Government proposal

ACT

of 2024,

on Cybersecurity

Parliament has adopted the following Act of the Czech Republic:

PART ONE
CYBERSECURITY

TITLE I
Basic provisions

§ 1
Subject matter

(1) This Act regulates the rights and obligations of persons, organisational units of the state and other public authorities in the field of ensuring cybersecurity and the competence and powers of the National Cyber and Information Security Agency (hereinafter referred to as "the Agency") and other public authorities.

(2) This Act applies to persons who are established in the territory of the Czech Republic. This Act shall also apply to persons providing electronic communications networks or services in the territory of the Czech Republic pursuant to another legal regulation[1], regardless of their place of establishment.

(3) This Act incorporates the relevant European Union legislation[2)], follows up on directly applicable European Union legal acts[3)].

---

[1] Act No. 127/2005 Coll., on electronic communications and on amendments of certain related laws (Electronic Communications Act), as amended.

[2)] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures to ensure a high common level of cybersecurity in the Union and amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972 and repealing Directive (EU) 2016/1148 (NIS 2 Directive).

[3)] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the "European Union Agency for Cyber Security"), on the certification of cybersecurity of information and communication technologies and repealing Regulation (EU) No 526/2013 (the "Cybersecurity Act").

Regulation (EU) 2021/887 of the European Parliament and of the Council of 20 May 2021 establishing a European Industrial, Technological and Research Centre of Competence for Cyber Security and a network of National Coordination Centres.

Regulation (EU) 2021/696 of the European Parliament and of the Council of 28 April 2021 establishing the Union Space Programme and the European Union Agency for the Space Programme and repealing Regulations (EU) No 912/2010, (EU) No 1285/2013 and (EU) No 377/2014 and Decision No 541/2014/EU.

Decision No 1104/2011/EU of the European Parliament and of the Council of 25 October 2011 on the conditions for access to the public regulated service offered by the global navigation satellite system established under the Galileo programme.

(4) This Act shall not apply to information or communication systems handling classified information.

§ 2
Definition of terms

(1) For the purposes of this Act
   a) data means records of actions, facts or information and sets of such actions, facts or information, including traffic data[4)] and metadata[5)], in particular in the form of text, figures, graphs, images, audio and video,
   b) information means processed, interpreted or organized data that has meaning and context,
   c) asset means, a physical or digital means, person or activity related to the processing of information and data in electronic form,
   d) primary asset means an asset in the form of processed information or provided service,
   e) supporting asset means an asset that ensures the operation of the primary assets, in particular an employee, supplier, technical asset, building and other delimited space in which the regulated service asset is located, and
   f) technical asset means a technical or software means or equipment.

(2) For the purposes of this Act
   a) cyberspace means a set of electronic communications networks and other technologies, in which information and data are processed in electronic form,
   b) information security means ensuring the confidentiality, integrity and availability of information and data,
   c) threat means any potential circumstance, event or action that may cause cybersecurity event or cybersecurity incident, that may damage, disrupt or otherwise adversely affect assets, their users or other persons,
   d) significant threat means a threat that, based on its technical characteristics, can be assumed to have the potential to significantly affect the assets of the regulated service provider or users of regulated services to the extent that it causes significant harm, damage or disruption,
   e) cybersecurity event means an event that may result in a cybersecurity incident,
   f) cybersecurity incident means a breach of information security in cyberspace,
   g) cybersecurity incident management means actions leading to prevention, detection, analysis, mitigation, incident response and recovery, and
   h) vulnerability is a weakness in an asset or a weakness in a security measure that can be exploited by a threat.

(3) For the purposes of this Act

Regulation (EU) 2023/588 of the European Parliament and of the Council of 15 March 2023 establishing the Union Secure Connectivity Programme for the period 2023-2027.

[4] § 90 para. 1 of the Act No. 127/2005 Coll., on electronic communications and on amendments of certain related laws (Electronic Communications Act), as amended.

[5] § 2 point i) of the Act No. 123/1998 Coll., on the right to environmental information, as amended.

a) domain name system means a hierarchical distributed naming system which enables the identification of internet services and resources, allowing end-user devices to use internet routing and connectivity services to reach those services and resources,
b) the administration and operation of a top-level domain registry means an activity of administering a specific delegated top-level domain, including the registration of domain names within the top-level domain and the technical operation of name servers, the maintenance of databases providing for the administration and operation of the top-level domain and the distribution of top level domain zone files between name servers, except where the top-level domain registry uses top-level domain names only for its own use,
c) cloud computing service means an information society service as defined by law governing information society services that enables on-demand administration and broad remote access to a scalable and elastic pool of shareable computing resources, including where such resources are distributed across several locations,
d) data centre service means a service that encompasses structures, or groups of structures, dedicated to the centralised accommodation, interconnection and operation of information technology and network equipment providing data storage, processing and transport services together with all the facilities and infrastructures for power distribution and environmental control,
e) content delivery network means a network of geographically distributed servers for the purpose of ensuring high availability, accessibility or fast delivery of digital content and services to internet users,
f) social networking services platform means a platform that enables end-users to connect, share, discover and communicate with each other across multiple devices, in particular via chats, posts, videos and recommendations,
g) managed service means a service related to the installation, management, operation or maintenance of technical assets via assistance or active administration, carried out at customers' premises or at a distance,
h) managed security service means a service that consists of activities related to the cybersecurity risk management or the provision of assistance for such activities, and
i) entity providing domain name registration services means a registrar or an agent providing such services on behalf of registrar.

TITLE II
Regulated service provider

Section 1

Regulated service and the regime of its provider

§ 3
Regulated service

A regulated service is a service, which has been decided on by the Agency pursuant to § 6 paragraph 2.

§ 4
Conditions for registration of a regulated service

(1) The conditions for registration of a regulated service are met if

a) it is a service that is significant for the safeguarding of important social or economic activities or for security in the Czech Republic, in one of these sectors:
1. public administration and the exercise of public authority,
2. energy,
3. manufacturing,
4. food industry,
5. chemical industry,
6. water management,
7. waste management,
8. transport,
9. digital infrastructure and services,
10. financial market,
11. health,
12. science, research and education,
13. postal and courier services,
14. defence industry,
15. space industry, and

b) the service provider is a medium or large enterprise within the meaning of the Commission Recommendation 2003/361/EC of 6 May 2003 on the definition of micro and small and medium-sized enterprises (hereinafter referred to as "Commission Recommendation 2003/361/EC")[6)] or is important for the

[6] Communication of the Ministry of Industry and Trade No. 7/2023 on the publication of the Czech version of Commission Recommendation 2003/361/EC of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises.

safeguarding of significant social or economic activities or for security in the Czech Republic.

(2) The list of services referred to in paragraph 1(a) and the definition of the conditions of significance of the provider referred to in paragraph 1(b) shall be established by Decree issued by the Agency.

§ 5

Furthermore, the conditions for registration of a regulated service are met if

a) it is a service referred to in Article 4(1)(a); and
   1. its provider is the sole provider of the service in the Czech Republic and the service is essential to the maintenance of important social or economic activities in the state,
   1. disruption to this service could have a significant impact on the security of the Czech republic, internal order or life and health,
   2. a disruption of that service could give rise to significant systemic risks, in particular in sectors where such a disruption could have a cross-border impact; or
   3. the provider is, because of its specific importance at regional or national level, essential for a particular type of service or sector or for other interrelated sectors in the Czech Republic,
b) its disruption can cause a major disruption affecting more than 125,000 people through threats to the security of the Czech Republic, its internal order, life and health, property values or the environment,
c) its disruption is likely to cause significant interference with the ability to provide another regulated service of a provider of regulated service under the higher obligations regime; or
d) its provider is a critical infrastructure entity under the legislation governing crisis management and critical infrastructure; in such a case the regulated service is the service corresponding to the designated critical infrastructure element.

§ 6
Notification and registration of a regulated service

(1) For the purposes of issuing a decision on the registration of a regulated service, a provider of a service meeting the conditions for the registration of a regulated service pursuant to § 4(1) shall be obliged to notify the Agency of that service within 60 days of the date on which the conditions were met.
(2) The Agency shall decide on the registration of a regulated service if the conditions for the registration of a regulated service pursuant to § 4(1) or § 5 are met.
(3) Proceedings for registration of a regulated service meeting the conditions for registration under § 5 may be initiated only ex officio.

(4) A decision on the registration of a regulated service pursuant to paragraph 2 may be the first act of the Agency in the proceedings. An appeal against a decision on the registration of a regulated service shall not have suspensive effect.

§ 7
Special provisions for determining a size of an enterprise

By way of derogation from the rules of Commission Recommendation 2003/361/EC, for the purposes of this Act

a) Article 3(4) of Commission Recommendation 2003/361/EC shall not apply,
b) organisational units of the State[7)], local self-government units and the Czech National Bank shall not be regarded as enterprises,
c) persons whose technical assets are wholly separate from the technical assets used for the provision of the regulated service by a person being assessed shall not be considered to be a partner or connected enterprise; and
d) for determining the size of a provider of regulated service in the science, research and education sector, which is not an enterprise, the rules for determining the size of an enterprise under Commission Recommendation 2003/361/EC, including the special rules provided for in this Act, shall apply mutatis mutandis.

§ 8
Regime of the provider of regulated service

(1) The provider of regulated service is subject to the higher obligations regime if it is of significant economic, social or security importance for the Czech Republic because of its size, number of users, geographic spread of the service, impact on the functioning of a sector or another provider of regulated service, or the riskiness of its operation. A provider of regulated service that is not subject to the higher obligations regime under the first sentence shall be subject to the lower obligations regime.
(2) The division of providers according to the provided regulated services into the regimes referred to in paragraph 1 shall be determined by Decree issued by the Agency.
(3) If a regulated service is registered by decision of the Agency on the basis of meeting the conditions for registration pursuant to § 5, its provider is subject to the higher obligations regime.

§ 9

(1) The provider of regulated service is obliged to notify the Agency of changes to the regulated service that may lead to a change in the regime of its provider no later than 60 days from the date on which the change to the regulated service occurred.

[7] § 3 of Act No. 219/2000 Coll., on the Property of the Czech Republic and its Representation in Legal Relations, as amended.

(2) When changing the regime of the provider of regulated service from the lower obligations regime to the higher obligations regime, new deadlines for the commencement of compliance with the obligations under § 11(1), § 13(4) and § 15(4) shall apply.

§ 10
Cancellation of registration of a regulated service

(1) If the service no longer meets the conditions for registration of a regulated service pursuant to § 4(1) or § 5, the Agency shall decide to cancel the registration of the regulated service.
(2) Proceedings for cancellation of the registration of a regulated service shall be initiated at the request of its provider. Proceedings may also be initiated ex officio. The decision on the cancellation of the registration of a regulated service may be the first act in the proceedings. An appeal against a decision on the cancellation of the registration of the regulated service is not admissible if the Agency has granted the request in full.
(3) A written decision on the cancellation of the registration of a regulated service shall not be issued in the case where the Agency has granted the application in full or where it has decided to cancel the registration of the regulated service in proceedings initiated ex officio. In such cases, the decision shall take effect upon entry in the file. The Agency shall inform the party of the proceedings in writing of the cancellation of the registration of the regulated service.

Section 2

Obligations of the provider of regulated service and countermeasures

§ 11
Data reporting

(1) The provider of regulated service shall report no later than 30 days from the date of delivery of the decision on registration of the regulated service
   a) contact details, which means the identification data of natural persons who are authorised to act on behalf of the provider of the regulated service in matters governed by this Act, and
   b) supplementary data, which means information on the ownership structure of the provider of the regulated service, technical data relating to the regulated service and information on its geographical spread and cross-border provision.
(2) The provider of the regulated service is obliged to report changes only to the data referred to in paragraph 1 which are not reference data held in the basic registers, within 14 days of the date of the change.

§ 12
Determination of the scope of cybersecurity management system

(1) The scope of cybersecurity management system (hereinafter referred to as the "defined scope") includes assets related to the provision of regulated services.
(2) To define the defined scope, the provider of the regulated service shall:
   a) identify all its primary assets,
   b) assess whether the primary assets are related to the provision of the regulated service, and
   c) for primary assets identified under letter b), identify supporting assets.
(3) The provider of regulated service records assets that are part of the defined scope, as well as primary assets that have been excluded from the defined scope, including reasons for their exclusion.
(4) Primary assets that have not yet been assessed under paragraph 2(b) and supporting assets that have not yet been identified under paragraph 2(c) are part of the defined scope.
(5) The provider of regulated service is obliged to regularly review and update the defined scope.

§ 13
Security measures

(1) Security measures are organizational and technical measures aimed at ensuring the proper provision of regulated services and the cybersecurity of assets.
(2) The provider of the regulated service is obliged to implement and carry out security measures within the defined scope, as stated in § 14, to the extent necessary to ensure the cybersecurity of the regulated service.
(3) The content of the security measures and the method of their implementation and execution are specified by the Decree issued by the Agency.
(4) The provider of regulated service must begin fulfilling the obligation to implement and carry out security measures for each regulated service no later than 1 year from the date of receipt of the decision on the registration of the regulated service.
(5) If the provider of regulated service implements or carries out security measures through a supplier, they are obliged to select their supplier in accordance with the requirements arising from the security measures and to include the requirements arising from the security measures into the contracts with the supplier.

