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

StF: BGBl. I Nr. 111/2018 (NR: GP XXVI RV 369 AB 418 S. 53. BR: AB 10099 S. 887.)

Der Nationalrat hat beschlossen:

Inhaltsverzeichnis

Federal Act to Ensure a High Level of Security of Network and Information Systems (Network and Information Systems Security Act – NIS Act)

⇐ Original version

Click here for checking the up-to-date list of amendments
in the Austrian Legal Information System.

Disclaimer: The English translation at hand of the authentic German text is unofficial and serves merely information purposes. The official wording and authentic version in German can be found in the Austrian Federal Law Gazette (Bundesgesetzblatt; BGBl.), online available at ris.bka.gv.at. The reader should also bear in mind that some provisions will remain unclear without certain background knowledge of the Austrian legal and political system.

The National Council has resolved:

Table of contents

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,

Section 1
General provisions

Constitutional provision

§ 1. (constitutional provision) The enactment, repeal, amendment and execution of provisions as contained in this Federal Act are the responsibility of the federal government, even in matters where the Federal Constitutional Law *(B-VG, Bundes-Verfassungsgesetz)*, Federal Law Gazette No 1/1930, provides otherwise. This does not apply to matters in which the federal provinces and municipalities exercise public-law powers. The matters regulated in this Federal Act fall under the purview of direct federal administration.

Subject matter and objectives of this Federal Act

§ 2. This Federal Act lays down measures designed to achieve a high level of security of network and information systems of operators of essential services in the sectors of

1. energy,
2. transport,
3. banking,
4. financial market infrastructures,
5. health,
6. drinking water supply,
7. digital infrastructure,

and of digital service providers and entities of public administration.

Definitions

§ 3. For the purposes of this Federal Act, the following definitions apply:

1. “network and information system” means
   a) an electronic communications network within the meaning of § 3 subpara 11 of the Telecommunications Act 2003 *(TKG, Telekommunikationsgesetz 2003)*, Federal Law Gazette I No 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,

b) any device or group of interconnected or related devices, one or more of which, pursuant to a program, perform automatic processing of digital data, or

c) digital data stored, processed, retrieved or transmitted by elements covered under (a) and (b) for the purposes of their operation, use, protection and maintenance;

2. “security of network and information systems (NIS)” means the ability to prevent, detect, resist and eliminate security incidents;

3. “NIS Directive” means Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union, OJ L 194, 19.7.2016, p. 1;

4. “Inner Circle of the Operational Coordination Structure (ICOCS)” means an inter-ministerial structure for coordination at the operational level regarding the security of network and information systems, composed of representatives of the Federal Chancellor, the Federal Minister of the Interior, the Federal Minister of Defence and the Federal Minister for Europe, Integration and Foreign Affairs, who must undergo security vetting for access to secret information before the start of their participation;

5. “Operational Coordination Structure (OCS)” means a structure for coordination at the operational level regarding the security of network and information systems, composed of the ICOCS and the CSIRTs (§ 14);

6. “security incident” means any disturbance of the availability, integrity, authenticity or confidentiality of network and information systems which has resulted in a restriction of continuity or a failure of the service operated with significant impact; when determining the significance of the impact, the following parameters in particular must be taken into account: the prospective

a) number of users affected by the security incident, in particular users relying on the service for the provision of their own services,

b) duration of the security incident,

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;

c) geographical spread with regard to the area affected by the security incident;

d) impact on economic and societal activities.

7. “incident” means any event other than a security incident which has an actual adverse effect on the availability, integrity, authenticity or confidentiality of network and information systems;

8. “risk” means any circumstance or event having a potential adverse effect on the security of network and information systems;

9. “essential service” means a service provided in one of the sectors referred to in § 2 which is essential, in particular, for the maintenance of the public health service, the public supply of water, energy and vital goods, public transport or the functioning of public information and communication technology, and whose availability depends on network and information systems;

10. “operator of essential services” means an entity established in Austria that provides an essential service;

11. “qualified body” means an entity established in Austria which was determined by the Federal Minister of the Interior, pursuant to § 18 para 1, to be suitable for auditing the security measures taken by operators of essential services;

12. “digital service” means a service within the meaning of § 3 subpara 1 of the E-Commerce Act *(ECG, E-Commerce-Gesetz)*, Federal Law Gazette I No 152/2001, which is an online marketplace, an online search engine or a cloud computing service;

13. “digital service provider” means any legal person or registered business partnership other than a microenterprise or small enterprise within the meaning of Article 1 and Article 2 paras 2 and 3 of the Annex to Commission Recommendation 2003/361/EC of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises, OJ L 124, 20.5.2003, p. 36, that provides a digital service in Austria and

a) has its main establishment in Austria or

b) does not have its main establishment in the European Union but has designated a representative;

