Government proposal

ACT

of dd.mm.yyyy,

on Cyber Security

Parliament has adopted the following Act of the Czech Republic:

PART ONE
CYBER SECURITY

TITLE I
Basic provisions

§ 1
Subject matter

(1) This Act regulates the rights and obligations of authorities and persons and the scope and powers of the National Agency for Cyber and Information Security (hereinafter referred to as "the Agency") and other public authorities in the field of cyber security.
(2) This Act incorporates the relevant European Union legislation[1]), follows up on directly applicable European Union legal acts[2]) and regulates the cyber security in the Czech Republic.
(3) This Act shall not apply to information or communication systems handling classified information.

[1)] 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).

[2)] 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.

§ 2
Definition of terms

(1) For the purposes of this Act
   a) assets mean primary assets and supporting assets relevant to the collection, handling, storage, use, sharing, dissemination or other processing of information and data in electronic form,
   b) primary assets are information and services, where information also means data, including operational data, and service also means processes,
   c) supporting assets mean employees, suppliers, facilities and technical assets,
   d) technical asset means technical and software resources and equipment, where technical and software resources and equipment also includes communications equipment, electronic communications networks and industrial, control or other similar specific assets,
   e) regulated service is a service the disruption of which could have a significant impact on the provision of important social or economic activities and for the provision of which assets are used,
   f) provider of a regulated service is an authority or person that provides one or more regulated services,
   g) cybersecurity management the activities of a provider of a regulated service under this Act aimed at ensuring the cybersecurity of the regulated service.

(2) For the purposes of this Act
   a) cyberspace is a digital environment consisting of assets that enable the creation, exchange and further processing of information and data,
   b) information security means ensuring the confidentiality, integrity and availability of information and data,
   c) cyber threat is any potential circumstance, event or action that may damage, disrupt or otherwise adversely affect assets, their users or others, thereby causing a cyber security event or cyber security incident,
   d) significant cyber threat is a cyber 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 material or non-material harm,
   e) cyber security event is an event that may cause a cyber security incident,
   f) cyber security incident is a breach of information security within assets,
   g) cyber security incident management means actions leading to prevention, detection, analysis, mitigation, incident response and recovery,
   h) important supplier is one that enters into a legal relationship with a regulated service provider that is important from an information security perspective within the defined scope of cybersecurity management,
   i) strategically important regulated service, the disruption of the security of which could lead to a significant limitation or threat to services to the citizens of the state and the operation of the state,

j) provider of a strategically important service a provider of a regulated service that provides one or more strategically important services,
k) vulnerability is a weakness in an asset or a weakness in a security measure that can be exploited by one or more threats.

TITLE II
Regulated service provider

Determination of the regulated service and the regulated service provider regime

§ 3
Criteria of regulated services

A regulated service is defined by criteria for identification of regulated service or criteria for determination of regulated service.

§ 4
Criteria for the identification of regulated service

(1) The criteria for the identification of regulated service consist of the service criterion and the criterion of the provider of the regulated service. The criteria for identification of regulated service shall be laid down in implementing legislation.
(2) The implementing legislation shall set out the criteria for identifying a regulated service in the following sectors
a) public administration,
b) energy,
c) manufacturing industry,
d) food industry,
e) chemical industry,
f) water resource management,
g) waste management,
h) transport,
i) digital infrastructure and services,
j) financial market,
k) healthcare,
l) science, research and education,
m) postal and courier services,
n) military industry,
o) space industry.

§ 5
Criteria for determination of regulated service

Furthermore, a regulated service is a service of an authority or person determined by a decision of the Agency if

1) it is a service listed in the implementing legislation setting out the criteria for identification of regulated services; and
   a) the authority or person is the sole provider of the service in the Czech Republic and the service is essential to the maintenance of essential social or economic activities in the state,
   b) disruption to this service could have a significant impact on public safety or public health,
   c) 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
   d) the authority or person is, because of its specific importance at regional or national level, essential for a particular sector or type of service or for other interrelated sectors in the Czech Republic,
2) its disruption can cause a major disruption affecting more than 125,000 people through threats to life, health, property, internal or public order, security or the environment,
3) its disruption is likely to cause significant interference with the ability to provide another regulated service of the same or another provider of a regulated service under a higher obligation regime; or
4) the authority or person 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 critical infrastructure element identified with that entity.

§ 6
Regime of obligations of regulated service provider

(1) The regulated service provider regime sets out the level of obligations imposed on regulated service providers under this Act.

(2) The regulated service provider scheme is
   a) higher obligations regime, or
   b) lower obligations regime.

(3) The regime of regulated service provider is set out in implementing legislation. If the authority or person providing the regulated service is determined by a decision of the Agency pursuant to § 5, it shall always be a provider of a regulated service under the regime of higher obligations.

§ 7
Regulated service provider regime in case of provision of multiple regulated services

(1) Each regulated service provider shall have only one regime for all regulated services provided.

(2) A provider of a regulated service that is subject to a higher obligations regime for at least one regulated service it provides shall be subject to the higher obligations regime and shall comply with the obligations arising from this Act under the higher obligations regime in respect of all regulated services it provides.

§ 8
Registration of regulated service provider

(1) The provider of the regulated service is obliged to report to the Agency the fulfilment of the criteria for the identification of the regulated service by reporting the registration data pursuant to § 12(2)(a).
(2) The registration under paragraph 1 shall be carried out by the provider of the regulated service no later than 30 days from the date on which it becomes aware that the criteria for the identification of the regulated service have been met, but no later than 90 days from the date on which the criteria for the identification of the regulated service have been met.
(3) The Agency shall register a provider of a regulated service if it becomes aware of the fulfilment of the criteria for the identification of a regulated service pursuant to the implementing legislation and the provider of the regulated service fails to register pursuant to paragraph 1 within the time limit referred to in paragraph 2.
(4) In addition, the Agency shall register the provider of the regulated service or regulated service on the basis of the decision of the Agency on the determination of the regulated service pursuant to § 5. In the event that as a result of the decision pursuant to the preceding sentence the regime of the provider of the regulated service is changed from the regime of higher obligations to the regime of lower obligations, no new time limits for the commencement of compliance with the obligations pursuant to § 12(3), § 14(3) and § 16(4) shall apply.

§ 9
Change of registration of regulated service provider

(1) The provider of a regulated service is obliged to amend the registration of the provider of a regulated service if the criteria for the identification of each additional regulated service are met and to proceed in accordance with § 8(1) and (2).
(2) The regulated service provider is obliged to change the registration of the regulated service provider in the event that the criteria for the identification of the regulated service are met and to proceed in accordance with § 8(1) and (2).

§ 10
Entry in the register of regulated service providers

(1) The Agency shall without undue delay enter the regulated service provider and the regulated service into the register of regulated service providers on the basis of the

registration of the regulated service provider or a change in the registration of the regulated service provider pursuant to § 8 and § 9.

(2) A regulated service provider registered in the register of regulated service providers is obliged to fulfil all obligations arising from the law towards the registered regulated services from the moment of delivery of the notification of registration in the register of regulated service providers until the moment of delivery of the notification of deletion from the register of regulated service providers pursuant to § 11.

§ 11
Deletion from the register of regulated service providers

(1) If the Agency becomes aware that a provider of a regulated service registered in the register of regulated service providers on the basis of registration pursuant to § 8(1) and (3) or § 9(1) no longer provides a service that meets the criteria for identification of a regulated service pursuant to the implementing legislation, the Agency shall delete the registered regulated service from the register of regulated service providers and shall notify the provider of the regulated service of this fact in written form.

(2) If the Agency becomes aware that a provider of a regulated service whose service has been determined by a decision of the Agency pursuant to § 5 is no longer providing a service that meets the criteria for determination as a regulated service, the Agency shall decide that the service provided by the provider of the regulated service does not meet the criteria for designation as a regulated service. Once the decision comes into force, the Agency shall delete the registered regulated service from the register of regulated service providers and notify the regulated service provider in writing of this fact.

(3) If the Agency becomes aware that an authority or person registered in the register of providers of regulated services no longer provides any service that meets the criteria for the identification of a regulated service or a service determined by a decision of the Agency on meeting the criteria for the identification of a regulated service, the Agency shall remove the authority or person from the register of providers of regulated services and shall notify the authority or person in writing of this fact.

Obligations of the regulated service provider

§ 12
Reporting of registration data by the regulated service provider

(1) The provider of the regulated service shall report registration, contact and other additional data and changes thereto to the Agency. The provider of the regulated service is responsible for the accuracy and completeness of the reported data.

(2) The data reported are
   a) registration data, which means information related to the identification of the provider of the regulated service and the regulated service provided by it,
   b) contact details, which means information relating to the identification of natural persons who are authorised to act for the provider of the regulated service in matters governed by this Act, and
   c) additional data, which is other information necessary for the performance of the Agency's activities under this Act.

(3) The provider of a regulated service is obliged to report the data referred to in paragraph 2(b) and (c) for each regulated service no later than 30 days from the date of receipt of the written notification of its entry in the register of providers of regulated services pursuant to § 10(1).

(4) The provider of the regulated service is obliged to report changes only to the data referred to in paragraph 2 which are not reference data held in the basic registers, within 15 days of the change.

(5) The provider of the regulated service is obliged to ensure sufficient substitutability of natural persons who are entitled to act on behalf of the provider of the regulated service in issues governed by this Act.

(6) The content, format and method of reporting registration, contact and supplementary data shall be laid down in implementing legislation.

§ 13

Determination of the scope of cybersecurity management by regulated service provider

(1) Regulated service provider
   a) identifies all primary assets across the organisation,
   b) identify which primary assets identified under point (a) are related to the provision of the regulated service,
   c) for primary assets identified under point (b), identify and designate the related organisational parts of the organisation and supporting assets.

(2) The organisational parts and assets identified under paragraph 1(b) and (c) shall constitute the scope of the cybersecurity management (hereinafter referred to as the 'defined scope').

