybersicherheitsbehörde ebenfalls die Datenschutzbehörde zu unterrichten.

(3) Verhängt die Datenschutzbehörde gegen eine wesentliche oder wichtige Einrichtung aufgrund eines Cybersicherheitsvorfalles, der zur Verletzung des Schutzes personenbezogener Daten im Sinne des Art. 4 Nr. 12 DSGVO geführt hat, gemäß Art. 58 Abs. 2 Buchstabe i DSGVO eine Geldbuße, hat sie über diesen Umstand den Bundesminister für Inneres zu informieren und ihm eine Ausfertigung des Straferkenntnisses zu übersenden. Für den Fall, dass die Verwaltungsübertretung bereits von der

zuständigen Bezirksverwaltungsbehörde verfolgt wird, informiert die Cybersicherheitsbehörde die Bezirksverwaltungsbehörde über diesen Umstand.

Internationale Zusammenarbeit

§ 22. (1) Erbringt eine Einrichtung ihre Dienste in mehr als einem Mitgliedstaat der Europäischen Union oder erbringt sie ihre Dienste in einem oder mehreren Mitgliedstaaten und befinden sich ihre Netz- und Informationssysteme in einem oder mehreren anderen Mitgliedstaaten, arbeitet die Cybersicherheitsbehörde mit den zuständigen Behörden der betreffenden Mitgliedstaaten zusammen und unterstützt diese.

(2) Die Zusammenarbeit nach Abs. 1 umfasst dabei mindestens Folgendes:

1. über die zentralen Anlaufstellen unterrichtet die Cybersicherheitsbehörde die zuständigen Behörden in den anderen betreffenden Mitgliedstaaten über die Aufsichts- und Durchsetzungsmaßnahmen und konsultiert sie zu diesen;
2. die Cybersicherheitsbehörde kann eine andere zuständige Behörde ersuchen, Aufsichts- oder Durchsetzungsmaßnahmen zu ergreifen;
3. auf begründetes Ersuchen einer anderen zuständigen Behörde leistet die Cybersicherheitsbehörde der ersuchenden Behörde in einem ihren zur Verfügung stehenden Ressourcen angemessenen Umfang Rechtshilfeersuchen, damit die Aufsichts- oder Durchsetzungsmaßnahmen wirksam, effizient und kohärent durchgeführt werden können. Die Rechtshilfeersuchen kann die Erteilung von Auskünften und die Durchführung von Aufsichtsmaßnahmen, einschließlich der Durchführung von Vor-Ort-Kontrollen, externen Aufsichtsmaßnahmen und gezielten Überprüfungen umfassen.

(3) Die Cybersicherheitsbehörde darf ein Rechtshilfeersuchen nur ablehnen, wenn sie für die erbetene Rechtshilfe nicht zuständig ist, die ersuchte Rechtshilfe in keinem angemessenen Verhältnis zu ihren Aufsichtsaufgaben steht oder das Ersuchen Informationen betrifft oder Tätigkeiten umfasst, deren Offenlegung oder Ausführung wesentlichen Interessen im Bereich der nationalen Sicherheit, der öffentlichen Sicherheit oder der Landesverteidigung zuwiderlaufen würde. Bevor die Cybersicherheitsbehörde einen solchen Antrag ablehnt, konsultiert sie die anderen betreffenden zuständigen Behörden sowie – auf Ersuchen eines der betreffenden Mitgliedstaaten – die Kommission und die ENISA.

(4) Die Cybersicherheitsbehörde kann, wenn dies gemäß Abs. 3 möglich und im gegenseitigen Einvernehmen geschieht, gemeinsame Aufsichtsmaßnahmen durchführen.

Peer Reviews

§ 23. (1) Die Cybersicherheitsbehörde kann an den in Art. 19 NIS-2-Richtlinie angeführten Peer Reviews teilnehmen. Diese Peer Reviews umfassen zumindest einen der folgenden Punkte:

1. den Stand der Umsetzung der Risikomanagementmaßnahmen und der Berichtspflichten gemäß §§ 32 und 34;
2. das Cybersicherheitsniveau der Kapazitäten, einschließlich der verfügbaren finanziellen, technischen und personellen Ressourcen, und die Wirksamkeit bei der Durchführung der Aufgaben der zuständigen Behörden;
3. die operativen Kapazitäten der CSIRTs;
4. den Stand der Umsetzung der Rechtshilfeersuchen gemäß § 22;
5. den Stand der Umsetzung der Vereinbarungen über den Austausch von Informationen im Bereich der Cybersicherheit gemäß § 36;
6. spezifische Fragen mit grenz- oder sektorübergreifendem Charakter.

(2) Die ENISA und die Kommission nehmen als Beobachter an den Peer Reviews teil.

(3) Vor Beginn der Peer Reviews ist gemeinsam der Umfang und die Zielsetzung festzulegen. Dabei ist insbesondere auf die Eignung der teilnehmenden Personen und etwaige Verschwiegenheit- oder Geheimhaltungspflichten Rücksicht zu nehmen. Die Cybersicherheitsbehörde stellt den beigezogenen Sachverständigen für Cybersicherheit die für die Bewertung erforderlichen Informationen zur Verfügung, vorbehaltlich der nationalen Rechtsvorschriften über den Schutz vertraulicher oder als Verschlusssache eingestufter Informationen und der Wahrung grundlegender Funktionen des Staates wie der nationalen Sicherheit. Sämtliche durch die Peer Reviews erlangten Informationen dürfen nur zu diesem Zweck verwendet werden. Die an dem Peer Review beteiligten Sachverständigen für Cybersicherheit geben keine sensiblen oder vertraulichen Informationen, die im Laufe des Peer Reviews erlangt wurden, an Dritte weiter.

(4) Die Cybersicherheitsbehörde kann, wenn sie Gegenstand des Peer Review ist, unter Mitteilung stichhaltiger Gründe Einwände gegen die Benennung bestimmter Sachverständiger für Cybersicherheit erheben.

(5) Die an Peer Reviews beteiligten Sachverständigen für Cybersicherheit erstellen Berichte über die Ergebnisse und Schlussfolgerungen der Peer Reviews. Zu den sie betreffenden Berichtsentwürfen kann die Cybersicherheitsbehörde Stellung nehmen; diese Stellungnahmen werden den Berichten beigefügt.

3. Hauptstück
Wesentliche und wichtige Einrichtungen und Einrichtungen, die Domänennamen-Registrierungsdienste erbringen

1. Abschnitt
Wesentliche und wichtige Einrichtungen

Wesentliche und wichtige Einrichtungen

§ 24. (1) Als wesentliche Einrichtungen gelten,

1. unabhängig von der Unternehmensgröße,
   a. qualifizierte Vertrauensdiensteanbieter,
   b. Namenregister der Domäne oberster Stufe (TLD Namenregister),
   c. Domänennamensystem-Diensteanbieter,
   d. Einrichtungen im Sektor der öffentlichen Verwaltung auf Bundesebene gemäß Abs. 4,
   e. Einrichtungen, die von der Cybersicherheitsbehörde als wesentliche Einrichtung eingestuft wurden (§ 26) sowie
   f. Einrichtungen, die als kritische Einrichtungen im Sinne der Richtlinie (EU) 2022/2557) ermittelt wurden;
2. Einrichtungen, die ein mittleres Unternehmen gemäß § 25 Abs. 3 betreiben und Anbieter öffentlicher elektronischer Kommunikationsnetze sowie Anbieter öffentlich zugänglicher elektronischer Kommunikationsdienste sind;
3. Einrichtungen der in Anlage 1 dieses Gesetzes genannten Art, die ein großes Unternehmen gemäß § 25 Abs. 2 betreiben.

(2) Als wichtige Einrichtung gelten

1. Einrichtungen der in den Anlagen 1 und 2 dieses Gesetzes genannten Art, die ein großes oder mittleres Unternehmen betreiben sowie
2. Einrichtungen im Sektor der öffentlichen Verwaltung auf Landesebene gemäß Abs. 5 und
3. unabhängig von ihrer Größe
   a. Anbieter von öffentlichen elektronischen Kommunikationsnetzen oder von öffentlich zugänglichen Kommunikationsdiensten,
   b. Vertrauensdiensteanbieter, und
   c. Einrichtungen, die von der Cybersicherheitsbehörde als wichtige Einrichtung eingestuft wurden (§ 26 Abs. 1)

   und diese Einrichtung nicht bereits eine wesentliche Einrichtung nach Abs. 1 ist.

(3) Einrichtungen im Sektor der öffentlichen Verwaltung sind Einrichtungen, die

1. zum Zweck eingerichtet wurden, im öffentlichen Interesse liegende Aufgaben nicht gewerblicher Art zu erfüllen,
2. der Aufsicht des Bundes oder eines Landes unterstehen oder an die Weisungen eines obersten Organs gebunden sind oder ein Leitungs- oder Aufsichtsorgan haben, das mehrheitlich aus Mitgliedern besteht, die von Bundes- oder Landesbehörden oder von anderen auf Bundes- oder Landesebene eingerichteten Körperschaften des öffentlichen Rechts eingesetzt worden sind, oder an denen der Bund oder ein Land mit mindestens 50 vH des Stamm-, Grund- oder Eigenkapitals beteiligt ist oder Mitglieder der Bundesregierung sind und
3. ermächtigt sind, im Rahmen ihrer gesetzlich übertragenen Aufgaben Bescheide zu erlassen, die Rechte Einzelner im grenzüberschreitenden Personen-, Waren, Dienstleistungs- oder Kapitalverkehr berühren,

mit Ausnahme der Gemeinden sowie Gemeindeverbände.

(4) Einrichtungen im Sektor der öffentlichen Verwaltung auf Bundesebene sind Einrichtungen gemäß Abs. 3, die zudem zur Besorgung von Angelegenheiten der Bundesverwaltung berufen sind und entweder als Bundesbehörden eingerichtet wurden oder Rechtspersönlichkeit besitzen.

(5) Einrichtungen im Sektor der öffentlichen Verwaltung auf Landesebene sind die Ämter der Landesregierungen und die Bezirkshauptmannschaften sowie Einrichtungen gemäß Abs. 3, die zudem zur Besorgung von Angelegenheiten der Landesverwaltung berufen sind und Rechtspersönlichkeit besitzen.

