COLLECTION OF LAWS

SLOVAK REPUBLIC

Year 2024

Announced: 19. 12. 2024 Time version of the regulation effective from: 1. 1. 2025

The content of the document is legally binding.

366

ACT of 28

November 2024, amending

and supplementing Act No. 69/2018 Coll. on cybersecurity and amending and supplementing certain acts, as amended by later regulations, and amending and supplementing certain acts

The National Council of the Slovak Republic has adopted this law:

Article I

Act No. 69/2018 Coll. on Cybersecurity and on Amendments to Certain Acts, as amended by Act No. 373/2018 Coll., Act No. 134/2020 Coll., Act No. 287/2021 Coll., Act No. 55/2022 Coll. and Act No. 231/2022 Coll., is amended as follows:

1. Sections 1 and 2, including the headings, shall read as follows:

"§ 1
Subject of the law

This law regulates

a) conditions for managing and ensuring cybersecurity, in particular

1. the status and obligations of the operator of the essential service,
2. safety measures,
3. reporting a cyber security incident, a significant cyber threat, an event averted at the last moment and vulnerability,
4. addressing a cyber security incident,
5. measures against ICT products, ICT services or ICT processes threatening cybersecurity and against harmful content,

b) management in the field of cybersecurity, in particular

1. the organization, competence and obligations of public authorities in the field of cyber security security,
2. the tasks and scope of the national cybersecurity certification authority,
3. national cybersecurity strategy,
4. National plan for response to large-scale cyber security incidents and cyber crises,
5. unified cybersecurity information system,
6. cooperation and exchange of information,

c) the organization and scope of cyber security incident response units (hereinafter referred to as the "CSIRT unit") and their accreditation,

d) cybersecurity audit and supervision of the fulfilment of the obligations of the operator of the essential service under this Act or obligations imposed on the basis of this Act (hereinafter referred to as "supervision").".

§ 2
Scope of the law

(1) This Act applies to information systems established and operated under the jurisdiction of the Ministry of Defence of the Slovak Republic to the extent determined by the central authority in the manner pursuant to Section 33(5).

(2) If it is a person who provides a DNS service, a domain name registration service, a cloud computing service, a data center service, a content delivery network, a managed service, a security service, an online marketplace service, an Internet search engine service or a social network service platform, it may be entered in the register of operators of essential services and this Act shall apply to it even if it does not have a permanent residence, place of business or registered office in the territory of the Slovak Republic,

a) has a permanent residence, place of business or registered office in a Member State of the European Union or a state that is a contracting party to the Agreement on the European Economic Area (hereinafter referred to as "Member State of the European Union") and in the territory of the Slovak Republic

1. most often makes decisions regarding security measures to manage risks,

2. implements measures to maintain cybersecurity if it cannot be determined permanent residence, place of business or registered office pursuant to letter a),

3. has the establishment with the highest number of employees among establishments located in the Member States of the European Union,

b) does not have a permanent residence, place of business or registered office in a Member State of the European Union and

1. its representative has a permanent residence, place of business or registered office in the territory of the Slovak Republic pursuant to Section 21(1),

2. it is subject to the obligation pursuant to Section 21(1), but does not have a designated representative with a permanent residence, place of business or registered office in the Slovak Republic or in another Member State of the European Union pursuant to Section 21(1).

(3) This Act does not apply to:

a) requirements for securing networks and information systems according to the general regulation on the protection of classified information,

b) specific provisions on the tasks and powers of the intelligence service in protecting cyberspace according to a special regulation,1)

c) provisions of special regulations on the investigation, detection and prosecution of criminal offences,2)

d) requirements for the security of networks and information systems in the banking, finance or financial system sector pursuant to a separate regulation,3) including standards and principles issued or adopted by the European Central Bank, the European System of Central Banks, the Eurosystem or the European Supervisory Authorities,4) as well as the supervision and control of compliance with these requirements, and also to payment systems and securities clearing and settlement systems and their infrastructures supervised or operated by the European Central Bank or the Eurosystem pursuant to a separate regulation.5)".

The footnotes to references 1 and 3 read:

„1) Section 2, paragraph 1, letter g), paragraph 3 of the Act of the National Council of the Slovak Republic No. 46/1993 Coll. on the Slovak Information Service, as amended by Act No. 151/2010 Coll.
Section 4, paragraph 3, Section 5, paragraph 1, letters c) and h) and Section 7 of Act No. 500/2022 Coll. on Military Intelligence.

Act No. 319/2002 Coll. on the Defence of the Slovak Republic, as amended.
3) Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience of the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011 (OJ L 333, 27.12.2022).".

The footnotes to references 6 and 7 are deleted.

2. In Section 3, letter f) reads:

"f) availability means a guarantee that data or a service provided is accessible to the user, information system, network or device at the time when it is needed and requested,".

3. In Section 3, letter g), the word "information" is replaced by the word "data".

4. In Section 3, letters i) and j) shall read as follows:

"i) risk means the potential for loss or disruption resulting from a cybersecurity incident, expressed as a combination of the extent of such loss or disruption and the probability of the cybersecurity incident occurring;

j) cyber threat means a cyber threat pursuant to Article 2(8) of Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on Information and Communication Technology Cybersecurity Certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (hereinafter referred to as “Regulation (EU) 2019/881”),”.

5. In Section 3, new letters k) and l) are inserted after letter j) to read: "k) significant

cyber threat means a cyber threat that, based on its technical characteristics, can be assumed to have the potential to cause a serious cyber security incident or may have another serious impact on the network and information system of the entity or users of the entity's services by causing significant damage,9)

l) cyber crisis means a period during which there is an imminent threat of a large-scale cyber security incident or a large-scale cyber security incident continues, ".

The footnote to reference 9 reads:

„9) Section 125(1) of the Criminal Code.”.

The previous letters k) to p) are designated as letters m) to r).

6. In Section 3, letters m) to r) shall read as follows:

"m) cyber security incident means an event threatening the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or services provided or accessible through networks and information systems, n) large-scale cyber security incident means a cyber security incident that causes disruption at a level exceeding

the ability of the Slovak Republic to respond to it, or that has a significant impact on at least two Member States of the European Union, o) cyber security incident response means an activity and procedure aimed at preventing, detecting, analysing and mitigating a cyber security incident or at responding to and recovering from it,

p) a last-minute event means an event that could have compromised the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or services provided or accessed through these networks and information systems, but the occurrence of which was successfully prevented or did not occur, q) vulnerability means any undesirable state or error of a technical or software resource, or a deficiency in a process, including

an incorrect security configuration, which can be exploited by a cyber threat, r) ICT product means an ICT product pursuant to Article 2(12) of Regulation (EU) 2019/881.

7. Section 3 is supplemented with letters s) to b), which read as follows:

"s) ICT service means an ICT service pursuant to Article 2(13) of Regulation (EU) 2019/881,

t) ICT process means an ICT process pursuant to Article 2(14) of Regulation (EU) 2019/881,

u) European cybersecurity certificate means a European cybersecurity certificate pursuant to Article 2(11) of Regulation (EU) 2019/881,

(v) TLD administrator means a person to whom a specific top-level domain (TLD) has been assigned and who is responsible for the administration of the TLD, including the registration of domain names within the TLD, and for the technical operation of the TLD, including the operation of name servers, the maintenance of its databases, and the distribution of TLD zone files within the name servers, regardless of whether any of these operations are performed by the person himself or through another person;

w) DNS service means a hierarchical distributed naming system that enables the identification of Internet services and resources and the use of Internet routing and connectivity services by end-user devices to access those services and resources,

x) domain name registration service means a service performed by a registrar or an agent acting on behalf of a registrar, the purpose of which is to create the right to use a second-level domain by the domain holder to the agreed extent, for an agreed period of time and under agreed conditions,

y) a key service is a service for the maintenance of important social areas or economic activities, in which the impact of a cyber security incident in the information system or network on whose functioning the provision of the service depends may cause

1. a threat to the availability, authenticity, integrity or confidentiality of data stored, transmitted or processed or related services provided or accessible through these networks and information systems, affecting more than 25,000 persons,

2. limitation or disruption of a critical entity, its essential service or critical infrastructure,

3. economic loss of more than 0.1% of gross domestic product according to data from the immediately preceding fiscal year, or

4. economic loss or material damage to at least one user more than 250,000 euros,

z) significant impact on public order, security or public health means an impact where the impact of a cyber security incident in an information system or network on whose functioning the provision of a service depends may cause a disruption of public order, security, a threat to public health, an emergency or distress which may

1. require the performance of rescue work or the performance of activities and measures related to with providing assistance in times of need,

2. cause more than 100 injuries requiring medical treatment or the death of at least one person,

aa) significant systemic risk means the risk of a system disruption that may have serious negative consequences or fundamentally hinder the maintenance of cybersecurity, thereby endangering the life or health of persons, the economic functioning of the state, public order, the safety or property of persons, or endangering security interests

Slovak Republic,

and (b) a person who, due to his or her special importance at national or regional level, is a critical person whose disruption due to a cyber security incident may require the performance of rescue work or the performance of activities and measures related to the provision of assistance in distress,".

8. The current text of § 3 is designated as paragraph 1 and is supplemented by paragraph 2, which reads:

"(2) The operator of a basic service is the person who is registered in the register of operators

basic service.".

9. In Section 4, the introductory sentence, the word "implements" is replaced by the word "implements".

10. In Section 4, letter b), the words “and construction” are deleted, after the words “Ministry of the Environment of the Slovak Republic”, the word “and” is replaced by a comma, and after the words “Ministry of Investments, Regional Development and Informatization of the Slovak Republic”, the words “and the Administration of State Material Reserves of the Slovak Republic” are inserted.

11. In Section 5, paragraph 1, letter d), the words “and the national response plan for large-scale cyber security incidents and cyber crises, is the authority for managing cyber crises and performs the role of the national coordinator for managing large-scale cyber security incidents and cyber crises,” are inserted after the words “in the Slovak Republic.”

12. In Section 5(1)(e), a comma and the words “for national cooperation and” are inserted after the words “is the national contact point for cybersecurity” and the words “and the North Atlantic Treaty Organization” are deleted.

13. In Section 5, Paragraph 1, Letters f) and h), the words “and the North Atlantic Treaty Organization” are deleted.

14. In Section 5(1)(i), the words “digital service providers” are replaced by the words "with scientific institutions and academic institutions".

15. In Section 5(1), letters k) and l) read as

follows: “k) acts in the matter of designating an entity as an operator of an essential service and its entry in the register of operators of an essential service, l)

maintains and

administers 1. the register of operators of an essential

service, 2. the list of accredited CSIRT units, 3. the

list of authorised conformity assessment bodies, 4. the list of issued

European cybersecurity certificates, 5. the list of notified bodies accredited within the

scope of the certification scheme
cybersecurity pursuant to Article 49 of Regulation (EU) 2019/881,”.

16. In Section 5, paragraph 1, letter o) reads:

"o) determines the central authority for the sector according to Annex No. 1 or Annex No. 2 in accordance with its areas of competence according to a special regulation10aaa) and performs the tasks of the central authority for the type of entity according to Annex No. 1 and Annex No. 2,".

The footnote to reference 10aaa) reads: " 10aaa) Act

No. 575/2001 Coll., as amended.".

17. In Section 5, paragraph 1, letter r), the words “and declares” are inserted after the word “sends” and the following are added at the end: the words "warnings or declares a state of cyber crisis,".

18. In Section 5, paragraph 1, letter s) reads:

"s) receives national reports on cybersecurity incidents, threats, events at any time
cyber and averted in the last
vulnerabilities,".

19. In Section 5(1)(t), a comma is inserted after the words “on cyber security incidents” and the words "cyber threats and vulnerabilities".

20. In Section 5, paragraph 1, letter u) reads:

"u) carries out supervision,"

21. In Section 5, paragraph 1, letter w), the words "science, research and sports" are replaced by the words "research, development and youth".

22. The footnote to reference 10aa reads:

" 10aa) Articles 58, 60(2) and 61 of Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communication technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (OJ L 111, 21.12.2019, p. 1).

on cybersecurity (OJ L 151, 7.6.2019).".

23. In Section 5, paragraph 1, letter aa) reads:

"aa) carry out control and supervision pursuant to Article 58(7)(a) and (b) of Regulation (EU) 2019/881 and take measures pursuant to Article 58(8)(c) of Regulation (EU) 2019/881,".

24. In Section 5, paragraph 1, letter a) is deleted.

The previous letters ad) to ag) are referred to as letters ac) to af).

25. Section 5a, including the title, reads as follows:

"Section 5a

Cybersecurity Certification System

(1) A cybersecurity certification system is a set of rules and procedures for managing individual cybersecurity certification schemes.

(2) A cybersecurity certification scheme is a set of rules, technical requirements, technical standards and procedures that apply to the certification or conformity assessment of specific ICT products, ICT services or ICT processes.

(3) Cybersecurity certification for assurance levels basic, significant or high according to a special regulation10b) shall be performed only by an accredited person.10c) Only the authority may be an accredited person for cybersecurity certification for assurance level high10d).10e)".

The footnotes to references 10b to 10e read: " 10b) Article 52 of Regulation (EU) 2019/881. 10c) Article 60 of Regulation (EU) 2019/881. Section 19(2) of Act No. 53/2023 Coll. on the accreditation of conformity assessment bodies.

10d) Article 52(7) of Regulation (EU) 2019/881.

10e) Article 56(6) of Regulation (EU) 2019/881.".

The footnotes to references 10f and 10g are deleted.

26. In Section 6, paragraph 1, the words "and digital services" are replaced by the words "or in Annex No. 2". 27. Section 6 is supplemented by paragraphs 5 to 8, which read as follows:

"(5) The Office, through the national CSIRT unit, shall, for the purposes of disclosing vulnerabilities or preventing their misuse, act as a coordinator in matters of communication on detected or reported vulnerabilities between the operator of the essential service, the manufacturer or supplier of the ICT product or ICT service and other affected persons. For the purposes referred to in the first sentence, the Office, through the national CSIRT unit

a) identifies and contacts the persons concerned,

b) communicates the vulnerability with the manufacturer or provider of the ICT product or service ICT,

c) notify the operator of the essential service of the vulnerability that concerns it and recommend measures to prevent its misuse; measures in the area of control and resolution of cyber security incidents are not affected by this,

d) provides assistance to persons reporting vulnerabilities,

(e) manages the disclosure of vulnerabilities.

(6) The Office shall ensure that it is possible to report vulnerabilities also through the unified cybersecurity information system, including anonymous reports, and at the request of the reporter, shall ensure that his anonymity is maintained in relation to the reported facts.

(7) If the vulnerability concerns a service for which a CSIRT unit in another Member State of the European Union provides services, the Authority shall forward the vulnerability notification to that CSIRT unit and inform the notifier thereof.

(8) The Office, through the national CSIRT unit, shall carry out non-invasive detection and assessment of vulnerabilities of publicly accessible networks and information systems in the cyberspace of the Slovak Republic, which shall not have a negative impact on these networks and information systems, nor on the services they provide and the activities they ensure.".

28. Section 7, including the title, reads as follows:

"Section 7

National Cybersecurity Strategy and National Response Plan for Large-Scale Cybersecurity Incidents and Cyber Crises

(1) The National Cybersecurity Strategy is a basic strategic document that comprehensively determines the strategic approach of the Slovak Republic to ensuring a high level of cybersecurity. The National Cybersecurity Strategy includes policies and a national response plan to large-scale cybersecurity incidents and cyber crises, which is a specific plan of partial tasks and resources.

(2) The National Cybersecurity Strategy shall include in particular:

a) objectives and priorities,

b) a governance framework to achieve objectives and

priorities, c) a governance framework to clarify the roles and responsibilities of stakeholders at national level and their list,

d) a mechanism for identifying relevant resources and assessing risks,

e) identification of measures to ensure preparedness and response to and recovery from cyber threats, vulnerabilities and cyber security incidents, including cooperation between the public and private sectors,

f) a framework for enhanced coordination between competent authorities under this Act for the purpose of exchanging information on risks, cyber threats and cyber security incidents,

g) a plan including necessary measures to increase the general level of awareness of citizens of the Slovak Republic on cybersecurity.

(3) Within the framework of the national cybersecurity strategy, policies are adopted, in particular, to ensure

a) cybersecurity in the supply chain of ICT products and ICT services, b) taking into account

cybersecurity requirements for ICT products and ICT services in public procurement, including when it comes to cybersecurity certification, cryptographic measures and the use of open source products,

c) vulnerability management, including supporting and facilitating coordinated disclosure vulnerabilities,

d) maintaining the general availability, integrity and confidentiality of essential communication open internet protocols and infrastructure,

e) supporting the development and integration of advanced technologies with the aim of implementing state-of-the-art risk management measures,

f) support and development of education and training in the field of cybersecurity,

qualifications in the field of cybersecurity, awareness-raising and research and development initiatives in the field of cybersecurity, as well as guidelines on good practices and controls for security education and acquisition of knowledge and skills, aimed at citizens of the Slovak Republic and other interested persons,

g) support for academic institutions and research institutions in the development, improvement and implementation of cybersecurity tools and secure network infrastructure,

h) procedures and appropriate information sharing tools to support the voluntary sharing of cybersecurity information between operators of essential services and other persons, subject to the conditions for sharing,

(i) strengthening cybersecurity and the ability to identify and deter cyberattacks threat and restore the original state after a cybersecurity incident,

j) support for active cyber protection.

(4) The central authority and other state administration bodies shall cooperate with the Office in developing a national cybersecurity strategy and, for this purpose, shall be obliged to provide the Office with information to the necessary extent.

(5) The National Cybersecurity Strategy is approved by the Government of the Slovak Republic on proposal of the Office, for a period of five years.