(3) The regulated service provider shall keep a documented record of the identification and determination of the organisational parts and assets referred to in paragraph 1, including a record of the primary assets that have been excluded from the defined scope and the reasons leading to their exclusion.

(4) Until the obligations under paragraphs 1 and 3 are met, the specified scope is deemed to consist of the regulated service of the regulated service provider, while the supporting assets are all the supporting assets of the organisation and other supporting assets related to the provision of the regulated service.

(5) Assets that have not yet been identified and determined in accordance with paragraph 1 or included in the defined scope in accordance with paragraph 4 shall

be deemed to be part of the defined scope until such time as those changes are included in the process of identifying and determining the organisational parts and assets comprising the defined scope in accordance with paragraph 1 and a documented record is maintained in accordance with paragraph 3.

§ 14
Security measures

(1) Security measures are actions designed to ensure the proper provision of a regulated service and the cybersecurity of assets. Security measures are organisational and technical measures.

(2) The provider of a regulated service is obliged to introduce and implement security measures pursuant to § 15 within the specified scope, at least to the extent and in the manner specified in the implementing legislation.

(3) A regulated service provider shall begin to comply with the obligation to introduce and implement the security measures referred to in paragraph 2 for each regulated service no later than 1 year from the date of receipt of written notification of its entry in the register of regulated service providers pursuant to § 10(1).

(4) The implementing legislation shall lay down security measures appropriate to the regime of the regulated service provider.

§ 15
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. 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. cyber security event and cyber security incident management,
   13. business continuity management and
   14. cybersecurity audit,

b) technical measures
   1. physical security,

2. security of communication networks,
3. Identity management and authentication,
4. access control,
5. detection of cyber security events,
6. recording of safety and relevant operational events,
7. evaluating cyber security 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 regime of reduced obligations, the security measures are

a) ensuring a minimum level of cyber security,
b) top management responsibilities,
c) risk management,
d) human resource security,
e) business continuity management,
f) access control,
g) identity management and permissions,
h) detection and recording of cyber security events,
i) dealing with cyber security incidents,
j) security of communication networks,
k) application security and
l) cryptographic algorithms.

§ 16
Cybersecurity incident reporting

(1) The provider of a regulated service under the higher obligations regime is obliged to report to the Agency all cyber security incidents originating in cyberspace within the specified scope.

(2) The provider of a regulated service under the regime of lower obligations is obliged to report to the National CERT all cyber security incidents that originate in cyberspace and have a significant impact on the provision of the regulated service, within a specified scope.

(3) The method of determining the significant impact of a cyber security incident on the provision of a regulated service by a provider of a regulated service under the regime of reduced obligations shall be determined by implementing legislation.

(4) The provider of a regulated service shall begin to comply with the obligation to report cyber security incidents pursuant to paragraphs 1 and 2 for each regulated service no later than 1 year from the date of receipt of written notification of its entry in the register of regulated service providers pursuant to § 10(1).

(5) An authority or person may voluntarily report cyber security incidents, especially those in which intentional culpability can be inferred, as well as report cyber security events or cyber threats via the Agency's website. Vulnerabilities may also be reported anonymously through the Agency's website, particularly to ensure coordinated disclosure of vulnerabilities by the Government CERT. This is without prejudice to the obligation of the regulated service provider under paragraphs 1 and 2.

(6) This provision shall be without prejudice to the information obligation under another legal regulation or directly applicable European Union legal act governing the protection of personal data.

§ 17
Requirements for reporting cyber security incidents

(1) The regulated service provider shall submit an initial report to the Agency or the National CERT without undue delay after the discovery of a cybersecurity incident, but no later than 24 hours, indicating whether it believes that the cybersecurity incident was caused by illegal or arbitrary interference or could have a cross-border impact.

(2) The Agency shall notify the provider of a regulated service under the higher obligations regime without undue delay, and no later than 24 hours after the reporting of a cybersecurity incident pursuant to paragraph 1, based on the content of the report and other relevant information, whether the cybersecurity incident at the provider of a regulated service under the higher obligations regime has a significant impact on the cyberspace of the State. The significance of the impact on national cyberspace shall be determined by the significance of the impact on the provision of the regulated service, the sector in which the cybersecurity incident occurred and the current situation in the cyberspace of the Czech Republic.

(3) In the event of a report of a cyber security incident with a significant impact on the provision of a regulated service pursuant to § 16(2) or on the national cyberspace pursuant to paragraph 2, the provider of the regulated service shall submit a report beyond the initial report pursuant to paragraph 1 to the Agency or the National CERT

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[3]) shall provide a notification under this point within 24 hours of becoming aware of the cybersecurity incident,

[3)] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

b) upon request of the Agency or the National CERT, an interim report on significant changes in the status of cyber security incident management; and
c) no later than 30 days after the submission of the notification referred to in point (a), a final report; in the event that the cybersecurity incident is still ongoing after the expiry of that period, the regulated service provider shall submit an interim report on the current status of the management of the cybersecurity incident without undue delay after the expiry of the period and then a final report no later than 30 days after the resolution of the cybersecurity incident.

(4) A regulated service provider shall report cybersecurity incidents, including voluntary reports under this Act, through the NCSIB Portal. If it is not possible to use the NCSIB Portal, the provider of the regulated service shall send the report under the regime of higher obligations to the electronic mail address of the Agency designated for receiving reports of cyber security incidents or to the data box of the Agency. In such a case, the provider of a regulated service under a lower obligation regime shall send the report to the e-mail address of the National CERT for receiving cyber security incident reports or to its data mailbox.

(5) The content, format and method of reporting a cyber security incident, and the content of the interim report on the current status of cyber security incident management and the final report shall be determined by implementing legislation.

§ 18
Cybersecurity incident management

(1) The Agency or the National CERT shall provide the Regulated Service Provider with a statement on the cyber security incident without undue delay, but no later than 24 hours after receipt of the initial report pursuant to § 17.

(2) At the request of the affected regulated service provider, the Agency or the National CERT shall provide methodological support for the implementation of possible mitigation measures, and other technical support, as appropriate, to manage a reported cyber security incident with a significant impact on the regulated service provider or the national cyberspace.

(3) Everyone is obliged to provide the necessary information and other necessary cooperation in the management of a cyber security incident at the request of the Agency, unless the purpose pursued cannot be achieved otherwise or would otherwise be substantially impeded. The requested assistance need not be provided if it is prevented by a statutory or governmental duty of confidentiality or other legal obligation.

(4) Data on cybersecurity incidents, events, cyber threats and vulnerabilities are kept in the records pursuant to § 45.

(5) Paragraphs (1) to (4) shall apply mutatis mutandis to the management of cyber security incidents reported voluntarily pursuant to § 16(5).

§ 19
Information obligation of the regulated service provider

(1) Where the provider of a regulated service considers it appropriate, it shall notify the users of the regulated service without undue delay of a cybersecurity incident with a significant impact that could adversely affect the provision of such service. The Agency is entitled to impose an obligation on the provider of a regulated service that is affected by a cybersecurity incident with a significant impact to inform the users of the regulated service about the incident. In the decision imposing this obligation, the Agency shall specify the scope of the information obligation.

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

§ 20
Countermeasures

(1) Countermeasures are actions needed to protect assets from a cyber threat or cyber security vulnerability or cyber security incident, or to address a cyber security incident that has already occurred.

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

(3) Unless the Agency provides otherwise in the countermeasure, the provider of the regulated service is obliged to notify the Agency of the implementation of the countermeasure and its result without undue delay, but at the latest within the time limit specified in the countermeasure. The content, format and method of notification shall be laid down in implementing legislation. Everyone is obliged to provide the necessary cooperation to the Agency in securing the necessary documents for the countermeasure. The required cooperation need not be provided if it is prevented by a legal or State-recognised obligation of confidentiality or the fulfilment of another legal obligation.

§ 21
Alert

(1) The Agency, after consultation with the regulated service provider concerned, is entitled, for reasons of protection of internal or public order and security, protection of life and health of persons or protection of the economy of the state, to inform the

public about a cyber security incident or violation of obligations under this Act, or to order the regulated service provider concerned to do so by decision.

(2) The Agency shall inform the public of the facts referred to in paragraph 1 via its website.

(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 can issue a warning if it becomes aware of a serious cyber threat or cyber security vulnerability.

(2) The provider of a regulated service under the higher obligations regime shall take into account warnings within the specified scope, unless the Agency or other legislation provides otherwise.

(3) The Agency shall notify the affected regulated service providers of the warning and publish it on the Agency's official notice board. The Agency shall not publish a warning if its publication could jeopardise the provision of cyber security, the effectiveness of countermeasures issued under this Act, other legitimate interests of the State or could identify the authority or person who reported the cyber threat, vulnerability or related cyber security 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 cyber security incident,

b) to protect assets from a cyber security incident, or

c) to enhance asset protection based on the analysis of an already resolved cybersecurity incident.

(2) Reactive countermeasures are obliged to 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 into the hands of the addressee within 72 hours of its issuance, it is considered to be delivered and enforceable upon its publication on the Agency's official notice board. 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 does not have suspensive effect.

(4) If the countermeasure referred to in paragraph 1 concerns an unspecified group of authorities or persons, the Agency shall adopt such countermeasure 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 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) The provider of the regulated service concerned or anyone who demonstrates that his or her rights, obligations or interests may be directly affected by a measure of a general nature may submit comments on a measure of a general nature issued pursuant to paragraph 4 within 30 days from the day it was published on the Agency's official notice board. On the basis of the comments submitted, the Agency may amend or repeal the general nature measure.

Relationship between the regulated service provider and its suppliers

§ 24
Supplier management and relationship to public procurement

(1) The provider of a regulated service is obliged to take into account the requirements resulting from security measures when selecting a supplier for its specified scope.
(2) Where possible, the provider of the regulated service is obliged to take account of the requirements resulting from security measures in contracts with its suppliers.
(3) Taking into account the requirements resulting from security measures when selecting a supplier to the extent necessary to fulfil the obligations under this Act cannot be considered an unlawful restriction of competition or an unjustified barrier to competition.

