Entwurf

Bundesgesetz zur Gewährleistung eines hohen Sicherheitsniveaus von Netz- und Informationssystemen (Netz- und Informationssystemsicherheitsgesetz – NISG)

Der Nationalrat hat beschlossen:

Inhaltsverzeichnis

1. Abschnitt
Allgemeine Bestimmungen

§ 1. Verfassungsbestimmung
§ 2. Gegenstand und Ziele des Gesetzes
§ 3. Begriffsbestimmungen

2. Abschnitt
Aufgaben und Strukturen

§ 4. Aufgaben des Bundeskanzlers
§ 5. Aufgaben des Bundesministers für Inneres
§ 6. Zentrale Anlaufstelle
§ 7. Koordinierungsstrukturen
§ 8. Strategie für die Sicherheit von Netz- und Informationssystemen

3. Abschnitt
Befugnisse und Datenverarbeitung

§ 9. Befugnisse zur Vorbeugung von Sicherheitsvorfällen
§ 10. Datenverarbeitung
§ 11. Gemeinsame Verarbeitung

4. Abschnitt
Computer-Notfallteams

§ 12. Aufgaben der Computer-Notfallteams
§ 13. Anforderungen und Eignung eines Computer-Notfallteams

5. Abschnitt
Verpflichtungen für Betreiber wesentlicher Dienste, Anbieter digitaler Dienste und Einrichtungen des Bundes

§ 14. Ermittlung der Betreiber wesentlicher Dienste
§ 15. Sicherheitsvorkehrungen für Betreiber wesentlicher Dienste
§ 16. Meldepflicht für Betreiber wesentlicher Dienste
§ 17. Ausnahmen von Verpflichtungen für Betreiber wesentlicher Dienste
§ 18. Sicherheitsvorkehrungen und Meldepflicht für Anbieter digitaler Dienste
§ 19. Sicherheitsvorkehrungen und Meldepflicht für Einrichtungen des Bundes
§ 20. Freiwillige Meldungen

6. Abschnitt
Strukturen und Aufgaben im Falle der Cyberkrise

§ 21. Cyberkrise

§ 22. Koordinationsausschuss

7. Abschnitt
Strafbestimmungen

§ 23. Verwaltungsstrafbestimmungen

8. Abschnitt
Schlussbestimmungen

§ 24. Personenbezogene Bezeichnungen
§ 25. Bezugnahme auf Richtlinien
§ 26. Verweisungen
§ 27. Vollziehung
§ 28. Inkrafttreten

1. Abschnitt
Allgemeine Bestimmungen

Verfassungsbestimmung

§ 1. (Verfassungsbestimmung) Die Erlassung, Aufhebung 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 diesen Vorschriften geregelten Angelegenheiten können in unmittelbarer Bundesverwaltung besorgt werden.

Gegenstand und Ziele des Gesetzes

§ 2. (1) Mit diesem Bundesgesetz werden Maßnahmen festgelegt, mit denen ein hohes Sicherheitsniveau von Netz- und Informationssystemen von Betreibern wesentlicher Dienste (§ 3 Z 8) in den Sektoren

1. Energie,
2. Verkehr,
3. Bankwesen,
4. Finanzmarktinfrastrukturen,
5. Gesundheitswesen,
6. Trinkwasserversorgung und
7. Digitale Infrastruktur

sowie von Anbietern digitaler Dienste (§ 3 Z 10) und Einrichtungen des Bundes (§ 3 Z 15) erreicht werden soll. Diese Betreiber, Anbieter und Einrichtungen sind von hoher Bedeutung für das Funktionieren des Gemeinwesens, weil durch einen Sicherheitsvorfall (§ 3 Z 6) Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit oder Funktionsfähigkeit von staatlichen Einrichtungen eintreten würden.

(2) Zu diesem Zweck sieht dieses Bundesgesetz insbesondere Folgendes vor:

1. die Festlegung von Aufgaben und Behördenzuständigkeiten (§§ 4 und 5) sowie Befugnissen zur Gewährleistung eines hohen Sicherheitsniveaus von Netz- und Informationssystemen (§§ 9 bis 11);
2. die Einrichtung einer zentralen Anlaufstelle (Single Point of Contact - SPOC; § 6);
3. die Einrichtung einer nationalen Koordinierungsstruktur (§ 7);
4. die Festlegung einer nationalen Strategie für die Sicherheit von Netz- und Informationssystemen (§ 8);
5. die Einrichtung von Computer-Notfallteams (§§ 12 und 13);
6. die Verpflichtung zur Einrichtung von Sicherheitsvorkehrungen und Festlegung von Meldepflichten für Betreiber wesentlicher Dienste (§§ 15 und 16), Anbieter digitaler Dienste (§ 18) und Einrichtungen des Bundes (§ 19).

Begriffsbestimmungen

§ 3. Im Sinne dieses Bundesgesetzes bedeutet

1. „Netz- und Informationssystem“
   a) ein elektronisches Kommunikationsnetz im Sinne des § 3 Z 11 Telekommunikationsgesetz 2003 (TKG 2003), BGBl. I Nr. 70/2003,

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

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

2. „Netz- und Informationssystemsicherheit (NIS)“ die Fähigkeit von Netz- und Informationssystemen, Sicherheitsvorfällen (Z 6) vorzubeugen, diese abzuwehren und zu beseitigen;
3. „NIS-RL“ die Richtlinie (EU) 2016/1148 über Maßnahmen zur Gewährleistung eines hohen Sicherheitsniveaus von Netz- und Informationssystemen in der Union, ABl. Nr. L 194 vom 19.07.2016 S. 1;
4. „NIS-Büros“ die beim Bundeskanzler und Bundesminister für Inneres jeweils zur Erfüllung der diesen gemäß §§ 4 und 5 zugewiesenen Aufgaben eingerichteten Organisationseinheiten;
5. „Operative Koordinierungsstruktur (OpKoord)“ eine Struktur zur Koordination auf der operativen Ebene im Bereich der Netz- und Informationssystemsicherheit;
6. „Sicherheitsvorfall“ eine erhebliche Störung der Verfügbarkeit, Integrität, Authentizität oder Vertraulichkeit von Netz- und Informationssystemen, die zu einem Ausfall oder einer Einschränkung der Verfügbarkeit des betriebenen wesentlichen oder digitalen Dienstes geführt hat; bei der Beurteilung der Erheblichkeit sind insbesondere folgende Parameter zu berücksichtigen: Die voraussichtliche
   a) Zahl der von dem Sicherheitsvorfall betroffenen Nutzer, insbesondere der Nutzer, die den Dienst für die Bereitstellung ihrer eigenen Dienste benötigen,
   b) Dauer des Sicherheitsvorfalls,
   c) geografische Ausbreitung in Bezug auf das von dem Sicherheitsvorfall betroffene Gebiet und
   d) Auswirkung auf wirtschaftliche und gesellschaftliche Tätigkeiten;
7. „Risiko“ alle Umstände oder Ereignisse, die potenziell nachteilige Auswirkungen auf die Sicherheit von Netz- und Informationssystemen haben;
8. „Betreiber wesentlicher Dienste“ eine Einrichtung, die einen wesentlichen Dienst (§ 14 Abs. 2) in einem der in § 2 Abs. 1 genannten Sektoren erbringt;
9. „digitaler Dienst“ ein Dienst im Sinne des § 3 Z 1 E-Commerce-Gesetz (ECG), BGBl. I Nr. 152/2001, bei dem es sich um einen Online-Marktplatz (Z 12), eine Online-Suchmaschine (Z 13) oder einen Cloud-Computing-Dienst (Z 14) handelt;
10. „Anbieter digitaler Dienste“ eine juristische Person
    a) mit Hauptniederlassung in Österreich oder
    b) ohne Hauptniederlassung in der Europäischen Union, die einen Vertreter (Z 11) namhaft gemacht hat,

