Government proposal

LAW

from dd.mm.yyyy ,

on cyber security

The Parliament passed the following law of the Czech Republic:

PART ONE
CYBER SECURITY

TITLE I
Basic provisions

§ 1
Subject of modification

(1) This Act regulates the rights and obligations of institutions and persons and the competence and powers of the National Office for Cyber and Information Security (hereinafter referred to as the "Office") and other public authorities in the field of cyber security.
CELEX 32022L2555

(2) This law incorporates the relevant regulation of the European Union [1)], builds on the directly applicable regulations of the European Union [2)] and regulates the provision of cyber security in the Czech Republic.
CELEX 32022L2555, 32019R0881, 32011D1104, 32021R0887 32021R0696

(3) This law does not apply to information or communication systems that handle 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 cyber security in the Union and amending Regulation (EU) No. 910/2014 and Directive (EU) 2018/1972 and repealing Directive (EU) 2016/1148 (NIS Directive 2).

[2)] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on the ENISA agency ("European Union Agency for Cyber Security"), on the certification of information and communication technology cyber security and on the repeal of 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 Competence Center for Cybersecurity and a Network of National Coordination Centres.

Regulation (EU) 2021/696 of the European Parliament and of the Council of 28 April 2021 establishing a Union Space Program and establishing a European Union Agency for the Space Program 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 of access to the public regulated service offered by the global satellite navigation system created on the basis of the Galileo programme.

§ 2
Definition of terms

(1) For the purposes of this Act,

a) asset means 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) the primary asset is information and services, whereby information also means data, including operational data, and service means processes,

c) supporting assets are employees, suppliers, buildings and technical assets,

d) technical asset means technical and software means and equipment , where technical and software means and equipment also means communication means, electronic communications networks and industrial, management or other similar specific assets,

e) a regulated service is a service whose disruption could have a significant impact on the security of important social or economic activities and for the provision of which assets are used,

f) regulated service provider means an authority or person that provides one or more regulated services,

g) cyber security management means the activity of the regulated service provider under this Act aimed at ensuring the cyber security of the regulated service .

(2) For the purposes of this Act, the following shall be understood:

a) cyberspace is a digital environment made up of assets enabling the creation, exchange and further processing of information and data,

b) information security, ensuring the confidentiality, integrity and availability of information and data,

c) cyber threat any potential circumstance, event or action that may damage, disrupt or otherwise adversely affect assets , their users or other persons , thereby causing a cyber security event or cyber security incident,

d) significant cyber threat means a cyber threat that, based on its technical characteristics, can be assumed to have the potential to seriously affect the assets of the regulated service provider or users of regulated services to the extent that it causes significant property or non-property damage,

e) k cyber security event an event that can cause a cyber security incident,

f) a cyber security incident of breach of information security within assets,

g) by managing a cyber security incident, actions leading to ensuring prevention, detection, analysis, reduction of the impact of the incident, response to the incident and subsequent recovery,

h) a significant supplier is one who enters into a legal relationship with a regulated service provider that is significant from the point of view of information security within the established scope of cyber security management,

i) a service regulated by a strategically important service, whose security breach could lead to a significant restriction or threat to services for the citizens of the state and the functioning of the state,
j) strategically important service provider means a regulated service provider that provides one or more strategically important services,
k) vulnerability a weak point in an asset or a weak point in a security measure that can be exploited by one or more threats.
CELEX 32022L2555

TITLE II
Regulated service provider

Part 1
Determination of the regulated service and the regime of the regulated service provider

§ 3
Criteria for a regulated service

A regulated service is defined by criteria for identifying a regulated service or criteria for determining a regulated service.

§ 4
Criteria for identifying a regulated service

(1) The criteria for identifying a regulated service are made up of the service criterion and the regulated service provider criterion. The criteria for identifying a regulated service shall be established by the implementing legislation.
(2) The implementing legislation sets out the criteria for identifying a regulated service in these sectors
a) public administration,
b) energy,
c) manufacturing industry,
d) food industry,
e) chemical industry,
f) water 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.
CELEX 32022L2555

§ 5
Criteria for determining the regulated service

Furthermore, a regulated service is a service established by a body or person by decision of the Office in the event that

a) it is a service specified in the implementing legislation establishing criteria for the identification of regulated services and
   1. the body or person is the only provider of this service in the Czech Republic and this service is essential for maintaining necessary social or economic activities in the state,
   2. disruption of this service could have a significant impact on public safety or public health;
   3. a disruption of this service could create significant systemic risks, particularly in industries where such a disruption could have a cross-border impact, or
   4. due to its specific importance at the regional or national level, the body or person is essential for a specific industry or type of service or for other interconnected industries in the Czech Republic,
b) its violation may cause serious interference in the lives of more than 125,000 people, through threats to life, health, property value, internal or public order, safety or the environment,
c) its violation may cause a serious interference with the ability to provide another regulated service of the same or another regulated service provider under the regime of higher obligations, or
d) the authority or person is a subject of critical infrastructure according to the legal regulation governing crisis management and critical infrastructure; in such a case, the regulated service is the service corresponding to the critical infrastructure element designated for this entity.
   CELEX 32022L2555

§ 6
Regulated service provider regime

(1) Regulated service provider regime sets the level of obligations imposed on regulated service providers under this Act.
(2) Regulated service provider mode is
   a) regime of higher duties, or
   b) regime of lower duties.
(3) The regulated service provider regime is established by implementing legislation. If an authority or person providing a regulated service is designated by a decision of the Office pursuant to § 5, it is always a regulated service provider under the regime of higher obligations.

CELEX 32022L2555

§ 7

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

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

(2) It applies that a provider of a regulated service to whom a regime of higher obligations has been established for at least one regulated service provided by him has a regime of higher obligations established and fulfills the obligations arising from this Act in the regime of higher obligations for all regulated services that he provides.

CELEX 32022L2555

§ 8

Registration of a regulated service provider

(1) The provider of the regulated service is obliged to report to the Office the fulfillment of the criteria for identifying the regulated service, by filling in the registration data in accordance with § 12 paragraph 2 letter and).

(2) The provider of the regulated service is obliged to register according to paragraph 1 no later than 30 days from the day on which it finds that the criteria for identifying the regulated service have been fulfilled, but no later than 90 days from the day on which the criteria for identifying the regulated service have been fulfilled.

(3) The Authority shall register a regulated service provider in the event that it becomes aware of the fulfillment of the criteria for identifying a regulated service according to the implementing legislation and the regulated service provider does not register according to paragraph 1 within the period according to paragraph 2.

(4) The Office will further register a provider of a regulated service or a regulated service based on the Office's decision to determine a regulated service pursuant to § 5. In the event that, as a result of the decision pursuant to the previous sentence, the regime of the provider of the regulated service changes from a regime of higher obligations to a regime of lower obligations, new deadlines for starting the fulfillment of obligations according to § 12 paragraph 3, § 14 paragraph 3 and § 16 paragraph 4 do not apply.

CELEX 32022L2555

§ 9

Change of registration of a regulated service provider

(1) The provider of the regulated service is obliged to change the registration of the provider of the regulated service if the criteria for the identification of each other

regulated service are met and to proceed similarly according to Section 8, paragraphs 1 and 2.

(2) The provider of a regulated service is obliged, in the event that, within the framework of fulfilling the criteria for identifying a regulated service, there is a change in the regime of the provider of the regulated service, to change the registration of the provider of the regulated service and to proceed similarly according to § 8, paragraphs 1 and 2. When changing the regime of the provider of a regulated service from from the regime of higher obligations to the regime of lower obligations, the new deadlines for starting the fulfillment of obligations according to § 12 paragraph 3, § 14 paragraph 3 and § 16 paragraph 4 do not apply.

§ 10

Enrollment in the register of providers of regulated services

(1) The Office shall without undue delay enter the regulated service provider and the regulated service in the register of regulated service providers based on the registration of the regulated service provider or the change in the registration of the regulated service provider pursuant to § 8 and § 9. The Office shall notify the regulated service provider of this fact in writing.

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

CELEX 32022L2555

§ 11

Deletion from the register of providers of regulated services

(1) If the Office learns that a provider of a regulated service registered in the register of regulated service providers on the basis of registration pursuant to § 8 paragraphs 1 and 3 or § 9 paragraph 1 no longer provides a service that meets the criteria for identifying a regulated service according to the implementing legislation, the Office registered regulated service delete from the register of providers of regulated services and notify the providers of regulated services in writing of this fact.

(2) If the Authority learns that the regulated service provider, whose service was determined by the Authority's decision pursuant to § 5, no longer provides a service that meets the criteria for determining a regulated service, the Authority will decide that the service provided by the regulated service provider does not meet the criteria for determining a regulated service . After the decision becomes legally binding, the Office will 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 Office learns that a body or person registered in the register of regulated service providers no longer provides any service that meets the criteria for identifying a regulated service or a service determined by the Office's decision to meet the criteria for determining a regulated service, the Office will delete this body or person from the register of regulated service providers and o this body or person shall notify this fact in writing.

Part 2
Obligations of the regulated service provider

§ 12
Data reporting by the regulated service provider

(1) The provider of the regulated service reports registration, contact and other supplementary data and their changes to the Office. The provider of the regulated service is responsible for the correctness and completeness of the reported data.

(2) The reported data 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 data, which means information related to the identification of natural persons who are authorized to act on behalf of the regulated service provider in matters regulated by this Act, and

c) supplementary data, which are additional information needed for the performance of the Office's activities pursuant to this Act.

(3) The provider of the regulated service is obliged to report the data according to paragraph 2 letter b) and c) for each regulated service no later than 30 days from the date of delivery of the written notification of its registration in the register of regulated service providers pursuant to § 10, paragraph 1.

(4) The provider of the regulated service is obliged to report changes only to those data according to paragraph 2, which are not reference data kept in basic registers, no later than 15 days after their change.

(5) The provider of the regulated service is obliged to ensure sufficient representation of natural persons who are authorized to act on behalf of the provider of the regulated service in matters regulated by this law.

(6) The content, format and method of reporting registration, contact and additional data shall be determined by an implementing legal regulation.

CELEX 32022L2555

§ 13
Determination of the scope of cyber security management by the regulated service provider

(1) Regulated service provider
   a) identifies all primary assets within the entire organization,
   b) shall determine which primary assets identified under letter a) are related to the provision of a regulated service,
   c) for primary assets determined under letter b) identify and determine the related organizational parts of the organization and supporting assets.

(2) Organizational parts and assets identified according to paragraph 1 letter b) and c) form the scope of cyber security management (hereinafter referred to as the "specified scope").

(3) The provider of the regulated service shall keep a documented record of the identification and determination of organizational parts and assets pursuant to paragraph 1, including records of primary assets that were removed from the specified scope and the justification for their removal.

(4) Until the fulfillment of the obligations under paragraphs 1 and 3, it is considered that the specified scope consists of the regulated service of the provider of the regulated service, and the supporting assets are all the supporting assets of the organization and other supporting assets related to the provision of the regulated service.

(5) Assets that have not yet been identified and determined under paragraph 1 or included in the determined scope under paragraph 4 are considered to be part of the determined scope until such changes are included in the process of identifying and determining the organizational parts and assets forming the determined scope under paragraph 1 and there is no documented record of them according to paragraph 3.
CELEX 32022L2555

§ 14
Safety measures

(1) Security measures are actions aimed at ensuring the proper provision of a regulated service and the cyber security of assets. Security measures are organizational and technical measures.

