ACT

No 181/2014 Coll.

of July 23, 2014

on Cyber Security and Change of Related Acts

(The Act on Cyber Security)

as amended by Act No. 104/2017 Coll., Act No. 183/2017 Coll., Act No. 205/2017 Coll., Act No. 35/2018 Coll., Act No. 111/2019 Coll., Act No. 12/2020 Coll., Act No. 261/2021 Coll., Act No. 226/2022 Coll.

The Parliament has adopted the following Act of the Czech Republic:

PART ONE
CYBER SECURITY (Sections 1–33)

CHAPTER I
Basic provisions (Sections 1-3a)

Section 1
[Subject of the Act]

(1) This Act regulates the rights and obligations of persons and the competence and power of public authorities in the field of cyber security.

(2) This Act incorporates the relevant legislation of the European Union[6)], at the same time it follows up on a directly applicable legislation of the European Union[17)] and regulates the security of electronic communication networks and information systems.

(3) This Act shall not apply to information and communication systems handling classified information.

Definition of terms

Section 2

For the purpose of this Act:

a) Cyberspace means a digital environment enabling the creation, processing and exchange of information created by information systems and electronic communications services and networks[1)]

b) Critical information infrastructure means an element or system of elements of the critical infrastructure in the sector of communication and information systems[2)] within the field of cyber security

c) Security of information means ensuring confidentiality, integrity and availability of information

d) Important information system means an information system operated by a public authority that execute public powers that is neither a critical information infrastructure nor an information

system of essential service, and which may endanger or noticeably limit the execution of public powers in the case of an information security breach

e) Operator of the information system means an authority or a person that determines the purpose of the processing of information and the conditions for the operation of the information system

f) Operator of the communication system is an authority or a person, that determines the purpose of the communication system and the conditions for its operation

g) Administrator of the information or communication system is an authority or a person that ensures the functionality of technical and software tools that constitute the information or communication system

h) Important network means an electronic communication network[1)] providing direct international connectivity to public communication networks or providing direct connection to a critical information infrastructure

i) Essential service means a service the provision of which is dependent on electronic communication networks[7)] or information systems, and the disruption of which may have a significant impact on the security of societal or economic activities in any of the following sectors:

   1. Energy
   2. Transport
   3. Banking
   4. Financial market infrastructures
   5. Health sector
   6. Water resource management
   7. Digital infrastructure
   8. Chemical industry

j) Information system of essential service means an information system on which the provision of an essential service is dependent

k) Operator of an essential service means an authority or a person that provides the essential service and is identified by the National Cyber and Information Security Agency (hereinafter "the Agency") pursuant to Section 22a; for the purposes of meeting the information obligations according to the relevant legal regulation of the European Union[8)], also authorities and persons specified in Section 3, letters (c) and (d) are considered to be the operators of an essential service

l) Digital service means a service of information society according to the Act on Certain Information Society Services[9)] that consists of the provision of:

   1. An online marketplace that enables consumers and/or traders to conclude online sales or service contracts with traders[10)] either on the online marketplace's website or on a trader's website that uses computing services provided by the online marketplace
   2. A search engine that allows to perform searches of, in principle, all websites on the basis of a query on any subject in the form of a keyword, phrase or other input, and returns links in which information related to the requested content can be found, or

3. Cloud computing that enables access to a scalable and elastic pool of shareable computing resources

m) A relevant public authority means an authority in the field of cyber security

Section 3

Authorities and persons that are bound by obligations in the cyber security field are as follows:

a) An electronic communication service provider and an entity operating an electronic communications network[1)], unless they are authorities and persons specified in letter (b)

b) An authority or a person administrating an important network, unless they are the operator or the administrator of a communication system specified in letter (d)

c) An operator and an administrator of a critical information infrastructure information system

d) An operator and an administrator of a critical information infrastructure communication system

e) An operator and an administrator of an important information system

f) An operator and an administrator of an information system of essential service, unless they are the operator or the administrator specified in letters (c) or (d)

g) An operator of an essential service, unless they are the operator or the administrator specified in letter (f)

h) A digital service provider

Section 3a

[Representative of a digital service provider]

(1) A digital service provider that provides such service in the Czech Republic, does not have a registered office in the European Union and did not appoint a representative in another Member State of the European Union (hereinafter "another Member State"), is obliged to appoint a representative in the Czech Republic. A representative of a digital service provider is a person which is established in the Czech Republic and which is authorised to represent a digital service provider in relation to the obligations under this Act on the basis of power of attorney.

(2) When a digital service provider has a registered office outside the European Union and has appointed a representative in the Czech Republic, the provider is considered to be established in the Czech Republic and is subject to the obligations under this Act.

(3) When a digital service provider has a registered office in the Czech Republic or has an appointed representative here but the electronic communication networks and information systems this entity uses are located in another Member State, the Agency shall collaborate with the relevant public authority of the concerned Member State when performing its competences.

CHAPTER II

System for ensuring cyber security (Sections 4-20)

Security measures

Section 4

[Ensuring information security in information systems]

(1) Security measure means a set of actions aiming at ensuring the security of information in information systems and the availability and reliability of electronic communications services and networks[1)] in cyberspace.

(2) The authorities and persons specified in Section 3 letters (c) to (f) shall introduce and implement security measures to the extent necessary to ensure the cyber security of a critical information infrastructure information system, a critical information infrastructure communication system, an information system of essential service and an important information system, and to keep security documentation on them.

(3) A digital service provider shall introduce and implement appropriate and adequate security measures for the electronic communications networks and information systems the provider uses in connection with the provision of its service, taking into account information security, cyber security incident management, business continuity management, monitoring, auditing, testing and compliance with international regulations.

(4) The authorities and persons specified in Section 3 letters (c) to (f) shall take into account the requirements resulting from the security measures when selecting a supplier for their information or communication system and include those requirements in the contract they conclude with the supplier. Taking into account the requirements resulting from the security measures referred to in the first sentence to the extent necessary to fulfil the obligations under this Act shall not be regarded as an unlawful restriction of competition or an unjustified barrier to competition.

(5) Before concluding a contract with a cloud computing service provider, public authorities shall determine the security level of the requested cloud computing with regard to the nature of the information or communication system concerned in accordance with the implementing legislation and to ensure that the security rules for the provision of cloud computing services established by the Agency are complied with and that the information and data stored for them by the cloud computing service provider, including the possibility of real-time supervision of the stored information and data, are available to them upon request without undue delay.

(6) The cloud computing service provider and the public authority shall further agree in the contract on the manner and amount of reimbursement of the reasonable costs incurred for the implementation of the security rules and the implementation of the customer's security policy.

(7) Taking into account the requirements resulting from the security policy, security rules, security measures and other conditions agreed in the contract pursuant to paragraph 5, which are necessary for the fulfilment of the obligations under this Act, shall not be considered as an unlawful restriction of competition or an unjustified barrier to competition.

Section 4a

(1) Authorities and persons who became operators of information or communication systems of a critical information infrastructure, or operators of important information systems, and who are not administrators of such a system, are obliged to immediately and provably inform the

administrator of the system of this fact and the fact that this administrator became a public authority or a person specified in Section 3, letters (c), (d) or (e).

(2) Authorities and persons who became operators or administrators of information or communication systems of a critical information infrastructure are obliged to immediately and provably inform the entity operating the electronic communications network to which their concerned critical information infrastructure information system is connected to, of this fact and the fact that this entity fulfilled the requirements for becoming a public authority or a person specified in Section 3, letter (b).

(3) Authorities and persons that are identified as operators of an essential service pursuant to Section 22a and are not at the same time the operators or administrators of their information systems of essential service are obliged to immediately and provably inform the operator or the administrator of this information system of essential service of their identification and of the fact that the operator or the administrator fulfilled the requirements to becoming a public authority or a person specified in Section 3, letter (f).

Section 5

[Security, organisational and technical measures]

(1) Security measures are
   a) Organisational measures, and
   b) Technical measures.

(2) Organisational measures are
   a) Information security management system,
   b) Risk management,
   c) Security policy,
   d) Organisational security,
   e) Setting security requirements for suppliers,
   f) Asset management,
   g) Human resources security,
   h) Operations and communications management,
   i) Personnel access control,
   j) Acquisition, development and maintenance,
   k) Cyber security event management and cyber security incident management,
   l) Business continuity management, and
   m) Supervision and audit.