    und einen digitalen Dienst (Z 9) in Österreich anbietet und kein Kleinstunternehmen oder kleines Unternehmen im Sinne von Art. 1 und Art. 2 Abs. 2 und 3 des Anhangs der Empfehlung 2003/361/EG der Kommission vom 6. Mai 2003 betreffend die Definition der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen, ABl. Nr. L 124 vom 20.05.2003 S. 36, ist;
11. „Vertreter“ eine in Österreich niedergelassene natürliche oder juristische Person, die ausdrücklich benannt wurde, um im Auftrag eines nicht in der Europäischen Union niedergelassenen Anbieters digitaler Dienste zu handeln, und an die sich die NIS-Büros oder Computer-Notfallteams – statt an den Anbieter digitaler Dienste – hinsichtlich der Pflichten dieses Anbieters digitaler Dienste gemäß diesem Bundesgesetz wenden können;
12. „Online-Marktplatz“ einen digitalen Dienst, der es Verbrauchern oder Unternehmern ermöglicht, Online-Kaufverträge oder Online-Dienstleistungsverträge mit Unternehmern entweder auf der Website des Online-Marktplatzes oder auf der Website eines Unternehmers, die von dem Online-Marktplatz bereitgestellte Rechendienste verwendet, abzuschließen;
13. „Online-Suchmaschine“ einen digitalen Dienst, der es Nutzern ermöglicht, Suchen grundsätzlich auf allen Websites oder auf Websites in einer bestimmten Sprache anhand einer Abfrage zu einem beliebigen Thema in Form eines Stichworts, einer Wortgruppe oder einer anderen Eingabe vorzunehmen, und der daraufhin Links anzeigt, über die Informationen im Zusammenhang mit dem angeforderten Inhalt gefunden werden können;

14. „Cloud-Computing-Dienst“ einen digitalen Dienst, der den Zugang zu einem skalierbaren und elastischen Pool gemeinsam nutzbarer Rechenressourcen ermöglicht;
15. „Einrichtungen des Bundes“ die Bundesministerien, die Gerichtshöfe des öffentlichen Rechts, der Rechnungshof, die Volksanwaltschaft, die Präsidentschaftskanzlei und die Parlamentsdirektion; weitere Dienststellen können vom zuständigen Bundesminister durch Verordnung bestimmt werden;
16. „Kooperationsgruppe“ ein gemäß Art. 11 NIS-RL (Z 3) eingerichtetes Gremium, das sich aus Vertretern der Mitgliedstaaten der Europäischen Union, der Europäischen Kommission und der Europäischen Agentur für Netz- und Informationssicherheit (ENISA) zusammensetzt und der Unterstützung und Erleichterung der strategischen Zusammenarbeit sowie des Informationsaustausches zwischen den Mitgliedstaaten der Europäischen Union zum Aufbau von Vertrauen und zur Erreichung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Europäischen Union dient;
17. „CSIRT-Netzwerk“ ein gemäß Art. 12 NIS-RL (Z 3) eingerichtetes Gremium, das sich aus Vertretern der Computer-Notfallteams der Mitgliedstaaten der Europäischen Union und des europäischen Computer-Notfallteams zusammensetzt, und zum Aufbau von Vertrauen zwischen den Mitgliedstaaten der Europäischen Union beitragen und eine rasche und wirksame operative Zusammenarbeit fördern soll;
18. „Cyberkrise“ ein Sicherheitsvorfall, der eine gegenwärtige und unmittelbare Gefahr für die Aufrechterhaltung wichtiger gesellschaftlicher Funktionen darstellt und schwerwiegende Auswirkungen auf die Gesundheit, Sicherheit oder das wirtschaftliche und soziale Wohl großer Teile der Bevölkerung oder das effektive Funktionieren von staatlichen Einrichtungen nach sich ziehen kann;
19. „Cyberkrisenmanagement“ ein Koordinierungsverfahren zur Bewältigung von Cyberkrisen.

2. Abschnitt
Aufgaben und Strukturen

Aufgaben des Bundeskanzlers

§ 4. (1) Dem Bundeskanzler kommen folgende strategische Aufgaben zu:

1. Koordination einer Strategie (§ 8) und eines jährlichen Berichts zur Sicherheit von Netz- und Informationssystemen;
2. Vertretung von Österreich in der Kooperationsgruppe (§ 3 Z 16) sowie in anderen EU-weiten und internationalen Gremien für Netz- und Informationssystemsicherheit, denen strategische Aufgaben zugewiesen sind;
3. Koordination der öffentlich-privaten Zusammenarbeit im Rahmen der Österreichischen Strategie für Cyber Sicherheit (ÖSCS) und der Cybersicherheitsstrategie der Europäischen Union;
4. Festlegen von Kriterien für die Parameter des § 3 Z 6 lit. a bis d (§ 16 Abs. 7);
5. Unterrichtung der Öffentlichkeit über einen Sicherheitsvorfall, der mehrere der in § 2 Abs. 1 genannten Sektoren betrifft;
6. Ermittlung von Betreibern wesentlicher Dienste sowie Erstellung und laufende Aktualisierung einer Liste von Diensten, die gemäß § 14 Abs. 2 als wesentlich gelten (§ 14 Abs. 1);
7. Festlegen von Sicherheitsvorkehrungen für Betreiber wesentlicher Dienste, die jedenfalls zur Gewährleistung der Anforderungen nach § 15 Abs. 1 geeignet sind (§ 15 Abs. 6);
8. Konsultation mit den zuständigen Behörden anderer Mitgliedstaaten, wenn Anbieter digitaler Dienste ihre Hauptniederlassung in Österreich haben, sich ihre Netz- und Informationssysteme aber in einem anderen Mitgliedstaat befinden.

