69

Act

of January 30, 2018

on Cybersecurity and on Amendments and Supplements to certain Acts

The National Council of the Slovak Republic adopted the following Act:

Section I

Article 1
Purpose of the Act

This Act regulates

a) organisation, competencies and obligations of public administration authorities in the field of cybersecurity,
b) National Cybersecurity Strategy,
c) Cybersecurity Single Information System,
d) organisation and competencies of the units for cybersecurity incidents handling (hereinafter referred to as "CSIRT unit") and their accreditation,
e) status and obligations of the operator of essential service and digital service provider,
f) security measures,
g) cybersecurity assurance system,
h) inspection of compliance with this Act and audit.

Article 2
Scope of the Act

(1) This Act sets forth the minimum requirements for cybersecurity assurance.

(2) This Act does not apply to

a) the requirements for the networks and information systems assurance under the general legal regulation on protection of classified information,
b) special provisions on the tasks and authorisations of the state authority upon cyberspace protection under specific legal regulation,[1])
c) provisions of specific legal regulations on crime investigation, detection and prosecution,[2])
d) requirements related to network and information system security and cybersecurity incidents reporting in banking, finances or financial system sector according to the specific legal regulation,[3]) including the

---

[1]) Article 2 (1) item g), (3) of the Act of the National Council of the Slovak Republic No. 46/1993 Coll. on the Slovak Information Service, as amended by the Act No. 151/2010 Coll.
Article 2 (1) items c) and h), (2) and Article 4a of the Act of the National Council of the Slovak Republic No. 198/1994 Coll. on Military Intelligence, as amended.
Act No. 319/2002 Coll. on the Defence of the Slovak Republic, as amended.

[2]) For example, Act No. 398/2015 Coll. on the European Protection Order in Criminal Matters and on Amendments and Supplements to certain Acts, Act No. 91/2016 Coll. On Criminal Liability of Legal Persons and on Amendments and Supplements to certain Acts, as amended.

standards and principles issued or adopted by the European Central Bank, European System of Central Banks, Eurosystem or European supervisory authorities,[4]) if their effect is at least equal to the effects of obligations under this Act, and including the decisions, standards, and principles issued or adopted by the National Bank of Slovakia, if their aim is to achieve a higher level of network and information system security than under this Act, nor on the payment systems and clearing systems of securities supervised or operated by the European Central Bank or Eurosystem pursuant to specific legal regulation,[5])

e) requirements for the networks and information systems assurance in the sector according to specific legal regulation,[6]) if their aim is to achieve a higher level of network and information system security,

f) specific legal regulation.[7])

Article 3a
Definition of Basic Terms

For the purpose of this Act means

a) network and information system an electronic communication system, information system, any equipment and communication system or data created, stored, processed, obtained or transferred therein through an electronic communication network or information system, for the purpose of operating, using, protecting and maintaining these networks and systems,

b) cyber space a global dynamic open system of networks and information systems consisting of activated elements of the cyber space, natural persons performing activities in this system and relations and interactions among them,

c) continuity a strategic and tactical capability of the organisation to plan and respond to the occurrences and incidents with the aim to continue performing its activities at an acceptable level determined in advance,

d) confidentiality a guarantee that the information will not be disclosed to unauthorised parties or processes,

e) availability a guarantee that the data or information is for the user, information system, network or equipment available at the moment when necessary and required,

f) integrity a guarantee that the information has stayed intact, complete and correct and has not been distorted,

g) cybersecurity a state in which the networks and information systems have the capability to resist, at a certain reliability level , against any conduct threatening the availability, authenticity, integrity or

---

[3]) For example, Articles 28c, 28d, 45 (8) and 64 (4) of the Act No. 492/2009 Coll. on Payment Services and on Amendments and Supplements to certain Acts, 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 EU L 201, 27/07/2012), as amended, Article 14 of the Act No. 429/2002 Coll. on Stock Exchange, as amended, Commission Delegated Regulation (EU) 2017/584 of 14 July 2016 supplementing Directive 2014/65/EU of the European Parliament and of the Council with regard to regulatory technical standards specifying organisational requirements of trading venues (OJ EU L 87, 31/03/2017).

[4]) For example, Article 127 (2) of the Treaty on the Functioning of the European Union, as amended (OJ EU C 202, 07/06/2016), Article 12 (12.1), Article 22 of the Protocol (No. 4) of the Statute of the European System of Central Banks and of the European Central Bank, as amended (OJ EU C 202, 07/06/2016), Article 2 of the Act of the National Council of the Slovak Republic No. 566/1992 Coll. on the National Bank of Slovakia, as amended, Article 2 (9) of the Act No. 747/2004 Coll. on the Financial Market Supervision and on Amendments and Supplements to certain Acts, as amended by the Act No. 132/2013 Coll.

[5]) For example, Article 3 (3.1), Article 22 of the Protocol (No. 4) of the Statute of the European System of Central Banks and of the European Central Bank, as amended (OJ EU C 202, 07/06/2016), Regulation of the European Central Bank (EU) No 795/2014 of 3 July 2014 on oversight requirements for systemically important payment systems (ECB/2014/28) (OJ L 217, 23/07/2014).

[6]) Act No. 541/2004 Coll. on Peaceful Usage of Nuclear Energy (Atomic Act) and on Amendments and Supplements to some Acts, as amended.
Act No. 275/2006 Coll. on Public Administration Information Systems and on Amendments and Supplements to some Acts, as amended.

[7]) For example, Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (OJ EU L 257, 28/ 08/ 2014), Act No. 166/2003 Coll. on Privacy Protection against Unauthorised Use of Information-Technology Means and on Amendments and Supplements to certain Acts (Act on Protection against Interception), as amended, Act No. 45/2011 Coll. on Critical Infrastructure, Act No. 351/2011 Coll. on Electronic Communications, as amended.

confidentiality of the stored, transferred, or processed data or related services provided and available through these networks and information systems,

h) risk a level of cyber threat expressed by the probability of occurrence of the undesired phenomenon and its consequences,

i) threat each adequately identifiable circumstance or occurrence against the networks and the information systems with a possible negative impact on cybersecurity,

j) cybersecurity incident any occurrence that as a consequence of disruption of the network and information system security, or violation of the security policy or binding methodology, has a negative impact on cybersecurity or which results in
   1. the loss of data confidentiality, destruction of data or disruption of system integrity,
   2. limitation or rejection of availability of essential service or digital service,
   3. high probability of compromising the activities of essential service or digital service, or
   4. threat to information security,

k) essential service a service included in the list of essential services, while
   1. depending on the networks and the information systems and being an activity at least in one sector or sub-sector according to Annex No. 1,
   2. being a public administration information system,[8]) or
   3. being an element of the critical infrastructure,[9])

l) operator of essential service a public administration authority or an entity operating at least one service under item k),

m) digital service a service, included in Annex No. 2,

n) digital service provider a legal entity or natural person- entrepreneur providing digital service while employing at least 50 employees and having an annual turnover or overall annual balance of over EUR 10,000,000,

o) cybersecurity incident handling all procedures related to reporting, detection, analysis and response to cybersecurity incident and limiting its consequences.

Article 4
Competencies of Public Administration Authorities

The competencies in the field of cybersecurity are performed by the

a) National Security Authority (hereinafter referred to as "the Authority")

b) The Authority, Ministry of Transport and Construction of the Slovak Republic, Ministry of Finance of the Slovak Republic, Ministry of Economy of the Slovak Republic, Ministry of Defence of the Slovak Republic, Ministry of Interior of the Slovak Republic, Ministry of Health of the Slovak Republic, Ministry of Environment of the Slovak Republic, Slovak Information Service, Office of the Deputy Prime Minister of the Slovak Republic for Investment and Informatization, and Military Intelligence (hereinafter referred to as "competent body"),

c) ministries and other central state administration authorities, [10]) other than competent body, General Prosecutor's Office of the Slovak Republic, Supreme Audit Office of the Slovak Republic, Health Surveillance Authority, Office for Personal Data Protection of the Slovak Republic, Regulatory Office for Network Industries and other public authorities in the scope of their competencies (hereinafter referred to as "other state administration body").

Article 5
The Authority

(1) The Authority in the field of cybersecurity

---

[8]) Article 2 (1) item b) of the Act No. 275/2006 Coll. as amended by the Act no. 570/2009 Coll.

[9]) Article 2 item a) of Act No. 45/2011 Coll.

[10]) Articles 3 and 21 of the Act No. 575/2001 Coll. on the Structure of Activities of the Government and Central State Administration Bodies, as amended.

a) manages and coordinates carrying out of state administration,
b) determines the standards, operational procedures, issues the methodology and policy of behaviour in cyberspace,
c) determines the principles for preventing cybersecurity incidents and principles for their handling,
d) elaborates the National Cybersecurity strategy and the annual report on the state of cybersecurity in the Slovak Republic in cooperation with the respective state authorities,
e) is a national point of contact for cybersecurity for foreign entities and ensures cooperation with the respective points of contact of other member states of the European Union and the North Atlantic Treaty Organisation,
f) carries out obligations of notification and reporting in relation to the appropriate authorities of the European Union and the North Atlantic Treaty Organisation and participates in and supports forming cybersecurity partnerships at a national and international level,
g) ensures membership of the Slovak Republic in the Cooperation Group and in the Network of CSIRT Units,
h) in cooperation with the Ministry of Foreign and European Affairs of the Slovak Republic develops international cooperation and monitors the effects of activities in the field of cybersecurity on the foreign policy interests of the Slovak Republic as well as its partners within the European Union and the North Atlantic Treaty Organisation,
i) cooperates with the competent bodies, other state administration authorities and CSIRT Units, operators of essential services and digital service providers so as to fulfil the tasks according to this Act,
j) administers and operates the Cybersecurity Single Information System,
k) based on notification of the competent body, operator of essential service, digital service provider, or upon its own initiative, it determines
    1. an essential service and includes it in the list of essential services,
    2. a digital service and includes it in the list of digital services,
    3. a digital service provider and includes it in the registry of digital service providers,
    4. an operator of essential service and includes it in the registry of operators of essential services,
l) manages and maintains
    1. the list of essential services,
    2. registry of operators of essential services,
    3. list of digital services,
    4. registry of digital service providers,
    5. list of accredited CSIRT units,
m) systematically gathers, concentrates, analyses and evaluates information on the state of cybersecurity in the Slovak Republic,
n) accredits CSIRT Units, except for the National CSIRT Unit and the Governmental CSIRT Unit and includes them in the list of accredited CSIRT Units,
o) fulfils the tasks of the competent authority for digital services,
p) ensures and is responsible for coordinated cybersecurity incidents handling at the national level,
q) handles cybersecurity incidents, declares alerts and warnings of serious cybersecurity incidents, imposes the obligation to take reactive measures and approves the protective measure,
r) sends early warnings,
s) gathers domestic reports on cybersecurity incidents,
t) gathers reports on cybersecurity incidents from abroad and ensures cooperation with international organisations and authorities of other states when handling cybersecurity incidents of cross-border nature,
u) performs inspection, issues decisions on imposing remedial measures and levies fines for offences or administrative offences,
v) performs an audit or requests the conformity assessment body to perform an audit at the operator of essential service,
w) issues expertize standards, and in cooperation with the Ministry of Education, Science, Research and Sport of the Slovak Republic, performs and ensures security awareness building,
x) coordinates research and development.