(6) Einrichtungen im Sektor der öffentlichen Verwaltung, deren Tätigkeiten überwiegend in den Bereichen nationale Sicherheit, öffentliche Sicherheit, militärische Landesverteidigung oder Strafverfolgung ausgeübt werden sowie Einrichtungen des Universitäts-, Hochschul- und Schulwesens, Einrichtungen der Gerichtsbarkeit, Einrichtungen der Gesetzgebung, einschließlich der Parlamentsdirektion sowie die Österreichische Nationalbank gelten nicht als wesentliche oder wichtige Einrichtungen. Für Vertrauensdiensteanbieter kommt dieser Absatz nicht zur Anwendung.

(7) Gegenüber Einrichtungen, die in den Anwendungsbereich der Verordnung (EU) 2022/2554 fallen, gehen die einschlägigen Bestimmungen dieser Verordnung und nationaler Durchführungsbestimmungen vor. Dies gilt auch für jene Einrichtungen, die gemäß Art. 2 Abs. 4 Verordnung (EU) 2022/2554 im Rahmen der innerstaatlichen Durchführung von deren Anwendungsbereich ausgenommen wurden.

(8) IKT-Drittdienstleister gemäß Art. 3 Nr. 23 der Verordnung (EU) 2022/2554 unterliegen auch den Bestimmungen dieses Bundesgesetzes.

Ermittlung der Unternehmensgröße

§ 25. (1) Die Einstufung einer Einrichtung als „mittleres Unternehmen“ oder als „großes Unternehmen“ richtet sich nach der Anzahl der Mitarbeiter, dem Jahresumsatz und der Jahresbilanzsumme. Diese Einstufung erfolgt unter Anwendung der Art. 1 bis 6 des Anhangs der Empfehlung der Kommission vom 06.05.2003 betreffend die Definition der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen, 2003/361/EG, ABl. Nr. L 124 vom 20.5.2003 S. 36, mit Ausnahme des Art. 3 Abs. 4 des Anhangs dieser Empfehlung.

(2) Eine Einrichtung gilt als „großes Unternehmen“, wenn sie zumindest 250 Mitarbeiter beschäftigt oder wenn sie einen Jahresumsatz von über 50 Millionen Euro erzielt und sich die Jahresbilanzsumme auf über 43 Millionen Euro beläuft.

(3) Eine Einrichtung gilt als „mittleres Unternehmen“, wenn sie zumindest 50 Mitarbeiter beschäftigt, oder wenn sie einen Jahresumsatz von über zehn Millionen Euro erzielt und sich die Jahresbilanzsumme auf über zehn Millionen Euro beläuft, sofern sie nicht bereits als großes Unternehmen gilt.

Größenunabhängige Einstufung als wesentliche oder wichtige Einrichtung

§ 26. (1) Die Cybersicherheitsbehörde hat eine Einrichtung der in den Anlagen 1 oder 2 genannten Art, die aufgrund ihrer Unternehmensgröße nicht als wesentlich oder als wichtig gilt, aus den in Abs. 3 genannten Gründen mit Bescheid als wesentliche Einrichtung oder als wichtige Einrichtung einzustufen.

(2) Die Cybersicherheitsbehörde hat eine wichtige Einrichtung mit Bescheid als wesentliche Einrichtung einzustufen, sofern dies aus den in Abs. 3 genannten Gründen geboten ist.

(3) Aus folgenden Gründen hat eine Einstufung einer Einrichtung als wesentliche Einrichtung oder als wichtige Einrichtung zu erfolgen:

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

Ausnahmen von Verpflichtungen für wesentliche oder wichtige Einrichtungen aufgrund sektorspezifischer Rechtsakte der Europäischen Union

§ 27. (1) Sofern wesentliche oder wichtige Einrichtungen aufgrund sektorspezifischer unionsrechtlicher Rechtsakte verpflichtet sind, entweder eigene Risikomanagementmaßnahmen zu ergreifen oder erhebliche Cybersicherheitsvorfälle zu melden und

1. die jeweiligen Bestimmungen dieser sektorspezifischen Rechtsakte ein zumindest gleichwertiges Cybersicherheitsniveau im Vergleich zu jenen nach diesem Bundesgesetz (§§ 32 und 34) gewährleisten und
2. der Bundesminister für Inneres diese Bestimmungen und deren Gleichwertigkeit durch Verordnung festgestellt hat,

gelten diese sektorspezifischen Bestimmungen anstelle der in diesem Bundesgesetz geregelten Bestimmungen.

(2) Bei Beurteilung der Gleichwertigkeit ist auf den Inhalt sowie den Zweck der sektorspezifischen unionsrechtlichen Bestimmungen sowie auf die potenziellen Auswirkungen der aufgrund dieser Bestimmungen zu ergreifenden Maßnahmen auf das Cybersicherheitsviveau Bedacht zu nehmen. Dabei sind insbesondere der Inhalt, der Umfang sowie die konkrete Ausgestaltung der sektorspezifischen Bestimmungen zu berücksichtigen.

Territorialität

§ 28. (1) Wesentliche und wichtige Einrichtungen sowie Einrichtungen, die Domänennamen-Registrierungsdienste erbringen, unterliegen den Bestimmungen dieses Hauptstücks nur hinsichtlich jener Niederlassungen, die sich in Österreich befinden.

(2) Abweichend von Abs. 1 gelten die Bestimmungen dieses Hauptstücks für folgende Einrichtungen nur unter den hier angeführten Bedingungen:

1. für Anbieter öffentlicher Kommunikationsnetze oder Anbieter öffentlich zugänglicher elektronischer Kommunikationsdienste, sofern sie ihre Dienste in Österreich erbringen;
2. für DNS-Diensteanbieter, TLD-Namenregister, Einrichtungen, die Domänennamen-Registrierungsdienste erbringen, Anbieter von Cloud-Computing-Diensten, Anbieter von Rechenzentrumsdiensten, Betreiber von Inhaltszustellnetzen, Anbieter von verwalteten Diensten, Anbieter von verwalteten Sicherheitsdiensten sowie Anbieter von Online-Marktplätzen, Online-Suchmaschinen oder Plattformen für Dienste sozialer Netzwerke, sofern sie
   a. ihre Hauptniederlassung in Österreich haben oder
   b. sie weder in Österreich, noch in einem anderen Mitgliedstaat der Europäischen Union einen Vertreter gemäß Abs. 4 bestellt haben;
3. für Einrichtungen im Sektor der öffentlichen Verwaltung im Sinne des § 24 Abs. 3, unabhängig ihres Niederlassungsortes innerhalb der Europäischen Union.

(3) Als Hauptniederlassung gemäß Abs. 2 Z 2 wird jeweils die Niederlassung in demjenigen Mitgliedstaat der Europäischen Union betrachtet, in dem die Entscheidungen im Zusammenhang mit den Risikomanagementmaßnahmen vorwiegend getroffen werden. Kann dies nicht eindeutig bestimmt werden oder werden solche Entscheidungen nicht in der Europäischen Union getroffen, so gilt als Hauptniederlassung der Mitgliedstaat, in dem die Risikomanagementmaßnahmen gesetzt werden. Kann dies nicht ermittelt werden, so gilt die Hauptniederlassung als in jenem Mitgliedstaat gelegen, in dem die betreffende Einrichtung die Niederlassung mit der höchsten Beschäftigtenzahl in der Europäischen Union hat.

(4) Hat eine wesentliche oder wichtige Einrichtung gemäß Abs. 2 Z 2 keine Niederlassung in der Europäischen Union, bietet aber Dienste innerhalb Österreichs an, muss sie einen Vertreter für Österreich benennen, sofern sie einen solchen nicht bereits in einem anderen Mitgliedstaat der Europäischen Union benannt hat. Wurde kein Vertreter benannt, gelten für die wesentliche oder wichtige Einrichtung die Bestimmungen nach diesem Hauptstück und die Cybersicherheitsbehörde kann nach dem 4. Abschnitt dieses Hauptstücks vorgehen.

(5) Die Benennung eines Vertreters durch eine in Abs. 2 Z 2 genannte Einrichtung lässt rechtliche Schritte, die gegen die Einrichtung selbst eingeleitet werden könnten, unberührt.

(6) Erhält die Cybersicherheitsbehörde von einem anderen Mitgliedstaat der Europäischen Union ein Rechtshilfeersuchen zu einer in den Abs. 1 und 2 genannten Einrichtung, die in Österreich Dienste anbietet oder ein Netz- und Informationssystem betreibt, kann sie innerhalb der Grenzen des Rechtshilfeersuchens geeignete Aufsichts- und Durchsetzungsmaßnahmen nach diesem Bundesgesetz in Bezug auf die betreffende Einrichtung ergreifen. § 22 gilt sinngemäß.

2. Abschnitt
Pflichten

Register der Einrichtungen

§ 29. (1) Die Cybersicherheitsbehörde führt ein Register der wesentlichen und wichtigen Einrichtungen sowie der Einrichtungen, die Domänennamen-Registrierungsdienste erbringen.

(2) Die in Abs. 1 genannten Einrichtungen, haben sich bei der Cybersicherheitsbehörde zu registrieren und folgende Angaben zu übermitteln:

1. den Namen der Einrichtung;
2. die Anschrift und aktuelle Kontaktdaten, einschließlich der E-Mail-Adressen und Telefonnummern sowie gegebenenfalls ihren gemäß § 28 Abs. 4 benannten Vertreter;
3. den Sektor, Teilsektor und die Art der Einrichtung gemäß Anlage 1 oder 2;
4. die Mitgliedstaaten der Europäischen Union, in denen sie Dienste erbringen;
5. gegebenenfalls die IP-Adressbereiche der Einrichtung;
6. die Anschrift der Hauptniederlassung der Einrichtung und ihrer sonstigen Niederlassungen in der Europäischen Union oder, falls sie nicht in der Europäischen Union niedergelassen ist, die Anschrift ihres nach § 28 Abs. 4 benannten Vertreters;
7. Informationen über die in § 25 angeführten Schwellenwerte und ob es sich um eine wesentliche oder wichtige Einrichtung handelt.

(3) Die Registrierung nach Abs. 2 hat innerhalb von drei Monaten ab Inkrafttreten des Gesetzes zu erfolgen. Einrichtungen, die erst nach diesem Zeitpunkt als wesentliche oder wichtige Einrichtungen gelten oder erst nach diesem Zeitpunkt Domänennamen-Registrierungsdienste erbringen, haben sich unverzüglich, in jedem Fall aber innerhalb von drei Monaten, zu registrieren.

(4) Die in Abs. 1 genannten Einrichtungen teilen der Cybersicherheitsbehörde Änderungen der Angaben

1. gemäß Abs. 2 Z 1, 2 und 3 unverzüglich, in jedem Fall aber innerhalb von zwei Wochen ab dem Tag der Änderung, und
2. gemäß Abs. 2 Z 4 bis 7 unverzüglich, in jedem Fall aber innerhalb von drei Monaten ab dem Tag der Änderung, mit.