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

(3) The provider of a regulated service shall begin fulfilling the obligation to introduce and implement security measures pursuant to paragraph 2 for each regulated service no later than 1 year from the date of delivery of written notification of its registration in the register of providers of regulated services pursuant to Section 10, paragraph 1.

(4) The implementing legislation establishes security measures corresponding to the regulated service provider's regime.
CELEX 32022L2555

§ 15
List of security measures

(1) For providers of regulated services in the regime of higher obligations, they are
   a) organizational measures
      1. information security management system,
      2. responsibilities of senior management,
      3. security roles,
      4. security policy management and security documentation,
      5. asset management,
      6. risk management,
      7. supplier management,
      8. security of human resources,
      9. change management,
      10. acquisition, development and maintenance,
      11. access control,
      12. managing cyber security events and cyber security incidents,
      13. business continuity management a
      14. cyber security audit,
   b) technical measures
      1. physical security,
      2. security of communication networks,
      3. identity management and verification,
      4. control of access rights,
      5. detection of cyber security events,
      6. recording 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, management and similar specific technical assets.

(2) For providers of regulated services in the regime of lower obligations, they are security measures
   a) ensuring a minimum level of cyber security,
   b) responsibilities of senior management,
   c) risk management,
   d) security of human resources,
   e) business continuity management,
   f) access control,
   g) identity management and their authorization,

h) detection and recording of cyber security events,
i) solving cyber security incidents,
j) security of communication networks,
k) application security and
l) cryptographic algorithms.
CELEX 32022L2555

§ 16
Reporting of cyber security incidents

(1) The provider of a regulated service in the regime of higher obligations is obliged to report to the Office all cyber security incidents originating in cyberspace within the specified scope.
(2) The provider of the regulated service in 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 to the National CERT within the 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 in the regime of lower obligations is determined by the implementing legislation.
(4) The provider of the regulated service shall begin fulfilling 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 delivery of the written notification of its registration in the register of regulated service providers pursuant to § 10, paragraph 1.
(5) An authority or person can voluntarily report cyber security incidents, especially those where intentional culpability can be inferred, as well as report cyber security events or cyber threats via the Office's website. Vulnerabilities can also be reported anonymously through the Office's website, especially for the purpose of ensuring the coordinated publication of vulnerabilities by the Government CERT. This does not affect the obligation of the provider of the regulated service according to paragraphs 1 and 2.
(6) This provision does not affect the obligation to provide information pursuant to another legal regulation or a directly applicable regulation of the European Union governing the protection of personal data.
CELEX 32022L2555

§ 17
Requirements for reporting cyber security incidents

(1) The regulated service provider shall, without undue delay after discovering a cyber security incident, but no later than within 24 hours, submit an initial report to the Authority or the National CERT, stating whether it believes that the cyber

security incident was caused by an illegal or arbitrary intervention or that it could have a cross-border impact .

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

(3) In the case of reporting a cyber security incident with a significant impact on the provision of a regulated service pursuant to Section 16, paragraph 2, or on the state's cyber space pursuant to paragraph 2, the provider of the regulated service shall, beyond the scope of the initial report pursuant to paragraph 1, submit to the Office or the National CERT

a) without undue delay, but no later than 72 hours after the detection of a cyber security incident, a notification updating the information referred to in paragraph 1, presenting an initial assessment of the cyber security incident and indicating the impact and indicators of compromise, if available; provider of trust-building services [3)] submits a notification under this letter within 24 hours of becoming aware of this cyber security incident,

b) at the request of the Authority or the National CERT, an ongoing report on significant changes in the state of cyber security incident management, and

c) no later than 30 days after submission of the notification under letter a) a final report; in the event that the cyber security incident is still ongoing after the expiration of the specified period, the provider of the regulated service shall submit, without undue delay, an interim report on the current status of the management of the cyber security incident and then a final report no later than 30 days after the resolution of the cyber security incident.

(4) The provider of the regulated service reports cyber security incidents, including voluntary reports under this Act, through the NÚKIB Portal. If the NÚKIB Portal cannot be used, the provider of the regulated service in the regime of higher obligations will send a report to the Office's e-mail address designated for receiving reports of cyber security incidents, or to the Office's data box . -In such a case, the provider of the regulated service in the regime of lower obligations will send the report to the National CERT e-mail address designated for receiving reports of cyber security incidents, or to its data box.

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

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

CELEX 32022L2555

§ 18
Handling cyber security incidents

(1) The Authority or the National CERT shall provide the regulated service provider with its statement on the cyber security incident without undue delay, no later than 24 hours after receiving the initial report pursuant to Section 17.
(2) At the request of the affected provider of the regulated service, the Office or the National CERT will provide methodological support for the implementation of possible mitigating measures, and any other technical support for managing a reported cyber security incident with a significant impact on the provider of the regulated service or on the cyberspace of the state.
(3) Everyone is obliged to provide, at the request of the Office, the necessary information and other necessary cooperation in managing a cyber security incident, if the intended purpose cannot be achieved otherwise or its achievement would otherwise be significantly more difficult. The requested cooperation may not be provided if it is prevented by a legal or state-recognized obligation of confidentiality or the fulfillment of another legal obligation.
(4) Data on cyber security incidents, events, cyber threats and vulnerabilities are kept in records according to § 45.
(5) Paragraphs 1 to 4 apply mutatis mutandis when dealing with cyber security incidents reported voluntarily in accordance with § 16, paragraph 5.
CELEX 32022L2555

§ 19
Information obligation of the regulated service provider

(1) If the provider of the regulated service considers it appropriate, it will notify the users of the regulated service without undue delay of a cyber security incident with a significant impact that could negatively affect the provision of this service. The Authority is authorized to impose on the provider of a regulated service that is affected by a cyber security incident with a significant impact, the obligation to inform users of the regulated service about this incident. In the decision to impose this obligation, the Office determines the scope of the information obligation.
(2) The provider of the regulated service is obliged, without undue delay, to inform the user of the regulated service who may be affected by a significant cyber threat in an appropriate and comprehensible manner about such steps that the user can take in response to this threat, so that the possible impact of its implementation on this user is as small as possible . Where possible and appropriate, the regulated service provider shall also inform the user of this significant cyber threat.
CELEX 32022L2555

§ 20
Countermeasures

(1) Countermeasures are actions that are needed to protect assets from a cyber threat or vulnerability in the field of cyber security or from a cyber security incident, or to deal with a cyber security incident that has already occurred.

(2) Countermeasures are
   a) warning,
   b) warning a
   c) reactive countermeasures.

(3) Unless the Office stipulates otherwise in the countermeasure, the provider of the regulated service is obliged to notify the Office of the implementation of the countermeasure and its result without undue delay, but no later than within the time limit set by the countermeasure . The content, format and method of notification shall be determined by the implementing legal regulation. Everyone is obliged to provide the Office with the necessary cooperation in providing documents for the issuance of countermeasures. The requested cooperation may not be provided if it is prevented by a legal or state-recognized obligation of confidentiality or the fulfillment of another legal obligation.
   CELEX 32022L2555

§ 21
Warning

(1) After consultation with the regulated service provider concerned, for reasons of protection of internal or public order and security, protection of life and health of persons or protection of the state's economy, the Office is entitled to inform the public about a cyber security incident or a violation of the obligations set out in this Act, or to impose a decision on the concerned regulated service provider to do so himself.

(2) The Office informs the public about the facts according to paragraph 1 through its website.

(3) The decision of the Office according to paragraph 1 can be the first act in the proceedings and the resolution against it does not have a suspensive effect.
   CELEX 32022L2555

§ 22
Warning

(1) The Authority will issue a warning if it becomes aware of a serious cyber threat or cyber security vulnerability.

(2) The provider of the regulated service in the regime of higher obligations will take into account the warning within the set scope, unless the Office or another legal regulation stipulates otherwise.

(3) Warning The Office will notify the affected regulated service providers and publish it on the Office's official board. The Office will not publish a warning if its publication could jeopardize the provision of cyber security, the effectiveness of countermeasures issued pursuant to this law, other legitimate interests of the state, or if it could be used to identify the body or person who reported the cyber threat, vulnerability or related cyber security incident .
CELEX 32022L2555

§ 23
Reactive countermeasures

(1) The Authority will issue a decision imposing an obligation on the provider of the regulated service to implement reactive countermeasures
   a) to address an imminent or ongoing cyber security incident,
   b) to secure assets against a cyber security incident, or
   c) in order to increase asset protection based on the analysis of an already resolved cyber security incident.
(2) The provider of the regulated service is obliged to implement reactive countermeasures within the specified scope, unless the Office or another legal regulation stipulates otherwise.
(3) The decision on the obligation to implement reactive countermeasures can be the first step in the procedure. If the decision cannot be delivered to the addressee within 72 hours of its issuance, it will be delivered to him by posting it on the official board of the Office and it will be enforceable at that moment. The Office can also issue a decision according to the first sentence in on-site proceedings according to the administrative regulations. Dissolution filed against the decision according to paragraph 1 does not have a suspensory effect.
(4) If the countermeasure pursuant to paragraph 1 is intended to concern a more precisely defined range of authorities or persons, the Office shall issue it in the form of a measure of a general nature.
(5) The measure of a general nature according to paragraph 4 becomes effective the moment it is posted on the Office's official board; the provisions of § 172 of the Administrative Code do not apply. The Office will also notify the providers of the regulated service affected by the issuance of measures of a general nature.
(6) The affected provider of a regulated service or anyone who proves that his rights, obligations or interests may be directly affected by a measure of a general nature may submit comments to a measure of a general nature issued pursuant to paragraph 4 within 30 days from the date of its posting on the Office's official board. The Office can change or cancel measures of a general nature on the basis of comments submitted.
CELEX 32022L2555

Part 3
Relationship between the regulated service provider and its suppliers

§ 24
Management of suppliers and relation to the awarding of public contracts

(1) The provider of the 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 into account the requirements arising from security measures in the contracts with its suppliers.
(3) Taking into account the requirements arising from security measures when choosing a supplier to the extent necessary to fulfill the obligations under this Act cannot be considered an illegal restriction of economic competition or an unjustified obstacle to economic competition.
CELEX 32022L2555

§ 25
Special arrangement for the transfer of information and data from a significant supplier

(1) In the event of an imminent cyber security incident, at the initiative of a regulated service provider in the regime of higher obligations, who has unsuccessfully called on a significant supplier to fulfill its contractual obligation to hand over information and data, the Authority may, by decision, impose on the significant supplier the obligation to hand over to the provider of a regulated service in the regime of higher obligations information and data related to operation of assets used to provide a regulated service. If a significant supplier does not have information or data related to the operation of assets used to provide a regulated service or, given the factual circumstances, it is not expedient to require it to take measures and release them, the Office may also impose the obligation according to the previous sentence on another body or person who possesses the required information and data . In the decision, the Authority can determine the format, scope, method and deadline of the transfer and establish the obligation to safely dispose of this information and data and their copies after the transfer.
(2) The initiative according to paragraph 1 must contain the justification of the request with regard to the imminent cyber security incident, a detailed description of the previous negotiations between the significant supplier and the regulated service provider in the regime of higher obligations, especially with regard to the non-fulfillment of the contractual obligation of the significant supplier and the possible consequences if the requested information is not handed over and data.
(3) The decision to impose the obligation to transfer information and data according to paragraph 1 may be the first act in the procedure. Dissolution against the decision according to the first sentence does not have a suspensory effect.