(2) For the purpose of ensuring fulfilling of the tasks under this Act, the Authority may conclude a written cooperation agreement with a natural person. The cooperation agreement must contain the actual form and terms and conditions of the cooperation, and the natural person must be authorized to handle classified information of the respective classification level if necessary for the fulfilment of the tasks.

Article 6
National CSIRT Unit

(1) The Authority has the status of National CSIRT Unit with competencies for the Slovak Republic and must comply with the terms and conditions of accreditation according to Article 14 and perform the tasks of a CSIRT Unit according to Article 15 for all the sectors and sub-sectors listed in Annex No. 1 and digital services, except for the sectors and sub-sectors for which the tasks of CSIRT Unit are performed by the competent bodies. The National CSIRT Unit is included in the list of accredited CSIRT Units.

(2) The National CSIRT Unit acts as a competent body within the scope of Article 9 (1) item a) unless the competent body does not ensure this task in the manner according to Article 9 (2).

(3) Other state administration bodies may participate in the activities of the National CSIRT Unit by delegating their representatives and by other forms of cooperation, in the scope and manner according to the concluded cooperation agreements.

(4) Fulfilling of the tasks of the Authority under Paragraphs 1 and 2 does not dispense the operator of essential service nor the competent body from the responsibility for carrying out the obligations under this Act nor for carrying out the obligations regarding the networks and information systems according to specific legal regulation..

Article 7
National Cybersecurity Strategy

(1) The National Cybersecurity Strategy is an initial strategic document that comprehensively determines the strategic approach of the Slovak Republic to ensuring cybersecurity. The National Cybersecurity Strategy includes an action plan as an actual plan of partial tasks and resources.

(2) The National Cybersecurity Strategy contains mainly

a) goals, priorities and the framework of management in order to achieve these goals and priorities, including the tasks and responsibilities of the public administration authorities and other relevant entities,
b) identification of measures related to the readiness, response and restoration, including cooperation between the public sector and the private sector,
c) description of the security environment,
d) definition of security threats,
e) identification of necessary resources,
f) determination of the education programs, programs for security awareness building, increase of awareness and professional training,
g) definition of the research and development plans,
h) risk assessment plan for the purposes of risk identification,
i) list of entities involved in carrying out of the National Cybersecurity Strategy,
j) identification of the main foreign political partners.

(3) Competent bodies and other state administration bodies cooperate with the Authority so as to elaborate the National Cybersecurity Strategy and for this purpose are obliged to provide it information in the necessary extent.

(4) National Cybersecurity Strategy is to be approved by the Government of the Slovak Republic.

Article 8
Cybersecurity Single Information System

(1) The Cybersecurity Single Information System is an information system, whose administrator and operator is the Authority and it provides efficient management, coordination, registering and inspection of carrying out of state administration in the field of cybersecurity and CSIRT Units. The Cybersecurity Single Information System is also meant for processing and evaluating of data and information on the state of cybersecurity and can be used at the time of crisis planning during peace, state management in crisis situations during outside of the time of war and state of war,[11]) as well as for the necessary activities during the time of war or state of war.

(2) The Cybersecurity Single Information System contains a communication system for cybersecurity incidents reporting and handling and a central early warning system. The Cybersecurity Single 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 Cybersecurity Single Information System contains the

a) registry of competent bodies,
b) list of essential services,
c) registry of operators of essential services,
d) list of digital services,
e) registry of digital service providers,
f) registry of cybersecurity incidents,
g) list of accredited CSIRT Units,
h) methodologies, guidelines, standards, policies and announcements,
i) information and data necessary for using the Cybersecurity Single Information System ,
j) alerts and warnings and other information for minimising, averting or remedying of the consequences of a cybersecurity incident.

(3) The communication system for cybersecurity incidents reporting and handling of is a communication system that ensures systematic gathering, concentrating, analysing and evaluating of cybersecurity incidents information.

(4) The central early warning system is an information system ensuring timely exchange of information on the threats, cybersecurity incidents and risks related thereto between the Authority and the entities according to Paragraph 5.

(5) The non-public part of the Cybersecurity Single Information System is directly accessed in electronic form in real time, in the scope determined by the Authority or a specific legal regulation[12]) and based on material scope, by

a) competent body,
b) CSIRT Unit included on the list of accredited CSIRT Units,
c) operator of essential service and digital service provider,

---

[11]) For example, Act No. 319/2002 Coll., as amended, Act No. 387/2002 Coll. on State Government during Crises outside of Wartime and State of War, as amended, Act No. 179/2011 Coll. on Economic Mobilisation and on Amendments and Supplements to Act No. 387/2002 Coll. on State Government during Crises outside Wartime and State of War, as amended.

[12]) For example, Regulation (EU) No 1092/2010 of the European Parliament and of the Council of 24 November 2010 on European Union macro-prudential oversight of the financial system and establishing a European Systemic Risk Board (OJ EU L 331, 15/12/2010), Regulation (EU) No 468/2014 of the European Central Bank of 16 April 2014 establishing the framework for cooperation within the Single Supervisory Mechanism between the European Central Bank and national competent authorities and with national designated authorities (SSM Framework Regulation) (ECB/2014/17) (OJ EU L 141, 14/05/2014), Act of the National Council of the Slovak Republic No. 566/1992 Coll., as amended, Article 15 (2) of the Act of the National Council of the Slovak Republic No. 46/1993 Coll, as amended by Act No. 444/2015 Coll.

d) National Bank of Slovakia,
e) Office for Personal Data Protection of the Slovak Republic
f) other public administration authority upon decision of the Authority.

(6) The entity that is obliged, under this Act, to provide information, data and reports through the Single Information System of Cybersecurity, must provide them free of charge and immediately after having learnt about the fact establishing this obligation. Information, data and reports are provided in the manner determined by the functionality of the Single Information System of Cybersecurity.

Article 9
Competent Body

(1) The competent body, in the scope of its competencies for the sector or sub-sector according to Annex No.1, is responsible for ensuring cybersecurity by

a) fulfilling the tasks of CSIRT Unit according to Paragraph 2,
b) providing the Authority with required assistance and information obtained from its own activities important for ensuring cybersecurity; information is only provided under the condition that its provision does not result in jeopardising the fulfilling of a certain task according to specific legal regulation[13]) or disclosure of its sources, means, and identity of the persons acting in its favour, or jeopardising international intelligence cooperation,
c) cooperating with other competent bodies and operators of essential services in their competencies while fulfilling the tasks under this Act,
d) building security awareness, coordinated cooperation at all levels of cybersecurity management and applying security approach and conduct policy in the cyber space,
e) in cooperation with the Authority, determining specific sectoral identification criteria according to Article 18 (3),
f) identifying the essential services and operator of essential service and submitting their up-to-date list to the Authority for the purpose of including in the list of essential services and registry of operators of essential services,
g) cooperating with similar foreign institutions.

(2) The competent body, for the purposes of fulfilling the tasks according to Paragraph 1 item a), in the scope of its competencies for the sector or sub-sector according to Annex No. 1, establishes and operates an accredited CSIRT Unit, or for this purpose uses an accredited CSIRT Unit, established and operated by another competent body, if they so agree. Using the services of an accredited CSIRT Unit established and operated by another competent body, is carried out based on a contract.

(3) The contract under Paragraph 2 must contain the period during which the accredited CSIRT Unit is used, a list of persons in the competencies of the competent body, who will be responsible for provision of data and information and their scope, obligations of reporting changes affecting the proper functioning of the accredited CSIRT Unit and identification of operating costs that the competent body is to pay.

Article 10
Tasks of Other State Administration Body

(1) In order to ensure continuity and risk management regarding securing the networks and information systems, other than essential services, and the process of cybersecurity incidents handling, other state administration body and competent body in the scope of its competencies is responsible for ensuring cybersecurity by taking and carrying out suitable and adequate security measures according to Article 20.

---

[13]) Act of the National Council of the Slovak Republic No. 46/1993 Coll., as amended.
Act of the National Council of the Slovak Republic No. 198/1994 Coll., as amended.

(2) The other state administration body further provides the Authority with required assistance and information obtained from its own activities important for ensuring cybersecurity; information is only provided under the condition that its provision does not result in jeopardising the fulfilling of a certain task according to a specific legal regulation[19]) or disclosure of its sources, means, and identity of the persons acting in its favour, or jeopardising international intelligence cooperation.

Article 11
Governmental CSIRT Unit

The Governmental CSIRT Unit is hereby established under the Office of Deputy Prime Minister the Slovak Republic for Investment and Infomatization of for the sub-sector of public administration information systems. The Governmental CSIRT Unit must meet the accreditation conditions according to Article 14 and fulfil the tasks according to Article 15. The Governmental CSIRT Unit is included in the list of accredited CSIRT Units.

Article 12
Confidentiality and Personal Data Protection

(1) Whoever fulfills or has fulfilled tasks under this Act or in relation thereto, is to maintain secrecy of the facts that they have learned in relation to task fulfilling according to this Act if they are not known to the public. The secrecy obligation lasts even after termination of the cooperation agreement according to Article 5 (2), employment or similar labour relation, including employment in the civil service.[14]) The provisions concerning the secrecy liability under this Act do not affect the secrecy obligation or keeping secrets under specific legal regulation.[15])

(2) The waiver of secrecy obligation according to Paragraph 1 is to be decided within the

a) Authority by its director,
b) other entity by its statutory body.

(3) For the purpose of acting before a public administration authority, for the purpose of criminal proceedings, notification of the fact indicating that a crime has been committed or reporting of criminality or other antisocial activity[16]) the secrecy obligation as stated in Paragraph 1, does not apply to the operator of essential service and the digital service provider and its employees.

---

[14]) Act No. 73/1998 on the Civil Service of Members of the Police Force, the Slovak Intelligence Service, the Court Guards and Prison Wardens Corps and the Railway Police, as amended.
Act No. 311/2001 Coll. the Labour Code, as amended.
Act No. 552/2003 Coll. on Performing Work in the Public Interest, as amended.
Act No. 281/2015 Coll. on Civil Service of Professional Soldiers, as amended.
Act No. 55/2017 Coll. on Civil Service and on Amendments and Supplements to certain Acts.