(6) The National Response Plan for Large-Scale Cybersecurity Incidents and Cyber Crises is a strategic document that determines the objectives and methods of managing large-scale cybersecurity incidents and cyber crises and contains in particular a) objectives, preparation and measures in the

area of preparedness for the emergence of a large-scale cyber security incident; security incident and cyber crisis,

b) the roles of crisis management bodies in managing cyber crises within the scope of their authorisations under special regulations, c)

cyber crisis management procedures, including their integration into crisis management outside wartime and a state of war, and procedures and methods of information exchange,

d) identification of relevant data subjects and the necessary infrastructure and other resources,

(e) measures and tasks to ensure effective participation in, and support for, the coordinated management of large-scale cybersecurity incidents and cyber crises at European Union level.

(7) National plan for response to large-scale cyber security incidents and cyber crisis and its amendment is approved by the Government of the Slovak Republic at the proposal of the Office.

(8) The central authority and other state administration bodies shall cooperate with the Authority in developing a national response plan for large-scale cyber security incidents and cyber crises and shall, for this purpose, provide the Authority with information to the necessary extent.".

29. In Section 8, paragraphs 2 and 3 read as follows:

"(2) The unified cybersecurity information system includes a communication system for reporting and resolving cybersecurity incidents and a central early warning system. The unified information system consists of a public part and a non-public part and access to it is free of charge. The public part of the unified cybersecurity information system includes a) a register of central authorities,

b) register of operators of essential services,

c) list of accredited CSIRTs,

d) methodologies, guidelines, standards, policies and notices, e)

information necessary for the use of the unified cyber security information system security,

f) warnings, cautions and other information intended to minimize, avert or remediation of the consequences of a cyber security incident,

g) a tool for registering changes, reporting changes and other related tools.

(3) The communication system for reporting and resolving cyber security incidents is a communication system that ensures

a) reports pursuant to

Section 24, b) systematic collection, concentration, analysis and evaluation of information about cyber security incidents,

c) communication between the national CSIRT, the government CSIRT and accredited CSIRTs in the Slovak Republic and such CSIRTs in another Member State of the European Union, including the exchange of information and data necessary for effective cooperation in ensuring their tasks in the field of cybersecurity.".

30. In Section 8, paragraph 4 and Section 20, paragraph 5, letter e), the word “threats” is replaced by the words “cybernetic threats".

31. In Section 8(5)(c), the words “and the digital service provider” are deleted.

32. In § 9, paragraphs 1 and 2, § 10a, paragraph 1, § 15, paragraph 1 and § 32, paragraph 2, after the words “according to Annex No. 1” the following shall be inserted: insert the words "or Annex No. 2".

33. In Section 9, paragraph 1, letter e) is deleted.

The previous letters f) and g) are referred to as e) and f).

34. In Section 9(1)(e), the words “basic service and” and the words “list of basic services and” shall be replaced by they release.

35. In Section 10, the words "systems that are not a basic service and the process of resolving cyber security incidents, another state administration body and the central body" are replaced by the words "systems and the process of resolving cyber security incidents, another state administration body".

36. In Section 12(3), the words “and the digital service provider” are deleted.

37. In Section 12(4), the words “or a state of cyber crisis” are inserted after the word “warnings”.

38. In Section 12(5), the words “to the digital service provider” are deleted, and the word “their” is replaced by with the word "his".

39. In Section 15, paragraph 2, letter d), the words “vulnerabilities, cyber threats” are inserted after the word “records”. threats, cyber crises and".

40. In Section 15, paragraph 2 is supplemented with letters h) to l), which read as follows:

"h) providing assistance with network and information system monitoring or carrying out such monitoring in agreement with the network administrator or network operator or information system operator,

i) performing non-invasive vulnerability assessment and assessment of publicly accessible networks and information systems within the scope of the CSIRT unit pursuant to paragraph 1, which does not have a negative impact on these networks and information systems, as well as on the services they provide and the activities they ensure,

j) carrying out an assessment of vulnerabilities identified pursuant to point h), in agreement with the network administrator or network operator or information system operator,

k) cooperation with the national CSIRT unit and other CSIRT units,

l) using suggestions, experience and cooperation with persons active in the field of cybersecurity.".

41. In Section 15, paragraph 4, the words “or the digital service provider” are deleted. 42. Section 15 is supplemented with a paragraph 5, which reads as follows:

"(5) The person performing the tasks of the CSIRT unit may determine the manner, scope and prioritization of means and resources in the provision of preventive services and reactive services through objective criteria based on an analysis of vulnerability risks, cyber threats, cyber crises and cyber security incidents." 43. Section 16 is supplemented by paragraph 4, which reads as follows:

"(4) The person performing the tasks of the CSIRT shall ensure cooperation with the Office, the competent central authority and other CSIRTs, as well as with CSIRTs from other Member States of the European Union and participation in peer reviews organised within the framework of cooperation between the Member States of the European Union, the European Commission and the European Union Agency for Cybersecurity.".

44. Sections 17 and 18, including the headings, shall read as follows:

"Section 17

Basic service operator

(1) The following shall be entered in the register of operators of essential services:

a) a central state administration body and another state body with nationwide jurisdiction, b) a critical entity,

c) a person, regardless of whether the size requirements for a medium-sized enterprise are met, who carries out activity in any of the sectors according to Annex No. 1 or Annex No. 2 and which

1. is an undertaking providing a public electronic communications network or a public electronic communication service,

2. is a trusted service provider,

3. is the administrator of the TLD,

4. provides DNS service, 5. is the only provider of a service in the Slovak Republic that is a key service,

6. provides a service the disruption of which could have a significant impact on public order, safety or public health,

7. provides a service or has a position such that a disruption in the provision of the service or an intervention in the position could give rise to a significant systemic risk, particularly in a sector in which such a disruption or intervention could have a cross-border impact,

8. is critical for a specific sector due to its particular importance at national or regional level, or

9. is an economic mobilization subject who has been imposed a measure under a special regulation,23)

d) a state body exercising its powers in at least two districts and a higher territorial unit, if the disruption of their activities could have a significant impact on public order, safety or public health; the provision of letter a) is not affected by this, e) a person who meets at least the size requirements for a medium-sized enterprise and carries out activities in one of the sectors according to Annex No. 1 or Annex No. 2,

f) a city, if the disruption of the exercise of its powers could have a significant impact on public order, safety or public health,

g) administrator of public administration information technology23a,

h) a person who provides a domain name registration service regardless of whether the conditions are met size for a medium-sized enterprise or

(i) a third party that has significant influence in ensuring cybersecurity and has a contract with the operator of the essential service that operates the critical essential service.

(2) A person who carries out an activity pursuant to paragraph 1 is obliged, within 60 days from the date on which the activity shall commence to implement, notify the Office. The notification pursuant to the preceding sentence must include a)

the name, registered office and contact details, including electronic addresses, public IP addresses and telephone numbers,

b) a list of the Member States of the European Union in which it operates or provides services service,

c) name, registered office and contact details of the representative pursuant to Section 21(1).

(3) The Office shall enter the person referred to in paragraph 1 into the register of operators of essential services.

a) after prior consultation with the competent central authority, on its own initiative or upon a reasoned request from a person pursuant to paragraph 1, or

(b) at the proposal of the competent central authority.

(4) The Office shall immediately notify the operator of the essential service of the entry in the register of operators of essential services through the unified cybersecurity information system and deliver it to the electronic mailbox in accordance with a special regulation; 23b) a special decision shall not be issued.

(5) The rights and obligations of the operator of the essential service arise for the operator of the essential service on the date specified in the notification of entry into the register of operators of the essential service, but not earlier than the thirtieth day following the date of such entry.

(6) If there is a change in the registered facts, the Office shall make a change in the register of operators of essential services, even without a proposal. The operator of essential services shall be obliged to notify any change in the registered facts that is not reference data within 14 days at the latest through the unified cybersecurity information system of the Office. Paragraphs 3 to 5 shall apply mutatis mutandis to the implementation of the change and the obligation to notify it.

(7) The Office may delete an operator of a basic service from the register of operators basic service a)

based on a reasoned request from the operator of the basic service, after prior consultation with the competent central authority, no later than 60 days from the date of receipt of the reasoned request,

b) on the basis of a notification from the central authority, or c) on

its own initiative in justified cases.

(8) The Office shall inform the operator of the essential service of the deletion of the operator of the essential service from the register of operators of the essential service.

§ 18
Critical essential service

(1) The critical basic service is

a) the exercise of the powers of a central state administration body10) or another state body with nationwide powers,

b) activity in the sector according to Annex No. 1, except for the public administration sector, if it is carried out by a person, which exceeds the size limits set for a medium-sized enterprise,23c)

c) qualified trusted service,

d) TLD management,

e) DNS service,

f) provision of a public electronic communications network or a public electronic communications service by a person who meets at least the size requirement for a medium-sized enterprise,

g) carrying out an activity or having a status pursuant to Section 17(1)(c) five to ninth point,

h) provision of essential services to critical entities, or

i) information activities and electronic services performed using information technology public administration,23a) designated by the authorities.

(2) If an operator of an essential service performs at least one of the critical essential services, it is an operator of a critical essential service and is obliged to notify the Authority of this fact.

(3) The fact that an operator of an essential service operates a critical essential service, as well as any change in these facts, shall be recorded by the Office in the register of operators of an essential service; Section 17(3) shall apply mutatis mutandis to this notification and the method of recording, as well as to the obligation to notify changes and to their recording.

The footnotes to references 23 to 23c read: " 23) Act No. 179/2011 Coll., as amended. 23a) Act No. 95/2019 Coll., on information technologies in public administration and on amendments to certain acts, as amended. 23b) Act No. 305/2013 Coll., on the electronic form of the exercise of powers of public authorities and on amendments to certain acts (e-Government Act), as amended.

23c) 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).".

45. In Section 19, paragraph 1 reads:

"(1) The operator of an essential service is obliged, within 12 months from the date of entry in the register of operators of an essential service, to adopt, comply with and implement general security measures, depending on the risk analysis carried out, at least to the extent of the security measures pursuant to Section 20, and to implement them with the aim of ensuring cybersecurity and resilience. For the purposes of fulfilling the obligation pursuant to the first sentence, the operator of an essential service shall adopt, comply with and implement sectoral security measures, if they are established;24) the obligation to adopt measures pursuant to Section 20(4) shall not be affected by this. A person providing any of the services or performing any of the activities pursuant to Section 2(2) shall implement security measures pursuant to a separate regulation.24a)".

The footnotes to references 24 and 24a read:

" 24) For example, Regulation (EU) 2022/2554, Act No. 541/2004 Coll. on the peaceful use of nuclear energy (Atomic Act) and on amendments and supplements to certain acts, as amended, Act No. 95/2019 Coll. as amended, Decree of the Nuclear Regulatory Authority of the Slovak Republic No. 430/2011 Coll. on nuclear safety requirements, as amended by Decree No. 103/2016 Coll. 24a) Commission Implementing

Regulation (EU) 2024/2690 of 17 October 2024 laying down rules for the application of Directive (EU) 2022/2555 with regard to technical and methodological requirements for cyber risk management measures and specifying the cases in which an incident is considered significant, in relation to DNS service providers, TLD name managers, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, managed security service providers, providers of online marketplaces, internet search engines and social networking service platforms and trust service providers (OJ L, 2024/2690, 18.10.2024).".

46. In Section 19, paragraph 2, the following sentences are added at the end: "During the duration of the contractual relationship, the third party is obliged to implement and implement security measures in accordance with the written contract and this Act and is obliged to submit to the control of the implementation of these measures by the operator of the essential service. If the contract under the first sentence is concluded with the operator of the essential service that operates a critical essential service, the control may also be carried out by the Office; for this purpose, the third party has the status of the operator of the essential service. The conclusion of the contract under the first sentence must not hinder competition.".

47. In Section 19(3), the words “or to a digital service provider” are deleted.

48. In Section 19, paragraph 6 is supplemented with letters f) to i), which read as follows:

"f) analyze the dependencies of its assets, information systems, ICT products used and ICT services of third parties in the supply chain and services provided in order to identify the possible impacts of a cybersecurity incident,

g) adopt, comply with and implement security measures taking into account the Office's security methodologies and policies, the latest security trends, examples of good practice and international standards,

h) create and implement an effective mechanism for timely informing the statutory body and responsible senior employees about cyber threats, vulnerabilities, cyber security incidents, events averted at the last minute, possible impacts of cyber security incidents, results of risk analysis and the status of implementation of risk treatment with the aim of compliance with this Act,

i) notify the Office of the appointment or change of the statutory body, if this change is not reference data.".

49. In Section 19, paragraph 7, the words “in the data pursuant to Section 17, paragraph 4” are replaced by the words “in the recorded data, except for reference data”, the following words are added at the end: “and if the operator of an essential service operates a critical essential service, it is obliged to report to the Office also information on the conclusion of a contract with a third party on ensuring the fulfillment of security measures and notification obligations, which has a significant impact on ensuring cybersecurity, as well as information on its termination” and the following sentence is added: “The Office shall make a change in the register of operators of an essential service, even without a proposal.”.

50. In Section 19(8), the words "continuity of essential service" are replaced by the words "continuity of activity".

51. In Section 20, paragraphs 1 to 3 shall read as follows:

"(1) Security measures for the purposes of this Act are tasks, processes, roles and technologies in the organizational, personnel, physical and technological areas, the aim of which is to achieve, guarantee and maintain cybersecurity during the life cycle of networks and information systems and operational technologies. Security measures are implemented on the basis of a risk analysis and taking into account the security methodologies and policies of the Office, the latest security trends and international standards and in accordance with security standards in the field of cybersecurity and are adopted with the aim of a) identifying vulnerabilities, cyber threats and risks,

b) protect preventive information assets from cyber threats and prevent the emergence of

a cyber security incident,

c) detect cyber security incidents, d) respond to identified

vulnerabilities and cyber security incidents and minimize their impact on networks and information systems, and

e) restore networks and information systems, remedy negative impacts following a cyber security incident, and restore the services provided to a state of continuous and uninterrupted provision.

(2) Security measures shall be taken at least for

a) organization and management of information security and cybersecurity,

b) vulnerability and cyber threat management, c) asset

management and cyber threat and risk management,

d) event and cybersecurity incident management, e) business continuity

management, backup, disaster recovery and crisis management,

f) security in the acquisition, development and maintenance of networks, information systems, applications and configurations,

g) procedures for assessing the effectiveness of measures, compliance management and control

activities, h) cryptographic measures and principles for the use of cryptography,

i) human resources security and capabilities,

j) identity and access management,

k) security in the operation of networks and information systems, l)

protection against malicious code and unwanted content,

m) system security, network security and communication security,

n) monitoring, recording and reporting of events,

o) physical security, environmental security and terminal equipment management, p) records

protection, privacy and information labeling,

q) supply chain, r) procurement

and use of certified ICT products, ICT services and ICT processes.

(3) Security measures shall be adopted and implemented to the extent and in the manner specified in Section 32(1)(b) or a special regulation24), if issued, and on the basis of approved security documentation, which must be up-to-date and must correspond to the actual situation.".

52. In Section 20, paragraph 4 is supplemented with letters g) to i), which read as follows:

"g) determining and assigning tasks, roles and responsibilities according to the terms and conditions of the operator of the essential service and ensuring adequate education and retraining for all established roles,

h) designation of a specific person or persons responsible for approving security measures, supervision, control and audit, ensuring the adequacy of resources for cybersecurity management and for training,

(i) education and security awareness building in the field of cybersecurity.".

53. In Section 20, paragraph 6 is deleted.

The previous paragraph 7 is referred to as paragraph 6.

54. Sections 21 and 22, including the heading above Section 21, shall read as follows:

" Specific obligations

§ 21

(1) If it is a person providing any of the services or performing any of the activities pursuant to Section 2(2), or a person who is a third party who does not have a permanent residence, place of business or registered office in the territory of a Member State of the European Union and provides these services or performs these activities in the territory of the Slovak Republic, it is obliged to have a designated representative with a permanent residence, place of business or registered office in the territory of the Slovak Republic or in the territory of another Member State of the European Union in which it also provides these services or performs these activities, throughout the entire period of providing these services or performing these activities.

(2) If it concerns a person providing any of the services or carrying out any of the activities pursuant to Section 2(2) to which the scope of this Act applies and whose networks and information systems are located in another Member State of the European Union, the Office shall cooperate with the competent authority of the Member State of the European Union in exercising its powers pursuant to this Act.

(3) If a person provides any of the services or performs any of the activities pursuant to Section 2(2) to which this Act applies, he or she is obliged to notify the Office in writing, upon request, via the unified cybersecurity information system, of any change, without delay and no later than three months from the date of the change, to any of these data.

a) name,

b) classification according to Annex No. 1 or Annex No. 2,

c) the address of the establishment where any of the activities pursuant to Section 2(2) are carried out and the address of each establishment established pursuant to law in the territory of a Member State of the European Union,

d) the address of the registered office, permanent residence or place of business of the representative pursuant to paragraph 1, if he is obliged to designate it,

e) contact details at least in the scope of the electronic address and telephone number, f)

contact details of the representative, if he is obliged to appoint one, at least in the scope of the electronic address and telephone number,

g) the Member State of the European Union in which it provides a service or carries out an activity,

h) the range of IP addresses it uses.

(4) The Office shall notify any change in data notified pursuant to paragraph 3 without delay.
The European Union Agency for Cybersecurity.

§ 22

(1) The TLD administrator and the person providing the domain name registration service are obliged to record and maintain a separate record of the domain name registration data upon domain registration.