(5) Der Bundesminister für Inneres legt in einer Verordnung die Anforderungen an die Angaben gemäß Abs. 2 fest, einschließlich der Art der Übermittlung sowie der Verwendung bestimmter Formulare.

(6) Die zentrale Anlaufstelle leitet die in Abs. 2 genannten Angaben, mit Ausnahme der in Abs. 2 Z 5 und Z 7 genannten Angaben, von DNS-Diensteanbietern, TLD-Namenregistern, Einrichtungen, die Domänennamen-Registrierungsdienste erbringen, Anbietern von Cloud-Computing-Diensten, Anbietern von Rechenzentrumsdiensten, Betreibern von Inhaltszustellnetzen, Anbietern von verwalteten Diensten, Anbietern von verwalteten Sicherheitsdiensten sowie Anbietern digitaler Dienste nach deren Erhalt unverzüglich an die ENISA weiter.

(7) Die Einrichtung hat die Erreichbarkeit über die Kontaktdaten gemäß Abs. 2 Z 2 jedenfalls für jenen Zeitraum sicherzustellen, in dem sie ihre Dienste zur Verfügung stellt.

Datenbank der Domänennamen-Registrierungsdaten

§ 30. (1) Die TLD-Namenregister und die Einrichtungen, die Domänennamen-Registrierungsdienste erbringen, haben in einer eigenen Datenbank genaue und vollständige Domänennamen-Registrierungsdaten zu sammeln.

(2) Eine Datenbank gemäß Abs. 1 hat die erforderlichen Angaben zu enthalten, anhand derer die Inhaber der Domänennamen und die Kontaktstellen, die die Domänennamen im Rahmen der TLD verwalten, identifiziert und kontaktiert werden können. Diese Angaben müssen die folgenden Informationen umfassen:

1. den Domänennamen;
2. das Datum der Registrierung;
3. den Namen des Domäneninhabers, seine E-Mail-Adresse und Telefonnummer;
4. die Kontakt-E-Mail-Adresse und die Telefonnummer der Anlaufstelle, die den Domänennamen verwaltet, falls diese sich von denen des Domäneninhabers unterscheiden.

(3) Die TLD-Namenregister und die Einrichtungen, die Domänennamen-Registrierungsdienste erbringen, haben Vorgaben und Verfahren, einschließlich Überprüfungsverfahren, zu etablieren, mit

denen sichergestellt wird, dass Datenbanken gemäß Abs. 1 genaue und vollständige Angaben enthalten, und diese Vorgaben und Verfahren öffentlich zugänglich zu machen.

(4) Die TLD-Namenregister und Einrichtungen, die Domänennamen-Registrierungsdienste erbringen, haben unverzüglich nach der Registrierung eines Domänennamens die nicht personenbezogenen Domänennamen-Registrierungsdaten öffentlich zugänglich zu machen.

(5) Die TLD-Namenregister und die Einrichtungen, die Domänennamen-Registrierungsdienste erbringen, haben auf rechtmäßige und hinreichend begründete Anträge aller Einrichtungen Zugang zu den erfragten Domänennamen-Registrierungsdaten zu gewähren. Die TLD-Namenregister und Einrichtungen, die Domänennamen-Registrierungsdienste erbringen, haben die Vorgaben und Verfahren im Hinblick auf die Offenlegung solcher Daten öffentlich zugänglich zu machen und alle Anträge auf Zugang unverzüglich und in jedem Fall innerhalb von 72 Stunden nach Eingang eines Antrags zu beantworten.

(6) Die Einhaltung der in den Abs. 1 bis 5 festgelegten Verpflichtungen darf nicht zu einer doppelten Erhebung von Domänennamen-Registrierungsdaten führen, außer dies ist technisch nicht anders möglich. Zu diesem Zweck haben die TLD-Namenregister und die Einrichtungen, die Domänennamen-Registrierungsdienste erbringen, miteinander zusammenzuarbeiten.

Governance

§ 31. (1) Die Leitungsorgane wesentlicher und wichtiger Einrichtungen haben die Einhaltung der Risikomanagementmaßnahmen nach § 32 sicherzustellen und zu beaufsichtigen.

(2) Leitungsorgane, die ihre Pflichten nach Abs. 1 verletzen, haften der Einrichtung für den schuldhaft verursachten Schaden, sofern sie nicht ohnehin den Bestimmungen des Organhaftpflichtgesetzes (OrgHG), BGBl. Nr. 181/1967, unterliegen.

(3) Die Leitungsorgane wesentlicher und wichtiger Einrichtungen müssen an für diese spezifisch gestalteten Cybersicherheitsschulungen teilnehmen. Die Einrichtungen haben den Mitarbeitern regelmäßig entsprechende Schulungen anzubieten, damit diese 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 erwerben können.

Risikomanagementmaßnahmen im Bereich der Cybersicherheit

§ 32. (1) Wesentliche und wichtige Einrichtungen haben geeignete und verhältnismäßige technische, operative und organisatorische Risikomanagementmaßnahmen in den Bereichen der Anlage 3 umzusetzen, 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 Cybersicherheitsvorfällen auf die Empfänger ihrer Dienste und auf andere Dienste zu verhindern oder möglichst gering zu halten.

(2) Diese Risikomanagementmaßnahmen haben

1. ein dem bestehenden Risiko angemessenes Cybersicherheitsniveau zu gewährleisten, unter Berücksichtigung
   a. des Stands der Technik und gegebenenfalls der einschlägigen nationalen, europäischen und internationalen Normen sowie Best-Practices sowie
   b. der Kosten der Umsetzung;
2. auf einem gefahrenübergreifenden Ansatz zu beruhen, der auf den Schutz von Netz- und Informationssystemen und deren physischer Umwelt vor Cybersicherheitsvorfällen abzielt sowie
3. zur Sicherheit der Lieferketten
   a) die spezifischen Schwachstellen der einzelnen unmittelbaren Anbieter und Diensteanbieter, die Gesamtqualität der Produkte und der Cybersicherheitspraxis ihrer Anbieter und Dienstanbieter, einschließlich der Sicherheit ihrer Entwicklungsprozesse sowie
   b) die Ergebnisse der gemäß Art. 22 Abs. 1 NIS-2-Richtlinie durchgeführten koordinierten Risikobewertungen in Bezug auf die Sicherheit kritischer Lieferketten,

gebührend zu berücksichtigen.

(3) Bei der Bewertung der Verhältnismäßigkeit der Risikomanagementmaßnahmen nach Abs. 1 sind das Ausmaß der Risikoexposition der Einrichtung sowie ihrer Dienste, die Größe der Einrichtung und die Wahrscheinlichkeit des Eintretens von Cybersicherheitsvorfällen und deren Schwere, einschließlich ihrer gesellschaftlichen und wirtschaftlichen Auswirkungen, gebührend zu berücksichtigen.

(4) Der Bundesminister für Inneres hat mit Verordnung Risikomanagementmaßnahmen in den Bereichen der Anlage 3 hinsichtlich technischer, operativer und organisatorischer Anforderungen

festzulegen. Ferner kann der Bundesminister für Inneres sektorspezifische Anforderungen an diese Risikomanagementmaßnahmen mit Verordnung festlegen.

Nachweis der Wirksamkeit von Risikomanagementmaßnahmen

§ 33. (1) Wesentliche und wichtige Einrichtungen haben innerhalb von sechs Monaten nach Aufforderung durch die Cybersicherheitsbehörde dieser eine Aufstellung umgesetzter Risikomanagementmaßnahmen gemäß § 32 zu übermitteln (Selbstdeklaration).

(2) Wesentliche Einrichtungen haben innerhalb von drei Jahren nach Aufforderung zur Selbstdeklaration, frühestens jedoch sechs Monate vor Ablauf dieser Frist, die Umsetzung der Risikomanagementmaßnamen gemäß § 32 gegenüber der Cybersicherheitsbehörde mittels einer Prüfung durch eine unabhängige Stelle nachzuweisen. Zu diesem Zweck übermittelt die jeweilige wesentliche Einrichtung der Cybersicherheitsbehörde einen von vertretungsbefugten Leitungsorganen der wesentlichen Einrichtung und der unabhängigen Stelle sowie den eingesetzten unabhängigen Prüfern unterzeichneten Prüfbericht über die Wirksamkeit der Umsetzung der Risikomanagementmaßnahmen gemäß § 32 einschließlich dabei festgestellter Mängel und einen diese Mängel adressierenden Maßnahmenplan.

(3) Die Cybersicherheitsbehörde kann wichtige Einrichtungen bei Vorliegen von Nachweisen, wie insbesondere einer Selbstdeklaration, oder sonstigen begründeten Hinweisen und Informationen, die nahelegen, dass eine wichtige Einrichtung ihren Verpflichtungen nach diesem Bundesgesetz wie insbesondere §§ 32 und 34 nicht nachkommt, auffordern, die Umsetzung der Risikomanagementmaßnahmen gemäß § 32 gegenüber der Cybersicherheitsbehörde mittels einer Prüfung durch eine unabhängige Stelle nachzuweisen. Abs. 2 gilt sinngemäß, wobei der Nachweis innerhalb von drei Jahren nach der Aufforderung gemäß erster Satz, frühestens jedoch sechs Monate vor Ablauf dieser Frist, zu übermitteln ist.

(4) Die Kosten von Prüfungen durch unabhängige Stellen nach Abs. 2 und 3 sind von der geprüften Einrichtung zu tragen, es sei denn, die Cybersicherheitsbehörde trifft amtswegig in hinreichend begründeten Fällen eine anderslautende Entscheidung.

(5) Wesentliche und wichtige Einrichtungen haben der Cybersicherheitsbehörde geplante Prüfungen gemäß Abs. 2 und 3 spätestens ein Monat vor Beginn derer Durchführung durch Übermittlung eines Prüfplans bekannt zu geben.

(6) Der Bundesminister für Inneres kann mit Verordnung die notwendigen Inhalte, das Format, die Struktur sowie die Art der Übermittlung der geforderten Nachweise und diesbezüglicher Informationen nach den Abs. 1, 2 und 5 festlegen.

Berichtspflichten

§ 34. (1) Wesentliche und wichtige Einrichtungen haben dem für sie zuständigen CSIRT, andernfalls dem nationalen CSIRT, unverzüglich jeden erheblichen Cybersicherheitsvorfall (§ 35) zu melden. Das CSIRT leitet die Meldung unverzüglich an die Cybersicherheitsbehörde weiter.