Aufgaben des Bundesministers für Inneres

§ 5. Dem Bundesminister für Inneres kommen folgende operative zentrale Aufgaben zu:

1. Betrieb einer zentralen Anlaufstelle (SPOC) für die Sicherheit von Netz- und Informationssystemen (§ 6);
2. Koordination der Operativen Koordinierungsstruktur (OpKoord) und des Inneren Kreises der Operativen Koordinierungsstruktur (IKDOK; § 7);
3. Entgegennahme und Analyse von Meldungen über Sicherheitsvorfälle und sonstige Störungen (§§ 16, 17 Abs. 2 und §§ 18 bis 20), regelmäßige Erstellung eines diesbezüglichen Lagebildes und die Weiterleitung der Meldungen sowie des Lagebildes und zusätzlicher relevanter

Informationen an inländische Behörden oder Stellen, insbesondere die Operative Koordinierungsstruktur (§ 7), soweit dies für den Empfänger eine wesentliche Voraussetzung zur Wahrnehmung einer ihm gesetzlich übertragenen Aufgabe bildet;

4. Erstellung und Weitergabe von zur Gewährleistung der Sicherheit von Netz- und Informationssystemen relevanten Informationen zur Vorbeugung von Sicherheitsvorfällen (§ 3 Z 6);
5. Überprüfung der Sicherheitsvorkehrungen (§§ 15 und 18) und die Einhaltung der Meldepflicht (§§ 16 und 18);
6. Unterrichtung der Öffentlichkeit über einzelne Sicherheitsvorfälle (§ 16 Abs. 6);
7. Leitung und Koordination des Cyberkrisenmanagements auf operativer Ebene (§§ 21 f).

Zentrale Anlaufstelle

§ 6. (1) Die für die Sicherheit von Netz- und Informationssystemen zuständige zentrale Anlaufstelle (SPOC) dient als Verbindungsstelle zur Gewährleistung der grenzüberschreitenden Zusammenarbeit mit den zuständigen Stellen in den anderen Mitgliedstaaten der Europäischen Union sowie der Kooperationsgruppe (§ 3 Z 16) und dem CSIRT-Netzwerk (§ 3 Z 17).

(2) Die zentrale Anlaufstelle

1. leitet eingehende Meldungen und Anfragen unmittelbar an die Mitglieder des IKDOK (§ 7) und Computer-Notfallteams (§ 12) weiter, soweit dies zur Erfüllung einer gesetzlich übertragenen Aufgabe dieser Behörden oder Computer-Notfallteams erforderlich ist und
2. unterrichtet über Aufforderung die zentralen Anlaufstellen in anderen Mitgliedstaaten, wenn ein Sicherheitsvorfall einen oder mehrere andere Mitgliedstaaten der Europäischen Union betrifft (§§ 16 Abs. 5, 18 Abs. 3 und 19 Abs. 4).

Koordinierungsstrukturen

§ 7. (1) Zur Erörterung und Aktualisierung des vom Bundesminister für Inneres erstellten Lagebildes über Risiken und Sicherheitsvorfälle, zur Erörterung der Erkenntnisse, die gemäß § 9 Abs. 1 und 2 sowie § 12 Abs. 4 letzter Satz gewonnen wurden, und zur Unterstützung des Koordinationsausschusses (§ 22) im Cyberkrisenmanagement wird ein IKDOK eingerichtet. Dieser setzt sich aus den NIS-Büros sowie einem Vertreter des Bundesministeriums für Landesverteidigung und des Bundesministeriums für Europa, Integration und Äußeres zusammen. Der IKDOK dient auch dem Austausch klassifizierter Informationen zwischen den Teilnehmern zur Wahrnehmung der Aufgaben nach Maßgabe ihrer Zuständigkeiten.

(2) Zur Erörterung eines gesamtheitlichen Lagebildes, das auch die freiwilligen Meldungen (§ 19 Abs. 3 und § 20) enthält, wird eine OpKoord (§ 3 Z 5) eingerichtet. Diese setzt sich aus dem IKDOK und den Computer-Notfallteams (§ 12) zusammen. Die OpKoord kann um Vertreter von Betreibern wesentlicher Dienste, Anbietern digitaler Dienste sowie Einrichtungen des Bundes erweitert werden, wenn deren Wirkungsbereich von einem Sicherheitsvorfall betroffen ist.

(3) Der Bundesminister für Inneres kann nähere Regelungen zum Zusammenwirken der Koordinierungsstrukturen gemäß Abs. 1 und 2, insbesondere über die Einberufung von Sitzungen, die Zusammensetzung sowie deren Entscheidungsfindung in einer Geschäftsordnung treffen.

Strategie für die Sicherheit von Netz- und Informationssystemen

§ 8. (1) Die Strategie für die Sicherheit von Netz- und Informationssystemen bestimmt die strategischen Ziele und angemessenen Politik- und Regulierungsmaßnahmen, mit denen ein hohes Sicherheitsniveau von Netz- und Informationssystemen im Bundesgebiet erreicht und aufrecht erhalten werden soll.

(2) Der Bundeskanzler teilt die Strategie für die Sicherheit von Netz- und Informationssystemen der Europäischen Kommission innerhalb von drei Monaten nach ihrer Festlegung mit. Elemente der Strategie, die die nationale Sicherheit berühren, sind nicht mitzuteilen.

3. Abschnitt
Befugnisse und Datenverarbeitung

Befugnisse zur Vorbeugung von Sicherheitsvorfällen

§ 9. (1) Der Bundesminister für Inneres ist zur Erfüllung der Aufgabe gemäß § 5 Z 4 ermächtigt, technische Einrichtungen zu betreiben, die Unregelmäßigkeiten oder Störungen von Netz- und Informationssystemen frühzeitig erkennen. Betreiber wesentlicher Dienste, Anbieter digitaler Dienste und

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

(2) Der Bundesminister für Inneres ist zur Erfüllung der Aufgabe gemäß § 5 Z 4 ermächtigt, technische Einrichtungen zu betreiben oder zu nutzen, um die Muster von Angriffen auf Netz- und Informationssysteme zu erkennen.

Datenverarbeitung

§ 10. (1) Der Bundeskanzler und der Bundesminister für Inneres dürfen die zur Wahrnehmung ihrer Aufgaben nach diesem Bundesgesetz (§§ 4 und 5) erforderlichen personenbezogenen Daten verarbeiten.

(2) Darüber hinaus ist der Bundesminister für Inneres zur Erfüllung der Aufgaben gemäß § 5 Z 4 und 5 ermächtigt, Identifikations- und Erreichbarkeitsdaten von Betreibern wesentlicher Dienste sowie Anbietern digitaler Dienste, die Aufstellung der vorhandenen Sicherheitsvorkehrungen sowie aufgedeckten Sicherheitsmängel (§ 15 Abs. 3), das Ergebnis der Einschau in die Netz- und Informationssysteme und diesbezügliche Unterlagen und die ausgesprochenen Empfehlungen (§ 15 Abs. 3), die Daten gemäß § 9 Abs. 1 und 2 sowie Verwaltungsdaten zu verarbeiten.