(2) The domain name registration data record contains the following data:

a) domain name,

b) the date of registration of the domain name,

c) first and last name or name of the domain holder,

d) contact details of the domain holder, at least including an email address and telephone number numbers,

e) contact details of the applicant for domain name registration at least to the extent of electronic address and telephone number, if it is a person other than the domain holder.

(3) The TLD administrator and the person providing the domain name registration service are obliged to adopt internal regulations and implement specific procedures to ensure the verification of data submitted for domain name registration, at least to the extent of the verification of data pursuant to paragraph 2 letter c), in order to ensure the compliance of the data pursuant to paragraph 2 with the facts. For these purposes, the persons referred to in the first sentence are authorised to obtain, record and copy data from an identity document even without the consent of the person concerned.

(4) The TLD administrator and the person providing the domain name registration service are obliged to publish, without delay after the registration of the domain name, free of charge, the data submitted during the registration of the domain name that are not personal data.24b)

(5) The Office and the central authority shall have access to the data submitted for the registration of a domain name for the purposes of performing state administration under this Act. The TLD administrator and the person providing the domain name registration service shall be obliged to provide the data referred to in the first sentence to the Office or the central authority upon request free of charge no later than 72 hours from the receipt of the request.

(6) If a special regulation provides for a public authority or another person to have access to data submitted for domain name registration, the TLD administrator and the person providing the domain name registration service are obliged to provide such data; the procedure pursuant to the second sentence of paragraph 5 shall apply to the provision of data.

(7) The TLD administrator and the person providing the domain name registration service are obliged to publish the internal regulations and information on the procedures for providing data pursuant to paragraphs 5 and 6 on their website free of charge.

(8) The TLD administrator and the person providing the domain name registration service are obliged to provide each other with the data necessary for the registration of the domain name so that, when registering the domain name, the applicant for the registration of the domain name is not obliged to submit such data that either of these persons is required to have by law.".

The footnote to reference 24b reads: " 24b) Act No. 18/2018 Coll. on the protection of personal data and on amendments and supplements to certain acts, as amended.".

55. Section 23, including the title, shall be deleted. 56.

Section 24, including the title, shall read as follows:

"Section 24

Messages

(1) The operator of the essential service is obliged to report every serious cyber incident security incident.

(2) A major cyber security incident is considered to be a large-scale cyber security incident and cyber security incident that a) caused or may cause a serious disruption to the operation of the operator of the essential service, or damage, other damage to property or loss of profit on a large scale,9)

b) has affected or may affect other persons by causing them damage, other harm or loss profit to a considerable extent.9)

(3) Reporting of a serious cyber security incident is carried out through the unified cybersecurity information system a) without undue delay, but no later than 24 hours after its detection, an early warning is reported, stating in particular whether the serious cybersecurity incident may have been caused by unlawful conduct or whether it may have a cross-border impact, and in the case of an operator of essential services that is a provider of trust services, the impact on the provision of trust services is also stated,

b) without undue delay, but no later than 72 hours from its detection, a notification of a serious cyber security incident shall be reported, updating and supplementing the information from the early warning, in particular stating the initial assessment of the cyber security incident, its severity and consequences, if it concerns an operator of an essential service who is a provider of trusted services, without undue delay, but no later than 24 hours from its detection,

c) at the request of the person operating the CSIRT unit, updated or other requested information on the progress of a serious cybersecurity incident is reported within a specified period,

d) no later than one month after the notification pursuant to letter b), a final report shall be submitted, which shall include, in particular, a detailed description of the serious cyber security incident, including its severity and consequences, the type of cyber threat or the root cause that likely caused the cyber security incident, the measures implemented and ongoing, and the cross-border impact, if any,

e) if it is a serious cybersecurity incident with cross-border impact that is still ongoing within the period referred to in letter d), an updated final report to the extent referred to in letter d) shall be reported within 30 days from the date of restoration of the proper operation of the network and information system; if at the time of submission of the final report referred to in letter d) the serious cybersecurity incident is still ongoing, further updated or other requested information and an updated final report shall be reported within 30 days from the date on which the serious cybersecurity incident was resolved.

(4) For the purpose of reporting serious cybersecurity incidents or ensuring cybersecurity, the Office may, instead of the procedure pursuant to Section 8(6), conclude a written contract on a different method and form of reporting cybersecurity incidents with the operator of the essential service, where this is justified by its status or the scope or content of its activities.

(5) The operator of the essential service shall also report via the unified cybersecurity information system:

a) a significant cyber threat that becomes known, b) an event averted at the last moment that could have caused a serious cyber threat security incident,

c) vulnerability of publicly available networks and information systems operated by it, which, according to available information and technical knowledge, may be exploited to cause a serious cyber security incident and the operator of the essential service could not take measures to eliminate it or reduce the risk in a reasonable time.

(6) The operator of the essential service and another person may report a cybersecurity incident, a cyber threat or an event averted at the last minute also voluntarily, above

the scope of the obligation under paragraph 1; the procedure under paragraph 3 shall be applied accordingly. The Office shall process and analyse voluntary reports under the first sentence to the extent that the technical conditions and capacities allow the Office to do so, so as to avoid an unreasonable burden on entities and restrictions on international cooperation. Voluntary reports under the first sentence shall not create any rights or obligations under this Act for a person who is not an operator of a basic service.

(7) A notification under paragraph 1 or paragraph 5 shall not affect the obligations of the operator of the essential service to adopt, comply with and implement security measures. A notification under paragraph 5 shall not affect the obligation under paragraph 1.

(8) An operator of an essential service to which Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience of the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011 (hereinafter referred to as "Regulation (EU) 2022/2554") applies shall fulfil the obligation under paragraph 1 by reporting serious ICT-related incidents through the competent authority pursuant to Regulation (EU) 2022/2554 to the Authority in the scope, manner and within the time limits laid down in Regulation (EU) 2022/2554.".

57. In Section 24a(1), the word “operator” is inserted after the word “importance”, the words “Section 24(6)” are replaced by the words “Section 24(4)” and a comma and the words “cyber crisis situation” are inserted after the words “warnings, warnings”.

58. In Section 24a(4), the reference “28a)” above the word “regulation” is replaced by the reference “24c)”.

The footnote to reference 24c reads: " 24c) Act No.

166/2003 Coll. on the protection of privacy against unauthorized use of information and technical means and on amendments to certain acts (Act on Protection against Wiretapping), as amended.".

59. Sections 25 and 26, including their headings, are deleted.

60. The heading of Section 27 reads: “Responses to cyber security incidents and cyber threats and resolving a cyber security incident”.

61. In Section 27(1), introductory sentence, the word “its” is replaced by the words “significant cyber” and in letter a) the words “warning and warning of a serious cyber security incident” are replaced by the words “warning, warning or state of cyber crisis”.

62. In Section 27(3), the words “and the digital service provider” are replaced by the words “or a third party that has significant influence in ensuring cybersecurity”.

63. In Section 27(5), the words “to the digital service provider” in all forms are replaced by the words “to a third party that has a significant influence in ensuring cybersecurity” in the relevant form.

64. In Section 27(6), the words “the digital service provider shall be obliged” are replaced by the words “a third party that has a significant influence in ensuring cybersecurity shall be obliged”.

65. In Section 27, paragraph 10 reads:

"(10) Due to the urgency and urgency of resolving a serious cyber security incident, detecting such a threat or possible cyber terrorism, the Office for the purposes of cyber defence28) shall inform the Military Intelligence, which shall proceed in accordance with special regulations.28a) The operator of the essential service reporting this cyber security incident shall, for the purposes of ensuring cyber defence, be obliged to provide the Military Intelligence with information to the necessary extent. The Office shall inform the Chairman of the Security Council of the Slovak Republic about the procedure pursuant to the first sentence.".

The footnote to reference 28a reads: " 28a) Act No.

319/2002 Coll., as amended. Section 7 of Act No. 500/2022 Coll.".

66. Section 27 is supplemented by paragraphs 11 and 12, which read as follows:

"(11) The Office shall declare a state of cyber crisis to the necessary extent and for the necessary time. The Office shall inform the Cybersecurity Committee of the Security Council of the Slovak Republic about the intention and reasons for declaring a state of cyber crisis, as well as the procedures for resolving it.28aa) Before formally declaring a state of cyber crisis, the Office shall promptly notify the Military Intelligence and the Slovak Information Service of this fact, so as not to hinder the performance of tasks under special regulations28ab) and shall inform the relevant central authority and the person who operates the relevant CSIRT unit. The Office shall revoke the state of cyber crisis when the reasons for which the state of cyber crisis was declared cease to exist. The declaration and revocation of the state of cyber crisis shall be carried out through mass media.

Measures and activities during a state of cyber crisis are defined by the National Response Plan for Large-Scale Cybersecurity Incidents and Crises.

(12) The Cybersecurity Office may request the cooperation of Military Intelligence in resolving a serious cyber security incident and cyber crisis or detecting such a threat. Military Intelligence shall provide the Office with cooperation pursuant to a special regulation.28ac)".

The footnotes to references 28aa to 28ac read: " 28aa) Section 10b of Act No. 110/2004 Coll. on the functioning of the Security Council of the Slovak Republic in peacetime, as amended.

28ab) For example, Act of the National Council of the Slovak Republic No. 46/1993 Coll., as amended, Act No. 500/2022 Coll.

28ac) Act no. 500/2022 Coll.

67. In Section 27a, paragraph 1, the introductory sentence, the word "basic" is deleted.

68. In Section 27a, paragraph 4 is deleted.

The previous paragraphs 5 to 8 are referred to as paragraphs 4 to 7.

69. In Section 27a, paragraphs 4 and 6, the words "providing a basic service" are replaced by the words "providing services".

70. Section 28, including the title, is deleted.

71. In Section 29(1), the words “essential service systems” are replaced by the words “service systems”, the words “support essential services” are replaced by the words “support services” and the following sentence is added at the end: “An essential service operator who is not an operator of a critical essential service may ensure compliance with the obligation to conduct a cybersecurity audit within the period specified in the previous sentence by verifying the effectiveness of the adopted security measures and compliance with the requirements set out in this Act by self-assessment through the unified cybersecurity information system in the manner specified in paragraph 8.”.

72. In Section 29, paragraph 2, the words "depending on the classification of information and the categorization of networks and information systems" are deleted.

73. In Section 29, paragraph 3, the words “accredited person” are replaced by the words “public administration entity pursuant to special regulation 31aa) accredited".

The footnote to reference 31aa reads: " 31aa) Section 3, paragraph 1 of Act No. 523/2004 Coll. on budgetary rules of public administration and on amendments and supplements to certain acts.".

74. Section 29 is supplemented by paragraphs 8 and 9, which read as follows:

"(8) An operator of an essential service that is not an operator of a critical essential service may, at the periodicity established pursuant to Section 32(1)(d), ensure compliance with the obligation to conduct a cybersecurity audit by conducting a self-assessment through the unified cybersecurity information system. The self-assessment shall be performed by the cybersecurity manager. Such an operator of an essential service is obliged to

undergo a cybersecurity audit within five years from the date of inclusion in the register of operators of essential services and subsequently according to the periodicity established under Section 32(1)(d). Self-assessment is not performed at the time of the obligation to conduct a cybersecurity audit.

(9) The operator of the essential service to which Regulation (EU) 2022/2554 applies shall carry out a review of the effectiveness of the security measures taken pursuant to Regulation (EU) 2022/2554 by the person referred to in paragraph 3.”.

75. After Section 29, Sections 29a to 29n are inserted, which, including the headings, read as follows:

"Section 29a

Supervision

(1) The Office shall carry out supervision

a) handling complaints,

b) inspection,

c) imposing measures to stop the breach of obligations and remedy the illegal situation (hereinafter referred to as "remedial measures"),

d) approving a remedial agreement, e) hearing

administrative offences and imposing disciplinary fines and penalties.

(2) The Office shall exercise supervision in relation to an operator of a basic service who has a permanent residence, place of business or registered office in the territory of the Slovak Republic, or a person pursuant to Section 2(2).

(3) When exercising supervision, the Office shall proceed in such a way that:

a) interfere with the rights and legally protected interests of persons only to the extent necessary for achieving the goal,

b) chose the means appropriately in relation to the consequences that the chosen means will cause on property, rights and legally protected interests of other persons,

c) take into account the manner, duration and seriousness of the breach of obligations.

(4) The subject of supervision is not the resolution of disputes arising from legal relationships between supervised entities and their employees, other persons performing activities for them, their clients and other service recipients, the hearing and decision-making of which is the responsibility of the competent courts or other authorities pursuant to special regulations.

(5) The performance of supervision shall not affect the obligations of the operator of the essential service and the powers of the Office and other authorities in the area of reporting pursuant to Section 24 and addressing cyber security incidents, cyber threats, near-miss events or vulnerabilities.

(6) Supervision shall be non-public to the extent necessary to maintain cybersecurity, prevent cybersecurity incidents or their continuation.

(7) The Office shall ensure and coordinate the provision of cooperation and assistance with authorities with powers similar to those of the Office under this Act or with CSIRT units of another Member State of the European Union for the purposes of supervision.

§ 29b

Handling complaints

(1) The Office shall handle complaints31d) concerning the breach of obligations of the operator of a basic service, if they are filed by a service consumer or a person whose main activity is the protection and enforcement of the rights and legally protected interests of service consumers or the area of cybersecurity.

(2) If the complaint pursuant to paragraph 1 is directed against a person to whom this Act does not apply and who falls within the jurisdiction of another Member State of the European Union, the Office shall forward the complaint to the competent authority of another Member State of the European Union.

(3) A special regulation applies to the handling of complaints pursuant to paragraph 1.31d)

Control

§ 29c

(1) The Office is authorized to carry out inspections of the fulfillment of the obligations of the operator of the basic services under this Act or obligations imposed under this Act.

(2) The inspection may also be carried out in the form of an on-site inspection.

(3) Control may also be exercised on a consolidated basis over groups of persons or special purpose entities of which the operator of the essential service is a part, if these persons are interconnected and have influence in ensuring the cybersecurity of the operator of the essential service or participate in its activities.

(4) The inspection shall

a) ascertains the status of the controlled facts and their compliance with the obligations under this Act or with the obligations imposed on the basis of this Act,

b) identify the causes and harmful consequences of deficiencies identified during the inspection,

c) ascertains compliance with the remedial measures imposed or taken (hereinafter referred to as "compliance with the measures taken").

§ 29d

(1) The inspection shall be carried out on the basis of a written authorization from the Director of the Office or by him/her. authorized representative (hereinafter referred to as "authorization to carry out the inspection").

(2) The authorization to carry out an inspection shall contain in particular:

a) designation of the inspection body,

b) designation of the controlled entity,

c) the names and surnames of the employees of the Office or members of the Office, or possibly also the invited person authorized to carry out the inspection,

d) subject of the inspection,

e) signature of the director of the office.

(3) If during the performance of the inspection, facts arise that require the authorisation to carry out the inspection to be amended or supplemented, an amendment to the authorisation to carry out the inspection shall be drawn up. The amendment to the authorisation to carry out the inspection shall consist of

an integral part of the mandate to carry out the inspection.

(4) The inspection shall be initiated by the first act of the Office against the operator of the essential service.

(5) In connection with the performance of the inspection, the Office is entitled to:

a) to request and collect from the operator of the essential service or from a person who has information, documents or other supporting documents necessary for the performance of the inspection (hereinafter referred to as the "third party"), within a specified period and to the extent, originals or officially certified copies of documents, writings, data records on storage media of computer equipment or transmitted in the network and their extracts and outputs, statements, information, documents and other supporting documents related to the inspection, to make copies of them and to handle them,

b) require cooperation from the operator of the essential service or from a third party within the scope of the authorisations necessary for the exercise of the authority's authorisations,

c) require the operator of the essential service to submit a written list of measures taken to remedy the deficiencies identified during the inspection and to eliminate the causes of their occurrence (hereinafter referred to as the "written list of measures taken") within the period specified by the Authority,

d) in justified cases, require the revision of the written list of measures taken and the submission of a revised written list of measures taken within a period determined by the Authority, if the Authority reasonably assumes that the measures taken are not effective, given the seriousness of the deficiencies,

e) require the operator of the essential service to comply with the measures taken within the period specified by the Authority and to require the submission of documentation proving compliance with the measures taken after the expiry of this period,

f) verify compliance with the measures taken.

(6) In connection with the performance of the inspection, the Office is authorized to enter, to the extent necessary, a building, facility, operation, means of transport, land of the operator of the essential service or a third party, or to enter a dwelling if it is also used for business or for the performance of other economic activities related to the provision of the service of the operator of the essential service.

(7) In connection with the performance of the inspection, the Office is obliged to:

a) in advance, no later than upon entry pursuant to paragraph 6, notify the operator of the essential service or a third party of the start date and purpose of the inspection, present an authorization to conduct the inspection, and allow the operator of the essential service or a third party to inspect their identity card or, in the case of an officer of the office, their service card, at their request,

b) confirm to the operator of the essential service or a third party the collection of the provided originals or officially certified copies of documents, writings, data records on storage media of computer equipment and their extracts and outputs, statements, information, documents and other supporting documents related to the inspection and ensure their proper protection against loss, destruction, damage and misuse,

c) return the things referred to in letter b) immediately after the purpose for which they were taken has been fulfilled, from whom they were taken, if they are not necessary for the proceedings pursuant to letter g),

d) inform the operator of the essential service of the draft partial report or of the draft report on its delivery, if deficiencies have been identified, and inform the operator of the essential service of the possibility of submitting written objections to the identified deficiencies, the deadline for submitting a written list of measures taken and the deadline for fulfilling the measures taken.

measures specified in the draft partial report or in the draft report within a reasonable period determined by the Office from the date of delivery of the draft partial report or draft report,

e) verify the justification of the objections submitted pursuant to letter d) and take into account the justified objections in the partial report or in the report and notify the operator of the essential service of the unfoundedness of the objections, together with the justification for their unfoundedness, in the partial report or in the report,

f) send a partial report or report to the operator of the essential service, g) report suspicions

of a crime, misdemeanor or other administrative offence to the authorities competent under special regulations, whereby these suspicions are not stated in the draft partial report, draft report, partial report or report in cases worthy of special attention.