§ 14
List of security measures

(1) For regulated service providers under the higher obligations regime, the following are
   a) organisational measures
      1. information security management system,
      2. top management responsibilities,
      3. establishment of security roles,

4. management of security policy and security documentation,
5. asset management,
6. risk management,
7. supplier management,
8. human resource security,
9. change management,
10. acquisition, development and maintenance,
11. access control,
12. cybersecurity event and cybersecurity incident management,
13. business continuity management and
14. cybersecurity audit,

b) technical measures

1. physical security,
2. security of communication networks,
3. identity and authentication management,
4. management of access rights and authorisations,
5. detection of cybersecurity events,
6. recording of cybersecurity events,
7. evaluating cybersecurity events,
8. application security,
9. cryptographic algorithms,
10. ensuring the availability of the regulated service; and
11. security of industrial, control and similar specific technical assets.

(2) For providers of regulated services under the lower obligations regime, the security measures are

a) minimum cybersecurity assurance scheme,
b) top management responsibilities,
c) asset management
d) risk management,
e) human resource security,
f) business continuity management,
g) access control,
h) identity and permissions management,
i) detection and recording of cybersecurity events,
j) cybersecurity incidents handling,
k) security of communication networks,
l) application security and
m) cryptographic algorithms.

§ 15
Cybersecurity incident reporting

(1) The provider of regulated service under the regime of higher obligations is required to report to the Agency, in accordance with the procedure under § 16, cybersecurity incidents that

occurred within the defined scope, originated in cyberspace, unless the intentional cause can be ruled out within the time limit specified in § 16 (1).

(2) The provider of regulated services under the regime of lower obligations is required to report cybersecurity incidents that occurred within the defined scope, originated in cyberspace, had a significant impact on the provision of the regulated service, and where intentional cause cannot be ruled out within the time limit specified in § 16 (1) to the national team for the coordination and management of cybersecurity incidents, events, and threats (hereinafter referred to as "National CERT").

(3) A cybersecurity incident is considered to have a significant impact on the provision of the regulated service if it caused or could cause serious operational disruption of services, financial losses, or could cause significant harm to other persons. The method of evaluating the significance of the impact of a cybersecurity incident on the provision of the regulated service by the provider of regulated services under the regime of lower obligations is determined by Decree issued by the Agency.

(4) The provider of regulated services shall begin fulfilling the obligation to report cybersecurity incidents under paragraphs 1 and 2 for each regulated service no later than 1 year from the date of receipt of the decision on the registration of the regulated service.

(5) The Agency also accepts voluntary reports of cybersecurity incidents, cybersecurity events, or cyber threats. Vulnerabilities can also be reported to the Agency.

§ 16
Procedure for reporting cybersecurity incidents

(1) The provider of regulated services shall, without undue delay, and no later than 24 hours after identifying a cybersecurity incident, submit an initial report containing their identification details, basic information about the cybersecurity incident, and whether they believe the cybersecurity incident was caused by unlawful interference or could have cross-border implications.

(2) The Agency shall inform the provider of regulated services under the regime of higher obligations, without undue delay and no later than 24 hours after the cybersecurity incident is reported under paragraph 1, whether the cybersecurity incident has a significant impact on the state's cyberspace. The significance of the impact on the state's cyberspace is determined by the severity of the impact on the provision of the regulated service, the affected sector, and the current situation in cyberspace with potential implications for the security of the Czech Republic.

(3) In the event of a report of a cybersecurity incident with a significant impact on the provision of the regulated service pursuant to § 15 (2) or on the national cyberspace pursuant to paragraph 2, the provider of the regulated service shall also submit

a) without undue delay, but no later than 72 hours after becoming aware of the cybersecurity incident, a notification updating the information referred to in paragraph 1, providing an initial assessment of the cybersecurity incident and indicating the impact and indicators of compromise, if available; the trust service provider according to

directly applicable European Union regulation[8] shall provide a notification under this point within 24 hours of becoming aware of the cybersecurity incident,

b) upon request of the Agency or the National CERT, an interim report on significant changes in the status of cybersecurity incident handling; and

c) no later than 30 days after submitting the report under letter a), a final report on the resolution of the cybersecurity incident; if the cybersecurity incident continues beyond the specified period, the provider of regulated services shall submit a progress report on the current status of handling the cybersecurity incident without undue delay after the period has expired, and then submit a final report on the resolution of the cybersecurity incident no later than 30 days after the incident is resolved.

(4) The provider of regulated services reports cybersecurity incidents, including voluntary reports under this law, through the NUKIB Portal. If the NUKIB Portal cannot be used, the provider of regulated services under the regime of higher obligations shall send the report to the email address of the Agency designated for receiving cybersecurity incident reports, or to the data mailbox of the Agency, and the provider of regulated services under the regime of lower obligations shall send the report to the National CERT's email address designated for receiving cybersecurity incident reports, or to the National CERT's data mailbox.

(5) The content requirements, format, and method of reporting cybersecurity incidents, progress reports on significant changes in the status of handling cybersecurity incidents, progress reports on the current status of handling cybersecurity incidents, and final reports on the resolution of cybersecurity incidents are determined by the Decree issued by the Agency.

§ 17
Cybersecurity incident handling

(1) The Agency or the National CERT shall provide, without undue delay and no later than 24 hours after receiving the initial report under § 16, its assessment of the cybersecurity incident to the provider of regulated service.

(2) At the request of the affected provider of regulated service, the Agency or the National CERT shall provide methodological support for the implementation of mitigating measures and, if necessary, additional technical support for managing the reported cybersecurity incident.

(3) Every person shall, upon the request of the Agency, provide necessary information and cooperation in managing the cybersecurity incident, if the intended purpose cannot be achieved otherwise or would otherwise be significantly hindered. The required cooperation does not need to be provided if it is prevented by a legal or state-recognized obligation of confidentiality or by fulfilling another legal obligation.

(4) Data on cybersecurity incidents, events, threats and vulnerabilities are kept in the records pursuant to § 46.

(5) Paragraphs 1 and 2 shall similarly apply to the handling of cybersecurity incidents reported under § 15(5) and cybersecurity incidents reported by another supervisory authority in

connection with the fulfilment of obligations under a special sectoral regulation according to § 70.

§ 18
Specific provisions on the obligations of providers of regulated services in the digital infrastructure and services sector

(1) A regulated service provider that is a provider of a regulated service of a domain name translation system, a trust service under a directly applicable regulation of the European Union[8], a TLD registry management and operation service, a cloud computing service, a data centre service, a content delivery network service, an online marketplace service[9)], internet search engine services[10)] under a directly applicable European Union regulation, social network platform services, managed services or managed security services, it shall, in relation to those regulated services, implement and enforce, within the specified scope, appropriate and proportionate security measures including at least risk management, security policy and documentation management, cybersecurity incident management, business continuity management, supplier management, secure acquisition, development and maintenance, application security, human resources security, cryptographic algorithms, access control and identity and authentication management , to the extent and in the manner set out in the Implementing Regulation of the European Commission laying down rules for the application of Directive (EU) 2022/2555 of the European Parliament and of the Council ('the Commission Implementing Regulation') as regards the technical and methodological requirements of the measures that those regulated service providers are required to take; § 13(2) shall not apply in relation to those regulated services.

(2) A provider of a regulated service that is a provider of a regulated service referred to in paragraph 1, with the exception of a trust services under a directly applicable regulation of the European Union, shall, in relation to that regulated service, be obliged to report, within a specified scope, all cybersecurity incidents with a significant impact on the provision of the regulated service; § 15(1) and (2) shall not apply in relation to that regulated service with respect to the definition of reportable incidents. The method for determining the significance of the impact of a cybersecurity incident on the provision of a regulated service shall be laid down in implementing Commission Regulation. With regard to the method of reporting cybersecurity incidents, the general provisions in § 15 and 16 shall apply, unless a specific procedure is laid down in a Commission implementing regulation.

(3) A provider of a regulated service who is a provider of a regulated service referred to in paragraph 1, with the exception of a trust services under a directly applicable regulation of the European Union, and who has its main establishment in another Member State of the European Union or in a Contracting State to the Agreement on the European Economic Area (hereinafter referred to as "another Member State"), or has an appointed representative in another Member State, shall comply with the obligations set out in this Act in relation to

[9] Act No. 634/1992 Coll., on Consumer Protection, as amended.

[10] Article 2(5) of Regulation (EU) 2019/1150 of the European Parliament and of the Council of 20 June 2019 on promoting fairness and transparency for business users of online intermediary services.

that regulated service only to the extent of paragraph 1. Obligations imposed by a decision or measure of a general nature of the Agency on the basis of this Act shall be binding for the provider of a regulated service pursuant to the first sentence only if the Agency expressly so provides in the decision or measure of a general nature.

(4) A provider of a regulated service referred to in paragraph 1 under the regime of higher obligations shall comply with the provisions of the Commission implementing regulation referred to in paragraphs 1 and 2 applicable to persons classified as essential entities. A provider of a regulated service referred to in paragraph 1 which is subject to a regime of lower obligations shall comply with the provisions of the Commission implementing regulation referred to in paragraphs 1 and 2 applicable to persons classified as important entities.

(5) The performance of the obligations of the provider of a regulated service referred to in paragraph 1 in relation to regulated services not referred to in paragraph 1 shall not be affected by this provision.

§ 19
Notification obligations

(1) Where the provider of a regulated service considers it appropriate for the purpose of ensuring the proper provision of the regulated service and the cybersecurity of assets, it shall without undue delay notify the users of the regulated service of a cybersecurity incident with a significant impact that could adversely affect the provision of that service. The Agency may impose an obligation or prohibition on a provider of a regulated service that is affected by a cybersecurity incident with a significant impact to inform the users of the regulated service of that incident. In the decision to impose an obligation or prohibition to inform pursuant to the preceding sentence, the Authority shall specify the scope of the information obligation or prohibition.

(2) The provider of the regulated service shall inform the user of the regulated service who may be affected by a significant threat, without undue delay, in an appropriate and comprehensible manner, of such steps that the user may take in response to that threat in order to minimise the potential impact of its realisation on that user. Where possible and appropriate, the regulated service provider shall also inform the user of the significant threat.

§ 20
Countermeasures

(1) The countermeasures are
   a) alert,
   b) warning and
   c) reactive countermeasures.

(2) Everyone shall provide the necessary cooperation to the Agency in gathering information for issuing countermeasures. The requested cooperation need not be provided if it is

prevented by a statutory or state-recognised duty of confidentiality or the fulfilment of another statutory obligation.

§ 21
Alert

(1) The Agency may, after consultation with the regulated service provider concerned, for reasons of protection of the security of the Czech Republic, internal order, life and health or property value, inform the public in the form of an alert about a cybersecurity incident or a breach of the obligations set out in this Act, or order the regulated service provider concerned to do so itself.
(2) The Agency shall inform the public about a cybersecurity incident or a breach of the obligations laid down in this Act pursuant to paragraph 1 through its website and shall inform regulated service providers, where appropriate, through the NUKIB Portal.
(3) A decision of the Agency pursuant to paragraph 1 may be the first act in the proceedings and an appeal against it shall not have suspensive effect.

§ 22
Warning

(1) The Agency will issue a warning if it becomes aware of a serious cybersecurity threat or vulnerability.
(2) The Agency will notify the affected regulated service providers of the warning via the NUKIB Portal and publish it on the Agency's official notice board. The Agency shall not publish the warning if publication could compromise the ensuring of cybersecurity, other legitimate government interests, or could identify the person who reported the threat, vulnerability, or related cybersecurity incident.

§ 23
Reactive countermeasures

(1) The Agency shall issue a decision requiring the provider of the regulated service to take reactive countermeasures
   a) to address an impending or ongoing cybersecurity incident,
   b) to protect assets from a cybersecurity incident, or
   c) to enhance asset protection based on the analysis of an already resolved cybersecurity incident.
(2) Reactive countermeasures must be implemented by the provider of the regulated service within the specified scope, unless the Agency or another legal regulation provides otherwise.
(3) The decision on the obligation to take reactive countermeasures may be the first act in the proceedings. If the decision cannot be delivered to the addressee by hand within 72 hours of its issue, it shall be delivered by posting it on the official notice board of the Agency and

shall be enforceable at that time. The decision referred to in the first sentence may also be issued by the Agency in an on-the-spot procedure under the Administrative Procedure Code. An appeal against a decision pursuant to paragraph 1 shall not have suspensive effect.

(4) If the countermeasure referred to in paragraph 1 concerns an unspecified group of authorities or persons, the Agency shall issue it in the form of a measure of a general nature.

(5) A measure of a general nature pursuant to paragraph 4 shall come into effect at the moment of its publication on the official notice board of the Agency; the provisions of § 172 of the Code of Administrative Procedure shall not apply. The Agency shall also notify the providers of the regulated service affected by the measure of a general nature.

(6) Unless the Agency specifies otherwise in the reactive countermeasure, the provider of the regulated service shall notify the Agency of the implementation of the reactive countermeasure and its result without undue delay, at the latest within the time limit specified in the reactive countermeasure.

