EnCaViBS

WP 2: The NIS Directive and its transposition into national law.

Member State:

Austria

Federal Law for a High Common Level of Security of Network and Information Systems

(Network and Information Systems Security Act - NIS Act)

Important notice:

This text is an unofficial translation conducted at the SnT/ University of Luxembourg in the framework of the research project EnCaViBS.

The original legal acts which Member States notified to the European Commission as national execution measures were retrieved from official national databases. In order to focus on the core of the research project, only selected transpositions have been translated.

The translations only serve the purpose of being an information resource; there is no guarantee whatsoever that the translations correctly correspond to the original versions of the laws. Therefore, evidently, the texts have no legal value. The original, as well as the translated version of the legal acts, are available at www.encavibs.uni.lu, where additional information on the research project may be found.

This research project is funded by the Luxembourg National Research Fund (FNR), C18/IS/12639666/EnCaViBS/Cole,

https://www.fnr.lu/projects/the-eu-nis-directive-enhancing-cybersecurity-across-vital-business-sectors-encavibs/.

Fonds National de la Recherche Luxembourg

Member State: Austria

Federal Law for a High Common Level of Security of Network and Information Systems (Network and Information Systems Security Act - NIS Act)

Federal Law Gazette Volume I No. 111/2018

(Version dated 20.12.2020)

Preamble/Promulgation Clause

The National Council has decided:

Table of Contents

1. Section

General Provisions

Constitutional Provision

§ 1. (Constitutional provision) The enactment, repeal, amendment and enforcement of provisions contained in this Federal Act are also federal matters, in respect of which the Federal Constitutional Act (B-VG), Federal Law Gazette No. 1/1930, provides otherwise. This does not apply in the area of sovereign administration of states and municipalities. The matters regulated in this federal law can be dealt with in the direct federal administration.

Object and Objectives of the Law

§ 2. With this federal law, measures are established with which a high level of security of network and information systems of operators of essential services in the sectors

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

as well as of providers of digital services as well as public administration bodies is to be achieved.

Definitions

§ 3. In the sense of this federal law

1. “Network and Information System” means

a) an electronic communication network within the meaning of § 3 no. 11 Telecommunications Act 2003 (TKG 2003), Federal Law Gazette Volume I No. 70/2003,

b) a device or a group of linked or interconnected devices, which separately or in groups automatically perform the processing of digital data, or

c) digital data, which are stored, processed, retrieved, or transmitted by the units specified in a and b, for the purpose of their operation, use, protection, and maintenance;

2. “Network and information systems security (NIS)” the ability to prevent security incidents, to recognise them, avert, and resolve them;

3. “NIS-RL” the Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union, Official Journal No. L 194 of 19.07.2016 p. 1;

4. “Inner Circle of the Operative Coordinating Structure (IKDOK)” an inter-ministerial structure for the coordination on the operational level in the area of security of network and information systems, consisting of representatives of the Federal Chancellor, the Federal Minister for Internal Affairs, the Federal Minister for Defence, and the Federal Minister for Europe, Integration and Foreign Affairs, who are required to undergo a security check for access to classified information before starting to participate;

5. “Operative Coordinating Structure (OpKoord)” a structure for the cooperation at the operational level in the area of security of network and information systems, consisting of the IKDOK and the computer emergency response team (§ 14):

6. “Security incident” a disruption of the availability, integrity, authenticity, or confidentiality of network and information systems which lead to a restriction of the availability or loss of the operational service with significant impact; when assessing the level of significance, the following parameters, in particular, must be taken into consideration. The anticipated

a) number of users affected by the security incident, in particular, of the users who require the service to provide their own services,

b) duration of the security incident,

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

d) the effect on commercial and social activities;

7. “incident” all events which actually have adverse effects on the availability, integrity, authenticity, or confidentiality of network and information systems, and which are not a security incident;

8. “Risk” all circumstances or events, which potentially have adverse effects on the security of network and information systems;

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

10. “Operators of essential services” an institution with an establishment in Austria, which provides an essential service;

11. “Qualified entity” an institution with an establishment in Austria, whose suitability for the review of the security measures of operators of essential services has been determined by the Federal Minister for Internal Affairs pursuant to § 18 (1);

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

13. “Service provider of digital services” a legal entity or registered partnership, which is offering a digital service in Austria and which is not a micro-enterprise or small enterprise within the meaning of Art. 1 and Art. 2 (2) and (3) of the Annex of the Commission Recommendation 2003/361/EC of 6 May 2003 concerning the definition of micro, small, and medium-sized enterprises, Official Journal No. L 124 of 20.05.2003 p. 36, has

a) its headquarters in Austria or

b) no headquarters in the European Union, who has nominated a representative;

14. “Representative” a natural person or legal entity or registered partnership, which has been expressly named to act on behalf of a provider of digital services not registered in the European Union, and which the Federal Chancellor, the Federal Minister for Internal Affairs, or the computer emergency response team can contact instead of the Service Provider of Digital Services, in respect of the obligations of this provider of digital services pursuant to this federal law;

15. “Online marketplace” a digital service which enables consumers or traders to conclude online sales or online service contracts with traders either on the website of the online marketplace or on the trader’s website, which uses computing services provided by the online marketplace;

16. “Online search engine” a digital service which enables users to perform searches of, in principle, all websites or on websites in a specific language on the basis of a query on any subject in the form of a keyword, a group of words or any other input, and which then displays links through which information related to the requested content can be found;