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

14. “representative” means any natural or legal person or registered business partnership established in Austria explicitly designated to act on behalf of a digital service provider not established in the European Union, which may be addressed by the Federal Chancellor, the Federal Minister of the Interior or the CSIRTs instead of the digital service provider with regard to the obligations of that digital service provider under this Federal Act;
15. “online marketplace” means a digital service that allows consumers or traders to conclude online sales or service contracts with traders either on the online marketplace’s website or on a trader’s website that uses computing services provided by the online marketplace;
16. “online search engine” means a digital service that allows users to perform searches of, in principle, all websites or websites in a particular language on the basis of a query on any subject in the form of a keyword, phrase or other input, and returns links in which information related to the requested content can be found;
17. “cloud computing service” means a digital service that enables access to a scalable and elastic pool of shareable computing resources;
18. “federal entities” means the Federal Ministries, the Courts of Public Law, the Court of Auditors, the Ombudsman Board, the Presidential Chancellery and the Parliamentary Administration; other federal agencies can be determined by ordinance by the competent federal minister;
19. “entities of public administration” means the federal entities and of those federal provinces which have made use of the option provided in § 22 para 5;
20. “Cooperation Group” means a body established pursuant to Article 11 of the NIS Directive, composed of representatives of the Member States of the European Union, the European Commission and the European Union Agency for Network and Information Security (ENISA), in order to support and facilitate strategic cooperation and the exchange of information among the Member States of the European Union and to develop trust and

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;

confidence, with a view to achieving a high common level of security of network and information systems in the European Union;

21. “CSIRTs network” means a body established pursuant to Article 12 of the NIS Directive, composed of representatives of the CSIRTs of the Member States of the European Union and the European computer security incident response team (CERT-EU), in order to contribute to the development of trust and confidence between the Member States of the European Union and to promote swift and effective operational cooperation;
22. “cyber crisis” means one or more security incidents which pose a present and direct threat to the maintenance of critical societal functions and which may have a serious impact on the health, the safety and security or the economic and social well-being of large parts of the population or on the effective functioning of governmental institutions;
23. “cyber crisis management” means a coordination procedure for dealing with cyber crises.

Section 2
Responsibilities and coordination structures

Tasks of the Federal Chancellor

§ 4. (1) The Federal Chancellor has the following strategic tasks:

1. coordinating the preparation of a strategy (§ 8) and of an annual report on the security of network and information systems;
2. representing Austria in the Cooperation Group and in other EU-wide and international bodies for the security of network and information systems which are charged with strategic tasks; the responsibilities of other ministries remain unaffected thereby;
3. coordinating public-private cooperation regarding the security of network and information systems;
4. operating the GovCERT pursuant to § 14 para 4;
5. informing the public about security incidents affecting several of the sectors referred to in § 2;

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;

6. identifying operators of essential services pursuant to § 16 para 1 as well as establishing and regularly updating a list of essential services;
7. consulting with the competent authorities in other Member States in cases where digital service providers have their main establishment in Austria but their network and information systems are located in another Member State;
8. determining the suitability of and granting authorisation to CSIRTs pursuant to § 15 para 3;
9. publishing and updating a list of CSIRTs pursuant to § 14 paras 1 and 4 in an appropriate form.

(2) In agreement with the Federal Minister of the Interior, the Federal Chancellor can specify the following by ordinance:

1. criteria for the parameters of § 3 subpara 6 (a) to (d);
2. detailed provisions for each of the sectors referred to in § 2, pursuant to § 16 para 2;
3. security measures pursuant to § 17 para 1;
4. exceptions to the obligations on operators of essential services pursuant to § 20 para 1.

(3) In agreement with the Federal Minister of the Interior and the Federal Minister of Defence, the Federal Chancellor determines, by ordinance, the distribution of their responsibilities as joint controllers pursuant to § 11 para 3.

Tasks of the Federal Minister of the Interior

§ 5. (1) The Federal Minister of the Interior has the following operational central tasks:

1. operating a single point of contact (SPOC) for the security of network and information systems (§ 6);
2. conducting the organisational management of the coordination structures ICOCS and OCS (§ 7);
3. receiving and analysing notifications about risks, incidents or security incidents, preparing regular situation assessments in this regard, and forwarding the notifications and situation assessments and any additional information of relevance to domestic authorities or bodies in accordance with Section 3;

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

4. preparing and sharing information relevant for ensuring the security of network and information systems in an effort to prevent security incidents;
5. performing audits of security requirements (§ 17 and § 21) and verifying compliance with the notification obligation (§ 19 and § 21);
6. determining and performing audits of qualified bodies (§ 18);
7. informing the public about individual security incidents (§ 10 para 1);
8. heading and coordinating cyber crisis management at the operational level (Section 6).

(2) In agreement with the Federal Chancellor, the Federal Minister of the Interior specifies, by ordinance, the requirements to be met by a qualified body or special criteria according to which an entity is, in any event, deemed a qualified body, and the procedure for determining qualified bodies.

Single point of contact

§ 6. (1) A competent single point of contact (SPOC) on the security of network and information systems, which exercises an operational liaison function to ensure cross-border cooperation with the competent bodies in other Member States of the European Union and with the Cooperation Group and the CSIRTs network, is established within the purview of the Federal Minister of the Interior.

(2) The single point of contact

1. forwards incoming notifications and requests directly to the members of the ICOCS and the CSIRTs (§ 14), insofar as this is necessary to fulfil any task assigned to the relevant member of the ICOCS or CSIRT by law, and
2. informs, upon request, the single points of contact in other Member States if a security incident concerns one or more other Member States of the European Union (§ 19 para 5, § 21 para 3 and § 22 para 4).

Coordination structures

§ 7. (1) The ICOCS is established to discuss and update the situation assessment on risks, incidents and security incidents prepared by the Federal Minister of the Interior, to discuss the findings obtained pursuant to § 13 paras 1 and

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.

2, and to support the coordination committee when it comes to cyber crisis management. The ICOCS also serves to exchange classified information between the participants in order to perform the tasks within their areas of responsibility.