[15]) For example, Article 37 (37.1) of Protocol (No. 4) of the Statute of the European System of Central Banks and of the European Central Bank, as amended (OJ EU C 202, 07/06/2016), Articles 17 to 20 of the Act No. 513/1991 Coll. Commercial Code, Article 39 of the Act of the Slovak National Council No. 323/1992 Coll. on Notaries and Notarial Activities (the Notarial Code), as amended, Article 23 of the Act of the National Council of the Slovak Republic No. 46/1993 Coll., Article 20 of the Act of the National Council of the Slovak Republic No. 198/1994 Coll., as amended by the Act No. 319/2012 Coll., Act No. 483/2001 on Banks and on Amendments and Supplements to some Acts, as amended, Article 23 of the Act No. 586/2003 Coll. on Advocacy and on Amendments and Supplements to the Act No. 455/1991 Coll. on Trade Licensing (the Trade Licensing Act), as amended by the Act No. 297/2008 Coll, Act No. 215/2004 Coll. on the Protection of Classified Information and on Amendments and Supplements to some Acts, as amended, Article 24 and 25 of the Act No. 576/2004 Coll. on Health Care, Services related to Health Care Provision and on Amendments and Supplements to some Acts, as amended, Article 11 of the Act No. 563/2009 Coll. on Administration of Taxes (Tax Regulation) and on Amendments and Supplements to some Acts, as amended, Article 63 of the Act No. 352/2011 Coll., as amended, Article 10 of the Act No. 324/2011 Coll. on Postal Services and on Amendments and Supplements to certain Acts.

[16]) Act No. 583/2008 Coll. on the Prevention of Crime and other Antisocial Activities and on Amendments and Supplements to some Acts.
Act No. 307/2014 Coll. on some Measures related to the Reporting of Antisocial Activities and on Amendments and Supplements to certain Acts.

(4) Reporting of cybersecurity incidents in the extent under this Act, informing on the reported cybersecurity incident, declaration of alert and warning in the manner under this Act is not considered a violation of the secrecy obligation pursuant to this Act and according to specific legal regulation.[15])

(5) The Authority shall be liable for the damage caused to the operators of essential services, digital service providers, their employees or to the person reporting the cybersecurity incident, which was caused by notification according to Paragraph 4.

(6) , , , According to specific legal regulation [17]) and for the absolutely necessary time, for the purpose of cybersecurity incident handling, in the scope necessary for its identification and ensuring cybersecurity, the Authority processes personal data in the Cybersecurity Single Information System in the interest of national security.

(7) The Authority ensures non-stop protection of data and information processed under this Act from illegal disclosure, abuse, damage, unauthorised destruction, theft and loss in the manner according to specific legal regulation. [18])

(8) Information and personal data obtained under this Act or in relation thereto may be used by the Authority only for fulfilling the tasks under this Act.

Article 13
Accreditation of CSIRT Unit

(1) Compliance of the CSIRT Unit with the terms and conditions of accreditation is assessed by the Authority based on an application.

(2) The application according to Paragraph 1 is submitted to the Authority in electronic form by the competent body that is to carry out the tasks of a CSIRT Unit; the documentation proving compliance with the CSIRT Unit accreditation terms and conditions is attached to the application.

(3) The proceedings according to Paragraph 1 commence upon the delivery date of the application to the Authority according to Paragraph 2. If the application is incomplete, the Authority requests the applicant to amend the application in a term of no less than ten days. Application not amended by the applicant in the required manner within the defined term is disregarded by the Authority.

(4) The Authority decides on the accreditation within 90 days since the delivery date of the complete application, and it issues a decision on accreditation if compliance of the CSIRT Unit with the accreditation terms and conditions of a CSIRT Unit is determined. The decision on accreditation is issued for a definite period of up to five years.

(5) Upon application, the Authority may repeatedly extend the validity of accreditation decision if no changes in the terms and conditions occurred, under which the accreditation decision was issued. According to the previous sentence, the application is submitted to the Authority at least six months before the expiration of the validity period of the accreditation decision to be extended. Paragraphs 2 to 4 apply accordingly for the proceedings and submitting of an application. If the Authority acknowledges accreditation extension, it issues a decision according to Paragraph 4 with an “extension” clause.

---

[17]) Article 23 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ EU L 119/89, 04/05/2016).

[18]) Article 5 of Regulation (EU) No. 2016/679.

(6) Upon application of the competent body, which is to fulfil the tasks of the CSIRT Unit,, the Authority also recognises accreditation of a CSIRT Unit having been accredited according to the legal regulation of another state or an international organisation if compliance with the CSIRT Unit accreditation terms and conditions is provably ensured; Article 14 item a) is not to be proven. Paragraphs 2 to 4 apply accordingly for the proceeding and submitting of an application. An accreditation decision is issued by the Authority pursuant to Paragraph 4 with an "recognition" clause maximally for the validity period that the CSIRT Unit had been accredited according to the legal regulation of another state or of an international organisation.

(7) The Authority includes the CSIRT Unit accredited under this Act in the list of accredited CSIRT Units.

Article 14
Terms and Conditions of CSIRT Unit Accreditation

Applicant for CSIRT Unit accreditation according to Article 13 proves by documentation that the CSIRT unit

a) has the required technical, technological equipment and staffing according to the generally binding legal regulation issued by the Authority,
b) has created the conditions enabling secured transmission and processing of data according to a specific legal regulation,[19])
c) protects information and data gathered in carrying out the obligations under this Act and and processes them so as not to disrupt their availability, confidentiality, authenticity and integrity,[20])
d) has documentation, information systems and other information-communication technologies in the secured area without disrupting their availability, confidentiality, authenticity and integrity.[20])

Article 15
Tasks of the CSIRT Unit

(1) The entity fulfilling the tasks of a CSIRT Unit in the scope of its competencies stated according to Annex No. 1, is responsible for cybersecurity incidents handling and carries out preventive services and reactive services.

(2) Preventive services focus on preventing cybersecurity incidents by
a) security awareness building,
b) training,
c) cooperation with other CSIRT Units,
d) monitoring and registering cybersecurity incidents,
e) connecting to the Cybersecurity Single Information System ,
f) providing information and data into the Cybersecurity Single Information System,
g) receiving and sending early warnings of cybersecurity incidents through the Cybersecurity Single Information System.

(3) Reactive services focus on cybersecurity incidents handling and are mainly
a) alert and warning,
b) cybersecurity incidents detection,
c) cybersecurity incidents analysis,
d) response, delimitation, handling and remedying of the consequences of cybersecurity incidents,

---

[19]) Act No. 215/2004 Coll., as amended.
Article 6 (10), Article 55 (9), Article 56 (7), Article 58 (4) and Article 69 of the Act No. 215/2004 Coll.

[20]) For example, STN ISO/IEC 27002 Information Technologies. Security Methods. Code of Practice for Information Security Management (ISO/IEC 27002:2013).

e) assistance in cybersecurity incidents handling on the spot,
f) response to cybersecurity incident,
g) support of responses to cybersecurity incidents,
h) coordination of responses to cybersecurity incidents,
i) draft measures for preventing further continuation, spreading and repeated occurrence of cybersecurity incidents.

(4) Reactive services are carried out by the CSIRT Unit in the presence of the operator of essential service or digital service provider.

Article 16
Obligations of the Entity fulfilling the Tasks of the CSIRT Unit

(1) The entity fulfilling the tasks of the CSIRT unit

a) has to ensure that its CSIRT Unit included in the list of accredited CSIRT Units continuously during its entire operation complies with the terms and conditions of CSIRT Unit accreditation according to Article 14, and at the same time fulfils all the tasks according to Article 15,
b) reports immediately to the Authority any changes with an impact on accreditation of the CSIRT Unit ,
c) solicits the opinion of the National Bank of Slovakia regarding the procedure of the competent body upon fulfilling the tasks under this Act, if the operator of essential service is a supervised financial market entity, [21]) supervised by the National Bank of Slovakia according to specific legal regulation.[22])

(2) If the accredited CSIRT Unit ceases to comply with the terms and conditions according to Article 14 or if it does not fulfil the tasks according to Article 15, the entity fulfilling the tasks of CSIRT Unit reports it immediately to the Authority; based on the report according to the previous sentence, the Authority cancels the accreditation decision and excludes the CSIRT Unit from the list of accredited CSIRT Units.

(3) The Authority may, based on its own findings, inform the entity carrying out the tasks of a CSIRT Unit on the deficiencies in compliance with the terms and conditions in Article 14 or tasks in Article 15 with indication of the period for their elimination. If the deficiencies, according to the previous sentence based on the announcement to the Authority, are not eliminated within the determined period, the Authority cancels the accreditation decision and excludes the CSIRT Unit from the list of accredited CSIRT Units.

Article 17
Essential Service, Operator of Essential Service and Inclusion in the List of Essential Services

(1) Service operator has to notify the Authority within 30 days if the service operator in the sector according to Annex No. 1 finds out that the identification criteria of the operated service according to Article 18 were exceeded.

(2) The Authority includes the essential service according to Article 3 item k) first point, in the list of essential services and its operator in the registry of operators of essential services
a) based on notification made by the operator of this service according to Paragraph 1,
b) based on the motion of competent body if the identification criteria of the operated service according to Article 18 were exceeded,
c) on its own initiative, if the Authority learned about exceeding of the identification criteria of the operated service according to Article 18 and the procedure according to item a) or item b) did not take place.

---

[21]) Article 1 (3) item a) of the Act No. 747/2004 Coll, as amended.
[22]) For example, Act No. 483/2001 Coll., as amended, Act No. 566/2001 Coll. on Securities and Investment Services and on Amendments and Supplements to some Acts, as amended, Act No. 429/2002 Coll., as amended, Act No. 747/2004 Coll., as amended, Act No. 492/2009 Coll., as amended.

(3) In cooperation with the competent body, the Authority includes the essential service according to Article 3 item k) second point, in the list of essential services and its operator in the registry of operators of essential services.

(4) The Authority includes the essential service according to Article 3 item k) third point, in the list of essential services and its operator in the registry of operators of essential services ex offo.

(5) The notification according to Paragraph1 must contain
a) name and registered seat,
b) contact details,
c) list of services concerned by identification criteria exceeding,
d) information on possible or existing cross-border overhand of the service,
e) percentage of market share of the service,
f) geographic distribution of the service,
g) information on alternative possibilities of maintaining the continuation of service in case of a cybersecurity incident.

(6) The Authority notifies to the operator of the service through the Cybersecurity Information System inclusion of the service in the list of essential services and its operator in the registry of operators of essential services.

Article 18
Identification Criteria of the Operated Service

(1) The identification criteria of the operated service are the impact criteria and specialc sectoral criteria.