§ 25
Special arrangements for the transfer of information and data from an important supplier

(1) In the event of an imminent cyber security incident, the Agency may, at the initiative of a provider of a regulated service under a higher obligation regime who has unsuccessfully called upon an important supplier to fulfil its contractual obligation to hand over information and data, by decision impose on the important supplier the obligation to hand over information and data related to the operation of assets used to provide the regulated service to the provider of the regulated service under a higher obligation regime. If the important 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 it to arrange for and provide such information or data, the Agency may also impose

the obligation under the preceding sentence on another authority or person that possesses the requested information and data. The Agency may, in the decision, specify the format, scope, manner and time limit for the transfer and impose an obligation to securely destroy the information and data and copies thereof after the transfer has taken place.

(2) The request referred to in paragraph 1 shall include a justification for the request with regard to the threat of a cyber security incident, a detailed description of the previous conduct between the major supplier and the regulated service provider under the regime of higher obligations, in particular with regard to the failure of the major supplier to fulfil its contractual obligation, and the possible consequences if the requested information and data is not handed over.

(3) The decision to impose an obligation to provide information and data pursuant to paragraph 1 may be the first act in the proceedings. An appeal against a decision under the first sentence shall not have suspensory effect.

(4) Negotiations on the reimbursement of the costs incurred for the transmission of information and data shall not be an obstacle to the proper fulfilment of the obligation to transmit information and data.

Strategically important service

§ 26
Criteria for a strategically important service

A strategically important service is defined by criteria for identifying a strategically important service in defined sectors or criteria for identifying a strategically important service.

§ 27
Criteria for the identification and designation of a strategically important service

(1) The implementing legislation shall lay down the criteria for identifying a strategically important service in the sectors
   a) public administration,
   b) Energy,
   c) transport and
   d) digital infrastructure and services.

(2) A strategically important service is also a regulated service established by the provider of a regulated service under the regime of higher obligations by a decision of the Agency in the event that a breach of the information security of the regulated service could cause a serious impact on the security of the Czech Republic or internal or public order.

Assessment mechanism for supply chain security

§28
Supplier risk assessment

(1) The Agency collects and evaluates information and data related to an institution or a person concerning a possible threat to the security of the Czech Republic, internal or public order or fulfilling the supplier risk criteria.

(2) The activities pursuant to paragraph 1 shall be prioritised by the Agency based on a risk-based approach and available capacities.

(3) For the purposes of the Assessment mechanism for supply chain security the following shall mean

a) a critical part of the defined scope shall be the assets of the defined 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 defined scope on the strategically important service at the level of high or critical in accordance with the implementing legislation; the critical part of the defined scope shall always comprise of at least the assets of the defined scope of the strategically important service that provide the non-negligible functions of the defined scope as specified in the implementing legislation,

b) a security-significant supply shall be a performance directed to a critical part of the specified scope consisting of the provision, development, manufacture, assembly, management, operation, or service of

i) a technical means or equipment with computing capability,

ii) a software means or equipment; or

iii) an information or communication service,

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

(4) The non-negligible functions of the specified scope and the supplier risk criteria and the method of their evaluation are established by the implementing legislation.

§ 29

(1) The Ministry of Industry and Trade, the Ministry of Foreign Affairs and the Ministry of the Interior shall, for the purpose of performing the activity pursuant to Section 28(1), provide the Agency, upon its request, without undue delay, but no later than within 30 days, with an opinion on the fulfilment of the supplier risk criteria by a specific body or person, or provide information, or another form of cooperation.

(2) The Prosecutor General's Agency, the Police of the Czech Republic, the Agency for the Protection of Competition, the Financial Analytical Agency, and the intelligence services of the Czech Republic shall, for the purpose of performing the activity pursuant to Section 28(1), provide the Agency with the requested information or other cooperation without undue delay, but not later than within 30 days.

(3) If the Agency does not obtain from its own activities or in accordance with the procedure referred to in paragraphs 1 and 2 the information necessary for the performance of the activities referred to in Section 28(1), the bodies and persons not referred to in paragraphs 1 and 2 shall provide such information or other cooperation upon request from the Agency.

(4) Providing information under this provision shall not constitute a breach of confidentiality under any other legal regulation. This is not in prejudice to the attorney's confidentiality duty under the legal regulation governing the practice of the profession.

§ 30
Limiting the risks associated with the supplier

(1) The Agency issues a measure of a general nature establishing conditions or prohibiting the use of a supplier's performance of a security-significant supply in a critical part of the specified scope, if it finds, based on an evaluation of the supplier risk criteria, a possible significant threat to the security of the Czech Republic or internal or public order. The time limit for consideration of the conditions or prohibition contained in a measure of a general nature shall be set by the Agency with regard to its impact on the provider of the strategically important service.

(2) The Agency, after consulting the other authorities referred to in Section 29(1) and (2) and the Ministry of Finance, shall deliver the draft measure of a general nature pursuant to paragraph 1 by public announcement and invite the supplier against whose performance the measure of a general nature is directed, and other affected persons to submit comments on the draft measure of a general nature. The deadline for submitting comments is set at 30 days unless the Agency states otherwise. Section 172(1) and (5), Section 173(1), first sentence, part of the sentence after the semicolon, and Section 173(1), second sentence of the Code of Administrative Procedure do not apply to the procedure under this provision.

(3) The Agency shall review at least once every three years the continuation of the findings on which a measure of a general nature was issued pursuant to paragraph 1. If the Agency identifies that these findings have ceased to exist, it will repeal the measure of a general nature referred to in paragraph 1 in accordance with the procedure laid down in paragraphs 1 and 2, in a similar manner.

§ 31
Exceptions to the Supplier Risk Limitation

(1) The Agency may, if the nature of the threat to the security of the Czech Republic or to internal or public order so permits, grant an exemption from the conditions or prohibition set out in a measure of a general nature pursuant to Section 30 if the implementation of the measure of a general nature by the provider of a strategically important service could substantially endanger the performance of the strategically important service.

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

(3) In the decision to grant the exemption, the Agency determines the conditions for its application. In case of a serious violation of the conditions for the application of the exemption or in case the reason for which it was granted ceases to exist, the Agency shall revoke the exemption by decision.

(4) The Agency will not grant an exemption if this would completely foil the purpose of a measure of a general nature pursuant to Section 30.

§ 32
Obligations related to supply chain security assessment

(1) The provider of a strategically important service is obliged to
   a) ascertain, with reasonable endeavour, information about suppliers of security-significant supplies and record that information at least to the extent of identifying all security-significant supplies and the suppliers of security-significant supplies who provide them; and
   b) report to the Agency the information referred to in point (a) and changes thereto within 10 days of becoming aware of it; the content, format and method of reporting are stipulated in the implementing legislation.

(2) A provider of a strategically important service shall begin to comply with the obligation to report information pursuant to paragraph 1 for each strategically important service no later than 1 year from the date of receipt of written notification of its entry in the register of providers of regulated services pursuant to Section 10(1).

(3) The information reported to the Agency pursuant to paragraph 1(b) and paragraph 2 and the information identified in accordance with the procedure under § 28 and § 29 are part of the register of suppliers of security-significant supplies.

§ 33
Limiting supplier-related risks in public procurement

A provider of a strategically important service in the position of a contracting authority under the law governing public procurement may terminate a public procurement contract without undue delay after it has ascertained that the performance cannot be continued without violating a measure of a general nature pursuant to Section 30.

Ensuring the availability of a strategically important service

§ 34

(1) The provider of a strategically important service is obliged to ensure the availability of a strategically important service within the critical part of the specified scope at the specified time and quality from the territory of the Czech Republic.
(2) The provider of a strategically important service is obliged to test the ability to ensure the provision of a strategically important service within the critical part of the specified scope from the territory of the Czech Republic at least once every two years.
(3) The provider of a strategically important service shall begin to fulfil the obligations referred to in paragraphs 1 and 2 for each strategically important service no later than one year from the date of delivery of the notification of the registration of the strategically important service in the register of providers of regulated services or from the delivery of the decision on the designation of the strategically important service pursuant to § 27(2).
(4) The specified time and quality of service shall be determined by the regulated service provider depending on the business continuity management objectives of the implementing legislation.
(5) For the purposes of this provision, the critical part of the specified scope is defined in § 28(3)(a).

TITLE III
Entity providing domain name registration service

Obligations of entities providing domain name registration services
§ 35

(1) The entity 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, in the manner specified by the implementing legislationi
   a) the name of the entity,

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 representative of the entity referred to in § 67,
c) up-to-date contact details, including e-mail addresses and telephone numbers of the entity or its representative as referred to in § 67,
d) the Member States of the European Union in which the entity provides its services; and
e) the range of public IP addresses of the entity.

(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.

§ 36

(1) The entity administering and operating the Internet Top Level Domain Registry and the entity 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 as regards 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, in particular
a) the domain name,
b) date of registration,
c) the name of the registrant,
d) the registrant's email address,
e) the telephone number of the registrant,
f) the email address and telephone number of the contact point managing the domain name if different from the registrant.

(3) The entity managing and operating the Internet Top Level Domain Registry and the entity providing domain name registration services shall establish policies and procedures to ensure the accuracy and completeness of the information maintained in the database, including verification procedures. Those policies and procedures shall be publicly available.

(4) The entity administering and operating the Internet Top Level Domain Registry and the entity 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.

(5) The entity administering and operating the Internet Top Level Domain Registry and the entity 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 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.

TITLE IV Other cybersecurity tools

§ 37
Exception to the right to information

Information the disclosure of which could jeopardise the provision of cyber security or the effectiveness of countermeasures issued under this Act, or information which is held in the records maintained by the Agency pursuant to § 45, shall not be disclosed under the legislation governing free access to information.

§ 38
State of cyber emergency

A state of cyber emergency is a state in which the security of information in cyberspace is threatened to a large extent, which could lead or would lead to a threat to the interests of the Czech Republic. This interest is in particular the preservation of its constitutionality, sovereignty and territorial integrity, the safeguarding of internal or public order and security, international obligations and defence, the protection of the economy, life, health or property and the environment, and the safeguarding of the functionality of regulated services.