(2) An OCS is established to discuss a holistic situation assessment, which also includes the voluntary notifications. The OCS can be expanded to include representatives of operators of essential services, digital service providers and entities of public administration where their sphere of activities is affected by a particular risk, incident or security incident. OCS participants are under an obligation to maintain confidentiality with regard to any information that becomes known to them as a result of their participation in accordance with the detailed provisions pursuant to para 3.

(3) The Federal Minister of the Interior can adopt rules of procedure laying down detailed provisions regarding the interaction of the coordination structures pursuant to paras 1 and 2, in particular regarding the convocation of meetings, their composition and their decision-making processes.

(4) The entities participating in the OCS may process and transfer to one another the personal data required for the purpose of organising the OCS and for performing the tasks pursuant to paras 1 and 2.

Strategy on the security of network and information systems

§ 8. (1) The strategy on the security of network and information systems defines, in particular, the strategic objectives and appropriate policy and regulatory measures with a view to achieving and maintaining a high level of security of network and information systems in the federal territory.

(2) The Federal Chancellor communicates the strategy on the security of network and information systems to the European Commission within three months from its adoption. Elements of the strategy which relate to national security are not to be communicated.

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:

Section 3
Powers and data processing

Data processing

§ 9. (1) For the purpose of ensuring a high level of security of network and information systems when performing their tasks under this Federal Act and for the purpose of safeguarding against and the prevention of threats to public security, the Federal Chancellor, the Federal Minister of the Interior, the Federal Minister of Defence, the Federal Minister for Europe, Integration and Foreign Affairs, and the CSIRTs pursuant to § 14 para 1 are entitled to process and transfer to one another and to the OCS members the required personal data within the meaning of Article 4 para 2 of Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (hereinafter: GDPR), OJ L 119, 4.5.2016, p. 1, as amended by the corrigendum in OJ L 314, 22.11.2016, p. 72, and within the meaning of § 36 of the Federal Act on the Protection of Natural Persons with regard to the Processing of Personal Data (Data Protection Act *[DSG, Datenschutzgesetz]*), Federal Law Gazette I No 165/1999.

(2) These personal data are the following:

1. personal data of participants and their organisational units which are required for organisational purposes to enable participation in the coordination structures and in the course of such participation;
2. personal data of persons implicated in risks, incidents and security incidents that are required for the purposes of discussing and updating the situation assessment prepared by the Federal Minister of the Interior, discussing the findings obtained pursuant to § 13 paras 1 and 2, and supporting the coordination committee;
3. personal data of persons involved in or affected by a particular case.

(3) For the purpose of analysing and handling risks, incidents and security incidents, the Federal Chancellor, the Federal Minister of the Interior and the Federal Minister of Defence are entitled to process and transfer to one another the following personal data in addition to the data referred to in para 2:

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

1. contact and identity data as well as technical data of the party submitting a notification and of the contact person;
2. contact and identity data as well as technical data of persons implicated in a notification regarding a risk, incident or security incident, such as, in particular, the victim and the attacker.

(4) For the purpose of fulfilling their tasks under § 4 and § 5, the Federal Chancellor and the Federal Minister of the Interior are entitled to process and transfer to one another the following personal data in addition to the data referred to in paras 2 and 3:

1. contact and identity data as well as technical data of operators of essential services, digital service providers, entities of public administration that have made use of the option provided in § 22 para 5, CSIRTs and competent authorities of other Member States;
2. contact and identity data as well as technical data of persons implicated in a notification regarding a risk, incident or security incident, such as, in particular, the victim and the attacker;
3. contact and identity data of participants and their organisational units that are required to enable participation in EU-wide, international and national bodies for the security of network and information systems and in the course of such participation.

(5) For the purpose of fulfilling his or her tasks under § 5 subparas 4 to 6, the Federal Minister of the Interior is entitled to process the following personal data in addition to the data referred to in paras 2 to 4:

1. contact and identity data as well as technical data of qualified bodies;
2. contact and identity data as well as technical data of persons in the context of audits of security measures;
3. technical data of persons gathered in the context of § 13.

(6) Any consultation, transfer and alteration of personal data must be logged in a revision-proof manner. The records must be kept for three years and deleted after expiry of that period.

(7) The right to erasure and the right to object pursuant to the GDPR or § 45 of the Data Protection Act are limited insofar as the retention or archiving of data is prescribed by law or by ordinance, or erasure is contrary to the public interest of

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

ensuring a high level of security of network and information systems, and the data subject cannot demonstrate grounds relating to his or her particular situation which override the objectives of limiting the relevant right. The competent data protection officer must be informed about the performance and outcome of such an assessment.

(8) With regard to integrated data processing systems, the right to restriction of processing pursuant to Article 18 of the GDPR or § 45 of the Data Protection Act is limited for the period required to verify the accuracy of a data subject's personal data, where such accuracy has been contested by the data subject, and for the period in which the data subject has exercised his or her right to object, pending the verification whether the legitimate grounds of the controller override those of the data subject.

(9) Each controller must independently perform the data protection obligations under the GDPR and Chapter 3 of the Data Protection Act with regard to the personal data processed, transferred or further processed in connection with the procedures conducted or measures taken by the relevant controller.

