– international organizations or other entities referred to in Article 4, subparagraphs 4 and 5 of this Act

– foundations, institutes and institutions established or co-founded by the Republic of Croatia for public benefit or charitable purposes, legal entities with public authority and legal entities to which the Republic of Croatia, on the basis of international treaties, recognizes legal personality in the Croatian legal system, in accordance with their activities or competencies covered by the subject matter of this Act

– civil society organizations

– legal entities entered in the court register.

Competences and obligations of the implementing body

Article 11

(1) Budget users, as implementing bodies, shall provide development cooperation to partner countries through their own development and humanitarian projects, programs and other activities, independently or in cooperation with entities referred to in Article 10 of this Act, in accordance with their competencies, plans and available budgetary resources.

(2) Budget users are obliged to submit to the Ministry, at its request, data on the use of funds for the provision of development cooperation in accordance with the rules of the OECD Development Assistance Committee, for the purpose of preparing the Report for which the Ministry is responsible.

Allocation of funds for bilateral development cooperation

Article 12

Funds for the implementation of bilateral development cooperation are allocated to:

– a financial contribution to a state administration body, a local and regional self-government unit, a competent professional service of the Government of the Republic of Croatia, a foundation, institute, legal entities referred to in Article 10 of this Act, or another implementing body or co-implementing body in the Republic of Croatia, a third country or partner country, an international organization, fund or other international institution with competences in the implementation of development cooperation, whereby the target partner country or region is defined

- contracting with civil society organizations through a public call in accordance with the criteria, standards and procedures for financing and contracting projects and programs for the beneficiaries of the state budget

– direct financial contributions to partner countries in the form of budget support and other financial instruments referred to in Article 9, subparagraphs 6 and 7 of this Act, in accordance with the conditions for approving such support and instruments

- financial instruments intended for private sector activities in development cooperation projects and programs from Article 9, subparagraph 5 of this Act, where the purpose and target partner country or region are defined.

Allocation of funds for multilateral development cooperation

Article 13.

Funds for the realization of multilateral development cooperation are allocated through the payment of contributions, membership fees or other financial payments through or in favor of international organizations, institutions, programs and funds and to legal entities from Article 10 of this Act, whereby the target partner country or region is not defined.

Conditions for awarding funds

Article 14.

Funds for the implementation of bilateral and multilateral development cooperation are allocated in accordance with the conditions and criteria for financing or co-financing development cooperation projects and programs and the strategic planning act referred to in Article 5 of this Act.

TRANSITIONAL AND FINAL PROVISIONS

Ongoing procedures and subordinate legislation

Article 15

(1) The procedures for contracting and implementing development cooperation projects and programmes that were initiated before the entry into force of this Act shall be completed in accordance with the provisions of the Act on Development Cooperation and Humanitarian Aid Abroad (Official Gazette, No. 146/08).

(2) The Government of the Republic of Croatia shall adopt the decision on the establishment of the Commission referred to in Article 7 of this Act within six months from the date of entry into force of this Act.

Termination of the Law

Article 16

On the date of entry into force of this Act, the Act on Development Cooperation and Humanitarian Aid Abroad (Official Gazette, No. 146/08) shall cease to be valid.

Entry into force

Article 17.

This Act shall enter into force on the eighth day following the date of its publication in the Official Gazette.

Class: 022-02/23-01/20

Zagreb, January 26, 2024.

CROATIAN PARLIAMENT

President
Croatian Parliament
Gordan Jandrokoviÿ, mp

254

Pursuant to Article 89 of the Constitution of the Republic of Croatia, I hereby adopt

DECISION

ON THE PROCLAMATION OF THE LAW ON CYBERNETICS SECURITY

I hereby promulgate the Cybersecurity Act, which was adopted by the Croatian Parliament at its session on January 26, 2024.

Class: 011-02/24-02/03

Reg. No.: 71-10-01/1-24-2

Zagreb, February 1, 2024.

President
Republic of Croatia
Zoran Milanoviÿ, senior

LAW

ABOUT CYBER SECURITY

PART ONE
BASIC PROVISIONS

Objective and subject matter of the Law

Article 1.

(1) This Act regulates the procedures and measures for achieving a high common level of cybersecurity, the criteria for the categories

gorization of key and important entities, cyber security requirements for key and important entities, special requirements for managing data on domain name registration and control of their implementation, voluntary cyber protection mechanisms, competent bodies in the field of cyber security and their tasks and powers, professional supervision over the implementation of cyber security requirements, misdemeanor provisions, monitoring of the implementation of this Act and other issues of importance in the field of cyber security.

(2) This Act establishes a framework for strategic planning and decision-making in the field of cyber security and establishes national frameworks for the management of large-scale cyber incidents and cyber crises.

(3) Achieving and maintaining a high common level of cybersecurity, in particular through the development and continuous improvement of cybersecurity policies and their implementation, developing national capabilities in the field of cybersecurity, strengthening cooperation and coordination of all relevant bodies, strengthening cooperation between the public and private sectors, promoting the development, integration and use of relevant advanced and innovative technologies, promoting and developing education and training in the field of cybersecurity, and development activities aimed at strengthening cybersecurity awareness are of national importance for the Republic of Croatia.

(4) The aim of this Act is to establish a cybersecurity management system that will ensure the effective implementation of procedures and measures to achieve a high level of cybersecurity in sectors of particular importance for the smooth performance of key social and economic activities and the proper functioning of the internal market.

List of annexes that are an integral part of the Act

Article 2.

The following are an integral part of this Law:

ÿ Annex I. High-criticality sectors (hereinafter referred to as: Annex I of this Act)

ÿ Annex II. Other critical sectors (hereinafter referred to as: Annex II of this Act)

ÿ Annex III. List of competences in the field of cybersecurity (hereinafter referred to as: Annex III of this Act) and

ÿ Annex IV. Mandatory content of the national strategic planning act in the field of cybersecurity (hereinafter: Annex IV of this Act).

Harmonization of regulations with European Union legal acts

Article 3.

This Act transposes into Croatian legislation Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 concerning measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No. 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS2 Directive) (OJ L 333/80, 27. 12. 2022).

Concepts

Article 4.

(1) For the purposes of this Act, certain terms have the following meanings:

1. active cyber protection is protection that introduces an advanced approach that, instead of a reactive response to incidents, involves their prevention, i.e. active prevention, detection, monitoring, analysis and mitigation of network and information security breaches.

attitude, combined with the use of capabilities applied both inside and outside the network and information system that is the target of the cyberattack

2. CSIRT is an abbreviation for Computer Security Incident Response Team, or the competent body for the prevention and protection against cyber incidents, for which the abbreviation CERT (Computer Emergency Response Team) is also used.

3. The CSIRT network is a network of national CSIRTs established for the purpose of developing trust and confidence and promoting rapid and effective operational cooperation among the Member States of the European Union (hereinafter: Member States), which, in addition to representatives of national CSIRTs, also consists of representatives of the competent authority for prevention and protection against cyber incidents in the European Union (CERT-EU).

4. digital service is any information society service, that is, any service that is usually provided for remuneration, at a distance, by electronic means and at the personal request of the recipient of the service, where within the meaning of this term:

a) "at a distance" means that the service is provided without the parties being present at the same time

b) "by electronic means" means that the service is sent from its origin and received at its destination by means of electronic processing equipment, including digital compression and storage of data, and that it is sent, transmitted and received in its entirety by wire, radio, light or other electromagnetic system

c) "at the personal request of the recipient of the service" means that the service is provided by transferring data at the personal request

5. electronic communications service is a service that is usually provided for remuneration via electronic communications networks, and includes, with the exception of services providing content or exercising editorial control over content transmitted using electronic communications networks and services, the following types of services:

a) "Internet access service" or a publicly available electronic communications service that enables access to the Internet and thus connection to almost all Internet endpoints, regardless of the network technology and terminal equipment used

b) "interpersonal communications service" means a service which is generally provided for a fee and which enables the direct interpersonal and interactive exchange of information via electronic communications networks between a limited number of persons, whereby the persons initiating or participating in the communication determine the recipient or recipients thereof. This service does not include services which enable interpersonal and interactive communication only as a minor ancillary feature which is intrinsically linked to another service and

c) services consisting, wholly or mainly, of the transmission of signals, such as transmission services used for the provision of machine-to-machine communication services and for broadcasting

6. The EU-CyCLONe network is a European network of cyber crisis liaison organisations established to act at the operational level as a mediator between the technical level (CSIRT network) and the political level, with the aim of creating an efficient operational assessment and management process during large-scale cyber incidents and cyber crises, as well as supporting the decision-making process on complex cyber issues at the political level.

7. ICT is information and communication technology

8. ICT process is an ICT process as defined in Article 2, item 14. Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (European Union Agency for Cybersecurity) and on cybersecurity certification in the field of information and communications technology and repealing Regulation (EU) No. 526/2013 (Cybersecurity Act) (Text with EEA relevance) (OJ L 151/15, 7.6.2019) (hereinafter: Regulation (EU) 2019/881)

9. ICT product is an ICT product as defined in Article 2. point 12 of Regulation (EU) 2019/881

10. ICT service is an ICT service as defined in Article 2, point 13 of Regulation (EU) 2019/881

11. Incident is an event that threatens the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or services offered or accessed by network and information systems.

12. Internet search engine means an Internet search engine as defined in Article 2(5) of Regulation (EU) 2019/1150 of the European Parliament and of the Council of 20 June 2019 on promoting fairness and transparency for business users of online intermediation services (OJ L 186, 11.7.2019)

13. online marketplace is a digital service that enables consumers to conclude distance contracts with other traders or consumers through the use of software, including websites, parts of websites or applications operated by or on behalf of a trader

14. research organization is an entity whose primary goal is to conduct applied research or experimental development in order to exploit the results of that research for commercial purposes, but which does not include educational institutions

15. An avoided incident is any event that could have jeopardized the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or services offered or accessed by network and information systems, but was successfully prevented or did not occur.

16. public electronic communications network is an electronic communications network that is used in whole or in part for the provision of publicly available electronic communications services that support the transmission of data between network endpoints.

17. public entities are legal entities founded by the Republic of Croatia or a local or regional self-government unit, legal entities performing public service, legal entities that are financed, pursuant to a special regulation, predominantly or entirely from the state budget or from the budget of a local or regional self-government unit, or from public funds, and companies in which the Republic of Croatia and local or regional self-government units have a separate or joint majority ownership, not including the Croatian National Bank.

18. The single point of contact is the national contact point responsible for national coordination and cooperation with other Member States on matters of security of network and information systems.

19. cyber threat is a cyber threat as defined in Article 2(8) of Regulation (EU) 2019/881

20. a large-scale cyber security incident is an incident at the level of the European Union that causes disruptions that exceed the ability of one member state to respond to the incident or that has a significant effect on at least two member states, as well as an incident at the national level that causes disruptions that exceed the ability of the sectoral CSIRT body to respond to the incident or that has a significant effect on at least two sectors, and in such cases cyber crisis management procedures are initiated, aligned with the existing national general crisis management framework and management framework cyber crises of the European Union

21. cyber security is cyber security as defined in Article 2, point 1 of Regulation (EU) 2019/881

22. Qualified trust service provider is a qualified trust service provider as defined in Article 3(20) of Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market and placing outside the the force of Directive 1999/93/EC (OJ L 257/73 28. 8. 2014 – hereinafter: Regulation (EU) No 910/2014)

23. qualified trust service is a qualified trust service as defined in Article 3(17) of Regulation (EU) No 910/2014

24. Content delivery network is a network of geographically distributed servers for the purpose of ensuring high availability, accessibility or rapid delivery of digital content and services to Internet users on behalf of content and service providers.

25. The network and information system consists of:

a) "electronic communications network" means transmission systems based on a permanent infrastructure or centralised management capacity and, where applicable, switching or routing equipment and other means, including parts of the network that are not active, which enable the transmission of signals by wire, radio, light or other electromagnetic systems, including satellite networks, fixed terrestrial networks (with circuit switching and packet switching, including the Internet), terrestrial mobile communications networks, electricity cable systems to the extent that they are used for the transmission of signals, broadcasting networks and cable television networks, regardless of the type of data transmitted

b) each device or group of connected or related devices, one or more of which programmatically executes automatic processing of digital data or

c) digital data that is stored, processed, obtained or transmitted by the elements described in subparagraphs a) and b) of this point, for the purpose of their operation, use, protection and maintenance

The 26th national act of strategic planning in the field of cyber security is a comprehensive framework that defines specific goals and priorities in the field of cyber security and management for their achievement

27. The competent authorities for the implementation of special laws are the Croatian National Bank, the Croatian Financial Services Supervisory Agency and the Croatian Civil Aviation Agency.

28. The competent authorities for the implementation of cybersecurity requirements are the central state authority for cybersecurity, the central state authority for information security, the regulatory authority for network activities, the state administration body responsible for the development of the digital society and the state administration body responsible for science and education.

29. The competent CSIRT is the CSIRT at the central state body for cybersecurity or the CSIRT at the Croatian Academic and Research Network – CARNET (hereinafter: CARNET), depending on the division of competences determined by this Act.

The 30th norm is the norm as defined in Article 2, point 1. Regulation (EU) No. 1025/2012 of the European Parliament and of the Council on European standardisation, amending Council Directives 89/686/EEC and 93/15/EEC and Directives 94/9/EC, 94/25/EC, 95/16/EC, 97/23/EC, 98/34/EC, 2004/22/EC EC, 2007/23/EC, 2009/23/EC and 2009/105/EC of the European Parliament and of the Council and repealing Council Decision 87/95/EEC and Decision No. 1673/2006/EC of the European Parliament and of the Council (OJ L 316, 14. 11. 2012 – hereinafter: Regulation (EU) No 1025/2012)

31. personal data means all data as defined in Article 4(1)(1) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119/1, 4 May 2016) (hereinafter: Regulation (EU) 2016/679), in particular information necessary to identify domain users and contact points managing domain names, as well as IP addresses (the Internet Protocol address used on each device connected to the Internet), unique resource locators (URLs), domain names, e-mail addresses, time stamps and other information which, in certain cases, within the framework of activities carried out pursuant to this Act, may reveal personal data

32. A serious cyber threat is a cyber threat that, based on its technical characteristics, can be assumed to have a serious impact on the network and information systems of an entity or users of the entity's services, causing significant material or non-material damage or interruption of services to users.

33. a platform for social network services is a platform that allows end users to connect with each other, share and discover content and communicate on multiple devices, especially through conversations, posts, videos and recommendations

34. Incident handling is all actions and procedures aimed at preventing, detecting, analyzing, stopping or responding to an incident and recovering from the incident.

35. Representative is a natural or legal person established in the European Union who has been expressly appointed by a domain name system service provider (hereinafter referred to as: DNS service provider), a registry of national top-level Internet domain names, a registrar, a cloud computing service provider, a data centre service provider, a content delivery network provider, a managed service provider, a managed security service provider, or an online marketplace provider, an online search engine provider or a social networking platform provider not established in the European Union to act on their behalf and to whom the competent authority or the CSIRT may address instead of the entity itself with regard to the obligations of that entity under this Act.

36. Private entities are natural or legal persons established and recognised as such under the national law of their place of business which can, acting in their own name, exercise rights and assume obligations.

37. Managed security services provider is a managed services provider that carries out or provides assistance for activities related to the management of cybersecurity risks.