(4) Negotiating the payment of costs incurred for the transfer of information and data must not be an obstacle to the proper fulfillment of the obligation to transfer information and data.
CELEX 32022L2555

Part 4
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 determining a strategically important service.
CELEX 32022L2555

§ 27
Criteria for identifying and determining a strategically important service

(1) The implementing legislation establishes the criteria for identifying a strategically important service in sectors
   a) public administration,
   b) energy,
   c) transportation and
   d) digital infrastructure and services.
(2) Furthermore, a strategically significant service is a regulated service provided by the regulated service provider under the regime of higher obligations by decision of the Office 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 .
CELEX 32022L2555

Part 5
Supply Chain Security Screening Mechanism

Examination of risks associated with the supplier
§ 28

(1) The Office collects and evaluates information and data related to an authority or person, which relate to a possible threat to the security of the Czech Republic, internal or public order or fulfillment of the supplier's riskiness criteria.
(2) Activities according to paragraph 1 are prioritized by the Office according to an approach based on risks and available capacities.
(3) For the needs of the supply chain security screening mechanism, it is understood

a) the critical part of the defined scope of assets of the defined scope of strategically important services, for which the provider of strategically important services, in accordance with the procedure according to the implementing legislation, has assessed the impact of information security violations on the defined scope of strategically important services as high or critical; the critical part of the specified scope is always at least the assets of the specified scope of strategically important services that ensure indispensable functions of the specified scope determined by the implementing legislation,

b) safety-significant delivery of performance aimed at the critical part of the specified scope consisting of provision, development, production, assembly, management, operation or service

1. technical means or equipment with computing capacity,
2. software or equipment, or
3. information or communication services,

c) the supplier of safety-relevant supply is the one who provides the provider of a strategically significant service directly or as a subcontractor with a safety-relevant supply.

(4) Indispensable functions of the specified scope and criteria of the supplier's riskiness and the method of their evaluation are determined by the implementing legislation.
CELEX 32022L2555

Section 29

(1) The Ministry of Industry and Trade, the Ministry of Foreign Affairs and the Ministry of the Interior, for the purpose of carrying out activities pursuant to Section 28, paragraph 1, shall provide the Office at its request without undue delay, but no later than within 30 days, with an opinion on the fulfillment of the supplier's riskiness criterion by a specific body or person, information or other cooperation .

(2) The Supreme State Attorney's Office, the Police of the Czech Republic, the Office for the Protection of Economic Competition, the Financial Analytical Office and the intelligence services of the Czech Republic shall provide the Office at its request without undue delay, but within 30 days at the latest, with the required information or other cooperation.

(3) If the Office does not obtain from its own activities or by the procedure according to paragraphs 1 and 2 the information necessary for the performance of activities according to § 28 paragraph 1, authorities and persons not mentioned in paragraphs 1 and 2 will provide this information or other cooperation based on the request of the Office.

(4) Providing information under this provision is not a breach of confidentiality under any other law. This does not affect the lawyer's obligation of confidentiality according to the legal regulation governing the practice of advocacy.

§ 30
Limitation of risks associated with the supplier

(1) The Authority shall issue a measure of a general nature, which sets the conditions or prohibits the use of the supplier's performance of a security-important supply in a critical part of the specified scope, if it detects a possible significant threat to the security of the Czech Republic or internal or public order based on the evaluation of the supplier's riskiness criteria. The deadline for taking into account the conditions or the prohibition contained in a measure of a general nature is determined by the Office, taking into account their impact on the provider of a strategically important service.

(2) Draft measures of a general nature pursuant to paragraph 1 The Office, after discussion with the other bodies listed in § 29 paragraphs 1 and 2 and the Ministry of Finance, will submit to the State Security Council

a) for information, if the deadline for taking into account the conditions or the prohibition contained in the measure of a general nature for the current or past performance of the supplier of a safety-relevant supply

1. is determined according to the depreciation period according to the legal regulation governing income taxation [4)], if this legal regulation stipulates it in relation to the security-important supply in question, or
2. is at least 5 years old, or

b) to be discussed, if the deadline for taking into account the conditions or the prohibition contained in the measure of a general nature for the current or past performance of the supplier of safety-relevant supplies

1. it is not determined according to the depreciation period according to the legal regulation governing income taxation [4)], if this legal regulation stipulates it in relation to the relevant safety-related delivery, or
2. is less than 5 years.

(3) After informing the members of the State Security Council according to paragraph 2 letter a) or after discussion according to paragraph 2 letter b) The Office shall deliver a draft measure of a general nature by public decree and invite the supplier against whom 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 30 days, unless the Office stipulates otherwise. The provisions of § 172 paragraphs 1 and 5, § 173 paragraph 1 of the first sentence, the part of the sentence after the semicolon, and § 173 paragraph 1 of the second sentence of the Administrative Code shall not be used for the procedure according to this provision.

(4) At least once every 3 years, the Office shall review the duration of the facts on the basis of which the measure of a general nature was issued pursuant to paragraph 1. If the Office finds that these facts have passed, it shall cancel the measure of a

[4)] Act No. 586/1992 Coll., on income taxes, as amended.

general nature pursuant to paragraph 1 following the procedure pursuant to paragraphs 1 and 2 similarly .
CELEX 32022L2555

§ 31
Exceptions to the limitation of risks associated with the supplier

(1) The Office may, if the nature of the given threat to the security of the Czech Republic or internal or public order permits, allow an exception to the conditions or prohibitions set by a measure of a general nature pursuant to § 30, if the implementation of a measure of a general nature by the provider of a strategically important service could substantially threaten the provision of a strategically important service .
(2) Proceedings for granting an exemption under paragraph 1 can be initiated at the request of the provider of a strategically important service or ex officio. The applicant is obliged to attach evidence proving the facts he is referring to in the application.
(3) In the decision on granting the exception, the Office shall determine the conditions for its application. In the event of a serious violation of the conditions for the application of the exception or in the event of the lapse of the reason for which it was granted, the Office shall cancel the exception by decision.
(4) The Office will not grant an exception if it would completely defeat the purpose of the general measure pursuant to Section 30 .
CELEX 32022L2555

§ 32
Obligations associated with checking the security of the supply chain

(1) The provider of a strategically important service is obliged
   a) to ascertain, with reasonable efforts, information about suppliers of safety-relevant supplies and record this information at least to the extent of identifying all safety-relevant supplies and the suppliers of safety-relevant supplies that provide them, and
   b) report to the Office the information according to letter a) and their changes within 10 days of their discovery; the content requirements, format and method of reporting are determined by the implementing legal regulation .
(2) The provider of a strategically significant service shall begin fulfilling the obligation to report information pursuant to paragraph 1 for each strategically significant service no later than 1 year from the date of delivery of written notification of its entry in the register of regulated service providers pursuant to Section 10, paragraph 1.
(3) Information reported to the Office pursuant to paragraph 1 letter b) and paragraph 2 and the information determined by the procedure according to § 28 and § 29 are part of the records of suppliers of safety-relevant supplies.

CELEX 32022L2555

§ 33

Limitation of risks associated with the supplier in public contracts

The provider of a strategically important service in the position of the contracting authority according to the legal regulation governing the awarding of public contracts may terminate the obligation from the contract for a public contract without undue delay after discovering that its performance cannot be continued without violating the measures of a general nature according to § 30.
CELEX 32022L2555

Part 6

Ensuring the availability of a strategically important service

Section 34

(1) The provider of a strategically important service is obliged to ensure the availability of a strategically important service within the scope of the critical part of the specified scope in 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 in the scope of a 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 fulfill the obligations set out in paragraphs 1 and 2 for each strategically important service no later than one year from the date of delivery of the notification on the registration of the strategically important service in the register of regulated service providers or from the delivery of the decision on the designation of the strategically important service pursuant to § 27 par. 2.
(4) The specified time and quality of the service are determined by the provider of the regulated service depending on the objectives of managing the continuity of activities according to the implementing legislation.
(5) For the purposes of this provision, the critical part of the specified scope is defined in § 28 paragraph 3 letter and).
CELEX 32022L2555

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 Office without undue delay, but no later than within 30 days from the day on which it started providing the domain name registration service, in the manner established by the implementing legal regulation
   a) entity name,
   b) the address of the main place of business and its other places of business in the territory of the member states of the European Union, or the representative of the entity according to § 67,
   c) current contact information, including e-mail addresses and telephone numbers of the subject, or his representative according to § 67,
   d) member states of the European Union in which the entity provides its services and
   e) the subject's public IP address range.

(2) In the event of changes in the data reported pursuant to paragraph 1, the entity providing domain name registration services shall update the reported data without undue delay, but no later than 90 days from the date of the change.
CELEX 32022L2555

Section 36

(1) The entity managing 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 laws governing the protection of personal data in respect of data that is personal data.

(2) The database according to paragraph 1 contains the information necessary to identify and contact domain name holders and contact points managing top-level domains, in particular
   a) domain name,
   b) Registration date,
   c) name of the registrant,
   d) e-mail address of the registrant,
   e) phone number of the registrant,
   f) the email address and telephone number of the point of contact managing the domain name, if different from the registrant.

(3) The entity managing and operating the registry of Internet top-level domains 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. These policies and procedures are publicly available.

(4) its registration data, which are not personal data, without undue delay after the registration of the domain name .

(5) The entity managing and operating the internet top-level domain registry and the entity providing domain name registration services provide access to specific domain name registration data based on lawful and duly justified requests from authorized access applicants in accordance with European Union legislation governing the protection of personal data, namely without undue delay, no later than 72 hours from the request for access. The policies and procedures for disclosing this data are publicly available.
CELEX 32022L2555

TITLE IV
Other tools for ensuring cyber security

§ 37
Exemption from the right to information

Information , the disclosure of which could threaten the provision of cyber security or the effectiveness of countermeasures issued pursuant to this Act, or information that is kept in the registers kept by the Office under § 45, is not provided in accordance with the legal regulations governing free access to information.

§ 38
State of cyber danger

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

§ 39
Declaration of a state of cyber danger

(1) The state of cyber danger can only be declared with the reasons and for the necessary period. The state of cyber danger is announced by the Director of the Office. The director of the Office immediately informs the government about the declaration of a state of cyber danger. A state of cyber danger can be declared for a maximum period of 30 days. This period can be extended by the Director of the Office only with the approval of the Government.

(2) The decision to declare a state of cyber danger must contain measures to deal with the state of cyber danger and their scope. The decision is published on the Office's official board and in other appropriate ways, especially through mass information media. The operator of a nationwide television or radio broadcast is obliged, based on the Office's request, to publish information on the declaration of a state of cyber danger immediately and without modification of the content and meaning. The decision becomes effective at the moment specified in it. A change in measures to address the state of cyber danger must be announced in a similar manner to the state of cyber danger.

(3) The state of cyber danger ends with the expiration of the period for which it was declared, unless the director of the Office or the government decides to cancel it before the expiration of this period. The government will also cancel the state of cyber danger if the conditions for declaring it are not met. The decision of the director of the Office or the government to cancel the state of cyber danger will be published on the official board of the Office and in other appropriate ways, especially through mass information media. This decision becomes effective at the time specified in it.

(4) If it is not possible to expediently avert the threat that has arisen within the framework of the state of cyber danger, the director of the Office will immediately request the government to declare a state of emergency. The validity of the measures to deal with the state of cyber danger announced by the director of the Office ends on the day the state of emergency is declared, unless the government decides otherwise. Measures to address the state of cyber danger, the validity of which will remain in force, are further considered emergency measures ordered by the government.