§ 29e

(1) When carrying out an inspection, the operator of the essential service is entitled to:

a) require confirmation of the collection of the provided originals or officially certified copies of documents, writings, data records on storage media of computer equipment and their extracts and outputs, statements, information, documents and other supporting documents related to the inspection,

b) submit written objections to the identified deficiencies, the deadline for submitting a written list of measures taken and the deadline for implementing the measures taken, specified in the draft partial report or in the draft report,

c) require the Office to send a draft partial report or a draft report,

d) require the authority or the invited person to show proof of authorization to conduct the inspection and require inspection of the identity card or, in the case of an officer of the authority, the service card, if the inspection is carried out on site.

(2) In connection with the performance of the inspection, the operator of the essential service is obliged to:

a) submit to the Authority or an invited person upon request the results of inspections or audits carried out by other authorities that are related to the inspection carried out by the Authority,

b) submit, within the time limit and to the extent determined by the office or the invited person, the requested originals or officially certified copies of documents, writings, data records on storage media of computer equipment or transmitted via the network and their extracts and outputs, statements, information, documents and other supporting documents related to the inspection, issue a written confirmation of their completeness upon request and allow the office or the invited person to make copies of them,

c) provide cooperation to the Office or the invited person, d)

take measures to correct the deficiencies identified during the inspection and to eliminate the causes of their occurrence stated in the partial report or in the report and submit to the Office a written list of the measures taken within the period specified by the Office,

e) submit and revise within the period specified by the Authority a written list of measures taken, if the office required its revision and submission,

f) to comply with the measures taken within a reasonable period determined by the

Authority, g) to submit, upon request by the Authority, documentation proving compliance with the measures taken,

h) create conditions for conducting an on-site inspection and refrain from any action that could jeopardize its initiation and proper conduct,

i) at the start of the on-site inspection, inform the authority or the invited person of the safety regulations applicable to the premises in which the on-site inspection is being carried out,

j) allow the authority or an invited person to enter a building, facility, operation, means of transport, land or a dwelling, if it is also used for business or for carrying out other economic activities related to the provision of a service by the operator of the essential service.

(3) The rights under paragraph 1 letters a) and d) also belong to a third party. The obligations under paragraph 2 letters a) to c) and h) to j) also belong to a third party.

(4) The costs incurred by the operator of the essential service or a third party in connection with the performance of the inspection shall be borne by the operator of the essential service or the third party.

§ 29f

(1) The Office shall prepare a draft partial report or a draft report and a partial report or report on the deficiencies identified during the inspection. If no deficiencies were identified, the Office shall prepare only a partial report or report.

(2) An interim report may be prepared if:

a) it is necessary or expedient to terminate the inspection in part of the inspected facts,

b) it is necessary to take measures to remedy the deficiencies identified without undue delay inspection and eliminate the causes of their occurrence or

c) the inspection is carried out at several operators of essential services.

(3) The draft report and the draft partial report shall contain in particular:

a) designation of the office,

b) the names, surnames and signatures of the employees of the Office or members of the Office and the invited person who carried out the inspection; the signature of these persons is not required in cases worthy of special attention if the draft report or draft partial report from the inspection carried out is signed by at least one employee of the Office or member of the Office who carried out the inspection,

c) designation of the operator of the basic service,

d) the objective of the

inspection, e) a description of the deficiencies identified during the inspection, together with their justification,

f) an indication of the specific obligations that have been breached, g) a list

of evidence demonstrating the identified deficiencies,

h) the date of preparation of the draft partial report or draft report, i) the deadline for

submitting objections to the identified deficiencies, the deadline for submitting a written a list of measures taken and the deadline for completing the measures taken,

j) the deadline for submitting a written list of measures taken,

k) the deadline for implementing the measures taken.

(4) A draft partial report or draft report shall be deemed to have been delivered, even if the operator of the basic service refuses to accept it, on the date of refusal to accept it. If a draft report or draft partial report cannot be delivered, these proposals shall be deemed to have been delivered on the date of return of the undelivered draft partial report or draft report.

the office, even if the operator of the basic service did not learn about it.

(5) If the operator of the essential service does not submit objections to the identified deficiencies, the deadline for submitting a written list of measures taken and the deadline for implementing the measures taken specified in the draft partial report or in the draft report within the period pursuant to paragraph 3(i), the identified deficiencies, the deadline for submitting a written list of measures taken and the deadline for implementing the measures taken shall be deemed accepted.

(6) Paragraph 3 letters a) to d) shall apply equally to the particulars of the partial report and report. The partial report and report shall also contain the date of its preparation. If deficiencies have been identified, the partial report and report shall contain, in addition to the particulars specified in the first and second sentences, also

a) date of delivery of the draft partial report or draft report for information
the operator of the essential service,

b) information on whether the operator of the essential service has submitted objections to the identified deficiencies, the deadline for submitting a written list of measures taken and the deadline for implementing the measures taken and the method of dealing with these objections,

c) after taking into account the merits of the objections submitted

1. a description of the identified deficiencies together with their justification,

2. an indication of the specific obligations that have been violated,

d) a list of evidence demonstrating the identified deficiencies, e) a

deadline for submitting a written list of measures taken and a deadline for compliance
measures taken.

(7) The inspection is completed on the date of sending the report to the operator of the essential service. Sending a partial report completes the part of the inspection to which the partial report relates.
If the inspection or part thereof is stopped for reasons worthy of special consideration, the inspection or part thereof shall be terminated by making a record stating the reason for stopping the inspection or part thereof. The Office shall immediately send a record of the stoppage of the inspection or part thereof to the operator of the essential service; this shall not apply if the operator of the essential service has ceased to exist.

(8) If, after the check, typing errors, calculations or other obvious inaccuracies are found, the partial report or report shall be corrected and the part of the partial report or report to which the correction relates shall be sent to the operator of the basic service and to all to whom the original partial report or report was sent.

§ 29g

(1) If justified by the special nature of the inspection, the Authority may invite an invited person to carry out the inspection with their consent. If an authority with powers similar to those of the Authority under this Act or a CSIRT unit of another Member State of the European Union requests participation in the inspection, the Authority shall invite the persons designated by them to participate in the inspection.

(2) The participation of an invited person in an inspection is considered to be another act in the general interest.

(3) Compensation for wages or salary in the amount of average earnings or compensation under a special regulation in connection with participation in an inspection shall be paid by the Office to the invited person, unless the invited person agrees otherwise with the Office; this does not apply to persons invited under paragraph 1.

(4) The powers provided for in Section 29d, paragraph 5, letters a) and b) and paragraph 6 and the obligations provided for in Section 29d, paragraph 7, letters a), b), e) and g) apply equally to the invited person.

(5) The employee of the Office and the invited person who carry out the inspection shall, when performing the inspection, tasks under this Act, the status of a public official under the Criminal Code.

§ 29h

(1) An employee of the Office or a member of the Office and an invited person are obliged to refrain from conduct that leads or could lead to their impartiality being called into question.

(2) An employee of the Office or a member of the Office and an invited person who are aware of facts that raise doubts about their impartiality in relation to the inspection being carried out, the operator of the essential service or a third party are obliged to notify the Director of the Office of these facts in writing.

(3) The operator of the essential service may submit written objections to the Office against the participation in the inspection of an employee of the Office, an official of the Office or an invited person, stating the reason for the objections, if it has doubts about the impartiality of the employee of the Office, an official of the Office or an invited person. The submission of objections shall not have a suspensive effect on the performance of the inspection.

(4) An employee of the Office or a member of the Office, or an invited person against whom written objections have been filed or who has made a notification pursuant to paragraph 2, are authorized, until the decision of the Director of the Office, to perform only those acts during the inspection that cannot be postponed.

(5) The Director of the Office is obliged to decide on the matter of bias of an employee of the Office or a member of the Office, or an invited person, no later than three working days from the date of delivery of written objections pursuant to paragraph 3 or notification pursuant to paragraph 2.

(6) An employee of the Office or a member of the Office and an invited person are obliged to maintain confidentiality regarding facts that they have learned in connection with the performance of the inspection; they may be exempted from this obligation by the Director of the Office. The obligation under the first sentence shall continue even after the termination of the service relationship, employment relationship or similar employment relationship.

Imposition of legal measures

§ 29i

(1) The Office may, before initiating proceedings for the imposition of a corrective measure, issue a preliminary measure, which, to the extent strictly necessary to prevent the occurrence of serious damage or other harm:

a) orders the operator of the essential service to do something, to refrain from doing something, or suffered something,

b) order the securing of items necessary for the taking of evidence.

(2) The delivery of the interim measure to the operator of the essential service shall be considered the first act in the proceedings for the imposition of a remedial measure and shall commence the proceedings. The proceedings for the imposition of a remedial measure shall not be limited by the scope and grounds of the interim measure issued.

(3) The Office shall revoke the interim measure on its own initiative as soon as the reason for which it was issued ceases to exist or if circumstances change such that the interim measure is no longer necessary or expedient; otherwise, the interim measure shall lapse upon the expiry of time, if it was issued for a certain period, or on the date on which the decision imposing the measure becomes final. If

the reasons for cancellation according to the first sentence apply only to part of the interim measure, the Office shall cancel the interim measure in part.

(4) An appeal against a decision on a preliminary injunction shall not have a suspensive effect.

(5) Paragraphs 1 to 4 shall not affect the possibility of issuing a preliminary injunction in proceedings for the imposition of a remedy.

§ 29j

(1) If the Office finds deficiencies in the activities of the operator of the essential service consisting in the fulfillment of the obligations of the operator of the essential service under this Act or obligations imposed on the basis of this Act, depending on the seriousness, scope, duration, consequences and nature of the deficiencies found, it may impose on the operator of the essential service the obligation

a) conduct a cybersecurity audit and make recommendations based on the results of this audit within the specified time limit,

b) take corrective measures,

c) inform the data subjects or the public about the risks or consequences of the breach obligations, or

d) prohibit the provision of the service until the illegal situation is rectified, if such a measure is absolutely necessary due to an immediate threat to life or health, other measures within the framework of supervision have not been effective and the rectification has not been carried out within the period determined by the authority; this does not apply if the operator of the essential service is a public authority or if it provides the service on the basis of an obligation imposed by law or on its basis.

(2) The Office may, in addition to imposing an obligation to take corrective measures, also impose on the operator of the essential service an obligation to pay a penalty in the amount of 0.5% of the highest possible amount of the fine that can be imposed for a breach of such an obligation, for each day of delay in fulfilling the obligation.

(3) In proceedings for the imposition of a corrective measure, the Office may also impose a fine for an administrative offence if it concerns a breach of an obligation that constitutes an administrative offence; Section 31 shall apply equally to determining the amount of the fine.

(4) If the operator of a basic service that operates a critical basic service fails to comply with the obligation under paragraph 1 letter a) or letter b), even within the additional period specified in the Office's notice, the Office may, depending on the seriousness, extent, duration, consequences and nature of the deficiencies found, prohibit the statutory body of the operator of a basic service or a member of the statutory body of the operator of a basic service, its senior employee at the highest level of management responsible for the relevant activity or the authorized representative entrusted with the performance of this activity from performing their function, employment or activity at the operator of a basic service, until such time as these obligations are fulfilled. The provision of the first sentence shall not apply if the operator of a basic service is a public authority to which this Act applies.

§ 29k

(1) If the operator of a basic service fails to fulfil the obligations imposed pursuant to Section 29j(1) properly and on time, the illegal situation persists and causes serious damage or other harm and contains elements of a criminal offence against the life, health or safety of persons, it may be obliged to temporarily restrict access by a court decision issued at the proposal of the Office.

a) customers affected by the illegal status of the service, or

b) to the online interface through which the infringement causing the infringement occurs illegal status.

(2) If the service provider is not able to restrict access pursuant to paragraph 1, the obligation to restrict access pursuant to paragraph 1 may be imposed secondarily on a person who is objectively capable of implementing such a restriction; compliance with this obligation does not confer any further rights or obligations on the person under this Act.

(3) The Office's proposal pursuant to paragraph 1 must contain:

a) identification of the operator of the essential service or the person pursuant to paragraph 2 who is obliged to restrict access pursuant to paragraph 1,

b) data on the online interface through which the infringement occurs causing an unlawful situation,

c) data on the scope and period of access restriction pursuant to paragraph 1,

d) justification for the need to restrict access pursuant to paragraph 1.

(4) In order to properly ascertain and identify the facts pursuant to paragraph 3 letter b), the Office and the court are authorized to request the cooperation of a public authority or a legal entity, which are obliged to comply with this request without delay, provided that this does not endanger the performance of the tasks of the intelligence service or reveal its sources, means, the identity of persons acting on its behalf, or endanger international intelligence cooperation.

(5) The court decision must also contain the data pursuant to paragraph 3. The court decision may include the authority's authorization to repeatedly extend the period of access restriction pursuant to paragraph 1.

(6) The Office shall deliver the court decision to the operator of the essential service and the person to whom an obligation to restrict access has been imposed pursuant to paragraph 1.

(7) If the Office is authorised, based on a court decision, to repeatedly extend the period of access restriction pursuant to paragraph 1, it shall issue a separate decision on each such extension.

§ 29l
Imperative action

(1) If, during the performance of supervision pursuant to Section 29a(1)(a) to (c), it has been reliably established that an operator of a basic service has breached an obligation in an individual case, the Authority shall be competent, without further proceedings, to issue an order imposing a sanction on the operator of a basic service for the breach of the obligation found. It shall not be an obstacle to assessing a breach of the obligation as an individual case if, during the performance of supervision, the Authority reliably establishes a repeated identical breach or several similar breaches of the obligation committed by the same operator of a basic service in other different cases.

(2) The order imposing a sanction may impose a fine of up to EUR 10,000 and a corrective measure, depending on the seriousness, extent, duration, consequences and nature of the deficiency found. The sanction under the first sentence may be imposed separately or concurrently and, for a persistent deficiency, also repeatedly; the sanction under the first sentence may be imposed repeatedly also for a repeated identical violation or several similar violations of the obligation committed by the same operator of the essential service in other different cases.

(3) An operator of an essential service to which an order imposing a sanction has been issued may:

to file a written objection to the issued order imposing a sanction with the authority within 15 days of its delivery, which must be justified. By timely filing of an objection with justification, the order imposing a sanction is revoked and the authority continues the procedure for imposing a corrective measure, while it is not bound by the scope of factual findings, legal qualification or type and amount of the sanction according to the revoked order imposing a sanction or other content of the revoked order imposing a sanction. If no other action was taken against the operator of the essential service before the order imposing a sanction was issued, after timely filing of an objection with justification, the delivery of the order imposing a sanction to the operator of the essential service is considered the first action in the procedure for imposing a corrective measure.

(4) An order imposing a sanction against which no objection with justification has been filed in time shall have the effect of a final decision against which no appeal may be filed.

§ 29m
Remedial agreement

(1) The Authority may at any time during the exercise of supervision propose to the operator of the basic services conclusion of a remediation agreement.

(2) The settlement agreement shall include:

a) designation of the operator of the essential service and the authority,

b) a description of the breaches of the obligations of the operator of the essential service to which the remedy relates, indicating the place, time and, where applicable, other circumstances under which the breach occurred, so that the description cannot be confused with another breach of obligations,

c) measures to eliminate the illegal situation and the timetable for their adoption, d) the extent and method

of compensation for damage or other harm to service users or other persons, if caused,

e) measures to prevent similar breaches of obligations in the future,

f) date, signature of the person authorised to act on behalf of the operator of the essential service and signature the director of the office.

(3) The Office may conclude a remedial agreement if the measures and compensation contained in the agreement are capable of eliminating the unlawful situation and adequately compensating for the damage or other harm incurred and if there is no other interest in continuing to exercise supervision.

(4) If a remedial agreement is concluded, the Authority shall cease supervision to the extent of the violations of obligations contained in the remedial agreement.

(5) The Office may re-initiate supervision in the matter of violation of obligations contained in the remedial agreement if

a) there has been a material change in any fact decisive for the conclusion of the remedial agreements,

b) the operator of the essential service fails to fulfil its obligations under the remediation agreement, or

(c) the conclusion of the remediation agreement was based on incomplete, incorrect or misleading information provided by the operator of the essential service.

§ 29n
Administrative fine

(1) A controlled entity that fails to fulfill its obligations under this Act when performing supervision and thereby prevents the conduct of the control pursuant to Sections 29c to 29h shall frustrate the result of the control.

or correction of identified deficiencies, the office may impose a fine of up to 1,500 euros.
When determining the administrative fine, the office takes into account the degree of difficulty in performing the inspection or the obstruction of the inspection result.

(2) A disciplinary fine pursuant to paragraph 1 may be imposed repeatedly, but not more than
total amount of 15,000 euros.

(3) A disciplinary fine may be imposed within two months from the date of discovery of the breach of obligation, but no later than one year from the date of the breach of obligation.

(4) The imposition of a disciplinary fine does not relieve the inspected entity of the obligation to proceed
in accordance with this law.

(5) The administrative fine is a revenue of the state budget.".

The footnote to reference 31d reads: " 31d) Act
No. 9/2010 Coll. on Complaints, as amended.".

76. In Section 30, paragraph 1, letter b), the words "Section 17, paragraph 4" are replaced by the words "Section 17, paragraph 2."

77. In Section 30, paragraph 1, letter d) is deleted.

The previous letter e) is referred to as letter d).