(2) Für die Zwecke der Meldung nach Abs. 1 haben die betroffenen Einrichtungen dem CSIRT Folgendes zu übermitteln:

1. unverzüglich, in jedem Fall aber innerhalb von 24 Stunden nach Kenntnisnahme des erheblichen Cybersicherheitsvorfalls, eine Frühwarnung, in der gegebenenfalls angegeben wird, ob der Verdacht besteht, dass der erhebliche Cybersicherheitsvorfall auf rechtswidrige und schuldhafte Handlungen zurückzuführen ist oder grenzüberschreitende Auswirkungen haben könnte;
2. unverzüglich, in jedem Fall aber innerhalb von 72 Stunden nach Kenntnisnahme des erheblichen Cybersicherheitsvorfalls, eine Meldung über den Cybersicherheitsvorfall, in der gegebenenfalls die unter Z 1 genannten Informationen aktualisiert werden und eine erste Bewertung des erheblichen Cybersicherheitsvorfalls, einschließlich seines Schweregrads und seiner Auswirkungen, sowie gegebenenfalls die Kompromittierungsindikatoren angegeben werden;
3. auf Ersuchen eines CSIRT oder gegebenenfalls der Cybersicherheitsbehörde einen Zwischenbericht über relevante Statusaktualisierungen;
4. spätestens einen Monat nach Übermittlung der Meldung des Cybersicherheitsvorfalls gemäß Z 2 einen Abschlussbericht, der Folgendes enthält:
   a) eine ausführliche Beschreibung des Cybersicherheitsvorfalls, einschließlich seines Schweregrads und seiner Auswirkungen;
   b) Angaben zur Art der Bedrohung und zugrundeliegender Ursachen, die wahrscheinlich den Cybersicherheitsvorfall ausgelöst hat;
   c) Angaben zu den getroffenen und laufenden Abhilfemaßnahmen;

d) gegebenenfalls die grenzüberschreitenden Auswirkungen des Cybersicherheitsvorfalls;

5. im Falle eines andauernden Cybersicherheitsvorfalls zum Zeitpunkt der Vorlage des Abschlussberichts gemäß Z 4 haben die betreffenden Einrichtungen zu diesem Zeitpunkt einen Fortschrittsbericht und einen Abschlussbericht innerhalb eines Monats nach Behandlung des Cybersicherheitsvorfalls zu übermitteln.

Abweichend von Z 2 unterrichtet ein Vertrauensdiensteanbieter das CSIRT in Bezug auf erhebliche Cybersicherheitsvorfälle, die sich auf die Erbringung seiner Vertrauensdienste auswirken, unverzüglich, in jedem Fall aber innerhalb von 24 Stunden nach Kenntnisnahme des erheblichen Cybersicherheitsvorfalls. Zusätzlich haben die betroffenen Einrichtungen alle Informationen zu übermitteln, die es dem CSIRT und der Cybersicherheitsbehörde ermöglicht zu ermitteln, ob der Cybersicherheitsvorfall grenzübergreifende Auswirkungen hat.

(3) Soweit ein erheblicher Cybersicherheitsvorfall die Erbringung des jeweiligen Dienstes der betroffenen Einrichtung beeinträchtigt, unterrichtet die Einrichtung die Empfänger ihrer Dienste unverzüglich über diesen erheblichen Cybersicherheitsvorfall und teilt, soweit möglich, alle Maßnahmen oder Abhilfemaßnahmen mit, die diese Empfänger als Reaktion auf diese Bedrohung ergreifen können. Die Verfahren zur Erfüllung der Abs. 2 und 3, einschließlich der Einstufung potentieller Kategorien von Cybersicherheitsvorfällen und des genauen Ablaufs der Meldung sind im Rahmen des § 32 Abs. 1 und 2 in Verbindung mit Punkt 11 („Umgang mit Cybersicherheitsvorfällen“) der Anlage 3 intern verbindlich festzusetzen.

(4) Das CSIRT übermittelt der meldenden Einrichtung unverzüglich und nach Möglichkeit innerhalb von 24 Stunden nach Eingang der Frühwarnung gemäß Abs. 2 Z 1 eine Antwort, einschließlich einer ersten Rückmeldung zu dem erheblichen Cybersicherheitsvorfall und, auf Ersuchen der Einrichtung, Orientierungshilfen oder operative Beratung für die Durchführung möglicher Abhilfemaßnahmen. Auf Ersuchen der betreffenden Einrichtung leistet das CSIRT zusätzliche technische Unterstützung. Wird bei dem erheblichen Cybersicherheitsvorfall ein strafrechtlich relevanter Hintergrund vermutet, gibt das CSIRT ferner Orientierungshilfen für die Meldung des Cybersicherheitsvorfalls an die Strafverfolgungsbehörden.

(5) Wenn der erhebliche Cybersicherheitsvorfall zwei oder mehr Mitgliedstaaten der Europäischen Union betrifft, unterrichtet die Cybersicherheitsbehörde im Wege der zentralen Anlaufstelle unverzüglich die zentralen Anlaufstellen der anderen betroffenen Mitgliedstaaten und die ENISA über den erheblichen Cybersicherheitsvorfall. Diese Mitteilung hat die gemäß Abs. 2 erhaltenen Informationen zu enthalten.

(6) Nach Anhörung der von einem Cybersicherheitsvorfall betroffenen Einrichtungen kann die Cybersicherheitsbehörde personenbezogene Daten gemäß §§ 42 und 43 nach erfolgter Interessenabwägung bezüglich der Auswirkungen auf die Betroffenen veröffentlichen, um die Öffentlichkeit über Cybersicherheitsvorfälle zu unterrichten, sofern die Sensibilisierung der Öffentlichkeit zur Verhütung oder zur Bewältigung von Cybersicherheitsvorfällen erforderlich ist, oder die Offenlegung des Cybersicherheitsvorfalls auf sonstige Weise im öffentlichen Interesse liegt.

(7) Die Cybersicherheitsbehörde hat jener Behörde, die in Umsetzung des Art. 9 Richtlinie (EU) 2022/2557 national als zuständige Behörde benannt oder eingerichtet wurde, Informationen über erhebliche Cybersicherheitsvorfälle, erhebliche Cyberbedrohungen und Beinahe-Vorfälle zur Verfügung zu stellen, die nach Abs. 1 von Einrichtungen, die im Sinne der Richtlinie (EU) 2022/2557 als kritische Einrichtungen gelten, gemeldet wurden. Dasselbe gilt für freiwillige Meldungen nach § 37.

(8) Die Cybersicherheitsbehörde hat der Regulierungsbehörde nach § 194 TKG 2021 und der KommAustria nach § 199 TKG 2021 Informationen über erhebliche Cybersicherheitsvorfälle, erhebliche Cyberbedrohungen und Beinahe-Vorfälle zur Verfügung zu stellen, die nach Abs. 1 von Anbietern öffentlicher elektronischer Kommunikationsnetze oder Anbietern öffentlich zugänglicher elektronischer Kommunikationsdienste gemeldet wurden. Dasselbe gilt für freiwillige Meldungen nach § 37.

Erheblicher Cybersicherheitsvorfall

§ 35. (1) Ein Cybersicherheitsvorfall gilt als erheblich, wenn er schwerwiegende Betriebsstörungen der erbrachten Dienste („Art der Einrichtung“ nach Anlage 1 und 2) oder schwerwiegende finanzielle Verluste für die betreffende Einrichtung verursacht hat oder verursachen kann oder er andere natürliche oder juristische Personen durch erhebliche materielle oder immaterielle Schäden beeinträchtigt hat oder beeinträchtigen kann. Zudem sind die betroffenen Netz- und Informationssysteme und deren Bedeutung für die Erbringung der Dienste der jeweiligen Einrichtung, die Schwere und die technischen Merkmale der Cyberbedrohung und sämtliche zugrundeliegende Schwachstellen, die ausgenutzt werden, sowie die Erfahrungen der Einrichtung mit ähnlichen Vorfällen zu berücksichtigen.

(2) Bei der Beurteilung, ob ein Cybersicherheitsvorfall als erheblich im Sinne des Abs. 1 einzustufen ist, sind folgende Kriterien zu berücksichtigen:

1. das Ausmaß der Abhängigkeit der in § 2 gelisteten Sektoren und nach Anlage 1 und 2 von nach Art der wesentlichen oder wichtigen Einrichtung gemäß § 24 in Verbindung mit Anlage 1 und 2 erbrachten Diensten;
2. die möglichen Auswirkungen von Cybersicherheitsvorfällen auf die Umwelt, die öffentliche Ordnung und Sicherheit, die öffentliche Gesundheit oder die Gesundheit der Bevölkerung oder eines großen Personenkreises;
3. der Marktanteil der jeweiligen Einrichtung auf dem Markt für die betreffenden Dienste gemäß Abs. 1;
4. das geografische Gebiet, das von einem Cybersicherheitsvorfall betroffen sein könnte, einschließlich allfälliger grenzüberschreitender Auswirkungen, unter Berücksichtigung der Schwachstellen, die mit dem Grad der Isolierung bestimmter geografischer Gebiete, wie insbesondere Berggebiete, verbunden sind;
5. gegebenenfalls die unternehmens- und sektorspezifischen Faktoren.

(3) Der Bundesminister für Inneres kann mit Verordnung weitere Kriterien und nähere Regelungen zu Abs. 2 für das Vorliegen eines erheblichen Cybersicherheitsvorfalls festlegen. Dabei können sektorspezifische Faktoren berücksichtigt werden.

3. Abschnitt
Informationsaustausch

Vereinbarungen über den Austausch von Informationen zur Cybersicherheit

§ 36. (1) Wesentliche und wichtige Einrichtungen sowie Einrichtungen, die nicht in den Anwendungsbereich dieses Bundesgesetzes fallen, können einander auf freiwilliger Basis relevante Cybersicherheitsinformationen, einschließlich Informationen über Cyberbedrohungen, Beinahe-Vorfälle, Schwachstellen, Techniken und Verfahren, Kompromittierungsindikatoren, gegnerische Taktiken, bedrohungsspezifische Informationen, Cybersicherheitswarnungen und Empfehlungen für die Konfiguration von Cybersicherheitsinstrumenten zur Aufdeckung von Cyberangriffen, übermitteln, sofern

1. dieser Informationsaustausch darauf abzielt, Cybersicherheitsvorfälle zu verhindern, aufzudecken, darauf zu reagieren oder sich von ihnen zu erholen oder ihre Folgen einzudämmen oder
2. durch diesen Informationsaustausch das Cybersicherheitsniveau erhöht wird, insbesondere indem Aufklärungsarbeit über Cyberbedrohungen geleistet wird, die Fähigkeit solcher Bedrohungen, sich zu verbreiten eingedämmt oder verhindert wird und eine Reihe von Abwehrkapazitäten, die Beseitigung und Offenlegung von Schwachstellen, Techniken zur Erkennung, Eindämmung und Verhütung von Bedrohungen, Eindämmungsstrategien, Reaktions- und Wiederherstellungsphasen unterstützt werden oder indem die gemeinsame Forschung im Bereich der Cyberbedrohungen zwischen öffentlichen und privaten Einrichtungen gefördert wird.