(5) Administrative regulations do not apply to decision-making and imposition of obligations under this Act during the state of cyber danger.

§ 40
Measures to address the state of cyber danger

(1) The Director of the Office is authorized during the state of cyber danger for the purpose of solving it

a) to provide material resources in the property of the Czech Republic, which are used by the Office, and which are necessary to solve a cyber security incident, or to secure assets against an imminent cyber security incident,

b) to request from authorities and persons information on material means, on production, operational and personnel capacities and on the volume of stocks in the specified types of material, while these authorities and persons are obliged to provide the Office with the required information completely and truthfully within the deadline set by the Office,

c) on the basis of a contract or record on the sharing of personnel capacities and material resources, request the preferential provision of personnel capacities or material resources and use these personnel resources and material resources,

while the requested authorities and persons are obliged to comply with the Office's request,

d) order work in standby mode,

e) to prohibit authorities and persons who have been invited to do so by the Office from using technical assets in the event that such assets are immediately threatened by a cyber security incident that may significantly damage or destroy them, or are already affected by such an incident,

f) to impose on authorities or persons the obligation to take measures to solve a cyber security incident or to secure assets against a cyber security incident and to notify the Office of the implementation of the measures and its result,

g) order authorities and persons to perform a vulnerability scan or penetration test, or

h) order authorities and persons to make available non-public communication networks in their administration for the needs of the Office.

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

a) to fulfill the measures used to solve and correct the state of cyber danger,

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

c) provide cooperation in publishing information about the state of the cyber threat, or

d) provide collaboration in addressing and remediating the cyber threat situation.

TITLE V
Performance of state administration

Part 1
Institutions involved in the performance of state administration in the field of cyber security

§ 41
National Office for Cyber and Information Security

(1) The Office is the central administrative office for the area of cyber security and for selected areas of classified information protection pursuant to the Act on the Protection of Classified Information and Security Competence. Through its activities, the Office participates in strengthening the security and resilience of the Czech Republic in cyberspace. The seat of the Office is Brno. The Office's income and expenses form a separate chapter of the state budget.

(2) The Office 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, which also dismisses him. The Director of the Office is responsible to the Prime Minister or an authorized member of the Government.

(3) Office

a) receives information on the fulfillment of the criteria for identifying a regulated service and registers regulated service providers,
b) determines the regulated service provider by decision and the regulated service if it fulfills the criteria for determining the regulated service,
c) determines by decision a strategically important service according to § 27 paragraph 2,
d) registers the regulated service provider in the register of regulated service providers and deletes the regulated service provider from this register,
e) changes the regime of the regulated service provider by decision in specified cases,
f) receives reports of registration, contact and additional data and their changes,
g) establishes security measures corresponding to the regime of the provider of the regulated service,
h) manages and operates the NÚKIB Portal,
i) informs the public about a cyber security incident in accordance with the procedures under this Act ,
j) issues countermeasures and receives notification of their implementation and outcome,
k) keeps records and lists in accordance with this Act and in accordance with legal regulations governing the protection of classified information ,
l) issues a decision on the obligation to hand over information and data related to the operation of assets used to provide the regulated service to the regulated service provider under the regime of higher obligations,
m) collects and evaluates information and data according to § 28 paragraph 1,
n) by measures of a general nature, it establishes conditions or prohibits the use of the supplier's performance of safety-relevant supplies in the critical part of the specified scope ,
o) reviews the duration of the facts on the basis of which a measure of a general nature was issued pursuant to letter n),
p) decides on requests for exemption and allows exemption from conditions or prohibitions set by measures of a general nature pursuant to Section 31,
q) negotiates with authorities and persons contracts and records on the sharing of personnel capacities and material resources for the purpose of fulfilling the legal powers of the Office ,
r) declares, manages and coordinates the state of cyber danger, imposes obligations and takes measures to avert the state of cyber danger and acts as a coordinating body in the state of cyber danger,
s) during the state of cyber danger, announces measures designed to solve and correct the state of cyber danger,
t) continuously prepares to ensure preparedness for solving and correcting the state of cyber danger,
u) concludes a public contract with the operator of the National CERT,
v) conducts inspections of the fulfillment of obligations under this Act and imposes corrective measures,

w) imposes administrative sanctions for non-compliance with the obligations stipulated by this Act and the Act on the Protection of Classified Information and on Security Qualification,

x) carries out control of the fulfillment of obligations under this Act and provides other necessary cooperation based on the request of the supervisory authority of another Member State,

y) issues a decision on the suspension of the validity of the European cyber security certificate or on the obligation of the conformity assessment entity to suspend the validity of the certificate or certificate according to § 60, and

z) submits a proposal to the court to suspend the performance of the management function pursuant to § 61 and issues a certificate under the same provision.

(4) Authority further

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

b) prepares and submits to the government for approval a national cyber security strategy and an action plan for its fulfillment and updates this strategy at least every 5 years,

c) performs state administration in the field of security of information and communication systems dealing with classified information and in the field of cryptographic protection, ensures the activities of the National Center for Communication Security, the National Center for the Distribution of Cryptographic Material, the National Center for Measuring Compromising Radiation and the National Center for the Security of Information Systems, which are part of it,

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

1. cooperates with authorities and persons who operate in these areas and in the field of cyber defense, especially with public corporations, research and development workplaces and with other CERT-type workplaces,
2. ensures international cooperation and negotiates and concludes agreements on international cooperation,
3. perform other tasks in accordance with the obligations resulting from the Czech Republic's membership in the European Union, the North Atlantic Treaty Organization and international treaties to which the Czech Republic is bound,
4. ensures prevention, education and methodical support and
5. provides research and development,

e) in accordance with the legal regulation governing crisis management and critical infrastructure, determines elements of critical infrastructure in the field of communication and information systems in the field of cyber security or sends to the Ministry of the Interior a draft of elements of critical infrastructure in the field of communication and information systems in the field of cyber security, the operator of which is an organizational unit of the state, and verifies their relevance every 2 years,

f) fulfills obligations towards the European Commission, the European Union Agency for Cyber Security, the Cooperation Group, the CSIRT Network, the European Network of Liaison Organizations for Cybercrisis Solutions and other entities according to the relevant regulation of the European Union,

g) is a 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 regulation of the European Union,

h) if necessary, participates in the peer review process according to the relevant regulation of the European Union,
CELEX 32022L2555

i) exercises its powers in the area of the public regulated service of the European Galileo satellite navigation program, in particular performs the functions of the relevant PRS authority according to Article 5 of Decision No. 1104/2011/EU of the European Parliament and of the Council,
CELEX 32011D1104

j) exercises jurisdiction in sub-areas related to security within the framework of the Union Space Program pursuant to Regulation No. 2021/696 of the European Parliament and of the Council,
CELEX 32021R0696

k) is a national cybersecurity certification body pursuant to Article 58 of the Cybersecurity Act,
CELEX 32019R0881

l) acts as the National Coordination Center for research and development in the field of cyber security for the Czech Republic according to the directly applicable regulation of the European Union [5)],
CELEX 32021R0887

m) establishes and supports platforms used to share information in the field of cyber security and establishes rules for their operation,
CELEX 32022L2555

n) publishes the Bulletin of the Office, which it publishes on its website and

o) performs other tasks stipulated by this Act and the Act on the Protection of Classified Information and on Security Qualification.

(5) Government CERT as part of the Authority

a) provides solutions, coordination, analysis and preventive action against
   1. cyber security threats,
   2. cyber security vulnerabilities, including vulnerability scanning,
   3. cyber security events and
   4. cyber security incidents, including their management,

b) acts as a point of contact for providers of regulated services in the regime of higher obligations,

c) tests the implementation and resilience of asset security, including performing penetration testing with the consent of the authorities or persons concerned,

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

d) is a 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 consultations to authorities and individuals in the field of cyber security,
h) receives and evaluates initiatives in the field of cyber security from authorities and persons,
i) can share data and information from its activities and from records kept by the Office with authorities and persons, if this is necessary for ensuring cyber security; if the Government CERT determines the level of protection of such shared information, authorities and persons are obliged to comply with this level of protection,
j) fulfills the role of the CSIRT team according to the relevant regulation of the European Union and represents the Czech Republic and participates in the functioning of relevant international groupings and associations in the field of cyber security, including the CSIRT Network,
k) in appropriate cases, forward without undue delay information on a cyber security incident with a significant impact concerning two or more Member States reported under § 16 and § 17 to the affected Member States and the European Union Agency for Cyber Security, while maintaining the confidentiality of the information provided, security and commercial interests reporting entity,
l) is involved in the research and development of cyber security tools and solutions and
m) prioritizes the provision of its services and the performance of its activities according to an approach based on risks and available capacities.
CELEX 32022L2555

§ 42
Operator of the National CERT

(1) The operator of the National CERT can only be a legal entity that
a) does not carry out or has not carried out activities against the interests of the Czech Republic in the sense of legal regulations governing the protection of classified information,
b) manages and operates relevant technical assets or participates in their management and operation, for at least 5 years,
c) has the technical prerequisites to perform activities according to paragraph 3,
d) is a member of a multinational organization operating in the field of cyber security,
e) does not have a due tax arrears recorded in the tax records in the Czech Republic and does not have a due arrears of insurance premiums or penalties for public health insurance and insurance premiums or penalties for social

security or contributions to the state employment policy due in the Czech Republic,

f) has not been legally convicted of the crime specified in § 7 of the Act on the Criminal Liability of Legal Entities and Proceedings against them,

g) is not a foreign person according to another legal regulation,

h) was not founded or established solely for the purpose of making a profit; this does not affect the possibility of the operator of the National CERT in his own name and on his own responsibility to carry out other economic activities in the field of cyber security not regulated by this Act, as long as this activity does not interfere with the fulfillment of the obligations specified in paragraph 3 and

i) concluded a public contract with the Office pursuant to Section 52 .

(2) The interested party proves the fulfillment of the conditions by submitting

a) sworn declaration in the case of paragraph 1 letter a) to d), g) and h) from the content of which it must be clear that the applicant meets the relevant prerequisites, a

b) confirmation of 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 in the case of paragraph 1 letter e), which must not be older than 30 days.

(3) The operator of the National CERT performs the activities of the National CERT, which

a) ensures the sharing of information on a national and international level in the field of cyber security to the extent according to this law and acts as a point of contact for providers of regulated services in the regime of lower obligations ,

b) receives reports of cyber security incidents, cyber security events, cyber threats and cyber security vulnerabilities and evaluates, records, preserves and protects this data ,

c) it provides methodological support, assistance and cooperation to providers of regulated services in the regime of lower obligations in the occurrence and management of a cyber security incident with a significant impact and in the disclosure of information about vulnerabilities in the field of cyber security .

d) conducts searches and assessments of vulnerabilities in the field of cyber security ,

e) transmits to the Office data on reported cyber threats, cyber security events, cyber security incidents pursuant to Section 16 and vulnerabilities in the field of cyber security ,

f) informs the competent authority of another Member State about a cyber security incident with a significant impact on the continuity of the provision of a regulated service in that Member State, without specifying the reporting person's identification data, and at the same time informs the Office about it, while preserving the safety and privacy interests of the reporting person,

g) receives and evaluates initiatives in the field of cyber security from authorities and persons ,

h) fulfills the role of the CSIRT team according to the relevant regulation of the European Union and participates in the functioning of international groups in the field of cyber security, including the CSIRT Network ,

i) if necessary, participates in the peer review process according to the relevant regulation of the European Union and

j) prioritizes the provision of its services and the performance of its activities according to an approach based on risks and available capacities .