Section 3

Relationship between the regulated service provider and its suppliers

§ 24
Special arrangements for the transfer of information and data from a supplier

(1) The Agency may, in the event of an impending or ongoing cybersecurity incident that could have a serious impact on the provision of a regulated service with an impact on the security of the Czech Republic, internal order, life and health, property values or the environment, at the initiative of a provider of a regulated service under the regime of higher obligations, who has unsuccessfully called on its supplier to transfer information and data, impose on that supplier the obligation to transfer to the provider of the regulated service information and data related to the operation of assets used to provide the regulated service. If that supplier does not possess the information or data related to the operation of the assets used to provide the regulated service or if, given the factual circumstances, it is impractical to require the supplier to provide it, the Agency may impose the obligation under the first sentence on anyone, who is in possession of the requested information and data. The Agency may, in a decision pursuant to the first and second sentences, specify the format, scope, manner and time limit for the transmission of such information and data and impose an obligation to securely destroy such information and data and all copies thereof after transmission.

(2) A request pursuant to paragraph 1 shall include a justification for the request with respect to an impending or ongoing cybersecurity incident, a detailed description of previous dealings between the supplier and the regulated service provider, and the possible consequences if the requested information and data is not transferred.

(3) The decision pursuant to paragraph 1 may be the first act in the proceedings. An appeal against a decision under the first sentence shall not have suspensive effect.

(4) The supplier or the person in possession of the requested information and data shall be entitled to reimbursement of the costs reasonably incurred by providing the information and data to the provider of the regulated service. Negotiations on the reimbursement of reasonable costs associated with the provision of information and data shall not be an obstacle to the proper fulfilment of the obligation to provide information and data.
(5) For the purposes of the enforcement of a decision under paragraph 1, information and data shall be considered movable property.

Section 4

Strategically important service

§ 25

(1) A strategically important service is a regulated service whose disruption could have a serious impact on the security of the Czech Republic or internal order. The Agency shall by decree determine the services in the sectors of public administration, energy, transport and digital infrastructure and the services that meet the conditions of a strategically important service under the first sentence.
(2) Information that the regulated service is a strategically important service is part of the justification for the decision to register the regulated service.
(3) The Agency shall also decide that the regulated service provided by the provider of the regulated service is a strategically important service if the disruption of the service could have a serious impact on the security of the Czech Republic or internal order.
(4) An appeal against a decision to designate a strategically important service pursuant to paragraph 3 shall not have suspensive effect.

§ 26

(1) The provider of regulated service shall notify the Agency of changes to the regulated service if they in result meet the conditions of a strategically important service pursuant to § 25(1) within 60 days of the date of the change to the regulated service.
(2) If the regulated service ceases to meet the conditions of a strategically important service pursuant to § 25(1), or if the reasons for the designation of a strategically important service pursuant to § 25(3) cease to exist, the procedure shall be similar to the procedure for cancellation of the registration of a regulated service pursuant to § 10.

Section 5

Assessment mechanism for supply chain security

Supplier risk assessment

§ 27

(1) For the purposes of the assessment of risks related to the supplier of a strategically important service provider, the Agency collects and evaluates information and data regarding the entity directly or indirectly providing a delivery into a strategically important service, and which are related to a possible threat to the security of the Czech Republic or internal order.

(2) For the purposes of the assessment mechanism for supply chain security the following terms shall be understood as follows:

a) a critical part of the specified scope shall be the assets of the specified scope of the strategically important service for which the provider of the strategically important service has assessed the impact of an information security breach on the specified scope of the strategically important service at the level of high or critical in accordance with the decree issued by the Agency; the critical part of the specified scope shall always comprise of at least the assets of the specified scope of the strategically important service that provide the indispensable functions of the strategically important service,

b) a security-significant delivery shall be a delivery directed to a critical part of the specified scope consisting in the providing, developing, manufacturing, assembling, managing, operating, or servicing of the assets, and

c) a supplier of a security-significant delivery shall be the one who provides, directly or as a subcontractor, a security-significant delivery to a provider of a strategically important service.

(3) The indispensable function is an activity or feature of an asset that supports the operation of a strategically important service, the disruption of which could have a serious impact on the provision of the strategically important service.

(4) The decree issued by the Agency shall provide the list of the indispensable functions of the strategically important services.

§ 28

(1) The Ministry of Industry and Trade, the Ministry of Foreign Affairs and the Ministry of the Interior shall, for the purpose of collection and evaluation of information and data pursuant to § 27(1), provide the Agency, upon its request, without undue delay, but not later than within 30 days after receipt of the request, with an opinion on the risk associated with the supplier or with the information the abovementioned institutions gathered during their activity.

(2) The Prosecutor General's Office, the Police of the Czech Republic, the Office for the Protection of Competition and the intelligence services of the Czech Republic shall, for the purpose of collection and evaluation of the information and data pursuant to § 27(1), provide the Agency, upon its request, without undue delay, but not later than within 30 days after receipt of the request, with the information the abovementioned institutions gathered during their activity.

(3) For the purpose of the collection and evaluation of the information and data pursuant to § 27(1), the Financial Analytical Office shall provide the Agency, upon its request, without undue delay, but not later than 30 days after receipt of the request, with the requested information the Financial Analytical Office gathered during its activity as per the legislation governing the measures against legitimisation of proceeds of crime and financing of terrorism and the legislation governing the implementation of international sanctions.

(4) Except for the institutions mentioned in paragraphs 1 to 3 above, everybody shall provide the Agency with necessary cooperation during the procurement of information necessary for collection and evaluation of information and data pursuant to § 27(1). The requested cooperation does not have to be provided in case the statutory or state-recognized obligation to maintain the confidentiality or compliance with another statutory obligation prevent the provision of such a cooperation or in case the Agency is capable of gathering the requested information based on its own activity or by the procedure set in the paragraphs 1 to 3 above.

§ 29
Mitigation of risks associated with supplier

(1) The Agency issues a measure of a general nature establishing conditions for or prohibition to the provider of the strategically important service regarding the use of the performance of a security-significant delivery supplier in a critical part of the specified scope, if the Agency finds, based on an evaluation of the supplier risk criteria fulfilment, a significant threat to the security of the Czech Republic or internal order. The Agency shall set the time limit for fulfilling the conditions or prohibition contained in a measure of a general nature with regard to its impact on the provider of the strategically important service, where the Agency shall, when setting the abovementioned time limit, take account of the depreciation time as per the legislation governing the income tax.

(2) The Agency shall consult the proposal of the measure of a general nature pursuant to Paragraph 1 above with the authorities referred to in § 28 Paragraphs 1 to 3 and the Ministry of Finance, and with the Czech Telecommunication Office and the Energy Regulatory Office in case the proposal of the measure of a general nature affects their jurisdiction. After consulting the proposal of the measure of a general nature pursuant to the first sentence, the Agency shall introduce the proposal to the members of the National Security Council for the purposes of their notification, unless the course of action pursuant to paragraph 3 below is taken.

(3) After the consultation pursuant to paragraph 2 above, the Agency shall table the proposal of the measure of a general nature to the government in case the period for complience with the prohibition contained in the proposal of the measure of a general nature regarding the current or previous performance by the security-significant delivery provider is:

a) shorter than the depreciation time as per the legislation governing the income tax, if the depreciation time is set by such a legislation in relation to the concerned security-significant delivery, or

b) shorter than 5 years after acquiring the security-significant delivery, if the depreciation time is not set by the legislation governing the income tax regarding the concerned security-significant delivery.

(4) The government shall instruct the Agency on the further course of action regarding the proposal of the measure of a general nature pursuant to paragraph 3 above.

(5) After notification of the members of the National Security Council pursuant to paragraph 2 and after the procedure pursuant to paragraphs 3 and 4 above, the Agency shall submit the proposal of the measure of a general nature by the means of public notice and call on the supplier the fulfilment of which is targeted by the measure of a general nature, and other subjects concerned, to submit objections to the proposal of the measure of a general nature. Unless the Agency specifies otherwise, the time limit to object the abovementioned proposal is 30 days. Provisions of § 172 (1) and (5) of the Rules of the Administration Procedure shall not apply to the procedure as per this provision.

(6) The Agency shall review the findings on which the measure of a general nature under paragraph 1 was issued at least once every four years. Should the Agency identify that these findings have ceased to exist, it shall repeal the measure of a general nature referred to in paragraph 1 in following a procedure similar to that set out in paragraphs 1 to 4.

§ 30

Exemptions from the risk mitigation measures associated with suppliers

(1) The Agency may, if the nature of the threat to the security of the Czech Republic or to internal order permits so, grant an exemption from the conditions or prohibition set out in a measure of a general nature pursuant to § 29 if the compliance with the measure of a general nature by the provider of a strategically important service could endanger the performance of the strategically important service substantially.

(2) The procedure for granting an exemption referred to in paragraph 1 shall be initiated at the request of the provider of a strategically important service. The provider of a strategically important service is required to provide evidence to prove the facts invoked in the application.

(3) The Agency shall set out the conditions for application of the exemption by the decision granting the exemption. In case of violation of the application conditions of the exemption or in case the reason for which it was granted ceases to exist, the Agency shall revoke the exemption by its decision.

§ 31

Obligations related to supply chain security assessment

(1) The provider of a strategically important service shall

a) ascertain, with reasonable endeavour, information about suppliers of security-significant deliveries,
b) keep records of information referred to in point a) at least to the scope enabling to identify all the security-significant deliveries and their suppliers, and
c) report the information to the Agency, referred to in point a) and changes thereto, within 10 days of becoming aware of it.

(2) A provider of a strategically important service shall begin to comply with the obligation to report the information pursuant to paragraph 1 within 1 year of the day the respective regulated service became a strategically important service.

(3) The information reported to the Agency pursuant to (1)(c) and (2) and the information ascertained in accordance with the procedure pursuant to § 27 and § 28 are part of the register of suppliers of the security-significant deliveries.

§ 32
Termination of contract resulting from the mitigation of supplier-related risks

The provider of a strategically important service may terminate the contract in case it is not possible to carry on the performance of the contract without violating a measure of a general nature referred to in § 29. The right of the provider of a strategically important service to terminate the contract pursuant to other legal regulation shall remain unaffected by the first sentence.

Section 6

Ensuring the availability of a strategically important service

§ 33

(1) The provider of a strategically important service shall ensure the availability of a strategically important service within the necessary scope, at the specified time and quality from the territory of the Czech Republic.

(2) The provider of a strategically important service shall test the ability to ensure the provision of a strategically important service within the necessary scope from the territory of the Czech Republic at least once every two years and draw up a report about the test.

(3) The provider of a strategically important service shall begin to comply with the obligations referred to in paragraphs 1 and 2 in relation to each strategically important service within 1 year of the day the respective regulated service became a strategically important service.

(4) The necessary scope shall be understood as the part of a strategically important service, the unavailability of which may have a serious impact on the security of the Czech Republic or the internal order. The Agency shall establish the list of parts of strategically important services constituting the necessary scope and the method of their specification by its decree or decision pursuant to § 25 (3).

(5) The specified time and quality of service shall be determined by the provider of a strategically important service, taking account of the nature and specifics of the provided

strategically important service, the purpose of its provision and gravity of impacts occurring on the side of the strategically important service´s user resulting from the disruption of its proper provision. The provider of a strategically important service shall draw up a report regarding determination of the specified time and quality of service.

TITLE III
A person providing domain name registration services and a person managing and operating a top-level domain registry

§ 34

Reporting of data of persons providing domain name registration services

(1) The person providing domain name registration services shall report to the Agency without undue delay, but no later than 30 days from the date on which it started providing domain name registration services, the following data:
   a) the name of the person,
   b) the address of the main establishment and of its other establishments in the territory of the Member States of the European Union or the Contracting States of the Agreement on the European Economic Area, and where applicable, the representative of the person referred to in § 67,
   c) up-to-date contact details, including e-mail addresses and telephone numbers of the person or its representative as referred to in § 67,
   d) the Member States of the European Union or the Contracting States of the Agreement on the European Economic Area in which the person provides its services; and
   e) the range of public IP addresses of the person.

(2) In the event of changes in the data reported pursuant to paragraph 1, the domain name registration service provider shall update the reported data without undue delay, but no later than 90 days from the date of the change.

(3) The format and method of reporting pursuant to paragraph 1 shall be determined by the Decree issued by the Agency.

§ 35
Collection of domain name registration data

(1) The person managing and operating the Top Level Domain Registry and the person providing domain name registration services shall collect and store accurate and complete domain name registration data in a dedicated database in accordance with the legislation

governing the protection of personal data and directly applicable European Union legislation[11)] with regard to data that are personal data.

(2) The database referred to in paragraph 1 shall contain the information necessary to identify and contact domain name holders and points of contact managing top-level domains, at least
   a) the domain name,
   b) the date of registration,
   c) the name of the domain name holder,
   d) the email address of the domain name holder,
   e) the telephone number of the domain name holder,
   f) the email address and telephone number of the contact point managing the domain name if different from the holder of the domain name.

(3) The person managing and operating the Top Level Domain Registry and the person providing domain name registration services shall establish publicly available policies and procedures to ensure the accuracy and completeness of the information maintained in the database, including procedures for verifying the identity of the domain name holder. Those policies and procedures shall not lead to duplication of data collected. To this end, the person managing and operating the Top Level Domain Registry and the person providing domain name registration services shall cooperate with each other. The person managing and operating the Top Level Domain Registry registry and the person providing domain name registration services shall enter into a written agreement to comply with these policies and procedures.