Data transfer

§ 10. (1) After consulting the operator of essential services or digital service provider affected by a security incident, the Federal Chancellor and the Federal Minister of the Interior can, within their respective sphere of activities, publish personal data pursuant to § 9 para 3 subpara 2 after having balanced the relevant interests with regard to the impact on data subjects, in order to inform the public about security incidents, where public awareness is necessary in order to prevent or to deal with a security incident, or where disclosure of the security incident is otherwise in the public interest. The Federal Minister of the Interior may require digital service providers to inform the public themselves.

(2) Data known to the Federal Chancellor, the Federal Minister of the Interior, the Federal Minister of Defence and the Federal Minister for Europe, Integration and Foreign Affairs as a result of performing their tasks under this Federal Act can be transferred to military bodies and authorities for the purposes of the country's military defence pursuant to Article 79 para 1 of the Federal Constitutional Law, to security authorities for the purposes of public safety matters and criminal justice, to

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

public prosecutors' offices and courts of justice for the purposes of criminal justice, and to domestic authorities, to the extent that this is an essential requirement for performing a task assigned to them by law.

(3) For the purpose of fulfilling his or her tasks pursuant to § 5 subpara 4, the Federal Minister of the Interior can transfer data pursuant to § 9 para 2 subpara 2 and para 3 subpara 2 to operators of essential services, digital service providers and entities other than operators of essential services or digital service providers if they are affected by a risk, incident or security incident.

(4) The Federal Minister of the Interior is entitled to transfer data pursuant to § 9 paras 2 to 5 to foreign security authorities and security organisations pursuant to § 2 paras 2 and 3 of the Federal Act on International Police Cooperation (Police Cooperation Act *[PolKG, Polizeikooperationsgesetz]*), Federal Law Gazette I No 104/1997, and to institutions of the European Union or the United Nations in accordance with the provisions on international mutual assistance in police matters.

(5) For the purpose of fulfilling his or her tasks pursuant to § 19 para 5, § 21 para 3 and § 22 para 4, the Federal Minister of the Interior is entitled, after having balanced the relevant interests with regard to the commercial interests of the entity concerned and the confidentiality of the information provided in the notification, to transfer personal data of persons implicated in a security incident to the single point of contact in the Member States affected by the security incident.

(6) The Federal Chancellor is entitled to transfer personal contact and identity data of operators of essential services and digital service providers to CSIRTs to enable them to perform their tasks pursuant to § 14 para 2.

(7) The Federal Chancellor is entitled to transfer identity data of operators of essential services to the federal provinces in whose territory the operator is established and to the supervisory authorities for the relevant sector in which the essential service is provided, to the extent that this is necessary for them to perform their tasks.

NIS notification analysis system

§ 11. (1) For the purpose of analysing notifications about risks, incidents and security incidents (§ 19, § 20 para 2, § 21 para 2, § 22 paras 2 and 3, and § 23 paras 1 and 2) and findings obtained pursuant to § 13 paras 1 and 2, the Federal Minister of the Interior must operate ICT solutions and make them available to the Federal Chancellor and the Federal Minister of Defence to support the assessment

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

of risks, incidents and security incidents in network and information systems and the preparation of situation assessments through strategic or operational analyses.

(2) Regarding the ICT solutions and IT procedures under para 1, the Federal Minister of the Interior, the Federal Chancellor and the Federal Minister of Defence are joint controllers pursuant to Article 4 para 7 in connection with Article 26 of the GDPR and § 36 of the Data Protection Act.

(3) The distribution of their responsibilities as joint controllers is determined by ordinanceby the Federal Chancellor in agreement with the Federal Minister of the Interior and the Federal Minister of Defence.

ICOCS platform

§ 12. (1) The Federal Minister of the Interior can operate an ICT solution for the purposes of organising the ICOCS and performing the tasks pursuant to § 7 para 1. If such an ICT solution is operated, it must be made available to the Federal Chancellor, the Federal Minister of Defence and the Federal Minister for Europe, Integration and Foreign Affairs.

(2) Regarding the ICT solution under para 1, the Federal Minister of the Interior, the Federal Chancellor, the Federal Minister of Defence and the Federal Minister for Europe, Integration and Foreign Affairs are joint controllers pursuant to Article 4 para 7 in connection with Article 26 of the GDPR and § 47 of the Data Protection Act. The obligations arising from the GDPR must be performed by the Federal Minister of the Interior, unless the following paragraphs expressly provide otherwise.

(3) If a data subject exercises his or her rights pursuant to the provisions of Chapter III of the GDPR or § 42 to § 45 of the Data Protection Act, the joint controllers must inform one another thereof without undue delay. Each of the joint controllers must independently perform the obligations in connection with the rights of data subjects with regard to the data collected and processed by the relevant controller.

Operation of ICT solutions to prevent security incidents

§ 13. (1) For the purpose of fulfilling the task pursuant to § 5 subpara 4, the Federal Minister of the Interior is authorised to operate ICT solutions to identify risks or incidents in network and information systems at an early stage. Operators of essential services, digital service providers and entities of public administration

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;

can participate in the ICT solutions operated by the Federal Minister of the Interior and determine which data are transferred to the Federal Minister of the Interior. In compensation for the participation in the ICT solutions, the Federation is entitled to a lump sum reflecting the average cost and specified by an ordinanceby the Federal Minister of the Interior.

(2) For the purpose of fulfilling the task pursuant to § 5 subpara 4, the Federal Minister of the Interior is authorised to operate or – after consent by the entity concerned has been obtained – use ICT solutions in order to recognise patterns of attacks against network and information systems. The GovCERT is also authorised to operate such ICT solutions for the purpose of performing the tasks pursuant to § 14 para 2 subparas 3 and 5, and may process the personal technical data derived therefrom as a controller pursuant to Article 4 para 7 of the GDPR and § 36 para 2 subpara 8 of the Data Protection Act.

