369 der Beilagen zu den Stenographischen Protokollen des Nationalrates XXVI. GP

Regierungsvorlage

Bundesgesetz, mit dem das Bundesgesetz zur Gewährleistung eines hohen Sicherheitsniveaus von Netz- und Informationssystemen (Netz- und Informationssystemsicherheitsgesetz – NISG) erlassen und das Telekommunikationsgesetz 2003 geändert wird

Der Nationalrat hat beschlossen:

Inhaltsverzeichnis

Artikel 1

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

Inhaltsverzeichnis

1. Abschnitt
Allgemeine Bestimmungen

Verfassungsbestimmung

§ 1. (Verfassungsbestimmung) 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. Dies gilt nicht im Bereich der Hoheitsverwaltung von Ländern und Gemeinden. Die in diesem Bundesgesetz geregelten Angelegenheiten können in unmittelbarer Bundesverwaltung besorgt werden.

Gegenstand und Ziel des Gesetzes

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

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

sowie von Anbietern digitaler Dienste sowie Einrichtungen der öffentlichen Verwaltung erreicht werden soll.

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, Sicherheitsvorfällen vorzubeugen, diese zu erkennen, 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. „Innerer Kreis der Operativen Koordinierungsstruktur (IKDOK)“ eine interministerielle Struktur zur Koordination auf der operativen Ebene im Bereich der Sicherheit von Netz- und Informationssystemen bestehend aus Vertretern des Bundeskanzlers, des Bundesministers für Inneres, des Bundesministers für Landesverteidigung und des Bundesministers für Europa, Integration und Äußeres, die vor Beginn der Teilnahme einer Sicherheitsüberprüfung für den Zugang zu geheimer Information zu unterziehen sind;
5. „Operative Koordinierungsstruktur (OpKoord)“ eine Struktur zur Koordination auf der operativen Ebene im Bereich der Sicherheit von Netz- und Informationssystemen bestehend aus dem IKDOK und den Computer-Notfallteams (§ 14);
6. „Sicherheitsvorfall“ eine Störung der Verfügbarkeit, Integrität, Authentizität oder Vertraulichkeit von Netz- und Informationssystemen, die zu einer Einschränkung der Verfügbarkeit oder zu einem Ausfall des betriebenen Dienstes mit erheblichen Auswirkungen 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. „Vorfall“ alle Ereignisse, die tatsächlich nachteilige Auswirkungen auf die Verfügbarkeit, Integrität, Authentizität oder Vertraulichkeit von Netz- und Informationssystemen haben und kein Sicherheitsvorfall sind;
8. „Risiko“ alle Umstände oder Ereignisse, die potenziell nachteilige Auswirkungen auf die Sicherheit von Netz- und Informationssystemen haben;
9. „wesentlicher Dienst“ einen Dienst, der in einem der in § 2 genannten Sektoren erbracht wird und der eine wesentliche Bedeutung insbesondere für die Aufrechterhaltung des öffentlichen Gesundheitsdienstes, der öffentlichen Versorgung mit Wasser, Energie sowie lebenswichtigen Gütern, des öffentlichen Verkehrs oder die Funktionsfähigkeit öffentlicher Informations- und Kommunikationstechnologie hat und dessen Verfügbarkeit abhängig von Netz- und Informationssystemen ist;
10. „Betreiber wesentlicher Dienste“ eine Einrichtung mit Niederlassung in Österreich, die einen wesentlichen Dienst erbringt;
11. „qualifizierte Stelle“ eine Einrichtung mit Niederlassung in Österreich, deren Eignung zur Überprüfung der Sicherheitsvorkehrungen von Betreibern wesentlicher Dienste vom Bundesminister für Inneres gemäß § 18 Abs. 1 festgestellt wurde;
12. „digitaler Dienst“ einen 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;
13. „Anbieter digitaler Dienste“ eine juristische Person oder eingetragene Personengesellschaft, die einen digitalen Dienst 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

   a) mit Hauptniederlassung in Österreich oder

b) ohne Hauptniederlassung in der Europäischen Union, die einen Vertreter namhaft gemacht hat;

14. „Vertreter“ eine in Österreich niedergelassene natürliche oder juristische Person oder eingetragene Personengesellschaft, die ausdrücklich benannt wurde, um im Auftrag eines nicht in der Europäischen Union niedergelassenen Anbieters digitaler Dienste zu handeln, und an die sich der Bundeskanzler, der Bundesminister für Inneres oder die Computer-Notfallteams – statt an den Anbieter digitaler Dienste – hinsichtlich der Pflichten dieses Anbieters digitaler Dienste gemäß diesem Bundesgesetz wenden können;
15. „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;
16. „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;
17. „Cloud-Computing-Dienst“ einen digitalen Dienst, der den Zugang zu einem skalierbaren und elastischen Pool gemeinsam nutzbarer Rechenressourcen ermöglicht;
18. „Einrichtungen des Bundes“ die Bundesministerien, die Gerichtshöfe des öffentlichen Rechts, den Rechnungshof, die Volksanwaltschaft, die Präsidentschaftskanzlei und die Parlamentsdirektion; weitere Dienststellen des Bundes können vom zuständigen Bundesminister durch Verordnung bestimmt werden;
19. „Einrichtungen der öffentlichen Verwaltung“ die Einrichtungen des Bundes und jener Länder, die von der Möglichkeit gemäß § 22 Abs. 5 Gebrauch gemacht haben;
20. „Kooperationsgruppe“ ein gemäß Art. 11 NIS-RL 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;
21. „CSIRTs-Netzwerk“ ein gemäß Art. 12 NIS-RL 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;
22. „Cyberkrise“ ein oder mehrere Sicherheitsvorfälle, die eine gegenwärtige und unmittelbare Gefahr für die Aufrechterhaltung wichtiger gesellschaftlicher Funktionen darstellen und schwerwiegende Auswirkungen auf die Gesundheit, die Sicherheit oder das wirtschaftliche und soziale Wohl großer Teile der Bevölkerung oder das effektive Funktionieren von staatlichen Einrichtungen nach sich ziehen können;
23. „Cyberkrisenmanagement“ ein Koordinierungsverfahren zur Bewältigung von Cyberkrisen.