(4) The operator of the National CERT shall proceed impartially and coordinate its activities with the Office when fulfilling the obligations referred to in paragraph 3.

(5) The operator of the National CERT performs activities according to paragraph 3 letter a), b) and e) to h) free of charge. The operator of the National CERT is obliged to incur the necessary costs for the proper and effective performance of the activities referred to in paragraph 3.

(6) The Office will publish on its website information about the operator of the National CERT, namely its business name or name, registered office address, personal identification number, data box identifier and website address.
CELEX 32022L2555

§ 43

Permanent commission for control of the activities of the Office

(1) Control of the Office's activities is carried out by the Chamber of Deputies, which establishes a special control body for this purpose (hereinafter referred to as the "control body").

(2) The control body consists of at least 7 members. The Chamber of Deputies determines the number of members in such a way that each parliamentary club established according to affiliation to the political party or political movement for which the deputies stood for election is represented; the number of members is always odd. Only a member of the Chamber of Deputies can be a member of the control body.

(3) If this law does not provide otherwise, another legal regulation applies to the actions of the control body and to the rights and obligations of its [6]members .

(4) Members of the control body may enter the premises of the Office accompanied by the director of the Office or an employee authorized by him.

(5) The director of the Office submits to the control body

a) report on the activities of the Office,

b) draft budget of the Office,

c) documents needed to control the implementation of the budget of the Office,

d) internal regulations of the Office,

e) upon request, a report on individual cyber security incidents of regulated service providers.

(6) If the control body believes that the activities of the Office illegally restrict or damage the rights and freedoms of citizens or that the decision-making activity of

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

the Office within the framework of administrative proceedings is affected by defects, it is entitled to demand the necessary explanation from the director of the Office.

(7) Any violation of the law by an employee of the Office in the performance of duties pursuant to this Act and in selected areas pursuant to the Act on the Protection of Classified Information and on Security Competence, which the control body discovers in the course of its activities, is required to be reported to the Director of the Office and the Prime Minister.

(8) The duty of confidentiality imposed on the members of the supervisory authority under the law does not apply to cases where the supervisory authority submits a notification pursuant to paragraph 7.

Part 2
Tools of state administration

§ 44
NÚKIB portal

(1) The Office is the administrator and operator of the NÚKIB Portal, which is used to exercise the Office's powers, share information, perform digital actions and provide digital services in accordance with this Act.

(2) Actions according to § 8 paragraph 1, § 9 paragraph 1, § 12 paragraph 1, § 16 paragraphs 1 and 2, § 20 paragraph 3, § 32 paragraph 1 letter b) and § 57 paragraph 1, the provider of the regulated service is obliged to perform exclusively electronically using remote access through form submissions. These actions can be performed in another way only -if the relevant provisions of this law allow it and if it is not possible to use the NÚKIB Portal to perform the action for objective reasons. An act that is not carried out in this way, in the format and structure established by the implementing legislation, is ineffective.

(3) Technical and organizational conditions of use of the NÚKIB Portal, content requirements, format, structure and method of execution of actions pursuant to paragraph 2 shall be determined by the implementing legal regulation.
CELEX 32022L2555

§ 45
Records maintained by the Office

(1) The office keeps records
   a) regulated service providers, entities providing domain name registration services and data reported by them,
   b) cyber security incidents, events, cyber threats and vulnerabilities,
   c) suppliers of safety-relevant supplies,

d) coordinated disclosure of vulnerabilities,
e) penetration tests and
f) performed inspections and inspection reports.

(2) In justified cases, the Office provides data from records to public authorities at their request, if this is necessary for the performance of their powers. The provided data can only be used for the purposes specified in the application. The applicant shall make reasonable efforts to ensure the information security of the data thus provided.

(3) In justified cases, the Office may provide data from the records to the National CERT, authorities or persons exercising competence in the field of cyber security abroad and other authorities or persons operating in the field of cyber security to the extent necessary to ensure the protection of cyber space.

(4) The employees of the Office are bound by the obligation of confidentiality regarding data from the records according to paragraph 1 letter b) to e). The obligation of confidentiality continues even after the end of the employment relationship with the Office. The Director of the Office may release the persons mentioned in this paragraph from the obligation of confidentiality, specifying the scope of the data and the scope of the release.

§ 46

Authorization of compliance assessment entities under the act on cyber security

(1) If a directly applicable regulation of the European Union issued on the basis of the act on cyber security establishes specific or additional requirements for conformity assessment bodies with the aim of ensuring their technical competence to assess cyber security requirements, the Office in accordance with Article 58 paragraph 7 letter e) of the act on cyber security decides on requests for authorization of the conformity assessment body, and if the authorized body of conformity assessment violates the requirements of the act on cyber security or a directly applicable regulation of the European Union issued on the basis of the act on cyber security, on the suspension of enforceability, on amendment or on cancellation authorization decision.

(2) In the application for authorization pursuant to paragraph 1, the subject of conformity assessment shall document the fulfillment of specific or additional requirements established by a directly applicable regulation of the European Union issued on the basis of the act on cyber security.

(3) In the decision to suspend the enforceability of the decision on authorization pursuant to paragraph 1, the Office shall set a deadline for remedial action. If the conformity assessment entity makes a correction, it shall notify the Office of this fact without undue delay. If the Office finds the remedial action to be sufficient, it will cancel the decision to suspend the enforceability of the authorization decision. If the authorized conformity assessment entity does not remedy the situation within the specified period, the Office will decide to change or cancel the authorization decision.

(4) The Office shall make a decision on the authorization request pursuant to paragraph 1 within 120 days from the initiation of the procedure at the latest, and in exceptional cases within 180 days.
CELEX 32019R0881

§ 47

National coordination center for research and development in the field of cyber security

(1) research and development in the field of cyber security, assesses the eligibility of the applicant for registration of membership in the Cyber Security Competence Community [7](hereinafter referred to as the "Community") according to the directly applicable regulation of the European Union .[8]

(2) Only an applicant for registration of membership in the Community (hereinafter referred to as the "applicant") can be a registered member of the Community, who proves to the Office
   a) basic eligibility of the applicant a
   b) special eligibility of the applicant.

(3) The application for registration of membership in the Community (hereinafter referred to as the "application") is submitted electronically via a form published on the website of the Office.

(4) The applicant is obliged to provide in the application true and complete data necessary for the assessment of his basic and special competence by the Office. During the duration of membership in the Community, the applicant who was registered as a member of the Community is obliged to report a change in these data or a fact decisive for the assessment of his basic and special eligibility within 30 days from the day when this change or fact occurred, or the applicant learned about it.
CELEX 32021R0887

§ 48

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

(1) An applicant has basic eligibility if
   a) has its registered office or place of business in the territory of the Czech Republic ,
   b) is not registered on the national sanctions list [9)] ,
   c) no, in the last 5 years before submitting the application, he has been legally convicted of a criminal offense, the substance of which is related to the applicant's business, or for an economic crime, a crime against property, a generally dangerous crime, a crime against the Czech Republic, a foreign state

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

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

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

and an international organization, a crime against order in public affairs; expunged convictions are not taken into account,

d) does not have a tax arrears recorded in the tax records in the Czech Republic,
e) does not have an arrears due in the Czech Republic on insurance premiums or penalties for public health insurance,
f) does not have an arrears due in the Czech Republic on insurance premiums or penalties for social security and contributions to the state employment policy and
g) it is not in liquidation [10], it was not against him a bankruptcy [11]decision has been issued) and compulsory administration has not been ordered against him according to another legal regulation [12].

(2) The applicant proves the fulfillment of the basic eligibility conditions according to paragraph 1 by submitting
a) extract from the records of the Criminal Register in relation to paragraph 1 letter c), which must not be older than 3 months,
b) confirmation of the relevant financial authority in relation to paragraph 1 letter d), which must not be older than 30 calendar days before the date of application submission,
c) written sworn statement in relation to excise tax in relation to paragraph 1 letter d),
d) written affidavit in relation to paragraph 1 letter e) a
e) confirmation of the relevant district social security administration in relation to paragraph 1 letter f), which must not be older than 30 calendar days before the date of application.

(3) For the applicant, if he is a legal entity, the Office will find out information about his beneficial owner in accordance with the legal regulation governing the registration of beneficial owners [13](hereinafter referred to as the "beneficial owner") from the registration of beneficial owners according to the same law (hereinafter referred to as the "registration of beneficial owners").

(4) An applicant is not eligible if
a) is a legal entity that has a real owner, if according to paragraph 3 it was not possible to find out information about its real owner from the register of real owners,
b) the real 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 real owner is the person listed on the national sanctions list [8].

[10] § 187 of the Civil Code.

[11] § 136 of Act No. 182/2006 Coll., on bankruptcy and methods of its resolution (Insolvency Act), as amended.

[12] 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 the addition of Act No. 586/1992 of the Czech National Council Coll., on income taxes, as amended, Act No. 363/1999 Coll., on the insurance industry and on the amendment of some related laws.

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

(5) If the applicant is a legal entity, he must fulfill the condition according to paragraph 1 letter c) to be fulfilled by this legal entity and at the same time each member of its statutory body. If a member of the applicant's statutory body is a legal entity, the condition according to paragraph 1 letter c) comply
   a) this legal entity,
   b) each member of the statutory body of this legal entity and
   c) the person representing this legal entity in the applicant's statutory body.

(6) The applicant is not eligible if the Office has issued a measure of a general nature pursuant to Section 30, paragraph 1, in which it has established the conditions for the use of the applicant's performance or has prohibited the use of the applicant's performance as a supplier of safety-critical supplies.
CELEX 32021R0887

§ 49

Special eligibility of the applicant for registration of membership in the Community

An applicant who proves that he is eligible for registration according to a directly applicable regulation of the European Union has special [14]eligibility .
CELEX 32021R0887

§ 50

Assessment of eligibility of the applicant for registration of membership in the Community

(1) If the applicant fulfills the conditions according to Section 47, paragraph 2, the Office will forward [the] applicant's application to the registering authority according to the directly applicable regulation of the European Union [15](hereinafter referred to as the "registering authority").

(2) In case of doubt as to whether the applicant fulfills the conditions according to § 47 paragraph 2, the Office will initiate proceedings on the applicant's ineligibility to register membership in the Community.

(3) After the decision on the ineligibility of the applicant to register membership in the Community issued in the procedure according to paragraph 2, the Office forwards the applicant's application to the registering authority and simultaneously informs the registering authority of the applicant's ineligibility to register membership in the Community.
CELEX 32021R0887

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

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

§ 51
Eligibility of the applicant for membership in the Community

(1) The Office continuously assesses the fulfillment of the requirements according to § 47 paragraph 2 throughout the duration of the membership of the applicant in the Community, whose application for registration in the Community was granted by the registering authority.
(2) In the event that the applicant, who is registered as a member of the Community, does not meet the conditions according to § 47 paragraph 2, the Office will initiate proceedings on the applicant's ineligibility for membership in the Community.
(3) After the decision on the ineligibility of the applicant for membership in the Community issued in the procedure according to paragraph 2, the Office notifies the registering body of the ineligibility of the applicant for membership in the Community.
CELEX 32021R0887

§ 52
Public contract with the operator of the National CERT

(1) The Office concludes a public contract with a legal entity selected in accordance with § 163 paragraph 4 of the Administrative Code for the purpose of cooperation in the field of cyber security and ensuring activities pursuant to § 42 paragraph 3 (hereinafter referred to as "public contract"). The procedure for the selection of the application is announced by the Office.
(2) The public law contract contains at least
   a) designation of the contracting parties,
   b) definition of the subject of the contract,
   c) Rights and obligations of the Contracting parties,
   d) conditions of cooperation of the contracting parties,
   e) the manner and conditions of withdrawal of the contracting parties from the public law contract,
   f) notice period and grounds for notice,
   g) prohibition of misuse of data obtained in connection with the performance of the activities referred to in § 42 paragraph 3,
   h) definition of the conditions for the performance of the activities of the National CERT according to § 42 paragraph 1 letter h) , a
   i) method of transmission and extent of data transmitted to the Office in the event of termination of the obligation.
(3) The Office publishes the public contract concluded pursuant to paragraph 1 in the Office's Gazette, with the exception of those parts of the public contract, the publication of which is not permitted by another legal regulation.
(4) If a public law contract is not concluded according to paragraph 1, or in the event of the termination of the obligation, the National CERT Office performs the activities.