38. Managed service provider is an entity that provides services related to the installation, management, operation or maintenance of ICT products, networks, infrastructure, applications or any other network and information systems, in the form of assistance or active management carried out at the client's premises or remotely.

39. DNS service provider is an entity that provides:

a) publicly available recursive domain name resolution services to internet end users and/or

b) authoritative domain name resolution services for use third parties, with the exception of root name servers

40. A trust service provider is a trust service provider that is defined in Article 3, point 19 of Regulation (EU) no. 910/2014

41. Vulnerability is a weakness, sensitivity or deficiency of an ICT product. or ICT services that a cyber threat can exploit

42. The registry of a national Internet top-level domain name is an entity to which a specific top-level Internet domain has been delegated and which is responsible for its management, including the registration of domain names within the top-level domain and the technical management of the top-level domain, including the management of its name servers, the maintenance of its databases and the distribution of files from the top-level domain zone to the name servers, regardless of whether the entity itself performs any of these operations or uses an external service provider to perform them, but situations in which the registry uses top-level domain names only for its own use are excluded. In the Republic of Croatia, this is CARNET

43. Registrar is an entity that provides domain name registration services, or a legal or natural person who performs independent activities authorized to register and administer .hr domains on behalf of the registry of top-level national Internet domains.

The 44th regulatory authority for network activities is the Croatian Regulatory Authority. to network agencies

45. Risk is the possibility of loss or disruption caused by an incident, expressed as a combination of the extent of such loss or disruption and the probability of that incident occurring.

46. Security of network and information systems is the ability of network and information systems to withstand, at a certain level of reliability, all events that may threaten the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or services that these network and information systems offer or provide access to.

47. systemic risk is the risk of disruptions in the functioning of the service, i.e. in the performance of activities, which could have serious negative consequences for one or more sectors or could have a cross-border effect

48. The Cooperation Group is a group established for the purpose of supporting and facilitating strategic cooperation and information exchange between Member States and developing trust and security at the European Union level in the field of cybersecurity.

The 49th central state body for information security is the Office of the National Security Council

The 50th central government agency for cyber security is the Security-Sno-Intelligence Agency

The 51st central state body for performing tasks in the technical areas of information security is the Information Security Institute.
system

52. Internet traffic exchange is a network instrument that enables the interconnection of more than two independent networks (autonomous systems), primarily for the purpose of facilitating the exchange of Internet traffic, that enables interconnection only for autonomous systems and that does not require Internet traffic between any two participating autonomous systems to pass through any third autonomous system and that does not modify or otherwise affect such traffic

53. entity is any public entity, private entity and public sector entity

54. public sector entities are state administration bodies, other state bodies, legal entities with public powers, local and regional self-government units, as well as private and public entities for which categorization is carried out on the basis of this Act due to their role in the management, development or maintenance of the state information infrastructure

55. The Domain Name System or DNS is a hierarchical naming system that allows the identification of Internet services and resources, thereby enabling end-user devices to use Internet routing and connectivity services to access those services and resources.

56. The education system includes early and preschool education, primary education, secondary education and higher education, monitoring, evaluation and development of the system and implementation of programs.

57. technical specification is a technical specification as defined in Article 2, point 4 of Regulation (EU) no. 1025/2012

The 58th state administration body responsible for the development of the digital society is the Central State Office for the Development of the Digital Society.

The 59th state administration body responsible for science and education is Ministry of Science and Education

60. The authority responsible for personal data protection is the Personal Data Protection Agency or another supervisory authority referred to in Articles 55 and 56. Regulation (EU) 2016/679

61. Third-party ICT service provider is an ICT service provider as defined in Article 3(19) of Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulation (EC) No.

1060/2009, (EU) No. 648/2012, (EU) No. 600/2014, (EU) No. 909/2014 and (EU) 2016/1011 (OJ L 333/1 27. 12. 2022 – hereinafter: Regulation (EU) 2022/2554)

62. The management body of a key and important entity is the body or bodies appointed in accordance with the law governing the establishment and operation of the entity, which have the authority to manage and conduct the affairs of the entity.

63. Data center service is a service that includes structures or groups of structures intended for the centralized placement, interconnection and operation of information technology equipment and networks for data storage, processing and transmission services, including all facilities and infrastructure for power distribution and environmental control.

64. trust service means a trust service as defined in Article 3(16) of Regulation (EU) No 910/2014

65. A cloud computing service is a digital service that enables on-demand administration and broad remote access to a scalable and elastic pool of shareable computing resources, including when such resources are distributed across multiple locations.

66. An employee of an entity is a natural person who, in an employment relationship, performs certain tasks for the entity, including a natural person who, under the company regulation, is a member of the management board or executive director or a natural person who, in another capacity under a special law, individually and independently or jointly and collectively, is authorized to manage the entity's affairs, or a natural person who, as a worker in an employment relationship, performs certain tasks for the entity.

(2) Expressions used in this Law that have a gender meaning refer equally to the masculine and feminine genders.

Application of special regulations on the protection of secrecy and confidentiality of data

Article 5.

(1) If, in the implementation of this Act, classified data or other data are created or used for which rules of conduct are established in special regulations to protect their secrecy or confidentiality, special regulations on their protection shall apply to such data.

(2) This Act does not apply to information systems of security accredited for handling classified information.

Application of personal data protection rules

Article 6.

(1) The application of the provisions of this Act shall not affect the obligations of providers of public electronic communications networks or providers of publicly available electronic communications services to process personal data in accordance with special regulations on the protection of personal data and the protection of privacy.

(2) The application of the provisions of this Act shall not affect the obligations of key and important entities to act in accordance with the provisions of Articles 33 and 34 of Regulation (EU) 2016/679 in the event of a personal data breach.

Relationship with the law governing the field of electronic communications

Article 7.

(1) The application of the provisions of this Act shall not affect the obligation to implement the basic requirements for electronic communications infrastructure and other related equipment prescribed by the law regulating the field of electronic communications.

(2) The application of the provisions of this Act does not affect the rules for managing the national top-level Internet domain and the rights and obligations of domain users prescribed by the law regulating the field of electronic communications.

Application of special laws in matters of cyber security

Article 8.

(1) If for key and important entities from individual sectors from Annex I and Annex II. of this Act, requirements prescribed by special laws which in their content and purpose correspond to the requirements of cyber security from this Law, or represent stricter requirements, the corresponding provisions of that special law shall apply to those entities in those matters related to those requirements and their implementation regulated by those regulations, including provisions on the supervision of the implementation of the requirements.

(2) The content and purpose of the requirements from paragraph 1 of this article correspond to the cyber security requirements from this Act if:

- are at least equivalent in effect to the cyber security risk management measures established by this Act

– a special law establishes immediate, if necessary automatic and direct access to incident notifications to the competent CSIRT and if the obligations to notify significant incidents under the special law are at least equivalent in effect to the obligations to notify significant incidents set out in this Act.

(3) Authorities that are competent for the sector or sub-sector and/or entity referred to in Annex I and Annex II of this Act under the special laws referred to in paragraph 1 of this Article and the authorities competent for the implementation of cybersecurity requirements shall, when applying paragraphs 1 and 2 of this Article, cooperate with each other and exchange relevant information and take into account the guidelines of the European Commission explaining the application of the relevant relevant European Union law.

PART TWO
CATEGORIZATION OF ENTITIES

CHAPTER I.
CRITERIA FOR IMPLEMENTING THE CATEGORIZATION OF ENTITIES

General criteria for implementing the categorization of key entities

Article 9.

The following are classified in the category of key entities:

- private and public entities from Annex I of this Act that exceed the upper limits for medium-sized entities of small businesses established by the law regulating the bases for the application of economic policy incentive measures aimed at the development, restructuring and market adaptation of small businesses

– qualified trust service providers, register of names of top national internet domains and DNS service providers, regardless of their size

– providers of public electronic communications networks or publicly available electronic communications services that represent medium-sized small business entities pursuant to the law regulating the basis for the application of economic policy incentive measures aimed at the development, restructuring and market adjustment of small businesses or that exceed the upper limits for medium-sized small business entities

– information intermediaries in the exchange of electronic invoices between entrepreneurs, regardless of their size and

– entities that are determined as critical entities based on the law regulating the area of critical infrastructure, regardless of their size.

General criteria for implementing the categorization of significant entities

Article 10.

The following are classified in the category of important entities:

– private and public entities from Annex II to this Act that represent medium-sized small business entities on the basis of laws regulating the basis for the application of economic policy incentive measures aimed at the development, restructuring and market adjustment of small businesses or that exceed the upper limits for medium-sized small business entities

- private and public entities from Annex I of this Act that are not identified as key entities on the basis of Article 9, subparagraph 1 of this Act, and represent an intermediate entity of a small economy based on the law regulating the bases for the application of economic policy incentive measures aimed at the development, restructuring and market adaptation of a small economy

– trust service providers that are not categorized as key entities pursuant to Article 9, subparagraph 2, of this Act, regardless of their size, and

– providers of public electronic communications networks or publicly available electronic communications services that are not categorized as key entities pursuant to Article 9, subparagraph 3 of this Act, regardless of their size.

Special criteria for implementing the categorization of key and important subjects

Article 11

By way of derogation from Article 9, subparagraph 1 and Article 10, subparagraphs 1 and 2 of this Act, private and public entities listed in Annex I and Annex II of this Act may be classified as key or important entities, regardless of their size, if:

– the entity is the sole provider of a service that is essential for maintaining key social or economic activities

– a disruption in the functioning of the service provided by the entity or a disruption in the performance of the entity's activities could have a significant impact on public safety, public protection or public health

- a disruption in the functioning of the service provided by the entity, or a disruption in the performance of the entity's activities, could cause significant systemic risks in the sectors listed in Annex I and Annex II. of this Act, especially in sectors where such disruption could have a cross-border effect or

– the entity is significant due to its particular importance at the national, regional or local level for a specific sector or type of service or for other interdependent sectors in the Republic of Croatia.

Categorization of public sector entities

Article 12

(1) The following entities are classified in the category of key entities, regardless of their size:

– state administration bodies and

- other state bodies and legal entities with public powers, depending on the results of an assessment of their importance for the smooth performance of key social or economic activities.

(2) By way of derogation from Article 9, subparagraph 1 and Article 10, subparagraph 2 of this Act, private and public entities that manage, develop or maintain the state information infrastructure in accordance with the law governing the state information infrastructure shall be classified as key entities, regardless of their size.

(3) Units of local and regional self-government are classified, regardless of their size, into the category of important entities, depending on the results of the assessment of their importance for the smooth performance of key social or economic activities.

Categorization of subjects from the education system

Article 13.

By way of derogation from Article 10, subparagraph 1 of this Act, private and public entities in the education system shall be classified, regardless of their size, into the category of important entities, depending on the results of an assessment of their special importance at the national or regional level for carrying out educational work.

Determination of jurisdiction based on territoriality

Article 14.

(1) Entities from Annex I and Annex II. of this Act are subject to the competences and powers prescribed by this Act if they provide services or perform activities in the territory of the European Union, and have a place of business in the territory of the Republic of Croatia.

(2) By way of derogation from paragraph 1 of this Article, providers of public electronic communications networks or publicly available electronic communications services shall be subject to the jurisdiction and powers prescribed by this Act if they provide their services on the territory of the Republic of Croatia, regardless of their country of establishment.

(3) By way of derogation from paragraph 1 of this Article, DNS service providers, national top-level domain name registries and registries, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, managed security service providers, online marketplace providers, online search engine providers or social media platform providers shall be subject to the jurisdiction and powers prescribed by this Act if they have their principal place of business in the territory of the Republic of Croatia or their representative has a place of business in the territory of the Republic of Croatia.

(4) An entity has its principal place of business within the meaning of paragraph 3 of this Article if, on the territory of the Republic of Croatia:

- predominantly makes decisions related to cybernetic security risk management measures or

– implements cybersecurity risk management measures when the Member State in which the decisions referred to in subparagraph 1 of this paragraph are made cannot be determined or such decisions are not made by the entity in the European Union, or

- has a business unit with the largest number of employees in the European Union when the member state in which it carries out the activities referred to in subparagraph 2 of this paragraph cannot be determined.

Application of the entity size criterion

Article 15

(1) When determining whether an entity represents a medium-sized entity of a small economy, i.e. an entity that exceeds the upper limits for medium-sized entities of a small economy based on the law regulating the bases for the application of economic policy incentive measures aimed at the development, restructuring and market adjustment of a small economy, the following shall be taken into account:

– the annual average of the total number of employees of the entity and

– the total annual operating income of the entity according to the financial statements for the previous year or the total assets of the entity if it is a corporate taxpayer, or the total fixed assets of the entity

an entity if it is a taxpayer for income tax, regardless of whether the entity also provides other services or performs other activities not covered by Annex I and Annex II of this Act.

(2) When categorizing entities, account shall be taken of the European Commission guidelines on the implementation of size criteria applicable to micro and small enterprises.

Application of the Law in case of double categorization of the subject

Article 16

If the entity is classified in the category of both key and important entities, the provisions of this Act relating to key entities shall apply to such an entity.

CHAPTER II.
LISTS OF KEY AND IMPORTANT ENTITIES

Inventory management

Article 17.

(1) The competent authorities for the implementation of cybersecurity requirements and the competent authorities for the implementation of special laws shall carry out the categorization of entities in accordance with this Act and establish and maintain lists of key and important entities.

(2) The competent authorities for the implementation of cybersecurity requirements and the competent authorities for the implementation of special laws are obliged to regularly, and at least once every two years, check the lists of key and important entities and, if necessary, update them.

Submission of data to the European Commission and the Cooperation Group

Article 18

(1) The single point of contact shall submit every two years:

– to the European Commission and the Cooperation Group, data on the number of key and important entities classified on the basis of Article 9, subparagraphs 1, 2, 3 and 5, Article 10 and Article 12, paragraph 1, subparagraph 1 and paragraph 3 of this Act, for each sector and subsector from Annex I and Annex II of this Act

– to the European Commission data on the number of key and important entities classified pursuant to Article 11 of this Act, the sector and subsector to which they belong, the type of service they provide and the provisions of Article 11 of this Act on the basis of which the categorization was carried out, and in addition, at its request, it may also submit data on the names of these entities to the European Commission.

(2) The competent authorities for the implementation of cybersecurity requirements and the competent authorities for the implementation of special laws are obliged to provide the single point of contact with the data necessary for the submission of data in accordance with paragraph 1 of this Article.

Notifications about the categorization of entities

Article 19

(1) The competent authorities for the implementation of cybersecurity requirements shall be obliged to inform all entities from the list referred to in Article 17, paragraph 1 of this Act that are under their jurisdiction of the implemented categorization of the entity and the obligations to which they are subject pursuant to this Act and the implementing regulation on cybersecurity requirements under this Act.

(2) Competent authorities for the implementation of cyber security requirements are obliged to notify the entities in relation to which, after updating the list of key and important entities, there has been a change in the categorization of the entity about the change in category and the fact that from the date Upon receipt of this notification, the obligations to which they are subject under this Act and the implementing regulation on cybersecurity requirements under this Act shall also change, with an indication of the significant changes that they must take into account depending on the change in the category being notified.

(3) The competent authorities for the implementation of cybersecurity requirements shall be obliged to inform entities that, after updating the list of key and important entities, are no longer considered to be key entities or important entities of that fact and of the fact that, from the date of receipt of that notification, they are no longer subject to the obligations to implement cybersecurity requirements under this Act.