2. Abschnitt
Zuständigkeiten und Koordinierungsstrukturen

Aufgaben des Bundeskanzlers

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

1. Koordination der Erstellung einer Strategie (§ 8) und eines jährlichen Berichts zur Sicherheit von Netz- und Informationssystemen;
2. Vertretung von Österreich in der Kooperationsgruppe sowie in anderen EU-weiten und internationalen Gremien für die Sicherheit von Netz- und Informationssystemen, denen strategische Aufgaben zugewiesen sind; die Zuständigkeiten anderer Ressorts bleiben davon unberührt;
3. Koordination der öffentlich-privaten Zusammenarbeit im Bereich der Sicherheit von Netz- und Informationssystemen;

4. Betrieb des GovCERT gemäß § 14 Abs. 4;
5. Unterrichtung der Öffentlichkeit über einen Sicherheitsvorfall, der mehrere der in § 2 genannten Sektoren betrifft;
6. Ermittlung von Betreibern wesentlicher Dienste gemäß § 16 Abs. 1 sowie Erstellung und laufende Aktualisierung einer Liste von wesentlichen Diensten;
7. 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;
8. Feststellung der Eignung und Ermächtigung von Computer-Notfallteams gemäß § 15 Abs. 3;
9. Veröffentlichung und Aktualisierung einer Liste der Computer-Notfallteams gemäß § 14 Abs. 1 und 4 in geeigneter Form.

(2) Der Bundeskanzler kann im Einvernehmen mit dem Bundesminister für Inneres mit Verordnung Folgendes festlegen:

1. Kriterien für die Parameter des § 3 Z 6 lit. a bis d;
2. nähere Regelungen zu jedem in § 2 genannten Sektor gemäß § 16 Abs. 2;
3. Sicherheitsvorkehrungen nach § 17 Abs. 1.
4. Ausnahmen von Verpflichtungen für Betreiber wesentlicher Dienste gemäß § 20 Abs. 1.

(3) Der Bundeskanzler legt im Einvernehmen mit dem Bundesminister für Inneres und dem Bundesminister für Landesverteidigung mit Verordnung die Aufteilung der Pflichten als gemeinsam datenschutzrechtlich Verantwortliche gemäß § 11 Abs. 3 fest.

Aufgaben des Bundesministers für Inneres

§ 5. (1) 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. organisatorische Leitung der Koordinierungsstrukturen IKDOK und OpKoord (§ 7);
3. Entgegennahme und Analyse von Meldungen über Risiken, Vorfälle oder Sicherheitsvorfälle, regelmäßige Erstellung eines diesbezüglichen Lagebildes und Weiterleitung der Meldungen sowie des Lagebildes und zusätzlicher relevanter Informationen an inländische Behörden oder Stellen nach Maßgabe des 3. Abschnitts;
4. Erstellung und Weitergabe von zur Gewährleistung der Sicherheit von Netz- und Informationssystemen relevanten Informationen zur Vorbeugung von Sicherheitsvorfällen;
5. Überprüfung der Sicherheitsvorkehrungen (§§ 17 und 21) und die Einhaltung der Meldepflichten (§§ 19 und 21);
6. Feststellung und Überprüfung der qualifizierten Stellen (§ 18);
7. Unterrichtung der Öffentlichkeit über einzelne Sicherheitsvorfälle (§ 10 Abs. 1);
8. Leitung und Koordination des Cyberkrisenmanagements auf operativer Ebene (6. Abschnitt).

(2) Der Bundesminister für Inneres legt im Einvernehmen mit dem Bundeskanzler mit Verordnung die Erfordernisse, die eine qualifizierte Stelle erfüllen muss, oder besondere Kriterien fest, nach denen eine Einrichtung jedenfalls als qualifizierte Stelle gilt sowie das Verfahren zur Feststellung qualifizierter Stellen.

Zentrale Anlaufstelle

§ 6. (1) Für die Sicherheit von Netz- und Informationssystemen wird eine zuständige zentrale Anlaufstelle (SPOC) beim Bundesminister für Inneres eingerichtet, die als operative Verbindungsstelle zur Gewährleistung der grenzüberschreitenden Zusammenarbeit mit den zuständigen Stellen in den anderen Mitgliedstaaten der Europäischen Union sowie der Kooperationsgruppe und dem CSIRTs-Netzwerk dient.

(2) Die zentrale Anlaufstelle

1. leitet eingehende Meldungen und Anfragen unmittelbar an die Mitglieder des IKDOK und Computer-Notfallteams (§ 14) weiter, soweit dies zur Erfüllung einer gesetzlich übertragenen Aufgabe des jeweiligen Mitglieds des IKDOK 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 (§§ 19 Abs. 5, 21 Abs. 3 und 22 Abs. 4).

Koordinierungsstrukturen

§ 7. (1) Zur Erörterung und Aktualisierung des vom Bundesminister für Inneres erstellten Lagebildes über Risiken, Vorfälle und Sicherheitsvorfälle, zur Erörterung der Erkenntnisse, die gemäß § 13 Abs. 1 und 2 gewonnen wurden, und zur Unterstützung des Koordinationsausschusses im Cyberkrisenmanagement wird der IKDOK eingerichtet. Dieser 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 enthält, wird eine OpKoord eingerichtet. Die OpKoord kann um Vertreter von Betreibern wesentlicher Dienste, Anbietern digitaler Dienste sowie Einrichtungen der öffentlichen Verwaltung erweitert werden, wenn deren Wirkungsbereich von einem Risiko, Vorfall oder Sicherheitsvorfall betroffen ist. Teilnehmer der OpKoord sind über die ihnen aufgrund der Teilnahme bekanntgewordenen Informationen zur Verschwiegenheit nach Maßgabe der näheren Regelungen gemäß Abs. 3 verpflichtet.

(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.