§ 53
Processing of personal data

(1) The Office and the operator of the National CERT process personal data -if they are necessary for the performance of their mandate. The Office and the operator of the National CERT transfer this data to public authorities or persons if it is necessary for the performance of their tasks and if this does not result in a breach of the obligation of confidentiality under this Act.

(2) The office and operator of the National CERT when processing personal data, which is covered by the directly applicable regulation of the European Union governing the protection of personal data,

a) may not limit the processing of personal data if the data subject denies their accuracy or has raised an objection to this processing and

b) may use personal data for purposes other than those for which they were collected within the scope of their competence.

(3) If the Office or the operator of the National CERT, within the scope of an activity covered by a directly applicable regulation of the European Union governing the protection of personal data, when dealing with a cyber security incident or a cyber security event, when preventing cyber threats or risks, or during the exercise of control, receives personal data that they process only for the purpose of fulfilling the obligations under this Act, for the duration of the fulfillment of these obligations, it does not need to continue

a) provide the data subject with information about corrections or deletions of personal data or restrictions on their processing,

b) ensure the data subject's access to personal data, or

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

CELEX 32022L2555

§ 54
Mutual cooperation with the member states of the European Union

(1) The Office cooperates in the application of this Act with the competent authorities of other Member States of the European Union (hereinafter referred to as "another Member State"), in particular it may provide and request cooperation in the form of

a) information sharing,

b) carrying out an inspection or other actions against the provider of the regulated service, or

c) coordination during inspections of regulated service providers providing regulated services in multiple Member States, including the possibility of inviting representatives of the competent authorities of another Member State to participate in the inspection.

(2) The Office can only refuse a request for cooperation

a) if he is not competent or if he does not have the authority to perform the required action,

b) if the request for cooperation is clearly disproportionate with regard to the capacities of the Office, or

c) if the request for information relates to or includes activities that, if disclosed or carried out, would be in conflict with the essential interests of the Czech Republic in the field of national security, public safety or defence.

(3) If a regulated service provider, which has its seat in another member state of the European Union, provides a service within the Czech Republic

a) domain name resolution (DNS),

b) administration and operation of the registry of Internet top-level domains,

c) cloud computing,

d) data center,

e) Content Delivery Networks (CDNs),

f) online marketplace,

g) internet search engine,

h) social networking platforms,

i) managed services (MSP), or

j) managed security services (MSSP),

the Office is authorized to carry out an inspection or other action against this person based on and to the extent of a request for cooperation from another Member State in which the regulated service provider has its main place of business.

(4) If the assets used for the provision of any of the services listed in paragraph 3 are located within the Czech Republic, but the provider of the regulated service has its main place of business located in another Member State, the Office is authorized in relation to these assets used for the provision of these services to carry out an inspection or another act based on and to the extent of a request for cooperation from another Member State in which the provider of the regulated service has its main place of business.

(5) The location of the main establishment means the place in the European Union where the person providing the services referred to in paragraph 3 mainly takes decisions related to the management of risks in the field of cyber security . If such a place cannot be determined according to the first sentence, or if such decisions are not taken in the European Union, it is considered that the main establishment is located in the Member State of the European Union where the actual actions leading to ensuring cyber security are carried out . If such a place cannot be determined according to the first and second sentences, it is considered that the main establishment is located in the Member State of the European Union where the person has an establishment with the highest number of employees.

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

CELEX 32022L2555

§ 55
Implementing legislation and enabling provisions

(1) The implementing legislation provides
   a) criteria for identifying a regulated service (§ 4),
   b) the method of determining the regime of the provider of the regulated service (§ 6 paragraph 3),
   c) security measures corresponding to the regime of the regulated service provider and peace and the manner of their introduction and implementation (§14 paragraphs 2 and 4),
   d) the method of determining the significant impact of a cyber security incident on the provision of a regulated service in the regime of lower obligations (§ 16, paragraph 3),
   e) content details, format and method of notification of countermeasure implementation and its result (§ 20, paragraph 3),
   f) criteria for identifying a strategically important service (§ 27 paragraph 1),
   g) non-permanent functions of the specified scope (§ 28 paragraph 4),
   h) criteria of the supplier's riskiness and the method of their evaluation (Section 28, paragraph 4),
   i) method of reporting data by an entity providing domain name registration services (§ 35, paragraph 1) a
   j) technical and organizational conditions for the use of the NÚKIB Portal, content requirements, format, structure and method of performing the actions referred to in § 44 paragraph 2 (§ 44 paragraph 3).

(2) Implementing legal regulations pursuant to paragraph 1 shall be issued by the Office in the form of a decree.

TITLE VI
Inspection, Remedies, Offenses and Penalties

§ 56
Control performed by the Office

(1) The office performs control in the field of cyber security. During the inspection, the Office ascertains how authorities and persons fulfill the obligations set forth in this Act, decisions and measures of a general nature issued by the Office pursuant to this Act, and observe the implementing legislation in the field of cyber security.

(2) During the performance of the inspection, the procedure is carried out according to the inspection procedure.

(3) Inspection according to this provision is carried out by authorized employees of the Office.
CELEX 32022L2555

§ 57
Corrective measures

(1) If the Office discovers deficiencies during the inspection, it may, by decision, order the inspected body or person to remove them within a specified period, or determine how to do so. In a decision, the Office may impose on the body or person the obligation to notify the Office of the implementation of the corrective measure and its result within a specified period. The requirements and method of reporting are determined by the implementing legal regulation.

(2) If the Office considers the factual findings to be sufficient, it may impose corrective measures pursuant to paragraph 1 even without carrying out an inspection.

(3) Dismissal against the decision to impose a corrective measure does not have a suspensive effect.
CELEX 32022L2555

§ 58
Offenses

(1) A provider of a regulated service under the higher obligations regime commits an offense by
   a) fails to register or change the registration of a regulated service provider pursuant to § 8 paragraphs 1 and 2 or § 9 paragraphs 1 or 2,
   b) does not report registration, contact data or other data or their change to the Office in accordance with § 12 paragraphs 1 and 4,
   c) does not ensure sufficient substitutability of natural persons authorized to act on behalf of the regulated service provider pursuant to § 12 paragraph 5,
   d) does not identify all primary assets in accordance with § 13 when determining the scope of cyber security management paragraph 1 letter and),
   e) when determining the scope of cyber security management, it shall not determine all primary assets related to the provision of a regulated service pursuant to § 13 paragraph 1 letter b) or organizational parts and supporting assets according to § 13 paragraph 1 letter C),
   f) does not keep a documented record of the identification and determination of organizational parts and assets in accordance with § 13 paragraph 3,
   g) does not introduce or implement security measures in violation of § 14,
   h) fails to report a cyber security incident pursuant to § 16, paragraph 1, or does not submit an initial incident report pursuant to § 17, paragraph 1, or does not complete any of the incident data pursuant to § 17, paragraph 3,
   i) does not provide information or cooperation in managing the incident according to § 18, paragraph 3,
   j) does not fulfill the obligation to inform the user of the regulated service about a cyber security incident with a significant impact established by the decision of the Office pursuant to § 19 paragraph 1,

k) does not fulfill the obligation to inform the user of the regulated service about a significant cyber threat and the steps that the user of the service can take in response to it according to § 19 paragraph 2,

l) fails to notify the implementation of countermeasures imposed by the Office and its result in accordance with § 20 paragraph 3,

m) does not fulfill the obligation imposed by the Office by decision on warning pursuant to § 21,

n) does not fulfill the obligation imposed by the decision to issue a reactive countermeasure or by a measure of a general nature issued by the Office pursuant to § 23,

o) does not take into account requirements resulting from security measures when selecting a supplier or in a contract with a supplier in violation of § 24 paragraph 1 or 2, or

p) does not fulfill any of the obligations imposed by the decision to impose a corrective measure according to § 57.

(2) A provider of a regulated service under the lesser obligations regime commits an offense by

a) fails to register or change the registration of a regulated service provider pursuant to § 8 paragraphs 1 and 2 or § 9 paragraphs 1 or 2,

b) does not report registration, contact data or other data or their change to the Office in accordance with § 12 paragraphs 1 and 4,

c) does not ensure sufficient substitutability of natural persons authorized to act on behalf of the regulated service provider pursuant to Section 12, paragraph 5 ,

d) when determining the scope of cyber security management, it does not identify all primary assets according to § 13 paragraph 1 letter and),

e) when determining the scope of cyber security management, it shall not determine all primary assets related to the provision of a regulated service pursuant to § 13 paragraph 1 letter b) or organizational parts and supporting assets according to § 13 paragraph 1 letter C),

f) does not keep a documented record of the identification and determination of organizational parts and assets in accordance with § 13 paragraph 3 ,

g) does not introduce or implement security measures in violation of § 14,

h) fails to report a cyber security incident pursuant to § 16, paragraph 2, or does not submit an initial incident report pursuant to § 17, paragraph 1, or does not complete any of the incident data pursuant to § 17, paragraph 3,

i) does not provide information or cooperation in managing the incident according to § 18, paragraph 3,

j) does not fulfill the obligation to inform the user of the regulated service about a cyber security incident with a significant impact established by the decision of the Office pursuant to § 19 paragraph 1,

k) does not fulfill the obligation to inform the user of the regulated service about a significant cyber threat and the steps that the user of the service can take in response to it according to § 19 paragraph 2,

l) fails to notify the implementation of countermeasures imposed by the Office and its result in accordance with § 20 paragraph 3,

m) does not fulfill the obligation imposed by the Office by decision on warning pursuant to § 21 ,

n) does not fulfill the obligation imposed by the decision to issue a reactive countermeasure or by a measure of a general nature issued by the Office pursuant to § 23,

o) does not take into account requirements resulting from security measures when selecting a supplier or in a contract with a supplier in violation of § 24 paragraph 1 or 2, or

p) does not fulfill any of the obligations imposed by the decision to impose a corrective measure according to § 57.

(3) A provider of a strategically important service commits an offense by

a) violates a condition or prohibition imposed by the Office in a measure of a general nature pursuant to § 30,

b) does not make a reasonable effort to find out information about the supplier of a safety-relevant supply in accordance with § 32 paragraph 1 letter and),

c) does not record information about the supplier of safety-relevant supplies in accordance with § 32 paragraph 1 letter and),

d) does not report to the Office information about the supplier of safety-relevant supplies or their change in accordance with § 32 paragraph 1 letter b),

e) does not ensure the availability of a strategically important service from the territory of the Czech Republic in the specified time and quality according to § 34 paragraph 1, or

f) does not test the ability to ensure the provision of a strategically important service according to Section 34, paragraph 2.