17. “Cloud computing service” a digital service which enables access to a scalable and elastic pool of shared computing resources;

18. “Federal Agencies” the Federal Ministries, the courts of public law, the Court of Auditors, the Ombudsman Board, the Office of the President, and the Parliamentary Directorate; other federal offices may be determined by the competent Federal Minister by way of ordinance;

19. “Public Administrative Agencies” the federal agencies and agencies of those states, which have used the option pursuant to § 22 (5);

20. “Cooperation Group” a committee established in accordance with Art. 11 NIS-RL, which consists of representatives from the Member States of the European Union, the European Commission, and the European Network and Information Security Agency (ENISA) and serves to support and facilitate strategic cooperation and the exchange of information between Member States of the European Union in order to build trust and achieve a high common level of security of network and information systems in the European Union;

21. “CSIRTs Network” a committee established in accordance with Art. 12 NIS-RL, which consists of representatives of the computer emergency response teams of the Member States of the European Union and the European computer emergency response team and which shall contribute to the building of trust between the Member States of the European Union and promote quick and effective operative cooperation;

22. “Cyber crisis” one or several security incidents, which pose a present and imminent threat to the maintenance of important societal functions, and which may have serious effects on the health, the security, or the economic and social welfare of large parts of the population or the effective functioning of state agencies;

23. “Cyber crisis management” a coordination procedure to address cyber crises.

2. Section

Competences and Coordination Structures

Functions of the Federal Chancellor

§ 4. (1) The following strategic functions are conferred to the Federal Chancellor:

1. Coordination of the establishment of a strategy (§ 8) and an annual report on the security of network and information systems;

2. Representing Austria in the Cooperation Group as well as in other EU-wide and international committees for the security of network and information systems that have been assigned strategic functions; the competences of other departments shall remain unaffected by this;

3. Coordination of the public-private cooperation in the area of the security of network and information systems;

4. Operation of the GovCERT pursuant to § 14 (4);

5. Informing the public of a security incident, which affects several sectors specified in § 2;

6. Determination of operators of essential services pursuant to § 16 (1), as well as the creation and regular updating of a list of essential services;

7. Consultation with the competent authorities of other Member States, when providers of digital services have their main establishment in Austria, but their network and information systems are located in another Member State;

8. Determination of the suitability and authorisation of computer emergency response teams pursuant to § 15 (3);
9. Publication and updating of a list of the computer emergency response teams pursuant to § 14 (1) and (4) in appropriate format.

(2) The Federal Chancellor may determine the following in agreement with the Federal Minister for Internal Affairs by way of ordinance:

1. Criteria for the parameters of § 3 no. 6 (a) to (d):

2. Detailed rules on each of the sectors specified in § 2, pursuant to § 16 (2);

3. Security measures according to § 17 (1).

4. Exceptions of obligations for operators of essential services pursuant to § 20 (1).

(3) The Federal Chancellor determines the division of the responsibilities as joint controllers under data protection law in agreement with the Federal Minister for Internal Affairs and the Federal Minister for Defence by way of ordinance pursuant to § 11 (3).

Functions of the Federal Minister for Internal Affairs

§ 5. (1) The following operational central functions are conferred to the Federal Minister for Internal Affairs:

1. Operation of a central point of contact (SPOC) for the security of network and information systems (§ 6);

2. Organisational management of the coordination structures IKDOK and OpKoord (§ 7);

3. Receipt and analysis of reports on risks, incidents, or security incidents, regular compilation of a situation report regarding these and forwarding reports as well as the situation report and additional relevant information to domestic authorities or offices according to the 3. section;

4. Compilation and forwarding of relevant information on the prevention of security incidents to ensure the security of network and information systems;

5. Checking the security measures (§ 17 and 21) and compliance with the reporting obligations (§§ 19 and 21);

6. Determination and auditing the qualified entities (§ 18);

7. Informing the public of individual security incidents (§ 10 (1));

8. Management and coordination of cyber crisis management at operational level (6. section).

(2) The Federal Minister for Internal Affairs determines by way of ordinance, in agreement with the Federal Chancellor, the requirements a qualified entity has to meet, or special criteria according to which an agency will be deemed to be a qualified entity in any case as well as the procedure to determine Qualified Entities.

Central Point of Contact

§ 6. (1) For the security of network and information systems, a competent central point of contact (SPOK) is set up at the Federal Minister for Internal Affairs, exercising an operative liaison function to ensure cross-border cooperation with the competent agencies in other Member States of the European Union as well as the Cooperation Group and the CSIRTs network.

(2) The central point of contact

1. Forwards incoming reports and enquiries directly to the members of IKDOK and the computer emergency response team (§ 14) insofar as this is necessary for the fulfilment of task legally assigned to the respective member of IKDOK or the computer emergency response team, and

2. Informs the central points of contact in other Member States upon request, if a security incident affects one or several other Member States of the European Union (§§ 19 (5), 21 (3), and 22 (4).

Coordination Structures

§ 7. (1) IKDOK is set up to discuss and update the situation report compiled by the Federal Minister for Internal Affairs on risks, incidents, and security incidents, to discuss the findings obtained pursuant to § 13 (1) and (2), and to support the Coordination Committee in Cyber Crisis Management. The latter also serves to exchange classified information between the participants in order to perform the tasks in accordance with their competences.