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

Strategie für die Sicherheit von Netz- und Informationssystemen

§ 8. (1) Die Strategie für die Sicherheit von Netz- und Informationssystemen bestimmt insbesondere 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

Datenverarbeitung

§ 9. (1) Der Bundeskanzler, der Bundesminister für Inneres, der Bundesminister für Landesverteidigung, der Bundesminister für Europa, Integration und Äußeres und die Computer-Notfallteams gemäß § 14 Abs. 1 sind berechtigt zur Gewährleistung eines hohen Sicherheitsniveaus von Netz- und Informationssystemen bei der Wahrnehmung ihrer Aufgaben nach diesem Bundesgesetz und zum Schutz vor und der Abwehr von Gefahren für die öffentliche Sicherheit die erforderlichen personenbezogenen Daten im Sinne des Art. 4 Z 2 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) (im Folgenden: DSGVO), ABl. Nr. L 119 vom 04.05.2016 S. 1, in der Fassung der Berichtigung ABl. Nr. L 314 vom 22.11.2016 S. 72, und § 36 des Bundesgesetzes zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten (Datenschutzgesetz – DSG), BGBl. I Nr. 165/1999, zu verarbeiten und einander sowie den Mitgliedern der OpKoord zu übermitteln.

(2) Dies sind folgende personenbezogene Daten:

1. von Teilnehmern und ihren Organisationseinheiten, die zur Ermöglichung und im Zuge der Teilnahme an den Koordinierungsstrukturen zu organisatorischen Zwecken erforderlich sind;
2. von Personen, die in Zusammenhang mit Risiken, Vorfällen und Sicherheitsvorfällen stehen, zwecks Erörterung und Aktualisierung des vom Bundesminister für Inneres erstellten Lagebildes, zur Erörterung der Erkenntnisse, die gemäß § 13 Abs. 1 und 2 gewonnen wurden, und zur Unterstützung des Koordinationsausschusses erforderlich sind;
3. von Personen, die an einem Geschäftsfall mitwirken oder davon betroffen sind.

(3) Der Bundeskanzler, der Bundesminister für Inneres und der Bundesminister für Landesverteidigung sind zum Zweck der Analyse und Bewältigung von Risiken, Vorfällen und Sicherheitsvorfällen berechtigt, über die in Abs. 2 genannten Daten hinaus folgende personenbezogene Daten zu verarbeiten und einander zu übermitteln:

1. Kontakt- und Identitätsdaten sowie technische Daten des Einmelders und der Kontaktperson;
2. Kontakt- und Identitätsdaten sowie technische Daten von Personen, die mit einer Meldung zu einem Risiko, Vorfall oder Sicherheitsvorfall in Zusammenhang stehen, wie insbesondere Opfer und Angreifer.

(4) Der Bundeskanzler und der Bundesminister für Inneres sind zur Erfüllung ihrer Aufgaben nach §§ 4 und 5 berechtigt, über die in Abs. 2 und 3 genannten Daten hinaus folgende personenbezogenen Daten zu verarbeiten und einander zu übermitteln:

1. Kontakt- und Identitätsdaten sowie technische Daten von Betreibern wesentlicher Dienste, Anbietern digitaler Dienste, Einrichtungen der öffentlichen Verwaltung, die von der Möglichkeit gemäß § 22 Abs. 5 Gebrauch gemacht haben, Computer-Notfallteams sowie von zuständigen Behörden anderer Mitgliedstaaten;
2. Kontakt- und Identitätsdaten sowie technische Daten von Personen, die mit einer Meldung zu einem Risiko, Vorfall oder Sicherheitsvorfall in Zusammenhang stehen, wie insbesondere Opfer und Angreifer;
3. Kontakt- und Identitätsdaten von Teilnehmern und ihren Organisationseinheiten, die zur Ermöglichung und im Zuge der Teilnahme an EU-weiten, internationalen und nationalen Gremien für die Sicherheit von Netz- und Informationssystemen erforderlich sind;

(5) Der Bundesminister für Inneres ist zur Erfüllung seiner Aufgaben nach § 5 Z 4 bis 6 berechtigt, über die in Abs. 2 bis 4 genannten Daten hinaus folgende personenbezogenen Daten zu verarbeiten:

1. Kontakt- und Identitätsdaten sowie technische Daten von qualifizierten Stellen;
2. Kontakt- und Identitätsdaten sowie technische Daten von Personen im Rahmen der Überprüfungen von Sicherheitsvorkehrungen;
3. technische Daten von Personen, die im Rahmen des § 13 ermittelt wurden.

(6) Jede Abfrage, Übermittlung und Änderung personenbezogener Daten ist revisionssicher zu protokollieren. Die Protokollaufzeichnungen sind drei Jahre aufzubewahren und danach zu löschen.

(7) Das Recht auf Löschung und auf Widerspruch gemäß DSGVO oder § 45 DSG wird insoweit beschränkt, als durch Gesetz oder Verordnung eine Aufbewahrungspflicht oder Archivierung vorgesehen ist oder der Löschung das öffentliche Interesse der Gewährleistung eines hohen Niveaus von Netz- und Informationssystemsicherheit entgegensteht und die betroffene Person nicht Gründe nachweisen kann, die sich aus ihrer besonderen Situation ergeben und welche die Ziele der Beschränkung des Rechtes überwiegen. Der zuständige Datenschutzbeauftragte ist über die Vornahme und das Ergebnis einer solchen Abwägung in Kenntnis zu setzen.

(8) Das Recht auf Einschränkung der Verarbeitung gemäß Art. 18 DSGVO oder § 45 DSG wird in Bezug auf integrierte Datenverarbeitungssysteme für die Dauer einer Überprüfung der von der betroffenen Person bestrittenen Richtigkeit ihrer personenbezogenen Daten sowie für den Zeitraum, in dem die betroffene Person ihr Recht auf Widerspruch geltend gemacht hat und noch nicht feststeht, ob die berechtigten Gründe des datenschutzrechtlich Verantwortlichen gegenüber denen der betroffenen Person überwiegen, beschränkt.