§ 39
Declaration of state of cyber emergency

(1) A state of cyber emergency can only be declared with reasons and for a strictly necessary period of time. The Director of the Agency shall declare a state of cyber emergency. The Director of the Agency shall immediately inform the Government of the declaration of the state of a cyber emergency. The state of cyber emergency may be declared for a period not exceeding 30 days. This period may be extended by the Director of the Agency only with the approval of the Government.

(2) The decision to declare a state of cyber emergency must include measures to address the state of cyber emergency and their scope. The decision shall be published on the official notice board of the Agency and by other appropriate means, in particular through mass media. The operator of a national television or radio is obliged to publish the information on the declaration of a state of cyber emergency without delay and without adjusting the content or purpose, upon request by the Agency. The decision comes into effect at the time specified therein. A change in the measures to deal with the state of cyber emergency shall be announced in a manner similar to that of the state of cyber emergency.

(3) A state of cyber emergency end after the expiry of the period for which it was declared unless the Director of the Agency or the Government decides to lift it before the expiry of that period. The Government shall also end the state of cyber emergency if the conditions for its declaration are not met. The decision of the Director of the Agency or the Government to end 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 decision comes into effect at the time specified therein.

(4) If it is not possible to effectively avert the threat within the framework of the state of cyber emergency, the Director of the Agency shall immediately request the Government to declare a state of emergency. Measures to address the state of cyber emergency declared by the Director of the Agency shall expire on the date of the declaration of the emergency, unless the Government decides otherwise. The cyber emergency measures that remain in force shall be deemed to be emergency measures ordered by the Government.

(5) The Code of Administrative Procedure does not apply to decisions and the imposition of obligations under this Act during a cyber emergency.

§ 40

Measures to deal with the state of cyber emergency

(1) The Director of the Agency is entitled during a state of cyber emergency to

a) provide resources in the property of the Czech Republic, which are in the use of the Agency and which are necessary to address a cyber security incident or to secure assets against a threatened cyber security incident,

b) to request information from authorities and persons on the means in kind, on production, operational and personnel capacities and on the volume of stocks in specified types of material, and these authorities and persons is obliged to provide the Agency with the requested information fully and truthfully within the time limit set by the Agency,

c) to request, on the basis of a contract or a record on the sharing of personnel capacities and resources in kind, the priority provision of personnel capacities or resources in kind and to use such personnel resources and resources in kind, whereby the requested authorities and persons are obliged to comply with the request of the Agency,

d) order work in standby mode,

e) prohibit the use of technical assets by authorities and persons who have been requested to do so by the Agency if such assets are imminently threatened by a cyber security incident that may significantly damage or destroy them, or are already affected by such an incident,

f) impose an obligation on authorities or persons to implement measures to address a cyber security incident and/or to secure assets against a cyber security

incident and to notify the implementation of the measures and the outcome thereof to the Agency,

g) order authorities and persons to conduct a vulnerability scan or penetration test; or

h) order authorities and persons to make non-public communication networks under their administration available for the use of the Agency.

(2) In a state of cyber emergency, authorities and persons who have been requested to do so by the Agency on the basis of measures issued by the Agency are obliged to

a) comply with measures to address and remedy the state of cyber emergency,

b) provide assistance in conducting a vulnerability scan or penetration test,

c) provide assistance in the disclosure of the state of cyber emergency; or

d) provide assistance in addressing and remediating the state of cyber emergency.

TITLE V
Exercise of State Administration

Institutions involved in the exercise of state administration in the field of cyber security

§ 41
National Agency for Cyber and Information Security

(1) The Agency is the central administrative authority for cyber security and for selected areas of protection of classified information under the Act on Protection of Classified Information and Security Clearance. Through its activities, the Agency contributes to strengthening the security and resilience of the Czech Republic in cyberspace. 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 responsible to the Prime Minister or to the member of the Government in charge.

(3) Agency

a) receives information on the fulfilment of the criteria for the identification of a regulated service and registers regulated service providers,

b) determines by decision the provider of the regulated service and the regulated service if it fulfils the criteria for determining the regulated service,

c) designate by decision a strategically important service pursuant to § 27(2),

d) enters the regulated service provider in the register of regulated service providers and deletes the regulated service provider from this register,

e) the decision changes the regime of the regulated service provider in specified cases,

f) receives reports of registration, contact and supplementary data and changes thereto,
g) establish security measures appropriate to the regulated service provider's regime,
h) manages and operates the NUCIB Portal,
i) inform the public about a cyber security incident in accordance with the procedures under this Act,
j) issue countermeasures and receive notification of their implementation and outcome,
k) maintains records and lists in accordance with this Act and the legislation governing the protection of classified information,
l) 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,
m) collect and evaluate the information and data referred to in § 28(1),
n) by a measure of a general nature, conditions or prohibits the use of the supplier's performance of a security-significant supply in a critical part of the specified scope,
o) examines the continuity of the facts on the basis of which the measure of a general nature under point (n) was issued,
p) decides on requests for exemption and grants exemptions from the conditions or prohibitions set out in a measure of a general nature pursuant to § 31,
q) negotiate contracts and records with bodies and persons for the sharing of staff capacity and resources in order to fulfil the statutory powers of the Agency,
r) declares, manages and coordinates a cyber emergency, imposes obligations and takes measures to avert a cyber emergency and acts as a coordinating authority during a cyber emergency,
s) during a cyber emergency, promulgate measures to address and remedy the cyber emergency,
t) continuously preparing to ensure preparedness to address and remediate cyber threats,
u) concludes a public contract with the operator of the National CERT,
v) carries out checks on the fulfilment of obligations under this Act and imposes corrective measures,
w) Imposes sanctions for failure to comply with the obligations set out in this Act and the Act on the Protection of Classified Information and Security Clearance,
x) carry out checks on compliance with obligations under this Act and provide other necessary assistance at the request of a supervisory authority of another Member State,
y) issue a decision on the suspension of a European cyber security certificate or on the obligation of a conformity assessment body to suspend the validity of a certificate or a certificate pursuant to § 60, and

z) apply to the court for the suspension of the exercise of the management function pursuant to § 61 and issue a certificate pursuant to the same provision.

(4) The Agency furthermore

a) performs analysis and monitoring of cyber threats and risks,

b) prepare and submit to the Government for approval a national cyber security strategy and an action plan for its implementation and update this strategy at least every 5 years,

c) performs state administration in the field of security of information and communication systems handling classified information and in the field of cryptographic protection, ensures the activities of the National Centre for Communication Security, the National Centre for Distribution of Cryptographic Material, the National Centre for Measurement of Compromising Radiation and the National Centre for Information Systems Security, which are its components,

d) in the field of cyber security, in selected areas of protection of classified information and in connection with

1. cooperates with bodies and persons active in these areas and in the field of cyber defence, in particular public corporations, research and development institutes and other CERTs,
2. ensures international cooperation and negotiates and concludes international cooperation agreements,
3. perform 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,
4. provides prevention, education and methodological support and
5. provides research and development,

e) 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 cyber security 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 cyber security, the operator of which is an organisational unit of the state, and verifies their actuality every 2 years,

f) fulfil its obligations towards the European Commission, the European Union Agency for Cybersecurity, the NIS Cooperation Group, the CSIRTs Network, the European Cyber Crisis Liaison Organisation Network and other entities in accordance with the relevant European Union legal act,

g) is the single point of contact for ensuring cross-border cooperation in the field of cyber security within the European Union and is the competent authority in the Czech Republic according to the relevant European Union legal act,

h) where appropriate, participate in the peer review process under the relevant European Union legal act,

i) performs activities in the field of the public regulated service of the European satellite navigation programme Galileo, in particular the functions of the competent PRS authority pursuant to Article 5 of Decision No 1104/2011/EU of the European Parliament and of the Council,
j) shall exercise competence in sub-areas related to security within the Union Space Programme in accordance with Regulation (EC) No 2021/696 of the European Parliament and of the Council,
k) is the national cybersecurity certification authority under Article 58 of the Cybersecurity Act,
l) acts as the National Coordination Centre for Research and Development in the field of cyber security for the Czech Republic according to the directly applicable European Union legal act[4]),
m) establish and support platforms for sharing information in the field of cybersecurity and set rules for their operation,
n) publishes the Bulletin of the Agency, which it publishes on its website; and
o) perform other tasks provided for by this Act and the Act on the Protection of Classified Information and Security Clearance.

(5) Government CERT as part of the Agency
a) provides solutions, coordination, analysis and preventive action against
1. cybersecurity threats,
2. cybersecurity vulnerabilities, including vulnerability scanning,
3. cyber security events and
4. cyber security incidents, including their management,
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 authorities or persons concerned,
d) is the coordinator for the purposes of coordinated vulnerability disclosure,
e) keeps records of cyber security incidents, events, cyber threats and vulnerabilities,
f) cooperates with authorities and persons working in the field of cyber security,
g) provides advice to authorities and individuals on cyber security,
h) receives and evaluates cybersecurity initiatives from authorities and individuals,
i) may share with authorities and persons data and information from its activities and from records maintained by the Agency, if necessary to ensure cybersecurity; if the Government CERT establishes a level of protection for the information so shared, authorities and persons are obliged to comply with that level of protection,
j) performs the role of the CSIRT team according to the relevant European Union legal act and represents the Czech Republic and participates in the functioning of relevant international groups and associations in the field of cyber security, including the CSIRTs Network,

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

k) in appropriate cases, transmit without undue delay information about a cyber security incident with a significant impact involving two or more Member States reported pursuant to § 16 and § 17 to the Member States 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 cyber security tools and solutions, and
m) prioritise the delivery of its services and the performance of its activities according to a risk-based approach and available capacity.