(2) An OpKoord is set up to discuss an overall situation report which also contains voluntary reports. The OpKoord may be extended to include representatives of operators of essential services, providers of digital services, as well as public administrative agencies, if their sphere of action is affected by a risk, incident, or security incident. Participants of OpKoord are bound to secrecy with regard to the information of which they become aware as a result of their participation in accordance with the more detailed regulations pursuant to para. 3.

(3) The Federal Minister for Internal Affairs may pass rules of procedure containing more detailed provisions on the cooperation of the coordination structures pursuant to para. 1 and 2, in particular, on convening of meetings, the composition as well as their decision-making.

(4) The agencies participating in the OpKoord may process and transfer to each other the personal data required for the purpose of the organisation of the OpKoord and for the performance of the tasks pursuant to para. 1 and 2.

Strategy for the Security of Network and Information Systems

§ 8. (1) The strategy for the security of network and information systems determines, in particular, the strategic goals and appropriate policy and regulatory measures, with which a high level of security of network and information systems is to be achieved and maintained in the federal territory.

(2) The Federal Chancellor informs the European Commission of the strategy for the security of network and information systems within three months after it has been determined. Elements of the strategy, which affect national security, are not to be disclosed.

3. Section

Powers and Data Processing

Data Processing

§ 9. (1) The Federal Chancellor, the Federal Minister for Internal Affairs, the Federal Minister for Defence, the Federal Minister for Europe, Integration and Foreign Affairs, and the computer emergency response team pursuant to § 14 (1) are entitled, in order to guarantee a high level of security of network and information systems when performing their tasks under this federal law and to the protection against and the defence against danger to public safety, to process and transmit to each other and to the members of OpKoord the necessary personal data within the meaning of Art. 4 no. 2s of the 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 No. L 119 of 04.05.2016, p. 1, in the corrected version, OJ No. L 314 of 22.11.2016, p. 72, and § 36 of the Federal Law on the Protection of Natural Persons during the Processing of Personal Data (Data Protection Act - DPA), Federal Law Gazette Volume I No. 165/1999.

(2) These are the following personal data:

1. Of participants and their organisational units, which are necessary for the facilitation and during the participation in the coordination structures for organisational purposes;

2. By persons who are connected to risks, incidents, and security incidents, for the purpose of discussing and updating the situation report compiled by the Federal Minister for Internal Affairs, for discussing the findings obtained pursuant to § 13 (1) and (2), and to support the Coordination Committee.

3. By persons involved in a business case or affected by it.

(3) The Federal Chancellor, the Federal Minister for Internal Affairs, and the Federal Minister of Defence are entitled to process and transmit to each other the following personal data beyond the data specified in para. 2, for the purpose of analysis and to address risk, incidents, and security incidents:

1. Contact and identity data as well as technical data of the reporting party and the contact person;

2. Contact and identity data as well as technical data of persons connected to a report on a risk, incident, or security incident such as, in particular, victim and attacker.

(4) The Federal Chancellor and the Federal Minister for Internal Affairs are entitled to process and transmit to each other the following personal data beyond the data specified in para. 2 and 3 for the purpose of performing their tasks, pursuant to §§ 4 and 5:

1. Contact and identity data as well as technical data of operators of essential services, providers of digital services, public administrative agencies, who have taken the option pursuant to § 22 (5), computer emergency response teams as well as by competent authorities of other Member States;

2. Contact and identity data as well as technical data of persons connected to a report on a risk, incident, or security incident such as, in particular, victim and attacker;

3. Contact and identity data of participants and their organisation units, which are necessary for the facilitation and during the participation in Eu-wide, international, and national committees for the security of network and information systems;

(5) The Federal Minister for Internal Affairs is entitled to process the following personal data beyond the data specified in para. 2 to 4, for the purpose of performing his tasks, pursuant to § 5 nos. 4 to 6:

1. Contact and identity dates as well as technical data of qualified entities;

2. Contact and identity data as well as technical data of persons during the course of checking security measures;

3. technical data of persons, which were determined within the scope of § 13.
(6) Any retrieval, transmission, and amendment of personal data must be recorded without there being any possibility of changes being made to it. The records must be retained for three years and subsequently deleted.

(7) The right to erasure and the right to object pursuant to GDPR or § 45 DSG is restricted to the extent that a retention obligation or archiving is provided for by law or regulation, or the erasure is contrary to the public interest of ensuring a high level of network and information system security and the data subject cannot demonstrate grounds arising from his or her particular situation which outweigh the objectives of the restriction of the right. The competent data protection officer must be notified about such consideration and the outcome.

(8) The right to restriction of processing pursuant to Art. 18 GDPR or § 45 DSG is restricted in relation to integrated data processing systems for the duration of a review of the accuracy of the personal data disputed by the data subject, as well as for the period in which the data subject has asserted his or her right to object and it has not yet been established whether the legitimate grounds of the controller under data protection law override those of the data subject.

(9) The obligations under data protection law according to the GDPR and the 3. main part of the DSG must be independently fulfilled by each data controller with regard to those personal data which are processed, transmitted or processed further in connection with the procedure conducted by the controller or the measures placed by the controller.