(3) Technical measures are
   a) Physical security,
   b) A tool to protect the integrity of communications networks,
   c) A tool to verify the identity of users,
   d) A tool for access authorisation management,

e) Malicious code protection tool,

f) A tool for recording the activities of the information or communication system, its users and administrators,

g) A tool for detecting cyber security events,

h) A tool for collecting and evaluating cyber security events,

i) Application security,

j) Cryptographic devices,

k) A tool for ensuring the level of availability of information, and

l) Security of industrial and control systems.

Section 6

[Implementing legislation]

Implementing legislation shall set out

a) Content of security measures,

b) Content and structure of security documentation,

c) Scope of the security measures for the authorities and persons specified in Section 3 letters (c) to (f),

d) Important information systems and their designation criteria,

e) Content and scope of security rules for public authorities using cloud computing providers, including security levels for the use of cloud computing by public authorities.

Section 6a

(1) The operator of an information or communication system of a critical information infrastructure or the operator of an important information system may assign the task of administrating the information or communication system of the critical information infrastructure or the task of administrating the important information system to another authority or person unless this contradicts another act.

(2) The administrator of the information or communication system of a critical information infrastructure or the administrator of an important information system shall transfer the data, operational data and information they have in relation to the administration of this system at the request of the operator of this system, without undue delay and in the agreed format. The provisions of legislation governing intellectual property rights are not affected by the transfer of the data, operational data and information.

(3) If the administrator of an information or communication system of a critical information infrastructure or the administrator of an important information system ceases administrating this system, they shall transfer the data, operational data and information they have in relation to the administration of this system that are needed for potential further administration of this information system or another use, and shall dispose of their copies in his digital environment in a secure way at the request of the operator of this system. The means of the disposal of the data,

operational data and information, as well as their copies, shall be set out by an implementing legislation.

(4) The administrator of an information or communication system of a critical information infrastructure, or the administrator of an important information system, is entitled to reimbursement of efficiently incurred costs for the transfer of the data, operational data and information pursuant to paragraphs 2 and 3; the costs shall be paid to the administrator by the operator of such a system.

Cyber security event and cyber security incident

Section 7

(1) A cyber security event is an event that may cause a breach in the security of information in information systems, a breach in the security of service provision or a breach of security and integrity of electronic communication networks[1)].

(2) A cyber security incident is a breach in the security of information in information systems, a breach in the security of service provision or a breach of security and integrity of electronic communication networks[1)] due to the cyber security event.

(3) Authorities and persons specified in Section 3, letters (b) to (f) are obliged to detect cyber security events in their important network, in their critical information infrastructure information system, in their information system of essential service or in their important information system.

Section 8

[Cyber security incident reporting]

(1) Authorities and persons specified in Section 3, letters (b) to (f) are obliged to report cyber security incidents in their important network, in their critical information infrastructure information system, or in their important information system immediately after their detection; this shall not affect their obligation to provide information according to another legal regulation[3)] or directly applicable European Union regulation governing personal data protection[11)]. If the cyber security incident has a significant impact on the continuity of the provision of an essential service, the essential service operator shall inform the Agency of this fact.

(2) A digital service provider is obliged to report a cyber security incident with a significant impact on the provision of their services without undue delay if they have access to the information for the assessment of the importance of the incident.

(3) Authorities and persons specified in 3, letters (b) and (h) shall report cyber security incidents to the operator of the national CERT.

(4) Authorities and persons specified in Section 3, letters (c) to (g) shall report cyber security incidents to the Agency.

(5) The obligation pursuant to paragraph 1 is also fulfilled by the operator of an information or communication system of a critical information infrastructure, or the operator of an important information system, when a cyber security incident is reported by the administrator of this system. The administrator of the information or communication system of a critical information

infrastructure or the administrator of an important information system shall inform the operators of this system of the reported cyber security incidents without undue delay.

(6) Authorities and persons not specified in Section 3 may report cyber security incidents to the operator of the national CERT or to the Agency.

(7) The implementing legislation shall set out the following:

a) The type, category and assessment of the importance of a cyber security incident

b) Requirements and the method of cyber security incident reporting

(8) If a cyber security incident that affected a digital service provider has a significant impact on the continuity of an essential service provision, the operator of the essential service is obliged to inform the Agency of this fact.

Record keeping

Section 9

(1) The Agency keeps a cyber security incident record (hereinafter "the incident record") which contains:

a) A cyber security incident report

b) The identification data of the system where the cyber security incident occurred

c) Information about the source of the cyber security incident

d) A procedure for handling the cyber security incident and its outcome

(2) The data specified in Section 20, letters (f) to (h) and (l) are part of the incident record.

(3) The Agency provides data from the incident record to authorities that execute public powers for the purpose of fulfilling tasks within their competence.

(4) The Agency may provide data from the incident record to the operator of the national CERT, to authorities in the field of cyber security abroad and to other persons operating in the field of cyber security in the extent necessary to ensure the protection of cyberspace.

Section 10

(1) Employees of the Czech Republic employed at the Agency who take a part in solving a cyber security incident are subject to the obligation of confidentiality with regard to the data from the incident record. The obligation of confidentiality shall last even after the termination of employment at the Agency.

(2) The Director of the Agency may exempt persons defined in paragraph 1 from the obligation of confidentiality with regard to the data from the incident record, providing a statement on the extent of the data access and the exemption.

Section 10a

Information which if accessed may jeopardise the ensuring of cyber security or the efficiency of measures issued on the basis of this Act, or information recorded in the incident record from which it

might be possible to identify the authority or person which reported the security incident, shall not be provided according to legal regulations governing free access to information.

Section 11
[Measures]

(1) Measures are actions that are needed to protect information systems or electronic communications services and networks[1)] from a threat in the field of cyber security or from a cyber security incident, or to resolve an already occurred cyber security incident.

(2) Measures are as follows:

a) Warning

b) Reactive measure

c) Protective measure

(3) Reactive measures are obligatorily applied by:

a) Authorities and persons specified in Section 3, letters (a) and (b) under the state of cyber emergency or under the state of emergency[4)] declared on the basis of a request specified in Section 21(6)

b) Authorities and persons specified in Section 3, letters (c) to (f)

(4) Protective measures are obligatorily applied by authorities and persons specified in Section 3, letters (c) to (f).

Section 12
[Warning]

(1) The Agency shall issue a warning if, particularly on the grounds of its own operation or on the grounds of a notification of the operator of the national CERT or public authorities in a field of cyber security abroad, it observes that there is a threat in the field of cyber security.

(2) A warning shall be issued by the Agency on its website and the Agency shall also inform authorities and persons specified in Section 3 whose contact details are kept on the record according to Section 16(4).

(3) In order to protect internal order and security, to protect people's lives and health, or to protect the state's economy, the Agency is entitled, after consulting the authority or person specified in Section 3, letters (c), (d), (f), (g) or (h) that is affected by the cyber security incident, to inform the public about the incident or assign the concerned authority or person to do so.

Reactive and protective measures

Section 13

(1) The Agency shall issue a decision on reactive measures to resolve the cyber security incident or to secure information systems or networks and electronic communication services[1)] from a cyber security incident, which is the first legal act in the given situation. If it is not possible to deliver the decision into the hands of the addressee within 3 days from the day of its issuance, it is considered to be delivered and enforceable upon its publication on the Agency's official notice board. The

decision in the first sentence may be issued by the Agency in on site proceedings according to the Code of Administrative Procedure.

(2) Appeal against the decision of the Agency pursuant to paragraph 1 does not have a suspensive effect.

(3) If a reactive measure to solve a cyber security incident or to protect information systems or electronic communication networks and services[1)] from a cyber security incident concerns an unspecified group of authorities and persons, the Agency shall adopt such a measure in the form of a measure of general nature.

(4) Authorities and persons specified in Section 3, letters (a) to (f) are obliged to notify the Agency about their application of a reactive measure and its outcome without undue delay. The requirements for the notice shall be set out by an implementing legislation.