(9) Die datenschutzrechtlichen Pflichten nach der DSGVO und dem 3. Hauptstück DSG sind von jedem datenschutzrechtlichen Verantwortlichen hinsichtlich jener personenbezogenen Daten, die im Zusammenhang mit den von ihm geführten Verfahren oder den von ihm gesetzten Maßnahmen verarbeitet, übermittelt oder weiterverarbeitet werden, selbstständig wahrzunehmen.

Datenübermittlung

§ 10. (1) Nach Anhörung des von einem Sicherheitsvorfall betroffenen Betreibers wesentlicher Dienste oder Anbieters digitalen Dienste können der Bundeskanzler und der Bundesminister für Inneres im Rahmen ihres jeweiligen Wirkungsbereichs personenbezogene Daten gemäß § 9 Abs. 3 Z 2 nach erfolgter Interessenabwägung bezüglich der Auswirkungen auf die datenschutzrechtlichen Betroffenen veröffentlichen, um die Öffentlichkeit über Sicherheitsvorfälle zu unterrichten, sofern die Sensibilisierung der Öffentlichkeit zur Verhütung oder zur Bewältigung von Sicherheitsvorfällen erforderlich ist, oder die Offenlegung des Sicherheitsvorfalls auf sonstige Weise im öffentlichen Interesse liegt. Der Bundesminister für Inneres kann von Anbietern digitaler Dienste verlangen, die Unterrichtung der Öffentlichkeit selbst zu unternehmen.

(2) Daten, die dem Bundeskanzler, dem Bundesminister für Inneres, dem Bundesminister für Landesverteidigung und dem Bundesminister für Europa, Integration und Äußeres aufgrund der Wahrnehmung ihrer Aufgaben nach diesem Bundesgesetz bekannt sind, können an militärische Organe und Behörden für Zwecke der militärischen Landesverteidigung gemäß Art. 79 Abs. 1 B-VG, an

Sicherheitsbehörden für Zwecke der Sicherheitspolizei und Strafrechtspflege, an Staatsanwaltschaften und ordentliche Gerichte für Zwecke der Strafrechtspflege sowie an inländische Behörden, soweit dies eine wesentliche Voraussetzung zur Wahrnehmung einer ihnen gesetzlich übertragenen Aufgabe ist, übermittelt werden.

(3) Der Bundesminister für Inneres kann zur Erfüllung seiner Aufgaben nach § 5 Z 4 Daten gemäß § 9 Abs. 2 Z 2 und Abs. 3 Z 2 an Betreiber wesentlicher Dienste, Anbieter digitaler Dienste sowie an Einrichtungen, die nicht Betreiber wesentlicher Dienste oder Anbieter digitaler Dienste sind, übermitteln, wenn diese von einem Risiko, Vorfall oder Sicherheitsvorfall betroffen sind.

(4) Der Bundesminister für Inneres ist berechtigt, Daten gemäß § 9 Abs. 2 bis 5 an ausländische Sicherheitsbehörden und Sicherheitsorganisationen gemäß § 2 Abs. 2 und 3 des Bundesgesetzes über die internationale polizeiliche Kooperation (Polizeikooperationsgesetz – PolKG), BGBl. I Nr. 104/1997, sowie Organe der Europäischen Union oder Vereinten Nationen entsprechend den Bestimmungen über die internationale polizeiliche Amtshilfe zu übermitteln.

(5) Der Bundesminister für Inneres ist berechtigt, zur Erfüllung seiner Aufgaben gemäß §§ 19 Abs. 5, 21 Abs. 3 und 22 Abs. 4 nach erfolgter Interessenabwägung bezüglich der wirtschaftlichen Interessen der betroffenen Einrichtung sowie der Vertraulichkeit der in der Meldung bereitgestellten Informationen, personenbezogene Daten von Personen, die in Zusammenhang mit einem Sicherheitsvorfall stehen, an die zentrale Anlaufstelle in dem von dem Sicherheitsvorfall betroffenen Mitgliedstaaten zu übermitteln.

(6) Der Bundeskanzler ist berechtigt, personenbezogene Kontakt- und Identitätsdaten von Betreibern wesentlicher Dienste und Anbietern digitaler Dienste an Computer-Notfallteams zur Wahrnehmung ihrer Aufgaben gemäß § 14 Abs. 2 zu übermitteln.

(7) Der Bundeskanzler ist berechtigt, Identitätsdaten von Betreibern wesentlicher Dienste an jene Länder, in deren Gebiet sich die Niederlassung des Betreibers befindet, sowie an die Aufsichtsbehörden, des jeweiligen Sektors, in welchem der wesentliche Dienst erbracht wird, soweit dies zur Wahrnehmung ihrer Aufgaben notwendig ist, zu übermitteln.

NIS-Meldeanalysesystem

§ 11. (1) Für die Analyse von Meldungen über Risiken, Vorfälle und Sicherheitsvorfälle (§§ 19, 20 Abs. 2, 21 Abs. 2, 22 Abs. 2 und 3 sowie 23 Abs. 1 und 2) sowie von Erkenntnissen, die gemäß § 13 Abs. 1 und 2 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, Vorfälle und Sicherheitsvorfällen für Netz- und Informationssysteme und 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 Z 7 in Verbindung mit Art. 26 DSGVO bzw. § 36 DSG.

(3) Die Aufteilung der Pflichten als gemeinsam datenschutzrechtliche Verantwortliche erfolgt durch Verordnung des Bundeskanzlers im Einvernehmen mit dem Bundesminister für Inneres und dem Bundesminister für Landesverteidigung.

IKDOK-Plattform

§ 12. (1) Der Bundesminister für Inneres kann für die Organisation des IKDOK und zur Wahrnehmung der Aufgaben gemäß § 7 Abs. 1 eine IKT-Lösung betreiben. Im Falle des Betriebs einer solchen ist sie dem Bundeskanzler, dem Bundesminister für Landesverteidigung und dem Bundesminister für Europa, Integration und Äußeres bereitzustellen.