Data Transfer

§ 10. (1) After hearing an operator of essential services or provider of digital services affected by a security incident, the Federal Chancellor and the Federal Minister for Internal Affairs may within their respective spheres of activity publish personal data in accordance with § 9 (3) no. 2 after weighing up the interests with regard to the effects on the data subjects under data protection law, in order to inform the public about security incidents, provided that raising public awareness is necessary to prevent or tackle security incidents, or the disclosure of the security incident is otherwise in the public interest. The Federal Minister for Internal Affairs may request providers of digital services to notify the public themselves.

(2) Data which is known to the Federal Chancellor, the Federal Minister for Internal Affairs, the Federal Minister for Defence, and the Federal Minister for Europe, Integration and Foreign Affairs due to the performance of their duties under this federal law, may be transferred to military bodies and authorities for purposes of military defence pursuant to Art. 79 (1) B-VG, to security agencies for the purposes of the security police and criminal justice, to public prosecutors and ordinary courts for the purposes of criminal justice as well as to domestic authorities, insofar as this is an essential prerequisite for the performance of a task assigned to them by law.

(3) In order to carry out the functions pursuant to § 5 no. 4, the Federal Minister for Internal Affairs may transfer data pursuant to § 9 2 no. 2 and 3 NO. 2 to operators of essential services, providers of digital services, as well as public administrative agencies, who are not operators of essential services or service providers of digital services, if these are affected by a risk, incident, or security incident.

(4) The Federal Chancellor is authorised to transfer data pursuant to § 9 (2) to (5) to foreign security authorities and security organisations pursuant to § 2 (2) and (3) of the Federal Law on the international police cooperation (Police Cooperation Act -PolKG), Federal Law Gazette Volume I No. 104/1997, as well as to institutions of the European Union or the United Nations in accordance with the provisions on the international administrative police cooperation.

(5) The Federal Minister for Internal Affairs is authorised to transfer personal data of persons connected to a security incident to the central point of contact in the member state affected by the security incident, in order to carry out his functions pursuant to §§ 19 (5), 21 (3), and 22 (4), after weighing up the interests with regard to the economic interests of the agency affected as well as the confidentiality of the information provided in the report.

(6) The Federal Chancellor is authorised to transfer personal contact and identity data of operators of essential services and providers of digital services to computer emergency response teams to carry out their functions in accordance with § 14 (2).

(7) The Federal Chancellor is authorised to transfer identity data of operators of essential services to those countries in whose territory the main establishment of the operator is located, as well as to the supervisory authorities of the respective sector in which the essential service is provided, insofar as this is necessary to carry out their tasks.

NIS Reporting Analysis System

§ 11. (1) For the analysis of reports on risks, incidents, and security incidents (§§ 19, 20 (2), 21 (2), 22 (2) and (3) as well as 23 (1) and (2)) as well as of findings, which have been obtained pursuant to § 13 (1) and (2), the Federal Minister for Internal Affairs must operate ICT solutions and provide these to the Federal Chancellor and the Federal Minister for Defence, to support the assessment of risks, incidents, and security incidents in relation to network and information systems and the compilation of a situation report by means of strategic or operative analysis.

(2) In respect of the ICT solutions and IT procedures of para. 1, the Federal Minister for Internal Affairs, the Federal Chancellor, and the Federal Minister for Defence are jointly the controllers under data protection law pursuant to Art. 4 no. 7 in conjunction with Art. 26 GDPR or § 36 DSG.

(3) The division of the obligations as joint controllers under data protection law is made by way of ordinance by the Federal Chancellor, in agreement with the Federal Minister for Internal Affairs and the Federal Minister for Defence.

IKDOK Platform

§ 12. (1) The Federal Minister for Internal Affairs may operate an ICT solution for the organisation of IKDOK and to perform his tasks pursuant to § 7 (1). In the event such solution is operated, it must be made available to the Federal Chancellor, the Federal Minister for Defence, and the Federal Minister for Europe, Integration and Foreign Affairs.

(2) In respect of the ICT solutions of para. 1, the Federal Minister for Internal Affairs, the Federal Chancellor, the Federal Minister for Defence, and the Federal Minister for Europe, Integration and Foreign Affairs are joint controllers under data protection law pursuant to Art. 4 no. 7 in conjunction with Art. 26 GDPR or § 47 DSG. Unless otherwise regulated in the following paragraphs, the obligations arising from GDPR are to be performed by the Federal Minister for Internal Affairs.

(3) If a data subject is asserting its rights in accordance with the provisions of Chapter 3 GDPR or §§ 42 to 45 DSG, the joint controllers under data protection law must inform each other of this without delay. Each of the joint controllers under data protection law shall, in respect of the data it collects and processes, independently perform the duties relating to the rights of data subjects.

Operation of ICT Solutions to Prevent Security incidents

§ 13. (1) For the purpose of carrying out the function pursuant to § 5 no. 4, the Federal Minister for Internal Affairs is authorised to operate ICT solutions, which identify risks or incidents in respect of network and information systems, at an early stage. Operators of essential services, providers of digital services, as well as public administrative agencies may participate in the ICT solutions operated by the Federal Minister for Internal Affairs and determine which data are transferred to the Federal Minister for Internal Affairs. For the participation in ICT solutions, the Federal Government shall be entitled to a lump sum as compensation, which shall be determined by way of a regulation issued by the Federal Minister of the Interior in accordance with the average costs.