(3) Jedes NIS-Büro darf von dem anderen NIS-Büro, den Computer-Notfallteams und den Betreibern wesentlicher Dienste und Anbietern digitaler Dienste jene Auskünfte verlangen, die sie als wesentliche Voraussetzung zur Erfüllung ihrer Aufgaben benötigt. Die ersuchten Stellen sind verpflichtet, unverzüglich Auskunft zu erteilen.

(4) Jede Abfrage, Übermittlung und Änderung personenbezogener Daten ist so zu protokollieren, dass eine Zuordnung zu einem NIS-Büro möglich ist. Die Protokollaufzeichnungen sind drei Jahre aufzubewahren und danach zu löschen.

Gemeinsame Verarbeitung

§ 11. (1) Der Bundeskanzler, der Bundesminister für Inneres und der Bundesminister für Landesverteidigung sind als gemeinsam Verantwortliche gemäß Art. 4 Z 7 iVm Art. 26 Abs. 1 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 (Datenschutz-Grundverordnung), ABl. Nr. L 119 vom 4.5.2016 S. 1, (im Folgenden: DSGVO) zum Zweck der Bewertung von Risiken für Netz- und Informationssysteme sowie zur Erstellung eines Lagebilds mittels strategischer oder operativer Analyse ermächtigt, personenbezogene Daten nach Maßgabe der folgenden Bestimmungen in der Art gemeinsam zu verarbeiten, dass jeder Verantwortliche auch auf jene Daten in der Datenverarbeitung Zugriff hat, die dieser vom anderen Verantwortlichen zur Verfügung gestellt wurden. Es dürfen zu natürlichen und juristischen Personen, die mit einem Sicherheitsvorfall oder einer sonstigen Störung in unmittelbarer Verbindung stehen, die erforderlichen Identifikations- und Erreichbarkeitsdaten sowie die erforderlichen Sachdaten einschließlich Daten zu Zeit, Ort, Grund und Art des Sicherheitsvorfalls oder der sonstigen Störung sowie weitere in der Meldung (§§ 16 ff) enthaltene Informationen und Verwaltungsdaten verarbeitet werden. Gleiches gilt für die Erkenntnisse, die gemäß § 9 Abs. 1 und 2 gewonnen wurden.

(2) Die Erfüllung von Informations-, Auskunfts-, Berichtigungs-, Löschungs- und sonstigen Pflichten nach den Bestimmungen der DSGVO gegenüber der betroffenen Person obliegt jedem Verantwortlichen nur hinsichtlich jener personenbezogener Daten, die im Zusammenhang mit den von ihm geführten Verfahren oder den von ihm gesetzten Maßnahmen verarbeitet werden. Nimmt eine betroffene Person unter Nachweis ihrer Identität ein Recht nach der DSGVO gegenüber einem gemäß dem ersten Satz unzuständigen Verantwortlichen wahr, ist sie an den zuständigen Verantwortlichen zu verweisen.

(3) Der Bundesminister für Inneres übt die Funktion des Auftragsverarbeiters gemäß Art. 4 Z 8 iVm Art. 28 Abs. 1 DSGVO aus. Er ist in dieser Funktion verpflichtet, die Datenschutzpflichten gemäß Art. 28 Abs. 3 lit. a bis h DSGVO wahrzunehmen.

(4) Übermittlungen durch die NIS-Büros der gemäß § 10 Abs. 1 und 2 sowie Übermittlungen durch die NIS-Büros und den Bundesminister für Landesverteidigung der gemäß Abs. 1 verarbeiteten personenbezogenen Daten sind zulässig an Sicherheitsbehörden für Zwecke der Sicherheitspolizei und Strafrechtspflege, an militärische Organe und Behörden für Zwecke der militärischen Landesverteidigung gemäß Art. 79 Abs. 1 B-VG, an die Datenschutzbehörde für Zwecke des Art. 33 DSGVO, an Staatsanwaltschaften und ordentliche Gerichte für Zwecke der Strafrechtspflege und an sonstige in- und

ausländische Behörden oder Stellen, soweit dies zur Aufgabenerfüllung erforderlich ist. Im Übrigen sind Übermittlungen nur zulässig, wenn hiefür eine ausdrückliche gesetzliche Ermächtigung besteht.

(5) Die Protokollierungsregelung des § 10 Abs. 4 findet auch auf diese Bestimmung Anwendung.

4. Abschnitt
Computer-Notfallteams

Aufgaben der Computer-Notfallteams

§ 12. (1) Zur Unterstützung der Betreiber wesentlicher Dienste und Anbieter digitaler Dienste bei der Bewältigung von Risiken und Sicherheitsvorfällen wird ein nationales Computer-Notfallteam eingerichtet. Betreiber wesentlicher Dienste können für ihren Sektor (§ 2 Abs. 1) ein sektorenspezifisches Computer-Notfallteam einrichten.

(2) Computer-Notfallteams gemäß Abs. 1 kommen jedenfalls folgende Aufgaben zu

1. Entgegennahme von Meldungen (§§ 16, 18 Abs. 2 und 20) über Sicherheitsvorfälle oder sonstige Störungen bei Betreibern wesentlicher Dienste oder Anbietern digitaler Dienste;
2. Weiterleitung von Meldungen (Z 1) an den Bundesminister für Inneres;
3. Ausgabe von Frühwarnungen, Alarmmeldungen und Handlungsempfehlungen sowie Bekanntmachung und Verbreitung von Informationen über Risiken und Sicherheitsvorfälle;
4. Erste allgemeine technische Unterstützung bei der Reaktion auf einen Sicherheitsvorfall;
5. Beobachtung und Analyse von Risiken und Sicherheitsvorfällen sowie Lagebeurteilung;
6. Teilnahme an der OpKoord (§ 7 Abs. 2) und Beteiligung am CSIRT-Netzwerk (§ 3 Z 17).

(3) Sektorenspezifische Computer-Notfallteams (Abs. 1 zweiter Satz) können für Zwecke des Abs. 2 Z 3 und 5 im Auftrag eines Betreibers wesentlicher Dienste Daten gemäß § 9 Abs. 1 zweiter Satz analysieren, die durch eine bei diesem Betreiber wesentlicher Dienste eingerichteten technischen Einrichtung gemäß § 9 Abs. 1 erster Satz gewonnen wurden. Für Anbieter digitaler Dienste gilt dies mit der Maßgabe, dass sie das nationale Computer-Notfallteam dazu beauftragen können.