(2) The impact criteria are determined by a generally binding legal regulation issued by the Authority and consider mainly
a) the number of users employing the essential service,
b) dependence of other sectors according to Annex 1from the essential service,
c) the impact that the cybersecurity incidents could have from the aspect of scope and duration on the economic and social activities and interests of the state, or on state security,
d) market share of the service operator,
e) geographic spread according to the area that the cybersecurity incident could affect,
f) significance of the operator of essential service from the aspect of maintaining continutty of service provision.

(3) The special sectoral criteria take into consideration the criteria defined by the generally binding legal regulation issued by the Authority.

(4) If the operator of service according to Annex No.1 finds out about exceeding the special sectoral criteria, it shall report it to the Authority within 30 days of the date when the excess was identified in the scope according to Article 17 (5) also without exceeding the impact criteria.

Article 19
Obligations of the Operator of Essential Services

(1) The operator of essential service must, within six months from the notification date of inclusion in the registryr of operators of essential services, take and carry out security measures at least in the scope of the security measures according to Article 20 and sectoral security measures, if adopted.

(2) The operator of essential service is obliged, at conclusion of a supplier contract for the execution of activities directly related to the operation of networks and information systems for the operator of an essential service (hereinafter referred to as "third party") to conclude a contract on ensuring of carrying out of security measures and notification obligations in accordance with the Act during the entire period of the validity of the contract.

(3) The operator of essential service is obliged, since the date of inclusion in the registry of operators of essential services, to announce this fact to the company providing electronic communication services or networks according to specific legal regulation,[23]) to which the network or information system of the essential services is connected. Based on information provision according to the previous sentence, the operator of essential service shall conclude a contract with the company according to Paragraph 2.

(4) Operator of essential service must inform third party in the necessary scope on the reported cybersecurity incident, provided that the performance of the contract according to Paragraph 2 became impossible, unless otherwise decided by the Authority. The secrecy obligation is hereby not affected.

(5) If the operator of essential service also provides this service in another member state of the European Union, the Authority in cooperation with the relevant authority of that member state decides according to the criteria of which member state the operator of essential services will be identified so as to be clearly identified as an operator of essential service in at least one of these member states.

(6) The operator of essential service is further obliged to

a) handle cybersecurity incidents,
b) immediately report any serious cybersecurity incident,
c) cooperate with the Authority and the competent body when handling the reported cybersecurity incident, and for this purpose to provide them with the necessary assistance, as well as information obtained from its own activities relevant for cybersecurity incident handling,
d) at the time of the cybersecurity incident, to provide proof or means of proof so that they may be used in a criminal proceeding,
e) inform the law enforcement authority or the Police force on the fact that a crime was committed that the cybersecurity incident is related to, if it learns about it in a plausible manner.

(7) The operator of essential service is obliged to report the changes in data according to Article 17 (5) within 30 days through the Cybersecurity Single Information System.

(8) The operator of essential service is not liable for the damage incurred to another entity by limitation of continuity of essential service at cybersecurity incident handling according to Article 27. The Authority is liable for the damage caused by limited continuity of essential service due to the cybersecurity incident by carrying out the obligations in the manner according to the previous sentence.

Article 20
Security Measures

(1) For the purposes of this Act, security measures mean tasks, processes, roles and technologies in the organisational, personnel and technical area, whose aim is to ensure cybersecurity during the life cycle of networks and information systems. Security measures performed depending on the classification of information and categorisation of networks and information systems and in compliance with the security

[23]) Article 5 (1) of the Act No. 351/2011 Coll, as amended by the Act No. 247/2015 Coll.

standards in the field of cybersecurity are taken in order to prevent cybersecurity incidents and minimise the impact of cybersecurity incidents on the continuity of service operation. Security measures are general: taken depending on the classification of information and categorisation of networks and information systems and in compliance with the security standards in the field of cybersecurity for all networks and information systems, and sectoral: taken based on the specifics of categorisation of the networks and information systems of the competent body in the scope of its competencies according to Annex No. 1 and in compliance with the security standards in the field of cybersecurity.

(2) Classification of information and categorisation of networks and information systems according to Paragraph 1 is performed based on significance, function and purpose of the information and information systems with regard to confidentiality, integrity, availability, service quality and inspection activity.

(3) Security measures are taken mainly for the field of

a) information security organisation,
b) management of assets, threats and risks,
c) personnel security,
d) management of supplier services, acquisition, development and maintenance of information systems,
e) technical vulnerabilities of the systems and equipment,
f) management of network and information system security,
g) operational management,
h) access management,
i) cryptographic measures,
j) cybersecurity incidents handling,
k) monitoring, testing of security and security audits,
l) physical security and security of environment,
m) process continuity management.

(4) Security measures must include at least

a) detection of cybersecurity incidents,
b) registration of cybersecurity incidents,
c) handling procedures and cybersecurity incidents handling,
d) identifying of a contact person for gathering and registration of reports,
e) connection to the central early warning system and to the communication system for cybersecurity incidents handling and reporting.

(5) Security measures are taken and executed based on an approved security documentation, which has to be up-to-date and apply to the actual state.

Article 21
Digital Service and Digital Service Provider

(1) The digital service provider is obliged within 30 days from the commencement of digital service provision notify the Authority of

a) its name and registered seat,
b) contact details,
c) the provided service,
d) name, registered seat and contact details of the representative according to Article 23.

(2) Based on the notification according to Paragraph 1 the Authority includes the service in the list of digital services and its provider in the registry of digital service providers.

(3) The Authority includes the service in the list of digital services and its provider in the registry of digital service providers also based on its own findings.

(4) The Authority announces to the provider of digital service including the service in the list of digital services and its provider in the registyr of digital service providers.

(5) The digital service provider is obliged to report any changes in the details according to Paragraph 1 within 30 days.

Article 22
Obligations of the Digital Service Provider

(1) The digital service provider is obliged within six months from the notification date of inclusion in the registry of digital service providers, take and carry out suitable and adequate security measures according to a specific legal regulation [24]) for the purposes of managing the risks related to jeopardizing digital service continuity and the cybersecurity incidents handling procedure. For this purpose, the digital service provider is obliged to allocate sufficient human, material and technical, time and financial resources so as to ensure digital service continuity.

(2) For the purpose of meeting the obligation according to Paragraph(1, the digital service provider assesses mainly

a) network and information system security and its ability to prevent and handle a cybersecurity incident,
b) the method of maintaining digital service continuity in case of a cybersecurity incident,
c) compliance of networks and information systems with the security standards in the field of cybersecurity.

(3) The digital service provider is obliged to

a) report immediately every cybersecurity incident if he has information, based on which it is possible to identify whether the cybersecurity incident has a substantial impact according to the specific legal regulation[24]) ,
b) handle the reported cybersecurity incident,
c) cooperate with the Authority during handling the reported cybersecurity incident.

(4) If a digital service provider uses operator of essential services for the provision of its digital service, it is obligeds to conclude a contract with the operator of essential services on carrying out of security measures and notification obligations under this Act during the entire term when the digital service provider uses the services of the operator of essential services for the provision of its digital service.

(5) The digital service provider shall informs a third part to the necessary extent of the reported cybersecurity incident should the performance of the contract become impossible, unless otherwise decided by the Authority. The secret obligation is hereby not affected.

Article 23
Representative of the digital service provider

(1) The representative of the digital service provider is a legal entity with registered seat in the Slovak Republic, or a natural person - entrepreneur having its place of business in the Slovak Republic, unless

---

[24]) Commission Implementing Regulation (EU) ... / ... laying down rules for application of Directive (EU) 2016/1148 of the European Parliament and of the Council as regards further specification of the elements to be taken into account by digital service providers for managing the risks posed to the security of network and information systems and of the parameters for determining whether an incident has a substantial impact.

otherwise stated in Paragraph 2, and which is authorised by the digital service provider in writing to act on its behalf and under its responsibility in relation to the obligations under this Act.

(2) If the digital service provider providing digital service in the Slovak Republic, does not have its registered seat in the European Union and has not appointed its representative in another member state of the European Union, it is obliged to appoint its representative in the Slovak Republic.

(3) If the digital service provider has its registered seat in the Slovak Republic or has its appointed representative here, but its networks and information systems are located in another European Union member state, the Authority will cooperate with the relevant authority of the member state of the European Union in carrying out state administration.

Article 24
Cybersecurity Incidents Reporting by the Operator of Essential Services

(1) The operator of essential services is obliged to report every serious cybersecurity incident, identified based on exceeding the criteria for individual categories of serious cybersecurity incidents.

(2) A serious cybersecurity incident is divided into the first category of Level (I), second category of Level (II), and third category of Level (III) according to the depending on

a) the number of users of the essential services or digital service affected by the cybersecurity incident,
b) duration of the cybersecurity incident,
c) geographic spread of the cybersecurity incident,
d) level of impediment to the functioning of the essential services or digital service,
e) scope of impact of the cybersecurity incident on the economic and social activities of the state.

(3) If the operator of essential service uses a digital service provider for provision of the essential services, the digital service provider is obliged to report every serious cybersecurity incident that affected the digital service provider.

(4) The cybersecurity incidents reporting is carried out through the Cybersecurity Single Information System.

(5) If until the cybersecurity incident reporting its effects have not ceased to exist, the operator of essential service is obliged to send an incomplete report of the cybersecurity incident, indicating the identifier of the unfinished report and complete this report immediately after restoration of due operation of the network and information system.

(6) For the purposes of cybersecurity incidents reporting and ensuring the functionality of the Cybersecurity Single Information System, the Authority may, instead of the procedure stated in Article 8 (6), conclude a written contract with the operator of essential services on the manner and form of cybersecurity incidents reporting.

Article 25
Cybersecurity Incidents Reporting by the Digital Service Provider

(1) The digital service provider is obliged to report a cybersecurity incident according to Article 22 (3) item a) in the manner as stated in Article 24 (4).

(2) If until the cybersecurity incident reporting its effects have not ceased to exist, the digital service provider is obliged to send an incomplete report of the cybersecurity incident, indicatinge the identifier of the unfinished report and completes this report immediately after restoration of due operation of the network and information system.

(3) For the purposes of cybersecurity incidents reporting and ensuring the functionality of the Cybersecurity Single Information System, the Authority may, instead of the procedure stated in Article 8 (6), conclude a written contract with the digital service provider on the manner and form of cybersecurity incidentsreporting .

Article 26
Voluntary Cybersecurity Incidents Reporting

(1) Voluntary cybersecurity incidents reporting, regardless of categorisation of the cybersecurity incident, is carried out through the Cybersecurity Single Information System.

(2) The Authority processes and analyses voluntary reports of cybersecurity incidents in the scope enabled by the technical conditions and capacities of the Authority so as to to prevent inadequate overload of the entities and not to restrict international cooperation.