(2) Der Informationsaustausch zwischen den wesentlichen und wichtigen Einrichtungen und gegebenenfalls ihrer Lieferanten oder Dienstleister hat im Wege von Vereinbarungen über den Informationsaustausch im Bereich der Cybersicherheit unter Beachtung des potentiell sensiblen Charakters der ausgetauschten Informationen zu erfolgen. In diesen Vereinbarungen können operative Elemente, einschließlich der Nutzung spezieller IKT-Plattformen und Automatisierungsinstrumente, der Inhalt und die Bedingungen der Vereinbarungen über den Informationsaustausch bestimmt werden.

(3) Die Cybersicherheitsbehörde unterstützt die Einrichtungen bei der Ausarbeitung von Vereinbarungen gemäß Abs. 2, insbesondere hinsichtlich der Anwendung der in § 15 Abs. 4 Z 8 genannten Konzepte.

(4) Wesentliche und wichtige Einrichtungen haben die Cybersicherheitsbehörde beim Abschluss von in Abs. 2 genannten Vereinbarungen oder über ihren Rücktritt von solchen Vereinbarungen zu unterrichten, sobald dieser wirksam wird.

Freiwillige Meldung relevanter Informationen

§ 37. (1) Wesentliche und wichtige Einrichtungen können unabhängig von ihrer Berichtspflicht nach § 34 freiwillig Cybersicherheitsvorfälle, Cyberbedrohungen und Beinahe-Cybersicherheitsvorfälle an das für sie zuständige CSIRT, in Ermangelung eines solchen an das nationale CSIRT, melden, das die Meldungen an die Cybersicherheitsbehörde weiterleitet.

(2) Einrichtungen, die nicht in den Anwendungsbereich dieses Bundesgesetzes fallen, können ebenfalls auf freiwilliger Basis Cybersicherheitsvorfälle, Cyberbedrohungen und Beinahe-Cybersicherheitsvorfälle an das sektorspezifische CSIRT, falls ein solches eingerichtet ist, andernfalls an das nationale CSIRT, melden, das die Meldungen zusammenfasst und an die Cybersicherheitsbehörde weiterleitet.

(3) Eine freiwillige Meldung muss weder die Identität der Einrichtung noch Informationen, die auf diese schließen lassen, beinhalten. Die Meldung kann personenbezogene Daten gemäß § 42 Abs. 2 enthalten. § 34 Abs. 2 gilt sinngemäß.

4. Abschnitt
Aufsicht und Durchsetzung

Aufsichtsmaßnahmen in Bezug auf wesentliche und wichtige Einrichtungen

§ 38. (1) Die Cybersicherheitsbehörde ist in Wahrnehmung ihrer Aufsichtsaufgaben zur Einhaltung der sich aus diesem Bundesgesetz ergebenden Verpflichtungen in Bezug auf wesentliche Einrichtungen neben § 33 befugt, folgende Maßnahmen zu ergreifen:

1. die Durchführung von Kontrollen der Umsetzung der Risikomanagementmaßnahmen gemäß § 32 durch Einschau, insbesondere in die diesbezüglichen Netz- und Informationssysteme und Unterlagen vor Ort, mittels Fernzugriff unter Mitwirkung der Einrichtung oder durch Begleitung der Prüfungen von unabhängige Stellen, jeweils nach vorangegangener Verständigung der betreffenden Einrichtung;
2. die Durchführung von Sicherheitsscans auf der Grundlage objektiver, nichtdiskriminierender, fairer und transparenter Risikobewertungskriterien, erforderlichenfalls in Zusammenarbeit mit der betreffenden Einrichtung;
3. die Anforderung von Informationen, die für die Bewertung der von der betreffenden Einrichtung umgesetzten Risikomanagementmaßnahmen gemäß § 32 erforderlich sind, einschließlich dokumentierter Cybersicherheitskonzepte, sowie der Einhaltung der Verpflichtungen zur Übermittlung von Informationen nach § 29;
4. die Anforderung des Zugangs zu Daten, Dokumenten und sonstigen Informationen, die zur Erfüllung der Aufsichtsaufgaben erforderlich sind;
5. die Ad-hoc-Prüfung einer wesentlichen Einrichtung, einschließlich solcher, die aufgrund eines erheblichen Cybersicherheitsvorfalls oder Verstoßes gegen dieses Bundesgesetz durch diese Einrichtung gerechtfertigt ist oder der Überprüfung einer übermittelten Selbstdeklaration gemäß § 33 Abs. 1 dienen.

(2) Erlangt die Cybersicherheitsbehörde durch Nachweise, wie insbesondere die Selbstdeklaration nach § 33 Abs. 1, oder sonstige begründete Hinweise und Informationen davon Kenntnis, dass eine wichtige Einrichtung mutmaßlich ihren Verpflichtungen nach diesem Bundesgesetz, insbesondere den §§ 32 und 34 nicht nachkommt, kann sie auch gegenüber wichtigen Einrichtungen Aufsichtsmaßnahmen gemäß Abs. 1 Z. 1 bis 4 setzen.

Durchsetzungsmaßnahmen in Bezug auf wesentliche und wichtige Einrichtungen

§ 39. (1) Die Cybersicherheitsbehörde ist zur Sicherstellung der Einhaltung der sich aus diesem Bundesgesetz ergebenden Verpflichtungen gegenüber wesentlichen und wichtigen Einrichtungen befugt, mit Verfahrensanordnung unter Setzung einer angemessenen Frist Maßnahmen anzuordnen, wie etwa solche zur Verhütung oder Behebung eines Cybersicherheitsvorfalls, zur Behebung festgestellter Mängel oder zur Beendigung von Zuwiderhandlungen gegen Verpflichtungen nach diesem Bundesgesetz.

(2) Kommt die Einrichtung einer Verfahrensanordnung gemäß Abs. 1 nicht nach, hat die Cybersicherheitsbehörde die nachweisliche Umsetzung der jeweiligen Maßnahmen unter Setzung einer angemessenen Frist mit Bescheid aufzutragen.

(3) Zudem ist die Cybersicherheitsbehörde zur Sicherstellung der Einhaltung der sich aus diesem Bundesgesetz ergebenden Verpflichtungen befugt, mit Bescheid

1. gegenüber wesentlichen und wichtigen Einrichtungen
   a. die Unterrichtung der potenziell von einer erheblichen Cyberbedrohung betroffenen Personen, einschließlich der Empfänger ihrer Dienste und sonstigen Tätigkeiten, über die Art der Bedrohung sowie über mögliche Abwehr- und Abhilfemaßnahmen zu anzuordnen,
   b. anzuordnen, einzelne Aspekte seitens der Cybersicherheitsbehörde aufgezeigter, nicht eingehaltener sich aus diesem Bundesgesetz ergebenden Verpflichtungen öffentlich bekannt

zu machen, sofern dies erforderlich ist, um das damit verbundene Risiko auf ein vertretbares Ausmaß zu reduzieren sowie

2. gegenüber wesentlichen Einrichtungen für einen bestimmten Zeitraum einen mit genau festgelegten Aufgaben betrauten Überwachungsbeauftragten zur Überwachung der Anforderungen gemäß §§ 32 und 34 zu benennen, um die Umsetzung der gemäß Abs. 1 mit Bescheid angeordneten Maßnahmen sicherzustellen. Die Cybersicherheitsbehörde hat die Aufgaben des Überwachungsbeauftragten auf jenen Umfang zu beschränken, der für die Einhaltung der Anforderungen an die Umsetzung der Risikomanagementmaßnahmen und der Berichtspflichten der wesentlichen Einrichtung unbedingt erforderlich ist.

(4) Kommt eine wesentliche Einrichtung dem Bescheid gemäß Abs. 2 nicht fristgerecht und nachweislich nach, ist die Cybersicherheitsbehörde befugt,

1. die zuständige Behörde zu ersuchen, die Zertifizierung oder Genehmigung für einen Teil oder alle von der Einrichtung erbrachten einschlägigen Dienste oder Tätigkeiten vorübergehend auszusetzen oder die nationale Behörde für die Cybersicherheitszertifizierung gemäß Art. 58 der Verordnung (EU) 2019/881 oder eine Konformitätsbewertungsstelle zu ersuchen, die Zertifizierung oder Genehmigung vorübergehend auszusetzen;
2. Leitungsorganen einer wesentlichen Einrichtung, einschließlich ihrer rechtlichen Vertreter, mit Bescheid vorübergehend zu untersagen, Leitungsaufgaben in dieser wesentlichen Einrichtung wahrzunehmen. Dieser Bescheid ist in einer allgemeinen Weise zu veröffentlichen, die geeignet erscheint, einen möglichst weiten Personenkreis zu erreichen.

(5) Die gemäß Abs. 4 verhängten vorübergehenden Aussetzungen und Untersagungen sind von der zuständigen Behörde oder der Cybersicherheitsbehörde unverzüglich aufzuheben, sobald die betreffende wesentliche Einrichtung nachweislich die gemäß Abs. 2 angeordneten Maßnahmen ergriffen hat.

(6) Die in Abs. 4 vorgesehenen Durchsetzungsmaßnahmen finden keine Anwendung auf Behörden und öffentliche Stellen, wie insbesondere in Formen des öffentlichen Rechts sowie des Privatrechts eingerichtete Stellen.