(4) Das Computer-Notfallteam der öffentlichen Verwaltung (GovCERT) ist beim Bundeskanzler eingerichtet. Neben der Entgegennahme und Weiterleitung von Meldungen gemäß § 19 Abs. 2 und 3 kommen dem GovCERT die Aufgaben gemäß Abs. 2 Z 3 bis 5 und Abs. 3 in Hinblick auf die Einrichtungen des Bundes, soweit es sich dabei nicht um das Bundeskanzleramt oder das Bundesministerium für Inneres handelt, zu. Das GovCERT ist ermächtigt, technische Einrichtungen zu betreiben oder zu nutzen, um die Muster von Angriffen auf Netz- und Informationssysteme zu erkennen.

(5) Das GovCERT und das nationale Computer-Notfallteam informieren ohne unnötigen Aufschub die NIS-Büros über Aktivitäten des CSIRT-Netzwerks, die zur jeweiligen Aufgabenerfüllung erforderlich sind, und nehmen an dessen Sitzungen teil.

(6) Computer-Notfallteams können die Aufgaben gemäß Abs. 2 Z 3 bis 5 auch gegenüber sonstigen Einrichtungen oder Personen wahrnehmen, sofern diese von einem Risiko oder einer Störung ihrer Netz- und Informationssysteme betroffen sind.

(7) Die Computer-Notfallteams sind zur Verarbeitung von personenbezogenen Daten ermächtigt, soweit dies zur Erfüllung der Aufgaben gemäß Abs. 2 erforderlich ist. Es dürfen zu natürlichen und juristischen Personen, die mit einem Sicherheitsvorfall oder einer sonstigen Störung in unmittelbarer Verbindung stehen, die erforderlichen Identifikations- und Erreichbarkeitsdaten sowie die erforderlichen Sachdaten einschließlich Daten zu Zeit, Ort, Grund und Art des Sicherheitsvorfalls oder der sonstigen Störung sowie weitere in der Meldung (§§ 16 ff) enthaltene Informationen und Verwaltungsdaten verarbeitet werden.

Anforderungen und Eignung eines Computer-Notfallteams

§ 13. (1) Computer-Notfallteams gemäß § 12 Abs. 1 haben jedenfalls folgende Anforderungen zu erfüllen:

1. Ihre Räumlichkeiten und die unterstützenden Netz- und Informationssysteme entsprechen den in Art. 32 DSGVO festgelegten Standards und werden an sicheren Standorten eingerichtet.
2. Ihre Betriebskontinuität ist sichergestellt, insbesondere durch
   a) die Verwendung eines geeigneten Systems zur Verwaltung und Weiterleitung von Anfragen und
   b) eine personelle, technische und infrastrukturelle Ausstattung, die eine ständige Bereitschaft und Verfügbarkeit gewährleistet.

3. Nachweis über die Unterstützung von Betreibern wesentlicher Dienste, wenn es sich um ein Computer-Notfallteam gemäß § 12 Abs. 1 zweiter Satz handelt.
4. Das zur Erfüllung der Aufgaben nach § 12 Abs. 2 heranzuziehende Personal ist fachlich geeignet und hat sich vor Beginn der Tätigkeit einer Sicherheitsüberprüfung gemäß §§ 55 ff des Sicherheitspolizeigesetzes (SPG), BGBl. Nr. 566/1991, für den Zugang zu geheimer Information zu unterziehen. Die Sicherheitsüberprüfung ist alle fünf Jahre zu wiederholen. Für die Durchführung der Sicherheitsüberprüfung ist vom Ersuchenden ein Pauschalsatz in der Höhe des in § 5 der Sicherheitsgebühren-Verordnung (SGV), BGBl. Nr. 389/1996, vorgesehenen Betrages zu entrichten.

(2) Das GovCERT hat die Anforderungen gemäß Abs. 1 mit Ausnahme von Z 3 zu erfüllen.

(3) Der Bundeskanzler hat im Einvernehmen mit dem Bundesminister für Inneres festzustellen, dass das nationale Computer-Notfallteam sowie über Antrag ein sektorenspezifisches Computer-Notfallteam die Anforderungen gemäß Abs. 1 erfüllt und geeignet ist, die Aufgaben gemäß § 12 Abs. 2 wahrzunehmen. Sofern es sich bei einem Computer-Notfallteam um eine private Einrichtung handelt, ist diese vom Bundeskanzler im Einvernehmen mit dem Bundesminister für Inneres zur Erfüllung der Aufgaben gemäß § 12 Abs. 2 Z 1 und 2 zu ermächtigen. Computer-Notfallteams haben Veränderungen hinsichtlich jener Umstände, die Voraussetzung für die Feststellung der Eignung oder die Erteilung der Ermächtigung waren, unverzüglich dem Bundeskanzler anzuzeigen. Die Ermächtigung ist ganz oder nur hinsichtlich der Erfüllung einzelner Aufgaben zu widerrufen, wenn eine für die Erteilung der Ermächtigung erforderliche Voraussetzung nicht mehr gegeben ist.

5. Abschnitt

Verpflichtungen für Betreiber wesentlicher Dienste, Anbieter digitaler Dienste und Einrichtungen des Bundes

Ermittlung der Betreiber wesentlicher Dienste

§ 14. (1) Nach Befassung des Bundesministers für Inneres und des zuständigen Bundesministers ermittelt der Bundeskanzler für jeden in § 2 Abs. 1 genannten Sektor jene Betreiber wesentlicher Dienste mit einer Niederlassung in Österreich, die einen wesentlichen Dienst gemäß Abs. 2 erbringen.

(2) Als wesentlich gilt ein Dienst, der eine wesentliche Bedeutung für die Aufrechterhaltung des öffentlichen Gesundheitsdienstes, der öffentlichen Versorgung mit Wasser, Energie sowie lebenswichtigen Gütern, des öffentlichen Verkehrs oder die Funktionsfähigkeit öffentlicher Informations- und Kommunikationstechnologie hat und dessen Verfügbarkeit zu einem überwiegenden Teil abhängig von Netz- und Informationssystemen ist. Für die Beurteilung, ob ein Dienst eine wesentliche Bedeutung hat, sind jedenfalls die folgenden sektorenübergreifenden Faktoren zu berücksichtigen:

a) Zahl der Nutzer, die den vom jeweiligen Betreiber eines wesentlichen Dienstes angebotenen Dienst in Anspruch nehmen;
b) Abhängigkeit anderer in § 2 Abs. 1 genannter Sektoren von dem von diesem Betreiber angebotenen Dienst;
c) Marktanteil des Betreibers wesentlicher Dienste;
d) geografische Ausbreitung des Gebiets, das von einem Sicherheitsvorfall betroffen sein könnte;
e) Auswirkungen von Sicherheitsvorfällen hinsichtlich Ausmaß und Dauer auf wirtschaftliche oder gesellschaftliche Tätigkeiten oder die öffentliche Sicherheit;
f) Bedeutung des Betreibers wesentlicher Dienste für die Aufrechterhaltung des Dienstes in ausreichendem Umfang, unter Berücksichtigung der Verfügbarkeit von alternativen Mitteln für die Bereitstellung des jeweiligen Dienstes.