(2) Für die IKT-Lösung des Abs. 1 sind der Bundesminister für Inneres, der Bundeskanzler, der Bundesminister für Landesverteidigung und der Bundesminister für Europa, Integration und Äußeres gemeinsam datenschutzrechtliche Verantwortliche gemäß Art. 4 Z 7 in Verbindung mit Art. 26 DSGVO bzw. § 47 DSG. Die sich aus der DSGVO ergebenden Pflichten sind, soweit die folgenden Absätze nicht ausdrücklich anderes regeln, vom Bundesminister für Inneres wahrzunehmen.

(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.

Betrieb von IKT-Lösungen zur Vorbeugung von Sicherheitsvorfällen

§ 13. (1) Der Bundesminister für Inneres ist zur Erfüllung der Aufgabe gemäß § 5 Z 4 ermächtigt, IKT-Lösungen zu betreiben, die Risiken oder Vorfälle von Netz- und Informationssystemen frühzeitig erkennen. Betreiber wesentlicher Dienste, Anbieter digitaler Dienste sowie Einrichtungen der öffentlichen Verwaltung 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.

(2) Der Bundesminister für Inneres ist zur Erfüllung der Aufgabe gemäß § 5 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 § 14 Abs. 2 Z 3 und 5 ermächtigt und darf die daraus gewonnenen personenbezogenen technischen Daten als datenschutzrechtlicher Verantwortlicher gemäß Art. 4 Z 7 DSGVO bzw. § 36 Abs. 2 Z 8 DSG verarbeiten.

4. Abschnitt
Computer-Notfallteams

Aufgaben und Zweck der Computer-Notfallteams

§ 14. (1) Zur Gewährleistung der Sicherheit von Netz- und Informationssystemen werden Computer-Notfallteams eingerichtet. Zu diesem Zweck unterstützen das nationale Computer-Notfallteam und sektorenspezifische Computer-Notfallteams Betreiber wesentlicher Dienste und Anbieter digitaler Dienste sowie das Computer-Notfallteam der öffentlichen Verwaltung (GovCERT) die Einrichtungen der öffentlichen Verwaltung bei der Bewältigung von Risiken, Vorfällen und Sicherheitsvorfällen.

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

1. Entgegennahme von Meldungen über Risiken, Vorfälle oder Sicherheitsvorfälle gemäß §§ 19, 21 Abs. 2 und 23 Abs. 1 und 2;
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, Vorfälle oder Sicherheitsvorfälle;
4. Erste allgemeine technische Unterstützung bei der Reaktion auf einen Sicherheitsvorfall;
5. Beobachtung und Analyse von Risiken, Vorfällen oder Sicherheitsvorfällen sowie Lagebeurteilung;
6. Teilnahme an den Koordinierungsstrukturen gemäß § 7 und Beteiligung am CSIRTs-Netzwerk.

(3) Betreiber wesentlicher Dienste können für ihren Sektor (§ 2) ein sektorenspezifisches Computer-Notfallteam einrichten, welches die Aufgaben gemäß Abs. 2 gegenüber den Betreibern wesentlicher Dienste, die es unterstützen, wahrnehmen. Sektorenspezifische Computer-Notfallteams können für Zwecke des Abs. 2 Z 3 und 5 im Auftrag eines Betreibers wesentlicher Dienste Daten gemäß § 13 Abs. 1 zweiter Satz analysieren, die durch eine bei diesem Betreiber wesentlicher Dienste eingerichtete IKT-Lösung gemäß § 13 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 § 22 Abs. 2 und 3, gegebenenfalls gemäß §§ 19 Abs. 2, 21 Abs. 2 und 23 Abs. 3, kommen dem GovCERT die Aufgaben gemäß Abs. 2 Z 3 bis 5 und Abs. 3 zweiter Satz in Hinblick auf die Einrichtungen der öffentlichen Verwaltung, soweit es sich dabei nicht um eine im IKDOK vertretene Einrichtung handelt, zu.

(5) Das GovCERT, das nationale Computer-Notfallteam und die sektorenspezifischen Computer-Notfallteams informieren ohne unnötigen Aufschub den Bundeskanzler sowie den Bundesminister für Inneres über Aktivitäten des CSIRTs-Netzwerks, die zu deren Aufgabenerfüllung nach diesem Bundesgesetz erforderlich sind, und können an dessen Sitzungen teilnehmen.

(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 einem Vorfall ihrer Netz- und Informationssysteme betroffen sind.

(7) Computer-Notfallteams sind als datenschutzrechtliche Verantwortliche gemäß Art. 4 Z 7 DSGVO ermächtigt, personenbezogene Daten gemäß § 9 Abs. 2 bis 4 zu verarbeiten, soweit dies zur Erfüllung der Aufgaben gemäß Abs. 2 erforderlich ist.

(8) Computer-Notfallteams sind zur Wahrnehmung der Aufgaben gemäß Abs. 2 Z 3, 5 und 6 berechtigt, personenbezogene Daten gemäß § 9 Abs. 2 Z 2 und Abs. 3 Z 2 an Betreiber wesentlicher Dienste, Anbieter digitaler Dienste, Einrichtungen der öffentlichen Verwaltung, Einrichtungen, die gemäß § 23 Abs. 2 gemeldet haben und an Teilnehmer des CSIRTs-Netzwerks sowie einander zu übermitteln.

Anforderungen und Eignung eines Computer-Notfallteams

§ 15. (1) Computer-Notfallteams gemäß § 14 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 § 14 Abs. 1 zweiter Satz handelt.
4. Das zur Erfüllung der Aufgaben nach § 14 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.
5. in Wahrnehmung ihrer Aufgaben gemäß § 14 Abs. 2 Z 1 und 2 haben sie sichere Kommunikationskanäle zu verwenden, die sie vorab mit dem Bundesminister für Inneres abgestimmt haben.

(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 § 14 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 § 14 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.