Section 4
Computer security incident response teams (CSIRTs)

Tasks and purpose of CSIRTs

§ 14. (1) CSIRTs are established to ensure the security of network and information systems. For this purpose, the national CSIRT and sector-specific CSIRTs support operators of essential services and digital service providers, and the Government Computer Emergency Response Team (GovCERT) supports the entities of public administration, in handling risks, incidents and security incidents.

(2) CSIRTs pursuant to para 1 have, in any event, the following tasks:

1. receiving notifications about risks, incidents or security incidents pursuant to § 19, § 21 para 2 and § 23 paras 1 and 2,
2. forwarding notifications (subpara 1) to the Federal Minister of the Interior,
3. providing early warning, alerts and recommendations for action as well as announcements and dissemination of information about risks, incidents or security incidents,
4. providing initial general technical support in responding to security incidents,

5. Beobachtung und Analyse von Risiken, Vorfällen oder Sicherheitsvorfällen sowie Lageberurteilung;
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,

5. providing risk, incident or security incident monitoring and analysis and situational awareness,
6. participating in the coordination structures pursuant to § 7 and participating in the CSIRTs network.

(3) Operators of essential services can establish a sector-specific CSIRT for their sector (§ 2) that performs the tasks pursuant to para 2 with regard to the operators of essential services supporting it. For the purposes of para 2 subparas 3 and 5, sector-specific CSIRTs can, on behalf of an operator of essential services, analyse data pursuant to the second sentence of § 13 para 1 that were derived from an ICT solution pursuant to the first sentence of § 13 para 1 implemented by the relevant operator of essential services. Regarding digital service providers, this applies with the proviso that they can task the national CSIRT with analysing such data.

(4) The Government Computer Emergency Response Team (GovCERT) is established within the purview of the Federal Chancellor. In addition to receiving and forwarding notifications pursuant to § 22 paras 2 and 3, and, if applicable, pursuant to § 19 para 2, § 21 para 2 and § 23 para 3, the GovCERT has the tasks pursuant to para 2 subparas 3 to 5 and the second sentence of para 3 with regard to entities of public administration, insofar as the relevant entity is not represented in the ICOCS.

(5) The GovCERT, the national CSIRT and the sector-specific CSIRTs must inform, without undue delay, the Federal Chancellor and the Federal Minister of the Interior about activities of the CSIRTs network which are necessary to fulfil their tasks under this Federal Act and may attend meetings of the CSIRTs network.

(6) CSIRTs can perform the tasks pursuant to para 2 subparas 3 to 5 also with regard to other entities or persons if such entities or persons are affected by a risk or incident in their network and information systems.

(7) As controllers pursuant to Article 4 para 7 of the GDPR, CSIRTs are authorised to process personal data pursuant to § 9 paras 2 to 4 to the extent that this is required to fulfil the tasks pursuant to para 2.

(8) For the purpose of performing the tasks pursuant to para 2 subparas 3, 5 and 6, CSIRTs are entitled to transfer personal data pursuant to § 9 para 2 subpara 2 and para 3 subpara 2 to operators of essential services, digital service providers,

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

entities of public administration, entities having submitted a notification pursuant to § 23 para 2 and members of the CSIRTs network and to one another.

Requirements for and suitability of CSIRTs

§ 15. (1) CSIRTs pursuant to § 14 para 1 must, in any event, meet the following requirements:

1. Their premises and the supporting network and information systems comply with the standards specified in Article 32 of the GDPR and are located in secure sites.
2. Their business continuity is ensured, in particular through
   a) the use of an appropriate system for managing and routing requests, and
   b) adequate staff, technical equipment and infrastructure to ensure availability and continuity at all times.
3. As far as CSIRTs pursuant to the second sentence of § 14 para 1 are concerned, evidence of support from operators of essential services must be provided.
4. The staff to be used to fulfil the tasks under § 14 para 2 are qualified and must undergo security vetting pursuant to § 55 et seqq. of the Security Police Act *(SPG, Sicherheitspolizeigesetz)*, Federal Law Gazette No 566/1991, for access to secret information before the start of their work. Security vetting must be repeated every five years. For the performance of security vetting, the person requesting to be vetted must pay a flat fee equivalent to the amount prescribed in § 5 of the Security Fees Ordinance *(SGV, Sicherheitsgebühren-Verordnung)*, Federal Law Gazette No 389/1996.
5. When performing their tasks pursuant to § 14 para 2 subparas 1 and 2, they must use secure communication channels agreed in advance with the Federal Minister of the Interior.

(2) The GovCERT must meet the requirements pursuant to para 1 with the exception of subpara 3.

(3) The Federal Chancellor must ascertain, in agreement with the Federal Minister of the Interior, that the national CSIRT and, upon request, a sector-specific CSIRT meets the requirements pursuant to para 1 and is suitable to perform the tasks pursuant to § 14 para 2. If a CSIRT is a private entity, it must be authorised by the

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;

Federal Chancellor, in agreement with the Federal Minister of the Interior, to fulfil the tasks pursuant to § 14 para 2 subparas 1 and 2. CSIRTs must notify, without undue delay, the Federal Chancellor of any changes with regard to the circumstances that were the prerequisites for determining their suitability or for granting the authorisation. The authorisation must be revoked entirely or only with regard to the fulfilment of individual tasks if any prerequisite required for granting the authorisation is no longer satisfied.