78. In Section 30, paragraph 1 is supplemented with letters e) and f), which read as follows:

"e) conducts a cybersecurity audit in violation of Section 29(3), or

f) conduct a self-assessment through the unified cyber security information system
security in violation of Section 29, paragraph 8.".

79. Section 31, including the title, reads as follows:

"Section 31

Administrative offenses

(1) The Office may impose a fine of between EUR 300 and EUR 500,000 on the operator of an essential service,
who commits an administrative offense by violating an obligation

a) notify the start of the performance of activities pursuant to Section 17, paragraph 2,

b) notify a change in data pursuant to Section 17, paragraph 6,

c) notify the operation of a critical basic service pursuant to Section 18(2),

d) pursuant to Section 19, paragraphs 2 to 4, paragraph 6, letter f) or paragraph 7,

e) keep the safety documentation up-to-date and in line with the actual situation according to
Section 20, paragraph 3,

f) pursuant to Section 29, paragraphs 1, 2, 5 or paragraph 8,

g) take corrective action within the time limit set out in the final audit report, in accordance with
Section 29, or

h) imposed by the Office pursuant to Section 29j, paragraph 1.

(2) The Authority may impose a fine of EUR 300 to EUR 7,000,000 or up to 1.4% of the total worldwide annual turnover for the previous accounting period, whichever is higher, on an operator of an essential service who commits an administrative offence by breaching the obligation

a) pursuant to Section 19, paragraph 1 or paragraph 6, letters a) to e) or letters g) to i),

b) accept the safety documentation pursuant to Section 20(3),

c) report a serious cybersecurity incident pursuant to Section 24(1) or (3),

d) send specified system information in an automated manner pursuant to Section 24a(1),

e) to address a cyber security incident based on a decision of the Authority pursuant to Section 27(3), to implement a reactive measure based on a decision of the Authority pursuant to Section 27(5) or to notify and demonstrate the implementation of a reactive measure and its result pursuant to Section 27(6), or

f) submit a protective measure for approval or implement an approved protective measure according to Section 27, paragraph 8.

(3) The Authority may impose a fine of EUR 500 to EUR 10,000,000 or up to 2% of the total worldwide annual turnover for the preceding accounting period, whichever is higher, on an operator of an essential service operating a critical essential service who commits an administrative offence by breaching any of the obligations referred to in paragraph 2.

(4) The Office may impose a fine of EUR 300 to EUR 500,000 on a person providing any of the services or performing any of the activities pursuant to Section 2, paragraph 2, to which the scope of this Act applies, who commits an administrative offence by failing to notify the Office of a change in data pursuant to Section 21, paragraph 3, upon request.

(5) The Office may impose a fine of EUR 500 to EUR 500,000 on a person providing any of the services or performing any of the activities pursuant to Section 2, paragraph 2 in the territory of the Slovak Republic who does not have a permanent residence, place of business or registered office in a Member State of the European Union, who has committed an administrative offence by failing to appoint a representative with a permanent residence, place of business or registered office in the territory of the Slovak Republic or in the territory of another Member State of the European Union in which he also provides these services or performs these activities pursuant to Section 21, paragraph 1.

(6) The Office may impose a fine of EUR 300 to EUR 500,000 on a TLD administrator and a person providing a domain name registration service who commits an administrative offence by violating the obligation to: a) keep a special

record of domain name registration data pursuant to Section 22(1),

b) adopt internal regulations, establish specific procedures to ensure data verification submitted when registering a domain name and publish them pursuant to Section 22(3),

c) make available the data submitted when registering a domain name pursuant to Section 22(4), or d)

provide the Office or the central authority with data pursuant to Section 22(5).

(7) The Office may impose a fine of between EUR 300 and EUR 500,000 on anyone who:

a) fails to provide information pursuant to Section 7(4) upon request by the Office,

b) fails to provide the Office with the required cooperation or information pursuant to Section

10a(1), c) uses a specific product, service or process in violation of Section 27a(4).

(8) The Authority may impose a fine of between EUR 300 and EUR 500,000 on a manufacturer or provider of products, services or processes who commits an administrative offence by issuing an EU declaration of conformity pursuant to Article 53 of Regulation (EU) 2019/881 that is contrary to the requirements laid down in a cybersecurity certification scheme issued pursuant to Article 49(7) of Regulation (EU) 2019/881.

(9) The Authority may impose a fine of EUR 300 to EUR 500,000 on a manufacturer or provider of certified products, services or processes or a manufacturer or provider of products, services and processes for which an EU declaration of conformity has been issued who commits an administrative offence by failing to publish in electronic form or update additional information on cybersecurity pursuant to Article 55(1)(a) to (d) of Regulation (EU) 2019/881.

(10) The Office may impose a fine of EUR 300 to EUR 500,000 on a conformity assessment body, a holder of a European cybersecurity certificate or an issuer of EU declarations of conformity who commits an administrative offence by:

a) fails to provide the national cybersecurity certification authority with the information necessary to perform its tasks pursuant to Article 58(8)(a) of Regulation (EU) 2019/881,

b) prevents the national cybersecurity certification authority from conducting an investigation in the form of an audit pursuant to Article 58(8)(b) of Regulation (EU) 2019/881.

(11) The Authority may impose a fine of EUR 300 to EUR 500,000 on a conformity assessment body or a holder of a European cybersecurity certificate who commits an administrative offence by not allowing the national cybersecurity certification authority access to the premises pursuant to Article 58(8)(d) of Regulation (EU) 2019/881.

(12) When imposing a fine for an administrative offence, the Office shall take into account the seriousness of the administrative offence, in particular the manner in which it was committed, its duration, consequences and the circumstances under which it was committed. If the harmful consequence is insignificant, or if the mere violation of an administrative offense is sufficient to punish, the office will not impose a fine.

(13) If, within one year from the date of entry into force of the decision imposing a fine, there is a repeated breach of the obligations for which the fine was imposed, the Office may impose a fine of up to twice the amount specified or calculated pursuant to paragraphs 1 to 11.

(14) Paragraphs 1 to 6 shall apply mutatis mutandis to a person providing any of the services or carrying out any of the activities pursuant to Section 2, paragraph 2, who is not established in the European Union but offers services within the European Union and has a designated representative in the territory of the Slovak Republic or does not have a designated representative in any Member State of the European Union.

(15) For the purposes of this Act, the total worldwide annual turnover under paragraphs 2 and 3 shall be understood as the sum of all sales, income or receipts from the sale of goods or services, excluding indirect taxes, to which is added the financial assistance provided. Turnover expressed in foreign currency shall be converted into euros, whereby the average of the reference exchange rates determined and announced by the European Central Bank or the National Bank of Slovakia, valid for the relevant accounting period, shall be used for the conversion of foreign currency into euros.33)

(16) The previous accounting period for the purposes of this Act is the accounting period for which the last financial statements were prepared.

(17) A fine for an administrative offence may be imposed within two years from the date of discovery of the violation. obligation, but no later than four years from the date on which the breach of obligation occurred.

(18) A fine for an administrative offence is payable within 30 days from the date on which the decision imposing it becomes final.

(19) If it is not possible to impose a sanction under this Act, the Office shall refer the matter to the competent authority.

(20) Fines for administrative offences are revenue of the state budget.”.

80. In Section 32(1), letter b) is deleted.

The previous letters c) to i) are referred to as letters b) to h).

81. In Section 32, paragraph 1, letter b), the words "paragraphs 1 and 6" are deleted.

82. In Section 32(1)(c), the words "Section 20(1)" are replaced by the words "Section 20".

83. In Section 32(1), letter d) is deleted.

The previous letters e) to h) are referred to as letters d) to g).

84. In Section 32(1)(d), the words “or self-assessment” are inserted after the words “cybersecurity audit rules”, the words “or self-assessment” are inserted after the words “periodicity of conducting a cybersecurity audit”, the words “certification scheme and” are replaced by the words “certification schemes,” and the words “(Section 29(1) to (5))” are deleted.

85. In Section 32, paragraph 1 is supplemented with letters h) and i), which read as follows:

"h) details of cybersecurity education and awareness-raising security,

i) details of reports pursuant to Section 24.".

86. In Section 33, paragraph 1, a comma and the words “Sections 27 to 27c” are inserted after the words “Section 29a, paragraph 1, letters a), b) and d) and Section 29l, except for the delivery of the order imposing the sanction and its requirements”.

87. In Section 33, paragraph 4 reads:

"(4) If an operator of a basic service falls under several sectors or if it falls under different central authorities, the scope of competence under this Act shall be determined by the Authority on the basis of prior consultation with the operator of a basic service concerned and the central authority.".

88. The footnote to reference 34 reads:

" 34) Section 7 of Act No. 500/2022 Coll.".

89. Section 33 is supplemented by paragraph 6, which reads as follows:

"(6) The National Bank of Slovakia and the Authority shall conclude a written cooperation agreement on the basic framework for reporting and resolving cybersecurity incidents and on reporting on the status of cybersecurity at the National Bank of Slovakia.".

90. After Section 34a, Section 34b is inserted, which, including the title, reads as follows:

"§ 34b

Transitional provisions for amendments effective from 1 January 2025

(1) An operator of an essential service under this Act as amended until 31 December 2024 shall be deemed to be an operator of a critical essential service under this Act as amended from 1 January 2025.

(2) The Office may, by 31 December 2026, also on its own initiative, decide which of the persons referred to in paragraph 1 is not an operator of a critical essential service on the grounds that it does not meet the conditions under Section 18(1) as amended from 1 January 2025.

(3) A digital service provider under this Act as amended until 31 December 2024 shall be considered an operator of a basic service under this Act as amended from 1 January 2025.

(4) The Office may also decide on its own initiative by 31 December 2026 which of the persons referred to in paragraph 3 is not an operator of a basic service on the grounds that it does not meet the conditions under Section 17(1) as amended from 1 January 2025.

(5) The operator of the essential service pursuant to paragraph 1 may, until 31 December 2026, adopt and implement security measures pursuant to regulations effective from 1 January 2025, also by adopting and implementing security measures pursuant to regulations effective until 31 December 2024.

(6) The Office shall request compliance with the obligation pursuant to Section 21(3) by 17 January 2025 and shall send the data notified in this way to the extent pursuant to Section 21(3) to the European Union Agency for Cybersecurity.

security within 30 days from the date of their notification to the Authority.

(7) The operator of the basic service pursuant to paragraph 1 may perform until 31 December 2026 audit according to regulations effective until December 31, 2024.

(8) The operator of the essential service may ensure compliance with the obligation to conduct a cybersecurity audit for Category I and II networks and information systems, which would be required to be conducted in 2025 and 2026, by conducting a self-assessment through the unified cybersecurity information system. The self-assessment shall be conducted by the cybersecurity manager and the operator of the essential service shall deliver the result of the self-assessment to the Authority without delay after its completion.

(9) The operator of the basic service for Category I and II networks and information systems may, by the procedure set out in paragraph 8, fulfil the obligation to conduct a cybersecurity audit, which was required to be conducted in 2024, by 30 September 2025.”.

91. After Section 35, Section 36 is inserted, which, including the title, reads as follows:

"§ 36

Repealing provisions effective from 1 January 2025

The following are repealed:

1. Decree of the National Security Office No. 164/2018 Coll., which determines identification criteria of the service operated (basic service criteria),
2. Decree of the National Security Office No. 165/2018 Coll., which determines the identification criteria for individual categories of serious cyber security incidents and the details of reporting cyber security incidents.".

92. The words "operator of essential services" and "operators of essential services" in all forms are replaced throughout the text of the Act by the words "operator of essential services" in the relevant form.

93. Annexes Nos. 1 to 3 read as follows:

"Annex No. 1
to Act No. 69/2018 Coll.

SECTORS WITH HIGH CRITICALITY

Sector	Subsector	Entity type	Central authority	Note
1. Energy	a) electrical energy	**electricity companies** - any person who carries out at least one of the following activities: generation, transmission, distribution, supply or purchase of electricity and which is in responsible for business in connection with these activities and technical tasks or maintenance; however, it does not include end customers, who sell electricity to customers, including its resale	Ministry of Economy Slovak Republic	Act No. 541/2004 Coll. on the peaceful use of nuclear energy (Atomic Act) and on amendments and supplements to certain acts, as amended Act No. 251/2012 Coll. on Energy and on Amendments to Certain Acts, as amended Act No. 321/2014 Coll. on energy efficiency and on amendments and supplements to certain acts, as amended Decree of the Nuclear Regulatory Authority of the Slovak Republic No. 430/2011 Coll. on nuclear safety requirements as amended by Decree No. 103/2016 Coll. Decree of the Ministry of Economy of the Slovak Republic No. 358/2013 Coll., establishing the procedure and conditions for the implementation and operation of smart metering systems in the electric power industry, as amended by later regulations
		distribution system operators – any person responsible for the operation, maintenance and, where necessary, development of the distribution system in a given area and, where appropriate, the development of its interconnections with other systems and for ensuring the long-term ability of the system to meet reasonable demand for electricity distribution		
		transmission system operators - any person responsible for the operation, maintenance and development of the transmission system in a given area and, where appropriate, the development of its interconnections with other systems and for ensuring the long-term ability of the system to meet reasonable demand for the transmission of electricity		

Sector	Subsector	Entity type	Central authority	Note
		nominated electricity market operator - any market operator designated by the competent authority to perform tasks related to one day-ahead market coupling or one intraday market coupling		
		Market participant - any natural person or legal entity that buys, sells or generates electricity, mediates aggregation or is a demand response operator or energy storage services also through the submission of trading orders on one or more electricity markets, including regulatory energy markets		
		charging point operators, who are responsible for the management and operation of a charging point that provides a charging service to end-users, including in the name and on behalf of the mobility service provider		
		holders of permits pursuant to Section 5(3)(a) to (d) of Act No. 541/2004 Coll.		
	b) thermal energy	**heat producers and suppliers**	Ministry of Economy Slovak Republic	Act No. 657/2004 Coll. on thermal energy, as amended

Sector	Subsector	Entity type	Central authority	Note
	c) district heating and cooling	**a producer or supplier of thermal energy** in the form of steam, hot and warm water from a central production source through a network to multiple buildings or multiple locations for space or process heating **a producer or supplier of thermal energy** in the form of chilled liquids from a central production source through a network to multiple buildings or locations for cooling spaces or processes	Ministry of Economy Slovak Republic	Act No. 309/2009 Coll. on the promotion of renewable energy sources and highly efficient combined heat and power generation and on amendments and supplements to certain acts, as amended Act No. 657/2004 Coll. on thermal energy, as amended
	d) oil	**pipeline operators**	Ministry of Economy Slovak Republic	Act No. 372/2012 Coll. on State Material Reserves and on Amendments to Act No. 25/2007 Coll. on electronic toll collection for the use of designated sections of roadways and on amendments and supplements to certain acts, as amended by Act No. 218/2013 Coll. Act No. 218/2013 Coll. on emergency stocks of oil and oil products and on addressing the oil emergency and on amending and supplementing certain acts, as amended by later regulations
		operators of facilities for the extraction, refining and processing of oil, its storage and transportation		
		central stock management entities - an organization to which the authority to act is delegated to procure, maintain or sell oil stocks, including emergency stocks and special stocks	Administration of State Material Reserves of the Slovak Republic	
	e) gas	**supplier companies -** any person who sells, including reselling, natural gas, including LNG, to customers	Ministry of Economy Slovak Republic	Act No. 251/2012 Coll. on Energy and on Amendments to Certain Acts, as amended

Sector	Subsector	Entity type	Central authority	Note
		Distribution network operators - any person who carries out distribution and is responsible for the operation, maintenance and, if necessary, development of the distribution network in a given area, or its interconnection with other networks and for ensuring the long-term ability of the network to meet reasonable demand after natural gas distribution		Act No. 321/2014 Coll. on energy efficiency and on amendments and supplements to certain acts, as amended
		transmission system operators - any person who carries out transmission and is responsible for the operation, security maintenance and, if necessary, development of the transmission network in the area, or its interconnection with other networks and for ensuring long-term the ability of the network to meet reasonable demand for natural gas transportation		
		storage facility operators - any person who carries out storage and is responsible for the operation of the storage facility		
		LNG facility operators - any person who carries out the liquefaction of natural gas or the import, unloading and LNG regasification and is responsible for the operation of the LNG facility		

Sector	Subsector	Entity type	Central authority	Note
		gas companies - any person carrying out at least one of the following activities: extraction, transportation, distribution, supply, purchase or storage of natural gas, including LNG, which is responsible for commercial tasks, technical tasks or maintenance in connection with with these activities, but does not include end customers		
		operators of natural gas refining and processing facilities		
	f) hydrogen	**operators of hydrogen production, storage and transport facilities**	Ministry of Economy Slovak Republic	Act No. 309/2009 Coll. on the support of renewable energy sources and highly efficient combined heat and power generation and on amendments and supplements to certain acts, as amended
2. Transportation	a) air transport	**air carriers -** an air transport undertaking with a valid operating licence or its equivalent	Ministry of Transport Slovak Republic	Act No. 143/1998 Coll. on Civil Aviation (Aviation Act) and on amendments and supplements to certain acts, as amended
		airport operator - an entity which, in conjunction with or without other activities, as the case may be, has the objective, under national laws, regulations or contracts, of administering and managing the infrastructure of an airport or a network of airports and of coordinating and controlling the activities of the individual operators at the airports or networks concerned, airports, including major airports, and entities operating auxiliary facilities located at airports		Regulation (EC) No 1072/2009 of the European Parliament and of the Council 549/2004 of 10 March 2004 laying down the framework for the creation of the single European sky (Framework Regulation) (OJ L 96, 31.3.2004) as amended Regulation (EC) No 1008/2008 of the European Parliament and of the Council of 24 September 2008 on common rules for the operation of air services in the Community (recast) (OJ L 111, 24.9.2008, p. 1). EU L 293, 31.10.2008) as amended Commission Regulation (EU) No 139/2014 of 12 February