(4) An entity providing domain name registration services commits an offense by

a) does not report data to the Office according to § 35 paragraph 1 or their change according to § 35 paragraph 2,

b) does not collect or store accurate and complete data on the registration of domain names in a dedicated database pursuant to § 36 paragraph 1 in accordance with the requirements of § 36 paragraph 2,

c) does not introduce or publish policies and procedures ensuring the accuracy and completeness of the information kept in the database, including verification procedures according to § 36 paragraph 3,

d) without undue delay after the registration of the domain name will not publish its registration data, which are not personal data, according to § 36 paragraph 4, or

e) will not provide access to specific data on domain name registration pursuant to § 36 paragraph 5 .

(5) An entity managing and operating a registry of internet top-level domains commits an offense by

a) does not collect or store accurate and complete data on the registration of domain names in a dedicated database pursuant to § 36 paragraph 1 in accordance with the requirements of § 36 paragraph 2,
b) does not introduce or publish policies and procedures ensuring the accuracy and completeness of the information kept in the database, including verification procedures according to § 36 paragraph 3,
c) without undue delay after the registration of the domain name will not publish its registration data, which are not personal data, according to § 36 paragraph 4, or
d) will not provide access to specific data on domain name registration pursuant to § 36 paragraph 5.

(6) An authority or person commits an offense by
a) does not provide cooperation in securing documents for the issuance of countermeasures pursuant to Section 20, paragraph 3,
b) does not transfer data and information according to § 25 paragraph 1,
c) does not provide information or other cooperation based on the Office's request pursuant to § 29 paragraph 3,
d) does not fulfill any of the obligations imposed by the decision to impose a corrective measure pursuant to § 57, or
CELEX 32022L2555
e) does not provide information or other cooperation necessary to assess the fulfillment of the criteria of the regulated service according to § 63, paragraph 2.

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

(8) In relation to a state of cyber danger, an authority or person commits an offense by
a) fails to comply with the measures used to solve and correct the state of cyber danger according to § 40 paragraph 2 letter and),
b) does not provide cooperation when performing a vulnerability scan or penetration test pursuant to § 40 paragraph 2 letter b),
c) does not provide cooperation in the publication of the announcement, progress and termination of the state of cyber danger according to § 40 paragraph 2 letter c), or
d) does not provide cooperation in solving and correcting the state of cyber danger according to § 40 paragraph 2 letter d).

(9) A natural person commits an offense by breaching the obligation of confidentiality pursuant to § 45 paragraph 4.

(10) The applicant commits an offense by providing false or grossly distorted information in the application for registration pursuant to Section 47, paragraph 4, or by withholding essential information.

(11) The applicant commits an offense if, during the period of membership in the Community according to § 47, he fails to indicate a change in the data required for

the assessment of his basic and special eligibility by the Office, conceals the change, or fails to indicate other facts decisive for the assessment of his basic and special eligibility, or conceals these facts.
CELEX 32021R0887

(12) The holder of the European Cyber Security Certificate commits an offense by not informing the relevant conformity assessment bodies of any vulnerabilities or irregularities subsequently discovered.

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

a) the EU issues a declaration of conformity, even if the conditions for its issuance are not met, as set out in the act on cyber security [16)],
b) does not keep documents and information according to Article 53, paragraph 3 of the act on cyber security,
c) does not submit a copy of the EU declaration of conformity to the Office and the ENISA agency pursuant to Article 53(3) of the Act on Cybersecurity, or
d) does not provide information on cyber security to the extent and in the manner specified in Article 55 of the Cyber Security Act.

(14) A legal entity or a natural person who undertakes a business commits an offense by

a) misuses the mark or mark of the European Cyber Security Certification System, the European Cyber Security Certificate, the EU Declaration of Conformity or another document under the Cyber Security Act,
b) falsifies or alters the European Cyber Security Certificate, EU Declaration of Conformity or other document under the Cyber Security Act,
c) carries out conformity assessment activities according to the act on cyber security to the guarantee level "high", although it is not authorized to do so according to Article 56 paragraph 6 of the act on cyber security,
d) as a conformity assessment body authorized under Article 60(3) of the Cybersecurity Act, issues a European Cybersecurity Certificate to a product, process or service that does not meet the criteria contained in a directly applicable European Union regulation issued on the basis of the Cybersecurity Act,
e) performs without authorization the activity of conformity assessment reserved by the directly applicable regulation of the European Union issued on the basis of the act on cyber security to the authorized entity of conformity assessment,
f) acts as an accredited conformity assessment body without accreditation pursuant to Article 60(1) of the Cyber Security Act or outside the scope of this accreditation, or
g) as a conformity assessment entity, does not fulfill the obligation imposed by the Office to suspend the validity of the certificate or certificate issued by it pursuant to Section 60, paragraph 1.
CELEX 32019R0881

[16)] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on the ENISA agency ("European Union Agency for Cyber Security"), on the certification of information and communication technology cyber security and on the repeal of Regulation (EU) No. 526/ 2013 (the “Cybersecurity Act”).

(15) A fine can be imposed for an offence

a) CZK 250,000,000 or up to 2% of the net worldwide annual turnover achieved by the legal entity or, if the accused is part of a consolidated entity, achieved by the consolidated entity for the immediately preceding accounting period, whichever of the given amounts is higher, if it is an offense under paragraph 1 letter a), letter d) to k) and letter m) to p), paragraph 3 letter a), e) and f), paragraph 6 letter b) and paragraph 8 letter a) and b).

b) CZK 175,000,000 or up to 1.4% of the net worldwide annual turnover achieved by the legal entity or, if the accused is part of a consolidated entity, achieved by the consolidated entity for the immediately preceding accounting period, depending on which of the given amounts is higher, if offense according to paragraph 2 letter a), letter d) to k) and letter m) to p) and paragraph 8 letter d).
CELEX 32022L2555

c) CZK 100,000,000, if it is an offense according to paragraph 1 letter b), paragraph 3 letter (b) and (c)

d) CZK 50,000,000, if it is an offense according to paragraph 1 letter c) al), paragraph 2 letter b), paragraph 3 letter d), paragraph 4 letter a) to e), paragraph 5 letter a) to d), paragraph 6 letter a) and c) to e), paragraph 7 and paragraph 13 letter and),

e) CZK 35,000,000, if it is an offense according to paragraph 2 letter c) al) and paragraph 8 letter C),

f) CZK 20,000,000, if it is an offense according to paragraph 13 letter b) to d) and paragraph 14 letter a) to c) and letter e) to g),
CELEX 32019R0881

g) CZK 2,000,000, if it is an offense according to paragraphs 10, 11 and 12 and paragraph 14 letter d),
CELEX 32019R0881, 32021R0887

h) CZK 50,000, if it is an offense according to paragraph 9.

§ 59
Common provisions on misdemeanors

(1) Violations under this Act are discussed and fines are collected by the Office.

(2) An act which exhibits the formal features of an offense under this Act is deemed to be socially harmful.

(3) On the procedure of the Office under this Act, the provisions of § 43, § 68 letter b), § 70, § 71, § 80 paragraph 3, § 88 paragraph 2, § 89, § 90 paragraph 3, § 95 paragraph 3 and § 96 paragraph 1 letter b) of the Act on Liability for Misdemeanors and Proceedings Regarding Them [17)] shall not apply.

(4) It applies that offenses consisting of a breach of an obligation imposed by a decision, a measure of a general nature or a corrective measure, offenses consisting of failure to register a regulated service provider, offenses related to

[17)] Act No. 250/2016 Coll., on liability for misdemeanors and their proceedings, as amended.

determining the scope of cyber security management, offenses related to taking into account the requirements arising from security measures when selecting a supplier or in contract with a supplier, offenses consisting of breach of obligations from the supply chain security review mechanism and offenses consisting of failure to report information and maintaining a state of failure to inform the Authority or users of the regulated service are continuing offenses.
CELEX 32022L2555

§ 60
Suspension of validity of certification

(1) In the event of non-fulfilment of the obligation to eliminate deficiencies identified during the inspection imposed by the Authority's decision on a regulated service provider in the regime of higher obligations, who holds a European cyber security certificate pursuant to the act on cyber security or another certificate or certificate related to ensuring the cyber security of the regulated service, the Authority may suspend the regulated service regulated services, the validity of the European cyber security certificate issued by the Authority or impose on the conformity assessment entity the obligation to suspend the validity of the certificate or certificate issued by it, until the deficiencies found during the inspection are eliminated, but at least for 6 months.
(2) The decision of the Office according to paragraph 1 can be the first act in the proceedings and the resolution against it does not have a suspensory effect.
(3) The participant in the procedure for issuing a decision according to paragraph 1 is always the regulated service provider in the regime of higher obligations, the validity of whose certificate is being decided.
(4) The Office will publish information on the suspension of the validity of the certificate or certificate on its website.
(5) The Authority will, however, first after the expiry of the period according to paragraph 1, check the fulfillment of the obligation to remove the deficiencies found during the inspection, and if it finds that the deficiencies have been eliminated, the Authority will issue a certificate to this effect, which is the basis for renewing the validity of the certificate or certificate.
CELEX 32022L2555

§ 61
Suspension of the management function

(1) At the proposal of the Office, the court may decide that a member of the statutory body of a legal entity, the head of a spin-off plant, a procurator or a natural person in business who, in direct connection with the implementation of the Office's decision, by which the regulated service provider under the regime of higher obligations was imposed the obligation to eliminate deficiencies found during the inspection, has repeatedly or seriously violated his obligations in the performance

of his management function, as a result of which the proper fulfillment of the Office's decision was thwarted, he may not perform this management function until the deficiencies identified during the inspection are eliminated, but for at least 6 months.

(2) The proposal can only be filed against a person performing a management function at a regulated service provider under the regime of higher duties and only in relation to a management function that is not a public function defined by a functional or time period and filled on the basis of direct or indirect election or appointment according to special legal regulations.

(3) The provisions of the Act on Business Corporations [18)] governing the exclusion of a member of a statutory body from the performance of a function shall apply mutatis mutandis in the parts of the legal effects of a final decision on the exclusion of a member of a statutory body, informing the registry court and liability for violation of a temporary ban on the performance of the function.

(4) The Office will publish information on the final decision on the suspension of the management function on its website.

(5) The Office, however, at the earliest after the expiry of the deadline according to paragraph 1, will carry out an inspection of the fulfillment of the obligation to remove the deficiencies found during the inspection and, if it finds that the deficiencies have been eliminated, the Office will issue a certificate to this effect, which is the basis for deleting the data on the suspension of the management function from the business register according to the Act on Public Registers of Legal and Natural Persons.

CELEX 32022L2555

§ 62
Relation to administrative and control regulations

(1) The office can impose a fine of up to CZK 100,000. The fine can be imposed repeatedly. The total amount of repeatedly imposed fines may not exceed CZK 10,000,000 or 1% of the net turnover achieved by a legal entity or an individual entrepreneur for the last completed accounting period, whichever is higher.

(2) In order to enforce the fulfillment of the obligation imposed by the decision of the Office, the Office may impose coercive fines up to the amount of CZK 10,000,000 or 1% of the net turnover achieved by a legal entity or an individual entrepreneur for the last completed accounting period, whichever of the given amounts is higher .

(3) CZK 10,000,000 can be imposed for an offense committed by a provider of a regulated service by failing to fulfill any of the obligations under the inspection regulations [19]as a controlled person.