(4) The personal contact and identity data of the CSIRTs must be published by the Federal Chancellor in an appropriate form.

Section 5

Obligations on operators of essential services, digital service providers and entities of public administration

Identification of operators of essential services

§ 16. (1) After consulting the Federal Minister of the Interior and the competent federal minister, the Federal Chancellor identifies, for each sector referred to in § 2, the operators of essential services with an establishment in Austria which provide an essential service.

(2) In agreement with the Federal Minister of the Interior, the Federal Chancellor can specify, by ordinance, detailed provisions regarding the sectors referred to in § 2. This ordinancemay include, without limitation, subsectors, areas, the related essential services and the types of entities eligible as operators of essential services. When assessing whether a service is of an essential nature, the following factors in particular must be taken into account:

1. the number of users relying on the service provided by the relevant operator of an essential service;
2. the dependency of other sectors referred to in § 2 on the service provided by that operator;
3. the market share of the operator of essential services;
4. the geographic spread with regard to the area that could be affected by a security incident;

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.

5. the impact that security incidents have, in terms of degree and duration, on economic and societal activities or public safety and security;
6. the importance of the operator of essential services for maintaining a sufficient level of the service, taking into account the availability of alternative means for the provision of that service.

In addition, sector-specific factors must also be taken into account where appropriate.

(3) Operators of essential services must name to the Federal Chancellor, within two weeks of service of the administrative decision pursuant to para 4 subpara 1, a point of contact for communicating with the Federal Chancellor, the Federal Minister of the Interior or the CSIRTs. The operator of essential services must ensure that the operator can be contacted through this point of contact at least during the period in which the operator provides an essential service pursuant to para 2. The operator of essential services must communicate any changes in the point of contact without undue delay.

(4) For the purposes of para 1, the Federal Chancellor fulfils the following tasks:

1. issuing an administrative decision identifying an operator of essential services pursuant to para 1; if the prerequisites for the administrative decision determining that a particular entity is an operator of essential services are no longer satisfied at a later point in time or if it turns out that they had never been satisfied in the first place, this must also be established in an administrative decision;
2. engaging in consultation with other Member States of the European Union where an operator of essential services provides a service pursuant to para 2 in one or more Member States of the European Union. The decision on whether an operator of essential services is to be identified pursuant to para 1 can only be taken after consultation with the other Member State(s) of the European Union;
3. establishing and regularly updating a list of essential services;
4. submitting the list (subpara 3) to the European Commission at least every two years.

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.

Security measures for operators of essential services

§ 17. (1) Operators of essential services must take appropriate and proportionate technical and organisational security measures to ensure the security of network and information systems which they use in the context of offering the essential service. Those security measures must have regard to the state of the art and must be appropriate to the reasonably identifiable risk.

(2) In cooperation with their sector associations, operators of essential services can propose sector-specific security measures to ensure compliance with the requirements laid down in para 1. The Federal Minister of the Interior determines, upon request, whether these measures are suitable to meet the requirements laid down in para 1.

(3) Operators of essential services must, at least every three years after service of the administrative decision pursuant to § 16 para 4 subpara 1, provide evidence to the Federal Minister of the Interior that they meet the requirements laid down in para 1. For this purpose, they must submit to the Federal Minister of the Interior a list of the security measures in place by presenting evidence of certifications or audits performed by qualified bodies, including any security deficiencies detected.

(4) To verify compliance with the requirements pursuant to para 1, the Federal Minister of the Interior can inspect the network and information systems used for providing the essential service and any related documents. For the purpose of such inspection, the Federal Minister of the Interior is entitled, after prior notification, to enter premises where network and information systems are situated. The inspection must be performed to the extent absolutely necessary with the least possible harm being done to the rights of the entity concerned and of third parties and to the operations.

(5) For the purpose of establishing compliance with the requirements laid down in para 1, the Federal Minister of the Interior is authorised to issue recommendations and, if required, set a reasonable period for complying with these recommendations and furnishing corresponding evidence, failing which operators of essential services are ordered by an administrative decision to comply with these recommendations.

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

Qualified bodies

§ 18. (1) The Federal Minister of the Interior decides, upon request, whether a particular entity is a qualified body.

(2) If the requirements or criteria pursuant to § 5 para 2 are no longer met, the qualified body is, in a first step, advised that it must comply with the requirements or criteria within a reasonable period. In the event of non-compliance, the Federal Minister of the Interior revokes the administrative decision issued pursuant to para 1.

(3) To verify compliance with the requirements and criteria for qualified bodies pursuant to § 5 para 2, the Federal Minister of the Interior can inspect their network and information systems and any related documents. The second and third sentences of § 17 para 4 apply.

(4) The Federal Minister of the Interior keeps a list of qualified bodies and their responsibilities, which is open to inspection by operators of essential services.

Notification obligation for operators of essential services

§ 19. (1) Operators of essential services must notify, without undue delay, the CSIRT competent in their case of any security incidents concerning any essential services they provide; the CSIRT forwards the notification to the Federal Minister of the Interior without undue delay.

(2) The entity responsible for receiving the notification pursuant to para 1 is the sector-specific CSIRT (second sentence of § 14 para 1), where such has been established and is supported by the operator of essential services concerned (§ 15 para 1 subpara 3), or else the national CSIRT, where such has been established, or else the GovCERT.