Darüber hinaus sind bei Bedarf auch sektorenspezifische Faktoren zu berücksichtigen.

(3) Betreiber wesentlicher Dienste haben dem Bundeskanzler innerhalb von zwei Wochen nach Zustellung des Bescheids gemäß Abs. 5 Z 1 eine Kontaktstelle für die Kommunikation mit den NIS-Büros und den Computer-Notfallteams zu nennen. Der Betreiber wesentlicher Dienste hat sicherzustellen, dass er über diese Kontaktstelle jedenfalls in jenem Zeitraum erreichbar ist, in dem er einen wesentlichen Dienst gemäß Abs. 2 zur Verfügung stellt. Er hat Änderungen der Kontaktstelle unverzüglich bekanntzugeben.

(4) Der Bundeskanzler kann im Einvernehmen mit dem Bundesminister für Inneres mit Verordnung für jeden in § 2 Abs. 1 genannten Sektor nähere Regelungen zu diesem sowie zu den sektorenübergreifenden Faktoren gemäß Abs. 2 lit. a bis f treffen und weitere sektorenspezifische

Faktoren gemäß Abs. 2 letzter Satz sowie jene Vorschriften zu Sicherheitsvorkehrungen und zur Meldepflicht, die zumindest ein gleichwertiges Sicherheitsniveau für Netz- und Informationssysteme gewährleisten (§ 17), festlegen.

(5) Für die Zwecke des Abs. 1 erfüllt der Bundeskanzler folgende Aufgaben:

1. Erlassung eines Bescheids, mit dem ein Betreiber wesentlicher Dienste gemäß Abs. 1 ermittelt wird. Dieser ist zu widerrufen, wenn Umstände über den Wegfall der Voraussetzungen für die Ermittlung bekannt werden.
2. Aufnahme von Konsultationen mit anderen Mitgliedstaaten der Europäischen Union, falls ein Betreiber wesentlicher Dienste einen Dienst gemäß Abs. 2 noch in einem oder mehreren Mitgliedstaaten der Europäischen Union bereitstellt. Die Entscheidung, ob ein Betreiber wesentlicher Dienste gemäß Abs. 1 zu ermitteln ist, kann erst nach erfolgter Konsultation mit dem oder den anderen Mitgliedstaaten der Europäischen Union getroffen werden.
3. Erstellung und laufende Aktualisierung einer Liste von Diensten, die gemäß Abs. 2 als wesentlich gelten.
4. Übermittlung der Liste (Z 3) an die Europäische Kommission mindestens alle zwei Jahre.

Sicherheitsvorkehrungen für Betreiber wesentlicher Dienste

§ 15. (1) Die Betreiber wesentlicher Dienste haben in Hinblick auf die von ihnen betriebenen wesentlichen Dienste (§ 14 Abs. 2) geeignete, dem Stand der Technik entsprechende Sicherheitsvorkehrungen zur Gewährleistung der NIS (§ 3 Z 2) zu treffen.

(2) Gemeinsam mit ihren Sektorenverbänden können die Betreiber wesentlicher Dienste sektorenspezifische Sicherheitsvorkehrungen zur Gewährleistung der Anforderungen nach Abs. 1 vorschlagen. Der Bundesminister für Inneres stellt auf Antrag fest, ob diese geeignet sind, die Anforderungen nach Abs. 1 zu erfüllen.

(3) Die Betreiber wesentlicher Dienste haben mindestens alle drei Jahre die Erfüllung der Anforderungen nach Abs. 1 auf geeignete Weise gegenüber dem Bundesminister für Inneres nachzuweisen. Dieser Nachweis kann ein Jahr nach Zustellung des Bescheids gemäß § 14 Abs. 5 Z 1 jederzeit verlangt werden. Zu diesem Zweck übermitteln die Betreiber wesentlicher Dienste eine Aufstellung der vorhandenen Sicherheitsvorkehrungen durch den Nachweis von Zertifizierungen oder durchgeführten Überprüfungen durch qualifizierte Stellen (Abs. 4), einschließlich der dabei aufgedeckten Sicherheitsmängel. Der Bundesminister für Inneres kann zur Kontrolle der Einhaltung der Anforderungen nach Abs. 1 Einschau in die Netz- und Informationssysteme und diesbezügliche Unterlagen nehmen. Zur Herstellung der Anforderungen nach Abs. 1 ist der Bundesminister für Inneres ermächtigt, Empfehlungen auszusprechen, für deren Befolgung und entsprechenden Nachweis erforderlichenfalls eine angemessene Frist zu setzen ist, widrigenfalls die Befolgung bescheidmäßig angeordnet wird.

(4) Der Bundesminister für Inneres sieht im Einvernehmen mit dem Bundeskanzler Erfordernisse, die eine qualifizierte Stelle erfüllen muss, durch Verordnung vor und entscheidet über das Vorliegen einer qualifizierten Stelle mittels Bescheid. Darüber hinaus kann er besondere Kriterien bestimmen, nach denen eine Stelle jedenfalls als qualifiziert gilt.

(5) Der Bundesminister für Inneres kann zur Kontrolle der Einhaltung der Erfordernisse an und Kriterien für qualifizierte Stellen nach Abs. 4 Einschau in deren Netz- und Informationssysteme und diesbezügliche Unterlagen nehmen.

(6) Der Bundeskanzler kann im Einvernehmen mit dem Bundesminister für Inneres Sicherheitsvorkehrungen, die jedenfalls zur Gewährleistung der Anforderungen nach Abs. 1 geeignet sind, durch Verordnung festlegen.

Meldepflicht für Betreiber wesentlicher Dienste

§ 16. (1) Die Betreiber wesentlicher Dienste haben das Vorliegen eines Sicherheitsvorfalls (§ 3 Z 6) unverzüglich an das für sie zuständige Computer-Notfallteam (Abs. 2) zu melden, das die Meldung unverzüglich an den Bundesminister für Inneres weiterleitet.

(2) Zuständig für die Entgegennahme der Meldung gemäß Abs. 1 ist das sektorenspezifische Computer-Notfallteam (§ 12 Abs. 1 zweiter Satz), sofern ein solches eingerichtet ist und der betroffene Betreiber wesentlicher Dienste dieses unterstützt (§ 13 Abs. 1 Z 3), andernfalls das nationale Computer-Notfallteam (§ 12 Abs. 1 erster Satz).

(3) Die Meldung muss sämtliche Angaben zum Sicherheitsvorfall und den technischen Rahmenbedingungen, die im Zeitpunkt der Meldung bekannt sind, enthalten, insbesondere die vermutete oder tatsächliche Ursache, die betroffene Informationstechnik, die Art der betroffenen Einrichtung oder

Anlage. Angaben über später bekanntgewordene Umstände sind ohne unangemessene weitere Verzögerung mitzuteilen. Die Meldung ist in einem geläufigen elektronischen Format unter Verwendung der durch die vom Bundesminister für Inneres festgelegten, sicheren Kommunikationskanäle zu übermitteln.