Section 14

In order to strengthen the protection of information systems or networks and electronic communication networks[1)] and on the basis of an analysis of an already solved cyber security incident, the Agency shall adopt a protective measure of general nature in which it sets out a method of strengthening the protection of information systems or networks and electronic communication networks[1)], and an appropriate period of its application for persons specified in Section 3, letters (c) to (f).

Section 15

(1) The measure of general nature pursuant to Section 13 or Section 14 shall come into effect at the moment of its publication on the official notice board of the Agency; the provisions of Section 172 of the Code of Administrative Procedure shall not apply. The Agency shall also inform authorities and persons specified in Section 3 whose contact details are kept in the record pursuant to Section 16(4) about the issuance of the measure of general nature.

(2) Comments on the measure of general nature adopted pursuant to Section 13 or 14 can be made within a period of 30 days from the day it was published on the official notice board of the Agency. The Agency may change or repeal the measure of general nature in response to the comments.

Section 15a

(1) In the case of an impending cyber security incident and based on the proposal of an information system operator who has, with no effect, asked the administrator to fulfil their obligation of transferring to the operator the data, operational data and information they have with regard to the administration of the information or communication system of a critical information infrastructure or the administration of an important information system, the Agency may impose the obligation to transfer the data, operational data and information the administrator has with regard to the administration of the system to the operator of the system; the proposal must contain a justification for this request with regard to the threat of an impending cyber security incident, a detailed description of previous communication between the administrator and the operator of the system, particularly with regard to the failure to fulfil the contractual obligations

by the administrator, and potential consequences if the data, operational data and information are not transferred.

(2) The decision to impose the obligation to transfer the data, operational data and information pursuant to paragraph 1 is the first legal act in the proceedings, is enforceable upon the delivery of this decision and appeal against such decision does not have a suspensive effect.

(3) The provision in Section 6a(4) shall be used similarly for the reimbursement of efficiently incurred costs for the transmission of data, operational data and information by the administrator of an information or communication system of a critical information infrastructure, or the administrator of an important information system pursuant to paragraph 1.

Section 16
[Contact details]

(1) Contact details mean the following:

a) For a legal person, the trading company or the name, registered office address, identification number of the person or similar number assigned abroad

b) For a natural person pursuing business, the trading company or the name including a differentiating amendment or other designation, registered office address and identification number of the person

c) For a public authority, its name, registered office address, identification number of a person, if assigned, or an identifier of the public authority if an identification number was not assigned

Also including information about a natural person that is entitled to act on behalf of the authority or the person specified in Section 3 in issues governed by this act, i.e. his/her name, surname, phone number and email address.

(2) Contact details and their changes shall be announced by:

a) Authorities and persons specified in Section 3, letters (a), (b) and (h) to the operator of the national CERT

b) Authorities and persons specified in Section 3, letters (c) to (g) to the Agency.

(3) Authorities and persons specified in Section 3, letters (c) to (g) shall immediately announce only changes to the details specified in paragraph 1, which are not referential details kept in basic registers.

(4) The Agency shall keep a contact details record containing details specified in paragraph 1.

(5) The Agency is entitled to request contact details collected by the operator of the national CERT pursuant to paragraph 2, letter (a) under the state of cyber emergency.

(6) The Agency is furthermore entitled to request the contact details of authorities and persons specified in Section 3, letter (h) collected by the operator of the national CERT for the purpose of their inspection.

(7) The template for contact details notice and its form shall be established by the implementing legislation.

Section 17

[The national CERT]

(1) The national CERT ensures the sharing of information on the national and international level in the field of cyber security under the provisions of this Act.

(2) The operator of the national CERT:

a) Receives notices about contact details from authorities and persons specified in Section 3, letter (a), (b) and (h); keeps a record of them and stores them

b) Receives cyber security incident reports from authorities and persons specified in Section 3, letters (b) and (h); keeps a record of them, stores and protects them

c) Evaluates cyber security incidents of authorities and persons specified in Section 3, letters (b) and (h)

d) Provides authorities and persons specified in Section 3, letters (a), (b) and (h) with methodical support, help and cooperation when a cyber security incident occurs

e) Acts as a point of contact for authorities and persons specified in Section 3, letters (a), (b) and (h)

f) Carries out vulnerability analyses in the cyber security field

g) Transfers to the Agency data on cyber security incidents reported pursuant to Section 8(3) without disclosing the reportee to the Agency

h) Transfers to the Agency upon request data pursuant to Section 16, paragraphs 5 and 6

i) Fulfils the role of a CSIRT team according to relevant European Union legislation[12)]

j) Informs the relevant public authority of another Member State about a cyber security incident with a significant impact on the continuity of the provision of essential or digital service in this Member State without stating the identification details of the announcer, and also informs the Agency, while maintaining the security and commercial interests of the announcer

k) Cooperates with CSIRT teams of other Member States

l) Receives reports about cyber security incidents from authorities and persons specified in Section 3, and if its capacities allow it, processes and provides the authorities and persons affected by the cyber security incident with methodical support, help and cooperation

(3) The operator of the national CERT may, on their own behalf and responsibility, also perform other business activities in the field of cyber security unspecified by this Act, if such an activity does not harm the fulfilment of obligations specified in paragraph 2.

(4) The operator of the national CERT shall coordinate their activities with the Agency while fulfilling their obligations specified in paragraph 2.

(5) The operator of the national CERT shall act impartially when fulfilling the obligations pursuant to paragraph 2.

Section 18

[The operator of the national CERT]

(1) The operator of the national CERT can only be a legal person which:

a) Fulfils the conditions specified in paragraph 2 and

b) Concluded a public-law contract with the Agency pursuant to Section 19

(2) The operator of the national CERT can only be a legal person which:

a) Does not carry out any activities against the interests of the Czech Republic according to the Act on the Protection of Classified Information, and has never done so

b) Has been administrating or operating information systems or electronic communications services and networks[1)], or has been participating in their administration and operation, for at least a period of 5 years

c) Has technological prerequisites for the field of cyber security

d) Is a member of a multinational organisation operating in the field of cyber security

e) Does not have any arrears in the tax record of tax authorities of the Czech Republic, or customs authorities of the Czech Republic, or in the record of taxes, social insurance and public health insurance

f) Has not been sentenced for committing a crime specified in Section 7 of Act no. 418/2011 Coll. on the Criminal Responsibility of Legal Persons and Proceedings against them

g) Is not a foreign person according to any other legal regulation

h) Was not founded or established solely to pursue financial gain; this is without prejudice to the possibility of the operator of the national CERT to act pursuant to Section 17(3)

(3) The interested applicant proves the fulfilment of conditions stated above by presenting the following:

a) A statutory declaration with regard to paragraph 2, letters (a) to (d), (g) and (h) and

b) Confirmation by the financial and customs authorities of the Czech Republic with regard to paragraph 2, letter (e).

(4) It must be clear from the content of the statutory declaration pursuant to paragraph 3, letter (a) that the applicant fulfils the relevant prerequisites. Confirmation pursuant to paragraph, 3 letter (b) that the applicant does not have any arrears in the tax record of tax authorities of the Czech Republic, in the record of customs authorities of the Czech Republic or in the record of taxes, social insurance and public health insurance, must not be older than 30 days. In order to prove the fulfilment of conditions specified in paragraph 2, letter (f), the Agency shall request a criminal record according to a different legal regulation[5)].

(5) The operator of the national CERT pursues activities pursuant to Section 17, paragraph 2, letters (a) to (c), (e) and (g) to (l) free of charge. The operator of the national CERT is obliged to incur the necessary costs for the efficient execution of the activities specified in Section 17(2).

(6) The Agency shall publish information about the operator of the national CERT on its website, that is the trading company or name, registered office address, identification number of the person, identification code of their data mailbox and their website.

Section 19

[Public-law contract]

(1) The Agency concludes a public-law contract (hereinafter referred to as „the Contract“) with a legal person chosen by the selection procedure pursuant to Section 163(4) of the Code of Administrative Procedure in order to cooperate in the field of cyber security and ensure activities specified in Section 17(2). The application procedure shall be announced by the Agency.