Article 27
Cybersecurity Incidents Handling

(1) In case of a serious cybersecurity incident or its threat, the Authority may

a) declare an alert and warning of serious cybersecurity incidents,
b) impose obligation to handle cybersecurity incident,
c) impose obligation to take reactive measures,
d) require draft measures and their execution to prevent further continuation, spreading, and repeated occurrence of the serious cybersecurity incident (hereinafter referred to as "safeguard measure").

(2) The Authority declares alerts and warnings through the Cybersecurity Single Information System. If an urgent national interest is concerned, the alert and warning is also declared through the mass media [25]) and on the Central Portal of Public Administration.

(3) The obligation to handle a cybersecurity incident is imposed by the Authority in a decision to the entity fulfilling the tasks of CSIRT Unit, to the operator of essential service and the digital service provider.

(4) Reactive measure is a direct response to a serious cybersecurity incident and is ensured by the services according to Article 15 (3) items b) to g).

(5) The obligation to take reactive measures is imposed by the Authority in a decision to the operator of essential service and the digital service provider, which are not active in handling the serious cybersecurity incident, or if the handling of the serious cybersecurity incident is obviously unsuccessful. The digital service provider may only be imposed to carry out reactive measures during a crisis situation.[26])

(6) The operator of essential service or the digital service provider is obliged to immediately report and prove, through the Cybersecurity Single Information System, execution of the reactive measure and its outcome.

(7) Safeguard measures are taken by the operator of essential services based on the analysis of the handled serious cybersecurity incident.

---

[25]) For example, Article 16 (3) item j) of the Act No. 308/2000 Coll. on Broadcasting and Retransmission and on Aendments and Supplements to the Act No. 195/2000 Coll. on Telecommunications, as amended, Article 6 (1) of the Act No. 167/2008 Coll. on Periodicals and Agency News and on Amendments and Supplements to some Acts (Press Act).

[26]) Act No. 387/2002 Coll., as amended.

(8) The operator of essential service is obliged, upon the call of the Authority, to submit the proposed safeguard measure for approval. The Authority approves the proposed measure in a decision and determines the period for its execution. Ift the operator of essential services does not propose a safeguard measure within the stated period, or if the proposed safeguard measure is obviously unsuccessful, the operator of essential service is obliged to cooperate with the Authority, the competent body and the entity operating the CSIRT Unit while preparing its proposal.

(9) If for the purposes of cybersecurity assurance, the Authority exhausts all manners of handling the serious cybersecurity incident under this Act, it shall submit information on the assumed impacts of the cybersecurity incident on the security of the state to the Security Council of the Slovak Republic as base for the crisis situation handling.[27])

(10) Due to the immediate necessity and urgency of handling the serious cybersecurity incident, for the purpose of cyber defence[28]), the Authority informs Military Intelligence that the serious cybersecurity incident is of Level III category or on the facts suggesting that the serious cybersecurity incident may be cyber terrorism. The operator of essential service and digital service provider reporting this cybersecurity incident, for the purposes of ensuring cyber defence, are obliged to provide information to Military Intelligence in the necessary extent. The Authority informs the chairman of the Security Council of the Slovak Republic on the procedure according to the first sentence.

Article 28
Inspection

(1) When conducting inspection of compliance with the provisions of this Act and its implementing regulation, the Authority operates on the basis of the basic rules for inspection activities stated in a specific legal regulation.[29])

(2) For the purposes of conducting an inspection the operator of essential service and the digital service provider have the rights and obligations of an inspected entity under a specific legal regulation[30]).

(3) The Authority carries out an inspection at the digital service provider if there is reasonable ground that the digital service provider does not meet the requirements determined by this Act.

Article 29

Audit

(1) The operator of essential service is obliged to verify the efficiency of the security measures adopted and meeting of the requirements stated by this Act by performing a cybersecurity audit within two years from inclusion of the operator of essential service in the registry of operators of essential services.

(2) The operator of essential services must verify the efficiency of the adopted security measures and meeting of the requirements stated by this Act by conducting an audit of cybersecurity in the scope defined according to a generally binding legal regulation issued by the Authority, with regard to the classification of information and categorisation of networks and information systems after each change having a significant impact on the carried out security measures and in the determined time interval.

---

[27]) For example, Article 1 (4) of the Constitutional Act No. 227/2002 Coll. on National Security in Time of War, State of War, Extraordinary State and State of Emergency, Article 2 item a) of the Act No. 387/2002 Coll.
[28]) Article 2 (2) of the Act No. 319/2002 Coll., as amended by the Act No. .../2018 Coll.
[29]) Articles 8 to 13 of National Council of the Slovak Republic Act No. 10/1996 Coll. on Control in Public Administration, as amended.
[30]) Article 12 of the Act of the National Council of the Slovak Republic No. 10/1996 Coll. as amended.

(3) The cybersecurity audit is carried out by the conformity assessment body according to a specific legal regulation,[31]) accredited as conformity assessment body in the field of cybersecurity.

(4) The operator of essential service is obliged to submit a final report on the results of the audit to the Authority together with the remedial measures and deadlines for their elimination within 30 days from the audit completion.

(5) Notwithstanding Paragraph 1, the Authority may, at any time, perform cybersecurity audit at the operator of essential service, or ask the conformity assessment body to perform such an audit at the operator of essential service with the aim to confirm the efficiency of the adopted security measures and meeting of the requirements stated in this Act.

(6) The costs of cybersecurity audit according to Paragraph 1 are borne by the operator of essential service and the costs of cybersecurity audit according to Paragraph 5 by the Authority.

Article 30
Offences

(1) A natural person commits an offence by

a) violatings the obligation specified in Article 12 (1),
b) providing false information in the notification according to Article 17 (5),
c) violating any of the obligations under Article 19 (1) to (4), (6) or (7),
d) not adopting security documentation under Article 20 (5), or
e) not having proceeded in compliance with the technical, organisational or personnel measures adopted by the operator of essential service.

(2) The Authority may levy a fine from EUR 100 to EUR 5,000 for an offence.

(3) The general regulation on offences[32]) is applied to offences and related hearings.

(4) The offences are heard by the Authority and the Authority levies the fines.

(5) Fines for offences constitute state budget revenue.

Article 31
Administrative Offences

(1) The Authority shall levy a fine from EUR 300 to EUR 30,000 against providers of essential service that commit an administrative offence by violating the obligation

a) under Article 19(2) to (4) or (7), or
b) to keep the security documentation up-to-date and conforming to the real state according to Article 20 (5).

(2) The Authority shall levy a fine from EUR 300 up to 1% from the total annual turnover for the previous accounting year, though not exceeding EUR 300,000, to the operator of essential service that commits an administrative offence by violating the obligation

---

[31]) Article 2 (13) of the Regulation (EC) No 765/2008 of the European Parliament and of the Council of 9 July 2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing Regulation (EEC) No 339/93 (OJ EU L 218, 13/) 08/ 2008).

[32]) Act of the Slovak National Council No. 372/1990 Coll. on Offences, as amended.

a) according to Article 17 (1),
b) according to Article 19 (1) or (6),
c) to adopt security documentation under Article 20 (5),
d) to report a serious cybersecurity incident according to Article 24 (1) or to send incomplete report according to Article 24 (5),
e) to handle a cybersecurity incident based on decision of the Authority according to Article 27 (3), to execute reactive measures based on decision of the Authority according to Article 27 (5) or to announce and prove execution of a reactive measure and its result according to Article 27 (6),
f) to submit safeguard measures for approval or to execute the approved safeguard measures according to Article 27 (8),
g) under Article 29 (1), (2) or (4), or
h) to execute a remedial measure by the deadline according to the final report on the audit results according to Article 29.

(3) The Authority will levy a fine from EUR 300 to EUR 30,000 against a digital service provider that commits an administrative offence by violating the obligation under Article 21 (5), Article 22 (4), or Article 23 (2).

(4) The Authority will levy a fine from from EUR 300 up to the amount of 1% from the total annual turnover for the previous accounting year, though not exceeding EUR 300,000, to the digital service provider that commits an administrative offence by violating the obligation under Article 21 (1), Article 22 (3), Article 24 (3), Article 25 (1) or (2) or the obligation to execute the reactive measure based on the decision of the Authority under Article 27 (5).

(5) The Authority will levy a fine from EUR 300 to EUR 100,000 against the entity that upon the call of the Authority does not provide information under Article 7 (3).

(6) When imposing a fine for an administrative offence, the Authority takes into consideration the severity of the offence, especially the manner in which it was committed, duration, consequences and the circumstances under which it was committed.

(7) The Authority shall levy a fine of up to double the amount laid out or calculated according to Paragraphs (1) to (6) if a repeated violation of obligations for which a fine was previously levied occurs within a period of one year from the date of the decision entry into force.

(8) The total annual turnover according to Paragraphs 2 to 4 for the purposes of this Act is understood as the sum of all sales, revenues or income from the sale of goods or services, without indirect taxes, that the provided financial aid is added to. The turnover expressed in foreign currency shall be converted to EUR; at the same time, for the foreign exchange conversion to EUR, the average of reference exchange rates will be used as stated and announced by the European Central Bank or the National Bank of Slovakia, valid at the respective accounting period.[33])

(9) For the purpose of this Act, under previous accounting period we understand the accounting period for which the last financial statements were issued.

(10) Fines for administrative offences may be levied within two years from the date on which a violation is discovered and no later than four years from the date on which the violation occurred.

(11) Effective date for a fine for an administrative offence is 30 days from the date of the decision imposing the fine.

---

[33]) Article 219 (1) to (3) of the Treaty on the Functioning of the European Union, as amended (OJ EU C 326 26/ 10/ 2012). Article 28 (2) of the Act of the National Council of the Slovak Republic No. 566/1992 Coll., as amended.

(12) Fines for administrative offences constitute state budget revenue.

Article 32
Authorisation Provisions

(1) The Authority determines by its generally binding legal regulation

a) details of the technical and technological equipment and staffing of the CSIRT Unit [Article (14) item a)],
b) identification criteria of the operated service (Article 18),
c) contents of security measures, contents and structure of the security documentation and scope of the general security measures (Article 20 (1) and (5)),
d) security and expertize standards in the field of cybersecurity (Article 5 (1) item w), Article 20 (1)),
e) identification criteria for respective categories of cybersecurity incidents and details of cybersecurity incidents reporting (Article 24 (1) and (4)),
f) rules and scope of cybersecurity audit and details of accreditation of the conformity assessment bodies and on the contents of the final report on the cybersecurity audit results according to (Article 29 (1) to (4)).

(2) The competent body in cooperation with the Authority is authorised to issue a generally binding legal regulation determining the sectoral security measures in the scope of their competencies according to Annex No. 1 and in compliance with the security standards in the field of cybersecurity.