(4) Die personenbezogenen Kontakt- und Identitätsdaten der Computer-Notfallteams sind vom Bundeskanzler in geeigneter Form zu veröffentlichen.

5. Abschnitt

Verpflichtungen für Betreiber wesentlicher Dienste, Anbieter digitaler Dienste sowie Einrichtungen der öffentlichen Verwaltung

Ermittlung der Betreiber wesentlicher Dienste

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

(2) Durch Verordnung kann der Bundeskanzler im Einvernehmen mit dem Bundesminister für Inneres nähere Regelungen zu den in § 2 genannten Sektoren bestimmen. Diese Verordnung kann insbesondere Teilsektoren, Bereiche, die dazugehörigen wesentlichen Dienste sowie Arten von Einrichtungen, die als Betreiber wesentlicher Dienste in Frage kommen, beinhalten. Bei der Beurteilung, ob ein Dienst eine wesentliche Bedeutung hat, sind insbesondere folgende Faktoren zu berücksichtigen:

1. Zahl der Nutzer, die den vom jeweiligen Betreiber eines wesentlichen Dienstes angebotenen Dienst in Anspruch nehmen;
2. Abhängigkeit anderer in § 2 genannter Sektoren von dem von diesem Betreiber angebotenen Dienst;
3. Marktanteil des Betreibers wesentlicher Dienste;
4. geografische Ausbreitung des Gebiets, das von einem Sicherheitsvorfall betroffen sein könnte;
5. Auswirkungen von Sicherheitsvorfällen hinsichtlich Ausmaß und Dauer auf wirtschaftliche oder gesellschaftliche Tätigkeiten oder die öffentliche Sicherheit;
6. 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 gegebenenfalls auch sektorenspezifische Faktoren zu berücksichtigen.

(3) Betreiber wesentlicher Dienste haben dem Bundeskanzler innerhalb von zwei Wochen nach Zustellung des Bescheids gemäß Abs. 4 Z 1 eine Kontaktstelle für die Kommunikation mit dem Bundeskanzler, dem Bundesminister für Inneres oder 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) 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. Fallen die Voraussetzungen für den Bescheid, mit dem festgestellt wurde, dass eine bestimmte Einrichtung Betreiber wesentlicher Dienste ist, nachträglich weg oder stellt sich heraus, dass sie von vornherein nicht vorgelegen sind, so ist dies ebenfalls mit Bescheid auszusprechen;
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 wesentlichen Diensten;
4. Übermittlung der Liste (Z 3) an die Europäische Kommission mindestens alle zwei Jahre.

Sicherheitsvorkehrungen für Betreiber wesentlicher Dienste

§ 17. (1) Zur Gewährleistung der NIS haben Betreiber wesentlicher Dienste in Hinblick auf die Netz- und Informationssysteme, die sie für die Bereitstellung des wesentlichen Dienstes nutzen, geeignete und verhältnismäßige technische und organisatorische Sicherheitsvorkehrungen zu treffen. Diese haben den Stand der Technik zu berücksichtigen und dem Risiko, das mit vernünftigem Aufwand feststellbar ist, angemessen zu sein.

(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 nach Zustellung des Bescheides gemäß § 16 Abs. 4 Z 1 die Erfüllung der Anforderungen nach Abs. 1 gegenüber dem Bundesminister für Inneres nachzuweisen. Zu diesem Zweck übermitteln sie eine Aufstellung der vorhandenen Sicherheitsvorkehrungen durch den Nachweis von Zertifizierungen oder durchgeführten Überprüfungen durch qualifizierte Stellen, einschließlich der dabei aufgedeckten Sicherheitsmängel an den Bundesminister für Inneres.

(4) Der Bundesminister für Inneres kann zur Kontrolle der Einhaltung der Anforderungen gemäß Abs. 1 Einschau in die Netz- und Informationssysteme, die für die Bereitstellung des wesentlichen Dienstes genutzt werden, und diesbezügliche Unterlagen nehmen. Zum Zweck der Einschau ist der Bundesminister für Inneres nach vorangegangener Verständigung berechtigt, Örtlichkeiten, in welchen Netz- und Informationssysteme gelegen sind, zu betreten. Die Ausübung der Einschau hat in dem unbedingt erforderlichen Ausmaß zu erfolgen und ist unter möglichster Schonung der Rechte der betroffenen Einrichtung und Dritter sowie des Betriebs auszuüben.

(5) 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.

Qualifizierte Stellen

§ 18. (1) Der Bundesminister für Inneres entscheidet über das Vorliegen einer qualifizierten Stelle auf Antrag.

(2) Bei Wegfall der Erfordernisse oder Kriterien gemäß § 5 Abs. 2 wird die qualifizierte Stelle zunächst darauf hingewiesen, dass sie die Erfordernisse oder Kriterien binnen einer angemessenen Frist zu erfüllen hat. Bei Nichterfüllung widerruft der Bundesminister für Inneres den Bescheid, der nach Abs. 1 ergangen ist.

(3) Zur Kontrolle der Einhaltung der Erfordernisse an und Kriterien für qualifizierte Stellen gemäß § 5 Abs. 2 kann der Bundesminister für Inneres Einschau in deren Netz- und Informationssysteme und diesbezügliche Unterlagen nehmen. § 17 Abs. 4 zweiter und dritter Satz gilt.

(4) Eine Liste von qualifizierten Stellen und deren Aufgabenbereich wird vom Bundesminister für Inneres geführt und in diese Betreibern wesentlicher Dienste Einsicht gewährt.

Meldepflicht für Betreiber wesentlicher Dienste

§ 19. (1) Betreiber wesentlicher Dienste haben einen Sicherheitsvorfall, der einen von ihnen bereitgestellten wesentlichen Dienst betrifft, unverzüglich an das für sie zuständige Computer-Notfallteam 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 (§ 14 Abs. 1 zweiter Satz), falls ein solches eingerichtet ist und der betroffene Betreiber wesentlicher Dienste dieses unterstützt (§ 15 Abs. 1 Z 3), andernfalls das nationale Computer-Notfallteam, sofern ein solches eingerichtet ist, ansonsten das GovCERT.