(4) The competent authorities for the implementation of cybersecurity requirements are obliged to inform the entities about the implemented categorization of the entity, as well as the changes referred to in paragraphs 2 and 3 of this Article, within 30 days from the date of the implemented categorization of the entity or the update of the list of key and important entities.

Obligations of entities from Annex I and Annex II. of the Act in data collection

Article 20

(1) For the purposes of categorizing entities in accordance with this Act and maintaining a list of key and important entities, entities from Annex I and Annex II to this Act shall, upon their request, provide the following information to the competent authorities for the implementation of cybersecurity requirements and to the competent authorities for the implementation of special laws:

– name of the entity

– address and updated contact information, including email addresses, IP address ranges and telephone numbers

– relevant sector, subsector and type of entity from Annex I and Annex II. of this Act

– list of Member States in which they provide services covered by the scope of this Act

- other data about the provision of its services or the performance of its activities essential for the implementation of the subject's categorization or the determination of jurisdiction over the subject.

(2) Deadlines for the submission of data pursuant to paragraph 1 of this Article shall be determined depending on the scope and complexity of the data to which the request relates, provided that the deadline set cannot be shorter than 15 days or longer than 45 days from the date of receipt of the request for the submission of data.

(3) The entities referred to in paragraph 1 of this Article shall be obliged to notify the competent authority for the implementation of cybersecurity requirements or the competent authority for the implementation of special laws without delay, within two weeks from the date of the change, of all changes to the data they have submitted to that authority in accordance with paragraph 1 of this Article.

Collecting data from other sources to implement subject categorization

Article 21

(1) State administration bodies, other state bodies, units of local and regional (regional) self-government, legal entities with public powers and public entities that within their scope collect data, i.e. keep registers, records and collections of data on entities from Annex I and Annex II. of this Act are obliged, free of charge, to the competent authorities for the implementation of cyber security requirements:

– regularly submit lists of entities from Annex I and Annex II of this Act, or enable access to the relevant data in registers, records and data collections electronically

– at the request of the competent authority for the implementation of cybersecurity requirements, for entities on the list referred to in subparagraph 1 of this paragraph, submit:

a) information about their size and/or

b) other data on entities, including data on the provision of their services or the performance of their activities, if such data is necessary for the categorization of entities in accordance with this Law or

c) refer them to a state administration body, another state body, a unit of local and regional self-government, a legal entity with public authority or a public entity that possesses such data.

(2) If data is submitted pursuant to this Article at the request of the competent authorities for the implementation of cybersecurity requirements, the deadlines for the submission of data shall be determined depending on the scope and complexity of the data to which the request relates, provided that the deadline set cannot be shorter than 15 days or longer than 45 days from the date of receipt of the request for the submission of data.

CHAPTER III.
SPECIAL REGISTER OF ENTITIES

Maintaining a special register of entities

Article 22

(1) The central state authority for cybersecurity shall establish and maintain a special register of the following entities:

– DNS service provider

– the registry of national top-level Internet domain names

– registrar

– cloud computing service providers

– data center service provider

– content delivery network providers

– managed service providers

– managed security service providers

– online marketplace providers

– Internet search engine providers and

– social media service platform provider.

(2) The register referred to in paragraph 1 of this Article shall be kept independently of the obligation to keep a list of key and important entities.

Data collection

Article 23

(1) Entities referred to in Article 22 of this Act are obliged to submit the following data to the central state authority for cybersecurity:

– name of the entity

– a list of services referred to in Article 22 of this Act provided by

- the address of the subject's main business establishment and its other business units or the address of its representative

– updated contact information, including email addresses and phone numbers of the entity and its representative

– list of member states in which the services referred to in Article 22 of this Act are provided

– Subject IP address ranges.

(2) Deadline for submission of data pursuant to paragraph 1 of this Article is 15 days from the date of receipt of the request for data delivery.

(3) Entities referred to in Article 22 of this Act shall, without delay, within three months from the date of the change, notify the central state authority for cybersecurity of all changes to the data they have submitted in accordance with paragraph 1 of this Article.

(4) Upon receipt, the data referred to in paragraphs 1 and 3 of this Article, except for the data referred to in paragraph 1, subparagraph 6 of this Article, shall be submitted without delay, through the single point of contact, to the European Cybersecurity Agency (hereinafter: ENISA).

Implementing regulation on the categorization of entities, keeping a list of key and important entities and a special register of entities

Article 24.

The criteria for classifying entities into the category of key or important entities based on the special criteria referred to in Article 11 of this Act, the criteria for conducting assessments referred to in Article 12, paragraph 1, subparagraph 2 and paragraph 3, and Article 13 of this Act, maintaining a list of key and important entities, collecting data for the purpose of conducting the categorization of entities in accordance with this Act, and maintaining a special register of entities referred to in Article 22 of this Act shall be prescribed by the Government of the Republic of Croatia (hereinafter: the Government) by regulation, at the proposal of the central state authority for cybersecurity.

PART THREE
CYBER SECURITY REQUIREMENTS

Scope of cybersecurity requirements

Article 25

(1) Cybersecurity requirements include procedures and measures that key and important entities are required to implement in order to achieve a high level of cybersecurity in the provision of their services or the performance of their activities, and consist of:

– cyber security risk management measure i

- the obligation to inform about significant incidents and serious cyber threats.

(2) Cybersecurity requirements apply to all network and information systems used by key and important entities in their business operations or in the provision of their services and all services provided by key and important entities or activities performed by them, regardless of whether the entity also provides other services or performs other activities not covered by Annex I and Annex II to this Act.

CHAPTER I.
CYBERNETIC SECURITY RISKS MANAGEMENT MEASURES AND VERIFICATION OF COMPLIANCE OF KEY AND IMPORTANT ENTITIES

Application of measures

Article 26

(1) Key and important entities are obliged to implement appropriate and proportionate measures to manage cyber security risks.

(2) The aim of implementing cybersecurity risk management measures is to protect network and information systems and the physical environment of these systems from incidents, taking into account all the dangers to which these systems are exposed.

(3) Cyber risk management measures include:

– technical, operational and organizational measures to manage the risks to which network and information systems are exposed that key and important entities use in their business or in the provision of their services, and

– measures to prevent or minimize the impact of incidents on the network and information systems of key and important entities, recipients of their services or on other sectors, entities and services.

(4) Key and important entities are obliged to implement cyber security risk management measures regardless of whether they manage and/or maintain their network and information systems themselves or use an external service provider for this.

(5) Key and important entities are obliged to implement cyber security risk management measures within one year from the date of delivery of the notification referred to in Article 19, paragraph 1 of this Act.

(6) When notifying an entity of a change in the categorization of an entity pursuant to Article 19, paragraph 2 of this Act, the competent authority for the implementation of cybersecurity requirements shall also indicate in the notification an appropriate deadline for the implementation of the obligations to which the entity is subject due to the change in category pursuant to this Act and the implementing regulation on cybersecurity requirements under this Act.

(7) The deadline referred to in paragraph 6 of this Article shall be determined depending on the scope and complexity of the obligations of which the entity is notified, provided that the deadline set cannot be shorter than 60 days or longer than six months from the date of receipt of the notification referred to in Article 19, paragraph 2 of this Act.

Obligation to ensure a level of security of network and information systems proportional to the identified risk

Article 27.

(1) Key and important entities are obliged to ensure a level of security of network and information systems proportional to the identified risk by implementing cyber security risk management measures.

(2) When assessing the proportionality of the administrative measures applied, cyber security risks are taken into account:

– the entity's degree of exposure to risks

– size of the subject

– the probability of incidents occurring and their severity, including their possible social and economic impact.

Method of implementation of cyber security risk management measures

Article 28.

(1) Cybersecurity risk management measures shall be implemented in a manner that, without imposing obligations or discriminating in favour of the use of a particular type of technology, takes into account the latest technical developments used within the framework of best security practices in the field of cybersecurity, as well as European and international standards and technical specifications relevant to the security of network and information systems, while also taking into account the cost of implementation.

(2) When implementing cyber security risk management measures, key and important entities are obliged to use certain ICT products, ICT services and ICT processes and managed security services that are certified on the basis of European cyber security certification programs or national cyber security certification schemes, if such an obligation is prescribed:

– relevant regulations of the European Union

– special regulations governing the area of provision certain services or the performance of certain activities

– by this Act or the regulation referred to in Article 24 of this Act.

Responsibility for implementing measures

Article 29

(1) The members of the management bodies are responsible for implementing cybersecurity risk management measures in accordance with this Act. bodies of key and important entities, i.e. heads of state administration bodies, other state bodies and executive bodies of local and regional self-government units (hereinafter: persons responsible for managing measures).

(2) Persons responsible for managing measures are required to approve cyber security risk management measures that the entity will implement in order to comply with the obligations set out in this Act and the implementing regulation on cyber security requirements, and to control their implementation.

(3) For the purpose of acquiring knowledge and skills in matters of managing cyber security risks and their impact on the services provided by the entity or the activity it performs, persons responsible for managing measures are obliged to:

– attend appropriate training

– enable the entity's employees to attend appropriate training.

(4) The provisions of this Article also apply to other natural persons who, based on their authority to supervise the conduct of the entity's business or in their capacity as legal representatives of the entity based on a power of attorney or other authority to represent or a power of attorney or other authority to make decisions on behalf of the entity, participate in making decisions on cybersecurity risk management measures and/or their implementation.

Cyber security risk management measures

Article 30

(1) Cybersecurity risk management measures include the following:

– risk analysis and information systems security policies

– handling incidents, including their monitoring, recording and reporting

- business continuity, such as backup management and recovery from accidents, work interruptions and incidents from Article 37 of this Act, and cybercrisis management

– supply chain security, including security aspects regarding the relationship between the entity and its direct suppliers or service providers

– security in the procurement, development and maintenance of network and information systems, including the elimination of vulnerabilities and their detection

– policies and procedures for assessing the effectiveness of cybersecurity risk management measures

– basic cyber hygiene practices and cybersecurity training

– policies and procedures regarding cryptography and, where appropriate, encryption

– human resource security, access control policies and management of software and hardware assets, including regular updating of the inventory of these assets

– use of multi-factor authentication or continuous authentication solutions, protected voice, video and text communications, and secure emergency communication systems within the entity, as appropriate.

(2) When assessing the proportionality of the measures applied under paragraph 1, subparagraph 4 of this Article, key and important entities shall take into account the vulnerabilities specific to each direct supplier and service provider and the general product quality and cybersecurity practices of their suppliers and service providers, as well as the results of coordinated

security risk assessment of key supply chains of ICT services, ICT systems or ICT products, carried out by the Cooperation Group together with the European Commission and ENISA.

(3) Cybersecurity risk management measures and the manner of their implementation shall be regulated by the regulation referred to in Article 24 of this Act.

Compliance checks of established cyber security risk management measures

Article 31

(1) Key and important subjects are obliged to check the compliance of the established cyber security risk management measures with the cyber security risk management measures prescribed by this Act and the regulation from Article 24 of this Act.

(2) The verification of compliance from paragraph 1 of this article is carried out in the process of auditing the cyber security of key and important entities and in the process of self-assessment of cyber security of important entities.

Cyber security auditors

Article 32

(1) The cyber security audit of key and important entities is carried out by cyber security auditors.

(2) Cybersecurity auditors are managed security service providers who have been issued:

– national security certificate for cybersecurity audit or

– an appropriate cybersecurity certificate based on a relevant European cybersecurity certification scheme.

(3) By way of exception to paragraph 2 of this Article, the cybersecurity auditor for state administration bodies and other state bodies is the central state body for performing tasks in the technical areas of information security.

(4) The cyber security auditors shall draw up a report on the cyber security audit.

National Cyber Security Audit Certification

Article 33.

(1) The national security certificate for cybersecurity audits is issued by the central state authority for performing tasks in the technical areas of information security based on the rules for security certification for cybersecurity audits.

(2) The rules referred to in paragraph 1 of this Article shall be adopted by the central state body responsible for performing tasks in the technical areas of information security, and they shall include:

– organizational and professional requirements that must be met by managed security service providers to conduct a cybersecurity audit

– rules, technical requirements, standards and procedures applied in the implementation of a cybersecurity audit, including the mandatory content of the report on the conducted cybersecurity audit and

– the procedure for issuing and revoking a national security certificate for cybersecurity audits, the rights and obligations of managed security service providers, and legal protection in that procedure.

(3) The rules referred to in paragraph 1 of this Article shall apply if an appropriate European cybersecurity certification scheme covering cybersecurity audits has not been adopted.

(4) The central state authority for performing tasks in the technical areas of information security shall maintain a publicly accessible register of providers of managed security services referred to in Article 32, paragraph 2, subparagraph 1 of this Act.

Conducting a cybersecurity audit

Article 34.

(1) Key entities are required to conduct a cyber security audit at least once every two years.

(2) Key entities are obliged to conduct a cybersecurity audit even before the expiry of the deadline referred to in paragraph 1 of this Article, when requested by the competent authority for the implementation of cybersecurity requirements pursuant to Article 79, paragraph 1, subparagraph 7 or Article 81, paragraph 1, subparagraph 2 of this Act.

(3) The cybersecurity audit referred to in paragraph 1 of this Article shall be conducted as a separate procedure or as part of a business audit or other compliance check of entities conducted on the basis of special regulations governing the provision of certain services or the performance of certain activities.

(4) Significant entities are obliged to conduct a cybersecurity audit when requested by the competent authority for the implementation of cybersecurity requirements pursuant to Article 79, paragraph 1, subparagraph 7 of this Act.

(5) Key and important entities are obliged to submit the report referred to in Article 32, paragraph 4 of this Act to the competent authority for the implementation of cybersecurity requirements without delay, and no later than eight days from the date of its receipt.

(6) By way of derogation from paragraph 5 of this Article, where a cybersecurity audit has been conducted at the request of the competent authority for the implementation of cybersecurity requirements pursuant to Article 79, paragraph 1, subparagraph 7 or Article 81, paragraph 1, subparagraph 2 of this Act, the entity for which the cybersecurity audit has been conducted shall submit the report referred to in Article 32, paragraph 4 of this Act to the competent authority for the implementation of cybersecurity requirements immediately upon receipt.

(7) The costs of conducting a cyber security audit shall be borne by key and important entities, unless otherwise prescribed by this Law.

Conducting a cybersecurity self-assessment

Article 35

(1) Significant entities are required to conduct a cybersecurity self-assessment at least once every two years.

(2) Important for conducting a cybersecurity self-assessment Entities may also use an external provider of such services.

(3) If the results of the conducted cybersecurity self-assessment show that cybersecurity risk management measures have been established in accordance with the cybersecurity risk management measures prescribed by this Act and the regulation referred to in Article 24 of this Act, relevant entities shall draw up a statement of compliance.

(4) If the results of the conducted cybersecurity self-assessment show that the established cybersecurity risk management measures are not in accordance with the cybersecurity risk management measures prescribed by this Act and the regulation referred to in Article 24 of this Act, relevant entities are obliged to establish a plan for further action, including a plan for a timely re-assessment of cybersecurity self-assessment and correction of identified deficiencies.

(5) Important entities shall submit the statement referred to in paragraph 3 of this Article and the plan referred to in paragraph 4 of this Article to the competent authority for the implementation of cybersecurity requirements without delay, and no later than eight days from the date of their compilation.

(6) The costs of implementing the cybersecurity self-assessment shall be borne by the relevant entities.