(4) The person administering and operating a Top Level Domain Registry and a person providing domain name registration services may, when establishing procedures for verifying the identity of a domain name holder, use an approach using an electronic identification means issued within a qualified electronic identification system under the law governing electronic identification.

(5) The person managing and operating the Top Level Domain Registry and the person providing domain name registration services shall, without undue delay after the registration of a domain name, publish the domain name registration data, which are not personal data.

(6) The person managing and operating the Top Level Domain Registry and the person providing domain name registration services shall provide access to specific domain name registration data on the basis of lawful and duly justified requests for access by legitimate applicants in accordance with European Union legislation[11] governing the protection of personal data, without undue delay and no later than 72 hours after the request for access. Policies and procedures for the publication of such data shall be publicly available.

[11] 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.

TITLE IV
Other means for ensuring cybersecurity

§ 36
Exception to the right to information

Information the disclosure of which could jeopardise the ensuring of cybersecurity or information which is held in the records maintained by the Agency pursuant to § 46, shall not be disclosed under the legislation governing free access to information or access to the information on the environment.

§ 37
State of cyber emergency

A state of cyber emergency may be declared if the security of information in cyberspace is significantly threatened or compromised, which may result in negative impacts on the provision of regulated services or may endanger the security of the Czech Republic, internal order, life and health, property values or the environment.

§ 38
Declaration of state of cyber emergency

(1) A state of cyber emergency may be declared only with reasons and for a strictly necessary period of time, up to a maximum of 30 days. The Agency shall declare a cyber emergency on the Agency's official notice board. The declaration of a cyber emergency shall take effect at the time specified therein. Information on the declaration of a cyber emergency shall be published by other appropriate means, in particular through the mass media.

(2) The Agency shall immediately inform the Government of the declaration of a cyber emergency and its extension. If the reasons for declaring a cyber emergency persist, the Agency may extend the declared cyber emergency accordingly, but not longer than 60 days from the date of its declaration. In the event that a significant threat or breach of information security in cyberspace cannot be averted during a state of cyber emergency or the reasons for declaring a state of cyber emergency persist beyond 60 days from the date of the declaration, the Agency shall immediately request the Government to declare a state of emergency to address the significant threat or breach of information security in cyberspace.

(3) In the event of a declared state of emergency, state of national emergency or state of war to address a significant threat or breach of information security in cyberspace, the cyber emergency remains in effect for the duration of the declared state of emergency, state of national emergency or state of war. Measures declared by the Agency under a state of cyber emergency shall remain in force in the event of a declaration of a state of emergency, a state of national emergency or a state of war to address a significant threat or breach of information security in cyberspace, unless the Government decides otherwise.

(4) A state of cyber emergency ends at the expiration of the period for which it was declared, unless the Agency or the Government decides to terminate it before the expiration of that period. This is without prejudice to paragraph 3. The termination of the state of cyber

emergency shall be published on the official notice board of the Agency and by other appropriate means, in particular through the mass media; the termination of the state of cyber emergency shall take effect at the time specified therein.

§ 39
Measures to be taken during the state of cyber emergency

(1) The Agency shall decide on the imposition of measures to address the significant threat or breach of information security in cyberspace during the state of cyber emergency. The Agency may

a) require everyone to provide, for the purpose of imposing measures under this provision and to a reasonable extent, information on material means, on production and operational capacities and human resources, and on the volume of stocks in specified types of material, and everyone shall provide the information within a time limit set by the Agency,

b) prohibit anyone from using technical assets if such assets are imminently threatened by, or already affected by, a cybersecurity incident that could significantly damage or destroy them,

c) order, after a consultation with any employer under the legislation governing employment relations or a service authority or security force under the legislation governing service relationships and the armed forces, on standby duty for specific employees of that employer or on standby duty for specific civil servants of that service authority or specific members of that security force or armed forces if necessary to address a significant threat or breach of information security in cyberspace. The first sentence of Article 95(1) of the Labour Code shall not apply,

d) impose an obligation on anyone to take action to address a cybersecurity incident or to safeguard assets from a cybersecurity incident and to report the implementation of the action and its outcome to the Agency,

e) order anyone to conduct a vulnerability scan or to identify and validate vulnerabilities by simulating a real attack (hereinafter "penetration test"),

f) order anyone to make non-public communications networks under its control available for use by the Agency, which shall use them in the manner usual for that communications network; or

g) impose on the operator of mass media the obligation to publish information on the declaration of a state of cyber emergency and on measures to be taken in the event of a state of cyber emergency; the operator of mass media shall immediately comply with the Agency's request and to publish the information without any modification, without reimbursement of costs.

(2) In addition, in order to address a significant threat or breach of information security in cyberspace, the Agency is authorized to provide material resources in the property of the Czech Republic that are in the use of the Agency and are necessary to address a cybersecurity incident or to secure assets against an impending cybersecurity incident to persons involved in the activities described above.

(3) In a state of cyber emergency, the person who has been requested to do so on the basis of the measures issued by the Agency shall implement the measures referred to in paragraph 1 and to tolerate the restrictions resulting therefrom and to provide the necessary cooperation to the Agency.

(4) Material resources provided, other than those that have been consumed, shall be returned to the Agency upon termination of the state of cyber emergency. The recipient shall return the resources within 60 days of the end of the state of cyber emergency. After this period, the recipient is entitled to use the material resources provided only on the basis of a contract concluded with the Agency. The draft contract shall be drawn up by the Agency on the basis of a request submitted by the recipient within 60 days of the end of the state of cyber emergency. If the recipient fails to submit the request within that period, the use of the means provided shall constitute an unauthorised use of the Agency's property. In the event of failure to return the resource provided, the procedure shall be in accordance with the legislation governing the management of State property.

(5) A decision on a measure under paragraph 1 may be the first act in the proceedings. If the decision cannot be served on the addressee by hand within 24 hours of its issue, it shall be served by posting it on the official notice board of the Agency and shall be enforceable at that time. The Agency may also issue the decision referred to in the first sentence in an on-the-spot procedure under the Administrative Procedure Code. An appeal against a decision pursuant to paragraph 1 shall not have suspensive effect.

(6) If the measure referred to in paragraph 1 is to concern an unspecified group of persons, the Agency shall issue it in the form of a measure of a general nature.

(7) A measure of a general nature pursuant to paragraph 6 shall enter into force at the moment of its posting on the official notice board of the Agency; the provision of § 172 of the Administrative Procedure Code shall not apply. The Agency shall also notify the providers of regulated service affected by the measure of a general nature.

§ 40
Compensation for damages

For the purposes of compensation for damages causally related to measures taken in a state of cyber emergency, the relevant provisions of the legislation governing crisis management and critical infrastructure shall apply mutatis mutandis.

§ 41
Compensation for limiting the right of ownership or imposing an obligation

For the purposes of compensation for the restriction of a property right or the imposition of an obligation in causal connection with measures taken in a cyber emergency, the relevant provisions of the legislation governing crisis management and critical infrastructure shall apply mutatis mutandis.

TITLE V
State administration and its oversight

Section 1

State administration in the field of cybersecurity

§ 42
National Cyber and Information Security Agency

(1) The Agency is the central administrative authority for cybersecurity and for selected areas of protection of classified information under the Act on Protection of Classified Information and Security Clearance. The seat of the Agency is Brno. The Agency's revenue and expenditure form a separate chapter of the State budget.

(2) The Agency is headed by a Director, who is appointed by the Government, after discussion in the Committee of the Chamber of Deputies responsible for security matters, and who is also dismissed by the Government. The Director of the Agency shall be accountable to the Government for the performance of their duties.

(3) The Agency

a) receives notifications of the regulated service or its changes,
b) decides on the registration of the regulated service,
c) determines by decision a strategically important service pursuant to § 25(3),
d) decides on the cancellation of the registration of a regulated service,
e) receives reports of contact and supplementary data and changes thereto,
f) determines security measures appropriate to the regulated service provider's regime,
g) manages and operates the NUKIB Portal,
h) informs the public about a cybersecurity incidents in accordance with the procedures under this Act,
i) issues countermeasures and receives notification of their implementation and outcome,
j) maintains records in accordance with this Act,
k) issues a decision on the obligation to transfer information and data related to the operation of assets used to provide the regulated service to the provider of the regulated service under the regime of higher obligations,
l) lays down, by measures of a general nature, conditions or prohibits the use of the supplier’s services or security-relevant supplies within a critical part of the defined necessary scope,
m) reviews the findings on the basis of which the measure of a general nature under point (l) was issued,
n) decides on requests for exemption and grants exemptions from the conditions or prohibitions set out in a measure of a general nature pursuant to § 29,
o) negotiates contracts and agreements for the sharing of human and material resources in order to exercise its powers and fulfill the duties assigned to it under this Act.,

p) declares, manages and coordinates the state of cyber emergency, imposes obligations and takes measures to avert the state of cyber emergency,
q) decides during a cyber emergency on measures to address and remedy the state of cyber emergency,
r) continuously prepares to ensure the management and remediation of cyber threats,
s) concludes a public contract with the operator of the National CERT,
t) monitors compliance with the obligations under this Act and imposes corrective measures.,
u) imposes sanctions for failure to comply with the obligations set out in this Act,
v) provides necessary cooperation at the request of a supervisory authority of another Member State,
w) issues a decision on the suspension of a European cybersecurity certificate or on the obligation of a conformity assessment body to suspend the validity of a certificate or a certificate pursuant to § 57, and
x) issues a decision on the prohibition or termination of the performance of a function in accordance with § 58.

(4) The Agency furthermore
a) performs analysis and monitoring of threats and risks,
~~b)~~ prepares a national cybersecurity strategy and an action plan for its implementation at least every 5 years and submits them to the Government for approval ,
c) in the field of cybersecurity
1. cooperates with bodies and persons active in this field and in the field of cyber defence, in particular public corporations, research and development institutes and other CERTs,
2. ensures international cooperation in accordance with the legislation governing the powers and functions of central administrative authorities,
3. performs other tasks in accordance with the obligations arising from the Czech Republic's membership in the European Union, the North Atlantic Treaty Organisation and international treaties to which the Czech Republic is bound, in accordance with the legislation governing the powers and functions of central administrative authorities,
4. ensures prevention, education and methodological support and
5. performs research and development,
d) according to the legal regulation governing crisis management and critical infrastructure determines the elements of critical infrastructure in the sector of communication and information systems in the field of cybersecurity or sends to the Ministry of the Interior a draft of the elements of critical infrastructure in the sector of communication and information systems in the field of cybersecurity, the operator of which is an organisational unit of the state, and verifies their actuality every 2 years,
e) fulfil its obligations towards the European Commission, the European Union Agency for Cybersecurity, the European Union Space Programme Agency, the NIS Cooperation Group, the Computer Security Incident Response Team Network (hereinafter “CSIRTs

Network"), the European Cyber Crisis Liaison Organisation Network and other entities in accordance with the relevant European Union legal act[12)],

f) is the single point of contact for ensuring cross-border cooperation in the field of cybersecurity within the European Union and ensures the posting of representatives to the NIS Cooperation Group, the CSIRT Network and the European Cyber Crisis Liaison Organisation Network,

g) participates, if necessary, in the process of peer review and creation of methodology and organizational aspects of peer review developed by the NIS Cooperation Group

h) performs activities in the field of the public regulated service of the European satellite navigation programme Galileo, in particular the functions of the competent public regulated service (PRS) authority according to the relevant European Union regulation[13)],

i) exercises powers in areas related to information and cybersecurity, security accreditation and security of systems and established services within the framework of the Space Program of the European Union, in particular performs the functions of the competent authority for satellite communication within the state administration (GOVSATCOM) according to directly applicable regulation of the European Union[14)],

j) exercises powers in areas related to information and cybersecurity, security accreditation and security of systems and established services within the framework of the European Union Program for secure connectivity, in particular performs functions of the competent authority for secure connectivity according to the directly applicable regulation European Union[15)],

k) is the national cybersecurity certification authority according to the directly applicable regulation European Union[16)],

l) acts as the National Coordination Centre for Research and Development in the field of cybersecurity for the Czech Republic according to the directly applicable European Union legal act[17)],

m) establishes and supports platforms for sharing information in the field of cybersecurity and set rules for their operation,

n) performs other tasks based on this Act and the Act on the Protection of Classified Information and on Security Clearance.

(5) The Agency furthermore

a) coordinates, analyses and acts preventively with regards to

1. cybersecurity threats,
2. cybersecurity vulnerabilities, including vulnerability scanning,
3. cybersecurity events and
4. cybersecurity incidents, including support in managing them,

[12] Directive (EU) 2022/2555 of the European Parliament and of the Council.

[13] Article 5 of Decision (EU) 1104/2011 of the European Parliament and of the Council.

[14] Article 68 of Regulation (EU) 2021/696 of the European Parliament and of the Council.

[15] Article 11 of Regulation (EU) 2023/588 of the European Parliament and of the Council.

[16] Article 58 of Regulation (EU) 2019/881 of the European Parliament and of the Council.