(2) The contract shall contain at least the following:

a) Designation of the parties

b) Definition of the subject of the contract

c) Rights and obligations of the contracting parties

d) Cooperation conditions of the contracting parties

e) Method and conditions of the parties' withdrawal from the contract

f) Withdrawal notice period and reasons for the withdrawal

g) Ban on the misuse of data acquired while performing activities specified in Section 17(2)

h) Definition of the conditions for the performance of the national CERT activities pursuant to Section 17(3) and

i) Method for the data transfer and the extent of the data transferred to the Agency in the case of contract termination

(3) The contract concluded pursuant to paragraph 1 shall be published in the Official Journal of the Agency, except for the parts of the contract the publishing of which is not allowed by another legal regulation.

(4) If the contract pursuant to paragraph 1 is not concluded, or if the contract is terminated, the activity of the national CERT shall be performed by the Agency.

Section 20

[Governmental CERT]

Governmental CERT as a part of the Agency:

a) Receives notices of contact details from authorities and persons specified in Section 3, letters (c) to (g)

b) Receives reports on cyber security incidents from authorities and persons specified in Section 3, letters (c) to (g)

c) Evaluates data on cyber security events and cyber security incidents from a critical information infrastructure, information system of essential service, important information systems and other information systems of public administration

d) Provides authorities and persons specified in Section 3, letters (c) to (g) with methodical support and help

e) Cooperates with authorities and persons specified in Section 3, letters (c) to (g) when a cyber security incident or a cyber security event occurs

f) Receives suggestions and data from authorities and persons specified in Section 3, and from other authorities and persons, and evaluates these suggestions and data

g) Receives data from the operator of the national CERT and evaluates this data

h) Receives data from public authorities that operate in the field of cyber security abroad and evaluates this data

i) Provides data from the incident record pursuant to Section 9(4) to the operator of the national CERT, to authorities operating in the field of cyber security abroad and to other legal or natural persons operating in the field of cyber security

j) Carries out vulnerability analyses in the field of cyber security

k) Informs the relevant public authority of another Member State of a cyber security incident with a significant impact on the continuity of the provision of essential services in this Member State, or an incident concerning the provision of digital services in this Member State, without disclosing the identification details of the reportee, and while maintaining the security and commercial interests of the reportee

l) Receives reports of cyber security incidents from authorities and persons that are not specified in Section 3; governmental CERT processes the reports, and if its capabilities allow it and is the report concerns a cyber security incident with a significant impact, governmental CERT provides authorities and persons affected by a cyber security incident with methodical support, help and cooperation

m) Fulfils the role of a CSIRT team according to relevant European Union legislation[12)]

n) Cooperates with CSIRT teams of other Member States.

CHAPTER III
State of cyber emergency

Section 21

(1) A state of cyber emergency is a state in which there is a high measure of threat to the security of information of information systems or electronic communication network services or to the security and integrity of electronic communication networks[1)], and this could lead to breaches or threats to the interests of the Czech Republic in line with the meaning of the Act on the Protection of Classified Information.

(2) The Director of the Agency shall decide on the declaration of a state of cyber emergency. The decision about the declaration of a state of cyber emergency is published on the official notice board of the Agency. Information about the declaration of a state of cyber emergency is announced in broadcast on national radio and television. The operator of the national television or radio is obliged to immediately broadcast the information about the declaration of a state of cyber emergency based on the request of the Agency without adjusting the content and without reimbursement of incurred costs.

(3) The decision of the declaration of a state of cyber emergency comes into effect at the moment set out in this decision. The state of cyber emergency is announced for a necessary period of time,

7 days at the longest. This period of time can be extended by the Director of the Agency; the total period of time for which the state of cyber emergency is declared shall not exceed 30 days.

(4) During the time in which the state of cyber emergency is declared, the Director of the Agency shall inform the government of remedial procedures adopted under the state of cyber emergency and of the current status of threats which led to the declaration of the state of cyber emergency. Under a state of cyber emergency and under a state of emergency[4)] in cases pursuant to paragraph 6, the Agency is entitled to issue a decision or a measure of general nature pursuant to Section 13 also to authorities and persons specified in Section 3, letters (a) and (b).

(5) A state of cyber emergency cannot be declared when a threat to the security of information of information systems or electronic communication network services or to the security and integrity of electronic communication networks[1)] can be averted by actions of the Agency according to this Act.

(6) If it is not possible to avert the threat to the security of information of information systems or electronic communication network services or to the security and integrity of electronic communication networks[1)] within the scope of the state of cyber emergency, the Director of the Agency shall immediately ask the government to declare a state of emergency[4)]. The decision and the measures of general nature issued by the Agency pursuant to Section 13 before declaring a state of emergency shall remain in force, unless they are in conflict with the crisis measures issued by the government.

(7) The state of cyber emergency shall end after the expiry of the period for which it was declared, unless the Director of the Agency decides to lift it before the expiry of this period or to declare a state of emergency[4)].

CHAPTER IV
Exercise of state administration (Sections 21a-22c)

The Agency
Section 21a

(1) An agency with a registered office in Brno is established as the central body of state administration for cyber security and for selected fields in the protection of classified information according to the Act on the Protection of Classified Information and on Security Eligibility. The income and expenses of the Agency form a separate part of the state budget.

(2) The head of the Agency is a Director who is appointed by the government after consideration by a parliamentary committee relevant for the matters of security, and who is also removed by the government.

(3) The Director of the Agency is responsible to the prime minister or an entrusted government member.

Section 22

[Activities and powers of the Agency]

The Agency

a) Establishes security measures,

b) Issues measures,

c) Executes state administration in the field of security of information and communication systems handling classified information and in the field of cryptographic protection, ensures the activities of the National Centre for Communication Security, the National Centre for Distribution of Cryptographic Material, National Centre for Measurement of Compromising Radiation and the National Centre for Information Systems Security, which are part of it, and performs other tasks in accordance with the obligations arising from the membership of the Czech Republic in the European Union, the North Atlantic Treaty Organization and from international treaties by which the Czech Republic is bound, in selected areas of protection of classified information,

d) Keeps records in accordance with this Act and the Act on the Protection of Classified Information,

e) Imposes administrative penalties for failure to comply with the obligations set out in this Act and the Act on the Protection of Classified Information and on Security Eligibility,

f) Acts as a coordinating body in a state of cyber emergency,

g) Cooperates with authorities and persons operating in the field of cyber security and cyber defence, in particular with public corporations, research and development institutes and other CERT workplaces, and with authorities and persons operating in selected areas of protection of classified information,

h) Ensures international cooperation in the field of cyber security and in selected areas of protection of classified information,

i) Negotiates and concludes agreements on international cooperation in the field of cyber security and in selected areas of protection of classified information,

j) Provides for the prevention, education, and methodological support in the field of cyber security and in selected areas of protection of classified information,

k) Provides for research and development in the field of cyber security and in selected areas of protection of classified information,

l) Concludes a public law contract with the operator of the national CERT,

m) Submits to the Ministry of the Interior, in accordance with the Crisis Act, a proposal of critical infrastructure elements in the sector of communication and information systems in the field of cyber security, operated by an organisational unit of the state,

n) Designates in accordance with the Crisis Act, elements of critical infrastructure in the sector of communication and information systems in the field of cyber security, unless they are elements referred to in letter (m),

o) Verifies every 2 years that the designation of critical infrastructure elements referred to in letters (m) and (n) is up to date,

p) Designates the operator of the essential service and the information system of essential service,

q) Develops and submits to the Government for approval a national cyber security strategy[13)] and an action plan for its implementation and updates the strategy at least every 5 years,

r) Acts as the single point of contact for ensuring cross-border cooperation in the field of cyber security within the European Union,

s) Acts as the competent authority in the Czech Republic and fulfils information obligations towards the European Commission and the Cooperation Group according to relevant EU legislation[14]),

t) Informs the public about a cyber security incident pursuant to Section 12 (3),

u) Performs an analysis and monitoring of cyber threats and risks,

v) Exercises competence in the field of public regulated service of the European satellite navigation programme Galileo,

w) Publishes the Official Journal of the Agency, and makes it available on its website,

x) Performs other tasks in the field of cyber security set out in this Act and in selected areas of protection of classified information pursuant to the Act on the Protection of Classified Information and on Security Eligibility,

y) Is a cybersecurity certification authority pursuant to Article 58 of the Cybersecurity Act[17)].