Article 33
Common Provisions

(1) The Administrative Procedure Code does not apply to the proceedings of the Authority pursuant to Article 13 (7), Article 16 (2) and (3), Article 17 (6), Article 21 (4) and Article 27.

(2) Information, data and reports pursuant to this Act shall be submitted to the Authority electronically by means of an electronic form, the template of which is published by the Authority through the Cybersecurity Single Information System and the Central Public Administration Portal as part of the electronic forms module.

(3) If a service meets the requirements for the essential service as well as a digital service, it is considered to be n essential service and is included only in the list of essential services and its operator is included in the registry of operators of essential services.

(4) If an essential service falls under several sections or subsections according to Annex No. 1, the competencies of this Act shall be exercised by the competent body designated by the Authority.

Temporary and Final Provisions
Article 34

(1) The Authority makes the Cybersecurity Single Information System available in accordance with Article 8 within 18 months from the entry into force of this Act.

(2) An entity existing on the date of the entry into force of this Act is obliged to notify the Authority pursuant to Article 18 (1) from the date of exceeding the identification criteria pursuant to Article 18 (1), at the latest six months after the entry into force of this Act.

(3) An entity existing on the date of the entry into force of this Act is obliged to submit the information pursuant to Article 21 (1) to the Authority within six months after the entry into force of this Act.

(4) The competent body is obliged to deliver to the Authority a list pursuant to Article 9 (1) item e) within 30 days from the date of detection of the exceeding of the identification criteria pursuant to Article 18 (1) by the service provider existing on the date of the entry into force of this Act, at the latest six months after the entry into force of this Act.

(5) By 9 November 2018, the Authority includes the service in the list of Essential services and its operator in the registry of operators of essential services if they are not yet listed; this applies also for digital service and its provider.

(6) Within two years from the date of the entry into force of this Act, the operator of essential service included in the registry of operators of essential services pursuant to Paragraph 5 is obliged to adopt security measures pursuant to Article 20.

(7) Within two years from the date of the entry into force of this Act, the digital service provider included in the registry of digital service providers pursuant to Paragraph 5 is obliged to adopt security measures pursuant to Article 22 (1).

(8) Contracts concluded for the performance of activities pursuant to Article 19 (2) are to be put into accord with this Act by the operator of essential service at the latest two years after the date of the entry into force of this Act.

(9) The operator of essential service is required to submit to the cybersecurity audit and submit a final report on the audit results to the Authority at the latest three years after the expiry of the period under Paragraph 5.

(10) With regards to the establishment of the Government CSIRT Unit according to Article 11, from the date of the entry into force of this Act, the rights and obligations arising from state employment relations, labour law relations and other legal relations of employees ensuring carrying out of activities of the CSIRT Unit of the budget organization DataCentrum established by the Ministry of Finance of the Slovak Republic (hereinafter referred to as the "DataCentrum"), as well as rights and obligations arising from other legal relations related with these activities, transfer from the DataCentrum and the Ministry of Finance of the Slovak Republic to the Office of the Deputy Prime Minister for Investment and Informatization of the Slovak Republic. The state property, which was managed by DataCentrum or the Ministry of Finance of the Slovak Republic by 31 March 2018 and serves to ensure carrying out of the activities of the CSIRT Unit of DataCentrum, transfers to the Office of the Deputy Prime Minister for Investment and Informatization of the Slovak Republic since the date of the entry into force of this Act. Details on transfer of these rights and obligations and on the transfer of state property management are settled by an agreement between the Ministry of Finance of the Slovak Republic, DataCentrum and the Office of the Deputy Prime Minister for Investments and Informatization of the Slovak Republic stating especially the type and extent of the property, rights and obligations to be transferred.

Article 35

This Act adopts the legally binding acts of the European Union listed in Annex No. 3.

Section II

Act of the National Council of the Slovak Republic No. 198/1994 Coll. on Military Intelligence as amended by Act No. 166/2003 Coll., Act No. 178/2004 Coll., Act No. 319/2012 Coll., Act No. 444/2015 Coll. and Act No. 281/2015 Coll. is amended as follows:

1. A new letter h) is inserted after letter g) of paragraph 1 of Article 2 and reads:

"h) activities and threats in cyberspace,[1ba])".

The previous letters h) to j) shall be marked as letters i) to k).

The footnote to reference 1ba reads:
"[1ba]) Article 3 (b) of Act No. .../2018 Coll. on Cybersecurity and on Amendments to some Acts."

2. A new paragraph 2 is inserted after paragraph 1 of Article 2 and reads:

"(2) Where necessary to prevent activities and threats under paragraph 1, Military Intelligence shall carry out appropriate security measures."

Previous paragraphs 2 to 6 are referred to as paragraphs 3 to 7.

3. Article 4a is inserted after Article 4 with the following text:

"§ 4a
Centre for Cyber Defence of the Slovak Republic

(1) Military Intelligence performs roles in the area of cyberspace defence (hereinafter referred to as "cyber defence")[2d]) and cybersecurity to the extent set forth in a specific legal regulation,[2e]) through the Centre for Cyber Defence of the Slovak Republic (hereinafter referred to as the "Centre"), which is a special organisational unit of the Military Intelligence.

(2) The Centre acquires, concentrates, analyses and evaluates information relevant to cyber defence, informs affected parties and suggests appropriate measures.

(3) The Centre is entitled to require compliance from the owner or operator of facilities of special importance, other important facilities[2f]) and critical infrastructure elements[2g]), as well as information to the extent necessary to ensure cyber defence.

(4) In order to ensure the fulfilment of tasks under this Act, the Centre shall have direct and full real-time electronic access to the Cybersecurity Single Information System of [2h])".

The footnotes to references 2d to 2h read:

"[2d]) Article 2 (2) of Act No. 319/2002 Coll. on Defence of the Slovak Republic, as amended by Act No. .../2018 Coll.
[2e]) Act No. .../2018 Coll.
[2f]) Article 27 (5) of Act No. 319/2002 Coll. as amended by Act No. 330/2003 Coll.
[2g]) Article 2 a) of Act No. 45/2011 Coll. on Critical Infrastructure.

[2h]) Article 8 of Act No. .../2018 Coll.".

4. A new article 14 b is inserted after article14 a with the following text:

“14b

Unless it is contrary to the specific legal regulation, 4) so as to prevent activities and threats according to Article 2 Paragraph 1, the Military Intelligence is authorized to acquire, accumulate and evaluate information derived from signals in the electromagnetic spectre. While fulfilling these tasks the Military intelligence is regarded as national authority with reference to national and foreign authorities with similar subject field and competencies. "

Section III.

Act No. 73/1998 Coll. on the Civil Service of the Police Force, the Slovak Information Service, the Prison and Judicial Guards Corps of the Slovak Republic and the Railway Police as amended by Act No. 58/1999 Coll., Act No. 181/1999 Coll., Act No. 356/1999 Coll., Act No. 224/2000 Coll., Act No. 464/2000 Coll., Act No. 241/2001 Coll., Act No. 98/2002 Coll., Act No. 328/2002 Coll., Act No. 422/2002 Coll., Act No. 659/2002 Coll., Act No. 212/2003 Coll., Act No. 201/2004 Coll., Act No. 178/2004 Coll , Act No.365/2004 Coll., Act No. 382/2004 Coll., Act No. 201/2004 Coll., Act No. 732/2004 Coll., Act No. 201/2004 Coll., Act No. 727/2004 Coll., Act No. 69/2005 Coll., Act No. 69/2005 Coll., Act No. 623/2005 Coll., Act No. 342/2007 Coll., Act No. 513/2007 Coll., Act No. 61/2008 Coll., Act No. 278/2008 Coll., Act No. 491/2008 Coll., Act No. 445/2008 Coll., Act No. 70/2009 Coll., Act No. 60/2010 Coll., Act No. 151/2010 Coll., Act No. 543/2010 Coll., Act No. 547/2010 Coll., Act No. 48/2011 Coll., Act No. 79/2012 Coll., Act No. 361/2012 Coll., Act No. 345/2012 Coll., Act No. 80/2013 Coll., Act No. 462/2013 Coll., Act No. 307/2014 Coll., Act No. 406/2015 Coll. and Act No. 125/2016 Coll. is amended as follows:

1. A new letter t) is added to Article 84 (2) and reads:

"t) bonus for performing cybersecurity activities."

2. A new Article 102c is inserted after Article 102b and reads:

"§ 102c
Supplementary Payment for Special Activities

(1) A supplementary payment of up to 90% of the total of the salary and the upper limit of the years' retirement allowance may be granted to a policeman performing particularly significant tasks or extremely demanding activities in the field of cybersecurity.

(2) The supplementary payment referred to in Paragraph 1 shall is to be determined by the Minister depending on the complexity, responsibility and extent of cybersecurity activities.

(3) The supplementary payment referred to in Paragraph 1 is to be rounded up to 50 euro cent.".

Section IV

Act No. 483/2001 Coll. on Banks and on Amendments to Some Acts as amended by Act No. 430/2002 Coll., Act No. 510/2002 Coll., Act No. 165/2003Coll., Act No. 603/2003 Coll., Act No. 215/2004 Coll., Act No. 554/2004 Coll., Act No. 747/2004 Coll., Act No. 69/2005 Coll., Act No. 340/2005 Coll., Act No. 341/2005 Coll., Act No. 214/2006 Coll., Act No. 644/2006 Coll., Act No. 209/2007 Coll., Act No. 659/2007 Coll., Act No. 297/2008 Coll., Act No. 552/2008 Coll., Act No. 66/2009 Coll., Act No. 186/2009 Coll., Act No. 276/2009 Coll., Act No. 492/2009 Coll., Act No. 129/2010 Coll., Act No. 46/2011 Coll., Act No. 130/2011 Coll., Act No. 314/2011 Coll., Act No. 394/2011 Coll., Act No. 520/2011 Coll., Act No. 547/2011 Coll., Act No. 234/2012 Coll., Act No. 352/2012 Coll., Act No. 132/2013 Coll., Act No. 352/2013 Coll., Act No. 213/2014 Coll., Act No. 371/2014 Coll., Act No. 374/2014 Coll., Act No. 35/2015 Coll., Act No. 252/2015 Coll., Act No. 359/2015 Coll., Act No. 392/2015 Coll., Act No. 405/2015 Coll., Act No. 437/2015 Coll., Act No. 90/2016 Coll., Act No. 91/2016 Coll., Act No. 125/2016 Coll., Act No. 292/2016 Coll., Act No. 298/2016 Coll., Act No. 299/2016 Coll., Act No. 315/2016 Coll., Act No. 386/2016 Coll. and Act No. 2/2017 Coll. is amended as follows:

Article 91 shall be supplemented by paragraph 13, which reads as follows:

"(13) Compliance with the obligation of a bank, a foreign bank and branches of a foreign bank to notify the National Security Authority for the purposes of fulfilment of their obligations in the field of cybersecurity according to a special regulation shall not be considered a breach of bank secrecy.[86j])".