[17] Regulation (EU) 2021/887 of the European Parliament and of the Council.

b) acts as a contact point for regulated service providers under the higher obligations regime,
c) tests the implementation and resilience of asset security, including conducting penetration testing with the consent of the entity affected by the testing,
d) is the coordinator for the purposes of coordinated vulnerability disclosure,
e) maintains records of cybersecurity incidents, events, cyber threats and vulnerabilities,
f) cooperates in the field of cybersecurity,
g) provides consultations in the field of cybersecurity,
h) receives and evaluates initiatives and submissions in the field of cybersecurity,
i) shares data and information from its activities and from records maintained by the Agency, if necessary for ensuring cybersecurity; determines the mandatory level of protection for the data and information shared in this way,
j) performs the role of the CSIRT team and represents the Czech Republic and participates in the functioning of relevant international groups and associations in the field of cybersecurity, including the CSIRTs Network,
k) in appropriate cases, transmit without undue delay information about a cybersecurity incident with a significant impact involving two or more Member States reported pursuant to § 15 and § 16 to the Member States or Contracting States of the Agreement on the European Economic Area concerned and to the European Union Agency for Cybersecurity, while maintaining the confidentiality of the information provided and the security and business interests of the reporting entity,
l) is involved in research and development of cybersecurity tools and solutions, and
m) prioritises the delivery of its services and the performance of its activities according to a risk-based approach and available capacity.

§ 43
National CERT

(1) The National CERT
a) ensures, to the extent provided for in this Act, the sharing of information at national and international level in the field of cybersecurity and acts as a contact point for providers of regulated services under the regime of lower obligations,
b) receives reports of cybersecurity incidents, cybersecurity events, cyber threats and cybersecurity vulnerabilities and evaluates, records, stores and protects this data,
c) provides methodological support, assistance and cooperation to regulated service providers under the lower obligation regime in the occurrence and management of a high-impact cybersecurity incident and in the disclosure of information on cybersecurity vulnerabilities,
d) conducts searches and assessments of cybersecurity vulnerabilities,
e) transmits to the Agency data on reported cyber threats, cybersecurity events, cybersecurity incidents under § 15 and cybersecurity vulnerabilities,
f) informs the competent authority of another Member State, without identifying the reporting entity, of a cybersecurity incident with a significant impact on the continuity of the provision of a regulated service in that Member State, and at the same time inform

the Agency thereof, while preserving the security and privacy interests of the reporting entity,

g) receives and evaluates initiatives from authorities and individuals in the cybersecurity field,
h) performs the role of a CSIRT team and participates in the functioning of international cybersecurity groups, including the CSIRTs Network,
i) participates, where appropriate, in the peer review; and
j) prioritises the delivery of its services and the performance of its activities according to a risk-based approach and available capacity.

(2) The activities of the National CERT referred to in paragraph 1 shall be carried out by the operator of the National CERT, who shall act impartially.

(3) The operator of the National CERT shall carry out the activities referred to in paragraph 1(a), (b) and (e) to (h) free of charge. The operator of the National CERT shall incur the necessary costs for the proper and efficient performance of the activities referred to in paragraph 1.

(4) The operator of the National CERT may only be a legal entity that

a) does not or has not acted against the interest of the Czech Republic according to the legal regulations governing the protection of classified information,
b) manages and operates or participates in the management and operation of relevant technical assets for at least 5 years
c) fulfils the technological prerequisites to carry out the activities referred to in paragraph 1,
d) is a member of a multinational organisation operating in the field of cybersecurity,
e) has no arrears registered in the Czech Republic, with the exception of arrears for which it is permitted to postpone their payment or to spread their payment into instalments,
   1. with the authorities of the Financial Administration of the Czech Republic,
   2. with the authorities of the Customs Administration of the Czech Republic,
   3. on insurance payments and penalties for public health insurance, and
   4. on insurance payments and penalties for social security and state employment policy contributions,
f) has not been finally convicted of a criminal offence unless he is treated as if he had not been convicted,
g) does not have itsmain establishment outside the Czech Republic,
h) does not carry out activities in the field of cybersecurity unregulated by this Act which could interfere with the fulfilment of the obligations referred to in paragraph 1, and
i) holds a valid certificate of an entrepreneur for access to classified information at least for the classification level Confidential under the Classified Information Protection and Security Clearance Act.

(5) A prerequisite for the operation of the National CERT is the conclusion of a public contract pursuant to § 53. The applicant for the operation of the National CERT shall demonstrate compliance with the conditions referred to in paragraph 4 by submitting

a) a statutory declaration with regard to paragraph 4, letters a) to d), g) and h), the contents of which must show that the tenderer fulfils the relevant requirements,

b) an extract from the criminal record in the case of paragraph (4)(f), which must not be older than 3 months,
c) a certificate from the competent health insurance institution in the case of paragraph 4(e)(3) and the competent district social security administration in the case of paragraph 4(e)(4), which must not be older than 30 days; and
d) a valid certificate of an entrepreneur for access to classified information at least for the classification level Confidential according to the Classified Information Protection and Security Clearance Act.

(6) The Agency shall publish information about the operator of the National CERT on its website, namely its business name or name, registered Agency address, personal identification number, data box identifier and the address of its website.

Section 2

Oversight of the exercise of state Administration powers in the area of cybersecurity

§ 44
Permanent Commission for the Oversight of the Agency's Activities

(1) The activities of the Agency are audited by the Chamber of Deputies, which establishes a special oversight body for this purpose (hereinafter referred to as the "Oversight Body").
(2) The Oversight Body shall consist of at least 7 members. The Chamber of Deputies shall determine the number of members so that each of the parliamentary groups constituted according to the affiliation of 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 Oversight Body.
(3) Members of the Oversight Body may enter the premises of the Agency accompanied by the Director of the Agency or an employee authorised by him/her.
(4) The Director of the Agency shall submit to the Oversight Body
a) a report on the activities of the Agency,
b) the draft budget of the Agency,
c) the documents needed to audit the implementation of the Agency 's budget,
d) the internal regulations of the Agency,
e) on request, a report on individual cybersecurity incidents of regulated service providers.
(5) If the Oversight Body considers that the activities of the Agency unlawfully restrict or infringe the rights and freedoms of citizens, it is entitled to request the necessary explanation from the Director of the Agency.
(6) Any violation of the law by an employee of the Agency in the performance of duties under this Act and in selected areas under the Act on the Protection of Classified Information and on Security Clearance, which the Oversight Body discovers in the course of its activities, is obliged to notify the Director of the Agency and the Prime Minister. The obligation of

confidentiality imposed on the members of the supervisory authority under the Act shall not apply to cases where the Oversight Body makes a notification pursuant to the first sentence.

Section 3

Instruments of state administration

§ 45
The NUKIB Portal

(1) The Agency is the administrator and operator of the NUKIB Portal. The NUKIB Portal is used to carry out the activities under this Act, which are the exercise of the powers of the Agency, the sharing of information, the performance of digital acts and the provision of digital services in accordance with the legal regulation governing digital services.

(2) Actions under § 6(1), § 9(1), § 10(2), § 11, § 15(1) and (2), § 23 (6), § 26 (1) and § 31(1)(c) must be carried out exclusively electronically using remote access and via form submissions. Such acts may be performed by other means only if the provisions of this Act so permit and if, for reasons beyond the control of the person performing the act, it is not possible to use the NUKIB Portal to perform the act. An act which is not performed in the manner referred to in the first or second sentence, in the format and structure laid down by the Agency's Decree, shall be ineffective.

(3) The technical and organisational conditions for the use of the NUKIB Portal, the content, format, structure and method of performing the actions referred to in paragraph 2 shall be laid down in Decree issued by the Agency.

§ 46
Records kept by the Agency

(1) The Agency keeps records of
   a) regulated services, including their providers and the data reported by them,
   b) persons providing domain name registration services and the data reported by them,
   c) cybersecurity incidents, events, threats and vulnerabilities,
   d) suppliers of security-relevant supplies,
   e) coordinated vulnerability disclosure,
   f) penetration tests and
   g) inspections carried out and inspection reports.

(2) In justified cases, the Agency shall provide data from the records to public authorities at their request if this is necessary for the exercise of their powers. The data provided may be used only for the purposes specified in the request. The public authority shall make reasonable efforts to ensure the information security of the data so provided.

(3) The Agency may, in justified cases, provide data from the records of the National CERT to those operating in the field of cybersecurity abroad and to those operating in the field of cybersecurity to the extent necessary to ensure the protection of cyberspace.
(4) Employees of the Agency shall be bound by a duty of confidentiality with regard to the data contained in the records referred to in paragraph 1(c) to (f). The obligation of confidentiality shall continue after the termination of the employment relationship with the Agency. The Director of the Agency may exempt the persons referred to in this paragraph from the obligation of confidentiality, specifying the scope of the data and the extent of the exemption.

§ 47
Authorisation of conformity assessment bodies under the Cybersecurity Act

(1) Where a directly applicable regulation of the European Union adopted on the basis of Regulation (EU) 2019/881 of the European Parliament and of the Council (hereinafter referred to as the "Cybersecurity Act") lays down specific or additional requirements for conformity assessment bodies to ensure their technical competence to assess cybersecurity requirements, the Agency shall, in accordance with Article 58(7)(e) of the Cybersecurity Act, decide on applications for authorisation of a conformity assessment body; this shall also apply to the procedure referred to in paragraph 3.
(2) The conformity assessment body shall demonstrate in the application for authorisation under paragraph 1 compliance with the specific or additional requirements set out in a directly applicable European Union legal act issued on the basis of the Cybersecurity Act.
(3) The Agency shall decide on the suspension, limitation or withdrawal of the authorisation if the authorised conformity assessment body violates the requirements of the Cybersecurity Act or a directly applicable regulation of the European Union adopted on the basis of the Cybersecurity Act.
(4) In the decision to suspend the authorisation pursuant to paragraph 3, the Agency shall set a time limit for remedial action. If the conformity assessment body remedies the situation, it shall inform the Agency without undue delay. If the Agency finds that the remedy is sufficient, it shall revoke the decision to suspend the authorisation. If the authorised conformity assessment body fails to remedy the situation within the time limit set, the Agency shall decide to restrict or withdraw the authorisation.
(5) The Agency shall decide on the application for authorisation pursuant to paragraph 1 within 120 days of the initiation of the proceedings, or in exceptional cases within 180 days.

§ 48
National Coordination Centre for Cybersecurity Research and Development

(1) The Agency, as the National Coordination Centre for Research and Development in the field of cybersecurity, assesses the eligibility of an applicant for registration as a member

of the Cybersecurity Community of Competence[18] (hereinafter referred to as the "Community") in accordance with the directly applicable European Union legal act[19].

(2) Only an applicant for registration of membership in the Community who provides evidence to the Agency of
   a) the basic eligibility; and
   b) the special eligibility.

(3) The application for registration of membership in the Community shall be submitted electronically using the form published on the website of the Agency.

(4) An applicant for registration as a member of the community shall provide in the application referred to in paragraph 3 the true and complete information necessary for the assessment of his basic and special eligibility by the Agency. During the period of membership of the community, the member of the community shall report any change in those data or in the facts relevant for the assessment of basic and specific eligibility within 30 days from the date on which the change or the fact occurred.

§ 49
Basic eligibility

(1) Basic eligibility shall be fulfilled by a person who
   a) has its registered office in the Czech Republic,
   b) is not on the national sanctions list[20], or the Czech Republic does not apply international sanctions against it under a directly applicable regulation of the European Union or under a legal regulation governing the implementation of international sanctions,
   c) has a clean criminal record; a person shall be deemed to have a clean criminal records if he/she has not been convicted by a court of law of a criminal offence, the facts of which are related to his/her business, or of an economic offence, an offence against property, a generally dangerous offence, an offence against the Czech Republic, a foreign state and an international organisation, an offence against public order, an offence against humanity, an offence against peace and a war crime, unless they are regarded as if they had not been convicted; where the applicant for registration of membership of a community or a member of a community is a legal person, the condition of having clean criminal record must be fulfilled by that legal person and by each member of its statutory body; where the applicant's statutory body is a legal person, the condition of good character must be fulfilled by
      1. this legal entity,
      2. each member of the statutory body of that legal person,
      3. a person representing that legal person on the statutory body of the community registrant or community member,

[18] Article 8 of Regulation (EU) 2021/887 of the European Parliament and of the Council of 20 May 2021.

[19] Article 8(4) of Regulation (EU) 2021/887 of the European Parliament and of the Council of 20 May 2021.

[20] Act No. 1/2023 Coll., on restrictive measures against certain serious conduct in international relations (Sanctions Act).

d) has no arrears registered in the Czech Republic, with the exception of arrears for which it is permitted to postpone their payment or to spread their payment into instalments,
   1. with the authorities of the Financial Administration of the Czech Republic,
   2. with the authorities of the Customs Administration of the Czech Republic,
   3. on insurance payments and penalties for public health insurance, and
   4. on insurance payments and penalties for social security and state employment policy contributions,

e) is not in liquidation[21)], has not been the subject of an insolvency proceedings and has not been placed under receivership under any other legal provision[22)].

(2) Basic eligibility shall not be fulfilled by a person who

a) has a beneficial owner and it has not been possible to ascertain the details of its beneficial owner from a full statement of valid data and data which have been deleted without replacement, or with replacement by new data, under the legislation governing the registration of beneficial owners (hereinafter referred to as the 'beneficial owner') from the register of beneficial owners under the same legislation[23)] (hereinafter referred to as the 'register of beneficial owners'), or,

b) has a beneficial owner who is registered on the national sanctions list[20)] or is subject to international sanctions by the Czech Republic pursuant to a directly applicable European Union regulation or pursuant to a legal regulation governing the implementation of international sanctions.