Section 22a

[The identification of an operator of essential service and an information system of essential service]

(1) The Agency shall identify an operator of essential service and an information system of essential service by decision if they fulfil the sectoral and impact criteria that take into account the importance of:

   a) The services provided in individual sectors as specified in Section 2, letter (i) and

   b) The impact of a cyber security incident, particularly on:

      1. The extent and quality of essential service provision to users dependent on it

      2. Economic and societal activities and public safety

      3. The mutual dependency of other sectors referred to in Section 2, letter (i)

   Sectoral and impact criteria for the determination of an operator of essential service and specifications for determining the importance of an impact of the disruption of an essential service on the security of social and economic activities shall be set out in an implementing legislation.

(2) If the Agency finds that the authority or the person identified as an essential service operator pursuant to paragraph 1 also provides the concerned service in another Member State, it shall consult the relevant authority of the concerned Member State on this matter.

(3) Appeal against the decision of the Agency on the identification of an operator of essential service and an information system of essential service is not admissible.

(4) The Agency verifies if the requirements for determining an operator of essential service and an information system of essential service are fulfilled at least every 2 years from the issuance of a

decision identifying the operator of essential service and the information system of essential service.

Section 22b

[Authorisation of conformity assessment bodies under the Cybersecurity Act]

(1) Where a directly applicable legislation of the European Union issued on the basis of the Cybersecurity Act sets specific or additional requirements to which conformity assessment bodies are subject in order to guarantee their technical competence to evaluate the cybersecurity requirements, the Agency shall, in accordance with Article 58 (7) letter (e) of the Cybersecurity Act[17)], decide on applications for authorisation of a conformity assessment body, and where an authorised conformity assessment body infringes the requirements of the Cybersecurity Act[17)] or of a directly applicable legislation of the European Union issued on the basis of the Cybersecurity Act, the Agency shall decide on suspension of enforceability, amendment or revocation of the decision on authorisation.

(2) In the application for authorisation pursuant to paragraph 1, the conformity assessment body shall demonstrate the compliance with the specific or additional requirements set out in a directly applicable legislation of the European Union issued on the basis of the Cybersecurity Act.

(3) In the decision on suspension of enforceability of the decision on authorisation pursuant to paragraph 1, the Agency shall set out a period for seeking redress. If the conformity assessment body rectifies the situation, it shall notify the Agency without undue delay. In case the Agency finds the rectification to be sufficient, it shall repeal the decision on suspension of enforceability of the decision on authorisation. If the authorised conformity assessment body fails to seek remedy within the specified period of time, the Agency shall decide on amendment or revocation of the decision on authorisation.

(4) The Agency shall issue the decision on an application for authorisation pursuant to paragraph 1 within 120 days from the initiation of the proceedings at the latest, in exceptional cases within 180 days.

Section 22c

[Personal data processing]

(1) The Agency and the operator of the national CERT shall process personal data as necessary for the exercise of their powers. The Agency and the operator of the national CERT shall transmit such data to public authorities or persons where necessary for the performance of their tasks.

(2) While processing the personal data covered by Regulation (EU) 2016/679 of the European Parliament and of the Council, the Agency and the operator of the national CERT

a) Does not have to restrict the processing of personal data where the data subject contests the accuracy of the processing or objected to such processing, and

b) May, in the exercise of its powers, use the personal data for purposes other than those for which they were collected.

(3) Where the Agency or the operator of the national CERT, in the course of an activity to which Regulation (EU) 2016/679 of the European Parliament and of the Council applies, in dealing with a cyber security incident or a cyber security event and/or in preventing cyber threats or risks, receives personal data which it processes solely for the purpose of carrying out its obligations under this Act, it shall not, for the duration of the performance of those obligations, furthermore, be required to

a) Provide the data subject with information on the rectification or erasure of personal data or the restriction of their processing,

b) Provide the data subject with access to the personal data, or

c) Rectify or supplement personal data at the request of the data subject.

CHAPTER V
Supervision, corrective measures and offences (Sections 23-27)

Section 23
[Inspection]

(1) The Agency performs inspections in the field of cyber security. During inspections, the Agency uncovers how authorities and persons specified in Section 3, letters (a) to (g) fulfil their obligations set out in this Act and in decisions and measures of general nature issued by the Agency according to this Act, and how they comply with the implementing legislation in the field of cyber security. If there is a reason to suspect the digital service provider does not fulfil the obligations set out by this Act, the Agency shall perform an inspection.

(2) The inspection shall be performed in the appropriate way according to the Inspections Code.

(3) Authorised staff of the Agency shall perform the inspection.

Section 24
[Corrective measures]

(1) If the Agency finds a deficiency, it shall order the inspected authority or person to remedy it within a specified period of time. It may also set out the method of the remedy.

(2) If the information or communication system of a critical information infrastructure, the information system of an essential service or an important information system is imminently jeopardised by a cyber security incident that may cause damage or destroy it due to the found deficiencies, the Agency may prohibit the inspected authority or person to use the system or its part until the found deficiency is remedied.

Supervision of the activities of the Agency

Section 24a

[Supervisory body of the Chamber of Deputies]

(1) The Chamber of Deputies performs supervision over the activities of the Agency and establishes a special supervisory body for this purpose (hereinafter referred to as the "supervisory body").

(2) The supervisory body shall be composed of at least 7 members. The Chamber of Deputies shall set the number of members so that each of the parliamentary party groups constituted according to the affiliation to the political party or political movement for which the deputies stood as candidates in the elections is represented; the number of members shall always be odd. Only a Member of the Chamber of Deputies may be a member of the supervisory body.

(3) Unless otherwise set out in this Act, other legislation shall apply mutatis mutandis to the proceedings of the supervisory body and to the rights and obligations of its members[15)].

(4) Members of the supervisory body may enter the premises of the Agency accompanied by the Director of the Agency or an employee authorised by the Director.

(5) The Director of the Agency shall submit to the supervisory body

a) A report on the activities of the Agency,

b) A budget proposal of the Agency,

c) Documents necessary for inspection of the implementation of the Agency's budget,

d) Internal regulations of the Agency,

e) Upon request, a report on individual cyber security incidents from critical information infrastructure, important information systems and information systems of essential service.

Section 24b

(1) If the supervisory body assumes the Agency unlawfully limits or violates citizens' rights and freedoms, or that the Agency's decision-making within administrative proceedings is hindered by errors, it is entitled to require a necessary explanation from the Director of the Agency.

(2) The supervisory body is obliged to inform the Director of the Agency and the Prime Minister of any breach of the law it learns about through its activity, which was caused by an employee of the Agency and which occurred when fulfilling obligations set out under this Act and in selected areas governed by the Act on the Protection of Classified Information and on Security Eligibility.

Section 24c

The obligation of confidentiality legally imposed on the members of the supervisory body shall not be applicable to cases when the supervisory body submits the information pursuant to Section 24b(2).

Offences

Section 25

(1) An electronic communications service provider and an entity providing an electronic communications network commits an offence by failing to

a) Comply with an obligation imposed by the Agency in a decision or in a measure of general nature pursuant to Section 13 in a state of cyber emergency or a state of emergency,

b) Notify the Agency without undue delay of the outcome of the implementation of a reactive measure pursuant to Section 13(4),

c) Notify contact details or a change thereof pursuant to Section 16(2) letter (a), or

d) Comply with any of the obligations imposed by a corrective measure pursuant to Section 24.

(2) An authority or a person providing an important network commits an offence by failing to

a) Detect cyber security events as referred to in Section 7(3),

b) Report a cyber security incident pursuant to Section 8(1) and (3),

c) Comply with an obligation imposed by the Agency in a decision or a measure of general nature pursuant to Section 13 in a state of cyber emergency or a state of emergency,

d) Notify the Agency without undue delay of the outcome of the implementation of a reactive measure pursuant to Section 13(4),

e) Notify contact details or a change thereof pursuant to Section 16(2) letter (a), or

f) Comply with any of the obligations imposed by a corrective measure pursuant to Section 24.