(7) Bei der Ergreifung von Durchsetzungsmaßnahmen gemäß Abs. 1 bis 3 ist den Umständen des Einzelfalls Rechnung zu tragen und dabei zumindest Folgendes gebührend zu berücksichtigen:

1. die Schwere des Verstoßes und die Wichtigkeit der Bestimmungen, gegen die verstoßen wurde, wobei insbesondere Folgendes immer als schwerer Verstoß anzusehen ist:
   a) wiederholte Verstöße;
   b) eine unterlassene Meldung oder Behebung von erheblichen Cybersicherheitsvorfällen;
   c) eine Nichtbehebung von Mängeln nach verbindlicher Anweisung der Cybersicherheitsbehörde;
   d) eine willentliche Behinderung von Prüfungen oder Überwachungstätigkeiten, die nach der Feststellung eines Verstoßes von der Cybersicherheitsbehörde angeordnet wurden, sowie
   e) eine bewusste Übermittlung falscher oder grob verfälschender Informationen in Bezug auf die Umsetzung der Risikomanagementmaßnahmen oder Berichtspflichten gemäß §§ 32 und 34;
2. die Dauer des Verstoßes;
3. einschlägige frühere Verstöße der betreffenden Einrichtung;
4. der verursachte materielle oder immaterielle Schaden, darunter finanzieller oder wirtschaftlicher Verlust, Auswirkungen auf andere Dienste und die Zahl der betroffenen Nutzer;
5. der etwaige Vorsatz oder die etwaige Fahrlässigkeit jener Person, die den Verstoß verursacht hat;
6. die von der Einrichtung umgesetzten Risikomanagementmaßnahmen zur Verhinderung oder Minderung des materiellen oder immateriellen Schadens;
7. die Einhaltung genehmigter Verhaltensregeln oder genehmigter Zertifizierungsverfahren;
8. der Umfang der Zusammenarbeit der verantwortlichen natürlichen oder juristischen Personen mit der Cybersicherheitsbehörde.

Nutzung der europäischen Schemata für die Cybersicherheitszertifizierung

§ 40. Die Cybersicherheitsbehörde kann wesentliche und wichtige Einrichtungen dazu verpflichten, spezielle IKT-Produkte, -Dienste und -Prozesse zu verwenden, die von der wesentlichen oder wichtigen Einrichtung entwickelt oder von Dritten beschafft werden und die im Rahmen europäischer Schemata für die Cybersicherheitszertifizierung, die gemäß Art. 49 der Verordnung (EU) 2019/881 angenommen wurden, zertifiziert sind, um die Erfüllung bestimmter in § 32 genannter Anforderungen nachzuweisen. In

diesem Zusammenhang hat die Cybersicherheitsbehörde mit der nationalen Behörde für die Cybersicherheitszertifizierung zusammenzuarbeiten.

Verfahren vor dem Bundesverwaltungsgericht

§ 41. Rechtsmittel gegen Entscheidungen der Cybersicherheitsbehörde gemäß § 7 Abs. 4 und 10, § 10 Abs. 7, sowie § 39 Abs. 2, 3 und 4 Z 2 haben, abweichend von § 13 des Verwaltungsgerichtsverfahrensgesetzes (VwGVG), BGBl. I Nr. 33/2013, keine aufschiebende Wirkung. Das Bundesverwaltungsgericht kann die aufschiebende Wirkung im betreffenden Verfahren auf Antrag zuerkennen, wenn nach Abwägung aller berührten Interessen mit dem Vollzug des Bescheides oder mit der Ausübung der mit dem Bescheid eingeräumten Berechtigung für den Beschwerdeführer ein schwerer und nicht wiedergutzumachender Schaden verbunden wäre.

4. Hauptstück
Datenschutz

Datenverarbeitung

§ 42. (1) Der Bundeskanzler, der Bundesminister für Inneres, der Bundesminister für Landesverteidigung, der Bundesminister für europäische und internationale Angelegenheiten und die CSIRTs sind jeweils als Verantwortliche im Sinne des Art. 4 Nr. 7 DSGVO und § 36 Abs. 2 Z 8 DSG, berechtigt, zur Gewährleistung eines hohen Cybersicherheitsniveaus bei der Wahrnehmung ihrer Aufgaben nach diesem Bundesgesetz sowie zum Schutz vor und der Abwehr von Gefahren für die öffentliche Sicherheit die erforderlichen personenbezogenen Daten im Sinne des Art. 4 Nr. 1 DSGVO und § 36 Abs. 2 Z 1 DSG zu verarbeiten.

(2) Bei den in Abs. 1 genannten personenbezogenen Daten handelt es sich insbesondere um Kontakt- und Identitätsdaten natürlicher und juristischer Personen, wie etwa Vor- und Familienname, Firmenname, Wohnadresse, Firmenadresse, Telefonnummer, E-Mail-Adresse oder User- und Account-Name, unternehmensbezogene Daten, wie unternehmerische Aufzeichnungen, Bilanzdaten oder Daten aus der Gewinn- und Verlustrechnung, sowie technische Daten, wie etwa AS-Nummer, Domain-Name, Hashes, Host-Name, IP-Adresse, Log-Files, Metadaten, Network-Dump, Ports, Rechnername, RIPE-Handle oder Uniform Resource Locator (URL).

(3) Für die Verarbeitungsvorgänge von personenbezogenen Daten sind Protokollaufzeichnungen jedenfalls betreffend die Erhebung, Abfrage, Übermittlung, Änderung und Löschung zu führen, drei Jahre aufzubewahren und danach zu löschen.

(4) Personenbezogene Daten sind unverzüglich zu löschen, wenn die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, nicht mehr notwendig sind. Nach Ablauf von fünf Jahren sind die Daten jedenfalls zu löschen.

(5) Hinsichtlich der Verarbeitung personenbezogener Daten nach dem 3. Abschnitt des 2. Hauptstücks, dem 1., 2. und 4. Abschnitt des 3. Hauptstücks besteht kein Widerspruchsrecht gemäß Art. 21 DSGVO sowie kein Recht auf Einschränkung der Verarbeitung gemäß Art. 18 DSGVO oder § 45 DSG.

Datenübermittlung

§ 43. (1) Der Bundesminister für Inneres, der Bundeskanzler, der Bundesminister für Landesverteidigung und der Bundesminister für europäische und internationale Angelegenheiten sind ermächtigt, die aufgrund der Wahrnehmung ihrer Aufgaben nach diesem Bundesgesetz verarbeiteten Daten

1. einander für Zwecke der ihnen nach diesem Bundesgesetz zugewiesenen Aufgaben,
2. den Mitgliedern der OpKoord (§ 14) für Zwecke der ihr nach diesem Bundesgesetz zugewiesenen Aufgaben,
3. an militärische Behörden für Zwecke der militärischen Landesverteidigung gemäß Art. 79 Abs. 1 B-VG,
4. an Sicherheitsbehörden für Zwecke der Sicherheitspolizei und Strafrechtspflege,
5. an Staatsanwaltschaften und ordentliche Gerichte für Zwecke der Strafrechtspflege sowie
6. an jene Behörden, die in Umsetzung des Art. 9 der Richtlinie (EU) 2022/2557 innerstaatlich als zuständige Behörden benannt oder eingerichtet wurden und an sonstige inländische Behörden, soweit dies jeweils eine wesentliche Voraussetzung zur Wahrnehmung einer ihnen gesetzlich übertragenen Aufgaben ist,

zu übermitteln.

(2) Der Bundesminister für Inneres ist berechtigt, Daten gemäß § 42 Abs. 2 an ausländische Sicherheitsbehörden und Sicherheitsorganisationen gemäß § 2 Abs. 2 und 3 des Polizeikooperationsgesetzes (PolKG), BGBl. I Nr. 104/1997, sowie an Organe der Europäischen Union oder Vereinten Nationen entsprechend den Bestimmungen über die internationale polizeiliche Amtshilfe zu übermitteln.

(3) Der Bundesminister für Inneres ist zudem berechtigt, Daten, die er zur Wahrnehmung seiner Aufgaben nach diesem Bundesgesetz verarbeitet, an wesentliche und wichtige Einrichtungen und mit diesen im Rahmen des Schutzes ihrer Netz- und Informationssysteme zusammenarbeitenden Dritten gemäß § 17 sowie an sonstige Einrichtungen, die von einem Risiko oder Cybersicherheitsvorfall betroffen sind, an CSIRTs zur Wahrnehmung ihrer Aufgaben gemäß § 8 Abs. 1, an die ENISA gemäß § 5 Abs. 2 Z 2, § 29 Abs. 6 und § 34 Abs. 5, an die zentralen Anlaufstellen der von einem erheblichen Cybersicherheitsvorfall betroffenen Mitgliedstaaten der Europäischen Union gemäß § 34 Abs. 5, an die zuständigen Behörden in der Europäischen Union gemäß § 22 und an EU-CyCLONe gemäß § 16 zu übermitteln.

(4) Die CSIRTs sind berechtigt, Daten zur Erfüllung ihrer Aufgaben nach diesem Bundesgesetz einander, an wesentliche und wichtige Einrichtungen gemäß § 8 Abs. 1, 2 und 8 sowie § 34 Abs. 4, an sonstige Einrichtungen und Personen gemäß § 8 Abs. 11, an Teilnehmer des CSIRTs-Netzwerks gemäß § 8 Abs. 1 Z 6, an nationale CSIRTs von Drittländern oder gleichwertigen Stellen oder Sicherheitsdienstleistern gemäß § 8 Abs. 9 sowie an inländische Behörden, soweit dies eine wesentliche Voraussetzung zur Wahrnehmung einer ihnen gesetzlich übertragenen Aufgabe ist, übermitteln.

5. Hauptstück
Strafbestimmungen

Allgemeine Bedingungen für die Verhängung von Geldstrafen

§ 44. (1) Den Bezirksverwaltungsbehörden obliegt die Verhängung von Verwaltungsstrafen gemäß § 45. Der Bundesminister für Inneres hat der zuständigen Bezirksverwaltungsbehörde die Begehung einer Verwaltungsübertretung gemäß § 45 anzuzeigen. Die Bezirksverwaltungsbehörde hat dem Bundesminister für Inneres einen jährlichen Bericht über eingeleitete Verwaltungsstrafverfahren sowie die Gründe für die Nichteinleitung oder Einstellung von Verwaltungsstrafverfahren nach standardisierten Vorgaben bis zum 31. März des Folgejahres zu übermitteln.

(2) Die Bezirksverwaltungsbehörde kann Geldstrafen gegen eine juristische Person verhängen, wenn Verwaltungsübertretungen gemäß § 45 Abs. 1 und 4 durch Personen begangen wurden, die entweder allein oder als Teil eines Organs der juristischen Person gehandelt haben oder eine Führungsposition innerhalb einer juristischen Person aufgrund

1. der Befugnis zur Vertretung der juristischen Person,
2. der Befugnis, Entscheidungen im Namen der juristischen Person zu treffen, oder
3. einer Kontrollbefugnis innerhalb der juristischen Person

innehaben.