(3) Furthermore, the basic eligibility shall not be fulfilled by a person whose supplies been subject to conditions set by the Agency in a measure of a general nature pursuant to § 29(1) or whose supplies has been prohibited by a measure of a general nature pursuant to § 29(1).

(4) The clean criminal record referred to in paragraph (c) shall be evidenced by an extract from the criminal record and by a document proving that the condition of clean criminal records has been met, issued by the State in which the natural person has resided continuously for more than 3 months in the last 5 years or the legal person has carried on business for at least 3 months in the last 5 years, in particular by an extract from the criminal record or an equivalent document issued by a competent judicial or administrative authority of that State, or by an extract from the criminal record in the annex to which this information is contained, or by an affidavit if the foreign State does not issue an extract or document pursuant to this paragraph. The extract from the criminal record and other documents proving clean criminal record must not be older than 3 months. For the purpose of proving clean criminal record, the Agency shall request, in accordance with the legal regulation governing the registration of natural and legal persons who have been finally convicted by the courts in criminal proceedings, an extract from the criminal record. The application for an extract from the criminal record and the extract from the criminal record shall be submitted in electronic form in a manner allowing remote access.

[21)] § 187 of Act No. 89/2012 Coll., the Civil Code, as amended.

[22)] For example, Act No. 21/1992 Coll., on Banks, as amended, Act No. 87/1995 Coll., on Savings and Credit Cooperatives and Certain Related Measures and on Supplementing Act No. 586/1992 Coll., on Income Taxes, as amended, Act No. 363/1999 Coll., on Insurance and on Amendments to Certain Related Acts (Insurance Act), as amended.

[23] Act No. 37/2021 Coll., on the registration of beneficial owners, as amended.

(5) The basic eligibility shall be evidenced by
   a) by submitting a confirmation statement from the competent health insurance institution in the case of paragraph 1(d)(3) and the competent district social security administration in the case of paragraph 1(d)(4), which must not be older than 30 days,
   b) an affidavit that the community registrant or community member is not insolvent in the case of paragraph 1(e), unless insolvency proceedings are pending against him or her; and
   c) an extract from a foreign register similar to the register of beneficial owners, which must not be older than 30 days, if the beneficial owner of the applicant for registration of community membership or community member is a person established in the territory of a Member State of the European Union or a Member State of the European Free Trade Association.

§ 50
Special eligibility

Special eligibility is fulfilled by those who are eligible for membership of the community under a directly applicable European Union regulation[24)].

§ 51
Assessing the eligibility of a community membership applicant

(1) If the applicant for the registration of the Community membership fulfils the conditions of basic and specific eligibility pursuant to § 49 and § 50, the Agency shall refer the applicant's application to the registering authority pursuant to the directly applicable legal act of the European Union[17)] (hereinafter referred to as the "Registering Authority").
(2) The Agency shall initiate proceedings for the ineligibility of an applicant for community membership registration if the applicant for community membership registration does not meet the conditions of basic and special eligibility under § 49 and § 50.
(3) The Agency will issue a decision on the ineligibility of the applicant for community membership registration. If it is proved that the applicant has the basic and special eligibility for membership of the community in accordance with § 49 and 50, the Agency shall discontinue the ineligibility proceedings.
(4) When the decision on the ineligibility of the applicant for registration of community membership issued in the proceedings under paragraph 2 comes into force, the Agency shall forward the application of the applicant for registration of community membership to the Registering Authority and at the same time notify the Registering Authority of the ineligibility of the applicant for registration of community membership.

[24)] Article 8(3) of Regulation (EU) 2021/887 of the European Parliament and of the Council of 20 May 2021.

§ 52
Status of the Community membership

(1) The Agency shall continuously assess the fulfilment of the conditions of basic and special eligibility of a member of the community in accordance with § 49 and § 50 throughout the duration of his/her membership in the community.
(2) In the event that a community member ceases to meet the basic and special eligibility requirements under § 49 and § 50, the Agency shall initiate proceedings to determine his or her ineligibility for continued membership in the community.
(3) The Agency shall issue a decision on the ineligibility of the community member for continued membership. If it is established that the community member continues to fulfil the basic and special eligibility requirements under § 49 and § 50, the Agency shall discontinue the proceedings.
(4) When the decision on the ineligibility of a community member for continued membership of the community issued in proceedings under paragraph 2 comes into force, the Agency shall notify the Registering Authority of the ineligibility of the community member for continued membership of the community.

§ 53
Public contract with the operator of the National CERT

(1) The Agency shall conclude a public law contract with a legal entity selected in accordance with the procedure under § 163(4) of the Administrative Procedure Code for the purpose of cooperation in the field of cybersecurity and the provision of activities under § 43(1) (hereinafter referred to as the "public law contract"). Application selection procedure shall be announced by the Agency.
(2) The public law contract shall contain at least
   a) designation of the contracting parties,
   b) definition of the subject matter of the contract,
   c) the rights and obligations of the parties,
   d) the terms of cooperation between the Parties,
   e) the manner and conditions of withdrawal of the parties from the public contract,
   f) notice period and grounds for termination of the contract,
   g) the prohibition of misuse of data obtained in connection with the performance of the activities referred to in § 43(1),
   h) definition of the conditions for the performance of the activities of the National CERT pursuant to § 43(1)(h), and
   i) the method of transmission and the extent of the data to be transmitted to the Agency in the event of termination of the contract.
(3) The Agency shall publish the public law contract concluded pursuant to paragraph 1 on the Official Notice Board of the Agency, except for those parts of the public law contract which cannot be published under any other legal regulation.
(4) In the absence of a public law contract pursuant to paragraph 1, or in the event of termination of the obligation, the activities of the National CERT shall be carried out by the Agency.

§ 54
Mutual cooperation with the Member States of the European Union

(1) The Agency shall cooperate in the application of this Act with the competent authorities of other Member State, and in particular it may provide and request assistance in the form of
   a) information sharing,
   b) carrying out inspections or other actions against the provider of the regulated service; or
   c) coordination of inspections of regulated service providers providing regulated services in more than one Member State, including the possibility of inviting representatives of the competent authorities of another Member State to participate in the inspection.

(2) The Agency may only refuse a request for cooperation
   a) it is not the competent authority or does not have the authority to carry out the requested action,
   b) if the request for assistance is manifestly disproportionate in relation to the capacity of the Agency; or
   c) if the request concerns information or involves activities which, if disclosed or carried out, would be contrary to the essential interests of the Czech Republic in the field of national security, public security or defence.

(3) Where a provider of a regulated service which has its main establishment in another Member State provides within the Czech Republic a service referred to in § 18(1), with the exception of a trust service pursuant to a directly applicable regulation of the European Union[8)], the Agency may, in relation to the provision of that regulated service, carry out an inspection or other act in respect of that person only on the basis of and to the extent of a request for cooperation from the other Member State in which the provider of the regulated service has its main establishment.

(4) Where assets used for the provision of any of the services referred to in § 18(1), with the exception of a trust service pursuant to a directly applicable regulation of the European Union[8)], are located within the Czech Republic, but the provider of the regulated service has its main establishment in another Member State, the Agency shall be entitled to carry out an inspection or other act in relation to those assets used for the provision of those services on the basis of and to the extent of a request for cooperation from the other Member State in which the provider of the regulated service has its main establishment.

(5) The location of the main establishment shall mean the place in a Member State of the European Union or a Contracting State to the Agreement on the European Economic Area where the person providing the services referred to in paragraph 3 predominantly takes decisions relating to cybersecurity risk management, in particular the registered office of the company. Where such a place cannot be determined in accordance with the first sentence, or where such decisions are not taken in a Member State of the European Union or a Contracting State to the Agreement on the European Economic Area, the main establishment shall be deemed to be located in the Member State of the European Union where the actual acts leading to the provision of cybersecurity are carried out. Where such a place cannot be determined in accordance with the first and second sentences, the main establishment shall be deemed to be located in a Member State of the European Union or a

Contracting State to the Agreement on the European Economic Area where the person has the establishment with the largest number of employees.

(6) The provisions of paragraph 3 shall also apply to an entity providing a domain name registration service within the Czech Republic.

TITLE VI
Inspection by the Agency, corrective and other measures, offences and penalties

§ 55
Inspection by the Agency

(1) The Agency carries out inspections in the field of cybersecurity. When carrying out an inspection, the Agency shall ascertain how the obligations laid down by or on the basis of this Act and directly applicable European Union regulations in the field of cybersecurity are fulfilled.

§ 56
Corrective measures

(1) If the Agency finds that a provider of regulated service or another person does not fulfil the obligations set out in this Act or on the basis of this Act, it may order them to remedy the identified deficiencies within a specified period of time or specify how. In the decision, the Agency may impose an obligation to notify the Agency of the implementation of the corrective measure and its result within a specified period of time.

(2) The decision referred to in paragraph 1 may be the first act in the proceedings and an appeal against it shall not have suspensive effect.

§ 57
Suspension of certification

(1) The Agency may, in the event of non-compliance with the obligation to remedy the identified deficiencies imposed by a decision of the Agency pursuant to § 56(1) to a provider of regulated service under the higher obligations regime who holds a European cybersecurity certificate under the Cybersecurity Act or another certificate or certificate related to ensuring cybersecurity of the regulated service, suspend the validity of the European cybersecurity certificate issued by the Agency or impose on the conformity assessment body the obligation to suspend the validity of the certificate or certificate issued by the Agency until the identified deficiencies have been remedied, for a period of at least 6 months.

(2) A decision of the Agency under paragraph 1 may be the first act in the proceedings and the appeal against it shall not have suspensory effect.

(3) The Agency shall publish information on the suspension of the validity of a certificate or certification on its website.

(4) The Agency shall issue a certificate of compliance with the obligation to remedy the identified deficiencies, which shall be the basis for the renewal of the certificate or certification, if it finds that the deficiencies have been remedied, but not before the expiry of the period referred to in paragraph 1.

§ 58
Suspension of the exercise of management functions

(1) The Agency may prohibit a member of the statutory body who, in direct connection with the implementation of a decision of the Agency pursuant to § 56(1) imposing an obligation on a provider of regulated service under the higher obligations regime to remedy identified deficiencies, has repeatedly or seriously violated his/her duties in the performance of his/her function, as a result of which the proper implementation of the decision of the Agency has been thwarted, from exercising that function until the identified deficiencies have been remedied, for a period of at least 6 months.
(2) The decision referred to in paragraph 1 may be issued only in respect of a person exercising the function of a member of the statutory body of regulated service provider under the higher obligations regime, and only in relation to a function which is not a public function defined by a term of office or a period of time and occupied on the basis of direct or indirect election or by appointment pursuant to another legal regulation.
(3) The Agency shall issue a decision lifting the ban on the exercise of the function if it finds that the deficiencies have been remedied, but not before the expiry of the period referred to in paragraph 1.
(4) The Agency shall without undue delay send the final decision on the prohibition to perform the function or on its revocation to the court that maintains the commercial register pursuant to another legal regulation; the Agency shall also publish information on such decisions on its website. The entry of information on the suspension of the exercise of management functions in the Commercial Register shall be similar to the entry of information that a member of the statutory body has been suspended from exercising his function under the law governing companies and cooperatives.
(5) If a legal person is a member of the statutory body, this provision shall also apply to the natural person who represents that legal person in the performance of its functions.
(6) A decision under paragraphs 1 and 3 may be the first act in the proceedings and an appeal against it shall not have suspensive effect.

§ 59
Offences by a provider of regulated services

(1) A provider of regulated service under the higher obligations regime commits an offence by failing to
   a) notify the Agency of changes to the regulated service pursuant to § 9(1),
   b) report contact details or supplementary data or changes thereto to the Agency pursuant to § 11,

c) identify, for the purpose of defining the defined scope, all primary assets pursuant to § 12(2)(a) or supporting assets pursuant to § 12(2)(c), or by failing to review or update their defined scope on a regular basis pursuant to § 12(5),
d) assess, for the purpose of defining the defined scope, whether the primary assets identified pursuant to § 12(2)(a) are related to the provision of the regulated service or fails to review or update that assessment on a regular basis pursuant to § 12(5),
e) record assets pursuant to § 12(3),
f) introduce or implement security measures pursuant to § 13(2) or § 18(1),
g) select their supplier in accordance with the requirements arising from the security measures or failing to include the requirements arising from the security measures in the contracts with the supplier in breach of § 13(5)
h) submit an initial incident report pursuant to § 16(1) or failing to complete any of the incident data pursuant to § 16(3) or failing to report cybersecurity incident pursuant to § 18(2),
i) provide information or cooperation in the management of an incident pursuant to with § 17(3),
j) comply with the obligation or prohibition to inform users of the regulated service about a cybersecurity incident with a significant impact as set out in the decision of the Agency pursuant to § 19(1),
k) comply with the obligation to inform the user of regulated service of a significant threat and the steps that the user of the service may take in response to it pursuant to § 19(2),
l) comply with the obligation imposed by an alert decision pursuant to § 21(1),
m) comply with a reactive countermeasure imposed pursuant to § 23(1) or § 23(4),
n) notify an implementation of a countermeasure and its outcome pursuant to § 23(6),
o) comply with an obligation imposed by a corrective measure pursuant to § 56(1).