Implementing regulation for cybersecurity self-assessment

Article 36

The rules, technical requirements, standards, forms and procedures applied during the cybersecurity self-assessment, including the content of the declaration of conformity, will be regulated by the regulation referred to in Article 24 of this Act.

CHAPTER II.
NOTIFICATION OBLIGATIONS ABOUT CYBERNETIC THREATS AND INCIDENTS

Notification of significant incidents

Article 37.

(1) Key and important entities are obliged to notify the competent CSIRT of any incident that has a significant impact on the availability, integrity, confidentiality and authenticity of data relevant to the entity's business and/or the continuity of the services they provide or the activities they perform (hereinafter: significant incident).

(2) An incident is considered a significant incident:

– if it has caused or may cause serious disruptions in the functioning of the services provided by the entity or the activities it performs or financial losses for the entity

– if it has affected or could affect other physical or legal persons person by causing significant material or non-material damage.

(3) Key and important entities are obliged to submit the notifications from paragraph 1 of this article to criminal prosecution authorities in cases where there are grounds for suspecting that significant incidents were caused by the commission of a criminal offense, based on the provisions of the law governing criminal proceedings.

(4) Key and important entities are obliged to start delivering the notification referred to in paragraph 1 of this Article within 30 days from the date of delivery of the notification referred to in Article 19, paragraph 1 of this Act.

Notification of service recipients

Article 38.

(1) Key and important entities are obliged to inform recipients of their services about significant incidents that could be affected by such an incident.

(2) In the event of a serious cyber threat, key and important entities are obliged to inform recipients of their services who could be affected by such a threat of all possible protection measures or legal remedies that they can use to prevent or compensate for the damage caused and, if necessary, inform recipients of the service about the serious cyber threat itself.

(3) Key and important entities shall commence the delivery of the notification referred to in paragraphs 1 and 2 of this Article within 30 days from the date of delivery of the notification referred to in Article 19, paragraph 1 of this Act.

Notification on a voluntary basis

Article 39

Key and important entities can voluntarily notify the competent CSIRT of any incident, cyber threat and avoided incident.

Notification of a significant incident with cross-border and cross-sector impact

Article 40

(1) The single point of contact, at the request of the competent CSIRT or at its own discretion, informs the single points of contact of the affected member state and ENISA about a significant incident with cross-border effects, especially if the incident concerns two or more member states.

(2) The single point of contact, at the request of the competent CSIRT or according to its own assessment, shall inform the state administration bodies competent for the affected sectors about a significant incident with cross-sectoral impact.

Notifying the public of a significant incident

Article 41

If it is necessary to inform the public in order to prevent or resolve an ongoing significant incident or if the publication of information about a significant incident is in the public interest for some other reason, the competent CSIRT and, where appropriate, the CSIRTs or competent authorities of other affected Member States may, after consulting the single point of contact, the competent authority for the implementation of cybersecurity requirements or the competent authority for the implementation of specific laws, depending on the division of competences in Annex III to this Act, and the affected entity, inform the public about the significant incident or request a key and important entity to do so.

Notifying the single point of contact and ENISA

Article 42

(1) Competent CSIRTs shall notify the single point of contact of significant incidents, other incidents, serious cyber threats and near misses notified to them by key and important entities pursuant to Articles 37 and 39 of this Act, in accordance with its guidelines.

(2) The single point of contact shall submit to ENISA every three months a summary report including anonymised and aggregated data on significant incidents, other incidents, serious cyber threats and near misses notified by key and important entities to the competent CSIRT pursuant to Articles 37 and 39 of this Act.

A national platform for the collection, analysis and exchange of data on cyber threats and incidents

Article 43

(1) Information on the basis of Articles 37 and 39 of this Act and exchange of data on cyber threats and incidents between competent authorities from Annex III. of this Act is carried out through a national platform for the collection, analysis and exchange of data on cyber threats and incidents, as a single entry point for notification of cyber threats and incidents.

(2) The development and management of the national platform referred to in paragraph 1 of this article is the responsibility of CARNET.

Implementing regulation on notification of cyber threats and incidents

Article 44.

Criteria for determining significant incidents, including criterion thresholds if necessary due to the specificities of a particular sector, types and content of notifications from Articles 37 to 40 of this Act, deadlines for their submission, handling of these notifications, including the actions of the competent CSIRT in response to notifications received from

Articles 37 and 39 of this Act, rights of access and other issues relevant to the use of the national platform for collecting, analyzing and exchanging data on cyber threats and incidents, including the possibility of using other methods of delivering information from Articles 37 and 39 of this Act, are prescribed by the decree from Article 24 of this Act.

CHAPTER III.
SPECIAL REQUIREMENTS FOR MANAGEMENT OF DOMAIN NAME REGISTRATION DATA

The purpose of implementing specific requirements for the management of domain name registration data

Article 45

In order to ensure a reliable, resilient and secure domain name system, the registry of national Internet top-level domain names and registrars are required to implement specific requirements for the management of domain name registration data.

Content of information in databases on domain name registration and identification of domain users

Article 46

(1) The registry of top national Internet domain names and registrars are obliged to ensure that the domain name registration database contains information necessary for the identification of domain users and registrars who manage domain names and for contact with them, namely:

– domain name

– registration date

– the name of the domain user and his e-mail address and contact phone number

– the e-mail address and telephone number to contact the registrar who manages the domain name.

(2) The registry of national top-level Internet domain names and registrars are obliged to establish the identity of the domain user and verify his identity on the basis of identification documents, or documents, data or information obtained from a credible, reliable and independent source, including, if the domain user has one, a qualified certificate for an electronic signature or electronic seal or any other secure, remote or electronic, identification procedure regulated, recognised, approved or accepted by the relevant national authorities.

(3) Failure of the applicant for domain registration and the domain user to comply with the obligations prescribed by this Act constitutes grounds for denial of domain registration or deletion of the domain.

Obligations of the registry of national Internet top-level domain names and registrars

Article 47

(1) If the application for domain registration does not contain all the information referred to in Article 46, paragraph 1, subparagraphs 1 to 3 of this Act, the registry of national top-level Internet domains and registrars shall be obliged to reject such an application and notify the applicant of the denial of domain registration or temporary deactivation of the domain and the inability to use it until the application is duly submitted, within eight days from the date of receipt of such notification.

(2) The registry of national top-level Internet domain names and registrars are obliged to periodically, and at least once a year, conduct checks for all their domain users on the existence of domain users, as well as on the compliance of domain users' actions with the obligations under the regulations governing the organization and management of national top-level Internet domains.

(3) In the event of unavailability of the domain user within the framework of multiple checks referred to in paragraph 2 of this Article on various registered contact details of the domain user, or if abuse of rights or other improper conduct of the domain user is established, the registry of national top-level Internet domain names and registrars are obliged to delete such a domain.

(4) The registry of national top-level Internet domain names and registrars are obliged to establish and publicly publish database management policies referred to in Article 46 of this Act, which must also include procedures for verifying data from domain registration applications.

(5) The registry of national top-level Internet domain names and registrars shall, without delay, publicly publish information on the registration of domain names that is not personal data after the registration of a domain name.

Data storage and access to domain user data

Article 48.

(1) The Registry of National Top-Level Internet Domain Names and registrars shall be obliged to keep the data, information and documentation collected pursuant to Articles 46 and 47 of this Act for 25 years from the termination of the user's right to use the domain.

(2) The documentation referred to in paragraph 1 of this Article must contain:

– identification documents and other documentation on the basis of which the identity of the domain user was determined

– request for domain registration and other documentation related to domain registration.

(3) The registry of national top-level Internet domain names and registrars are obliged to deliver or otherwise provide access to data on the domain user to law enforcement authorities and the competent CSIRT, the body responsible for the protection of personal data and other legal entities with public powers, as well as to state bodies in the exercise of public powers, upon their reasoned request, without delay, and no later than 72 hours from receipt of the request.

(4) The registry of national top-level Internet domain names and registrars are obliged to delete personal data about the domain user after the expiry of the retention period referred to in paragraph 1 of this Article, and to destroy the documentation referred to in paragraph 2 of this Article in accordance with the regulations on the protection of personal data.

(5) The registry of national top-level Internet domain names and registrars shall be obliged to indicate in their management policies referred to in Article 47, paragraph 4 of this Act their obligation to act in accordance with paragraphs 1 and 3 of this Article.

(6) Technical and organizational measures for the protection of personal data of domain users are regulated by special regulations governing the organization and management of the national top-level Internet domain.

Implementation of compliance control with special requirements for management of name registration data

Article 49

The state administration body responsible for science and education shall monitor the compliance of the actions of the registry of top-level national Internet domains and registrars with the special requirements for the management of domain name registration data from Articles 45 to 48 of this Act.

PART FOUR
VOLUNTARY MECHANISMS OF CYBERNETICS PROTECTION

Implementation of cyber security self-assessments and notification of incidents and cyber threats on a voluntary basis

Article 50

(1) Any entity that is not categorized as a critical and important entity in accordance with this Law may:

– conduct cybersecurity self-assessments for network and information systems used in its business or in the provision of its services

– voluntarily notify the competent CSIRT of any significant incident, other incidents, cyber threats or avoided incidents, provided that it periodically conducts cybersecurity self-assessments referred to in subparagraph 1 of this paragraph.

(2) The possibility of self-assessment of cyber security and voluntary notification from paragraph 1 of this article will be regulated by the decree from article 24 of this law.

National system for detecting cyber threats and protecting cyberspace

Article 51

(1) In order to increase overall capability and resilience in the area of cybersecurity, the central state authority for cybersecurity shall continuously develop a national system for detecting cyber threats and protecting cyberspace (hereinafter: the national system).

(2) The national system may be accessed voluntarily by key entities, important entities and other entities not categorized as key or important entities in accordance with this Act, depending on the assessment of the criticality of the entity carried out by the central state authority for cybersecurity.

(3) Access to the national system may be implemented as a mandatory cyber protection measure for public sector entities, if such an obligation is prescribed by the regulation referred to in Article 24 of this Act.

(4) Access to the national system shall be carried out on the basis of agreements concluded between the central state authority for cybersecurity and the entity accessing the system.

(5) Accession to the national system does not affect the obligations of key and important entities referred to in Article 25 of this Act, but represents an additional measure of cyber protection.

Criteria for the implementation of the assessment of the subject's criticality

Article 52

(1) The assessment of the criticality of an entity referred to in Article 51, paragraph 2 of this Act shall be carried out on the basis of the following criteria:

– the importance and significance of the services provided by the entity or the activities performed by the entity in relation to other providers of the same or similar services and activities in the Republic of Croatia

- the importance of network and information systems used by the entity in providing services or performing activities and their exposure to risks, dangers and threats in cyberspace and

- the state of the network and information systems used by the entity in providing services or performing activities, related to the way of designing, managing and maintaining network and information systems of the entity's security systems, as well as the relevant European and international standards and security practices applied.

(2) Assessment of the criticality of the entity referred to in Article 51, paragraph 2 of this The law is implemented on the basis of:

– the entity's request to join the national system or

– a proposal for accession to the national system submitted by a state administration body or regulatory body competent for the sector to which the entity belongs.

(3) The requests and proposals referred to in paragraph 2 of this Article shall be submitted the central state authority for cybersecurity.

(4) Submission of requests and proposals for accession to the national system, collection of data necessary for conducting an assessment of the criticality of entities for the purpose of accession to the system and implementation of accession of entities to the national system shall be regulated by the regulation referred to in Article 24 of this Act.

Voluntary exchange of information on cyber security

Article 53

(1) Key entities, important entities and other entities not categorized as key or important entities in accordance with this Act may voluntarily exchange cybersecurity information with each other for the purpose of increasing the level of cybersecurity or handling incidents.

(2) The exchange of information referred to in paragraph 1 of this article may include information related to cyber threats, including information on the source of the threat, avoided incidents, vulnerabilities, techniques and procedures, threat indicators, tactics, techniques and procedures of cyber attackers, indicators of compromise, cyber security warnings and recommendations on the configuration of cyber security tools to detect cyber attacks.

(3) The exchange of information referred to in paragraph 2 of this Article shall take place between the entities referred to in paragraph 1 of this Article and, where appropriate, their suppliers or service providers through information exchange mechanisms established specifically for these purposes.

(4) The mechanisms referred to in paragraph 3 of this article are established on the basis of an agreement on the voluntary exchange of information on cyber security.

(5) The agreement referred to in paragraph 4 of this Article shall determine the conditions for accession to the mechanism established by the agreement, the content of the information to be exchanged, the possibility of using dedicated platforms and other tools for automated information exchange, as well as all other operational elements essential for the efficient and secure exchange of information.

(6) Key and important entities shall notify the competent authority for the implementation of cybersecurity requirements of their participation in the mechanisms for the voluntary exchange of cybersecurity information referred to in paragraph 3 of this Article, and public sector entities that are categorized as key entities shall additionally request the opinion of the central state cybersecurity authority regarding such participation and the scope of information that they may exchange with other stakeholders involved.

Coordinated vulnerability detection

Article 54.

(1) Every natural and legal person can anonymously report a vulnerability.

(2) Vulnerability reports are submitted to the CSIRT vulnerability disclosure coordinator.

(3) The CSIRT Vulnerability Disclosure Coordinator acts as a trusted intermediary who, as necessary, facilitates the interaction between the natural or legal person reporting the vulnerability and the manufacturer or provider of potentially vulnerable ICT products or ICT services, at the request of either party.

(4) The tasks of the CSIRT vulnerability disclosure coordinator are to identify and contact the entities concerned, provide assistance to natural or legal persons reporting vulnerabilities, and negotiate a timeframe for the coordinated disclosure and management of vulnerabilities affecting multiple entities.

(5) The CSIRT vulnerability detection coordinator ensures the implementation of further measures regarding the reported vulnerability and ensures the anonymity of the natural or legal person reporting the vulnerability.

(6) When exchanging data on reported vulnerabilities, the CSIRT vulnerability coordinator is required to ensure the anonymity of the vulnerability reporter using the technique of removing direct identifiers, the technique of generalization, the technique of random data modification, or other known techniques.

(7) When, for the purpose of implementing the tasks referred to in paragraph 4 of this Article, it is necessary to store data on the vulnerability reporter, the CSIRT vulnerability detection coordinator shall keep records of the stored data.

(8) The CSIRT vulnerability detection coordinator is obliged to keep the data and records referred to in paragraph 7 of this Article for a maximum of three years from the vulnerability report, and after the expiry of that period, the personal data of the vulnerability reporter shall be deleted and the records referred to in paragraph 7 of this Article shall be destroyed in accordance with the regulations on the protection of personal data.

(9) The CSIRT vulnerability detection coordinator submits information on newly discovered vulnerabilities to the competent CSIRTs from this Act, together with instructions on how to further notify the entities under their jurisdiction of vulnerabilities.

(10) Competent CSIRTs draw up guidelines intended for users of vulnerable ICT products or ICT services on how to mitigate the risks arising from discovered vulnerabilities and deliver notifications with best practices to the entities they are in charge of on the basis of this Act.

(11) If the reported vulnerability could have a significant impact on entities in more than one Member State, the CSIRT vulnerability coordinator shall, as appropriate, cooperate with CSIRTs from other Member States that have been designated vulnerability coordinators within the CSIRT network.

(12) The tasks of the CSIRT vulnerability detection coordinator are performed by CSIRT at the central state authority for cybersecurity.