(3) The notification must include all relevant information regarding the security incident and the technical environment known at the time of the initial notification, in particular the presumed or actual cause, the information technology concerned, the type of entity or facility concerned. Any information on circumstances surrounding the security incident which have become known at a later point in time must be communicated in subsequent notifications and ultimately in a final notification without any further undue delay. The notification must be submitted in a standardised electronic format.

(4) Where an operator of essential services relies on a digital service provider, any significant impact on the continuity of the essential services due to a security

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,

incident affecting the digital service provider must be notified by that operator of essential services.

(5) Where a security incident experienced by an operator of essential services concerns one or more other Member States of the European Union, the Federal Minister of the Interior or the competent CSIRT must inform, through the single point of contact (SPOC), the single point of contact in those Member States.

Exceptions to the obligations on operators of essential services

§ 20. (1) § 17 or § 19 do not apply if the provision of an essential service is subject to rules related to security measures or notification obligations under Union law or under subject-specific legislation based on provisions of Union law which ensure at least an equivalent level of security of network and information systems, and if the Federal Chancellor, by ordinance, in agreement with the Federal Minister of the Interior, specifies these rules and determines that they are appropriate.

(2) The Financial Market Authority *(FMA, Finanzmarktaufsicht)* must communicate notifications of major operational or security incidents as referred to in § 86 para 1 of the Payment Services Act 2018 *(ZaDiG, Zahlungsdienstegesetz 2018)*, Federal Law Gazette I No 17/2018, of payment service providers identified as operators of essential services to the Federal Minister of the Interior without undue delay.

Security measures and notification obligation for digital service providers

§ 21. (1) Digital service providers must take appropriate and proportionate technical and organisational security measures to ensure the security of network and information systems which they use in the context of offering the digital service. Having regard to the state of the art, those measures must ensure a level of security of network and information systems appropriate to the reasonably identifiable risk posed, and must take into account the following elements:

a) the security of systems and facilities,

b) security incident handling,

c) business continuity management,

d) monitoring, auditing and testing,

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.

e) compliance with international standards.

(2) Digital service providers must notify, without undue delay, the national CSIRT, where such has been established, or else the GovCERT of any security incidents concerning any digital services they provide; the national CSIRT or the GovCERT forwards the notification to the Federal Minister of the Interior without undue delay. The obligation to notify a security incident only applies where the digital service provider has access to the information needed to assess the impact of a security incident. § 19 para 3 applies *mutatis mutandis*.

(3) Where a security incident experienced by a digital service provider concerns one or more other Member States of the European Union, the Federal Minister of the Interior or the competent CSIRT pursuant to para 2 must inform, through the single point of contact (SPOC), the single point of contact in those Member States.

(4) If evidence of any circumstances demonstrating that a digital service provider does not comply with its obligations pursuant to para 1 becomes known to the Federal Minister of the Interior, the Federal Minister of the Interior is authorised to require the digital service provider concerned to provide evidence of appropriate security measures. For that purpose, the digital service provider concerned must provide a list of the security measures in place. The Federal Minister of the Interior can also inspect the network and information systems used for providing the digital service and any related documents. The second and third sentences of § 17 para 4 apply. For the purpose of establishing compliance with the requirements laid down in para 1, the Federal Minister of the Interior is authorised to issue recommendations and, if required, set a reasonable period for complying with these recommendations and furnishing corresponding evidence, failing which digital service providers are ordered by an administrative decision to comply with these recommendations.

Security measures and notification obligation for entities of public administration

§ 22. (1) Federal entities must take appropriate and proportionate technical and organisational security measures to ensure the security of network and information systems which they use in the context of offering vital services. Those security measures must have regard to the state of the art and must be appropriate to the reasonably identifiable risk.

(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

(2) Federal entities, insofar as the relevant entity is not represented in the ICOCS, must notify, without undue delay, the GovCERT of any security incidents concerning any vital services they provide; the GovCERT forwards the notification to the Federal Minister of the Interior without undue delay. § 19 para 3 applies *mutatis mutandis*. Notifications of security incidents concerning an entity represented in the ICOCS are made within the ICOCS.

(3) Entities of public administration can submit notifications of risks and incidents to the GovCERT, which forwards the notifications in aggregated form to the Federal Minister of the Interior. § 23 paras 4 and 5 apply *mutatis mutandis*. Notifications of risks and incidents concerning an entity represented in the ICOCS can be made within the ICOCS on a voluntary basis.

(4) Where a security incident experienced by an entity of public administration concerns one or more other Member States of the European Union, the Federal Minister of the Interior or the GovCERT must inform, through the single point of contact (SPOC), the single point of contact in those Member States.

(5) Federal provinces can declare, by means of provincial legislation, that the obligations pursuant to paras 1 and 2 also apply to vital services provided by their entities. These provincial entities are the offices of the provincial governments and other provincial and municipal agencies that may be declared as such by the relevant provincial bodies.

(6) Federal provinces must inform the Federal Chancellor in writing of any adoption of provincial legislation pursuant to para 5 and any repeal thereof. If a federal province makes use of the option provided in para 5, the provisions relating to federal entities also apply to entities of the relevant province.

Voluntary notifications

§ 23. (1) Operators of essential services or digital service providers can submit notifications of risks and incidents to the CSIRT which is also competent for any mandatory notifications on their part and which forwards the notifications in aggregated form to the Federal Minister of the Interior.