(2) A provider of regulated service under the lower obligations regime commits an offence by failing to
a) notify the Agency of changes to the regulated service pursuant to § 9(1),
b) report contact details or supplementary data or changes thereto to the Agency pursuant to § 11,
c) identify, for the purpose of defining the defined scope, all primary assets pursuant to § 12(2)(a) or supporting assets pursuant to § 12(2)(c), or by failing to review or update their defined scope on a regular basis pursuant to § 12(5),
d) assess, for the purpose of defining the defined scope, whether the primary assets identified pursuant to § 12(2)(a) are related to the provision of the regulated service or fails to review or update that assessment on a regular basis pursuant to § 12(5),
e) record assets pursuant to § 12(3),
f) introduce or implement security measures pursuant to § 13(2) or § 18(1),
g) select their supplier in accordance with the requirements arising from the security measures or failing to include the requirements arising from the security measures in the contracts with the supplier in breach of § 13(5)
h) submit an initial incident report pursuant to § 16(1) or failing to complete any of the incident data pursuant to § 16(3) or failing to report cybersecurity incident pursuant to § 18(2),

i) provide information or cooperation in the management of an incident in pursuant to with § 17(3),
j) comply with the obligation or prohibition to inform users of the regulated service about a cybersecurity incident with a significant impact as set out in the decision of the Agency pursuant to § 19(1),
k) comply with the obligation to inform the user of regulated service of a significant threat and the steps that the user of the service may take in response to it pursuant to § 19(2),
l) comply with the obligation imposed by an alert decision pursuant to § 21(1),
m) comply with a reactive countermeasure imposed pursuant to § 23(1) or § 23(4),
n) notify an implementation of a countermeasure and its outcome pursuant to § 23(6),
o) comply with an obligation imposed by a corrective measure pursuant to § 56(1).

(3) Furthermore, a provider of regulated service commits an offence as a provider of strategically important service by failing to
a) notify the Agency of changes to the regulated service pursuant to § 26(1),
b) comply with a condition or prohibition imposed by the Agency in a measure of a general nature pursuant to § 29,
c) obtain information about the supplier of a security-significant delivery pursuant to § 31(1)(a),
d) record information about the supplier of a security-significant delivery pursuant to § 31(1)(a),
e) notify the Agency of information about the supplier of a security-significant delivery or a change thereof pursuant to § 31(1)(c),
f) ensure the availability of a strategically important service from the territory of the Czech Republic within the specified time and quality pursuant to § 33(1), or
g) test the ability to ensure the provision of a strategically important service as referred to in § 33(2) or to keep a record thereof,
h) specify the time and quality of availability of a strategically important service from the territory of the Czech Republic or to keep a record of this pursuant to § 33(5).

(4) The offence is punishable by a fine of up to
a) 250 000 000 CZK or up to 2 % of the annual worldwide net turnover of the undertaking, pursuant to Articles 101 and 102 of the Treaty on the Functioning of the European Union, of which the defendant is a member for the immediately preceding financial year, whichever is the higher, in case of an offence under paragraph 1(a), (c) to (m) and (o) or paragraph 3(a), (b), (f) or (g),
b) 175 000 000 CZK or up to 1,4 % of the annual worldwide net turnover of the undertaking, pursuant to Articles 101 and 102 of the Treaty on the Functioning of the European Union, of which the defendant is a member for the immediately preceding financial year, whichever is the higher, in case of an offence under paragraph 2(a), (c) to (m) and (o),
c) 100 000 000 CZK in case of an offence under paragraph 1(b) or paragraph 3(c), (d) or (h)
d) 50 000 000 CZK in case of an offence under paragraph 1(n), paragraph 2(b) or paragraph 3(e), or
e) 35 000 000 CZK in case of an offence under paragraph 2(n).

§ 60
Offences by other persons in the field of cybersecurity

(1) A person commits an offence by failing to
   a) fulfil the obligation to notify the service to the Agency pursuant to the § 6(1),
   b) provide information or cooperation in the management of an incident in accordance with § 17(3),
   c) provide the necessary cooperation to the Agency in gathering information for issuing countermeasures pursuant to § 20(2),
   d) comply with an obligation imposed by a decision pursuant to § 24(1),
   e) provide the necessary cooperation following a request from the Agency pursuant to § 28(4),
   f) comply with the obligation to implement measures, in connection with the state of cyber emergency, to address a significant threat or breach of information security in cyberspace imposed by a decision or a measure of a general nature pursuant to § 39,
   g) comply with an obligation imposed by a corrective measure pursuant to § 56(1),
   h) comply with the decision on the suspension of the exercise of the management functions pursuant to § 58, or
   i) provide information or other cooperation necessary to assess compliance with the conditions referred to in § 64(2).

(2) A natural person commits an offence by breaching the obligation of confidentiality under § 46(4).

(3) A person providing domain name registration services commits an offence by failing to
   a) report to the Agency the data referred to in § 34(1) or a change thereof pursuant to § 34(2),
   b) collect or maintain accurate and complete domain name registration data in the dedicated database referred to in § 35(1) in accordance with the requirements of § 35(2),
   c) implement or publish policies and procedures to ensure the accuracy and completeness of the information held in the database, including the verification procedures referred to in Article 36(3),
   d) without undue delay after the registration of the domain name, fails to publish its registration data, which are not personal data of the domain name holder, in accordance with § 35(5); or
   e) provide access to specific domain name registration data pursuant to § 35(6).

(4) A person administering and operating Top Level Domain (TLD) registry commits an offence by failing to
   a) collect or maintain accurate and complete domain name registration data in the dedicated database referred to in § 35(1) in accordance with the requirements of § 35(2),
   b) implement or publish policies and procedures to ensure the accuracy and completeness of the information held in the database, including the verification procedures referred to in Article 35(3),

c) publish, without undue delay after the registration of the domain name, its registration data, which are not personal data of the domain name holder, in accordance with § 35(5); or
d) provide access to specific domain name registration data pursuant to § 35(6).

(5) An applicant for registration as a member of the community commits an offence by making false or misleading statements in an application for registration under § 48(4), or by omitting information which may be relevant to the assessment of his basic and specific eligibility by the Agency.

(6) A member of the community commits an offence by failing to disclose, during the period of membership of the community under § 48(4), a change in the information required for the assessment of his basic and special eligibility by the Agency or to disclose other facts relevant to the assessment of his basic and special eligibility.

(7) The offence is punishable by a fine of up to
a) 250 000 000 CZK or up to 2 % of the annual worldwide net turnover of the undertaking, pursuant to Articles 101 and 102 of the Treaty on the Functioning of the European Union, of which the defendant is a member for the immediately preceding financial year, whichever is the higher, in case of an offence under paragraph 1(a) or (d),
b) 100 000 000 CZK in case of an offence under paragraph 1(f),
c) 50 000 000 CZK in case of an offence under paragraph 1(b), (c), (e), (g) or (i), paragraph 3 or paragraph 3,
d) 20 000 000 CZK in case of an offence under paragraph 1(h),
e) 2 000 000 CZK in case of an offence under paragraph 5 or paragraph 6, or
f) 50 000 CZK in case of an offence under paragraph 2.

§ 61
Offences in the field of cybersecurity certifications

(1) A legal or natural person commits an offence by
a) misusing the mark or designation of a European cybersecurity certification scheme, a European cybersecurity certificate, an EU declaration of conformity or any other document under the Cybersecurity Act,
b) forging or altering a European Cybersecurity Certificate, EU Declaration of Conformity or other document under the Cybersecurity Act,
c) performing a compliance assessment activity under the Cybersecurity Act to the level of assurance 'high', although it is not authorised to do so under Article 56(6) of the Cybersecurity Act,
d) as a conformity assessment body authorised under Article 60(3) of the Cybersecurity Act, issue a European cybersecurity certificate for a product, process or service that does not meet the criteria contained in a directly applicable European Union legal act issued on the basis of the Cybersecurity Act,
e) carrying out, without authorisation, a conformity assessment activity reserved to an authorised conformity assessment body by a directly applicable legal act of the European Union issued on the basis of the Cybersecurity Act,

f) acting as an accredited conformity assessment body without accreditation under Article 60(1) of the Cybersecurity Act or outside the scope of that accreditation; or
g) as a conformity assessment body, failing to comply with the obligation imposed by the Agency to suspend the validity of a certificate or attestation issued by it pursuant to § 57(1).

(2) The holder of a European Cybersecurity Certificate commits an offence by failing to inform the relevant conformity assessment bodies of any vulnerabilities or irregularities subsequently identified.

(3) A manufacturer or provider of products, services or processes issuing an EU declaration of conformity commits an offence by
a) issuing an EU declaration of conformity even though the conditions laid down in the Cybersecurity Act are not met,
b) not keeping documents and information as referred to in Article 53(3) of the Cybersecurity Act,
c) failing to submit a copy of the EU Declaration of Conformity to the Agency and ENISA in accordance with Article 53(3) of the Cybersecurity Act; or
d) not providing cybersecurity information to the extent and in the manner specified in Article 55 of the Cybersecurity Act.

(4) The offence is punishable by a fine of up to
a) CZK 50 000 000 in case of an offence under paragraph 1(a) to (e),
b) CZK 20 000 000 in case of an offence under paragraph 1(f) or (g) or paragraph 3(a), or
c) CZK 2 000 000 in case of an offence under paragraph 2 or paragraph 3 (b) to (d).

§ 62
Common provisions on offences

(1) Offences under this Act shall be dealt with by the Agency.

(2) The provisions of § 68(b), § 70, § 71, § 80(3), § 88(2), § 89, § 95(3) and § 96(1)(b) of the Offences Liability and Procedure Act[25)] shall not apply to the Agency's procedure under this Act.

§ 63
Relationship to the Administrative Procedure Code and Inspection Code

(1) Pursuant to § 62 of the Administrative Code, the Agency may impose a fine of up to CZK 100 000. The fine may be imposed repeatedly. The total amount of repeatedly imposed fines may not exceed CZK 10 000 000 or 1 % of the net turnover achieved by the legal entity or natural person for the last completed accounting period, whichever is higher.

(2) In order to enforce compliance with an obligation imposed by a decision of the Agency, the Agency may impose coercive fines of up to CZK 10 000 000 or 1% of the net turnover achieved by a legal entity or an entrepreneurial natural person for the last completed accounting period, whichever is higher.

[25)] Act No. 250/2016 Coll., on Liability for Offences and Proceedings Thereon, as amended.

(3) A fine of up to CZK 10 000 000 may be imposed for an offence committed by a provider of a regulated service who, as a inspected person, fails to fulfil any of the obligations under § 10(2) of the Inspection Code.

PART TWO
COMMON, TRANSITIONAL AND FINAL PROVISIONS

§ 64
Cooperation

(1) Public authorities are obliged to provide the Agency with the necessary cooperation to exercise its powers under this Act without undue delay. The public authorities and the Agency shall cooperate with each other in the exercise of their powers under this Act and shall be entitled to request opinions on decisions prepared within their respective areas of competence and shall endeavour to achieve a consensus of such opinions. The public authorities and the Agency shall also, to the extent necessary for the exercise of the competences of the public authorities and the Agency, share information on threats, vulnerabilities and incidents and on measures taken in response to such threats, vulnerabilities and incidents. The provisions of § 46(2) and (3) shall not be affected. The law enforcement authorities may restrict or postpone the performance of these obligations to the extent necessary or for the period necessary if the purpose of the criminal proceedings would be jeopardised or defeated by the provision of such cooperation.

(2) Anyone who may reasonably be presumed to meet the conditions for registration of a regulated service shall, without undue delay, and unless otherwise provided for in other legislation, provide the information necessary to assess fulfilment of those conditions and any other necessary cooperation without payment. The requested cooperation need not be provided if a legal or State-recognised obligation of confidentiality prevents it.

(3) The ministries, other central administrative authorities and the Czech National Bank responsible for designating critical infrastructure elements pursuant to the legal regulation governing crisis management and critical infrastructure shall inform the Agency without undue delay of the designation of critical infrastructure elements and the reasons for the designation.

(4) For the purposes of exercising its powers, the Agency may request the General Financial Directorate to provide information obtained in the course of tax administration which is necessary to establish whether the person under review meets the conditions for registration of a regulated service pursuant to § 4(1). The provision of information pursuant to this provision shall not constitute a breach of the duty of confidentiality under the Tax Code; nor shall the use of such information by the Agency pursuant to this Act constitute a breach of that duty of confidentiality.

(5) The Agency and the Agency for Personal Data Protection are mutually entitled to request information and require cooperation in order to avoid double punishment for violation of

the same obligation imposed by both this Act and the legislation governing the protection of personal data. The imposition of other penalties under this Act is not affected.

(6) For the purposes of exercising the powers of the Agency under this Act, the Ministry of Justice shall enable the Agency to obtain, in a manner allowing remote access, from the register of beneficial owners a full extract of valid data and data that have been deleted without replacement or with replacement with new data pursuant to the legal regulation governing the registration of beneficial owners[23)].