(3) Die Meldung muss sämtliche relevante Angaben zum Sicherheitsvorfall und den technischen Rahmenbedingungen, die im Zeitpunkt der Erstmeldung bekannt sind, enthalten, insbesondere die vermutete oder tatsächliche Ursache, die betroffene Informationstechnik, die Art der betroffenen Einrichtung oder Anlage. Angaben über später bekanntgewordene Umstände zum Sicherheitsvorfall sind in Nachmeldungen und letztendlich in einer Abschlussmeldung ohne unangemessene weitere Verzögerung mitzuteilen. Die Meldung ist in einem standardisierten elektronischen Format 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.

Ausnahmen von Verpflichtungen für Betreiber wesentlicher Dienste

§ 20. (1) Die §§ 17 oder 19 sind nicht anwendbar, wenn für die Erbringung eines wesentlichen Dienstes im Unionsrecht oder in Materiengesetzen, die auf unionsrechtlichen Bestimmungen beruhen, Vorschriften zu Sicherheitsvorkehrungen oder zur Meldepflicht bestehen, die zumindest ein gleichwertiges Sicherheitsniveau für Netz- und Informationssysteme gewährleisten, und der Bundeskanzler diese Vorschriften und deren Eignung mittels Verordnung im Einvernehmen mit dem Bundesminister für Inneres festlegt.

(2) Die Finanzmarktaufsichtsbehörde hat Meldungen von schwerwiegenden Betriebs- oder Sicherheitsvorfällen nach § 86 Abs. 1 des Zahlungsdienstegesetzes 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

§ 21. (1) Zur Gewährleistung der NIS haben Anbieter digitaler Dienste in Hinblick auf die Netz- und Informationssysteme, die sie für die Bereitstellung des digitalen Dienstes nutzen, geeignete und verhältnismäßige technische und organisatorische Sicherheitsvorkehrungen zu treffen. Diese haben unter Berücksichtigung des Stands der Technik ein Sicherheitsniveau der Netz- und Informationssysteme zu

gewährleisten, das dem bestehenden mit vernünftigem Aufwand feststellbaren 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, der einen von ihnen bereitgestellten digitalen Dienst betrifft, unverzüglich an das nationale Computer-Notfallteam, sofern ein solches eingerichtet ist, ansonsten an das GovCERT 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. § 19 Abs. 3 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 zuständige Computer-Notfallteam gemäß Abs. 2 im Wege der zentralen Anlaufstelle (SPOC) die zentrale Anlaufstelle in diesen Mitgliedstaaten darüber zu unterrichten.

(4) Der Bundesminister für Inneres ist, wenn ihm nachweisliche 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 stellt der betroffene Anbieter digitaler Dienste eine Aufstellung der vorhandenen Sicherheitsvorkehrungen zur Verfügung. Der Bundesminister für Inneres kann dazu auch Einschau in die Netz- und Informationssysteme, die für die Bereitstellung des digitalen Dienstes genutzt werden, und diesbezügliche Unterlagen nehmen. § 17 Abs. 4 zweiter und dritter Satz gilt. 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 der öffentlichen Verwaltung

§ 22. (1) Zur Gewährleistung der NIS haben Einrichtungen des Bundes in Hinblick auf die Netz- und Informationssysteme, die sie für die Bereitstellung wichtiger Dienste nutzen, geeignete und verhältnismäßige technische und organisatorische Sicherheitsvorkehrungen für zu treffen. Diese haben den Stand der Technik zu berücksichtigen und dem Risiko, das mit vernünftigem Aufwand feststellbar ist, angemessen zu sein.

(2) Eine Einrichtung des Bundes, soweit es sich nicht um eine im IKDOK vertretene Einrichtung handelt, hat einen Sicherheitsvorfall, der einen von ihr bereitgestellten wichtigen Dienst betrifft, unverzüglich an das GovCERT zu melden, welches die Meldung unverzüglich an den Bundesminister für Inneres weiterleitet. § 19 Abs. 3 gilt sinngemäß. Bei Sicherheitsvorfällen, die eine im IKDOK vertretene Einrichtung betreffen, erfolgt die Meldung im Rahmen des IKDOK.

(3) Risiken und Vorfälle können von Einrichtungen der öffentlichen Verwaltung an das GovCERT gemeldet werden, das die Meldungen zusammengefasst an den Bundesminister für Inneres weiterleitet. § 23 Abs. 4 und 5 gilt sinngemäß. Bei Risiken und Vorfällen, die eine im IKDOK vertretene Einrichtung betreffen, erfolgt die freiwillige Meldung im Rahmen des IKDOK.

(4) Wenn ein Sicherheitsvorfall bei einer Einrichtung der öffentlichen Verwaltung 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.

(5) Ein Land kann durch Landesgesetz die Pflichten gemäß Abs. 1 und 2 auch in Hinblick auf die von seinen Einrichtungen erbrachten wichtigen Dienste für anwendbar erklären. Diese Einrichtungen der Länder sind die Ämter der Landesregierungen und weitere Dienststellen der Länder und Gemeinden, die gegebenenfalls von den jeweils in Betracht kommenden Organen des Landes als solche erklärt werden.

(6) Ein Land hat die Erlassung eines Landesgesetzes gemäß Abs. 5 sowie eine allfällige Aufhebung dem Bundeskanzler schriftlich mitzuteilen. Macht ein Land von der Möglichkeit gemäß Abs. 5 Gebrauch, so sind die Bestimmungen für Einrichtungen des Bundes auch für Einrichtungen des Landes anzuwenden.

Freiwillige Meldungen

§ 23. (1) Risiken und Vorfälle können von Betreibern wesentlicher Dienste oder Anbietern digitaler Dienste an das für sie auch im Falle einer Meldepflicht zuständige Computer-Notfallteam gemeldet werden, das die Meldungen zusammengefasst an den Bundesminister für Inneres weiterleitet.