(3) An administrator of information or communication system of a critical information infrastructure commits an offence by failing to

a) Introduce or implement security measures or maintain security documentation, in breach of Section 4(2),

b) Take into account the requirements resulting from the security measures when selecting a supplier, in breach of Section 4(4), or by concluding a contract with such a supplier in breach of Section 4(4),

c) As a public authority, in breach of Section 4(5), classify the requested cloud computing with a security level, by failing to ensure compliance with security rules for the provision of cloud computing services or compliance with availability conditions, and/or by concluding a contract with a cloud computing service provider in breach of Section 4(6),

d) Inform the system operator pursuant to Section 4a(1),

e) Inform the entity providing the electronic communications network pursuant to Section 4a(2),

f) Detect cyber security events pursuant to Section 7(3),

g) Report a cyber security incident pursuant to Section 8(1) and (4),

h) Comply with the obligation to inform the public imposed by the Agency pursuant to Section 12(3),

i) Comply with an obligation imposed by the Agency under Sections 13 or 14,

j) Notify the Agency without undue delay of the outcome of the implementation of a reactive measure pursuant to Section 13(4),

k) Notify the Agency of its contact details or a change thereof pursuant to Section 16(2) letter (b), or

l) Comply with any of the obligations imposed by a corrective measure pursuant to Section 24.

(4) An operator of information or communication system of a critical information infrastructure commits an offence by failing to

a) Introduce or implement security measures or maintain security documentation in breach of Section 4(2),

b) Take into account the requirements resulting from the security measures when selecting a supplier, in breach of Section 4(4), or by concluding a contract with such a supplier in breach of Section 4(4),

c) As a public authority, in breach of Section 4(5), classify the requested cloud computing with a security level, by failing to ensure compliance with security rules for the provision of cloud computing services or compliance with availability conditions, and/or by concluding a contract with a cloud computing service provider in breach of Section 4(6),

d) Inform the entity providing the electronic communications network pursuant to Section 4a(2),

e) Provide data, traffic data and information pursuant to Section 6a(2),

f) Provide data, traffic data and information pursuant to Section 6a(3),

g) Destroy copies of data, traffic data and information pursuant to Section 6a(3),

h) Allow the administrator to supervise the progress of the destruction of data, traffic data and information pursuant to Section 6a(3),

i) Detect cyber security events pursuant to Section 7(3),

j) Report a cyber security incident pursuant to Section 8(1) and (4),

k) Comply with the obligation to inform the public imposed by the Agency pursuant to Section 12(3),

l) Comply with an obligation imposed by the Agency under Sections 13 or 14,

m) Notify the Agency without undue delay of the outcome of the implementation of a reactive measure pursuant to Section 13(4),

n) Comply with an obligation imposed by the Agency in a decision pursuant to Section 15a(1),

o) Notify the Agency of its contact details or a change thereof pursuant to Section 16(2) letter (b), or

p) Comply with any of the obligations imposed by a corrective measure pursuant to Section 24.

(5) An administrator of an important information system commits an offence by failing to

a) Introduce or implement security measures or maintain security documentation in breach of Section 4(2),

b) Take into account the requirements resulting from the security measures when selecting a supplier, in breach of Section 4(4), or by concluding a contract with such a supplier in breach of Section 4(4),

c) As a public authority, in breach of Section 4(5), classify the requested cloud computing with a security level, by failing to ensure compliance with security rules for the provision of cloud computing services or compliance with availability conditions, and/or by concluding a contract with a cloud computing service provider in breach of Section 4(6),

d) Inform the system operator pursuant to Section 4a(1),

e) Detect cyber security events pursuant to Section 7(3),

f) Report a cyber security incident pursuant to Section 8(1) and (4),

g) Comply with an obligation imposed by the Agency under Sections 13 or 14,

h) Notify the Agency without undue delay of the outcome of the implementation of a reactive measure pursuant to Section 13(4),

i) Notify the Agency of its contact details or a change thereof pursuant to Section 16(2)(b), or

j) Comply with any of the obligations imposed by a corrective measure pursuant to Section 24.

(6) An operator of an important information system commits an offence by failing to

a) Introduce or implement security measures or maintain security documentation in breach of Section 4(2),

b) Take into account the requirements resulting from the security measures when selecting a supplier, in breach of Section 4(4), or by concluding a contract with such a supplier in breach of Section 4(4),

c) As a public authority, in breach of Section 4(5), classify the requested cloud computing with a security level, by failing to ensure compliance with security rules for the provision of cloud computing services or compliance with availability conditions, and/or by concluding a contract with a cloud computing service provider in breach of Section 4(6),

d) Provide data, traffic data and information pursuant to Section 6a(2),

e) Provide data, traffic data and information pursuant to Section 6a(3),

f) Destroy copies of data, traffic data and information pursuant to Section 6a(3),

g) Allow the administrator to supervise the progress of the destruction of data, traffic data and information pursuant to Section 6a(3),

h) Detect cyber security events pursuant to Section 7(3),

i) Report a cyber security incident pursuant to Section 8(1) and (4),

j) Comply with an obligation imposed by the Agency under Sections 13 or 14,

k) Notify the Agency without undue delay of the outcome of the implementation of a reactive measure pursuant to Section 13(4),

l) Comply with an obligation imposed by the Agency in a decision pursuant to Section 15a(1),

m) Notify the Agency of its contact details or a change thereof pursuant to Section 16(2) letter (b), or

n) Comply with any of the obligations imposed by a corrective measure pursuant to Section 24.

(7) An administrator of an information system of essential service commits an offence by failing to

a) Introduce or implement security measures or maintain security documentation in breach of Section 4(2),

b) Take into account the requirements resulting from the security measures when selecting a supplier, in breach of Section 4(4), or by concluding a contract with such a supplier in breach of Section 4(4),

c) As a public authority, in breach of Section 4(5), classify the requested cloud computing with a security level, by failing to ensure compliance with security rules for the provision of cloud computing services or compliance with availability conditions, and/or by concluding a contract with a cloud computing service provider in breach of Section 4(6),

d) Detect cyber security events pursuant to Section 7(3),

e) Report a cyber security incident pursuant to Section 8(1) and (4),

f) Comply with the obligation to inform the public imposed by the Agency pursuant to Section 12(3),

g) Comply with an obligation imposed by the Agency under Sections 13 or 14,

h) Notify the Agency without undue delay of the outcome of the implementation of a reactive measure pursuant to Section 13(4),

i) Notify the Agency of its contact details or a change thereof pursuant to Section 16(2) letter (b), or

j) Comply with any of the obligations imposed by a corrective measure pursuant to Section 24.

(8) An operator of an information system of essential service commits an offence by failing to

a) Introduce or implement security measures or maintain security documentation in breach of Section 4(2),

b) Take into account the requirements resulting from the security measures when selecting a supplier, in breach of Section 4(4), or by concluding a contract with such a supplier in breach of Section 4(4),

c) As a public authority, in breach of Section 4(5), classify the requested cloud computing with a security level, by failing to ensure compliance with security rules for the provision of cloud computing services or compliance with availability conditions, and/or by concluding a contract with a cloud computing service provider in breach of Section 4(6),

d) Detect cyber security events pursuant to Section 7(3),

e) Report a cyber security incident pursuant to Section 8(1) and (4),

f) Comply with the obligation to inform the public imposed by the Agency pursuant to Section 12(3),

g) Comply with an obligation imposed by the Agency under Sections 13 or 14,

h) Notify the Agency without undue delay of the outcome of the implementation of a reactive measure pursuant to Section 13(4),

i) Notify the Agency of its contact details or a change thereof pursuant to Section 16(2) letter (b), or

j) Comply with any of the obligations imposed by a corrective measure pursuant to Section 24.

(9) An operator of an essential service commits an offense by failing to

a) As a public authority, in breach of Section 4(5), classify the requested cloud computing with a security level, by failing to ensure compliance with security rules for the provision of cloud computing services or compliance with availability conditions, and/or by concluding a contract with a cloud computing service provider in breach of Section 4(6),

b) Inform the administrator or operator of the information system of essential service pursuant to Section 4a(3),

c) Report a significant impact on the continuity of the provision of the essential service pursuant to Section 8(1), (4) or (8),

d) Comply with the obligation to inform the public imposed by the Agency pursuant to Section 12(3),

e) Notify the Agency of its contact details or a change thereof pursuant to Section 16(2) letter (b), or

f) Comply with any of the obligations imposed by a corrective measure pursuant to Section 24.