[18)] Act No. 90/2012 Coll., on commercial companies and cooperatives (Act on Commercial Corporations), as amended.

[19)] § 10 paragraph 2 of Act No. 255/2012 Coll., on inspection (inspection regulations), as amended.

(4) The execution of the Office's decision imposing the obligation to hand over or otherwise deal with information and data is governed by the provisions of the Administrative Code governing the execution by removal of movable property.

PART TWO
COMMON AND TRANSITIONAL PROVISIONS

TITLE I
Common Provisions

§ 63
Cooperation

(1) Public authorities are obliged to provide the Office with initiatives, information and other forms of cooperation necessary for the exercise of powers and for the purpose of fulfilling the duties of the Office, which are established by this law, without undue delay, and unless a special regulation provides otherwise, even without payment. Public authorities and the Office cooperate with each other in the exercise of the powers entrusted to the Office by this Act, they are entitled to request opinions on the prepared decisions issued within the limits of their competence, and they strive to achieve agreement between these opinions. Furthermore, to the extent necessary for the performance of the tasks of the public authorities and the Office, the public authorities and the Office share information about cyber threats, vulnerabilities and incidents and about the measures taken in response to these threats, vulnerabilities and incidents. The provisions of § 45 paragraphs 2 and 3 are not affected by this.

(2) Authorities and persons who can reasonably be assumed to fulfill the criteria for the identification or designation of a regulated service are obliged to provide the information necessary to assess the fulfillment of the criteria for a regulated service and other necessary cooperation without undue delay, and unless a special regulation provides otherwise, even without payment . The requested cooperation may not be provided if it is prevented by a legal or state-recognized obligation of confidentiality.

(3) Ministries, other central administrative authorities and the Czech National Bank, responsible for determining elements of critical infrastructure according to the legal regulation governing crisis management and critical infrastructure, without undue delay inform the Office about the determination of elements of critical infrastructure and the reasons for the determination.

(4) The Office is entitled to request from the General Financial Directorate the provision of information obtained in the course of tax administration, which is necessary for assessing whether the authority or person fulfills the criteria for identifying a regulated service according to § 3. The General Financial Directorate will comply with the request, unless the provision of information could lead to a

disruption of the proper performance of tax administration. The provision of information pursuant to this provision is not a breach of the duty of confidentiality under the Tax Code, nor is the use of this information by the Office pursuant to this Act.

(5) The Office and the Office for the Protection of Personal Data are mutually entitled to request information and require cooperation in order to avoid double punishment for the violation of the same obligation imposed both by this Act and by legal regulations governing the protection of personal data. This does not affect the imposition of other sanctions under this Act.

(6) For the purposes of exercising the authority of the Office under this Act, the Ministry of Justice shall enable the Office to obtain, in a way that enables remote access, from the records of beneficial owners a complete list of valid data and data that have been deleted without compensation or replaced with new data in accordance with the legal regulation governing the records of beneficial owners.
CELEX 32022L2555

§ 64
Information obligation of the Office

Office for the purpose of fulfilling the information obligation according to the relevant regulation of the European Union [20)]

a) informs the European Commission and the Cooperation Group every 2 years about the number of regulated service providers meeting the criteria for identifying a regulated service in individual sectors,
b) every 2 years informs the European Commission about the number of providers of regulated services fulfilling the criteria for determining a regulated service in individual sectors, the services they provide and the criteria for which they were designated,
c) every 3 months submits to the European Union Agency for Cyber Security a summary report including anonymized and aggregated data on cyber security incidents, cyber threats and significant cyber security events notified pursuant to § 16,
d) provides the European Union Agency for Cybersecurity with identification data about entities providing domain name registration services and providers of regulated services listed in § 54, paragraph 3, who have their main place of business in the territory of the Czech Republic or who have a representative established in the territory of the Czech Republic,
e) provides the European Union Agency for Cybersecurity with information for the coordinated disclosure of vulnerabilities,
f) informs the European Commission about the adoption of the national cyber security strategy and, to the extent that the security interests of the Czech Republic are not threatened, about the content of the strategy,

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

g) communicate to the European Commission the identification data of the authority responsible for supervision in the field of cyber security, the single point of contact for ensuring cross-border cooperation in the field of cyber security within the European Union, the authority for solving cyber crises, the CSIRT team and the coordinator designated for the purposes of coordinated disclosure of vulnerabilities,

h) provides the European Commission and the European Union Agency for Cyber Security with additional information and necessary cooperation.

CELEX 32022L2555

§ 65

Common and special provisions on proceedings before the Office

(1) The provisions of the Administrative Code governing the conduct of administrative proceedings shall not apply to the Office's procedures pursuant to § 8, § 9, § 10 and § 11, paragraphs 1 and 3.

(2) Proceedings for the designation of a regulated service according to § 5 can only be initiated ex officio.

(3) Dissolution is not admissible against the decision to designate a regulated service pursuant to § 5 and the decision to delete it from the register of providers of regulated services pursuant to § 11, paragraph 2 .

(4) If the procedure for deletion from the register of regulated service providers is to be initiated ex officio pursuant to Section 11, paragraph 2, the decision to delete from the register of regulated service providers may be the first act in the procedure; in such a case, the decision is not made in writing, the deletion decision becomes legally binding by recording it in the file, and the Office deletes it from the register of providers of regulated services.

§ 66

Protection of information

Parts of documents and records that contain classified information or information, the disclosure of which could jeopardize the provision of cyber security, the effectiveness of countermeasures pursuant to § 20 or measures of a general nature pursuant to § 30, are kept by the Office in proceedings pursuant to § 20, § 30 and § 31 separately outside the file .

§ 67

Representative for the Czech Republic

(1) A domain name registration service provider and a regulated service provider that is a domain name resolution system (DNS) service provider, an internet top-level domain registry management and operation provider, a cloud computing service provider, a data center service provider, a content delivery network service provider (CDN), an online marketplace service provider, an internet search

engine service provider, a social network platform service provider, a managed service provider (MSP) or a managed security service provider (MSSP) that provides this service in the Czech Republic does not have its main place of business 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 authorized by the provider of one of the listed regulated services to represent him in relation to the obligations under this Act. The appointment of a representative does not affect the responsibility of the provider of the regulated service or the entity providing domain name registration services for compliance with this law.

(2) In the event that an entity providing domain name registration services or a provider of any of the regulated services referred to in paragraph 1 has its main place of business outside the European Union and has established its representative in the Czech Republic, it is valid that it is established in the Czech Republic and is subject to the obligations under this Act. This also applies if the provider of one of the listed regulated services has its main place of business outside the European Union and has not established a representative in any member state of the European Union.

(3) The appointment of a representative does not affect the responsibility of the provider of the regulated service or the entity providing domain name registration services for compliance with this Act.

CELEX 32022L2555

§ 68

Financial security of the state of cyber danger

The financial security of the state of cyber danger for the current budget year is carried out according to another legal regulation [21)] . For this purpose

a) In the budget of its chapter for the relevant year, the Office allocates the amount of funds needed to ensure preparation for the state of cyber danger; and furthermore, in its budget for the relevant year, allocates a special-purpose reserve of financial resources for dealing with cyber risk situations and removing their consequences, and

b) the financial resources needed to ensure preparation for the state of cyber danger and the removal of its consequences allocated by the Office in the budgets of the chapters are considered a binding indicator of the state budget for the relevant year.

[21)] Act No. 218/2000 Coll., on budget rules and on the amendment of some related laws (budget rules), as amended.

§ 69
Intelligence services

(1) In the case of intelligence services [22], this Act shall be applied only to the extent of the provisions
   a) part one in the scope of chapter one, provisions § 8, § 9, § 10, § 11, § 12 with the exception of the data according to paragraph 2 letter c), § 13, § 14, § 15, § 22 and § 24 paragraph 2 and chapter four, and
   b) part two to the extent of § 65 paragraphs 1, 3 and 4.

(2) Where it is necessary to establish the regime of a regulated service provider in order to fulfill the obligation according to the previous paragraph, it applies that the intelligence service acts as a regulated service provider in the regime of higher obligations.

(3) The provisions of § 29 paragraph 2 and § 63 shall be applied if the fulfillment of these obligations is not prevented by a special regulation [23] or a statutory or state-recognized obligation of confidentiality.
CELEX 32022L2555

§ 70
Relation to sectoral legislation of the European Union

(1) If a directly applicable legal regulation of the European Union establishes obligations for institutions or persons in the field of implementation and implementation of security measures or reporting of cyber security incidents and these obligations have at least a comparable effect to the obligations imposed on these authorities or persons under this Act, the provisions of this Act governing the obligations to introduce and implement security measures and to report cyber security incidents do not apply to these authorities and persons, including provisions on the supervision of compliance with the aforementioned obligations.

(2) Provisions with a comparable effect to the obligations contained in this Act according to paragraph 1 are considered to be such provisions of directly applicable legislation of the European Union which
   a) in relation to the obligation to introduce and implement security measures, they correspond at least to the requirements set out in § 14 and § 15, or
   b) in relation to the obligation to report cyber security incidents, they meet at least the requirements set out in § 16 and § 17.

(3) Provisions with a comparable effect to the obligations contained in this Act pursuant to paragraph 1 shall further be considered to be such provisions of directly applicable European Union legislation, which the directly applicable European Union legal regulation itself stipulates.

[22] § 3 of Act No. 153/1994 Coll., on intelligence services, as amended.

[23] For example, Act No. 153/1994 Coll., on intelligence services, as amended.

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 significant information systems or digital service providers pursuant to § 3 of Act No. 181/2014 Coll. in the wording effective before the date of entry into force of this Act, by which the services provided fulfill the criteria of a regulated service according to this Act, for services and information systems regulated according to existing legal regulations, to the extent that these services and assets are regulated by this Act, at least
   a) obligations associated with the introduction and implementation of security measures, reporting of cyber security incidents and compliance with the Office's measures pursuant to Act No. 181/2014 Coll. in the version effective before the date of entry into force of this Act, in the event that, according to this Act, the provider of a regulated service is in the regime of higher obligations, or
   b) obligations associated with the introduction and implementation of security measures, reporting of cyber security incidents and compliance with the Office's measures pursuant to Act No. 181/2014 Coll. in the wording effective 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 in the regime of lower obligations, in the event that, according to this Act, the provider of a regulated service is in the regime of lower obligations, from the moment this Act takes effect until the expiry of the deadlines for starting the fulfillment of obligations under this Act, with the exception of the method of reporting cyber security incidents, which these providers of regulated services are obliged to implement according to this Act from the moment of delivery of the notification of registration in the register of regulated providers services.
2) In proceedings relating to the fulfillment of obligations imposed by law or on the basis of Act No. 181/2014 Coll. in the wording effective before the date of entry into force of this Act, the procedure shall be in accordance with existing legal regulations.
3) Warnings issued pursuant to Act No. 181/2014 Coll. as amended 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. in the version effective before the date of entry into force of this Act are considered reactive countermeasures issued pursuant to this Act.

5) The entry into force of this Act does 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 EFFECTIVITY

§ 72
Cancellation provisions

They cancel

1. Act No. 181/2014 Coll., on cyber security and on the amendment of related laws (Cyber Security Act).
2. Decree No. 82/2018 Coll., on cyber security.
3. Decree No. 437/2017 Coll., on criteria for determining the basic service operator.
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 takes effect on October 18, 2024.
CELEX 32022L2555

In Prague on dd.mm.yyyy

Prime Minister