(2) In order to fulfil the function pursuant to § 5 no. 4, the Federal Minister of Internal Affairs is authorised to operate ICT solutions or to use them after obtaining the consent of the affected institution in order to detect patterns of attacks on network and information systems. Likewise, the GovCERT is authorised to operate such ICT solutions for the purpose of carrying out the duties pursuant to § 14 (2 no. 3) and (5) and may process the personal technical data generated from this as controller under data protection law pursuant to Art. 4 no. 7 GDPR or § 36 (2 no. 8) DSG.

4. Section

Computer Emergency response Team

Functions and Purpose of the Computer Emergency Response Team

§ 14. (1) Computer emergency response teams are set up to ensure the security of network and information systems. For this purpose, the domestic computer emergency response team and sector-specific computer emergency response teams of operators of essential services and of providers of digital services as well as the computer emergency response team of the public administration (GovCERT) are supporting the public administration agencies when addressing risks, incidents, and security incidents.

(2) Pursuant to para. 1, computer emergency response teams have, in any event, the following functions:

1. Receipt of reports on risks, incidents, or security incidents pursuant to §§ 19, 21 (2), and 23 (1) and (2);

2. Forwarding reports (no. 1) to the Federal Minister of Internal Affairs;

3. Issue of early alerts, alarm messages, and recommendations for action as well as publication and dissemination of information on risks, incidents, or security incidents;

4. First general technical support during the response to a security incident;

5. Monitoring and analysis of risks, incidents, or security incidents as well as evaluation of the situation;

6. Participation in the coordination structures pursuant to § 7 and involvement in CSIRTs network.

(3) Operators of essential services may set up a sector-specific computer emergency response team for their sector (§ 2), which carries out the functions pursuant to para. 2 with respect to the operators of essential services which it supports. Sector-specific computer emergency response teams may, on behalf of an operator of essential services, analyse data pursuant to § 13 (1), sentence two, for the purposes of para. 2 no. 3 and 5, where such data has been obtained through an ICT solution set up at this operator of essential services pursuant to § 13 (1), sentence 1. For providers of digital services this applies providing that they may instruct the domestic computer emergency response team for this purpose.

(4) The computer emergency response team for the public administration (GovCERT) has been set up at the Federal Chancellor. Apart from the receipt and forwarding of reports in accordance with § 22 (2) and (3), if necessary, in accordance with §§ 19 (2), 21 (2), and 23 (3), the functions pursuant to § 2 no. 3 to 5 and § 3, second sentence with regard to the public administrative agencies fall to GovCERT, provided that it is not an agency represented in IKDOK.

(5) The GovCERT, the national computer emergency response team and the sector-specific computer emergency response teams shall notify the Federal Chancellor as well as the Federal Minister for Internal Affairs without undue delay about activities of the CSIRTs network, which are required under this federal law, and may attend its meetings.

(6) Computer emergency response teams may perform the functions pursuant to para. 2 no. 3 to 5 also in respect of other agencies or persons, provided that these are concerned by a risk or an incident affecting their network and information systems.

(7) As joint controllers under data protection law, computer emergency response teams are authorised pursuant to Art. 4 no. 7 GDPR to process personal data in accordance with § 9 (2) to (4), insofar as this is necessary to carry out the functions in accordance with § 2.

(8) Computer emergency response teams are authorised, in order to perform their functions pursuant to para. 2 no. 3, 5 and 6, to transfer personal data pursuant to § 9, para 2 no. 2 and para. 3 no. 2 to operators of essential services, Providers of Digital Services, Public Administrative Agencies, agencies, who have made reports pursuant to § 23 (2), and to participants of the CSIRTs network as well as to each other.

Requirements and Suitability of a Computer Emergency Response Team

§ 15. (1) Computer emergency response teams pursuant to § 14 (1) shall, in any event, meet the following requirements:

1. Their premises and supporting network and information systems correspond to the standards specified in Art. 32 GDPR and are set up at secure locations.

2. Its business continuity shall be ensured, in particular, by

a) the use of an appropriate system for the administration and referral of enquiries and

b) sufficient human resources and technical and infrastructural equipment which ensures permanent readiness and availability.

3. Evidence of the support to operators of essential services, where a computer emergency response team pursuant to § 14 (1) sentence two, is concerned.

4. The personnel to be involved in carrying out the functions according to § 14 (2) shall be professionally competent and must undergo a security check pursuant to §§ 55 et seqq. of the Security Police Law (SPG), Federal Law Gazette No. 566/1991, for access to classified information. The security check must be repeated every five years. To carry out the security check, the requesting party must pay a flat fee in the amount as specified in § 5 of the Security Fee Regulation (SGV), Federal Law Gazette No. 389/1996.

5. When carrying out their tasks pursuant to § 14 (2 no. 1 and 2), they must use secure communication channels which they have agreed upon with the Federal Minister for Internal Affairs in advance.

(2) The GovCERT must meet the requirement pursuant to para. 1 except no. 3.

(3) The Federal Chancellor must establish, in agreement with the Federal Minister for Internal Affairs, that the national computer emergency response team as well as upon request a sector-specific computer

emergency response team meets the requirements according to para. 1 and is suitable for performing the tasks in accordance with § 14 (2). If a computer emergency response team is a private entity, it must be authorised by the Federal Chancellor in agreement with the Federal Minister for Internal Affairs to carry out the functions pursuant to § 14, para. 2 no. 1 and 2. Computer emergency response teams shall notify the Federal Chancellor without delay of any changes with regard to those circumstances which were a prerequisite to establish the suitability or for granting the authorisation. The authorisation must be withdrawn fully or only with regard to the performance of individual tasks, if conditions that are essential for granting the authorisation are no longer met.