(10) A digital service provider commits an offense by failing to

a) Appoint a representative pursuant to Section 3a(1),

b) Introduce or implement security measures in breach of Section 4(3),

c) Report a cyber security incident pursuant to Section 8(2) and (3),

d) Comply with the obligation to inform the public imposed by the Agency pursuant to Section 12(3),

e) Notify contact details or a change thereof pursuant to Section 16(2) letter (a), or

f) Comply with any of the obligations imposed by a corrective measure pursuant to Section 24.

(11) A manufacturer or provider of products, services or processes issuing an EU statement of conformity commits an offence by:

a) Issuing an EU statement of conformity when the conditions for its issuance set out by the Cybersecurity Act[17)] are not met,

b) Failing to store documents and information pursuant to Article 53(3) of by the Cybersecurity Act[17)],

c) Failing to submit a copy of an EU statement of conformity to the Agency and to ENISA pursuant to Article 53(3) of the Cybersecurity Act[17)], or

d) Failing to provide information on cybersecurity to the extent and in the manner specified in Article 55 of the Cybersecurity Act[17)].

(12) A holder of a European cybersecurity certificate commits an offence by failing to inform the relevant conformity assessment bodies of any subsequently detected vulnerabilities or irregularities.

(13) A legal person or a natural person pursuing business commits an offence by:

a) Misusing a mark or a label of European cybersecurity certification scheme, a European cybersecurity certificate, an EU statement of conformity or ofc any other document under the Cybersecurity Act[17)],

b) Forging or altering a European cybersecurity certificate, an EU statement of conformity or any other document under the Cybersecurity Act[17)],

c) Performing a conformity assessment activity under the Cybersecurity Act[17)] for assurance level “high”, without being entitled to do so under Article 56(6) of the Cybersecurity Act[17)],

d) As a conformity assessment body authorised under Article 60(3) of the Cybersecurity Act[17)], by issuing a European cybersecurity certificate for a product, process or service that does not meet the criteria set out in a directly applicable legislation of the European Union issued on the basis of the Cybersecurity Act[17)],

e) Without being authorised, by performing a conformity assessment activity that is reserved to an authorised conformity assessment body by a directly applicable legislation of the European Union issued on the basis of the Cybersecurity Act[17)], or

f) Acting as an accredited conformity assessment body under Article 60(1) of the Cybersecurity Act[17)] or outside the scope of such accreditation.

(14) The offence is punishable by a fine of up to

a) CZK 5,000,000 if the offence is an offence under paragraphs 3(a), 4(a), 5(a), 6(a), 7(a), 8(a), 10(b), 12 or 13.

b) CZK 1,000,000, if the offence is an offence under paragraphs 1(a)(b) or (d), 2(a) to (d) or (f), 3(b) to (j) or (l), 4(b) to (n) or (p), 5(b) to (h) or (j), 6(b) to (l) or (n), 7(b) to (h) or (j), 8(b) to (h) or (j), 9(a) to (d) or (f), and 10(a)(c)(d)(f) or 11.

c) CZK 10,000 if the offence is an offence under paragraphs 1(c), 2(e), 3(k), 4(o), 5(i), 6(m), 7(i), 8(i), 9(e) or 10(e).

Section 26

(1) A natural person commits an offence by infringing the obligation specified in Section 10(1).

(2) For an offence pursuant to paragraph 1, a penalty of up to 50,000 CZK can be imposed.

Section 27

[Common provisions for offences]

Offences according to this Act are dealt with and penalties are collected by the Agency.

CHAPTER VI

Final provisions (Sections 28–33)

Section 28

[Enabling clause]

(1) The Agency and the Ministry of the Interior shall determine the important information systems and their determinative criteria pursuant to Section 6, letter (d) in a decree.

(2) The Agency shall set out the following points in a decree:

a) The content and structure of security documentation, the content of security measures and the extent of security measures pursuant to Section 6, letters (a) to (c), and the content and extent of security rules pursuant to Section 6, letter(e)

b) The type, category and assessment of the importance of cyber security incidents and the requirements and the method of cyber security incident reporting pursuant to Section 8(7).

c) Requirements for the notification of the application of a reactive measure and its outcome pursuant to Section 13(4)

d) A template of the contact details request notice and its form pursuant to Section 16(7)

e) Sectoral and impact criteria for determining an essential service operator and the specification of the importance of an impact of a disruption of essential service on the security of social and economic activities pursuant to Section 22a(1)

f) Means of the disposal of data, operation data and information, and their copies

Transitional provisions

Section 29

(1) Authorities and persons specified in Section 3, letters (a) and (b) shall send a notification of contact details pursuant to Section 16 within 30 days from the effective date of this Act.

(2) Authorities and persons specified in Section 3, letter (b) shall start fulfilling their obligation specified in Section 8, paragraphs 1 and 2 within 1 year from the effective date of this Act at the latest.

Section 30

[Tasks and deadlines for persons specified in Section 3 letters (c) and (d)]

Authorities and persons specified in Section 3 letters (c), (d) and (f)

a) Shall notify the contact details referred to in Section 16 no later than 30 days from the day of designation of their information system or communication system as a critical information infrastructure or designation of the information system as an information system of essential service,

b) Shall begin to comply with the obligation set out in Section 8(1) and (4) no later than 1 year from the date of designation of their information system or communication system as a critical information infrastructure or designation of the information system as an information system of essential service, and

c) Shall implement the security measures referred to in Section 4(2) no later than 1 year from the date of designation of their information system or communication system as a critical information infrastructure or designation of the information system as an information system of essential service.

Section 31

Authorities and persons specified in Section 3, letter (e) shall:

a) Send a notification of contact details pursuant to Section 16 at the latest within 30 days from the day on which their information system fulfilled the determination criteria to be identified as a critical information infrastructure

b) Start fulfilling their obligation specified in Section 8, paragraphs 1 and 4 at the latest within 1 year from the day on which the determination criteria of an important information system were fulfilled

c) Introduce a security measure pursuant to Section 4(2) at the latest within 1 year from the day on which the determination criteria of an important information system were fulfilled

Section 32

The activity of the national CERT shall be performed by the public authority or the person that performed the activity which is performed by the national CERT according to this Act until the public-law contract concluded pursuant to Section 19 comes into effect, but no longer than within 2 years from the effective date of this Act.

Section 33

[Common provisions]

(1) This Act shall only apply to such information or communication systems of intelligence services that fulfil the requirements for determining a critical information infrastructure in the extent of Sections 12 and 16; the provisions of Section 4 shall be applied to these systems adequately and the Agency shall not propose these to be critical infrastructure elements pursuant to Section 22(2) letter (m).

(2) This Act shall be applied to the information system of the Police of the Czech Republic and the General Inspection of Security Forces for analytical activities in criminal proceedings only in the extent of Sections 12 and 16; the provisions of Section 4 shall be applied to this system adequately. This does not apply if the system is a critical information infrastructure.

(3) This Act shall only be applied to digital service providers that are legal persons and not a micro-enterprise or a small enterprise[16)].

(4) This Act shall not be applied for digital service providers with registered offices in another Member State.

PART TWO

Section 34

Repealed

PART THREE

Amendment of the Electronic Communications Act (Section 35)

Section 35

Act No 127/2005 Coll. on Electronic Communications and on Change of Related Acts (Electronic Communications Acts), as amended by Act No 290/2005 Coll., Act No 361/2005 Coll., Act No 186/2006 Coll., Act No 235/2006 Coll., Act No 310/2006 Coll., Act No 110/2007 Coll., Act No 261/2007 Coll., Act No 304/2007 Coll., Act No 124/2008 Coll., Act No 177/2008 Coll., Act No 189/2008 Coll., Act No 247/2008 Coll., Act No 384/2008 Coll., Act No 227/2009 Coll., Act

No 281/2009 Coll., Act No 153/2010 Coll., Judgment of the Constitutional Court, No 94/2011 Coll., Act No 137/2011 Coll., Act No 341/2011 Coll., Act No 375/2011 Coll., Act No 420/2011 Coll., Act No 457/2011 Coll., Act No 458/2011 Coll., Act No 468/2011 Coll., Act No 18/2012 Coll., Act No 19/2012 Coll., Act No 142/2012 Coll., Act No 167/2012 Coll., Act No 273/2012 Coll., Act No 214/2013 Coll. and Act No 303/2013 Coll., is hereby amended as follows:

1. Paragraph 4 is added to Section 89, including footnote no. 62, which is worded as follows:

   "(4) The entrepreneur who ensures the operation of a public communication network or provides a publicly available electronic communications service is obliged to provide operational and localization data he has based on this Act free of charge and in a form that allows further electronic processing of the data for the user upon his/her request if the user could not record or save them due to a cyber security incident. The data shall be transferred immediately, if technically possible, and no later than within 3 days from the date on which the request was delivered, or in the case of ongoing communication, from the date on which it took place.