§ 42
Operator of the National CERT

(1) The operator of the National CERT may only be a legal entity that
a) does not carry out any activities against the interest of the Czech Republic according to the legal regulations governing the protection of classified information, and has never done so,
b) has been administrating or operating the relevant technical assets, or has been participating in their administration and operation for at least a period of 5 years,
c) has the technological prerequisites to carry out the activities referred to in paragraph 3,
d) is a member of a multinational organisation operating in the field of cyber security,
e) does not have any tax arrears due in the Czech Republic and no arrears of insurance premiums or penalties for public health insurance and social security premiums or penalties or contributions for state employment policy due in the Czech Republic,
f) has not been sentenced for committing a crime specified in Section 7 of Act no. 418/2011 Coll. on the Criminal Responsibility of Legal Persons and Proceedings against them
g) is not a foreign person according to any other legal regulation,
h) was not founded or established solely to pursue financial gain; this is without prejudice to the possibility of the operator of the National CERT to carry out, on its own behalf and under its own responsibility, other economic activities in the field of cyber security not regulated by this Act, provided that such activities do not interfere with the fulfilment of the obligations referred to in paragraph 3; and
i) has concluded a public law contract with the Agency pursuant to § 52.

(2) The applicant shall demonstrate compliance with the conditions by submitting
a) A statutory declaration with regard to paragraph 1, letters (a) to (d), (g) and (h), the contents of which must show that the tenderer fulfils the relevant requirements, and

b) confirmation by the competent authorities of the Financial Administration of the Czech Republic, the Customs Administration of the Czech Republic, the Czech Social Security Administration and the relevant insurance company with regard to paragraph 1(e), which must not be older than 30 days.

(3) The operator of the National CERT pursues activities of the National CERT, which
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 cyber security incidents, cyber security events, cyber threats and cyber security vulnerabilities and evaluates, records, stores and protects this data,
c) Provides methodological support, assistance and assistance to regulated service providers under the lower obligation regime in the occurrence and management of a high-impact cyber security incident and in the disclosure of information on cyber security vulnerabilities,
d) conducts searches and assessments of cyber security vulnerabilities,
e) transmits to the Agency data on reported cyber threats, cyber security events, cyber security incidents under § 16 and cyber security vulnerabilities,
f) inform the competent authority of another Member State, without identifying the whistleblower, of a cyber-security 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 whistleblower,
g) receives and evaluates cybersecurity initiatives from authorities and individuals,
h) performs the role of a CSIRT team in accordance with the relevant European Union legal act and participates in the functioning of international cybersecurity groups, including the CSIRTs Network,
i) participate, where appropriate, in the peer review process under the relevant European Union legislation; and
j) prioritise the delivery of its services and the performance of its activities according to a risk-based approach and available capacity.

(4) The operator of the National CERT shall act impartially and coordinate its activities with the Agency in the performance of the duties referred to in paragraph 3.

(5) The operator of the National CERT shall carry out the activities referred to in paragraph 3(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 execution of the activities referred to in paragraph 3.

(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.

§ 43
Permanent Commission for the Control of the Agency's Activities

(1) The activities of the Agency are audited by the Chamber of Deputies, which establishes a special audit body for this purpose (hereinafter referred to as the "Audit Body").

(2) The supervisory organ 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 Audit Body.

(3) Unless this Act provides otherwise, other legislation shall apply mutatis mutandis to the conduct of the supervisory body and to the rights and obligations of its members[5]).

(4) Members of the audit body may enter the premises of the Agency accompanied by the Director of the Agency or an employee authorised by him/her.

(5) The Director of the Agency shall submit to the Audit Body
   a) a report on the activities of the Agency,
   b) the draft budget of the Agency,
   c) the documents needed to control the implementation of the Agency 's budget,
   d) the internal rules of the Agency,
   e) on request, a report on individual cyber security incidents of regulated service providers.

(6) If the audit authority considers that the activities of the Agency unlawfully restrict or infringe the rights and freedoms of citizens or that the decision-making activities of the Agency within the framework of administrative proceedings are defective, it is entitled to request the necessary explanation from the Director of the Agency.

(7) 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 controlling authority discovers in the course of its activities, is obliged to notify the Director of the Agency and the Prime Minister.

(8) The obligation of confidentiality imposed on members of the supervisory authority under the Act shall not apply to cases where the supervisory authority makes a notification under paragraph 7.

[5)] Act No. 90/1995 Coll., on the Rules of Procedure of the Chamber of Deputies, as amended.

Instruments of state administration

§ 44
The NUKIB Portal

(1) The Agency is the administrator and operator of the NUKIB Portal, which is used to exercise the Agency's powers, share information, perform digital acts and provide digital services under this Act.

(2) A provider of a regulated service is obliged to carry out the acts referred to in § 8(1), § 9(1), § 12(1), § 16(1) and (2), § 20(3), § 32(1)(b) and § 57(1) exclusively electronically using remote access and form submissions. These acts may be performed in another way only if the relevant provisions of this Act allow it and if it is objectively not possible to use the NUKIB Portal to perform the act. An act that is not performed in this way, in the format and structure provided for in the implementing legislation, 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 tasks referred to in paragraph 2 shall be laid down in implementing legislation.

§ 45
Records kept by the Agency

(1) The Agency shall keep records of
   a) regulated service providers, domain name registration service providers and the data they report,
   b) cyber security incidents, events, cyber threats and vulnerabilities,
   c) suppliers of security-relevant supplies,
   d) coordinated vulnerability disclosure,
   e) penetration tests and
   f) checks 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 applicant shall make reasonable efforts to ensure the information security of the data so provided.

(3) In justified cases, the Agency may provide data from the records to the National CERT, authorities or persons exercising cybersecurity activities abroad and other authorities or persons 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(b) to (e). 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.

§ 46

Authorisation of conformity assessment bodies under the Cybersecurity Act

(1) Where a directly applicable legal act of the European Union issued on the basis of the Cybersecurity Act sets 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)(a)(i) of the Cybersecurity Act, provide for specific or additional requirements for conformity assessment bodies to ensure their technical competence to assess cybersecurity requirements. (e) of the Cybersecurity Act, the Agency shall decide on applications for the authorisation of a conformity assessment body and, where an authorised conformity assessment body is in breach of the requirements of the Cybersecurity Act or of a directly applicable legal act of the European Union issued on the basis of the Cybersecurity Act, on the suspension, amendment or revocation of the authorisation decision.

(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) In the decision to suspend the enforceability of the authorisation decision pursuant to paragraph 1, the Agency shall set a time limit for seeking redress. If the conformity assessment body remedies the situation, it shall notify the Agency without undue delay. If the Agency finds that the remedy is sufficient, it shall revoke the decision suspending the enforceability of the authorisation decision. If the authorised conformity assessment body fails to remedy the situation within the specified time limit, the Agency shall decide to amend or revoke the authorisation decision.

(4) 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.

§ 47

National Coordination Centre for Cyber Security Research and Development

(1) The Agency, as the National Coordination Centre for Research and Development in the field of cyber security, assesses the eligibility of an applicant for registration as a member of the Cyber Security Community of Competence[6)] (hereinafter

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

referred to as the "Community") in accordance with the directly applicable European Union legal act[7]).

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

(3) The application for registration of membership in the Community (hereinafter referred to as the "Application") shall be submitted electronically using the form published on the website of the Agency.

(4) The applicant is obliged to provide in the application true and complete information necessary for the assessment of his/her basic and special competence by the Agency. For the duration of the membership in the Community, the applicant who was registered as a member of the Community is obliged to report a change of these data or a fact decisive for the assessment of his/her basic and special eligibility within 30 days from the date when this change or fact occurred or the applicant became aware of it.

§ 48

Basic eligibility of an applicant for registration of membership in the Community

(1) An applicant has basic eligibility if
   a) has its registered Agency or place of business in the Czech Republic,
   b) is not on the national sanctions list[8]),
   c) has not been convicted in the last 5 years prior to the submission of the application for a criminal offence, the merits of which are related to the applicant's business, or for an economic offence, an offence against property, a generally dangerous offence, an offence against the Czech Republic, a foreign state or an international organisation, an offence against public order; convictions that have been overturned are not taken into account,
   d) has no tax arrears due in the Czech Republic,
   e) does not have any outstanding insurance premiums or penalties for public health insurance payable in the Czech Republic,
   f) has no arrears of social security contributions or penalties payable in the Czech Republic; and
   g) is not in liquidation[9]), has not been the subject of a bankruptcy order[10]) and has not been placed under receivership under any other legal provision[11]).

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

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

[9)] § 187 of the Civil Code.

[10)] § 136 of Act No. 182/2006 Coll., on bankruptcy and methods of its resolution (Insolvency Act), as amended.

[11)] 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.

(2) The applicant shall demonstrate compliance with the basic eligibility conditions referred to in paragraph 1 by submitting
   a) an extract from the criminal record in relation to paragraph 1(c), which must not be older than 3 months,
   b) a certificate from the competent tax Agency in relation to paragraph 1(d), which must not be older than 30 calendar days before the date of submission of the application,
   c) a written affidavit in respect of excise duty in relation to paragraph 1(d),
   d) a written affidavit in relation to paragraph 1(e) and
   e) a certificate from the competent district social security administration in relation to paragraph 1(f), which must not be older than 30 calendar days before the date of application.

(3) In the case of an applicant, if it is a legal person, the Agency shall ascertain the details of the applicant's beneficial owner pursuant to the legislation governing the registration of beneficial owners[12]) (hereinafter referred to as the "beneficial owner") from the register of beneficial owners pursuant to the same Act (hereinafter referred to as the "register of beneficial owners").

(4) An applicant is not eligible if
   a) is a legal person which has a beneficial owner, unless it has been possible to ascertain the details of its beneficial owner from the register of beneficial owners pursuant to paragraph 3,
   b) the beneficial owner is a person established outside the territory of the Member States of the European Union and the Member States of the European Free Trade Association, or
   c) the beneficial owner is a person listed on the national sanctions list[8)] .