Sector	Subsector	Entity type	Central authority	Note
		operators providing air traffic control (ATC) services such as a service provided for the purpose of: a) preventing collisions: - between aircraft and - in the operating area between aircraft and obstacles; and b) expediting and maintaining the orderly flow of air traffic		2014 laying down requirements and administrative procedures relating to aerodromes pursuant to Regulation (EC) No 216/2008 of the European Parliament and of the Council (OJ L 44, 14.2.2014) as amended Commission Implementing Regulation (EU) 2015/1998 of 5 November 2015 laying down detailed measures for the implementation of the common basic standards on aviation security (OJ L 299, 14.11.2015) as amended Commission Implementing Regulation (EU) 2017/373 of 1 March 2017 laying down common requirements for providers of air traffic management/air navigation services and for other air traffic management network functions, repealing Regulation (EC) No 482/2008, Implementing Regulations (EU) No 1034/2011, (EU) No 1035/2011 and (EU) 2016/1377 and amending Regulation (EU) No 677/2011 (OJ L 62, 8.3.2017) as amended Regulation (EU) 2018/1139 of the European Parliament and of the Council of 4 July 2018 on common rules in the field of civil aviation, establishing a European Union Aviation Safety Agency, and amending Regulations (EC) No 2111/2005, (EC) No 1008/2008, (EU) No 1139/2011 of the European Parliament and of the Council 996/2010, (EU) No. 376/2014 and Directives 2014/30/EU and 2014/53/EU of the European Parliament and of the Council and repealing Regulations (EC) No. 552/2004 and (EC) No. 216/2008 of the European Parliament and of the Council and

Sector	Subsector	Entity type	Central authority	Note
				Council Regulation (EEC) No 3922/91 (OJ L 212, 22.8.2018) as amended Commission Delegated Regulation (EU) 2022/1645 of 14 July 2022 laying down rules for the application of Regulation (EU) 2018/1139 of the European Parliament and of the Council with regard to information security risk management requirements with a potential impact on aviation safety for organisations subject to Commission Regulations (EU) No 748/2012 and (EU) No 139/2014, and amending Commission Regulations (EU) No 748/2012 and (EU) No 139/2014 (OJ L 248, 26.9.2022) Commission Implementing Regulation (EU) 2023/1769 of 12 September 2023 laying down technical requirements and administrative procedures for the approval of organisations involved in the design or production of air traffic management/air navigation services systems and constituents and amending Implementing Regulation (EU) 2023/203 (OJ L 228, 15.9.2023)

Sector	Subsector	Entity type	Central authority	Note
	b) rail transport	**infrastructure manager -** any body or undertaking responsible in particular for the establishment, management and maintenance of a railway infrastructure including traffic management, security and signalling; manager function infrastructure on the network or part of the network may be entrusted to different authorities or undertakings	Ministry of Transport Slovak Republic	Act of the National Council of the Slovak Republic No. 258/1993 Coll. on the Railways of the Slovak Republic, as amended by later regulations Act No. 513/2009 Coll. on Railways and on Amendments to Certain Acts, as amended Act No. 514/2009 Coll. on railway transport, as amended Act No. 332/2023 Coll. on public passenger transport and on amendments and supplements to certain acts
		railway companies - any public undertaking or private undertaking whose main activity is providing services to ensure the carriage of goods or passengers by rail, with the undertaking providing traction; this also includes undertakings which they only provide traction; this does not apply to undertakings providing traction for trolleybus and tram tracks, including operators of service facilities - any public entity or private entity responsible for the administration one or more service facilities or for the provision of one or more key services to railway undertakings		

Sector	Subsector	Entity type	Central authority	Note
	c) water transport	**companies operating inland, maritime and coastal passenger and cargo shipping ,** excluding the individual vessels operated by these companies	Ministry of Transport Slovak Republic	Act No. 338/2000 Coll. on inland navigation and on amendments and supplements to certain acts, as amended Act No. 435/2000 Coll. on Maritime Navigation, as amended Act No. 332/2023 Coll. on public passenger transport and on amendments and supplements to certain acts Regulation of the Government of the Slovak Republic No. 67/2007 Coll. on the monitoring and information system for maritime navigation, as amended
		port operators - as any designated part of land and water with borders defined by a Member State European Union, where a port is located, including the plants and installations designed to facilitate the operation of commercial waterborne transport; including their port facilities where there is mutual contact between the vessel and the port; this includes areas such as berths, service berths, moorings and quays, service berths and approaches from the sea, as appropriate, and entities operating activities and facilities within the port		
		operators of navigation and operational services - as a service intended to increase the safety and efficiency of navigation and to protect the environment, which is capable of interacting with traffic and can respond to traffic situations arising in the area of navigation and operational services		

Sector	Subsector	Entity type	Central authority	Note
	d) road transport	**road authorities responsible for the control of road traffic management –** any public authority responsible for planning, control or management of roads falling within its territorial jurisdiction, with the exception of public entities for which traffic management or the operation of intelligent transport systems is an insignificant part of their overall activity	Ministry of Transport Slovak Republic	Act No. 135/1961 Coll. on Roads (Road Act), as amended Act No. 8/2009 Coll. on road traffic and on amendments and supplements to certain acts, as amended Act No. 513/2009 Coll. on Railways and on Amendments to Certain Acts, as amended Act No. 249/2011 Coll. on the management of road safety and on amendments and supplements to certain acts, as amended Act No. 317/2012 Coll. on intelligent transport systems in road transport and on amendments and supplements to certain acts
		operators of intelligent transport systems, in which information and communication technologies are applied in the field of road transport, including infrastructure, vehicles and users, and in the field of traffic management and mobility management, as well as for interfaces with other modes of transport		
3. Finance	a) banking	**credit institutions** as defined in point (1) of Article 4 of Regulation (EU) No 575/2013, as amended	Ministry of Finance Slovak Republic	Regulation (EU) No 648/2012 of the European Parliament and of the Council of 4 July 2012 on OTC derivatives, central counterparties and trade repositories (OJ L 201, 27.7.2012), as amended (hereinafter referred to as 'Regulation (EU) No 648/2012, as amended') Regulation (EU) No 575/2013 of the European Parliament and of the Council of 26 June 2013 on prudential requirements for credit institutions and investment firms and amending Regulation (EU) No 648/2012 (OJ L 176, 27.6.2013) as amended (hereinafter referred to as the
	b) financial market infrastructure	**operators business locations**		
		central counterparties pursuant to Article 2, first point, of Regulation (EU) No. 648/2012, as amended - a legal entity that enters among the counterparties to contracts traded on one or more financial markets and becomes a buyer to to all sellers and sellers to all buyers		

Sector	Subsector	Entity type	Central authority	Note
	c) public finance management systems	**operators of systems** whose failure or damage would endanger the economic function of the state pursuant to Sections 6 and 17 of Act No. 291/2002 on the State Treasury, as amended and pursuant to Section 4 of Act No. 35/2019 Coll. on Financial Administration, as amended		"Regulation (EU) No 575/2013 as amended") Act No. 483/2001 Coll. on banks and on amendments and supplements to certain acts, as amended Act No. 566/2001 Coll. on securities and investment services and on amendments and supplements to certain acts (Securities Act), as amended Act No. 291/2002 Coll. on the State Treasury and on amendments and supplements to certain laws, as amended Act No. 429/2002 Coll. on the Stock Exchange, as amended Act No. 747/2004 Coll. on financial market supervision and on amendments and supplements to certain acts, as amended Act No. 492/2009 Coll. on payment services and on amendments and supplements to certain acts, as amended Act No. 371/2014 Coll. on resolution of crisis situations in the financial market and on amendments and supplements to certain acts, as amended Act No. 35/2019 Coll. on financial administration and on amendments and supplements to certain acts, as amended
4. Healthcare		**healthcare provider -** any person or any other entity that legally provides healthcare	Ministry of Health Slovak Republic	Regulation (EU) 2022/123 of the European Parliament and of the Council of 25 January 2022 on a strengthened role of the European Medicines Agency in terms of

Sector	Subsector	Entity type	Central authority	Note
		care in the territory of a Member State of the European Union		crisis preparedness and management in the field of medicinal products and medical devices (OJ L 20, 31.1.2022) as amended (hereinafter referred to as "Regulation (EU) 2022/123 as amended")
		entity providing a service having a significant impact on the protection, promotion and development of public health		Act No. 578/2004 Coll. on healthcare providers, healthcare professionals, professional organizations in healthcare and on amendments and supplements to certain acts, as amended
		National Health Information Center as the administrator of the database of the national health information system (national health administrative registers, national health registers, surveys of events characterizing the health status of the population, statistical reports in the health sector, data from the insured person's account, data from the register of birth records, register of insurance relationships of natural persons for the purpose of confirming temporary incapacity for work)		Act No. 581/2004 Coll. on health insurance companies, healthcare supervision and on amendments and supplements to certain acts, as amended Act No. 355/2007 Coll. on the protection, promotion and development of public health and on amendments and amendments to certain laws as amended Act No. 362/2011 Coll. on medicines and medical devices and on amendments and supplements to certain acts, as amended
		entity supervising public health insurance and the provision of healthcare		Act No. 153/2013 Coll. on the National Health Information System and on amendments and supplements to certain acts, as amended
		entity performing state supervision in the field of pharmacy and drug precursors, control over the production and wholesale distribution of medicines and medical devices		

Sector	Subsector	Entity type	Central authority	Note
		reference laboratories of the European Union, to provide support to national reference laboratories for the promotion of good practices and voluntary harmonisation of diagnostics, testing methods and the use of certain tests by the Member States of the European Union in order to achieve a uniform way in which the Member States of the European Union carry out surveillance, notification and reporting of diseases		
		an entity carrying out activities in the research and development of medicinal products, which is defined by a special legal regulation as: (a) any substance or combination of substances with properties suitable for treating or preventing disease in humans, or (b) any substance or combination of substances which may be used in or administered to human beings with a view to restoring, modifying or modifying physiological functions by its pharmacological, immunological or metabolic action or for the purpose of making a medical diagnosis		
		manufacturer of basic pharmaceutical products and pharmaceutical preparations listed in Section C, Division 21 of the statistical classification economic activities36) SK NACE Rev. 2		

Sector	Subsector	Entity type	Central authority	Note
		manufacturer of medical devices considered critical in a public health emergency within the meaning of Article 22 of Regulation (EU) 2022/123, as amended		
		health insurance company		
5. Water and atmosphere	a) drinking water	**suppliers and distributors of water** for drinking, cooking, food preparation or other domestic purposes, regardless of its origin and whether it was supplied from a distribution network, tanker or in bottles or containers; with the exception of distributors for whom the distribution of water is only part of their overall activity in the field of distribution of other commodities and goods, which is not considered an essential service	Ministry of the Environment of the Slovak Republic	Act No. 442/2002 Coll. on public water supply and public sewerage systems and on amendments to Act No. 276/2001 Coll. on regulation in network sectors, as amended Act No. 364/2004 Coll. on Waters and on Amendments to the Act of the Slovak National Council No. 372/1990 Coll. on Offences, as amended (Water Act), as amended Decree of the Ministry of the Environment of the Slovak Republic No. 636/2004 Coll., which establishes requirements for the quality of raw water and for monitoring the quality of water in public water supplies, as amended by Decree No. 354/2023 Coll. Decree of the Ministry of Health of the Slovak Republic No. 91/2023, which establishes indicators and limit values for drinking water quality and hot water quality, the procedure for monitoring drinking water, risk management of the drinking water supply system and risk management of house distribution systems
	b) wastewater - **enterprises** engaged in the collection, disposal or treatment of municipal wastewater,		Ministry of the Environment of the Slovak Republic	Act No. 442/2002 Coll. on public water supply and public sewerage and on amendments and supplements to the Act

Sector	Subsector	Entity type	Central authority	Note
		household waste water or industrial waste water, with the exception of undertakings for which the collection, disposal or treatment of municipal waste water, household waste water or industrial waste water is an insignificant part of their overall activity		No. 276/2001 Coll. on regulation in network industries, as amended Act No. 364/2004 Coll. on Waters and on Amendments to Act of the Slovak National Council No. 372/1990 Coll. on offences, as amended (Water Act), as amended Act No. 201/2009 Coll. on the State Hydrological Service and the State Meteorological Service, as amended
	c) meteorological service	**administrators and operators of the state hydrological network**		
		administrators and operators of the state meteorological network		
	d) water structures	**enterprises** operating water structures, their components or parts thereof that enable special water use or other water management		
6.1 Digital infrastructure		**Internet connection providers***	Ministry of Transport Slovak Republic	Act No. 452/2021 Coll. on electronic communications, as amended
		content delivery network providers*		
		providers of public electronic communications networks*		
		providers of publicly available electronic communications services*		
6.2 Digital infrastructure		**service providers DNS, except for root nameservers** **servers**	National Security Agency	Act No. 215/2004 Coll. on the protection of classified information and on amendments and supplements to certain acts, as amended

Sector	Subsector	Entity type	Central authority	Note
		TLD administrators		Act No. 272/2016 Coll. on trust services for electronic transactions in the internal market and on amendments to certain acts (Act on Trust Services), as amended Act No. 69/2018 Coll. on Cybersecurity and on Amendments to Certain Acts, as amended
		private sector cloud computing service providers*		
		private sector data center service providers*		
		trusted service providers		
		network administrators and operators and information systems relating to classified information		
		administrator and operator information system of the Office for Public Regulated Services		
		third party		
6.3 Digital infrastructure		**network administrators and operators and information systems related to the security of the Slovak Republic**	Ministry of the Interior Slovak Republic	
		cloud computing service providers*		
		data center service providers*		
6.4 Digital infrastructure		**administrators and network operators and information systems related to defense assurance Slovak Republic**	Ministry of Defense Slovak Republic	

Sector	Subsector	Entity type	Central authority	Note
7. ICT Service Management (Business-to-Business)		**managed service providers***	National Security Agency	
		managed security service providers*		
8.1 Public administration		**public administration entities at the level of the central state administration body and other state bodies with nationwide jurisdiction**	Ministry of the Interior Slovak Republic	Act No. 302/2001 Coll. on self-government of higher territorial units (Act on self-governing regions), as amended Act No. 575/2001 Coll. on the organization of government activities and the organization of central state administration, as amended Act No. 596/2003 Coll. on state administration in education and school self-government and on amendments and supplements to certain acts, as amended Act No. 355/2007 Coll. on the protection, promotion and development of public health and on amendments and supplements to certain acts, as amended
		public administration entities at the regional level, except in the area of financial administration		
8.2 Public administration		**public administration entities at the level of the central state administration body and another state body with nationwide competence in the area of financial administration**	Ministry of Finance Slovak Republic	Act No. 35/2019 Coll. on financial administration and on amendments and supplements to certain acts, as amended
		public administration entities at the regional level for the area of financial management		

Sector	Subsector	Entity type	Central authority	Note
8.3 Public administration		**administrators and operators of public administration information systems** supporting public administration services, services in the public interest and public services pursuant to Act No. 95/2019 Coll.	Ministry of Investments, Regional Development and Informatization of the Slovak Republic	Act No. 95/2019 Coll. on information technologies in public administration and on amendments and supplements to certain acts, as amended
9.Space		**operators of terrestrial infrastructure** owned, managed and operated by Member States of the European Union or private entities contributing to the provision of space services, with the exception of providers of public electronic communications networks	Ministry of the Interior Slovak Republic	Act No. 452/2021 Coll. on electronic communications, as amended

Explanations:
* **An Internet interconnection node** is a network device that enables the interconnection of more than two independent autonomous networks (autonomous systems), primarily for the purpose of mediating an Internet data stream that connects only autonomous systems and that does not require the Internet data stream between any pair of participating autonomous systems to pass through any third autonomous system, alter such data stream, or otherwise interfere with it.

Cloud computing is a digital service that enables on-demand management and remote broadband access to a scalable and flexible set of shareable computing resources, even if those resources are located in multiple locations.

A data center service is a service that includes structures or groups of structures dedicated to the centralized location, interconnection and operation of IT and network equipment providing data storage, processing and transport services, together with all facilities and infrastructures for electrical power distribution and environmental control.

A content delivery network is a network of geographically distributed servers to ensure high availability, accessibility, or rapid delivery of digital content and services to Internet users on behalf of content and service providers.

A public electronic communications network is an electronic communications network that is used wholly or mainly for the provision of publicly available electronic communications services that support the transmission of information between network endpoints.
An electronic communications service is a service normally provided for remuneration over electronic communications networks, which includes, with the exception of services providing content or exercising editorial control over content transmitted over electronic communications networks and services (internet access service, interpersonal communications service, services consisting wholly or mainly of the conveyance of signals, such as transmission services used for the provision of M2M communications services and for broadcasting).
A managed service provider is an entity that provides services related to the installation, management, operation or maintenance of ICT products, networks, infrastructure, applications or any other networks and information systems in the form of assistance or active management carried out either on-site or remotely.
A managed security service provider is a managed services provider that performs or provides assistance for activities related to cyber risk management.

The footnote to reference 36 reads: " 36)

Decree of the Statistical Office of the Slovak Republic No. 306/2007 Coll., issuing the Statistical Classification of Economic Activities.".

Annex No. 2
to Act No. 69/2018 Coll.