PART FIVE

STRATEGIC PLANNING AND MANAGEMENT CYBER SECURITY

National act of strategic planning in the field of cyber security

Article 55

(1) The Government, on the proposal of the central state body for cyber security, adopts a medium-term act of strategic planning in the field of cyber security.

(2) The strategic planning act referred to in paragraph 1 of this Article shall determine:

– specific objectives and priorities in the field of cybersecurity development that at least encompass the public policies from Annex IV to this Act, and

- the framework for monitoring and evaluating the implementation of goals and priorities from subparagraph 1 of this paragraph.

(3) For the purpose of developing measures for the implementation of special goals and priorities of the strategic planning act from paragraph 1 of this article, an action plan for its implementation is drawn up.

(4) Reporting, monitoring and evaluation of the strategic planning act referred to in paragraph 1 of this article shall be carried out in accordance with the regulation regulating the area of strategic planning and management of the development of the Republic of Croatia.

(5) The central state authority for cybersecurity shall notify the European Commission of the adoption of the strategic planning act referred to in paragraph 1 of this Article within three months of its adoption, or within three months of the adoption of its amendments and/or supplements.

Management of large-scale cyber incidents and cyber crises

Article 56

(1) The central state authority for cybersecurity is the authority responsible for managing large-scale cyber incidents and cyber crises (hereinafter: cyber crisis management).

(2) The Government, on the proposal of the body responsible for cyber crisis management, shall adopt a national cyber crisis management program.

(3) The national program referred to in paragraph 2 of this article determines the capacities, means and procedures for managing cyber crises and determines in more detail:

- cybercrisis management goals, including goals for the development of national preparedness measures, as well as compliance with the European Union cybercrisis management framework

– coherence with the national general framework for crisis management

– measures and activities to strengthen national preparedness

- the plan for the implementation of national preparedness measures, including the plan for training activities and the implementation of exercises that are an integral part of the plan from Article 58 of this Act

– tasks and responsibilities of bodies involved in cyber crisis management

- the role of the public and private sector and the infrastructure essential for managing cyber crises and

– national procedures and coordination at the national level necessary to ensure support for coordinated cyber crisis management carried out at the European Union level and the effective participation of the Republic of Croatia in such management.

(4) An integral part of the national program referred to in paragraph 2 of this article are the standard operating procedures that determine in more detail:

- cybercrisis management procedures, including their integration into the general framework of national crisis management and

– all issues relevant to data exchange.

(5) The body responsible for cyber crisis management shall notify the European Commission and the EU-CyCLONe network of the adoption of the national programme referred to in paragraph 2 of this Article within three months of its adoption, or of its amendments or the adoption of a new programme.

Assessing the state of cyber security

Article 57

(1) For the purpose of exchanging acquired knowledge and experience, strengthening trust, strengthening capacities and capabilities in the field of cybersecurity, and improving policies in the field of cybersecurity, self-assessment procedures of the state of cybersecurity shall be organized and implemented.

(2) Self-assessments of the state of cybersecurity shall also be organised and carried out at the national level (hereinafter referred to as: national self-assessments), independently of the implementation of self-assessments carried out by Member States within the framework of peer assessments carried out in accordance with the methodology established by the Cooperation Group, the European Commission and ENISA.

(3) Within the framework of national self-assessments, the level of implementation of cybersecurity requirements prescribed by this Act, the level of cyber capacities, including available financial, technical and human resources, the effectiveness of the performance of tasks and the level of implementation of cooperation between the competent authorities for the implementation of cybersecurity requirements, competent CSIRTs, competent authorities for the implementation of special laws and competent authorities from the law regulating the area of critical infrastructure, the level of implementation of mechanisms for the exchange of information on cybersecurity referred to in Article 53 of this Act and special issues of a cross-sectoral nature shall be assessed.

(4) The methodology for the implementation of Member States' self-assessments adopted by the Cooperation Group, the European Commission and ENISA shall be applied to national self-assessments in an appropriate manner.

(5) Plans and programs for the implementation of self-assessments carried out by member states within the framework of peer assessments from paragraph 2 of this article and national self-assessments are adopted by the Government, upon the proposal of the central state body for cyber security.

(6) Before commencing the peer reviews referred to in paragraph 2 of this Article, the central state cybersecurity authority shall consider the existence of risks of conflicts of interest of the cybersecurity experts appointed to carry them out and shall inform the other Member States, the Cooperation Group, the European Commission and ENISA of the identified risks.

(7) Where there are justified reasons for opposing the appointment of an individual cybersecurity expert to conduct peer reviews referred to in paragraph 2 of this Article, the central state cybersecurity authority shall inform the appointing Member State thereof.

Cybersecurity exercises

Article 58

(1) In order to achieve the maximum level of preparedness, especially in the event of cyber crises, cybersecurity exercises are conducted to verify available capacities and capabilities in the field of cybersecurity, test established communication mechanisms, as well as exchange acquired knowledge, experiences and best practices, and strengthen trust.

(2) Cybersecurity exercises are organized and conducted based on the Cybersecurity Exercise Implementation Plan adopted by the Government at the proposal of the central state body for cybersecurity, for a period of two years.

(3) The Cybersecurity Exercise Implementation Plan shall include:

a) international cybersecurity exercises – exercises conducted in the Republic of Croatia with the participation of experts from other Member States or other countries and international organizations, and exercises held abroad with the participation of representatives of competent authorities from the Republic of Croatia

b) national cybersecurity exercises – exercises planned, organized and conducted by the competent authorities under this Act, including the competent CSIRTs.

(4) The cybersecurity exercise implementation plan determines the number of planned exercises, exercise leaders, the name and objective of the exercises, the date and location of the exercises, the approximate number of exercise participants, the holders of financial obligations for the implementation of the exercises, and the content, deadlines and method of reporting on the implementation of the exercises.

(5) Proposals for plans for the implementation of cybersecurity exercises shall be prepared by the central state authority for cybersecurity in cooperation with other competent authorities for the implementation of cybersecurity requirements, competent CSIRTs and competent authorities for the implementation of special laws.

PART SIX

COMPETENT AUTHORITIES IN THE FIELD OF CYBERNETICS SECURITY

CHAPTER I.

COMPETENT AUTHORITIES FOR THE IMPLEMENTATION OF CYBER SECURITY REQUIREMENTS

Tasks of competent authorities for the implementation of cybersecurity requirements

Article 59

(1) The competent authorities for the implementation of cybersecurity requirements shall perform the following tasks:

- carry out the categorization of entities in accordance with this Law and establish and maintain lists of key and important entities

– conduct expert supervision over key and important entities in the implementation of cybersecurity requirements in accordance with this Act and the regulations referred to in Article 24 of this Act

- in matters of categorization of entities, actions in the event of significant incidents and professional supervision, they closely cooperate and coordinate their work with the state administration bodies responsible for the individual sector in which the entities under their jurisdiction operate.

– cooperate closely and exchange relevant information with personal data protection authorities in resolving incidents that have led to personal data breaches, or with law enforcement authorities when incidents are the result of criminal activities

– cooperate with each other and exchange relevant information and experiences in the implementation of this Act

– cooperate and exchange relevant information with the national coordination centre designated pursuant to Regulation (EU) 2021/887 of the European Parliament and of the Council of 20 May 2021 establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres (OJ L 202/1, 8.6.2021)

– cooperate with the relevant CSIRTs and

- perform other tasks that are prescribed by this Law to be performed by the authorities responsible for the implementation of cyber security requirements.

(2) Competent authorities for the implementation of cyber security requirements perform the tasks referred to in paragraph 1 of this Article according to the division of competences from Annex III. of this Act.

(3) If an individual entity falls under the jurisdiction of two or more bodies listed in Annex III to this Act, in order to avoid duplication and overlap in the performance of tasks, the central state body for cybersecurity, in cooperation with all bodies competent for the entity, shall draw up a protocol on the actions of the competent bodies, taking into account primarily the main activity of the entity.

(4) The procedure for drafting the protocol referred to in paragraph 3 of this Article shall be initiated by the central state authority for cybersecurity ex officio, at the proposal of one of the competent authorities pursuant to Annex III to this Act or at the proposal of the entity.

Application of cybersecurity requirements to competent authorities for the implementation of cybersecurity requirements

Article 60

(1) Competent authorities for the implementation of cybersecurity requirements that are not categorized as key or important entities in accordance with this Act are obliged to:

- apply the requirements of cyber security from Article 25 of this Act in accordance with the provisions of the regulation from Article 24 of this Act that refer to key entities and

– at least once every two years, conduct cyber security self-assessments for the network and information systems they use in their business and report on the conducted cyber security self-assessments to the central state authority for cyber security.

(2) For the purposes of paragraph 1, subparagraph 1 of this Article, the tasks of the CSIRT- and is carried out by the central state authority for cybersecurity.

Tasks of the central state authority for cybersecurity

Article 61

(1) The central state authority for cybersecurity, in addition to the ve from Article 59 of this Act, performs the following tasks:

- coordinates the preparation and adoption of the act of strategic planning from cyber security areas

– directs and monitors the implementation of the strategic planning act from the cybersecurity field

- improves cyber security risk management measures by planning the development of the cyber security regulatory framework

- monitors the implementation of this Act and provides recommendations, opinions, guidelines and instructions related to the implementation of cyber security requirements

- encourages the establishment of mechanisms for the voluntary exchange of information on cyber security from Article 53 of this Act and provides recommendations, guidelines and instructions for their easier establishment

– as the body responsible for cyber crisis management, coordinates activities related to cyber crisis management at the national level

– participates in the work of the EU-CyCLONe network and coordinates activities related to cyber crisis management at the European Union level on behalf of the Republic of Croatia

– performs the tasks of a single point of contact

- performs the tasks of the CSIRT body according to the division of competences from Annex III. of this Act

- carries out activities for the purpose of detecting cyber threats and protecting the national cyber space

– produces reports on the state of cybersecurity

– cooperates with other competent authorities under this Act

– achieves international cooperation in cybersecurity matters within the framework of its competences established by this Act, and

- performs other tasks prescribed by this Law
to be carried out by the central state authority for cybersecurity.

(2) The central state authority for cyber security is the Security Intelligence Agency.

Tasks of the single point of contact

Article 62

The single point of contact performs the following tasks:

– inform the European Commission without delay of the names of the competent authorities referred to in Article 54, paragraph 12, Article 56, paragraph 1, Article 61, paragraph 1, subparagraphs 6, 7 and 8, and Article 70, paragraph 1 of this Act, as well as their tasks and any subsequent changes to the information provided

– informs the European Commission without delay of the provisions of this Act governing the imposition of fines and of any subsequent changes to the information provided

– participates in the work of the Cooperation Group

– ensures cross-border cooperation of competent authorities for the implementation of cybersecurity requirements, competent authorities for the implementation of specific laws and competent CSIRTs with relevant authorities in other Member States and, where appropriate, with the European Commission and ENISA

– ensures cross-sectoral cooperation between competent authorities for the implementation of cybersecurity requirements, competent authorities for the implementation of specific laws and competent CSIRTs with other relevant authorities at the national level

– develops guidelines on the content of notifications, the method and deadlines for notifying the single point of contact about received notifications of significant incidents, other incidents, cyber threats and avoided incidents, and

- performs other tasks that are prescribed by this Law to be performed by a single point of contact.

National Cyber Security Center

Article 63

The National Center for Cyber Security is established in the Security Intelligence Agency to perform the tasks referred to in Articles 59, 61 and 62 of this Act.

CHAPTER II.
COOPERATION OF COMPETENT AUTHORITIES AT THE NATIONAL LEVEL

Cooperation with competent authorities for the implementation of special laws

Article 64.

(1) The central state authority for cybersecurity and other competent authorities for the implementation of cybersecurity requirements and competent authorities for the implementation of special laws shall cooperate with each other and exchange relevant information and experiences.

(2) The central state authority for cybersecurity shall provide assistance in the implementation of supervisory activities carried out on the basis of special laws referred to in Article 8 of this Act, when requested by the competent supervisory authorities.

(3) The assistance referred to in paragraph 2 of this Article shall be provided on the basis of a cooperation agreement regulating all relevant issues relating to the coordination and implementation of supervisory activities, including a mechanism for the exchange of relevant information on supervision and access to information related to the cybersecurity of entities to which the special laws referred to in Article 8 of this Act apply.

(4) The central state authority for cybersecurity shall inform the Supervisory Forum established pursuant to Article 32, paragraph 1 of Regulation (EU) 2022/2554 of the supervisory activities carried out pursuant to this Act over key and important entities designated as key third party ICT service providers pursuant to Article 31 of Regulation (EU) 2022/2554.

Cooperation with competent authorities under the law governing the area of critical infrastructure

Article 65

(1) Competent authorities for the implementation of cyber security requirements and competent authorities from the law governing the area of critical infrastructure cooperate with each other and exchange relevant information, namely information on:

- determination of subjects as critical subjects based on the law governing the area of critical infrastructure

– the risks, threats and incidents to which critical entities are exposed, as well as the measures taken in response to risks, threats and incidents, regardless of whether these risks, threats and incidents originate from cyber or physical space

– the cybersecurity requirements and physical protection measures implemented by these entities, and

– the results of supervisory activities carried out over the actions of critical entities in accordance with this Act or the law regulating the area of critical infrastructure.

(2) Competent authorities from the law governing the area of critical infrastructure may request the competent authorities for the implementation of cyber security requirements and the competent authorities for the implementation of special laws to exercise their supervisory powers over entities that have been determined as critical entities.

(3) The exchange of information on critical subjects takes place within the framework established by the agreement of the central state body for cyber security and the competent coordinating body of the state administration from the law governing the area of critical infrastructure.

(4) The agreement from paragraph 3 of this article regulates all essential issues related to the exchange of information and coordination of competent authorities, including the method of exchanging information from paragraph 1 of this article, as well as information about the conducted supervision of critical entities.

CHAPTER III.
CSIRT RESPONSIBILITIES

CSIRT tasks

Article 66

(1) The CSIRT performs the following tasks:

– monitors and analyzes cyber threats, vulnerabilities and incidents and, upon their request, provides assistance to key and important entities regarding the monitoring of their network and information systems in real or near real time

– provides early warnings and announcements and informs key and important entities, other competent authorities under this Act or other relevant stakeholders about cyber threats, vulnerabilities and incidents, if possible in near real time

– processes received notifications about incidents and, if circumstances allow, after receiving notification about the incident, delivers relevant information to key and important entities regarding further action, especially information that could contribute to the effective resolution of the incident

– responds to incidents and provides assistance to key and important subjects, at their request or with their consent

– at the request of key and important entities, conducts proactive scanning of network and information systems of key and important entities, in order to detect vulnerabilities with a potentially significant impact

- collects and analyzes computer forensic data and conducts a dynamic analysis of risks and incidents in the sectors for which he is responsible, and prepares an overview of the situation in the sector in terms of cyber security

- adopts guidelines for harmonizing and improving the state of implementation of the notification obligation from Articles 37 and 38 of this Act and the implementation of voluntary notification from Article 39 of this Act

– in cooperation with the competent authority for the implementation of cyber security requirements, determines the cross-border and cross-sectoral effects of significant incidents

– cooperates with other CSIRTs at national and international level

– participates in the work of the CSIRT network

- provides mutual assistance in accordance with its capacities and competences to other members of the CSIRT network, upon their request

- cooperates and, as necessary, exchanges relevant information with sectoral or intersectoral communities of key and important subjects established on the basis of the agreement on voluntary exchange of information on cyber security from Article 53 of this Act

– cooperates with relevant stakeholders from the private sector and, for the purpose of establishing such cooperation, promotes the adoption and implementation of common or standardized practices, categorization and taxonomy plans in relation to incident handling, cyber crisis management and coordinated vulnerability disclosure pursuant to Article 54 of this Act

– contributes to the introduction and use of tools for secure information exchange

– participates in the implementation of peer reviews conducted in accordance with the methodology established by the Cooperation Group, the European Commission and ENISA

– participates in the implementation of self-assessments of the state of cybersecurity carried out at the national level, and

– performs other tasks prescribed by this Act to be performed by the competent CSIRT.