(3) Juristische Personen können wegen Verwaltungsübertretungen gemäß § 45 Abs. 1 und 4 auch verantwortlich gemacht werden, wenn mangelnde Überwachung oder Kontrolle durch eine in Abs. 2 genannte Person die Begehung dieser Verstöße durch eine für die juristische Person tätige Person ermöglicht hat.

(4) Von der Bestrafung eines Verantwortlichen gemäß § 9 des Verwaltungsstrafgesetzes 1991 (VStG), BGBl. Nr. 52/1991, ist abzusehen, wenn für denselben Verstoß bereits eine Verwaltungsstrafe gegen die juristische Person verhängt wird.

(5) Bei der Strafbemessung sind insbesondere die in § 39 Abs. 7 genannten Umstände zu berücksichtigen.

(6) Hat die Datenschutzbehörde bereits eine Geldbuße gemäß Art. 58 Abs. 2 Buchstabe i DSGVO für einen Verstoß verhängt, darf die Bezirksverwaltungsbehörde keine Geldstrafe nach dem vorliegenden Bundesgesetz verhängen, wenn dem Verstoß dasselbe Verhalten zu Grunde liegt, das Gegenstand der Geldbuße nach Art. 58 Abs. 2 Buchstabe i DSGVO war.

Verwaltungsstrafbestimmungen

§ 45. (1) Wer

1. sich bei der Cybersicherheitsbehörde nicht fristgerecht gemäß § 29 Abs. 3 registriert oder im Zuge der Registrierung wissentlich falsche oder unvollständige Angaben übermittelt,

2. der Cybersicherheitsbehörde Änderungen gemäß § 29 Abs. 4 nicht im dort vorgegebenen Zeitraum bekannt gibt,
3. unter den gemäß § 29 Abs. 2 Z 2 übermittelten Kontaktdaten nicht in jenem Zeitraum erreichbar ist, in dem die jeweilige Einrichtung ihre Dienste zur Verfügung stellt (§ 29 Abs. 7),
4. seiner Verpflichtung, Cybersicherheitsschulungen für Leitungsorgane gemäß § 31 Abs. 3 vorzusehen nicht nachkommt,
5. seiner Verpflichtung, Cybersicherheitsschulungen für Mitarbeiter (Arbeitnehmer) gemäß § 31 Abs. 3 vorzusehen, nicht nachkommt,
6. Risikomanagementmaßnahmen gemäß § 32 nicht umsetzt oder deren Umsetzung nicht nachweisen kann,
7. eine Selbstdeklaration gemäß § 33 Abs. 1 nicht oder nicht innerhalb sechs Monate nach Aufforderung übermittelt,
8. in einer Selbstdeklaration gemäß § 33 Abs. 1 wissentlich falsche Angaben über die Umsetzung von Risikomanagementmaßnahmen macht,
9. nicht oder nicht innerhalb der in § 33 Abs. 2 erster Satz vorgesehenen Frist seiner Verpflichtung zur Übermittlung eines Prüfberichts gemäß § 33 Abs. 2 oder § 33 Abs. 3 nachkommt,
10. eine geplante Durchführung einer Prüfung gemäß § 33 Abs. 5 der Cybersicherheitsbehörde nicht zumindest ein Monat vor dem geplanten Beginn dieser Prüfung bekanntgibt,
11. seiner Verpflichtung zur Meldung eines erheblichen Cybersicherheitsvorfalls gemäß § 34 Abs. 1 und Abs. 2 sowie den damit zusammenhängenden Berichtspflichten nicht entspricht,
12. seiner Verpflichtung zur unverzüglichen Unterrichtung der Empfänger der Dienste einer wesentlichen oder wichtigen Einrichtung gemäß § 34 Abs. 3 nicht entspricht,
13. seiner Verpflichtung zur Bekanntgabe von Abschlüssen sowie Rücktritten von Vereinbarungen zum Informationsaustausch gemäß § 36 Abs. 4 nicht entspricht,
14. die Durchführung einer Kontrolle der jeweiligen Einrichtung gemäß § 38 Abs. 1 Z 1 be- oder verhindert,
15. die Durchführung von Sicherheitsscans betreffend der jeweiligen Einrichtung gemäß § 38 Abs. 1 Z 2 be- oder verhindert,
16. seiner Verpflichtung zur Bereitstellung von Informationen einschließlich dokumentierter Sicherheitskonzepte gemäß § 38 Abs. 1 Z 3 nicht entspricht,
17. seiner Verpflichtung zur Gewährung des Zugangs zu Daten, Dokumenten oder sonstigen Informationen auf Anforderung gemäß § 38 Abs. 1 Z 4 nicht entspricht,
18. die Durchführung einer Ad-hoc-Prüfung der jeweiligen Einrichtung gemäß § 38 Abs. 1 Z 5 be- oder verhindert,
19. den gemäß § 39 Abs. 2 sowie Abs. 3 Z 1 lit. a und b angeordneten Maßnahmen nicht fristgerecht nachkommt,
20. den Überwachungsbeauftragten gemäß § 39 Abs. 3 Z 2 bei seiner Tätigkeit behindert,
21. seiner Verpflichtung zur Verwendung spezieller IKT-Produkte, -Dienste und -Prozesse gemäß § 40 nicht nachkommt,

begeht eine Verwaltungsübertretung und ist mit einer Geldstrafe nach Maßgabe der Abs. 2 und 3 zu bestrafen.

(2) Wer als wesentliche Einrichtung (§ 24 Abs. 1) eine Verwaltungsübertretung nach Abs. 1 begeht, ist mit Geldstrafe in Höhe von bis zu 10 000 000 EUR 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, zu bestrafen.

(3) Wer als wichtige Einrichtung (§ 24 Abs. 2) eine Verwaltungsübertretung nach Abs. 1 begeht, ist mit Geldstrafe in Höhe von bis zu 7 000 000 EUR oder bis zu 1,4 % des gesamten weltweiten im vorangegangenen Geschäftsjahr getätigten Umsatzes des Unternehmens, dem die wichtige Einrichtung angehört, je nachdem, welcher Betrag höher ist, zu bestrafen.

(4) Wer

1. als unabhängige Stelle die Durchführung einer Kontrolle gemäß § 7 Abs. 3 be- oder verhindert,
2. seiner Verpflichtung zur Führung einer Datenbank gemäß § 30 Abs. 1 nicht nachkommt,
3. entgegen § 30 Abs. 3 über keine Vorgaben und Verfahren, einschließlich Überprüfungsverfahren, verfügt oder diese Vorgaben und Verfahren nicht öffentlich zugänglich macht,

4. entgegen § 30 Abs. 4 nicht unverzüglich nach der Registrierung eines Domänenamens die nicht personenbezogenen Domänennamen-Registrierungsdaten öffentlich zugänglich macht,
5. entgegen § 30 Abs. 5 trotz rechtmäßigen und begründeten Antrags keinen Zugang zu den Domänennamen-Registrierungsdaten gewährt, alle Anträge auf Zugang nicht unverzüglich, längstens jedoch innerhalb von 72 Stunden nach Eingang des jeweiligen Antrags, beantwortet oder die Vorgaben und Verfahren im Hinblick auf die Offenlegung solcher Daten nicht öffentlich zugänglich macht,

ist mit Geldstrafe bis zu 50 000 EUR und im Wiederholungsfall bis zu 100 000 EUR zu bestrafen.

(5) Diese Bestimmung findet keine Anwendung auf Behörden und sonstige Stellen der öffentlichen Verwaltung, wie insbesondere in Formen des öffentlichen Rechts sowie des Privatrechts eingerichtete Stellen.

Nichteinhaltung von Verpflichtungen durch Stellen der öffentlichen Verwaltung

§ 46. (1) Der Bundesminister für Inneres hat der zuständigen Bezirksverwaltungsbehörde die Nichteinhaltung der sich aus diesem Bundesgesetz ergebenden Verpflichtungen durch Behörden und sonstige Stellen der öffentlichen Verwaltung, wie insbesondere in Formen des öffentlichen Rechts sowie des Privatrechts eingerichtete Stellen, anzuzeigen. § 44 Abs. 1 zweiter Satz gilt.

(2) **(Verfassungsbestimmung)** Die Bezirksverwaltungsbehörde hat die Nichteinhaltung der sich aus diesem Bundesgesetz ergebenden Verpflichtungen durch Behörden und sonstige Stellen der öffentlichen Verwaltung, wie insbesondere in Formen des öffentlichen Rechts sowie des Privatrechts eingerichtete Stellen, mit Bescheid festzustellen sowie eine angemessene Frist zur Herstellung des rechtmäßigen Zustandes anzuordnen. Wird der rechtmäßige Zustand nicht fristgerecht hergestellt, hat die Bezirksverwaltungsbehörde nach Rechtskraft des Bescheides die Nichteinhaltung dieser Verpflichtungen in einer allgemeinen Weise zu veröffentlichen, die geeignet scheint, einen möglichst weiten Personenkreis zu erreichen. Diese Veröffentlichung darf nur insoweit erfolgen, als diese keine Gefahr für die öffentliche Ordnung oder Sicherheit darstellt.

6. Hauptstück
Schlussbestimmungen

Personenbezogene Bezeichnungen

§ 47. Alle in diesem Bundesgesetz verwendeten personenbezogenen Bezeichnungen gelten gleichermaßen für alle Geschlechter. Bei der Anwendung der Bezeichnung auf bestimmte natürliche Personen ist die jeweils geschlechtsspezifische Form zu verwenden.

Durchführung und Umsetzung von Rechtsakten der Europäischen Union

§ 48. Durch dieses Bundesgesetz werden

1. die Richtlinie (EU) 2022/2555 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148, ABl. Nr. L 333 vom 27.12.2022 S. 80, umgesetzt;
2. die Verordnung (EU) 2021/887 zur Einrichtung des Europäischen Kompetenzzentrums für Industrie, Technologie und Forschung im Bereich der Cybersicherheit und des Netzwerks nationaler Koordinierungszentren, ABl. Nr. L 202 vom 08.06.2021 S. 1, durchgeführt.

Verweisungen

§ 49. Verweisungen in diesem Bundesgesetz auf andere Bundesgesetze sind als Verweisungen auf die jeweils geltende Fassung zu verstehen, soweit nichts anderes angeordnet wird.

Vollziehung

§ 50. (1) Mit der Vollziehung dieses Bundesgesetzes sind betraut

1. hinsichtlich § 15 die Bundesregierung;
2. hinsichtlich § 13 der Bundesminister für Inneres gemeinsam mit dem Bundeskanzler und dem Bundesminister für Landesverteidigung;
3. hinsichtlich § 14 der Bundesminister für Inneres gemeinsam mit dem Bundeskanzler, dem Bundesminister für Landesverteidigung und dem Bundesminister für europäische und internationale Angelegenheiten;
4. hinsichtlich der übrigen Bestimmungen der Bundesminister für Inneres.