§ 65
Information obligation of the Agency

(1) The shall Agency for the purpose of fulfilling its information obligation
   a) inform the European Commission and the Cooperation Group every 2 years of the number of regulated service providers meeting the conditions for regulated service registration under § 4(1) in each sector,
   b) inform the European Commission every 2 years of the number of regulated service providers meeting the conditions for registration of a regulated service under § 5(1) in each sector, the services they provide and the conditions for which they have been registered,
   c) submit to the European Union Agency for Cybersecurity every 3 months a summary report including anonymised and aggregated data on cybersecurity incidents, threats and significant cybersecurity events reported under § 15,
   d) provide the European Union Agency for Cybersecurity with identification data on persons providing domain name registration services and providers of regulated services referred to in § 54(3) who have their main establishment in the Czech Republic or who have an appointed representative in the Czech Republic,
   e) provide the European Union Agency for Cybersecurity with information for coordinated vulnerability disclosure,
   f) inform the European Commission of the adoption of the national cybersecurity strategy and, to the extent that the security interests of the Czech Republic are not jeopardised, of the content of the strategy,
   g) communicate to the European Commission the identification details of the authority responsible for cybersecurity oversight, the single point of contact for cross-border cybersecurity cooperation within the European Union, the cyber crisis management authority, the CSIRT, and the coordinator designated for the purposes of coordinated vulnerability disclosure,
   h) provide the European Commission and the European Union Agency for Cybersecurity with additional information and necessary cooperation.

(2) For the purpose of fulfilling the information obligation under paragraph 1, the Agency shall not provide information the disclosure of which would be contrary to the essential interests of the Member States of the European Union or the Contracting States to the Agreement on the European Economic Area in the field of national security, public security or defence. Information which is confidential under European Union or national rules, such as rules on the confidentiality of commercial information, shall be exchanged with the European

Commission and other competent authorities of the European Union only to the extent necessary in view of the purpose of the exchange. The exchange of information shall preserve the confidentiality of the information in question and protect the security and commercial interests of the person concerned.

§ 66
Protection of information

(1) Parts of documents and records containing classified information or information the disclosure of which could jeopardise the provision of cybersecurity, measures of a general nature pursuant to § 29 or defeat the purpose of criminal proceedings shall be kept separately outside the file by the Agency in proceedings pursuant to § 21 to § 23, § 29 and § 30.

(2) In judicial proceedings concerning a decision or measure of a general nature issued in proceedings pursuant to § 21 to § 23, § 29 and § 30, the Chairman of the Trial Chamber shall decide that the party to the proceedings shall be given access, to the extent necessary, to parts of documents and records kept separately outside the file, provided that his sovereignty cannot be compromised thereby, the territorial integrity, democratic foundations, security, internal order, life and health, the activities of the intelligence services or the Police of the Czech Republic, to jeopardise the ensuring of cybersecurity, measures of a general nature pursuant to § 29 or to jeopardise the purpose of the criminal proceedings. Before making a decision concerning classified information or unclassified information, the disclosure of which could defeat the jeopardise of criminal proceedings, the Chairman of the Trial Chamber shall request the opinion of the authority which provided the information; before making a decision concerning other information pursuant to paragraph 1, the Chairman of the Trial Chamber shall request the opinion of the Agency.

(3) The discussion of the information referred to in paragraph 1 shall be conducted in such a way that the duty of confidentiality of that information is respected, provided that the Chairman of the Trial Chamber shall decide on the scope of the persons who will take part in the discussion of that information. Evidence may be taken by way of questioning in respect of those circumstances only if the person under an obligation of confidentiality has been released from that obligation by the competent authority. Confidentiality may not be waived where the activities of the intelligence services or the Police of the Czech Republic could be jeopardised or seriously disrupted. A similar procedure shall also apply in cases where evidence is taken otherwise than by questioning.

(4) The authority which has provided classified information shall identify the circumstances referred to in paragraph 3 which it claims cannot be exempted from confidentiality, and the Chairman of the Trial Chamber shall decide that the parts of the file to which those circumstances relate shall be separated if the activities of the intelligence services or the Police of the Czech Republic could otherwise be jeopardised or seriously disrupted.

§ 67
Representative for the Czech Republic

(1) A person providing domain name registration services and a regulated service provider that is a provider of a regulated service of a domain name translation system, a TLD registry management and operation service, a cloud computing service, a data centre service, a content delivery network service, an online marketplace service[9)], an internet search engine service under a directly applicable regulation of the European Union[10)], a social network platform service, a managed service or a managed security service, which provides this service in the Czech Republic, does not have its main establishment in a Member State of the European Union or a Contracting State to the Agreement on the European Economic Area and has not appointed a representative in another Member State, shall be obliged to appoint a representative in the Czech Republic. A representative shall be a person established in the Czech Republic who has been authorised by a person providing domain name registration services or a provider of one of the regulated services listed above to represent them in relation to the obligations under this Act.

(2) Where an entity providing domain name registration services or a provider of any of the regulated services referred to in paragraph 1 has its main establishment outside the European Union or a Contracting State to the Agreement on the European Economic Area and has established a representative in the Czech Republic, it shall be deemed to be established in the Czech Republic and subject to the obligations under this Act. This shall also apply where the person providing domain name registration services or the provider of any of the regulated services referred to in paragraph 1 has its main establishment outside a Member State of the European Union or a Contracting State to the Agreement on the European Economic Area and has not appointed a representative in any Member State of the European Union or a Contracting State to the Agreement on the European Economic Area.

(3) The appointment of a representative shall be without prejudice to the responsibility of a regulated service provider or an entity providing domain name registration services for compliance with this Act.

§ 68
Funding in the state of cyber emergency

Funding with regards to the state of the cyber emergency for the current fiscal year shall be made in accordance with the legal regulation governing budgetary rules[26)]. For this purpose

a) the Agency shall allocate in its chapter budget for the relevant year the amount of financial resources necessary to ensure preparation for a state of cyber emergency; and shall allocate in its budget for the relevant year a dedicated reserve of funds for dealing with the state of cyber emergency and its consequences; and

[26] Act No. 218/2000 Coll., on Budget Rules and on Amendments to Certain Related Acts (Budget Rules), as amended.

b) the financial resources required to ensure preparation for the state of cyber emergency and the elimination of the consequences of a threat to the security of the Czech Republic, internal order, life, health, property values or the environment allocated by the Agency in the budget of its chapter are considered a binding indicator of the state budget for the relevant year.

§ 69
Intelligence services

(1) Intelligence services[27] are not regulated service providers.
(2) Intelligence services
   a) report contact details and changes thereto to the Agency,
   b) adequately implement the security measures referred to in § 13 and § 14(1) of this Act; and
   c) take reasonable account of the warning under § 22, unless the Agency or other legislation provides otherwise.
(3) Provisions of § 17(3), § 39 and § 55 to § 63 shall not apply to intelligence services.
(4) The provisions of § 28(2) and § 64(1) shall apply in the case of intelligence services, unless the performance of these duties is prevented by special legislation[28] or by a statutory or state-recognised obligation of confidentiality. The transmission of information by the intelligence services shall always be governed by the Intelligence Services Act[29]. Military intelligence may also transmit information in the manner provided for in the Military Intelligence Act.[30]

§ 70
Relationship to sectoral legislation of the European Union

(1) If a directly applicable regulation of the European Union or another legal regulation that incorporates the relevant regulation of the European Union provides for obligations in the area of establishing and implementing security measures or reporting cybersecurity incidents and these obligations have at least comparable effect to the obligations under this Act, the provisions of this Act governing the obligations to establish and implement security measures and report cybersecurity incidents shall not apply, including the provisions on supervision of compliance with those obligations.
(2) Provisions having comparable effect to the obligations contained in this Act pursuant to paragraph 1 shall be deemed to be those provisions of a directly applicable European Union regulation or other legislation transposing the relevant European Union regulation which
   a) in relation to the obligation to introduce and implement security measures, comply at least with the requirements set out in §s 13 and 14, or

[27] § 3 of Act No. 153/1994 Coll., on the Intelligence Services of the Czech Republic, as amended.
[28] For example, Act No. 153/1994 Coll., on the Intelligence Services of the Czech Republic, as amended.
[29] § 8(3) of Act No. 153/1994 Coll., on the Intelligence Services of the Czech Republic, as amended
[30] § 16b(1) or § 16f(2) of Act No 289/2005 on Military Intelligence, as amended.

b) in relation to the obligation to report cybersecurity incidents, comply at least with the requirements set out in § 15 and 16.

(3) In addition, such provisions of a directly applicable European Union legal act shall be deemed to have comparable effect to the obligations contained in this Act pursuant to paragraph 1 as the directly applicable European Union legal act itself so provides.

§ 71
Transitional provisions

(1) Administrators of essential service information systems, administrators of information and communication systems of critical information infrastructure, administrators of significant information systems or digital service providers pursuant to § 3 of Act No. 181/2014 Coll., as in force before the date of entry into force of this Act, whose services meet the conditions for the registration of a regulated service pursuant to § 4(1), shall comply with, for services and information systems regulated pursuant to existing legislation, to the extent that such services and assets are regulated by this Act, at least

a) obligations related to the introduction and implementation of security measures, reporting of cybersecurity incidents and compliance with the measures of the Agency pursuant to Act No. 181/2014 Coll., as amended, in the event that it is a provider of a regulated service under the regime of higher obligations under this Act; or

b) obligations related to the introduction and implementation of security measures, reporting of cybersecurity incidents and compliance with the measures of the Agency pursuant to Act No. 181/2014 Coll., as amended, within the scope of the duties imposed by this Act to the providers of regulated services under the regime of lower obligations in the event that it is a provider of a regulated service under the regime of lower obligations under this Act,

starting from the date of entry into force of this Act until the expiry of the deadlines for commencing compliance with the obligations under this Act, with the exception of the method of reporting cybersecurity incidents, which these regulated service providers are obliged to fulfil under this Act from the date of delivery of the decision on registration of the regulated service.

(2) In proceedings relating to the fulfilment of an obligation imposed before the date of entry into force of this Act by or on the basis of Act No. 181/2014 Coll., as amended, the procedure shall be in accordance with Act No. 181/2014 Coll., as amended.

(3) Warnings issued before the date of entry into force of this Act pursuant to 181/2014 Coll., as amended, shall be deemed to be warnings issued pursuant to this Act.

(4) Reactive measures and protective measures issued before the date of entry into force of this Act pursuant to Act No. 181/2014 Coll., as amended, shall be deemed to be reactive countermeasures issued pursuant to this Act.

(5) Public law contracts concluded pursuant to Act No. 181/2014 Coll., as amended, shall expire upon the expiration of 1 year from the date of entry into force of this Act.

(6) In the event that a National CERT provider does not, on the effective date of this Act, hold a valid business certificate for access to classified information at the Confidential classification level pursuant to the Classified Information Protection and Security Clearance

Act, the provider shall apply for such a certificate without undue delay and provide evidence of this fact to the Agency. The operator of the National CERT must submit the certificate referred to in the first sentence to the Agency without undue delay, but no later than 1 year after the date of entry into force of this Act.

§ 72
Repeal provisions

The following are repealed:

1. Act No. 181/2014 Coll., on Cybersecurity and on Amendments to Related Acts (Act on Cybersecurity).
2. Decree No. 317/2014 Coll., on significant information systems and their determining criteria.
3. Decree No. 205/2016 Coll., amending Decree No. 317/2014 Coll., on significant information systems and their determining criteria.
4. Part Two of Act No. 104/2017 Coll., amending Act No. 365/2000 Coll., on public administration information systems and amending certain other acts, as amended, Act No. 181/2014 Coll., on cybersecurity and amending related acts (Act on Cybersecurity), and certain other acts.
5. Part two hundred and twenty-ninth of Act No. 183/2017 Coll., amending certain acts in connection with the adoption of the Act on Liability for Offences and Proceedings thereon and the Act on Certain Offences.
6. Part One of Act No. 205/2017 Coll., amending Act No. 181/2014 Coll., on Cybersecurity and on Amendments to Related Acts (Act on Cybersecurity), as amended by Act No. 104/2017 Coll., and certain other acts.
7. Decree No. 437/2017 Coll., on the criteria for determining the operator of essential service.
8. Part Six of Act No. 35/2018 Coll., amending certain acts regulating the number of members of special control bodies of the Chamber of Deputies.
9. Decree No. 82/2018 Coll., on security measures, cybersecurity incidents, reactive measures, filing requirements in the field of cybersecurity and data disposal (Cybersecurity Decree).
10. Part thirty-second of Act No. 111/2019 Coll., amending certain acts in connection with the adoption of the Personal Data Processing Act.
11. Part Nine of Act No. 12/2020 Coll., on the Right to Digital Services and on Amendments to Certain Acts.
12. Decree No. 360/2020 Coll., amending Decree No. 317/2014 Coll., on significant information systems and their determining criteria, as amended by Decree No. 205/2016 Coll.
13. Decree No. 573/2020 Coll., amending Decree No. 437/2017 Coll., on criteria for determining the operator of essential service.
14. Part one hundred and fifty-third of Act No. 261/2021 Coll., amending certain acts in connection with further computerisation of procedures of public authorities.

15. Decree No. 315/2021 Coll., on security levels for the use of cloud computing by public authorities.
16. Act No. 226/2022 Coll., amending Act No. 181/2014 Coll., on cybersecurity and amending related acts (Act on cybersecurity), as amended.
17. Decree No. 190/2023 Coll., on security rules for public authorities using the services of cloud computing providers.

§ 73
Effectiveness

This Act shall enter into force on ...