(2) When performing the tasks referred to in paragraph 1 of this Article, the CSIRT shall give priority to priority tasks according to the risk assessment, and when processing received notifications, based on this Act, it shall give priority to processing notifications about significant incidents.

(3) When the cooperation referred to in paragraph 1, subparagraph 9 of this Article includes the participation of the CSIRT in international cooperation networks and/or or cooperation with CSIRTs of third countries, the CSIRT is required to use appropriate protocols for information exchange.

Conducting proactive non-intrusive scanning of publicly available network and information systems

Article 67

(1) In order to detect vulnerable or insecurely configured network and information systems, the CSIRT may conduct proactive non-intrusive scanning of publicly available network and information systems of key and important entities under its jurisdiction.

(2) The scanning referred to in paragraph 1 of this Article must not have a negative impact on the functioning of the services provided by the key and important entity and on the activities it performs.

(3) The competent CSIRT is obliged to inform the key and important subject about discovered vulnerabilities or insecurely configured network and information systems based on the scan from paragraph 1 of this article.

Cooperation of entities with the competent CSIRT and the absence of liability of the CSIRT for the damage caused

Article 68.

(1) Key and important entities are obliged to cooperate with the competent CSIRT and exchange necessary information with it in the incident resolution process.

(2) In performing its tasks, the CSIRT cannot be held liable for damage caused by an incident to the network and information systems of key and important entities.

Ensuring conditions for performing the tasks of the competent authority CSIRT

Article 69

The competent CSIRT is obliged to:

– ensure a high level of availability of their communication services by avoiding single points of failure, with the availability of means for two-way communication and clearly defined and known communication channels for their clients and associates

– ensure the confidentiality and reliability of the activities they carry out

– locate your premises and support information systems in secure locations

– ensure that the appropriate system for managing requests for incident resolution is in place

– ensure a sufficient number of trained employees, as well as equipment with redundant systems and appropriate workspaces, in order to ensure continuity in performing CSIRT tasks and develop the technical capabilities necessary to perform CSIRT tasks

– have a secure and resilient communication and information infrastructure for the exchange of information with key and important entities and other relevant stakeholders from this Law, and

– provide other resources necessary for the effective performance of CSIRT tasks.

Determining the responsibilities of a CSIRT

Article 70

(1) The central state authority for cybersecurity, through the National Cybersecurity Center and CARNET, through the National CERT, shall perform the tasks of the CSIRT at the national level, according to the division of competences set out in Annex III to this Act.

(2) For the purposes of Article 50, paragraph 1, subparagraph 2 of this Act, the central state cybersecurity authority shall perform the tasks of the CSIRT for state bodies, legal entities with public authority and local and regional self-government units, and CARNET shall perform the tasks of the CSIRT for public and private entities, including the public.

Tasks of public interest

Article 71

The tasks established by this Act for the central state authority for cybersecurity, the competent authorities for the implementation of cybersecurity requirements and the competent CSIRTs, including tasks related to cooperation, assistance and exchange of information, at the national and international level, are necessary to ensure the effective implementation of procedures and measures to achieve a high level of cybersecurity in sectors of particular importance for the smooth performance of key social and economic activities and the proper functioning of the internal market, and the performance of these tasks is in the public interest.

PART SEVEN
PROTECTION AND PROCESSING OF PERSONAL DATA AND ACCESS TO INFORMATION

Protection and processing of personal data

Article 72

Regulation (EU) 2016/679 applies to the processing of personal data carried out by the competent authorities for the implementation of cybersecurity requirements and the competent CSIRTs within the framework of their tasks prescribed by this Act.

Restrictions on the use and right of access to information

Article 73

(1) Lists of key and important subjects, as well as all other records generated within the framework of the implementation of this Act, shall be used and exchanged exclusively for the purpose of carrying out the requirements of this Act, while respecting the need to limit access to those records, under the conditions prescribed by the law governing the protection of natural persons with regard to the processing and exchange of personal data for the purposes of preventing, investigating, detecting or prosecuting criminal offences or executing criminal sanctions.

(2) The lists and other records referred to in paragraph 1 of this Article constitute information in relation to which it is possible to restrict the right of access to the user of the right to access information and reuse of information, depending on the results of the proportionality and public interest test carried out in accordance with the provisions of the law governing the right to access information.

Obligation to report breaches involving personal data breaches

Article 74

(1) If the competent authority for the implementation of cybersecurity requirements, during the professional supervision of the implementation of cybersecurity requirements or the performance of other activities under this Act, becomes aware of a breach of the obligations under Article 25 of this Act committed by a key or important entity that includes a breach of personal data, it shall be obliged to notify the authority competent for the protection of personal data of that breach and the established facts without undue delay.

(2) If the breach referred to in paragraph 1 of this Article is reported by a body responsible for personal data protection established in another Member State, the body responsible for implementing cybersecurity requirements shall also report the same breach to the Personal Data Protection Agency.

PART EIGHT

PROFESSIONAL SUPERVISION OF THE IMPLEMENTATION OF REQUESTS CYBER SECURITY

CHAPTER I.
IMPLEMENTATION OF PROFESSIONAL SUPERVISION

Implementation of professional supervision over the key entity

Article 75

(1) Expert supervision of the implementation of cybersecurity requirements (hereinafter: expert supervision) in a key entity shall be carried out at least once every three to five years.

(2) Professional supervision of a key entity shall be carried out even before the expiry of the deadlines referred to in paragraph 1 of this Article if the competent authority for the implementation of cybersecurity requirements has information indicating that the entity is not implementing cybersecurity risk management measures in accordance with the prescribed obligations or that it is not fulfilling the obligations related to reporting cyber threats and incidents in the prescribed manner and within the prescribed or set deadlines or that it is not acting in accordance with the requests of the competent authorities referred to in this Act.

(3) The timetable for the implementation of expert supervision from paragraph 1 of this article is determined by the annual work plan of the competent authority for the implementation of cyber security requirements.

(4) For the purpose of determining the timetable for the implementation of expert supervision referred to in paragraph 1 of this Article and deciding on priorities in the implementation of supervision, the competent authority for the implementation of cybersecurity requirements may classify key entities according to their risk category.

Conducting professional supervision over a significant entity

Article 76

(1) Professional supervision of a significant entity is carried out when the competent authority for the implementation of cybersecurity requirements has information indicating that the entity is not implementing cybersecurity risk management measures in accordance with the prescribed obligations or that it is not fulfilling obligations related to reporting cyber threats and incidents in the prescribed manner and within the prescribed or set deadlines or that it is not acting in accordance with the requests of the competent authorities under this Act.

(2) For the purpose of determining the timetable for the implementation of expert supervision referred to in paragraph 1 of this Article and deciding on priorities in the implementation of supervision, the competent authority for the implementation of cybersecurity requirements may classify important entities according to the risk category. things.

Method of conducting expert supervision and notification of supervision implementation

Article 77

(1) The competent authorities for the implementation of cybersecurity requirements shall conduct expert supervision:

- in such a way that in the supervised subject there is immediate insight into the data, documentation, conditions and methods of implementation of the measures managing cyber security risks, fulfilling prescribed obligations to inform about cyber threats and incidents, and acting according to the requirements of competent authorities from this Act or

- by inspecting the reports on the conducted cyber security audits and, if necessary, other, additionally requested and submitted data and documentation of the supervised entity.

(2) The competent authority for the implementation of cybersecurity requirements shall be obliged to notify the supervised entity of the implementation of the expert supervision referred to in paragraph 1, subparagraph 1 of this Article no later than five days before the start of the supervision.

(3) By way of derogation from paragraph 2 of this Article, when expert supervision is carried out pursuant to Article 75, paragraph 2 and Article 76, paragraph 1 of this Act, the expert supervision referred to in paragraph 1, subparagraph 1 of this Article may be carried out without prior notice:

– in the event that there are reasons indicating the need for urgent action by the entity with a significant incident or

– to prevent or mitigate risks arising from a serious cyber threat.

(4) When conducting the expert supervision referred to in paragraph 1, subparagraph 1 of this Article, the competent authority for the implementation of cybersecurity requirements shall take into account the impact of the supervision on the work and operations of the supervised entity and ensure that the implementation of the supervision does not lead to interruptions in the work and operations of the supervised entity, unless the expert supervision cannot be conducted in another manner.

Obligations of key and important entities within the scope of professional supervision

Article 78

Key and important entities are obliged to enable the implementation of expert supervision and ensure all conditions for the unhindered implementation of expert supervision, which in particular includes the obligation to:

- enabling unhindered access and use of premises, equipment, systems and other infrastructure or technical means of the supervised entity

– enabling access to and use of all necessary data and documentation, including making copies

- enabling conversations with competent and responsible persons of the supervised entity.

CHAPTER II.
AUTHORITIES OF COMPETENT AUTHORITIES FOR THE IMPLEMENTATION OF CYBERNETIC SECURITY REQUIREMENTS IN THE EXECUTION OF PROFESSIONAL SUPERVISION

General supervisory measures for key and important entities

Article 79

(1) The competent authority for the implementation of cybersecurity requirements is authorized to perform expert supervision:

– conduct direct access to data, documentation, and network and information systems

– directly verify the conditions and methods of implementing cybersecurity risk management measures, including random checks

- directly gain insight into the documentation of the execution of the prescribed obligations to inform about cyber threats and incidents and other procedures according to the requirements of the competent authorities from this Act

- request data and documentation necessary for evaluating the proportionality of cyber security risk management measures applied by the entity

- request reports on cyber security audits carried out by the cyber security auditor referred to in Article 32 of this Act and other relevant evidence on the implementation of cyber security policies referred to in Article 30 of this Act

- request other data, documentation and information necessary for the implementation of supervision

– request the implementation of a targeted cybersecurity audit.

(2) When implementing the supervisory measures referred to in paragraph 1, subparagraphs 4 to 6 of this Article, the competent authority for the implementation of cybersecurity requirements shall state its purpose and specify in more detail the data, documentation and other information it requests from the entity.

(3) When the supervisory measure referred to in paragraph 1, subparagraph 7 of this Article is applied, the competent authority for the implementation of cybersecurity requirements shall prepare an additional cybersecurity analysis based on objective, non-discriminatory, fair and transparent risk assessment criteria, if necessary in cooperation with the supervised entity, in order to determine recommendations for improving the situation or reducing the risks to which the entity is or may be exposed.

Targeted cybersecurity audits

Article 80

(1) The implementation and scope of a targeted cybersecurity audit shall be determined depending on the available data on the assessment of the risks to which the supervised entity is or may be exposed.

(2) The costs of a targeted cybersecurity audit shall be borne by the supervised entity.

(3) By way of derogation from paragraph 2 of this Article, the costs of a targeted cybersecurity audit may be borne by the competent authority for the implementation of cybersecurity requirements if the assessment is carried out within the framework of the implementation of urgent measures that need to be taken to avoid or prevent significant incidents or mitigate the consequences of significant incidents or other risks to which the supervised entity is exposed, which have or may have a cross-border or cross-sectoral impact.

Special supervisory measures for key entities

Article 81

(1) In addition to the supervisory measures referred to in Article 79 of this Act, when performing professional supervision over a key entity, the competent authority for the implementation of cybersecurity requirements is authorized to request the implementation of:

- regular cyber security audits, when it has information from which it follows that the entity did not conduct the cyber security audit within the deadlines specified in Article 34, paragraph 1 of this Act, and

- extraordinary cyber security audits, in the event of a significant incident or when it is established that irregularities, deficiencies or omissions in the implementation of cyber security risk management measures have been identified in a previously conducted cyber security audit that have not been remedied in the meantime, or it has information that the subject is not implementing cyber security risk management measures in accordance with this Act and the regulations from Article 24 of this Act.

(2) Article 34, paragraph 7 of this Act shall apply to the costs of cybersecurity audits conducted pursuant to paragraph 1 of this Article.

(3) When a special supervisory measure referred to in paragraph 1, subparagraph 2 of this Article is applied in the event of a significant incident, the competent authority for the implementation of cybersecurity requirements shall prepare an additional cybersecurity analysis referred to in Article 79, paragraph 3 of this Act. of cyber security requirements may:

CHAPTER III.
CORRECTIVE MEASURES, TEMPORARY SUSPENSIONS AND PROHIBITIONS OF PERFORMING ACTIVITIES

Corrective measures for key and important subjects

Article 82

(1) The competent authority for the implementation of cybersecurity requirements, depending on the results of expert supervision, may impose the following corrective measures on key and important entities:

- issue warnings about violations of this Act and regulations from Article 24 of this Act

– issue binding instructions or orders requiring them to eliminate identified deficiencies or violations of this Act and the regulations referred to in Article 24 of this Act, specifying the measures that the entity should implement in order to prevent significant incidents or eliminate their consequences

- to order them to stop acting in violation of this Act and the regulation from Article 24 of this Act and not to repeat such an act

- to order them to ensure that their cyber security risk management measures are in accordance with prescribed obligations or to fulfill their obligations to inform about cyber threats and incidents in a prescribed manner and within a prescribed or set deadline, i.e. to act in a certain manner and/or within a set time limit according to the requirements of the competent authorities from this Act

- to order them to implement within a reasonable period of time the recommendations given in the report on the performed cyber security audit or in the framework of the prepared security analyzes and

- order to publish aspects of violations of this Act and the regulation from Article 24 of this Act in a certain manner.

(2) The instructions and orders from paragraph 1 of this article must contain a deadline for the implementation of corrective measures and a deadline for notification of the implementation of the pronounced corrective measures.

(3) If a key or important entity fails to comply with the imposed corrective measures referred to in paragraph 1, subparagraphs 1 to 5 of this Article, the competent authority for the implementation of cybersecurity requirements shall set the entity an additional appropriate deadline for the implementation of corrective measures.

(4) By way of derogation from paragraph 3 of this Article, in exceptional cases, the supervised entity shall not be given an additional appropriate deadline for implementing corrective measures if this would prevent the taking of urgent measures ordered to prevent or respond to significant incidents.

Special corrective measure for key entities

Article 83

(1) In addition to the corrective measures referred to in Article 82 of this Act, the competent authority for the implementation of cybersecurity requirements may appoint an officer for a specific period of time to monitor the compliance of a key entity with cybersecurity requirements.

(2) The decision on appointment referred to in paragraph 1 of this Article must include the period for which the officer for monitoring the entity's compliance with cybersecurity requirements is appointed and his/her tasks.

Temporary suspensions and prohibitions of activities

Article 84.

(1) If a key entity does not act in accordance with the pronounced corrective measures from Article 82 of this Act, the competent authority for the implementation

- request the competent authority to temporarily suspend the authorization issued to the entity for providing services or performing activities from Annex I or Annex II. of this Act

- demand from the competent body a temporary ban on the performance of management duties in the key entity by natural persons from Article 29 of this Act.