(4) Nimmt ein Betreiber wesentlicher Dienste die Dienste eines Anbieters digitaler Dienste in Anspruch, so ist jede erhebliche Auswirkung auf die Verfügbarkeit der wesentlichen Dienste, die von einem den Anbieter digitaler Dienste beeinträchtigenden Sicherheitsvorfall verursacht wurde, von diesem Betreiber wesentlicher Dienste zu melden.

(5) Wenn ein Sicherheitsvorfall bei einem Betreiber wesentlicher Dienste einen oder mehrere andere Mitgliedstaaten der Europäischen Union betrifft, hat der Bundesminister für Inneres oder das zuständige Computer-Notfallteam im Wege der zentralen Anlaufstelle (SPOC) die zentrale Anlaufstelle in diesen Mitgliedstaaten darüber zu unterrichten.

(6) Nach Anhörung des von einem Sicherheitsvorfall betroffenen Betreibers wesentlicher Dienste kann die zuständige Behörde die Öffentlichkeit über einzelne Sicherheitsvorfälle unterrichten, sofern die Sensibilisierung der Öffentlichkeit zur Verhütung von Sicherheitsvorfällen oder zur Bewältigung aktueller Sicherheitsvorfälle erforderlich ist oder wenn die Offenlegung des Sicherheitsvorfalls auf sonstige Weise im öffentlichen Interesse liegt. Die zuständige Behörde kann verlangen, dass der Betreiber wesentlicher Dienste dies unternimmt.

(7) Der Bundeskanzler kann im Einvernehmen mit dem Bundesminister für Inneres Kriterien für die Parameter des § 3 Z 6 lit. a bis d durch Verordnung festlegen.

Ausnahmen von Verpflichtungen für Betreiber wesentlicher Dienste

§ 17. (1) Die §§ 15 und 16 sind nicht anwendbar, wenn für die Erbringung eines wesentlichen Dienstes im Unionsrecht oder in Materiengesetzen, die auf unionsrechtlichen Bestimmungen beruhen, Vorschriften zu Sicherheitsvorkehrungen und zur Meldepflicht bestehen, die zumindest ein gleichwertiges Sicherheitsniveau für Netz- und Informationssysteme gewährleisten.

(2) Die Finanzmarktaufsichtsbehörde hat Meldungen von schwerwiegenden Betriebs- oder Sicherheitsvorfällen nach § 86 Abs. 1 Zahlungsdienstegesetz 2018 (ZaDiG 2018), BGBl. I Nr. 17/2018, von Zahlungsdienstleistern, die als Betreiber wesentlicher Dienste ermittelt wurden, unverzüglich an den Bundesminister für Inneres zu übermitteln.

Sicherheitsvorkehrungen und Meldepflicht für Anbieter digitaler Dienste

§ 18. (1) Anbieter digitaler Dienste haben in Hinblick auf die von ihnen betriebenen digitalen Dienste (§ 3 Z 9) geeignete Sicherheitsvorkehrungen zur Gewährleistung der NIS (§ 3 Z 2) zu treffen. Diese Vorkehrungen müssen unter Berücksichtigung des Stands der Technik ein Sicherheitsniveau der Netz- und Informationssysteme gewährleisten, das dem bestehenden Risiko angemessen ist, wobei Folgendem Rechnung getragen wird:

a) Sicherheit der Systeme und Anlagen,

b) Bewältigung von Sicherheitsvorfällen,

c) Betriebskontinuitätsmanagement,

d) Überwachung, Überprüfung und Erprobung,

e) Einhaltung der internationalen Normen.

(2) Anbieter digitaler Dienste haben einen Sicherheitsvorfall (§ 3 Z 6) unverzüglich an das nationale Computer-Notfallteam zu melden, das die Meldung unverzüglich an den Bundesminister für Inneres weiterleitet. Die Pflicht zur Meldung eines Sicherheitsvorfalls gilt nur, wenn der Anbieter digitaler Dienste Zugang zu Informationen hat, die benötigt werden, um die Auswirkung eines Sicherheitsvorfalls zu bewerten. § 16 Abs. 3 und 6 gilt sinngemäß.

(3) Wenn ein Sicherheitsvorfall bei einem Anbieter digitaler Dienste einen oder mehrere andere Mitgliedstaaten der Europäischen Union betrifft, hat der Bundesminister für Inneres oder das nationale Computer-Notfallteam im Wege der zentralen Anlaufstelle (SPOC) die zentrale Anlaufstelle in diesen Mitgliedstaaten darüber zu unterrichten.

(4) Der Bundesminister für Inneres ist, wenn ihm Umstände bekannt werden, dass ein Anbieter digitaler Dienste seinen Pflichten gemäß Abs. 1 nicht nachkommt, ermächtigt zu verlangen, dass dieser Nachweise über geeignete Sicherheitsvorkehrungen erbringt. Zu diesem Zweck übermittelt der betroffene Anbieter digitaler Dienste eine Aufstellung der vorhandenen Sicherheitsvorkehrungen. Der Bundesminister für Inneres kann dazu auch Einschau in die Netz- und Informationssysteme und diesbezügliche Unterlagen nehmen. Zur Herstellung der Anforderungen nach Abs. 1 ist der

Bundesminister für Inneres ermächtigt, Empfehlungen auszusprechen, für deren Befolgung und entsprechenden Nachweis erforderlichenfalls eine angemessene Frist zu setzen ist, widrigenfalls die Befolgung bescheidmäßig angeordnet wird.

Sicherheitsvorkehrungen und Meldepflicht für Einrichtungen des Bundes

§ 19. (1) Die Einrichtungen des Bundes haben in Hinblick auf die von ihnen betriebenen Dienste geeignete, dem Stand der Technik entsprechende Sicherheitsvorkehrungen zur Gewährleistung der NIS (§ 3 Z 2) zu treffen.

(2) Soweit es sich bei der Einrichtung des Bundes nicht um das Bundeskanzleramt oder das Bundesministerium für Inneres handelt, hat diese einen Sicherheitsvorfall (§ 3 Z 6) unverzüglich an das GovCERT (§ 12 Abs. 4) zu melden, das die Meldung unverzüglich an den Bundesminister für Inneres weiterleitet. § 16 Abs. 3 gilt sinngemäß. Bei Sicherheitsvorfällen, die das Bundeskanzleramt oder das Bundesministerium für Inneres betreffen, erfolgt die Meldung im Rahmen des IKDOK.