   _____

   62) Section 7, paragraph 2, Act No. 181/2014 Coll. on Cyber Security and Change of Related Acts (the Act on Cyber Security)."

2. The word "or" is repealed in Section 118, paragraph 14, letter y).

3. The dot at the end of Section 118, paragraph 14 is replaced by the word "or" and letter ad) is added to the paragraph, which is worded as follows:

   „ad) Not providing the data or providing them too late contrary to Section 89, paragraph 4.

4. The word "or" is replaced with a comma in Section 118, paragraph 22, letter a) and the words "or paragraph 14, letter ad)" are added to letter (a).

PART FOUR

Section 36

Repealed

PART FIVE

Amendment of the Act on the Operation of Radio and Television Broadcasting

Section 37

In Section 32(1) letter (k) of Act No. 231/2001 Coll. on the Operation of Radio and Television Broadcasting and on Amendments to Other Acts, as amended by Act No. 274/2003 Coll., the words "the state of cyber emergency," are added after the words "state of war".

PART SIX

EFFECT (Section 38)

Section 38

This Act shall become effective on January 1, 2015.

Hamáček, signed

Zeman, signed

Sobotka, signed

Transitional provisions of amendments:
Article IV of Act No. 104/2017 Coll.
Version effective from July 1, 2017

An administrator of an information or communication system of a critical information infrastructure, or an administrator of an important information system specified in Act No. 181/2014 Coll. in the version effective before this Act comes into effect shall:

a) Send a notification of contact details according to Section 16 of Act No. 181/2014 Coll., no later than within 30 days of the effective date of this Act

b) Start fulfilling the obligation specified in Section 8, paragraphs 1 and 3 of Act No. 181/2014 Coll., no later than within 6 months from the effective date of this Act

c) Introduce security measures according to Section 4, paragraph 2 of Act No. 181/2014 Coll, no later than within 6 months from the effective date of this Act. In case security measures are introduced, the administrator is entitled to reimbursement of the costs related to the implementation of the security measure; the cost of the administrator shall be reimbursed by the operator of the concerned system

Article IV of Act No. 205/2017 Coll.
Version effective from August 1, 2017

1. The Agency shall identify the operators of essential service and information systems of essential service according to Section 22a, paragraph 1 of Act No. 181/2014 Coll. In line with the wording of the version effective from the effective date of this Act to November 9, 2018.
2. Public authorities and legal or natural persons specified in Section 3, letter f) of Act No. 181/2014 Coll. in the version effective from the effective date of this Act shall:

a) Send a notification to the Agency with contact details according to Section 16, paragraph 1 of Act No. 181/2014 Coll. in the version effective on the date this Act comes into effect, within 30 days of the date on which they were informed according to Section 4a, paragraph 3 of Act No. 181/2014 Coll. in the version effective on the date this Act comes into effect

b) Start fulfilling their other obligations according to Act No. 181/2014 Coll. in the version effective on the date this Act comes into effect, within 1 year from the date on which they were informed according to Section 4a, paragraph 3 of Act No. 181/2014 Coll., in the version effective on the date this Act comes into effect

3. The digital service provider shall:
   a) Send a notification to the Agency with contact details according to Section 16, paragraph 1 of Act No. 181/2014 Coll. in the version effective on the date this Act comes into effect, within 30 days of the effective date of this Act
   b) Start fulfilling their other obligations arising from Act No. 181/2014 Coll. in the version effective from the date this Act comes into effect, within 1 year from the effective date of this Act
4. If the conditions of the contractual relations concluded with the supplier of their information or communication system do not comply with the requirements of Act No. 181/2014 Coll. in the

version effective from the effective date of this Act, public authorities and legal or natural persons specified in Section 3, letter c) to f) are obliged to bring the contractual relationship into conformity with these requirements within 1 year from the effective date of this Act.

5. Proceedings in the matter of administrative delicts and offences according to Act No. 181/2014 Coll. commenced and not concluded before the effective date of this Act shall be concluded by the National Cyber and Information Security Agency. The National Security Authority shall transfer to the National Cyber and Information Security Agency all documents and data on pending proceedings as of the effective date of this Act and shall draw up a protocol with the National Cyber and Information Security Agency about this transfer.

6. The use of rights and fulfilment of obligations arising from the contract concluded according to Section 19, paragraph 1 of Act No. 181/2014 Coll. shall be transferred to the National Cyber and Information Security Agency from the National Security Authority.

7. The National Security Authority shall, within 6 months of the effective date of this Act, transfer to the National Cyber and Information Security Agency all documents and data related to the execution of its responsibilities, which are transferred to the National Cyber and Information Security Agency on the effective date of this Act.

8. The use of rights and fulfilment of obligations arising from the employment of employees of the National Security Authority who secured the activity of the National Security Authority according to Act No. 181/2014 Coll. in the version effective before the effective date of this Act shall be transferred to the National Cyber and Information Security Agency on the effective date of this Act, as the activity of the National Security Authority is also transferred to the National Cyber and Information Security Agency.

9. The competence to manage the property owned by the state used by the National Security Authority shall be transferred to the Nation Cyber and Information Security Agency on the effective date of this Act, if this property was used to secure the activity of the National Security Authority according to Act No. 181/2014 Coll. in the version effective before the effective date of this Act, as securing this activity is also transferred to the National Cyber and Information Security Agency on the effective date of this Act.

10. The budgeted funds of chapter 308 – the National Security Authority according to Act No. 457/2016 Coll. on the State Budget of the Czech Republic for 2017, including the claims for unspent expenditures from the previous year related to the execution of the powers of the National Security Authority which shall be transferred to the National Cyber and Information Security Agency on the effective date of this Act, shall be transferred to the National Cyber and Information Security Agency on the effective date of this Act.

Footnotes:

1 Act No. 127/2005 Coll. On Electronic Communications and on Change of Related Acts (Electronic Communications Act), as amended.

2 Section 2 of Act No. 240/2000 Coll., on Crisis Management and on the Amendment of Certain Acts (the Crisis Act), as amended.

Governmental order No. 432/2010 Coll. on the Criteria for the Determination of a critical infrastructure element.

3 For example Section 98(4), and Section 99(4) of Act No. 127/2005 Coll., as amended.

4 Constitutional Act No. 110/1998 Coll. On the Security of the Czech Republic as amended by Constitutional Act No. 300/2000 Coll..

5 The Act No. 269/1994 Coll. on the Criminal Records Database, as amended.

6 Directive (EU) 2016/1148 of the European Parliament and of the Council of July 6, 2016 concerning measures for a high common level of security of network and information systems across the Union.

7 Section 2, letter (h) of Act No. 127/2005 Coll., as amended.

8 Article 5(7) of the Directive (EU) 2016/1148 of the European Parliament and of the Council.

9 Section 2, letter (a) of Act No. 480/2004 Coll., on Certain Information Society Services and amending Certain Acts (the Information Society Services Act).

10 Section 2(1), letters (a) and (b) of Act No. 634/1992 Coll. On the Protection of Consumers, as amended.
Section 419 and 420 of Act No. 89/2012 Coll., the Civil Code.

11 Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 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).

12 Article 9 of the Directive (EU) 2016/1148 of the European Parliament and of the Council.

13 Article 7 of the Directive (EU) 2016/1148 of the European Parliament and of the Council.

14 For example, Article 5(3), Article 7(3) and Article 8 of the Directive (EU) 2016/1148 of the European Parliament and of the Council.

15 The Act No. 90/1995 Coll. On the Rules of Procedure of the Chamber of Deputies, as amended.

16 Annex to the Commission Recommendation 2003/361/EC of May 6, 2003 on the Definition of Micro, Small and Medium-Sized Enterprises.

17 Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act).