(2) The measures from paragraph 1 of this article are applied only until the key entity acts in accordance with the pronounced corrective measures from article 82 of this Act.

(3) The measures from paragraph 1 of this article do not apply to state administration bodies, other state bodies, units of local and regional (regional) self-government, and public entities that, in their capacity as public law bodies, represent public contracting authorities in the sense of regulations regulating public procurement.

Circumstances that are taken into account when making decisions on the imposition of corrective measures, proposing temporary suspensions and bans on activities

Article 85

(1) When making decisions on imposing corrective measures referred to in Articles 82 and 83 of this Act or submitting a request pursuant to Article 84 of this Act, the competent authority for the implementation of cybersecurity requirements shall take into account:

- the seriousness of the violation and the importance of the provisions that the supervised entity violates

– duration of injury

– relevant previous violations committed by the same entity

- the damage caused, including financial or economic losses, effects on other services or activities and the number of affected users

– whether the supervised entity acted intentionally or negligently

– measures taken by the supervised entity to prevent or mitigate damage

– acting in accordance with relevant codes of conduct or rules and conditions of certification for the provision of services or the performance of activities and

– the level of cooperation of persons referred to in Article 29 of this Act with the competent authorities referred to in this Act.

(2) The following are considered serious violations referred to in paragraph 1, subparagraph 1 of this Article:

– repeated injuries

- failure to report or resolve significant incidents

– failure to eliminate irregularities and deficiencies in accordance with the instructions or orders of the competent authority for the implementation of cybersecurity requirements

- preventing or hindering the implementation of the cyber security audit procedure requested by the competent authority for the implementation of cyber security requirements or monitoring activities ordered on the basis of Article 83 of this Act and

- providing false or extremely inaccurate information related to the implementation of cyber security requirements or other obligations arising from this Act or the regulation from Article 24 of this Act for the supervised entity.

Imposition of fines

Article 86

(1) In addition to the corrective measures prescribed by this Act and the submission of a request in accordance with Article 84 of this Act, the competent authority for the implementation of cybersecurity requirements may file a report of authorization against key and important entities responsible for a misdemeanor. to the prosecutor or issue a misdemeanor order in accordance with the misdemeanor provisions of this Act.

(2) By way of exception to paragraph 1 of this Article, in professional supervisions, a report may not be filed with the authorized prosecutor or a misdemeanor order may not be issued in accordance with the misdemeanor provisions of this Act if the supervised entity has been imposed an administrative fine by the body competent for the protection of personal data for personal data breaches arising from the same conduct of the entity in accordance with Regulation (EU) 2016/679.

CHAPTER IV.
PROCEDURE FOR PROFESSIONAL SUPERVISION

Contents of the minutes

Article 87

(1) After conducting expert supervision, the competent authority for the implementation of cybersecurity requirements shall draw up a record of the supervision conducted (hereinafter: the record).

(2) A copy of the minutes shall be delivered to the head of the supervised entity, or to another responsible person for the supervised entity (hereinafter: responsible person).

(3) The minutes must contain an indication of the subject of the expert supervision, the established factual situation and instructions on the right to submit objections to the minutes.

(4) If violations of prescribed obligations or non-compliance with cybersecurity requirements are identified in the conducted professional supervision, the minutes must contain a description of the identified violations and non-compliance, the supervisory measures imposed and the obligation to notify about the corrective measures taken.

Comments on the minutes

Article 88.

(1) The responsible person may submit comments on the minutes, in writing, within the deadline set for submitting comments by the competent authority for the implementation of cybersecurity requirements.

(2) When determining the deadlines for submitting comments, account shall be taken of the size of the entity, the scope of the expert supervision carried out and the factual situation established in this regard, the supervisory measures applied, as well as the established results of the expert supervision.

(3) By way of derogation from paragraph 2 of this Article, in exceptional cases the supervised entity shall not be allowed to submit objections to the minutes if this would prevent the taking of urgent measures ordered to prevent significant incidents or respond to such incidents.

Action on comments to the minutes

Article 89

(1) If the competent authority for the implementation of cybersecurity requirements determines that the objections to the minutes are fully or partially justified, it shall draw up a supplementary minute in which it will decide on the objections.

(2) If the competent authority for the implementation of cyber security requirements determines that the objections to the record are completely unfounded, it is obliged to submit a written notification to the supervised entity.

(3) The supplementary record referred to in paragraph 1 or the notification referred to in paragraph 2 of this Article shall be delivered to the responsible person within 30 days of the date of receipt of the objections.

(4) Against the supplementary minutes and the notification referred to in paragraph 3 of this No comments are allowed on the article.

Court protection

Article 90

After the delivery of the supplementary report or notification from Article 89 of this Act, the authorized person of the supervised entity may file a lawsuit before the competent administrative court to request an assessment of the legality of the actions of the competent authority for the implementation of cyber security requirements in relation to the subject of expert supervision and the report compiled on the professional supervision carried out.

Binding instructions for state administration bodies, other state bodies and local and regional self-government units

Article 91

(1) If deficiencies and violations of this Act and the regulation referred to in Article 24 of this Act are identified in the expert supervision of state administration bodies, other state bodies and local and regional self-government units, and the supervised body fails to implement the prescribed corrective measures within the set deadline, the central state body for information security shall submit a report on the results of the expert supervision of that body to the central state body for cybersecurity.

(2) The central state authority for cybersecurity shall issue binding instructions on the implementation of measures that the head of the supervised body is obliged to ensure, specifying the deadline for the implementation of such measures, and shall inform the Government thereof.

Records of completed expert inspections

Article 92

(1) Competent authorities for the implementation of cybersecurity requirements They are obliged to keep records of the expert inspections carried out.

(2) The records referred to in paragraph 1 of this Article shall be kept in accordance with the guidelines of the central state authority for cybersecurity.

Professional supervision of providers of public electronic communications networks and providers of publicly available electronic communications services

Article 93

The tasks of professional supervision over the implementation of the provisions of this Act and the regulation referred to in Article 24 of this Act relating to professional supervision over providers of public electronic communications networks and providers of publicly available electronic communications services shall be performed by electronic communications inspectors in accordance with this Act and the law regulating the field of electronic communications.

CHAPTER V.

MUTUAL ASSISTANCE IN THE IMPLEMENTATION OF EXPERT SUPERVISIONS WITH COMPETENT AUTHORITIES OF OTHER MEMBER STATES

Implementation of supervision with cross-border elements

Article 94.

The competent authority for the enforcement of cybersecurity requirements may conduct expert supervision of a key or important entity that provides services in more than one Member State or provides services in one or more Member States and whose network and information systems are located in another Member State or in more than one Member State, with mutual assistance and in cooperation with the competent authorities of those Member States.

Mutual assistance frameworks

Article 95

(1) Mutual assistance referred to in Article 94 of this Act includes:

- sending notifications, via a single contact point, about the supervisory measures taken and the corrective measures imposed, as well as giving advice

– submitting a request for taking supervisory measures or imposing corrective measures and

– upon receipt of a reasoned request, providing assistance commensurate with its own resources so that the supervisory measures or the corrective measures imposed can be implemented in an effective, efficient and consistent manner.

(2) Mutual assistance referred to in paragraph 1, subparagraph 3 of this Article may include acting on requests for the provision of relevant information and taking supervisory measures or imposing corrective measures, including requests to conduct expert supervision or targeted cybersecurity audits.

(3) The competent authority for the implementation of cybersecurity requirements to which a request for mutual assistance in the implementation of expert supervision has been addressed may not refuse the request, unless it establishes that:

- is not competent to provide the requested assistance

– that the requested assistance is not proportionate to the powers of the competent authority or

– that the request relates to information or involves activities which, if disclosed or carried out, would be contrary to the interests of national security, public safety or defence.

(4) The competent authority for the implementation of cybersecurity requests shall, before rejecting the request referred to in paragraph 3 of this Article, consult with the competent authorities of the Member State that submitted the request.

(5) In the case referred to in paragraph 4 of this Article, at the request of the Member State involved, the competent authority for the implementation of cybersecurity requirements shall also consult the European Commission and the ENI. SA.

(6) The provisions of this Article shall also apply in the event of receipt of a request for mutual assistance in the implementation of expert supervision over entities referred to in Article 14, paragraph 3 of this Act that provide services or have network and information systems on the territory of the Republic of Croatia.

Joint implementation of supervisory measures

Article 96

The competent authority for the implementation of cybersecurity requirements may jointly implement supervisory measures under this Act with the competent authorities of other Member States.

CHAPTER VI.

CONTROL OF COMPLIANCE WITH SPECIAL REQUIREMENTS FOR MANAGEMENT OF DOMAIN NAME REGISTRATION DATA

The method of implementation of controls, notification of the implementation of controls and obligations of entities over which control is performed

Article 97

(1) Compliance control from Article 49 of this Act (hereinafter: compliance control) is carried out in each subject of control at least once a year.

(2) The state administration body responsible for science and education shall carry out compliance checks:

– by providing direct access to the register of national top-level Internet domain names and registrars with data, documentation, conditions and methods of implementing special requirements for managing data on domain name registrations referred to in Articles 45 to 48 of this Act, or

– by reviewing the requested and submitted data and documentation of the controlled entity.

(3) The state administration body responsible for science and education is obliged to inform the entity over which it conducts the control about the implementation of the controls referred to in paragraph 2, subparagraph 1 of this Article no later than five days before the start of the control.

(4) By way of derogation from paragraph 2 of this Article, a compliance check may be carried out without prior notice in the event of justified reasons for urgent action.

(5) The registry of national top-level Internet domain names and registrars are obliged to enable the implementation of compliance checks and ensure all conditions for their smooth implementation, which in particular includes the obligation to:

- enabling unhindered access and use of the premises, equipment, systems and other infrastructure or technical means of the registry of top national Internet domain names and registrars

– enabling access to and use of all necessary data and documentation, including making copies

– facilitating conversations with competent and responsible persons registry of national top-level Internet domain names and registrars.

Imposition of corrective measures

Article 98

(1) The state administration body responsible for science and education, depending on the results of the compliance control carried out, may:

- issue warnings about violations of this Act

– issue binding instructions or orders requiring the elimination of identified deficiencies or violations of this Act, specifying the measures that the entity must implement to eliminate these deficiencies or violations.

(2) Instructions and orders from paragraph 1 of this article must contain a deadline for the implementation of the ordered measures and a deadline for notification of their implementation.

Temporary suspension of authorizations issued for the provision of domain registration services

Article 99

(1) If the registrars do not act in accordance with the warnings, instructions or orders from Article 98 of this Act, the state administration body responsible for science and education will request CARNET to temporarily suspend the authorization issued to the entity for providing domain registration services.

(2) The measure referred to in paragraph 1 of this Article shall apply only until the entity complies with the warnings, instructions or orders referred to in Article 98 of this Act.

Records of inspections and court protection

Article 100.

When carrying out compliance checks, Articles 87 to 90 and Article 92, paragraph 1, of this Act shall be applied accordingly.

PART NINE
MINORITY PROVISIONS

Fines for key entities

Article 101.

(1) A fine of EUR 10,000.00 to EUR 10,000,000.00 or of 0.5% to a maximum of 2% of the total annual worldwide turnover of the entity concerned in the preceding financial year, whichever is the greater, shall be imposed on the key entity responsible for the offence:

– who does not take, partially takes or does not take within the prescribed time limit the measures for managing cyber security risks (Article 26 of this Act)

- who does not use certified ICT products, ICT services and ICT processes during the implementation of cyber security risk management measures, if such an obligation is prescribed for the subject (Article 28 of this Act)

– whose persons responsible for managing the measures do not approve cybersecurity risk management measures and/or do not control their implementation, or do not ensure the implementation of appropriate training for the purpose of acquiring knowledge and skills in cybersecurity risk management issues and their impact on the services provided by the entity or the activity it performs (Article 29 of this Act)

– who fails to notify of every significant incident or fails to submit notifications of significant incidents within the deadline (Article 37 of this Act)

– who fails to inform or fails to inform service recipients within the deadline of significant incidents and serious cyber threats and of all measures or legal remedies that these recipients may take in response to the threat (Article 38 of this Act)

- who does not conduct a cyber security audit at least once every two years (Article 34 of this Act)

– who fails to submit a report on the conducted cybersecurity audit to the competent authority for the implementation of cybersecurity requirements within the prescribed period (Article 34 of this Act)

- who prevents, hinders or complicates the implementation of a cyber security audit or does not bear the costs of the implementation of a cyber security audit (Article 34 of this Act)

– who does not cooperate with the competent CSIRT and does not exchange the necessary information with it in the incident resolution process (Article 68 of this Act)

– who does not cooperate with the competent authority in carrying out supervision or does not provide it with the requested data or documentation (Articles 77 and 79 of this Act)

– who fails to provide the competent authorities with unhindered access to the premises, equipment, systems and documentation necessary for conducting the supervision during expert supervision (Article 78 of this Act)

- who does not act or partially acts or does not act within the period set for it, according to the corrective measures pronounced in the professional supervision (Articles 82 and 83 of this Act).

(2) For the offence referred to in paragraph 1 of this Article, natural persons who, in accordance with Article 29 of this Act, are responsible for managing the measures of the key entity liable for the offence shall also be fined in the amount of EUR 1,000.00 to EUR 6,000.00.

(3) When deciding on the imposition of a penalty in accordance with paragraphs 1 and 2 of this Article and its amount, the circumstances referred to in Article 85 of this Act shall be taken into account.

Fines for important entities

Article 102.

(1) A fine of EUR 5,000.00 to EUR 7,000,000.00 or of 0.2% to a maximum of 1.4% of the total annual worldwide turnover of the entity concerned in the preceding financial year, whichever is the greater, shall be imposed on the following major entities:

– who does not take, partially takes or does not take within the prescribed time limit the measures for managing cyber security risks (Article 26 of this Act)

- who does not use certified ICT products, ICT services and ICT processes during the implementation of cyber security risk management measures, if such an obligation is prescribed for the subject (Article 28 of this Act)

– whose persons responsible for managing the measures do not approve cybersecurity risk management measures and/or do not control their implementation, or do not ensure the implementation of appropriate training for the purpose of acquiring knowledge and skills in cybersecurity risk management issues and their impact on the services provided by the entity or the activity it performs (Article 29 of this Act)

– who fails to notify of every significant incident or fails to submit notifications of significant incidents within the deadline (Article 37 of this Act)

– who fails to inform or fails to inform service recipients within the deadline of significant incidents and serious cyber threats and of all measures or legal remedies that these recipients may take in response to the threat (Article 38 of this Act)

- who does not conduct a self-assessment of cyber security at least once every two years (Article 35 of this Law)

– who fails to submit a declaration of compliance or a plan of further action to the competent authority for the implementation of cybersecurity requirements within the prescribed period (Article 35 of this Act)

- who prevents, hinders or hinders the implementation of a targeted cyber security audit or does not bear the costs of implementing a cyber security audit (Article 34 of this Act)

– who does not cooperate with the competent CSIRT and does not exchange the necessary information with it in the incident resolution process (Article 68 of this Act)

– who does not cooperate with the competent authority in carrying out supervision or does not provide it with the requested data or documentation (Articles 77 and 79 of this Act)

– who fails to provide the competent authorities with unhindered access to the premises, equipment, systems and documentation necessary for conducting the supervision during expert supervision (Article 78 of this Act)

- who does not act or partially acts or does not act within the time limit set for this according to the corrective measures pronounced in the professional supervision (Article 82 of this Act).