OTHER CRITICAL SECTORS

Sector	Subsector	Entity type	Central authority	Note
1. Postal and courier services		**postal company** that provides one or more postal services or postal payment services pursuant to the Postal Services Act	Ministry of Transport Slovak Republic	Act No. 324/2011 Coll. on postal services and on amendments and supplements to certain acts, as amended
2. Waste management		**an entrepreneur who,** when purchasing and subsequently selling waste, acts in his own name and on his own responsibility, including a trader who does not have physical possession of the waste, with the exception of undertakings for which waste management is not the main economic activity	Ministry of the Environment of the Slovak Republic	Act No. 79/2015 Coll. on waste and on amendments and supplements to certain acts, as amended Decree of the Ministry of the Environment of the Slovak Republic No. 366/2015 Coll. on the registration obligation and reporting obligation, as amended
		intermediary - an entrepreneur who organises the recovery of waste or the disposal of waste on behalf of other persons, including an intermediary who does not physically hold the waste, with the exception of undertakings for which waste management does not constitute the main economic activity		Decree of the Ministry of the Environment of the Slovak Republic No. 371/2015 Coll., implementing certain provisions of the Waste Act, as amended
		waste carrier - an entrepreneur who carries out waste transport for third-party use or for his own use; waste transport is understood as the movement of waste, with the exception of enterprises for which waste management is not the main economic activity		
3. Production and distribution of chemicals		suppliers, manufacturers, importers	Ministry of Economy Slovak Republic	Act No. 67/2010 Coll. on the conditions for placing chemical substances and chemical mixtures on the market and on the amendment

Sector	Subsector	Entity type	Central authority	Note
				and amendments to certain acts (Chemical Act) as amended
4. Food production, processing and distribution		food businesses engaged in wholesale distribution and industrial production and processing	Ministry of Agriculture and Rural Development Slovak Republic	Act of the National Council of the Slovak Republic No. 152/1995 Coll. on Food, as amended
5. Production	a) manufacture of medical devices and in vitro diagnostic medical devices b) manufacture of	manufacturer of the medical device or authorized representative	Ministry of Health Slovak Republic	Act No. 362/2011 Coll. on medicines and medical devices and on amendments and supplements to certain acts, as amended Act No. 346/2013 Coll. on the restriction of the use of certain hazardous substances in electrical and electronic equipment and amending Act No. 223/2001 Coll. on waste and on amendments and supplements to certain acts, as amended, as amended regulations
	computer, electronic and optical products	manufacturer of computer, electronic and optical products listed in Section C, Division 26 of the statistical classification economic activities36) SK NACE Rev. 2	Ministry of Economy Slovak Republic	
	c) production of electrical equipment	manufacturer of electrical equipment listed in Section C, Division 27 of the statistical classification economic activities36) SK NACE Rev. 2	Ministry of Economy Slovak Republic	
	d) manufacture of machinery and equipment nec	manufacturer of machinery and equipment n.e.c. listed in Section C, Division 28 of the statistical classification economic activities36) SK NACE Rev. 2	Ministry of Economy Slovak Republic	
	e) manufacture of motor vehicles, semi-trailers and trailers	manufacturer of motor vehicles, semi-trailers and trailers listed in the section C Division 29 Statistical Classification economic activities36) SK NACE Rev. 2	Ministry of Economy Slovak Republic	
	f) production of other means of transport	manufacturer of other means of transport listed in Section C, Division 30 of the statistical classification economic activities36) SK NACE Rev. 2	Ministry of Economy Slovak Republic	
6. Digital service providers*		online marketplace providers*	National Security Agency	Act No. 69/2018 Coll. on Cybersecurity and on Amendments

Sector	Subsector	Entity type	Central authority	Note
		Internet search engine providers		and amendments to certain laws as amended
		social network service platform providers*		
7. Research		research organizations*	Ministry of Education, Research, Development and Youth of the Slovak Republic	Act No. 243/2017 Coll. on public research institutions and on amendments and supplements to certain acts, as amended by Act No. 346/2021 Coll.

Explanations:
* **A digital service** is any service provided by an information society that is normally provided for a fee. remuneration, remotely, electronically and based on the individual request of the recipient of the services.
Remotely means that the service is provided without both parties being present at the same time.
By electronic means means that the service is sent from the place of origin and received at the place of destination by means of electronic equipment designed for processing (including digital compression) and storing data and is entirely transmitted, transmitted and received by wire, by radio waves, by optical means or by other electromagnetic means.
Based on the individual request of the service recipient means that the service is provided through the transfer of data at the individual request.
An online marketplace is a service that, using software, including a website, part of a website or an application, operated by or on behalf of a trader, enables consumers to conclude distance contracts with other traders or with consumers.
A social network service platform is a platform that enables end users to connect, share, discover and communicate with each other across multiple devices, particularly through chats, posts, videos and recommendations.

A research organization is an entity whose main objective is to conduct applied research or experimental development with the aim of using the results of this research for commercial purposes, but which does not include educational institutions.

Annex No. 3
to Act No. 69/2018 Coll.

LIST OF LEGALLY BINDING ACTS OF THE EUROPEAN UNION ADOPTED

Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972 and repealing Directive (EU) 2016/1148 (NIS Directive 2) (OJ L 333, 27.12.2022). “.

Article II

Act No. 455/1991 Coll. on Trade Licensing (Trade Licensing Act) as amended by Act No. 231/1991 Coll., Act No. 600/1992 Coll., Act No. 231/1992 Coll., Act of the National Council of the Slovak Republic No. 132/1994 Coll., Act of the National Council of the Slovak Republic No. 200/1995 Coll., Act of the National Council of the Slovak Republic No. 233/1995 Coll., Act of the National Council of the Slovak Republic No. 216/1996 Coll., Act of the National Council of the Slovak Republic No. 123/1996 Coll., Act of the National Council of the Slovak Republic No. 222/1996 Coll., Act of the National Council of the Slovak Republic No. 164/1996 Coll., Act of the National Council of the Slovak Republic No. 289/1996 Coll., Act of the National Council of the Slovak Republic No. 290/1996 Coll., Act No. 288/1997 Coll., Act No. 379/1997 Coll., Act No. 76/1998 Coll., Act No. 144/1998 Coll., Act No. 140/1998 Coll., Act No. 129/1998 Coll., Act No. 179/1998 Coll., Act No. 194/1998 Coll., Act No. 161/1998 Coll., Act No. 143/1998 Coll., Act No. 126/1998 Coll., Act No. 178/1998 Coll., Act No. 263/1999 Coll., Act No. 264/1999 Coll., Act No. 119/2000 Coll., Act No. 142/2000 Coll., Act No. 236/2000 Coll., Act No. 238/2000 Coll., Act No. 268/2000 Coll., Act No. 338/2000 Coll., Act No. 223/2001 Coll., Act No. 279/2001 Coll., Act No. 488/2001 Coll., Act No. 554/2001 Coll., Act No. 279/2001 Coll., Act No. 261/2001 Coll., Act No. 284/2001 Coll., Act No. 506/2002 Coll., Act No. 279/2001 Coll., Act No. 245/2003 Coll., Act No. 219/2003 Coll., Act No. 423/2003 Coll., Act No. 515/2003 Coll., Act No. 602/2003 Coll., Act No. 190/2003 Coll., Act No. 586/2003 Coll., Act No. 279/2001 Coll., Act No. 347/2004 Coll., Act No. 350/2004 Coll., Act No. 365/2004 Coll., Act No. 420/2004 Coll., Act No. 533/2004 Coll., Act No. 544/2004 Coll., Act No. 578/2004 Coll., Act No. 624/2004 Coll., Act No. 656/2004 Coll., Act No. 650/2004 Coll., Act No. 725/2004 Coll., Act No. 8/2005 Coll., Act No. 93/2005 Coll., Act No. 331/2005 Coll., Act No. 340/2005 Coll., Act No. 351/2005 Coll., Act No. 470/2005 Coll., Act No. 567/2005 Coll., Act No. 491/2005 Coll., Act No. 473/2005 Coll., Act No. 555/2005 Coll., Act No. 126/2006 Coll., Act No. 124/2006 Coll., Act No. 17/2007 Coll., Act No. 99/2007 Coll., Act No. 193/2007 Coll., Act No. 218/2007 Coll., Act No. 358/2007 Coll., Act No. 358/2007 Coll., Act No. 577/2007 Coll., Act No. 112/2008 Coll., Act No. 448/2008 Coll., Act No. 445/2008 Coll., Act No. 492/2009 Coll., Act No. 186/2009 Coll., Act No. 129/2010 Coll., Act No. 136/2010 Coll., Act No. 129/2010 Coll., Act No. 556/2010 Coll., Act No. 249/2011 Coll., Act No. 362/2011 Coll., Act No. 392/2011 Coll., Act No. 324/2011 Coll., Act No. 395/2011 Coll., Act No. 568/2009 Coll., Act No. 136/2010 Coll., Act No. 251/2012 Coll., Act No. 321/2012 Coll., Act No. 351/2012 Coll., Act No. 447/2012 Coll., Act No. 314/2012 Coll., Act No. 39/2013 Coll., Act No. 94/2013 Coll., Act No. 95/2013 Coll., Act No. 218/2013 Coll., Act No. 180/2013 Coll., Act No. 1/2014 Coll., Act No. 35/2014 Coll., Act No. 58/2014 Coll., Act No. 182/2014 Coll., Act No. 182/2014 Coll., Act No. 321/2014 Coll., Act No. 399/2014 Coll., Act No. 333/2014 Coll., Act No. 128/2015 Coll., Act No. 219/2014 Coll., Act No. 266/2015 Coll., Act No. 272/2015 Coll., Act No. 274/2015 Coll., Act No. 331/2015 Coll., Act No. 387/2015 Coll., Act No. 79/2015 Coll., Act No. 77/2015 Coll., Act No. 348/2015 Coll., Act No. 278/2015 Coll., Act No. 440/2015 Coll., Act No. 412/2015 Coll., Act No. 89/2016 Coll., Act No. 91/2016 Coll., Act No. 125/2016 Coll., Act No. 276/2017 Coll., Act No. 289/2017 Coll.,

Act No. 292/2017 Coll., Act No. 87/2018 Coll., Act No. 56/2018 Coll., Act No. 106/2018 Coll., Act No. 157/2018 Coll., Act No. 177/2018 Coll., Act No. 216/2018 Coll., Act No. 170/2018 Coll., Act No. 276/2017 Coll., Act No. 177/2018 Coll., Act No. 9/2019 Coll., Act No. 139/2019 Coll., Act No. 221/2019 Coll., Act No. 371/2019 Coll., Act No. 356/2019 Coll., Act No. 6/2020 Coll., Act No. 476/2019 Coll., Act No. 73/2020 Coll., Act No. 198/2020 Coll., Act No. 390/2019 Coll., Act No. 279/2020 Coll., Act No. 75/2021 Coll., Act No. 261/2021 Coll., Act No. 500/2021 Coll., Act No. 249/2022 Coll., Act No. 256/2022 Coll., Act No. 114/2022 Coll., Act No. 8/2023 Coll., Act No. 146/2023 Coll., Act No. 309/2023 Coll., Act No. 205/2023 Coll., Act No. 205/2023 Coll., Act No. 106/2024 Coll., Act No. 161/2024 Coll., Act No. 248/2024 Coll. and Act No. 292/2024 Coll. are amended as follows:

1. The footnote to reference 36cb reads:

" 36cb) Section 12, paragraph 4, letter a) of Act No. 192/2023 Coll. on the criminal record and on amendments and supplements to certain acts.".

2. In Annex No. 2 Related Trades, in group 214 Other, the trade with serial number 99 is added, which reads:

"

Ref. no.	Trade	Certificate of competency	Note	List
99.	Certified Cybersecurity Auditor	Cybersecurity Auditor Certificate	Section 29, paragraph 3 of Act No. 69/2018 Coll. on Cybersecurity and on Amendments to Certain Acts, as amended	

"

Article III

Act of the National Council of the Slovak Republic No. 145/1995 Coll. on Administrative Fees as amended by Act of the National Council of the Slovak Republic No. 123/1996 Coll., Act of the National Council of the Slovak Republic No. 224/1996 Coll., Act No. 70/1997 Coll., Act No. 1/1998 Coll., Act No. 232/1999 Coll., Act No. 3/2000 Coll., Act No. 142/2000 Coll., Act No. 211/2000 Coll., Act No. 468/2000 Coll., Act No. 553/2001 Coll., Act No. 96/2002 Coll., Act No. 118/2002 Coll., Act No. 215/2002 Coll., Act No. 237/2002 Coll., Act No. 418/2002 Coll., Act No. 457/2002 Coll., Act No. 465/2002 Coll., Act No. 477/2002 Coll., Act No. 480/2002 Coll., Act No. 190/2003 Coll., Act No. 217/2003 Coll., Act No. 245/2003 Coll., Act No. 450/2003 Coll., Act No. 469/2003 Coll., Act No. 583/2003 Coll., Act No. 5/2004 Coll., Act No. 199/2004 Coll., Act No. 204/2004 Coll., Act No. 347/2004 Coll., Act No. 382/2004 Coll., Act No. 434/2004 Coll., Act No. 533/2004 Coll., Act No. 541/2004 Coll., Act No. 572/2004 Coll., Act No. 578/2004 Coll., Act No. 581/2004 Coll., Act No. 633/2004 Coll., Act No. 653/2004 Coll., Act No. 656/2004 Coll., Act No. 725/2004 Coll., Act No. 5/2005 Coll., Act No. 8/2005 Coll., Act No. 15/2005 Coll., Act No. 93/2005 Coll., Act No. 171/2005 Coll., Act No. 308/2005 Coll., Act No. 331/2005 Coll., Act No. 341/2005 Coll., Act No. 342/2005 Coll., Act No. 468/2005 Coll., Act No. 473/2005 Coll., Act No. 491/2005 Coll., Act No. 538/2005 Coll., Act No. 558/2005 Coll., Act No. 572/2005 Coll., Act No. 573/2005 Coll., Act No. 610/2005 Coll., Act No. 14/2006 Coll., Act No. 15/2006 Coll., Act No. 24/2006 Coll., Act No. 117/2006 Coll., Act No. 124/2006 Coll., Act No. 126/2006 Coll., Act No. 224/2006 Coll., Act No. 342/2006 Coll., Act No. 672/2006 Coll., Act No. 693/2006 Coll., Act No. 21/2007 Coll., Act No. 43/2007 Coll., Act No. 95/2007 Coll., Act No. 193/2007 Coll., Act No. 220/2007 Coll., Act No. 279/2007 Coll., Act No. 295/2007 Coll., Act No. 309/2007 Coll., Act No. 342/2007 Coll., Act No. 343/2007 Coll., Act No. 344/2007 Coll., Act No. 355/2007 Coll., Act No. 358/2007 Coll., Act No. 359/2007 Coll., Act No. 460/2007 Coll., Act No. 517/2007 Coll., Act No. 537/2007 Coll., Act No. 548/2007 Coll., Act No. 571/2007 Coll., Act No. 577/2007 Coll.,