The footnote to reference 86j reads:
"[86j]) Act No. ...../2018 Coll. on cybersecurity and on the amendment of certain Acts.".

Section V

Act No. 319/2002 Coll. on the Defence of the Slovak Republic as amended by Act No. 330/2003 Coll., Act No. 545/2003 Coll., Act No. 570/2005 Coll., Act No. 333/2007 Coll., Act No. 452/2008 Coll., Act No. 473/2009 Coll. and Act No. 345/2012 Coll. is amended as follows:

1. A new paragraph 2 is inserted after paragraph 1 of Article 2 and reads:

"(2) State defence is also provided in cyberspace[1a]) through measures aimed at addressing serious cyber-security incidents according to a specific legal regulation[1b]) and the defence of facilities of particular importance, other important facilities and elements of critical infrastructure[1c]) from a cyber attack; such defence is provided by the Military Intelligence.[1d])".

Previous paragraphs 2 to 5 are referred to as paragraphs 3 to 6.

The footnotes to references 1a to 1c read:

"[1a]) Article 3 (b) of Act No. .../2018 Coll. on Cybersecurity and on Amendments to Some Acts.
[lb]) Article 27 (10) of Act No. .../2018 Coll.
[1c]) Article 2 a) of Act No. 45/2011 Coll. on Critical Infrastructure.
[ld]) Article 4a of the Act of the National Council of the Slovak Republic No. 198/1994 Coll. on Military Intelligence as amended by Act No. .../2018 Coll.".

2. At the end of Article 6 f), the comma is replaced by a semicolon and the following words are added: "§ 2 (2) applies to the protection of facilities of special importance and other important facilities in cyberspace,".

3. A new paragraph 2 is inserted after paragraph 1 of Article 18 and reads:

"(2) In the field of cyberspace defence of the state, business entities are required to provide the Military Intelligence with the requested co-operation and information important for securing the state's defence in the cyberspace.[15d])".

The previous paragraph 2 shall be marked as paragraph 3.

The footnote to reference 15d reads:

„[15d]) Article 4a (3) of the Act of the National Council of the Slovak Republic No. 198/1994 Coll. as amended by Act No. ... /2018 Coll.".

Section VI

Act No. 215/2004 Coll. on the Protection of Classified Information and on Amendments to some Acts as amended by Act No. 638/2005 Coll., Act No. 255/2006 Coll., Act No. 330/2007 Coll., Act No. 668/2007 Coll., Act No. 290/2009 Coll., Act No. 400/2009 Coll., Act No. 192/2011 Coll., Act No. 122/2013 Coll., Act No. 195/2014 Coll., Act No. 261/2014 Coll., Act No. 362/2014 Coll., Act No. 247/2015 Coll., Act No. 338/2015 Coll., Act No. 91/2016 Coll., Act No.125/2016 Coll., Act No. 340/2016 Coll., Act No. 301/2016 Coll., Act No. 51/2017 Coll. and Act No. 152/2017 Coll. is amended as follows:

1. In Article 24 Paragraph 2 item d) word “or” in the end is replaced by a comma.

2. In Article § 24 Paragraph 2 item e) full stop in the end of sentence is deleted and word “or” is added.
3. new letter f) is added to Article 24 (2) and reads:
"f) the proposed person fails to attend the security interview at the invitation of the Authority; Article 27 (4) applies to the request of the Authority accordingly.".

4. In Article 35 (2), the words "a person acting in favour of authorities according to specific legal regulations" shall be followed by a comma and the words "a person based on an agreement according to a specific legalregulation[18a])".

Footnote 18a reads:
"[18a]) Article 5 (2) of Act No. .../2018 Coll. on Cybersecurity and on Amendments to Some Acts.".5. Article 60 shall be supplemented by paragraph 9, which reads as follows:

"(9) Paragraphs 3 to 6 shall not apply to the provision of classified information between the armed forces of the Slovak Republic and the armed forces of another state, alliance and coalition partner or partner in a military operation under bilateral cooperation pursuant to a specific legal regulation[23a]); Minister of Defence shall decide on the provision of classified information under the preceding sentence and keep records of such decision."

Footnote 23a reads:
"[23a]) Article 11 (1) of Act No. 321/2002 Coll. on the Armed Forces of the Slovak Republic, as amended.".66. In Article 64, the paragraphs 2 and 3 shall be omitted.

The previous paragraph 4 shall be marked as paragraph 2.

7. In Article 64 (2), the word "Applicant" shall be replaced by "Entrepreneur under Paragraph 1".

1.

Section VII

Act No. 45/2011 Coll. on Critical Infrastructure is amended as follows:

1. In Article 1, paragraph 2 is deleted, including the footnote to reference 1. At the same time, the designation of paragraph 1 is deleted.

I

2. In Article 3 c), the words "Ministry of Finance of the Slovak Republic, Ministry of Transport, Construction and Regional Development of the Slovak Republic" shall be replaced by the words "Office of the Deputy Prime Minister for Investments and Informatization and the Ministry of Transport and Construction of the Slovak Republic".

3. In Article 9, the paragraph 4 shall be omitted.

4. In Article 10 (2), the words "security elements of information systems" shall be replaced by “security measures according to a specific legalregulation[4a])".

Footnote 4a reads:
"[4a]) Article 20 of Act No. .../2018 Coll. on Cybersecurity and on Amendments to some Acts.".

5. Annex No. 3 reads as follows (including the title):

"Annex No. 3 to Act No. 45/2011 Coll.

AREAS OF COMPETENCE OF CENTRAL AUTHORITIES

Sector	Sub-sector	Competent body

1. Transport	Road transport Air transport Water transport Rail transport	Ministry of Transport and Construction of the Slovak Republic
2. Electronic communications	Satellite communication Networks and services of fixed electronic communications and mobile electronic communications	Ministry of Transport and Construction of the Slovak Republic
3. Power engineering	Mining Electrical power Gas industry Petroleum and petroleum products	Ministry of Economy of the Slovak Republic
4. Post office	Provision of postal services, postal payments and procurement services	Ministry of Transport and Construction of the Slovak
5. Industry	Pharmaceutical industry Metallurgical industry Chemical industry	Ministry of Economy of the Slovak Republic
6. Public administration	Public administration information systems	Office of the Deputy Prime Minister for Investments and
7. Water and air	Weather service	Ministry of the Environment
	Water structures Provision of drinking water	of the Slovak Republic
8. Health care		Ministry of Health of the Slovak Republic

Section VIII.

Act No. 351/2011 Coll. on Electronic Communications as amended by Act No. 241/2012 Coll., Act No. 547/2011 Coll., Act No. 352/2013 Coll., Act No. 402/2013 Coll., Act No. 128/2014 Coll., Act No. 402/2013 Coll., Act No. 139/2015 Coll., Act No. 247/2015 Coll., Act No. 269/2015 Coll., Act No. 97/2015 Coll., Act No. 444/2015 Coll. Act No. 391/2015 Coll., Act No. 247/2015 Coll., Act No. 125/2016 Coll., Act No. 353/2016 Coll. and Act No. 386/2016 Coll. is amended as follows:

1. Article 8 shall be supplemented by paragraph 3, which reads as follows:

"(3) In exercising the competencies of the Authority as defined by this Act and the competencies of the National Security Authority established by a specific legal regulation[46d]), these authorities exchange the information and documents necessary to ensure cybersecurity in the scope and manner established by the concluded cooperation agreements. In the case of an exchange of information, the receiving body shall ensure the same level of confidentiality as the body providing the information.". The footnote to reference 46d reads:
"[46d]) Act No. .../2018 Coll. on Cybersecurity and on Amendments to Some Acts.".

2. Article 63 shall be supplemented by paragraph 17, which reads as follows:

"(17) The data subject to telecommunications secrecy under paragraph 1 b) to d) may be made available to the National Security Authority in the interest of state security for the purpose of cybersecurity incident handling, for the purpose of collection, processing and storage to the extent necessary to identify the cybersecurity incident and to ensure cybersecurity under the general cyber-security regulation.[46d])".

Section IX.

Act no 305/2013 on Electronic Form of Governance Conducted by Public Authorities and on Amendments to some Acts (E-Government Act) as amended by Act No. 214/2014 Coll., as amended by Act No. 29/2015 Coll., as amended by Act No. 130/2015 Coll., as amended by ActNno. 273/2015 Coll., as amended by Act No. 272/2016 Coll., as amended by Act No. 374/2016 Coll., as amended by Act No. 238/2017 Coll. is amended as follows:

In Article 60b paragraph 3 the words " 1 May 2018" are replaced by words "1 February 2019" and words " 30 April 2018" are replaced by "31 January 2019".

Section X.

Act No. 281/2015 Coll. on the Civil Service of Professional Soldiers and on Amendments to Some Acts, as amended by Act No. 378/2015 Coll. and Act No. 125/2016 Coll. is amended as follows:

1. A new letter i) is inserted after letter h) of Article 156 (1) and reads: "i) supplementary payment for special activities ,".

The previous letters i) to k) shall be marked as letters j) to l).

2. In Article 156 (2), the words "letters a) to i)" shall be replaced by the words "letters a) to j)".

3. Article 164a is inserted after Article 164 with the following text:

"**164a**
Supplementary Payment for Special Activities

(1) A professional soldier who carries out an activity that requires the execution of particularly important tasks or extremely demanding tasks in the field of cybersecurity may be awarded a supplementary payment for special activities of up to 90% of his/her salary.

(2) The positions and amount of the supplementary payment under Paragraph 1 are to be detailed in the Staff Regulations.

(3) The supplementary payment referred to in Paragraph 1 shall be rounded up to 50 euro cent.".

Article XI

This Act shall enter into force on 1 April 2018, with the exception of the provision in Section I Article 12 (6), which shall enter into force on 25 May 2018.