(5) If the applicant is a legal person, the condition referred to in paragraph 1(c) must be fulfilled by that legal person and by each member of its statutory body. If a member of the applicant's statutory body is a legal person, the condition referred to in paragraph 1(c) must be fulfilled by
   a) this legal entity,
   b) each member of the statutory body of the legal entity; and
   c) the person representing the legal person in the applicant's statutory body.

(6) An applicant is not eligible if the Agency has issued a measure of a general nature pursuant to § 30(1), in which it has set conditions for the use of the applicant's performance or has prohibited the use of the applicant's performance as a supplier of a security-significant supply.

[12)] Act No. 37/2021 Coll., on the registration of beneficial owners.

§ 49
Special eligibility of an applicant for registration of membership in the Community

Special eligibility is granted to an applicant who demonstrates that he or she is eligible for registration under a directly applicable European Union legal act[13]).

§ 50
Assessment of the eligibility of an applicant for registration of membership in the Community

(1) If the applicant fulfils the conditions pursuant to § 47(2), the Agency shall refer the applicant's application to the registering authority pursuant to the directly applicable legal act of the European Union[14]) (hereinafter referred to as the "registering authority").
(2) If there is any doubt as to whether the applicant meets the conditions under § 47(2), the Agency shall initiate proceedings to determine the applicant's ineligibility to register for membership in the Community.
(3) After the legal validity of the decision on the ineligibility of the applicant for registration of membership in the Community issued in the proceedings under paragraph 2, the Agency shall forward the applicant's application to the registering authority and at the same time notify the registering authority of the ineligibility of the applicant for registration of membership in the Community.

§ 51
Eligibility of the applicant for membership in the Community

(1) The Agency shall continuously assess compliance with the requirements under § 47(2) throughout the duration of the membership of the applicant in the Community whose application for registration in the Community has been granted by the Registration Authority.
(2) In the event that an applicant who is registered as a member of the Community does not meet the conditions under § 47(2), the Agency shall initiate proceedings to determine the applicant's ineligibility for membership in the Community.
(3) After the legal validity of the decision on the applicant's ineligibility for membership in the Community issued in the proceedings under paragraph 2, the Agency shall notify the registering authority of the applicant's ineligibility for membership in the Community.

13) Article 8(3) of Regulation (EU) 2021/887 of the European Parliament and of the Council of 20 May 2021.
14) Regulation (EU) 2021/887 of the European Parliament and of the Council of 20 May 2021.

§ 52
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 cyber security and the provision of activities under § 42(3) (hereinafter referred to as the "public law contract"). The Agency shall announce the procedure for the selection of the application.

(2) The public 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 notice,
   g) the prohibition of misuse of data obtained in connection with the performance of the activities referred to in § 42(3),
   h) defining the conditions for the performance of the activities of the National CERT pursuant to § 42(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 commitment.

(3) The Agency shall publish the public law contract concluded pursuant to paragraph 1 in the Bulletin 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.

§ 53
Processing of personal data

(1) The Agency and the operator of the National CERT shall process personal data as necessary for -the exercise of their competences. The Agency and the operator of the National CERT shall transmit such data to public authorities or persons if this is necessary for the performance of their tasks and if this does not violate the obligation of confidentiality under this Act.

(2) The Agency and the operator of the National CERT when processing personal data covered by directly applicable European Union legislation governing the protection of personal data,
   a) may not restrict the processing of personal data where the data subject contests the accuracy of the data or objects to such processing; and
   b) may, in the exercise of their powers, use personal data for purposes other than those for which they were collected.

(3) Where the Agency or the operator of the National CERT, in the course of an activity covered by a directly applicable European Union legal act governing the protection of personal data, in the course of dealing with a cyber security incident or a cyber security event, in the prevention of cyber threats or risks, or in the performance of an inspection, receives personal data which it processes solely for the purpose of carrying out its obligations under this Act, it shall not be required to further
   a) provide the data subject with information on rectification or erasure of personal data or restriction of processing,
   b) provide access to the personal data to the data subject; or
   c) correct or supplement personal data at the request of the data subject.

§ 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 States of the European Union (hereinafter referred to as "other Member State"), and in particular 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) if it is not legally competent or does not have the authority to perform the requested act,
   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 established in another Member State of the European Union provides a service within the Czech Republic
   a) domain name resolution (DNS),
   b) management and operation of the Internet Top Level Domain Registry,
   c) cloud computing,
   d) data center,
   e) content delivery networks (CDNs),
   f) online marketplace,
   g) Internet search engine,
   h) social network platforms,

i) managed services (MSP), or
j) Managed Security Services (MSSP),

the Agency is entitled to carry out an inspection or other action in respect of that person on the basis of and to the extent of a request for cooperation from another Member State in which the provider of the regulated service has its principal establishment.

(4) Where assets used for the provision of any of the services referred to in paragraph 3 are located within the Czech Republic, but the provider of the regulated service has its principal place of business 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 principal place of business.

(5) The location of the principal establishment means the place in the European Union where the person providing the services referred to in paragraph 3 predominantly takes decisions relating to the management of cyber security risks. Where such a place cannot be determined in accordance with the first sentence, or where such decisions are not taken in the European Union, 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 the Member State of the European Union 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.

§ 55
Implementing legislation and enabling provisions

(1) The implementing legislation shall lay down
a) criteria for identifying the regulated service (§ 4),
b) the method of determining the regulated service provider regime (§ 6(3)),
c) security measures appropriate to the regulated service provider's regime and the extent and manner of their introduction and implementation (§14(2) and (4)),
d) how to determine the significant impact of a cybersecurity incident on the provision of a regulated service under the regime of lower obligations (Article 16(3)),
e) the content, format and manner of notification of the implementation of the countermeasure and its outcome (§ 20(3)),
f) criteria for identifying a strategically important service (§ 27(1)),
g) non-negotiable functions of a specified scope (§ 28(4)),
h) the supplier's risk criteria and how they are to be evaluated (§ 28(4)),

i) the manner in which data is reported by the entity providing domain name registration services (§ 35(1)); and
j) the technical and organisational conditions for the use of the NUCIB Portal, the content, format, structure and manner of performing the tasks referred to in § 44(2) (§ 44(3)).

(2) The implementing legislation referred to in paragraph 1 shall be issued by the Agency in the form of a decree.

TITLE VI
Control, corrective measures, offences and penalties

§ 56
Control by the Agency

(1) The Agency carries out controls in the field of cyber security. When exercising control, the Agency shall ascertain how authorities and persons comply with the obligations laid down by this Act, decisions and measures of a general nature issued by the Agency pursuant to this Act, and comply with implementing legislation in the field of cyber security.
(2) The inspection shall be carried out in accordance with the inspection regulations.
(3) The control under this provision shall be carried out by authorised staff of the Agency.

§ 57
Corrective measures

(1) If the Agency finds deficiencies during the inspection, it may by decision order the inspected body or person to remedy them within a specified period of time, or specify how. In the decision, the Agency may impose an obligation on the institution or person to notify the Agency of the implementation of the corrective measure and its result within a specified time limit. The form and manner of reporting shall be laid down in the implementing legislation.
(2) If the Agency considers the findings of fact to be sufficient, it may impose the corrective measure referred to in paragraph 1 without carrying out an inspection.
(3) An appeal against a decision to impose a remedial measure shall not have suspensive effect.

§ 58
Offences

(1) A provider of a regulated service under the higher obligations regime commits an offence by

a) fails to register or amend the registration of a regulated service provider in accordance with § 8(1) and (2) or § 9(1) or (2),
b) fails to report registration, contact or other data or changes thereto to the Agency in accordance with § 12(1) and (4),
c) does not ensure sufficient substitutability of natural persons authorised to act for the provider of the regulated service pursuant to Article 12(5),
d) does not identify all primary assets as referred to in § 13(1)(a) when determining the scope of cybersecurity management,
e) in determining the scope of the cybersecurity management, does not identify all primary assets related to the provision of the regulated service as referred to in § 13(1)(b) or organisational parts and supporting assets as referred to in § 13(1)(c),
f) does not keep a documented record of the identification and designation of organisational parts and assets in accordance with § 13(3),
g) fails to introduce or implement security measures in breach of § 14,
h) fails to report a cybersecurity incident pursuant to § 16(1) or fails to submit an initial incident report pursuant to § 17(1) or fails to complete any of the incident data pursuant to § 17(3),
i) fails to provide information or cooperation in the management of an incident in accordance with § 18(3),
j) fails to comply with the obligation to inform users of the regulated service about a cyber security incident with a significant impact as set out in the decision of the Agency pursuant to § 19(1),
k) fails to comply with the obligation to inform the user of a regulated service of a significant cyber threat and the steps that the user of the service may take in response to it pursuant to § 19(2),
l) fails to notify the implementation of the countermeasure imposed by the Agency and its outcome pursuant to § 20(3),
m) fails to comply with an obligation imposed by the Agency by a warning decision pursuant to § 21,
n) fails to comply with an obligation imposed by a decision to issue a reactive countermeasure or a measure of a general nature issued by the Agency pursuant to § 23,
o) fails to take account of the requirements resulting from the safety measures in the selection of the supplier or in the contract with the supplier in breach of Article 24(1) or (2), or
p) fails to comply with any of the obligations imposed by a decision imposing a remedial measure pursuant to § 57.