Act No. 647/2007 Coll., Act No. 661/2007 Coll., Act No. 92/2008 Coll., Act No. 112/2008 Coll., Act No. 167/2008 Coll., Act No. 214/2008 Coll., Act No. 264/2008 Coll., Act No. 405/2008 Coll., Act No. 408/2008 Coll., Act No. 451/2008 Coll., Act No. 465/2008 Coll., Act No. 495/2008 Coll., Act No. 514/2008 Coll., Act No. 8/2009 Coll., Act No. 45/2009 Coll., Act No. 188/2009 Coll., Act No. 191/2009 Coll., Act No. 274/2009 Coll., Act No. 292/2009 Coll., Act No. 304/2009 Coll., Act No. 305/2009 Coll., Act No. 307/2009 Coll., Act No. 465/2009 Coll., Act No. 478/2009 Coll., Act No. 513/2009 Coll., Act No. 568/2009 Coll., Act No. 570/2009 Coll., Act No. 594/2009 Coll., Act No. 67/2010 Coll., Act No. 92/2010 Coll., Act No. 136/2010 Coll., Act No. 144/2010 Coll., Act No. 514/2010 Coll., Act No. 556/2010 Coll., Act No. 39/2011 Coll., Act No. 119/2011 Coll., Act No. 200/2011 Coll., Act No. 223/2011 Coll., Act No. 254/2011 Coll., Act No. 256/2011 Coll., Act No. 258/2011 Coll., Act No. 324/2011 Coll., Act No. 342/2011 Coll., Act No. 363/2011 Coll., Act No. 381/2011 Coll., Act No. 392/2011 Coll., Act No. 404/2011 Coll., Act No. 405/2011 Coll., Act No. 409/2011 Coll., Act No. 519/2011 Coll., Act No. 547/2011 Coll., Act No. 49/2012 Coll., Act No. 96/2012 Coll., Act No. 251/2012 Coll., Act No. 286/2012 Coll., Act No. 336/2012 Coll., Act No. 339/2012 Coll., Act No. 351/2012 Coll., Act No. 439/2012 Coll., Act No. 447/2012 Coll., Act No. 459/2012 Coll., Act No. 8/2013 Coll., Act No. 39/2013 Coll., Act No. 40/2013 Coll., Act No. 72/2013 Coll., Act No. 75/2013 Coll., Act No. 94/2013 Coll., Act No. 96/2013 Coll., Act No. 122/2013 Coll., Act No. 144/2013 Coll., Act No. 154/2013 Coll., Act No. 213/2013 Coll., Act No. 311/2013 Coll., Act No. 319/2013 Coll., Act No. 347/2013 Coll., Act No. 387/2013 Coll., Act No. 388/2013 Coll., Act No. 474/2013 Coll., Act No. 506/2013 Coll., Act No. 35/2014 Coll., Act No. 58/2014 Coll., Act No. 84/2014 Coll., Act No. 152/2014 Coll., Act No. 162/2014 Coll., Act No. 182/2014 Coll., Act No. 204/2014 Coll., Act No. 262/2014 Coll., Act No. 293/2014 Coll., Act No. 335/2014 Coll., Act No. 399/2014 Coll., Act No. 40/2015 Coll., Act No. 79/2015 Coll., Act No. 120/2015 Coll., Act No. 128/2015 Coll., Act No. 129/2015 Coll., Act No. 247/2015 Coll., Act No. 253/2015 Coll., Act No. 259/2015 Coll., Act No. 262/2015 Coll., Act No. 273/2015 Coll., Act No. 387/2015 Coll., Act No. 403/2015 Coll., Act No. 125/2016 Coll., Act No. 272/2016 Coll., Act No. 342/2016 Coll., Act No. 386/2016 Coll., Act No. 51/2017 Coll., Act No. 238/2017 Coll., Act No. 242/2017 Coll., Act No. 276/2017 Coll., Act No. 292/2017 Coll., Act No. 293/2017 Coll., Act No. 336/2017 Coll., Act No. 17/2018 Coll., Act No. 18/2018 Coll., Act No. 49/2018 Coll., Act No. 52/2018 Coll., Act No. 56/2018 Coll., Act No. 87/2018 Coll., Act No. 106/2018 Coll., Act No. 108/2018 Coll., Act No. 110/2018 Coll., Act No. 156/2018 Coll., Act No. 157/2018 Coll., Act No. 212/2018 Coll., Act No. 215/2018 Coll., Act No. 284/2018 Coll., Act No. 312/2018 Coll., Act No. 346/2018 Coll., Act No. 9/2019 Coll., Act No. 30/2019 Coll., Act No. 150/2019 Coll., Act No. 156/2019 Coll., Act No. 158/2019 Coll., Act No. 211/2019 Coll., Act No. 213/2019 Coll., Act No. 216/2019 Coll., Act No. 221/2019 Coll., Act No. 234/2019 Coll., Act No. 356/2019 Coll., Act No. 364/2019 Coll., Act No. 383/2019 Coll., Act No. 386/2019 Coll., Act No. 390/2019 Coll., Act No. 395/2019 Coll., Act No. 460/2019 Coll., Act No. 165/2020 Coll., Act No. 198/2020 Coll., Act No. 310/2020 Coll., Act No. 128/2021 Coll., Act No. 149/2021 Coll., Act No. 259/2021 Coll., Act No. 287/2021 Coll., Act No. 310/2021 Coll., Act No. 372/2021 Coll., Act No. 378/2021 Coll., Act No. 395/2021 Coll., Act No. 402/2021 Coll., Act No. 404/2021 Coll., Act No. 455/2021 Coll., Act No. 490/2021 Coll., Act No. 500/2021 Coll., Act No. 532/2021 Coll., Act No. 540/2021 Coll., Act No. 111/2022 Coll., Act No. 114/2022 Coll., Act No. 122/2022 Coll., Act No. 180/2022 Coll., Act No. 181/2022 Coll., Act No. 246/2022 Coll., Act No. 249/2022 Coll., Act No. 253/2022 Coll., Act No. 264/2022 Coll., Act No. 265/2022 Coll., Act No. 266/2022 Coll., Act No. 325/2022 Coll., Act No. 408/2022 Coll., Act No. 427/2022 Coll., Act No. 429/2022 Coll., Act No. 59/2023 Coll., Act No. 109/2023 Coll., Act No. 119/2023 Coll., Act No. 135/2023 Coll., Act No. 146/2023 Coll., Act No. 183/2023 Coll., Act No. 192/2023 Coll., Act No. 287/2023 Coll., Act No. 293/2023 Coll., Act No. 309/2023 Coll., Act No. 331/2023 Coll., Act

No. 332/2023 Coll., Act No. 530/2023 Coll., Act No. 120/2024 Coll., Act No. 142/2024 Coll., Act No. 160/2024 Coll., Act No. 161/2024 Coll., Act No. 162/2024 Coll., Act No. 246/2024 Coll., Act No. 292/2024 Coll., Act No. 307/2024 Coll. and Act No. 364/2024 Coll. are supplemented as follows:

In the Annex to the Tariff of Administrative Fees, Part VII. Electronic Communications, item 105 is added, which reads: "Item 105

Submission of an application for recognition of a training centre27g) ..... 300 euros"

The footnote to reference 27g reads:

" 27g) Section 52a of Act No. 452/2021 Coll. as amended by Act No. 366/2024 Coll.".

Article IV

Act No. 143/1998 Coll. on Civil Aviation (Aviation Act) and on amendments and supplements to certain acts as amended by Act No. 37/2002 Coll., Act No. 136/2004 Coll., Act No. 544/2004 Coll., Act No. 479/2005 Coll., Act No. 11/2006 Coll., Act No. 278/2009 Coll., Act No. 513/2009 Coll., Act No. 136/2010 Coll., Act No. 241/2011 Coll., Act No. 404/2011 Coll., Act No. 402/2013 Coll., Act No. 58/2014 Coll., Act No. 299/2014 Coll., Act No. 91/2016 Coll., Act No. 305/2016 Coll., Act No. 177/2018 Coll., Act No. 213/2019 Coll., Act No. 90/2020 Coll., Act No. 312/2020 Coll., Act No. 354/2021 Coll., Act No. 187/2022 Coll., Act No. 205/2023 Coll. and Act No. 161/2024 Coll. are amended as follows:

1. In Section 34a, paragraphs 7, 8 and 10 are deleted.

The previous paragraph 9 is referred to as paragraph 7.

2. In Section 34a, paragraph 7, the words "and 7" are replaced by the words "and Section 34b".

3. After Section 34a, Section 34b is inserted, which, including the title, reads as follows:

"34b"

Training in civil aviation security and cybersecurity

(1) A person pursuant to a special regulation8l) is obliged to complete professional training in security protection.

(2) Security training shall be provided by a security training instructor on the basis of a certificate for providing training issued by the Ministry and within the scope of the course content approved by the Ministry, unless otherwise provided for in this Act. A legal entity is authorised to provide security training through an instructor pursuant to the first sentence. The Ministry shall determine the scope and conditions for providing security training in a decision.

(3) A certificate of completion of security training shall be issued by the instructor referred to in paragraph 2 who conducted the training. The Ministry shall publish a sample certificate of completion of security training on its website.

(4) The Ministry may determine additional requirements for individual qualifications of a member of the security personnel, including the obligation to demonstrate theoretical knowledge and practical skills for the performance of this activity by means of a professional competence examination, and shall publish them on its website. The examination committee for assessing the professional competence of a member of the security personnel shall be appointed and dismissed by the Ministry.

(5) A person pursuant to a special regulation8m) is obliged to complete professional training from cybersecurity in civil aviation.

(6) Training in cybersecurity in civil aviation is carried out by a lecturer
training in cybersecurity in civil aviation, who a) holds a certificate issued by a

person accredited under a special regulation8n) as
bodies certifying persons in the field of cybersecurity,

b) meets the conditions of the knowledge standard issued pursuant to a special regulation8o) and

c) conducts training in cybersecurity in civil aviation within the scope of the content
courses according to paragraph 7.

(7) The scope and content of courses and details of training in cybersecurity in civil aviation shall be regulated by the National Civil Aviation Security Program of the Slovak Republic.”.

The footnotes to references 8l to 8o shall read: " 8l) Point

11.2. of the Annex to Commission Implementing Regulation (EU) 2015/1998 of 5 November 2015 laying down detailed measures for the implementation of the common basic standards on aviation security (OJ L 299, 14.11.2015) as amended. 8m) Point 11.2.8.2. of the Annex

to Implementing Regulation (EU) 2015/1998 as amended.

8n) Act No. 53/2023 Coll. on the accreditation of conformity assessment bodies.

8o) Annex No. 14 to the Decree of the National Security Office No. 492/2022 Coll., which establishes knowledge standards in the field of cybersecurity.".

4. In Section 47 letter k), the word “accreditation” is replaced by the word “certificate” and the words are deleted "and repeated training in the field of security protection".

5. In Section 48(1)(v), the words "Section 51(2) to (6)" are replaced by the words "Section 51(2) to (7)".

6. In Section 51, paragraph 1, letter e) is deleted.

The previous letter f) is referred to as letter e).

7. In Section 51, a new paragraph 2 is inserted after paragraph 1, which reads:

"(2) The Ministry shall impose a fine of up to EUR 40,000 on a person who provides training

a) in the field of security protection without a certificate,

b) in the area of security protection in violation of the conditions specified in the certificate,

c) in the field of security protection without approved course content,

d) in the field of security protection in conflict with the approved scope and content of the courses, e) in

cybersecurity in civil aviation without a certificate pursuant to Section 34b, paragraph 6, letter a)
or

f) on cybersecurity in civil aviation in conflict with the scope and content of the courses
training in cybersecurity in civil aviation.".

The previous paragraphs 2 to 8 are renumbered as paragraphs 3 to 9.

8. In Section 55(2)(i), the words "Section 34a(8)" are replaced by the words "Section 34b(2)".

9. After Section 57ja, Section 57jb is inserted, which, including the title, reads as follows:

"§ 57jb

Transitional provisions to amendments effective from 1 January 2025

(1) Proceedings initiated pursuant to Section 34a(8) as amended until 31 December 2024 and legally binding not completed by December 31, 2024 will be completed according to the regulations effective from January 1, 2025.

(2) A valid decision on granting accreditation pursuant to Section 34a(8) as amended until 31 December 2024, issued in accordance with the current regulations, shall remain valid until the expiry of the period for which

which was issued.

Article V

Act No. 541/2004 Coll. on the peaceful use of nuclear energy (Atomic Act) and on amendments and supplements to certain acts as amended by Act No. 238/2006 Coll., Act No. 21/2007 Coll., Act No. 94/2007 Coll., Act No. 335/2007 Coll., Act No. 408/2008 Coll., Act No. 120/2010 Coll., Act No. 145/2010 Coll., Act No. 350/2011 Coll., Act No. 143/2013 Coll., Act No. 314/2014 Coll., Act No. 54/2015 Coll., Act No. 91/2016 Coll., Act No. 125/2016 Coll., Act No. 96/2017 Coll., Act No. 18/2018 Coll., Act No. 87/2018 Coll., Act 177/2018 Coll., Act 308/2018 Coll., Act No. 279/2019 Coll., Act No. 310/2021 Coll., Act No. 363/2021 Coll., Act No. 146/2023 Coll., Act No. 205/2023, Act No. 309/2023 Coll. and Act No. 161/2024 Coll. are amended as follows:

1. In Section 4, paragraph 1, letter b) reads:

"b) carries out state supervision in the field of nuclear energy use, physical protection, cybersecurity and emergency planning,".

2. In Section 31, paragraph 11, letters a) and c) shall read as follows:

"a) enter at any time without restriction the facilities of the licensees and the premises of nuclear facilities and the premises in which nuclear materials, special materials and equipment are located or radioactive waste or spent nuclear fuel is handled, carry out inspection activities there, verify with professionally qualified employees, selected employees, if they are not currently performing activities with a direct impact on nuclear safety, their knowledge of regulations, determine the status, causes and consequences of operational incidents and incidents during the transport of radioactive materials, as well as check the status of emergency preparedness, carry out inspections of compliance with nuclear safety, physical protection, cyber security, compliance with operational regulations, verify the professional competence of the licensee's employees and participate in the investigation of operational incidents and incidents during the transport of radioactive materials,

c) request the submission of documentation, records or other documents necessary for the performance of inspection activities and request copies thereof and the provision of information and explanations, including the final report on the results of the cybersecurity audit pursuant to a special regulation38d) in areas related to nuclear safety, ".

The footnote to reference 38d reads: " 38d) Section 29 of Act No. 69/2018 Coll. on Cybersecurity and on Amendments to Certain Acts, as amended.".

Article VI

Act No. 452/2021 Coll. on electronic communications as amended by Act No. 533/2021 Coll., Act No. 351/2022 Coll., Act No. 205/2023 Coll., Act No. 287/2023 Coll., Act No. 46/2024 Coll., Act No. 108/2024 Coll. and Act No. 334/2024 Coll. is amended as follows: 1. In Section 4, paragraph 5 is supplemented by letter r), which reads:

"r) recognizes a training center pursuant to Section 52a.".

2. The footnote to reference 76 reads:

" 76) Section 12, paragraph 4, letter a) of Act No. 192/2023 Coll. on the criminal record and on amendments and supplements to certain acts.".

3. In Section 52(8), the second and third sentences are deleted.

4. After Section 52, Section 52a is inserted, which reads as follows:

"Section 52a

(1) A natural person who will operate the selected radio equipment equipped with devices

GMDSS on ships that are not mandatorily equipped with these devices is obliged to complete practical training at a training centre recognised by the Authority (hereinafter referred to as the "training centre") before taking the exam. Details on the procedure and method of recognition of a training centre pursuant to the first sentence, the scope of the mandatory technical equipment of the training centre and the requirements for the description of the course of the practical training plan (hereinafter referred to as the "practical training plan") shall be established by a generally binding legal regulation issued by the Authority.

(2) An application for recognition of a training centre may be submitted to the Office by a natural person or legal entity interested in carrying out practical training pursuant to paragraph 1 (hereinafter referred to as the "applicant for recognition of a training centre").

(3) The application for recognition of a training centre shall contain:

a) identification data of the applicant for recognition of a training centre in the scope

1. name and surname, identification number or tax identification number, if it has been assigned to him/her assigned, if it is a natural person,
2. business name, organization identification number or equivalent registration number assigned in another Member State and legal form, if it is a legal person,
3. business name, organization identification number, if assigned, or equivalent registration number assigned in another Member State, if it is a natural person – entrepreneur,

b) the postal address of the registered office of the applicant for recognition of a training centre in the European Union, and the address of the organisational branch in the Slovak Republic, if such an organisational branch has been established,

c) a person or persons who are authorized to act on behalf of a natural person or legal entity regarding the application and the contact details of this person or persons,

d) website, if established, e) expected

date of commencement of the training centre's activities,

f) annexes pursuant to paragraph 4.

(4) The annexes to the application for recognition of a training centre are:

a) practical training plan, b) practical

training curriculum and methodology according to a special regulation,86a)

c) sample certificate of completion of practical training, d) list of

professionally qualified trainers,

e) proof of payment of the administrative fee.

(5) The requirements that an applicant for recognition of a training centre must meet are:

a) basic technical equipment of the training centre, b) a professionally

qualified trainer,

c) curriculum and methodology of practical training according to the CEPT recommendation ERC/REC 31-04 and

d) practical training plan.

(6) A professionally qualified trainer is a person with a university degree in a study program focusing on electrical engineering, a person with a complete secondary vocational education in the field of electrical engineering or a holder of a recreational craft master's certificate of professional competence, level A or level B, pursuant to a special regulation.86a) A professionally qualified trainer must hold a Short Range Certificate (SRC) for the operator of a navigational mobile service.

(7) Based on a complete application for recognition of a training centre, the Office shall verify compliance with the requirements under paragraph 5. If the applicant for recognition of a training centre meets the requirements under paragraph 5, the Office shall issue a decision on recognition of the training centre, otherwise the Office shall reject the application for recognition of the training centre.

(8) The Office shall revoke the decision on the recognition of a training centre if the training centre:

a) has ceased to meet the requirements pursuant to paragraph 5 or established by a generally binding legal regulation pursuant to paragraph 1,

b) repeatedly violated the obligations under paragraphs 10 to 14, c)

requested the cancellation of the decision on the recognition of the training centre.

(9) The Office shall keep records of training centres and publish their list on its website.

(10) Training center is mandatory

a) provide each practical training of at least ten hours in accordance with the curriculum, the methodology and plan of practical training pursuant to paragraph 5 letters c) and d),

b) notify the Authority of any changes in the curriculum, methodology and plan of practical training and the list of trainers within five working days from the date the change occurred.

(11) The training centre shall inform the Authority in writing of the time and place of the practical training no later than three days in advance.

(12) The training centre shall issue a certificate of completion of practical training to the graduate of practical training, which shall contain a) the identification data

of the training centre pursuant to paragraph 3 letter a),

b) name, surname, title of the practical training graduate, c) date of birth

of the practical training graduate,

d) date of practical training, e) date and place of

issue of the certificate of completion of practical training,

f) name and signature of the person representing the training centre.

(13) The training centre keeps records of participants in practical training.

(14) The training centre shall send the Authority a list of graduates of practical training within seven days after the completion of practical training.”.

The footnote to reference 86a) reads: " 86a) Section

2, paragraph 1, letters a) and b) of the Decree of the Ministry of Transport, Posts and Telecommunications of the Slovak Republic No. 54/2002 Coll., which establishes details on the technical competence of a recreational craft and the professional competence of the captain of a recreational craft.".

5. Sections 103 to 107 are deleted.

The footnotes to references 116 to 118 are deleted.

6. In Section 117(20), the words "level (III) cyber security incident" are replaced by the words "serious cyber security incident".

7. In Section 124, paragraph 1, the words “Section 103, paragraphs 1 and 4, Section 104, paragraphs 1, 3 to 5,” and the words “Section 105,” are deleted.

8. In Section 124, paragraph 3, the words "Section 102, paragraphs 3 and 4, Section 106," are deleted.

Article VII

This Act shall enter into force on 1 January 2025.

Peter Pellegrini, inc.

in the name of Peter Žiga

Robert Fico, incl.

Publisher of the Collection of Laws of the Slovak Republic, content administrator and operator of the legal and information
the Slov-Lex portal available at the website www.slov-lex.sk is
Ministry of Justice of the Slovak Republic, Raÿianska 71, 813 11 Bratislava,
phone: +421 2 888 91 864, +421 2 888 91 865, e-mail: helpdesk@slov-lex.sk.