(2) Risiken, Vorfälle und Sicherheitsvorfälle, die Einrichtungen betreffen, die nicht als Betreiber wesentlicher Dienste ermittelt wurden, keine Anbieter digitaler Dienste oder Einrichtungen der öffentlichen Verwaltung sind, können von diesen an das zuständige Computer-Notfallteam gemeldet werden, das die Meldungen zusammengefasst an den Bundesminister für Inneres weiterleitet.

(3) Zuständig für die Entgegennahme von freiwilligen Meldungen gemäß Abs. 2 ist das sektorenspezifische Computer-Notfallteam, falls ein solches eingerichtet ist und von der meldenden Einrichtung unterstützt wird, andernfalls das nationale Computer-Notfallteam, sofern ein solches eingerichtet ist, ansonsten das GovCERT.

(4) Die freiwillige Meldung muss weder die Identität der Einrichtung noch Informationen, die auf diese schließen lassen, enthalten. § 19 Abs. 3 gilt sinngemäß.

(5) Um einen Beitrag zur Gewährleistung eines hohen Sicherheitsniveaus von Netz- und Informationssystemen zu leisten, kann die freiwillig meldende Einrichtung gemäß Abs. 1 und 2 personenbezogene Daten gemäß § 9 Abs. 3 Z 2 an das zuständige Computer-Notfallteam übermitteln.

6. Abschnitt
Strukturen und Aufgaben im Falle der Cyberkrise

Cyberkrise

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

Koordinationsausschuss

§ 25. (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

§ 26. (1) Eine Verwaltungsübertretung begeht, wer

1. eine Kontaktstelle nach § 16 Abs. 3 erster Satz nicht benennt, allfällige Änderungen gemäß § 16 Abs. 3 dritter Satz nicht bekannt gibt oder unter dieser nicht im gemäß § 16 Abs. 3 zweiter Satz vorgesehenen Zeitraum erreichbar ist;
2. den Nachweis nach § 17 Abs. 3 erster Satz oder § 21 Abs. 4 erster Satz nicht erbringt;
3. die Einschau gemäß § 17 Abs. 4 oder § 21 Abs. 4 dritter Satz verweigert;
4. die bescheidmäßig ergangenen Anordnungen nach § 17 Abs. 5 oder § 21 Abs. 4 letzter Satz nicht fristgerecht umsetzt oder
5. der Meldepflicht nach § 19 Abs. 1 iVm Abs. 3 und 4 oder § 21 Abs. 2 nicht nachkommt.

Die Begehung ist mit Geldstrafe bis zu 50.000 Euro, im Wiederholungsfall bis zu 100.000 Euro zu bestrafen.

(2) Zuständig sind die Bezirksverwaltungsbehörden. 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 im Inland nach dem Sitz des Vertreters.

(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 Geldstrafen gegen eine juristische Person oder eingetragene Personengesellschaft verhängen, wenn Verwaltungsübertretungen gemäß Abs. 1 durch Personen begangen wurden, die entweder allein oder als Teil eines Organs der juristischen Person oder der eingetragenen Personengesellschaft gehandelt haben und eine Führungsposition aufgrund

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

innehaben.

(5) Juristische Personen oder eingetragene Personengesellschaften 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 oder der eingetragenen Personengesellschaft tätige Person ermöglicht hat, sofern die Tat nicht den Tatbestand einer in die Zuständigkeit der Gerichte fallenden strafbaren Handlung erfüllt.

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

8. Abschnitt
Schlussbestimmungen

Personenbezogene Bezeichnungen

§ 27. Alle in diesem Bundesgesetz verwendeten personenbezogenen Bezeichnungen gelten gleichermaßen für alle Geschlechter.

Bezugnahme auf Richtlinien

§ 28. Durch dieses Bundesgesetz wird 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, umgesetzt.

Verweisungen

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

Vollziehung

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

Inkrafttreten

§ 31. (1) **(Verfassungsbestimmung)** § 1 in der Fassung BGBl. I Nr. XX/XXXX tritt mit Ablauf des Tages der Kundmachung dieses Bundesgesetzes in Kraft.

(2) §§ 2 bis 30 in der Fassung BGBl. I Nr. XX/XXXX treten mit Ablauf des Tages der Kundmachung dieses Bundesgesetzes in Kraft.

(3) Verordnungen auf Grund dieses Bundesgesetzes können frühestens mit dem Inkrafttreten dieses Bundesgesetzes in Kraft gesetzt werden.

Artikel 2
Änderung des Telekommunikationsgesetzes 2003

Das Telekommunikationsgesetz 2003 (TKG 2003), BGBl. I Nr. 70/2003, zuletzt geändert durch das Bundesgesetz BGBl. I Nr. 29/2018, wird wie folgt geändert:

1. In § 16a wird nach Abs. 5 folgender Abs. 5a eingefügt:

„(5a) Die Regulierungsbehörde hat eine erfolgte Mitteilung nach Abs. 5 unverzüglich an den Bundesminister für Inneres weiterzuleiten. Dieser hat die darin enthaltenen Informationen in das gemäß § 5 Z 3 Netz- und Informationssystemsicherheitsgesetz (NISG), BGBl. I Nr. XX/XXXX, zu erstellende Lagebild aufzunehmen, das im Rahmen der Koordinierungsstrukturen (§ 7 NISG) zu erörtern ist.“

2. In § 137 wird folgender Abs. XX angefügt:

„(XX) § 16a Abs. 5a in der Fassung des Bundesgesetzes BGBl. I Nr. XX/XXXX tritt mit Ablauf des Tages der Kundmachung dieses Bundesgesetzes in Kraft.“

REPUBLIK ÖSTERREICH Parlamentsdirektion SIEGEL	**Unterzeichner**	Parlamentsdirektion
	Datum/Zeit-UTC	2018-11-21T14:51:15+01:00
	Prüfinformation	Informationen zur Prüfung des elektronischen Siegels und des Ausdrucks finden Sie unter: https://www.parlament.gv.at/siegel
Hinweis	Dieses Dokument wurde elektronisch besiegelt.	