(2) A provider of a regulated service under the regime of reduced obligations commits an offence by
a) fails to register or amend the registration of a regulated service provider in accordance with § 8(1) and (2) or § 9(1) or (2),

b) fails to report registration, contact or other data or changes thereto to the Agency in accordance with § 12(1) and (4),
c) does not ensure sufficient substitutability of natural persons authorised to act for the provider of the regulated service pursuant to Article 12(5),
d) does not identify all primary assets as referred to in § 13(1)(a) when determining the scope of cybersecurity management,
e) in determining the scope of the cybersecurity management, does not identify all primary assets related to the provision of the regulated service as referred to in § 13(1)(b) or organisational parts and supporting assets as referred to in § 13(1)(c),
f) does not keep a documented record of the identification and designation of organisational parts and assets in accordance with § 13(3),
g) fails to introduce or implement security measures in breach of § 14,
h) fails to report a cyber security incident in accordance with § 16(2) or fails to submit an initial incident report in accordance with § 17(1) or fails to complete any of the incident data in accordance with § 17(3),
i) fails to provide information or cooperation in the management of an incident in accordance with § 18(3),
j) fails to comply with the obligation to inform users of the regulated service about a cyber security incident with a significant impact as set out in the decision of the Agency pursuant to § 19(1),
k) fails to comply with the obligation to inform the user of a regulated service of a significant cyber threat and the steps that the user of the service may take in response to it pursuant to § 19(2),
l) fails to notify the implementation of the countermeasure imposed by the Agency and its outcome pursuant to § 20(3),
m) fails to comply with an obligation imposed by the Agency by a warning decision pursuant to § 21,
n) fails to comply with an obligation imposed by a decision to issue a reactive countermeasure or a measure of a general nature issued by the Agency pursuant to § 23,
o) fails to take account of the requirements resulting from the safety measures in the selection of the supplier or in the contract with the supplier in breach of Article 24(1) or (2), or
p) fails to comply with any of the obligations imposed by a decision imposing a remedial measure pursuant to § 57.

(3) A provider of a strategically important service commits an offence by
a) violates a condition or prohibition imposed by the Agency in a measure of a general nature pursuant to § 30,
b) fails to make reasonable efforts to obtain information about the supplier of a security-significant supply as referred to in point (a) of Article 32(1),
c) it does not record information on the supplier of a security-significant supply pursuant to Article 32(1)(a),

d) fails to notify the Agency of information about the supplier of a security-significant supply or a change thereof pursuant to § 32(1)(b),
e) it does not ensure the availability of a strategically important service from the territory of the Czech Republic within the time and quality specified under § 34(1), or
f) does not test the ability to ensure the provision of a strategically important service as referred to in § 34(2).

(4) An entity providing domain name registration services commits an offence by
a) fails to report to the Agency the data referred to in § 35(1) or a change thereof pursuant to § 35(2),
b) fails to collect or maintain accurate and complete domain name registration data in the dedicated database referred to in § 36(1) in accordance with the requirements of § 36(2),
c) fails to establish 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, in accordance with § 36(4); or
e) shall not provide access to specific domain name registration data pursuant to § 36(5).

(5) An entity administering and operating an Internet top-level domain registry commits an offence by
a) fails to collect or maintain accurate and complete domain name registration data in the dedicated database referred to in § 36(1) in accordance with the requirements of § 36(2),
b) fails to establish 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),
c) without undue delay after the registration of the domain name, fails to publish its registration data, which are not personal data, in accordance with § 36(4); or
d) shall not provide access to specific domain name registration data pursuant to § 36(5).

(6) An authority or person commits an offence by
a) fails to provide cooperation in securing the grounds for issuing countermeasures pursuant to § 20(3),
b) fails to provide the data and information referred to in § 25(1),
c) fails to provide information or other cooperation following a request from the Agency pursuant to § 29(3),
d) fails to comply with any of the obligations imposed by a decision imposing a remedial measure pursuant to § 57, or
e) fails to provide information or other cooperation necessary to assess the fulfilment of the criteria for a regulated service pursuant to § 63(2).

(7) An authority or person who is not a provider of a regulated service commits an offence by failing to cooperate in the management of an incident in accordance with § 18(3).

(8) In the context of a cyber emergency, an institution or person commits an offence by

a) fails to comply with measures to address and remedy a cyber threat situation as referred to in § 40(2)(a),

b) fails to provide cooperation in conducting a vulnerability scan or penetration test pursuant to § 40(2)(b),

c) fails to provide cooperation in the public disclosure of the declaration, conduct and termination of a cyber emergency in accordance with § 40(2)(c), or

d) fails to provide cooperation in addressing and remedying a cyber threat situation pursuant to § 40(2)(d).

(9) A natural person commits an offence by breaching the duty of confidentiality under § 45(4).

(10) An applicant commits an offence by providing false or grossly misrepresented information or by omitting material information in an application for registration pursuant to § 47(4).

(11) An applicant commits an offence by failing to disclose a change in the information required for the assessment of his/her basic and special eligibility by the Agency, by concealing the change, or by failing to disclose other facts relevant to the assessment of his/her basic and special eligibility, or by concealing such facts during the period of membership of the Community under § 47.

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

(13) A manufacturer or provider of products, services or processes issuing an EU declaration of conformity commits an offence by

a) issue an EU declaration of conformity even though the conditions laid down in the Cybersecurity Act are not met[15)] ,

b) does not keep documents and information as referred to in Article 53(3) of the Cybersecurity Act,

c) fails 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) does not provide cybersecurity information to the extent and in the manner specified in Article 55 of the Cybersecurity Act.

(14) A legal or natural person commits an offence by

a) misuses 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,

[15] 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").

b) forges or alters a European Cyber Security Certificate, EU Declaration of Conformity or other document under the Cyber Security Act,

c) performs 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) carries 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) acts 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, fails to comply with the obligation imposed by the Agency to suspend the validity of a certificate or attestation issued by it pursuant to § 60(1).

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

a) CZK 250 000 000 or up to 2 % of the net worldwide annual turnover achieved by the legal person or, if the accused is part of a consolidation unit, achieved by the consolidation unit in the immediately preceding accounting period, whichever is higher, in the case of an offence under paragraph 1(a), (d) to (k) and (m) to (p), paragraph 3(a), (e) and (f), paragraph 6(b) and paragraph 8(a) and (b).

b) CZK 175 000 000 or up to 1,4 % of the net worldwide annual turnover achieved by the legal person or, if the accused is part of a consolidation unit, achieved by the consolidation unit in the immediately preceding accounting period, whichever is higher, if the offence is an offence under paragraph 2(a), (d) to (k) and (m) to (p) and paragraph 8(d).

c) CZK 100 000 000 if the offence is an offence under paragraph 1(b), paragraph 3(b) and (c),

d) CZK 50 000 000 if the offence is an offence under paragraph 1(c) and (l), paragraph 2(b), paragraph 3(d), paragraph 4(a) to (e), paragraph 5(a) to (d), paragraph 6(a) and (c) to (e), paragraph 7 and paragraph 13(a),

e) CZK 35 000 000 if the offence is an offence under paragraph 2(c) and (l) and paragraph 8(c),

f) CZK 20 000 000 if the offence is an offence under paragraph 13(b) to (d) and paragraph 14(a) to (c) and (e) to (g),

g) CZK 2 000 000 if the offence is an offence under paragraphs 10, 11 and 12 and paragraph 14(d),

h) CZK 50 000 if the offence is an offence under paragraph 9.

§ 59
Common provisions on offences

(1) Offences under this Act shall be heard and fines levied by the Agency.
(2) An act which has the formal characteristics of an offence under this Act shall be deemed to be socially harmful.
(3) The provisions of § 43, § 68(b), § 70, § 71, § 80(3), § 88(2), § 89, § 90(3), § 95(3) and § 96(1)(b) of the Offences Liability and Procedure Act[16]) shall not apply to the Agency's procedure under this Act.
(4) The following shall apply: offences consisting in the breach of an obligation imposed by a decision, a measure of a general nature or a corrective measure, offences consisting in the failure to register a provider of a regulated service, offences related to the determination of the scope of cyber security management, offences relating to the consideration of requirements arising from security measures in the selection of a supplier or in a contract with a supplier, offences relating to breaches of obligations under the supply chain security screening mechanism and offences relating to failure to notify information and maintain a state of non-communication to the Agency or users of the regulated service are continuing offences.

§ 60
Suspension of certification

(1) In the event of failure to comply with the obligation to remedy deficiencies identified during an inspection imposed by a decision of the Agency on a provider of a regulated service under the higher obligations regime who holds a European cyber security certificate under the Act on Cyber Security or another certificate or certificate related to ensuring cyber security of a regulated service, the Agency may suspend the European cyber security 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 it until the deficiencies identified during the inspection are remedied, but at least for 6 months.
(2) 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.
(3) The party to the procedure for issuing a decision under paragraph 1 shall always be the provider of the regulated service under the higher obligations regime whose certificate is being decided.
(4) The Agency shall publish information on the suspension of a certificate or certification on its website.
(5) The Agency shall, however, not earlier than after the expiry of the period referred to in paragraph 1, check the compliance with the obligation to remedy the deficiencies identified during the inspection and, if it finds that the deficiencies have

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

been remedied, the Agency shall issue a certificate to that effect, which shall be the basis for the renewal of the certificate or certificate.

§ 61
Suspension of the exercise of management functions

(1) The court may, on a motion of the Agency, decide that a member of the statutory body of a legal entity, head of a branch plant, proxy or an entrepreneurial natural person who, in direct connection with the implementation of a decision of the Agency imposing an obligation on a provider of a regulated service under the higher obligations regime to remedy deficiencies identified during an inspection, has repeatedly or seriously violated his/her duties in the exercise of his/her managerial function, as a result of which the proper implementation of the decision of the Agency has been thwarted, may not exercise that managerial function until the deficiencies identified during the inspection have been remedied, but at least for a period of 6 months.

(2) The application may be brought only against a person performing a management function of a regulated service provider under the regime of higher obligations and only in relation to a management function which is not a public function defined by term of Agency or time period and occupied by direct or indirect election or appointment pursuant to special legislation.

(3) The provisions of the Companies Act[17]) regulating the exclusion of a member of the statutory body from the exercise of his/her functions shall apply mutatis mutandis in respect of the legal effects of a final decision on the exclusion of a member of the statutory body, the notification of the registry court and liability for breach of the temporary ban on the exercise of functions.

(4) The Agency shall publish information on the final decision on the suspension of the performance of the management function on its website.

(5) The Agency shall, however, at the earliest after the expiry of the time limit referred to in paragraph 1, carry out a check on the fulfilment of the obligation to eliminate the deficiencies identified during the check and, if it finds that the deficiencies have been eliminated, the Agency shall issue a certificate to that effect, which shall serve as the basis for the deletion of the information on the suspension of the management function from the Commercial Register pursuant to the Act on Public Registers of Legal and Natural Persons.