(3) Störungen, die kein Sicherheitsvorfall (§ 3 Z 6) sind, können an das GovCERT gemeldet werden, das die Meldungen zusammengefasst an den Bundesminister für Inneres weiterleitet; die Nennung der meldenden Einrichtung kann dabei entfallen. § 20 zweiter und dritter Satz gilt sinngemäß. Bei sonstigen Störungen, die das Bundeskanzleramt oder das Bundesministerium für Inneres betreffen, erfolgt die freiwillige Meldung im Rahmen des IKDOK.

(4) Wenn ein Sicherheitsvorfall bei einer Einrichtung des Bundes einen oder mehrere andere Mitgliedstaaten der Europäischen Union betrifft, hat der Bundesminister für Inneres oder das GovCERT im Wege der zentralen Anlaufstelle (SPOC) die zentrale Anlaufstelle in diesen Mitgliedstaaten darüber zu unterrichten.

Freiwillige Meldungen

§ 20. Störungen, die kein Sicherheitsvorfall (§ 3 Z 6) sind oder die Betreiber von nicht wesentlichen Diensten betreffen, können an das Computer-Notfallteam gemeldet werden, das die Meldungen zusammengefasst an den Bundesminister für Inneres weiterleitet; die Nennung der meldenden Einrichtung kann dabei auf ihr Verlangen entfallen. Die freiwillige Meldung kann Angaben zur Störung sowie zu den technischen Rahmenbedingungen, insbesondere der vermuteten oder tatsächlichen Ursache, der betroffenen Informationstechnik, der Art der betroffenen Einrichtung oder Anlage sowie zum Sektor des Betreibers enthalten. § 16 Abs. 3 letzter Satz gilt.

6. Abschnitt
Strukturen und Aufgaben im Falle der Cyberkrise

Cyberkrise

§ 21. Die Entscheidung über das Vorliegen einer Cyberkrise erfolgt durch den Bundesminister für Inneres.

Koordinationsausschuss

§ 22. (1) Zur Beratung des Bundesministers für Inneres in Bezug auf die Entscheidung über das Vorliegen einer Cyberkrise und die operativen Maßnahmen zur Bewältigung einer Cyberkrise sowie der Bundesregierung zur Koordination der Öffentlichkeitsarbeit wird ein Koordinationsausschuss eingerichtet.

(2) Der Koordinationsausschuss wird vom Generaldirektor für die öffentliche Sicherheit geleitet und setzt sich aus dem Chef des Generalstabs, dem Generalsekretär des Bundeskanzleramtes und dem Generalsekretär für auswärtige Angelegenheiten zusammen. Der Ausschuss ist um weitere Vertreter von Bundes- oder Landesbehörden, Betreiber wesentlicher Dienste und Computer-Notfallteams sowie Einsatzorganisationen zu erweitern, wenn dies zur Bewältigung der Cyberkrise erforderlich ist.

(3) Der IKDOK unterstützt den Koordinationsausschuss durch Erstellung von anlassbezogenen Lagebildern und sein technisches Fachwissen.

7. Abschnitt
Strafbestimmungen

Verwaltungsstrafbestimmungen

§ 23. (1) Eine Verwaltungsübertretung begeht und ist von der zuständigen Bezirksverwaltungsbehörde mit Geldstrafe bis zu 50.000 Euro, im Wiederholungsfall bis zu 100.000 Euro zu bestrafen, wer

1. eine Auskunft nach § 10 Abs. 3 nicht unverzüglich erteilt;
2. eine Kontaktstelle nach § 14 Abs. 3 erster Satz nicht benennt, allfällige Änderungen gemäß § 14 Abs. 3 dritter Satz nicht bekannt gibt oder unter dieser nicht im gemäß § 14 Abs. 3 zweiter Satz vorgesehenen Zeitraum erreichbar ist;
3. den Nachweis nach § 15 Abs. 3 erster Satz oder § 18 Abs. 4 erster Satz nicht erbringt;
4. die Einschau gemäß § 15 Abs. 3 vierter Satz und Abs. 5 oder § 18 Abs. 4 dritter Satz verweigert;
5. die bescheidmäßig ergangenen Anordnungen nach § 15 Abs. 3 letzter Satz oder § 18 Abs. 4 letzter Satz nicht fristgerecht umsetzt oder
6. der Meldepflicht nach § 16 Abs. 1 iVm Abs. 3 und 4 oder § 18 Abs. 2 nicht nachkommt.

(2) Die örtliche Zuständigkeit für Verwaltungsübertretungen nach Abs. 1 richtet sich nach der Hauptniederlassung des Betreibers wesentlicher Dienste oder des Anbieters digitaler Dienste, in Ermangelung einer solchen nach dem Sitz des Vertreters (§ 3 Z 11).

(3) Eine Verwaltungsübertretung gemäß Abs. 1 liegt nicht vor, wenn die Tat den Tatbestand einer in die Zuständigkeit der ordentlichen Gerichte fallenden strafbaren Handlung bildet oder nach anderen Verwaltungsstrafbestimmungen mit strengerer Strafe bedroht ist.

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

(5) Juristische Personen können wegen Verwaltungsübertretungen gemäß Abs. 1 auch verantwortlich gemacht werden, wenn mangelnde Überwachung oder Kontrolle durch eine in Abs. 4 genannte Person die Begehung dieser Verstöße durch eine für die juristische Person tätige Person ermöglicht hat, sofern die Tat nicht den Tatbestand einer in die Zuständigkeit der Gerichte fallenden strafbaren Handlung erfüllt.

8. Abschnitt
Schlussbestimmungen

Personenbezogene Bezeichnungen

§ 24. Alle in diesem Bundesgesetz verwendeten personenbezogenen Bezeichnungen gelten gleichermaßen für Personen sowohl des weiblichen als auch männlichen Geschlechts.

Bezugnahme auf Richtlinien

§ 25. Durch dieses Bundesgesetz wird die Richtlinie (EU) 2016/1148, ABl. Nr. L 194 vom 19.07.2016 S. 1, umgesetzt.

Verweisungen

§ 26. Verweisungen in diesem Bundesgesetz auf andere Bundesgesetze sind als Verweisungen auf die jeweils geltende Fassung zu verstehen.

Vollziehung

§ 27. Mit der Vollziehung dieses Bundesgesetzes sind, soweit sie nicht der Bundesregierung obliegt, der Bundeskanzler und der Bundesminister für Inneres im Rahmen ihres Wirkungsbereiches betraut.

Inkrafttreten

§ 28. (1) **(Verfassungsbestimmung)** § 1 in der Fassung BGBl. I Nr. XX/2018 tritt mit 9. Mai 2018 in Kraft.

(2) §§ 2 bis 22 und §§ 24 bis 27 in der Fassung BGBl. I Nr. XX/2018 treten mit 9. Mai 2018 in Kraft.

(3) § 23 in der Fassung BGBl. I Nr. XX/2018 tritt mit Ablauf des Tages der Kundmachung dieses Bundesgesetzes in Kraft.

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