(2) Dem Bundesminister für Inneres obliegt zudem die Besorgung der allgemeinen Angelegenheiten der in § 4 Abs. 1 genannten Aufgaben.

Inkrafttretens-, Außerkrafttretens- und Übergangsbestimmungen

§ 51. (1) **(Verfassungsbestimmung)** Mit XXXX treten

1. §§ 1 und 46 Abs. 2 samt Überschrift in Kraft und
2. § 1 des Netz- und Informationssystemsicherheitsgesetzes (NISG), BGBl. I Nr. 111/2018 außer Kraft.

(2) Mit XXXX treten

1. das Inhaltsverzeichnis, die §§ 2 bis 51 samt Überschriften sowie die Anlagen 1 bis 3 in Kraft,
2. die restlichen Bestimmungen des NISG außer Kraft und
3. die Netz- und Informationssystemsicherheitsverordnung (NISV), BGBl. II Nr. 215/2019, und die Verordnung über qualifizierte Stellen (QuaSteV), BGBl. II Nr. 226/2019 außer Kraft.

(3) Verordnungen auf Grund dieses Bundesgesetzes können bereits ab dem auf seine Kundmachung folgenden Tag erlassen werden. Sie dürfen jedoch frühestens mit Inkrafttreten dieses Bundesgesetzes in Kraft gesetzt werden.

(4) Von dem der Kundmachung dieses Bundesgesetzes folgenden Tag an sind, soweit nicht bereits erfolgt, alle vorbereitenden Maßnahmen zu setzen, die für die Ermöglichung einer zeitgerechten Aufgabenwahrnehmung durch die Cybersicherheitsbehörde erforderlich sind.

(5) Die Wirksamkeit von Bescheiden, die gemäß § 15 Abs. 3 NISG in der Fassung BGBl. I Nr. 111/2018, erlassen wurden, wird durch das Inkrafttreten dieses Bundesgesetzes nicht berührt. Bescheide, die gemäß § 16 Abs. 1 und § 18 Abs. 1 NISG in der Fassung BGBl. I Nr. 111/2018, erlassen wurden, werden mit Inkrafttreten dieses Bundesgesetzes gegenstandslos, sofern nicht Abs. 6 oder 7 zur Anwendung gelangt.

(6) Sofern qualifizierte Stellen gemäß § 18 Abs. 1 NISG in der Fassung BGBl. I Nr. 111/2018, einen Antrag gemäß § 7 Abs. 2 an die Cybersicherheitsbehörde innerhalb von sechs Monaten ab Inkrafttreten von § 7 Abs. 13 Z 1 stellen, berechtigen die Bescheide gemäß § 18 Abs. 1 NISG in der Fassung BGBl. I Nr. 111/2018 die qualifizierten Stellen unter Heranziehung der bislang bei Überprüfungen von Betreibern wesentlicher Dienste eingesetzten Prüfer bis zum Abschluss des Zulassungsverfahrens gemäß § 7 Abs. 2 zur Ausübung der Aufgaben einer unabhängigen Stelle gemäß § 7 in Bezug auf wesentliche und wichtige Einrichtungen.

(7) Für Betreiber wesentlicher Dienste gemäß § 16 Abs. 1 NISG in der Fassung BGBl. I Nr. 111/2018, die auch als wesentliche Einrichtungen gemäß § 24 Abs. 1 gelten, beginnt die dreijährige Frist des § 33 Abs. 2 erster Satz für den erstmaligen Nachweis der Anforderungen des § 32 nicht ab der Aufforderung zur Selbstdeklaration, sondern ab dem Zeitpunkt des letzten Nachweises gemäß § 17 Abs. 3 NISG in der Fassung BGBl. I Nr. 111/2018.

Artikel 2
Änderung des Telekommunikationsgesetzes 2021

Das Telekommunikationsgesetz 2021 (TKG 2021), BGBl. I Nr. 190/2021, zuletzt geändert durch das Bundesgesetz BGBl. I Nr. 6/2024, wird wie folgt geändert:

1. § 44 lautet:

„(1) Betreiber und Anbieter haben nach Maßgabe anderer Rechtsvorschriften Maßnahmen für Cybersicherheit zu ergreifen. Für den Fall, dass diese Rechtsvorschriften nicht ausreichen, das in § 1 Abs. 2 Z 4 genannte Ziel der Aufrechterhaltung der Sicherheit der Netze und Dienste zu gewährleisten, ist die Regulierungsbehörde ermächtigt, im Einvernehmen mit dem Bundeskanzler, dem Bundesminister für Finanzen und dem Bundesminister für Inneres unter Bedachtnahme auf relevante internationale Vorschriften, die nationale Cybersicherheitsstrategie, die Art des Netzes oder des Dienstes, die technischen Möglichkeiten, den Schutz personenbezogener Daten und sonstige schutzwürdige Interessen von Nutzern mit Verordnung nähere Bestimmungen über technische und organisatorische Sicherheitsmaßnahmen festzulegen.

(2) In der Verordnung nach Abs. 1 kann auch angeordnet werden, dass Betreiber von öffentlichen Kommunikationsnetzen oder öffentlichen Kommunikationsdiensten, die ihre Netze oder Dienste in Österreich betreiben und über keinen Aufenthalt oder Sitz in der Europäischen Union verfügen, eine inländische Zustelladresse bekannt geben müssen, an die in Verfahren nach diesem Bundesgesetz

rechtskräftig zugestellt werden kann. Dies kann auch für Hersteller von Komponenten eines Netzes für elektronische Kommunikation oder für Bereitsteller von Dienstleistungen für solche Netze angeordnet werden, sofern sie ihre Waren oder Dienstleistungen in Österreich anbieten oder nach Österreich importiert werden und sie über keinen Aufenthalt oder Sitz in der Europäischen Union verfügen.

(3) Der Regulierungsbehörde werden darüber hinaus folgende Aufgaben übertragen:

1. Durchführung einer Branchenrisikoanalyse in Zusammenarbeit mit dem Bundeskanzleramt, den Bundesministerien für Finanzen, für Inneres und für Landesverteidigung, dem CSIRT sowie den Betreibern von Fest- und von Mobilfunknetzen in Abständen von jeweils zwei Jahren sowie Erstellung eines Abschlussberichts, der den teilnehmenden Institutionen zur Verfügung zu stellen und unter Beachtung des notwendigen Schutzes kritischer Infrastrukturen in einer bereinigten Version auf der RTR-Website zu veröffentlichen ist;
2. Mitwirkung an der Erstellung eines Mustersicherheitskonzepts für Betreiber gemäß § 4 Z 25 und Anbieter gemäß § 4 Z 36;
3. Mitwirkung in Arbeitsgruppen der ENISA sowie der NIS-Kooperationsgruppe.

(4) Eine Verordnung gemäß Abs. 1 ist in Bezug auf Rundfunknetze und die Übertragung von Rundfunksignalen von der KommAustria zu erlassen. Sind bei der Erledigung der in Abs. 3 genannten Aufgaben auch Rundfunknetze oder die Übertragung von Rundfunksignalen betroffen, ist insoweit das Einvernehmen mit der KommAustria herzustellen.“

2. In § 188 Abs. 5 entfallen die Z 1 bis 5 und erhalten die bisherigen Z 6 bis 16 die Ziffernbezeichnung „1.“ *bis* „11.“.

3. In § 198 entfällt Z 9 und erhalten die bisherigen Z 10 bis 26 die Ziffernbezeichnung „9.“ *bis* „25.“.

4. In § 200 Abs. 1 wird der Verweis „§ 198 Z 13, 17 und 20“ *durch den Verweis* „§ 198 Z 12, 16 und 19“ *ersetzt.*

5. In § 200 Abs. 5 wird der Verweis „§ 198 Z 13“ *durch den Verweis* „§ 198 Z 12“ *ersetzt.*

6. Dem § 217 wird folgender Abs. 4 angefügt:

„(4) § 44, § 188 Abs. 5, § 198 sowie § 200 Abs. 1 und 3 in der Fassung des Bundesgesetzes BGBl. I Nr. xxxx/xxxx treten mit xxxx in Kraft.“

Artikel 3
Änderung des Gesundheitstelematikgesetzes 2012

Das Gesundheitstelematikgesetz 2012, BGBl. I Nr. 111/2012, zuletzt geändert durch das Vereinbarungsumsetzungsgesetzes 2024 (VUG 2024), BGBl. I Nr. 191/2023, wird wie folgt geändert:

1. Im Inhaltsverzeichnis wird der Eintrag zu § 8a durch „Austrian Health CSIRT“*ersetzt.*

2. § 8a samt Überschrift lautet:

„Austrian Health CSIRT

§ 8a. (1) Der für das Gesundheitswesen zuständige Bundesminister oder die zuständige Bundesministerin hat zur Gewährleistung der Sicherheit von Netz- und Informationssystemen im Gesundheitswesen ein sektorspezifisches Computer-Notfallteam („Austrian Health CSIRT“**)** gemäß § 8 des Netz- und Informationssystemsicherheitsgesetz 2024 (NISG 2024), BGBl. I Nr. xxx/2024, für den Sektor Gesundheitswesen gemäß § 2 Z 5 NISG 2024 einzurichten und zu betreiben. Der für das Gesundheitswesen zuständige Bundesminister oder die zuständige Bundesministerin kann sich für die Wahrnehmung dieser Aufgabe des Austrian Health CSIRT eines Dienstleisters bedienen.

(2) Das Austrian Health CSIRT hat die Aufgaben gemäß § 8 Abs. 1 NISG 2024 für den Sektor Gesundheitswesen gemäß § 2 Z 5 NISG 2024 wahrzunehmen und dabei die Voraussetzungen gemäß § 9 NISG 2024 zu erfüllen.

(3) Wesentliche und wichtige Einrichtungen gemäß den §§ 24 ff NISG 2024 die dem Sektor Gesundheitswesen gemäß § 2 Z 5 NISG 2024 angehören, haben Meldungen gemäß den §§ 34 und 37 NISG 2024 an das Austrian Health CSIRT zu erbringen.“

3. Dem § 26 wird folgender Abs. xx angefügt:

„(18) Das Inhaltsverzeichnis sowie § 8a in der Fassung des Bundesgesetzes BGBl. I. Nr. xxx/2024 treten mit XXX in Kraft.“