(4) The personal contact and identity data of the computer emergency response teams are to be published by the Federal Chancellor in an appropriate format.

5. Section

Responsibilities for Operators of Essential Services, Providers of Digital Services as well as Public Administrative Agencies

Determination of Operators of Essential Services

§ 16. (1) After referral to the Federal Minister for Internal Affairs and the competent Federal Minister, the Federal Chancellor identifies for each of the sectors listed in § 2 the operators of essential services with an establishment in Austria, which are providing an essential service.

(2) The Federal Chancellor may determine, with the agreement of the Federal Minister for Internal Affairs, more detailed rules on the sectors listed in § 2, by issuing an ordinance. This ordinance may contain, in particular, partial sectors, areas, the associated essential services, as well as types of entities that can be considered as operators of essential services. When assessing whether a service is of essential importance, the following factors must be taken into account:

1. Number of users that are utilising the service offered by the respective operator of an essential service;

2. Dependence of other sectors listed in § 2 on the service offered by this operator;

3. Market share of the operator of essential services;

4. Geographical spread of the area which may be affected by a security incident;

5. Effects of security incidents with regard to extent and duration on economic or social activities or public safety;

6. Significance of the operator of essential services on the continuity of the service to a sufficient extent, taking into account the availability of alternative means for the provision of the respective service.

In addition, sector-specific factors are also to be considered, if necessary.

(3) Operators of essential services must inform the Federal Chancellor within two weeks of receipt of the notice pursuant to para. 4 no. 1 about a point of contact for communications with the Federal Chancellor, the Federal Minister for Internal Affairs, or the computer emergency response team. The operator of essential services must ensure that it can, in any event, be reached via this point of contact during the time period in which it provides an essential service pursuant to para. 2. It must announce any changes of the point of contact without undue delay.

(4) For the purposes of para. 1, the Federal Chancellor performs the following functions:

1. Issue of a decision by which an operator of essential services pursuant to para. 1 is determined. If the prerequisites for the decision establishing that a certain entity is an operator of essential services subsequently cease to exist or if it turns out that they did not exist in the first place, this shall also be determined by a decision;

2. Initiation of consultations with other Member States of the European Union, if an operator of essential services is offering a service pursuant to para. 2 also in another or several Member States of the European Union. The decision whether an operator of essential services pursuant to para. 1 can be established can only be made after consultation with this or other Member State(s) of the European Union;

3. Compilation and continuous updating of a list of essential services;

4. Transmission of the list (no. 3) to the European Commission at least every two years.

Security Measures for Operators of Essential Services

§ 17. (1) To ensure the NIS, operators of essential services must take appropriate and proportionate technical and organisational security measures with regard to the network and information systems they are using for the provision of the essential service. These must take into account the state of the art and be appropriate to the risk that can be determined with reasonable effort.

(2) Together with their sectoral associations, the operators of essential services may propose sector-specific security measures to ensure the requirements set forth in para. 1 are met. The Federal Minister for Internal Affairs determines upon request whether these are appropriate to meet the requirements of para. 1.

(3) The operators of essential services must provide evidence to the Federal Minister for Internal Affairs at least every three years after receipt of the decision pursuant to § 16 (4) no. 1 to show that the requirements under para. 1 are met. For this purpose, they shall transmit a list of the security measures in place by proof of certification or completed audits by qualified entities to the Federal Minister of Internal, including the security defects revealed in the process.

(4) The Federal Minister for Interior Affairs may inspect the network and information systems, which are used for the provision of the essential services, and documents in respect of these, in order to monitor compliance with the requirements pursuant to para. 1. For the purpose of the inspection, the Federal Minister for Interior Affairs is authorised to enter the sites in which network and information systems are located, after prior agreement. Inspections are to conducted to the extent absolutely necessary and with the greatest possible protection of the rights of the entity concerned and of third parties as well as of operation.

(5) The Federal Minister of Interior Affairs is authorised to make recommendations for the fulfilment of the requirements according to para. 1, and, if necessary, to set an appropriate deadline for compliance and corresponding evidence, failing which compliance shall be ordered by way of official decision.

Qualified Entities

§ 18. (1) The Federal Minister of Internal Affairs decides on the existence of a qualified entity upon request.

(2) If the requirements or criteria pursuant to § 5 (2) cease to exist, the qualified entity is informed of the fact that it must meet the requirements or criteria within a reasonable time period. In case of failure to

meet the requirements or criteria, the Federal Minister for Internal Affairs revokes the notice issued pursuant to para. 1.

(3) To monitor compliance with the requirements and criteria for qualified entities pursuant to § 5 (2), the Federal Minister for Internal Affairs may inspect their network and information systems and documents relating to these. The second and third sentence of § 17 (4) applies.

(4) A list of qualified entities and their area of responsibilities is maintained by the Federal Minister of Internal affairs and operators of essential services are granted access to it.

Reporting Obligation for Operators of Essential Services

§ 19. (1) Operators of essential services must report without undue delay a security incident which concerns an essential service provided by them to the competent computer emergency response team, which forwards the report immediately to the Federal Minister for Internal Affairs.