§ 62
Relationship to the Administrative Procedure Code and Inspection Code

(1) 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

[17] Act No. 90/2012 Coll., on Commercial Companies and Cooperatives (Act on Commercial Corporations), as amended.

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) For the purpose of enforcing 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.

(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 controlled person, fails to fulfil any of the obligations under the Inspection Code[18]).

(4) The execution of a decision of the Agency imposing an obligation to hand over or otherwise dispose of information and data shall be governed by the provisions of the Administrative Procedure Code governing execution by removal of movable property.

PART TWO
COMMON AND TRANSITIONAL PROVISIONS

TITLE I
Common provisions

§ 63
Interaction

(1) The public authorities are obliged to provide the Agency without undue delay and, unless otherwise provided for in a special regulation, without payment, with suggestions, information and other forms of cooperation necessary for the exercise of their powers and for the fulfilment of the Agency's obligations under this Act. In exercising the powers conferred on the Agency by this Act, the public authorities and the Agency shall cooperate with each other, shall be entitled to request opinions on decisions prepared within the scope of their competence and shall endeavour to achieve consistency in such opinions. The public authorities and the Agency shall also, to the extent necessary for the performance of the tasks of the public authorities and the Agency, share information on cyber threats, vulnerabilities and incidents and on measures taken in response to such threats, vulnerabilities and incidents. The provisions of Article 45(2) and (3) shall not be affected.

(2) The authorities and persons who may reasonably be assumed to fulfil the criteria for the identification or designation of a regulated service are obliged to provide, without undue delay and, unless otherwise provided for in a special regulation, without payment, the information necessary to assess the fulfilment of the criteria for a regulated service and other necessary cooperation. The requested cooperation

[18)] § § 10(2) of Act No. 255/2012 Coll., on Control (Control Regulations), as amended.

need not be provided if a statutory or publicly 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) The Agency is entitled to request from the General Financial Directorate the provision of information obtained in the course of tax administration which is necessary to assess whether an institution or person fulfils the criteria for identification of a regulated service pursuant to § 3. The General Financial Directorate shall comply with the request unless the provision of the information could undermine the proper performance of tax administration. The provision of information pursuant to this provision shall not constitute a breach of the obligation of confidentiality under the Tax Code, nor shall the use of such information by the Agency pursuant to this Act constitute a breach of such 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 competence 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.

§ 64
Information obligation of the Agency

The Agency for the purpose of fulfilling its information obligation under the relevant European Union legislation)[19]

a) inform the European Commission and the Cooperation Group every 2 years of the number of regulated service providers meeting the criteria for identifying a regulated service in each sector,

b) inform the European Commission every 2 years of the number of regulated service providers meeting the criteria for designation as a regulated service in each sector, the services they provide and the criteria for which they have been designated,

c) submit a summary report to the European Union Agency for Cyber Security every 3 months, including anonymised and aggregated data on cyber security

[19)] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022.

incidents, cyber threats and significant cyber security events reported under § 16,

d) provides the European Union Agency for Cyber Security with identification data on entities providing domain name registration services and providers of regulated services referred to in § 54(3), which have their main establishment in the Czech Republic or which have a representative established in the Czech Republic,
e) provides the European Union Agency for Cyber Security with information for coordinated vulnerability disclosure,
f) inform the European Commission of the adoption of the national cyber security 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 Cyber Security with additional information and necessary cooperation.

§ 65

General and special provisions on proceedings before the Agency

(1) The provisions of the Administrative Procedure Code governing the conduct of administrative proceedings shall not apply to the procedures of the Agency pursuant to § 8, § 9, § 10 and § 11(1) and (3).
(2) Proceedings for the determination of a regulated service pursuant to § 5 may be initiated only ex officio.
(3) No appeal is admissible against the decision to determine a regulated service pursuant to § 5 and the decision to remove a regulated service provider from the register pursuant to § 11(2).
(4) If the procedure for deletion from the register of regulated service providers is to be initiated ex officio pursuant to § 11(2), the decision on deletion from the register of regulated service providers may be the first act in the procedure; in such a case, the decision shall not be made in writing, the decision on deletion shall become legally binding by a record in the file and the Agency shall delete the service provider from the register of regulated service providers.

§ 66
Protection of information

Parts of documents and records containing classified information or information the disclosure of which could jeopardise the provision of cyber security, the effectiveness of countermeasures pursuant to § 20 or measures of a general nature pursuant to § 30 shall be kept separately outside the file by the Agency in proceedings pursuant to §s 20, 30 and 31.

§ 67
Representative for the Czech Republic

(1) An entity providing domain name registration services and a regulated service provider that is a provider of a domain name resolution system (DNS) service, a provider of management and operation of an Internet top-level domain registry, a provider of a cloud computing service, a provider of a data centre service, a provider of a content delivery network (CDN) service, a provider of an online marketplace service, an Internet search engine service provider, a social network platform service provider, a managed service provider (MSP) or a managed security service provider (MSSP), which provides this service in the Czech Republic, does not have its main establishment in the European Union and has not established a representative in another Member State of the European Union, is obliged to establish a representative in the Czech Republic. A representative is a person established in the Czech Republic who has been authorised by the provider of one of the regulated services listed above to represent it in relation to its obligations under this Act. The appointment of a representative shall be without prejudice to the responsibility of the provider of the regulated service or the entity providing domain name registration services for compliance with 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 principal place of business outside the European Union 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 if the provider of any of the regulated services referred to has its principal establishment outside the European Union and has not established a representative in any Member State of the European Union.

(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 pursuant to other legislation[20]). For this purpose

a) The Agency shall allocate in its chapter budget for the relevant year the amount of funds 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 cyber emergencies and their consequences; and
b) the funds required to ensure preparation for a state of cyber emergency and its consequences, which are 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) In the case of intelligence services[21]), this Act shall apply only to the extent of the provisions of
   a) Part One to the extent of Title One, the provisions of § 8, § 9, § 10, § 11, § 12, except for the information referred to in paragraphs § 2(c), § 13, § 14, § 15, § 22 and § 24(2) and Title Four, and
   b) Part Two to the extent of § 65(1), (3) and (4).

(2) Where it is necessary to establish a regulated service provider regime for the performance of the obligation under the preceding paragraph, the intelligence service shall act as a regulated service provider under the higher obligations regime.

(3) Provisions of § 29(2) and § 63 shall apply unless the performance of these duties is prevented by a special legislation[22]) or by a statutory or State-recognised duty of confidentiality.

§ 70
Relationship to sectoral legislation of the European Union

(1) Where a directly applicable legal act of the European Union imposes obligations on authorities or persons in the area of establishing and implementing security measures or reporting cyber security incidents, and such obligations have at least comparable effect to the obligations imposed on such authorities or persons under this Act, the provisions of this Act governing the obligations to establish and implement security measures and report cyber security incidents shall not apply to

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

[21)] § 3 of Act No. 153/1994 Coll., on Intelligence Services, as amended.

[22)] For example, Act No. 153/1994 Coll., on Intelligence Services, as amended.

such authorities or persons, including the provisions on the supervision of compliance with those obligations.

(2) Provisions having comparable effect to the obligations contained in this Act under paragraph 1 shall be deemed to be those provisions of directly applicable European Union legislation which

a) in relation to the obligation to establish and implement security measures, comply at least with the requirements set out in §s 14 and 15, or

b) in relation to the obligation to report cyber security incidents, comply at least with the requirements set out in §s 16 and 17.

(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.

TITLE II
Transitional provisions

§ 71
Transitional provisions

1) Administrators of basic service information systems, administrators of information and communication systems of critical information infrastructure, administrators of major 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 fulfil the criteria of a regulated service pursuant to this Act, shall, 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 cyber security incidents and compliance with the measures of the Agency pursuant to Act No. 181/2014 Coll. as in force before the date of entry into force of this Act, in the event that it is a provider of a regulated service under the regime of higher obligations under this Act; or

b) duties related to the introduction and implementation of security measures, reporting of cyber security incidents and compliance with the measures of the Agency pursuant to Act No. 181/2014 Coll. in the wording in force before the date of entry into force of this Act, to the extent of the obligations imposed by this Act on 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, from the moment of entry into force of this Act until the expiry of the time limits for commencing the performance of obligations under this Act, except for the method of reporting cyber security incidents, which such providers of regulated services are obliged to implement under this

Act from the moment of delivery of the notification of registration in the register of providers of regulated services.

2) Proceedings relating to the fulfilment of an obligation imposed by law or on the basis of Act No. 181/2014 Coll. in the version in force before the date of entry into force of this Act shall proceed in accordance with the existing legal provisions.
3) Warnings issued pursuant to Act No. 181/2014 Coll. as in force before the date of entry into force of this Act shall be deemed to be warnings issued pursuant to this Act.
4) Reactive measures and protective measures issued pursuant to Act No. 181/2014 Coll. as in force before the date of entry into force of this Act shall be deemed to be reactive countermeasures issued pursuant to this Act.
5) The entry into force of this Act shall not affect the validity of public contracts concluded pursuant to Act No. 181/2014 Coll. before the date of entry into force of this Act.

PART THREE
FINAL PROVISIONS AND EFFECTIVENESS

§ 72
Cancellation provisions

The following are cancelled

1. Act No. 181/2014 Coll., on Cyber Security and on Amendments to Related Acts (Cyber Security Act),
2. Decree No. 82/2018 Coll., on cyber security,
3. Decree No 437/2017 Coll., on criteria for determining the operator of the basic service,
4. Decree No. 317/2014 Coll., on significant information systems and their determining criteria,
5. Decree No. 315/2021 Coll., on security levels for the use of cloud computing by public authorities,
6. Decree No. XX/XXXX Coll., on security rules for the use of cloud computing services by public authorities.

§ 73
Effectiveness

This Act shall enter into force on 18 October 2024.

Prague, dd.mm.yyyy