(2) Entities which have not been identified as operators of essential services and which are not digital service providers or entities of public administration can submit notifications of risks, incidents and security incidents concerning them to the

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.

competent CSIRT, which forwards the notifications in aggregated form to the Federal Minister of the Interior.

(3) The entity responsible for receiving voluntary notifications pursuant to para 2 is the sector-specific CSIRT, where such has been established and is supported by the notifying entity, or else the national CSIRT, where such has been established, or else the GovCERT.

(4) Voluntary notifications need not include the entity's identity nor any information that might reveal the entity's identity. § 19 para 3 applies *mutatis mutandis.*

(5) To help ensure a high level of security of network and information systems, the entity submitting a voluntary notification pursuant to paras 1 and 2 can transfer personal data pursuant to § 9 para 3 subpara 2 to the competent CSIRT.

Section 6
Structures and tasks in the event of a cyber crisis

Cyber crisis

§ 24. The Federal Minister of the Interior decides whether a given situation constitutes a cyber crisis.

Coordination committee

§ 25. (1) A coordination committee is established to advise the Federal Minister of the Interior on decisions as to whether a given situation constitutes a cyber crisis and on operational measures to deal with a cyber crisis and to advise the federal government on the coordination of public relations work.

(2) The coordination committee is headed by the Director General for Public Security and is composed of the Chief of Defence Staff, the Secretary General of the Federal Chancellery and the Secretary General for Foreign Affairs. If required to deal with a cyber crisis, the committee is to be extended to include further representatives of federal or provincial authorities, operators of essential services and CSIRTs as well as emergency services.

(3) The ICOCS supports the coordination committee by preparing ad-hoc situation assessments and providing its technical expertise.

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

Section 7
Penal provisions

Administrative penal provisions

§ 26. (1) Whoever

1. fails to designate a point of contact pursuant to the first sentence of § 16 para 3, fails to communicate any changes pursuant to the third sentence of § 16 para 3 or cannot be contacted at that point of contact during the period stipulated in the second sentence of § 16 para 3;
2. fails to provide evidence pursuant to the first sentence of § 17 para 3 or the first sentence of § 21 para 4;
3. refuses inspection pursuant to § 17 para 4 or the third sentence of § 21 para 4;
4. fails to implement the orders issued in an administrative decision pursuant to § 17 para 5 or the last sentence of § 21 para 4 within due time; or
5. fails to comply with the notification obligation pursuant to § 19 para 1 in connection with paras 3 and 4 or § 21 para 2;

commits an administrative offence. Such administrative offence carries a fine of up to € 50,000 or, if the offence is committed repeatedly, up to € 100,000.

(2) The district administrative authorities have jurisdiction for such administrative offences. Territorial jurisdiction for administrative offences pursuant to para 1 is based on the place of main establishment of the operator of essential services or the digital service provider or, if there is no main establishment in Austria, on the place of the representative's seat.

(3) An administrative offence pursuant to para 1 is not deemed to exist where an act meets the elements of a criminal offence falling under the jurisdiction of the courts of justice or is subject to a more severe punishment under different administrative penal provisions.

(4) The district administrative authority can impose fines on legal persons or registered partnerships if persons who acted individually or as part of an executive body of a legal person or registered partnership and who have a leading position on the basis of

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.

1. a power of representation of the legal person or registered partnership,
2. an authority to take decisions on behalf of the legal person or registered partnership, or
3. an authority to exercise control within the legal person or registered partnership,

have committed an administrative offence pursuant to para 1.

(5) Legal persons or registered partnerships can also be held responsible for administrative offences pursuant to para 1 if the commission of such offences by a person acting for the legal person or registered partnership was made possible by a lack of supervision or control by one of the persons referred to in para 4, unless the act meets the elements of a criminal offence falling under the jurisdiction of the courts.

(6) The punishment of persons responsible pursuant to § 9 of the Administrative Penal Act 1991 *(VStG, Verwaltungsstrafgesetz 1991)*, Federal Law Gazette No 52/1991, can be dispensed with if an administrative penalty for the same offence has already been imposed on the legal person.

Section 8
Final provisions

Gender-specific terms

§ 27. All gender-specific terms used in this Federal Act apply equally to all genders.

Reference to directives

§ 28. This Federal Act serves to implement Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union, OJ L 194, 19.7.2016, p. 1.

References

§ 29. References in this Federal Act to other federal acts are deemed to be references to the federal acts as amended.

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. 111/2018 tritt mit Ablauf des Tages der Kundmachung dieses Bundesgesetzes in Kraft.

(2) §§ 2 bis 30 in der Fassung BGBl. I Nr. 111/2018 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.

Execution

§ 30. Unless the federal government is responsible for execution, the execution of this Federal Act is entrusted to the Federal Chancellor, the Federal Minister of the Interior, the Federal Minister of Defence and the Federal Minister for Europe, Integration and Foreign Affairs within their respective sphere of activities.

Entry into force

§ 31. (1) **(constitutional provision)** § 1, as promulgated in Federal Law Gazette I No 111/2018, enters into force after the end of the date of promulgation of this Federal Act.

(2) § 2 to § 30, as promulgated in Federal Law Gazette I No 111/2018, enter into force after the end of the date of promulgation of this Federal Act.

(3) Ordinances on the basis of this Federal Act may enter into force no earlier than at the time when this Federal Act enters into force.