(2) Competent for the receipt of the report pursuant to para. 1 is the sector-specific computer emergency response team (§ 14 (1) sentence two), if such has been set up and the affected operator of essential services supports this (§ 15 para. 1 no. 3), otherwise the national computer emergency response team, if such has been set up, otherwise the GovCERT.

(3) The report must contain all relevant information on the security incident and the technical framework conditions, which are known at the time of the initial report, in particular, the suspected or actual cause, the information technology affected and the type of the entity or facility affected. Information about circumstances of the security incident that become known subsequently must be communicated in follow-up reports and ultimately in a final report without any unreasonable further delay. The report must be transmitted in a standardised electronic format.

(4) If an operator of essential services utilises the services of a provider of digital services, every significant impact on the availability of the essential services due to a security incident affecting the provider of digital services, must be reported by this operator of essential services.

(5) If a security incident affecting an operator of essential services affects one or several other Member States of the European Union, the Federal Minister for Internal Affairs or the competent computer emergency response team must communicate this to the central point of contact in these Member States, via the central point of contact (SPOC).

Exceptions of Obligations for Operators of Essential Services

§ 20. (1) §§ 17 or 19 do not apply if for the provision of an essential service there are regulations on security measures or reporting obligations in EU law or special administrative laws based on provisions of EU law, which ensure at least an equivalent level of security for network and information systems, and the Federal Chancellor determines these regulations and their suitability by means of an ordinance in agreement with the Federal Minister for Internal Affairs.

(2) The Financial Markets Authority must communicate reports of serious operational or security incidents pursuant to § 86 (1) of the Payment Services Act 2018 (ZaDiG 2018), Federal Law Gazette Volume I No. 17/2018, affecting payment service providers, which have been identified as operators of essential services, to the Federal Minister for Internal Affairs without delay.

Security Measures and Reporting Obligations for Service Providers of Digital Services

§ 21. (1) To ensure the NIS, providers of digital services must take appropriate and proportionate technical and organisational security measures with regard to the network and information systems they are using for the provision of the digital service. These shall ensure a level of security of the network and information systems that is appropriate to the existing risk that can be determined with reasonable effort, taking into account the state of the art as well as the following:

a) Security of systems and facilities,

b) Handling of security incidents,

c) Business continuity management,

d) Monitoring, auditing, and testing,

e) Compliance with international standards.

(2) Providers of digital services must report a security incident regarding a digital service provided by them to the national computer emergency response team without delay, provided that such has been set up, otherwise to the GovCERT, which shall forward the report immediately to the Federal Minister for Internal Affairs. The reporting obligation in respect of a security incident only applies if the provider of digital services has access to information that is required to assess the effect of a security incident. § 19 (3) applies correspondingly.

(3) If a security incident affecting a provider of digital services affects one or several other Members States of the European Union, the Federal Minister for Internal Affairs or the competent computer emergency response team pursuant to para. 2 must notify the central point of contact in these Member States via the central point of contact (SPOC).

(4) The Federal Minister for Internal Affairs is authorised, if he becomes aware of demonstrable circumstances that a provider of digital services is not complying with its obligations under para 1, to demand that this provider provides evidence of appropriate security measures. For this purpose, the affected provider of digital services provides a list of the existing security measures. The Federal Minister for Interior Affairs may, for this purpose, also inspect the network and information systems, which are used for the provision of the digital service, and inspect documents in respect of these. § 17 (4) sentence two and three applies. For fulfilment of the requirements set in para. 1, the Federal Minister of Interior Affairs is authorised to make recommendations, if necessary, to set an appropriate deadline for compliance with the recommendations and proof of respective compliance, otherwise compliance shall be ordered by way of official decision.

Security Measures and Reporting Obligations for Public Administrative Agencies

§ 22. (1) To ensure the NIS, federal agencies must take appropriate and proportionate technical and organisational security measures with regard to the network and information systems they are using for the provision of essential services. These must take into account the state of the art and be appropriate to the risk that can be determined with reasonable effort.
(2) A federal agency, unless it is an agency represented in IKDOK, shall immediately report a security incident affecting an essential service it provides, to GovCERT, which shall forward the report to the Federal Minister of Internal Affairs without delay. § 19 (3) applies correspondingly. In the event of security incidents in respect of an agency represented in IKDOK, the report is made within IKDOK.

(3) Risks and incidents may be reported to GovCERT by public administrative agencies, GovCERT shall forward the reports in summarised version to the Federal Minister for Internal Affairs. § 23 (4) and (5)

applies correspondingly. In the event of risks and incidents in respect of an agency represented in IKDOK, the report is made voluntarily within IKDOK.

(4) If a security incident affecting a public administrative agency affects one or several other Member States of the European Union, the Federal Minister for Internal Affairs or GovCERT must communicate this to the central point of contact in these Member States, via the central point of contact (SPOC).

(5) A country may by way of state law declare the obligations pursuant to para. 1 and 2 applicable also with regard to the essential services provided by its agencies. These agencies of the States are the offices of the provincial governments and other offices of the countries and communities, which if necessary are declared as such by the respective eligible bodies of the country.

(6) A country must notify the Federal Chancellor in writing of the issue of a state law pursuant to para. 5 as well as of any repeal. If a country uses the option pursuant to para. 5, the provisions for the Federal Agencies shall apply also to agencies of the country.