The President of the Slovak Republic

The Chairman of the National Council of the Slovak Republic

The Prime minister of the Slovak Republic

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

Sector	Sub-sector	Service provider	Competent body
1. Banking		**Credit institutions** whose business is to receive deposits or other repayable funds from the public and to provide loans on their own account	Ministry of Finance of the Slovak Republic
		Administrators, operators and persons providing Treasury activities pursuant to the Act No. 291/2002 Coll. on State Treasury and Amendment and Supplements of certain Acts as amended	
2. Transport	Road transport	**Road transport authorities responsible for road traffic inspection** - any public body responsible for the planning, inspection or management of roads falling within its territorial jurisdiction	Ministry of Transport and Construction of the Slovak Republic

		Operators of smart transport systems using information and communication technologies in the field of road transport, including infrastructure, vehicles and users, and in the field of traffic management and mobility management as well as interfaces with other modes of transport	

		Administrators and operators of networks and information systems that are a component of critical infrastructure under Act No. 45/2011 Coll. on Critical Infrastructure, or which are directly connected to it	
	Air transport	**Air carrier** - an air transport provider with a valid operating license or its equivalent	
		Airport managing body - an entity which, with or without other activities, according to the situation, national laws, other legislation or contracts, serves to control and manage the infrastructure of an airport or airport network and coordination and inspection of the activities of individual operators at the airports concerned or in the relevant airport networks, airports, including main airports, and entities operating ancillary facilities located at airports	
		Operators providing air traffic control services (ATC) such as services for the purposes of a) collisions prevention - of aircrafts and - in the airspace between the aircraft and the obstacles; and a) speeding up and maintaining a proper air traffic flow	
		Administrators and operators of networks and information systems that are a component of critical infrastructure under Act No. 45/2011 Coll. on Critical Infrastructure, or which are directly connected to it	
	Water transport	**Companies operating inland, sea and coastal passenger and freight waterways**	
		Managing authorities of the port - as any designated part of land and water with the boundaries defined by the Member State where the port is situated, including establishments and facilities designed to facilitate the operation of commercial maritime transport; including their port facilities, where the ship and the port come into contact; these include areas such as anchorages, berths and access points from the sea, as appropriate, and entities operating activities and facilities within the port	

		Shipping and navigation service operators as a service designed to increase the safety and efficiency of ship transport and to protect the environment, which is capable of interacting with traffic and can respond to traffic situations arising in the field of shipping and navigation services	
		Administrators and operators of networks and information systems that are a component of critical infrastructure under Act No. 45/2011 Coll. on Critical Infrastructure, or which are directly connected to it	
	Rail transport	**Infrastructure operator** - any body or business entity responsible in particular for the establishment, management and maintenance of the railway infrastructure, including traffic control, security and alert management. Infrastructure operator functions in the network or part of the network may be entrusted to	
		Railway undertakings - any public or private undertaking, the principal activity of which is to provide services for the purpose of securing the transport of goods or persons by rail, providing traction; this includes only traction enterprises, including service facility operators - any public or private entity responsible for managing one or more service facilities or providing one or more key services to railway undertakings	
		Administrators and operators of networks and information systems that are a component of critical infrastructure under Act No. 45/2011 Coll. on Critical Infrastructure, or which are directly connected to it	
3. Digital infrastructure		**Provider of the Internet exchange node service** to interconnect networks that are separate from the technical and organisational point of view	National Security Authority
		Provider of domain name system services on the Internet	
		Entity managing or operating a register of top-level Internet domains	
4. Electronic communications	Satellite communication	**Administrators and operators of networks and information systems that are a component of critical infrastructure** under	Ministry of Transport and Construction

		Act No. 45/2011 Coll. on Critical Infrastructure	Slovak Republic
	Networks and services of fixed and mobile electronic communications	**Administrators and operators of networks and information systems that are a component of critical infrastructure** under Act No. 45/2011 Coll. on Critical Infrastructure	
5. Power engineering	Mining	**Administrators and operators of networks and information systems that are a component of critical infrastructure** under Act No. 45/2011 Coll. on Critical Infrastructure, or which are directly connected to it	Ministry of Economy of the Slovak Republic
	Electrical power	**Electricity undertakings** - any entity which carries out at least one of the following activities: production, transmission, distribution, supply or purchase of electricity, and which is responsible for commercial and technical tasks and/or maintenance in connection with these activities; this does not include end-users who sell electricity to customers, including resale	
		Distribution system operators - any entity responsible for the operation, maintenance and, where necessary, the development of the distribution system in the area concerned and, where appropriate, the development of its interconnection with other systems and ensuring the long-term ability of the system to meet reasonable demand for electricity distribution	
		Transmission system operators - any entity responsible for the operation, maintenance and development of the transmission system in the area concerned and, where appropriate, the development of its interconnection with other systems and ensuring the long-term ability of the system to meet reasonable demand for electricity transmission	
		Administrators and operators of networks and information systems that are a component of critical infrastructure under Act No. 45/2011 Coll. on Critical Infrastructure, or which are directly connected to it	
	Gas industry	**Supplier companies** - any entity which carries out sale, including resale, of natural gas, including LNG, to customers	
		Distribution network operators - any entity which carries out the distribution and is responsible for the operation, maintenance and, if necessary, the development of the distribution network in the area, or its interconnection with	

		other networks, and which ensures the long-term ability of the network to meet reasonable demand for natural gas distribution	
		Transport network operators - any entity which carries out the transport and is responsible for the operation, maintenance and, where necessary, the development of the transport network in the area, or its interconnection with other networks, and which ensures the long-term ability of the network to meet reasonable demand for natural gas	
		Storage operators - any entity which performs storage and is responsible for the operation of the container	
		LNG facility operators - any entity which carries out liquefaction of natural gas or import, unloading and re-gas of LNG and is responsible for the operation of the LNG facility	
		Gas undertakings - any entity carrying out at least one of the following activities: extraction, transport, distribution, supply, purchase or storage of natural gas, including LNG, which is responsible for commercial tasks, technical tasks and/or maintenance related to these activities, but does not include end-customers	
		Operators of natural gas refining and processing facilities	
		Administrators and operators of networks and information systems that are a component of critical infrastructure under Act No. 45/2011 Coll. on Critical Infrastructure, or which are directly connected to it	
	Petroleum and petroleum products	**Pipeline operators**	
		Operators of petroleum extraction, refining and processing facilities, storage and transport	
		Administrators and operators of networks and information systems that are a component of critical infrastructure under Act No. 45/2011 Coll. on Critical Infrastructure, or which are directly connected to it	
	Thermal energy	**Producers and suppliers of heat** according to Act No. 657/2004 Coll. on Thermal Energy	

6. Infrastructure of financial markets		**Operators of trade sites** pursuant to Act No. 429/2002 Coll. on the Stock Exchange, as amended.	Ministry of Finance of the Slovak Republic
		Central counterparties - a legal person entering between counterparties to contracts traded on one or more financial markets and becoming a buyer in relation to all sellers and a seller in relation to all buyers	
7. Post office	Provision of postal services, postal payments and procurement services	**Postal undertaking** providing one or more postal services or postal payment under the Postal Services Act	Ministry of Transport and Construction of the Slovak Republic
		Administrators and operators of networks and information systems that are a component of critical infrastructure under Act No. 45/2011 Coll. on Critical Infrastructure, or which are directly connected to it	
8. Industry	Pharmaceutical industry	**Manufacturer of medicinal products** pursuant to Act No. 362/2011 Coll. on Medicinal Products and Medical Devices and on Amendments to Some Acts, as amended	Ministry of Economy of the Slovak Republic
		Administrators and operators of networks and information systems that are a component of critical infrastructure under Act No. 45/2011 Coll. on Critical Infrastructure, or which are directly connected to it	
	Metallurgical industry	**Administrators and operators of networks and information systems that are a component of critical infrastructure** under Act No. 45/2011 Coll. on Critical Infrastructure, or which are directly connected to it	
	Chemical industry	**Suppliers, manufacturers, importers and downstream users of substances and mixtures** pursuant to Act No. 67/2010 Coll. on the conditions for marketing of chemical substances and chemical mixtures, as amended	
		Administrators and operators of networks and information systems that are a component of critical infrastructure under Act No. 45/2011 Coll. on Critical Infrastructure, or which are directly connected to it	
9. Water and air	Weather service	**Administrators and operators of the state hydrological network**	Ministry of Environment of the Slovak Republic
		Administrators and operators of networks and information systems that are a component of critical infrastructure under	

		Act No. 45/2011 Coll. on Critical Infrastructure or are directly connected to it	
		Administrators and operators of the state meteorological network	
		Administrators and operators of networks and information systems that are a component of critical infrastructure under Act No. 45/2011 Coll. on Critical Infrastructure, or which are directly connected to it	
	Water structures	**Administrators and operators of networks and information systems that are a component of critical infrastructure** under Act No. 45/2011 Coll. on Critical Infrastructure, or which are directly connected to it	
	Provision of drinking water	**Suppliers and distributors of water** for drinking, cooking, food preparation or other domestic purposes, irrespective of its origin and whether it has been supplied from the distribution network, tanks, bottles or containers; with the exception of distributors whose water distribution is only part of their overall activity in the distribution of other commodities and goods and is not regarded as	
		Administrators and operators of networks and information systems that are a component of critical infrastructure under Act No. 45/2011 Coll. on Critical Infrastructure, or which are directly connected to it	
10. Public administration	Security	**Administrators and operators of networks and information systems that are relevant to the security of the Slovak Republic**	Ministry of Interior of the Slovak Republic
	Public administration information systems	**Administrators and operators of networks and information systems of public administration** within the competence of the liable entity pursuant to Act No. 275/2006 Coll. supporting public administration services, public interest services and public services, as amended	Office of the Deputy Prime Minister for Investments and Informatization
		Administrators and operators of networks and information systems that are a component of critical infrastructure under Act No. 45/2011 Coll. on Critical Infrastructure, or which are directly connected to it	
	Defence	**Administrators and operators of networks and information systems that are relevant to the defence of the Slovak Republic**	Ministry of Defence of the Slovak Republic
	Intelligence services		

		Administrators and operators of networks and information systems operated by the intelligence service	Slovak Information Service
		Administrators and operators of networks and information systems operated by the intelligence service	Military Intelligence
	Classified information	**Administrators and operators of networks and information systems relating to classified information**	National Security Authority
11. Health care	Medical facilities (including hospitals and private clinics)	**Healthcare providers** - any person or any other entity legally providing healthcare in the territory of a Member State	Ministry of Health of the Slovak Republic
		Administrators and operators of networks and information systems that are a component of critical infrastructure under Act No. 45/2011 Coll. on Critical Infrastructure, or which are directly connected to it	

Types of digital services

(1) Online marketplace

(2) Internet search engine

(3) Cloud computing

Legend:

Online marketplace - a digital service that allows consumers or businesses to conclude an online purchase contract or service contracts with entrepreneurs either on the online store's website, or on the website of an enterprise using online computer services provided by the online marketplace.

Internet search engine - a digital service that allows users to search for any topic based on a keyword, sentence, or other input data in all websites or websites in a specific language, resulting in links to find information related to the required content.

Cloud computing service - a digital service that allows access to a scalable and flexible set of computing resources that can be shared.

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

List of adopted legally binding acts of the European Union

Directive 2016/1148 of the European Parliament and of the Council (EU) of 6 July 2016 on measures to ensure a high common level of network and information system security in the Union. (EU OJ L 194, 19 July 2016)