Voluntary Reports

§ 23. (1) Risks and incidents may be reported by operators of essential services or providers of digital services to the computer emergency response team which is also competent in the case of a reporting obligation, that then forwards summarised reports to the Federal Minister of Internal Affairs.

(2) Risks, incidents, and security incidents affecting entities which have not been determined as operators of essential services, and which are not providers of digital services, or public administrative agencies, can be reported to these to the competent computer emergency response team, which forwards summarised reports to the Federal Minister for Internal Affairs.

(3) Responsible for the receipt of voluntary reports pursuant to para. 2 is the sector-specific computer emergency response team, if such has been set up and the reporting entity supports this, otherwise the national computer emergency response team, if such has been set up, otherwise the GovCERT.

(4) The voluntary report does not have to contain the identity of the entity nor information indicating the identity of the entity. § 19 (3) applies correspondingly.

(5) To contribute to ensuring a high level of security for network and information systems, the voluntarily reporting entity pursuant to para. 1 and 2 may transfer personal data pursuant to § 9 para. 3 no. 2 to the competent computer emergency response team.

6. Section

Structures and Responsibilities in Case of a Cyber Crisis

Cyber Crisis

§ 24. The decision on the existence of a cyber crisis is made by the Federal Minister for Internal Affairs.

Coordination Committee

§ 25. (1) A Coordination Committee is set up for advising the Federal Minister for Internal Affairs in relation to the decision whether there is a cyber crisis and the operational measures to address a cyber crisis as well as the Federal Government in coordinating public relations work.

(2) The Coordination Committee is managed by the Director-General for Public Safety and consists of the Chief of General Staff, the Secretary-General of the Federal Chancellor's office, and the Secretary-General for Foreign Affairs. The committee shall be extended to include additional representatives of governmental or state authorities, operators of essential services and computer emergency response teams as well as emergency response organisations, if this is necessary to address the cyber crisis.

(3) IKDOK supports the Coordination Committee by compiling specific situation reports and its technical expertise.

7. Section

Penalty Clauses

Administrative Penalty Clauses

§ 26. (1) An administrative offence is being committed by anyone who

1. does not name a point of contact pursuant to § 16 (3), sentence one, does not announce any amendments pursuant to § 16 (3), sentence three or in accordance with this, is not contactable in the time period specified in § 16 (3), sentence two;

2. does not provide the evidence pursuant to § 17 (3), sentence one, or § 21 (4), sentence one;

3. does not permit inspection pursuant to § 17 (4) or § 21 (4), sentence three;

4. fails to implement the orders issued in accordance with a decision pursuant to § 17 (5) or § 21 (4), last sentence, in good time or

5. does not comply with the reporting obligation pursuant to § 19 (1) in conjunction with para. 3 and 4 or § 21 (2).

The offence is subject to a penalty of up to 50,000 euros, in case of recurrence up to 100,000 euros.

(2) The regional administrative authorities are competent in these matters. The local jurisdiction for administrative offences pursuant to para. 1 is determined by the head office of the operators of essential services or the Provider of Digital Services, in the absence of such in Austria, by the registered office of the representative.

(3) An administrative offence pursuant to para. 1 has not been committed if the act constitutes an offence falling within the jurisdiction of the ordinary courts or is punishable by a more severe penalty under other administrative penal provisions.

(4) The regional administrative authority may impose fines on a legal entity or registered partnership, if administrative offences pursuant to para. 1 have been committed by persons, who have acted either alone or as a part of a body of the legal entity or the registered partnership and hold a managerial position due to

1. the authority to represent the legal entity or the registered partnership,

2. the authority to make decisions on behalf of the legal entity or the registered partnership, or

3. a monitoring authority within the legal entity or the registered partnership.

(5) Legal entities or registered partnerships may also be held responsible for administrative offences pursuant to para. 1 if lack of supervision or control by a person referred to in para. 4 has enabled the

commission of such offences by a person acting on behalf of the legal entity or the registered partnership, provided that the act does not constitute an offence within the jurisdiction of the courts.

(6) Punishment of a responsible party pursuant to § 9 Administrative Penal Act 1991 (VStG), Federal Law Gazette No. 52/1991, may be waived if an administrative penalty is already being issued against the legal entity for the same offence.

8. Section

Final Provisions

Terms Referring to Persons

§ 27. All personal terms used in this Federal Law apply equally to all genders.

Reference to Guidelines

§ 28. With this Federal Law, the Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union, Official Journal No. L 194 of 19.07.2016 P. 1, has been implemented.

References

§ 29. References in this Federal Law to other federal laws shall be understood as references to the respective amended version.

Execution

§ 30. The Federal Chancellor, the Federal Minister of Internal Affairs, the Federal Minister of Defence and the Federal Minister for Europe, Integration and Foreign Affairs shall be entrusted with the implementation of this Federal Law within their spheres of activity, insofar as this is not the responsibility of the Federal Government.

Entry into Force

§ 31. (1) Constitutional provision) § 1 as it appears in the Federal Law Gazette Volume I No. 111/2018 enters into force at the end of the day on which this Federal Act is promulgated.

(2) §§ 2 to 30 in the version Federal Law Gazette Volume I No. 111/2018 enter into force at the end of the day on which this Federal Act is promulgated.

(3) Ordinances based on this Federal Act may come into force at the earliest when this Federal Act enters into force.