(2) For the offence referred to in paragraph 1 of this Article, natural persons who, in accordance with Article 29 of this Act, are responsible for managing the measures of a significant entity liable for the offence shall also be fined in the amount of EUR 500.00 to EUR 3,000.00.

(3) When deciding on the imposition of a penalty in accordance with paragraphs 1 and 2 of this Article and its amount, the circumstances referred to in Article 85 of this Act shall be taken into account.

Fines for failure to comply with the obligation to provide data

Article 103.

(1) A fine in the amount of EUR 2,000.00 to EUR 20,000.00
The following entities will be fined for the offence:

– from Annex I and Annex II of this Act if they do not submit or do not submit within the deadline the data necessary for the implementation of the categorization of entities or the maintenance of the list of key and important entities or do not notify in a timely manner about changes in data (Article 20 of this Act)

– from Article 22 of this Act if they do not submit or do not submit within the deadline the data necessary for maintaining a special register of entities or do not notify in a timely manner about changes in data (Article 23 of this Act).

(2) For the violation referred to in paragraph 1 of this Article, the responsible person of the entity referred to in paragraph 1 of this Article shall also be fined in the amount of EUR 200.00 to EUR 1,000.00.

Authorized prosecutor

Article 104.

(1) In the event of suspicion that a violation has been committed, the competent authority for the implementation of cybersecurity requirements shall file a report with the authorized prosecutor.

(2) The authorized prosecutor within the meaning of this Act is the competent state attorney who files the indictment.

(3) By way of derogation from paragraph 2 of this Article, the authorised prosecutor for pre-infringements committed by providers of public electronic communications networks and providers of publicly available electronic communications services shall be the regulatory authority for network activities.

(4) By way of derogation from paragraph 2 of this Article, the authorized prosecutor for misdemeanors committed by trust service providers is the state administration body responsible for the development of the digital society.

PART TEN
TRANSITIONAL AND FINAL PROVISIONS

Obligations of operators of essential services and digital service providers during the transitional period

Article 105.

Operators of key services and digital service providers who, until the entry into force of this Act, implemented measures to achieve a high level of cybersecurity in accordance with the provisions of the Act on Cybersecurity of Operators of Key Services and Digital Service Providers (Official Gazette, No. 64/18) and the Regulation on Cybersecurity of Operators of Key Services and Digital Service Providers (Official Gazette, No. 68/18) shall continue to implement measures based on these regulations until notification of the implemented categorization of the entity referred to in Article 19, paragraphs 1 and 3 of this Act is submitted.

Obligations of providers of public electronic communications networks, providers of publicly available electronic communications services and providers of trust services during the transitional period

Article 106.

(1) Providers of public electronic communications networks and providers of publicly available electronic communications services who, until the entry into force of this Act, implemented security measures

requests for the purpose of protecting the security of electronic communication networks and electronic communication services according to the provisions of Article 41 of the Electronic Communications Act ("Narodne novine", No. 76/22.) continue to implement requests based on Article 41 of that Act until notification of the carried out categorization of the subject from Article 19, paragraph 1 of this Act.

(2) Trust service providers who, until the entry into force of this Act, implemented security requirements for the purpose of protecting the security of trust services pursuant to the provisions of Regulation (EU) No. 910/2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC and the Act implementing Regulation (EU) No. 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (Official Gazette, No. 62/17) shall continue to implement requirements pursuant to those regulations until notification of the implemented categorization of the entity referred to in Article 19, paragraph 1 of this Act is submitted.

Transitional provision on concluded agreements on accession to the national system

Article 107.

Agreements on access to the national system concluded on the basis of the Decision on measures and activities to increase national capabilities for timely detection and protection against state-sponsored cyberattacks, Advanced Persistent Threat (ATP) campaigns and other cyber threats, class: 022-03/21-04/91, reg. no.: 50301-29/09-21-2, from 1 April 2021, remain in force until their expiry.

The deadline for compliance with the requirements related to the management of domain name registration data and the implementation of checks for existing domain users

Article 108.

The registry of national top-level Internet domain names and registrars are obliged to comply with the requirements of this Act relating to the management of domain name registration data and to conduct checks referred to in Article 47, paragraph 2 of this Act for existing domain users within one year from the date of entry into force of this Act.

Initiated procedures

Article 109.

(1) Proceedings initiated pursuant to the provisions of the Act on Cybersecurity of Operators of Key Services and Digital Service Providers (Official Gazette, No. 64/18) shall be completed pursuant to the provisions of that Act and regulations adopted pursuant to that Act.

(2) Proceedings initiated under the provisions of Article 41 of the Electronic Communications Act ("Narodne novine", No. 76/22) shall be completed in accordance with the provisions of that Act and the regulations adopted on the basis of that Act.

The deadline for the implementation of the first categorization of subjects

Article 110.

(1) Competent authorities for the implementation of cyber security requirements from Article 4, paragraph 1, point 28 of this Act and competent authorities for the implementation of special laws from Article 4, paragraph 1, point 27 of this Act kona will carry out the first categorization of subjects and deliver the notification about the carried out categorization of subjects within one year from the date of entry into force of this Act.

(2) The procedure for categorising entities and the delivery of notifications on the categorisation of entities shall be carried out within the period referred to in paragraph 1 of this Article for all operators of key services from the list referred to in Article 12 of the Act on Cybersecurity of Operators of Key Services and Digital Service Providers (Official Gazette, No. 64/18).

(3) The procedure for the first categorization of information intermediaries in the exchange of electronic invoices between entrepreneurs and the delivery of notification of the categorization carried out in accordance with this Act shall be carried out within three months of the entry into force of the law regulating the exchange of electronic invoices between entrepreneurs.

Deadline for establishing a special register of entities

Article 111.

The central state authority for cybersecurity shall establish a special register of entities referred to in Article 22 of this Act within one year from the date of entry into force of this Act.

The beginning of the deadline for the implementation of security audits and professional supervision

Article 112.

The deadlines for the implementation of cyber security audits from Article 34, paragraph 1 of this Act and expert supervision over the implementation of cyber security requirements from Article 75, paragraph 1 of this Act begin on the first following working day after the deadline from Article 26, paragraph 5 of this Act.

Adoption of implementing regulations

Article 113.

(1) The Government shall pass the decree from Article 24 of this Act within the deadline nine months from the date of entry into force of this Act.

(2) The government will adopt the medium-term strategic planning act referred to in Article 55 of this Act within 24 months from the date of entry into force of this Act.

(3) The government will adopt the national cybercrisis management program from Article 56 of this Act within three months from the date of entry into force of this Act.

(4) The Government will adopt the Cybersecurity Exercise Implementation Plan from Article 58 of this Act within 12 months from the date of entry into force of this Act.

(5) The Information Systems Security Institute shall adopt the rules referred to in Article 33, paragraph 1 of this Act within nine months from the date of entry into force of the regulation referred to in paragraph 1 of this Article.

Adoption of regulations on internal organization and internal order

Article 114.

(1) The Government shall, upon the proposal of the Head of the Office of the National Security Council, with the prior consent of the President of the Republic of Croatia, align the Regulation on the internal organization of the Office of the National Security Council with the provisions of this Act within 30 days from the date of entry into force of this Act.

(2) The Head of the Office of the National Security Council shall align the Regulations on the Internal Order of the Office of the National Security Council with the Regulation referred to in paragraph 1 of this Article, with the prior consent of the National Security Council, within 30 days from the date of entry into force of the Regulation.

(3) The Government shall, upon the proposal of the Director of the Security and Intelligence Agency, with the prior consent of the President of the Republic of Croatia, align the Regulation on the internal organization of the Security and Intelligence Agency with the provisions of this Act within 30 days from the date of entry into force of this Act.

(4) The Director of the Security and Intelligence Agency shall align the Rules of Procedure of the Security and Intelligence Agency with the Regulation referred to in paragraph 3 of this Article, with the prior consent of the Head of the Office of the National Security Council, within 30 days from the date of entry into force of the Regulation.

(5) The Government shall, upon the proposal of the Director of the Information Systems Security Institute, with the prior consent of the Council for the Coordination of Security and Intelligence Agencies, align the Regulation on the internal organization of the Information Systems Security Institute with the provisions of this Act within 30 days from the date of entry into force of this Act.

(6) The Director of the Information Systems Security Institute shall align the Regulations on the Internal Order of the Information Systems Security Institute with the Regulation referred to in paragraph 5 of this Article, with the prior consent of the Government, within 30 days from the date of entry into force of the Regulation.

Expiration of regulations

Article 115.

(1) On the date of entry into force of this Law, the following shall cease to be valid:

– Law on cyber security of operators of key services i digital service providers (Official Gazette, No. 64/18.)

– Article 17, paragraph 2, subparagraph 4 and Article 21 of the Information Security Act (Official Gazette, No. 79/07)

– Article 41 of the Electronic Communications Act ("Narod-ne novine", no. 76/22.)

– Regulation on cyber security of operators of key services i digital service providers (Official Gazette, No. 68/18) and

– Decision on the establishment of the National Council for Cybersecurity and Operational-Technical Coordination for Cybersecurity ("Narodne novine", no. 61/16, 28/18, 110/18, 79/19 and 136/20).

(2) Decision on measures and activities to increase national capabilities for timely detection and protection against state-sponsored cyberattacks, Advanced Persistent Threat (ATP) campaigns and other cyber threats, class: 022-03/21-04/91, registration number: 50301-29/09-21-2, from April 1, 2021, remains in force until the entry into force of the regulation referred to in Article 113 paragraph 1. of this Act.

Entry into force of the Law

Article 116.

This Act shall enter into force on the eighth day following the date of its publication in the Official Gazette.

Class: 022-02/23-01/94

Zagreb, January 26, 2024.

CROATIAN PARLIAMENT

President
Croatian Parliament
Gordan Jandrokoviÿ, mp

ANNEX I

HIGHLY CRITICAL SECTORS

Sektor	Podsektor	Vrsta subjekta
1. Energetika	(a) električna energija	– elektroenergetski subjekti koju obavljaju funkciju opskrbe električnom energijom, uključujući opskrbu električnom energijom koja se obavlja kao javna usluga Pojam *elektroenergetski subjekt* u smislu ovoga Zakona znači pravna ili fizička osoba koja nije krajnji kupac, a koja obavlja najmanje jednu od elektroenergetskih djelatnosti i koja je odgovorna za komercijalne i tehničke zadaće i zadaće održavanja koje su povezane s tim djelatnostima. Pojam *opskrba električnom energijom* u smislu ovoga Zakona znači kupnja i prodaja električne energije na veleprodajnom tržištu, prodaja električne energije krajnjim kupcima i skladištima energije, otkup električne energije od aktivnih kupaca, skladišta energije i proizvođača te agregiranje. Pojam *opskrba električnom energijom koja se obavlja kao javna usluga* u smislu ovoga Zakona znači opskrbu električnom energijom onih krajnjih kupaca koji imaju pravo na takav način opskrbe i slobodno ga izaberu ili koriste po automatizmu. Pojmovi *elektroenergetski subjekt, opskrba električnom energijom* i *opskrba električnom energijom koja se obavlja kao javna usluga* istovjetni su s pojmovima iz članka 3. stavka 1. točaka 17., 77. i 78. Zakona o tržištu električne energije („Narodne novine“, br. 111/21. i 83/23.) kojim je u hrvatsko zakonodavstvo preuzeta Direktiva (EU) 2019/944 Europskog parlamenta i Vijeća od 5. lipnja 2019. o zajedničkim pravilima za unutarnje tržište električne energije i izmjeni Direktive 2012/27/EU (SL L 158, 14. 6. 2019.).
		– operatori distribucijskog sustava Pojam *operator distribucijskog sustava* u smislu ovoga Zakona znači fizička ili pravna osoba odgovorna za pogon i vođenje, održavanje, razvoj i izgradnju distribucijske mreže na danom području, kao i zajedničkih postrojenja prema prijenosnoj mreži i, kada je to primjenjivo, međusobno povezivanje s drugim distribucijskim sustavima te za osiguravanje dugoročne sposobnosti distribucijske mreže da zadovolji razumne zahtjeve za distribuciju električne energije. Pojam *operator distribucijskog sustava* istovjetan je s pojmom iz članka 3. stavka 1. točke 71. Zakona o tržištu električne energije („Narodne novine“, br. 111/21. i 83/23.).
		– operatori prijenosnog sustava Pojam *operator prijenosnog sustava* u smislu ovoga Zakona znači fizička ili pravna osoba odgovorna za pogon i vođenje, održavanje, razvoj i izgradnju prijenosne mreže na danom području, prekograničnih prijenosnih vodova prema drugim prijenosnim mrežama, kao i zajedničkih postrojenja prema distribucijskoj mreži te za osiguravanje dugoročne sposobnosti prijenosne mreže da zadovolji razumne zahtjeve za prijenos električne energije. Pojam *operator prijenosnog sustava* istovjetan je s pojmom iz članka 3. stavka 1. točke 72. Zakona o tržištu električne energije („Narodne novine“, br. 111/21. i 83/23.).
		– proizvođači električne energije Pojam *proizvođač električne energije* u smislu ovoga Zakona znači fizička ili pravna osoba koja proizvodi električnu energiju. Pojam *proizvođač električne energije* istovjetan je s pojmom iz članka 3. stavka 1. točke 90. Zakona o tržištu električne energije („Narodne novine“, br. 111/21. i 83/23.).
		– nominirani operatori tržišta električne energije kako su definirani u članku 2. točki 8. Uredbe (EU) 2019/943 Europskog parlamenta i Vijeća od 5. lipnja 2019. o unutarnjem tržištu električne energije (SL L 158, 14. 6. 2019.)
		– sudionici na tržištu kako su definirani u članku 2. točki 25. Uredbe (EU) 2019/943 koji pružaju usluge agregiranja, upravljanja potrošnjom ili skladištenja energije Pojam *agregiranje* u smislu ovoga Zakona znači djelatnost koju obavlja fizička ili pravna osoba koja može kombiniranjem snage i/ili iz mreže preuzete električne energije više kupaca ili operatora skladišta energije ili snage i/ili u mrežu predane električne energije više proizvođača ili aktivnih kupaca ili operatora skladišta energije radi sudjelovanja na bilo kojem tržištu električne energije. Pojam *upravljanje potrošnjom* u smislu ovoga Zakona znači promjena u opterećenju kod krajnjih kupaca u

		odnosu na njihove uobičajene ili trenutačne obrasce potrošnje električne energije kao odgovor na tržišne signale, uključujući vremenski ovisnu promjenu cijene električne energije ili novčane poticaje, ili kao odgovor na prihvat ponude krajnjeg kupca za prodaju smanjenja ili povećanja potražnje po cijeni na organiziranim tržištima, kako je definirano u članku 2. točki 4. Provedbene uredbe Komisije (EU) br. 1348/2014 od 17. prosinca 2014. o izvješćivanju o podacima i provedbi članka 8. stavaka 2. i 6. Uredbe (EU) br. 1227/2011 Europskog parlamenta i Vijeća o cjelovitosti i transparentnosti veleprodajnog tržišta energije (Tekst značajan za EGP) (SL L 363, 18. 12. 2014.), pojedinačno ili putem agregiranja. Pojam *skladištenje energije* u smislu ovoga Zakona znači, u kontekstu elektroenergetskog sustava, odgađanje konačne uporabe električne energije do trenutka kasnijeg od onog u kojem je proizvedena ili pretvorba električne energije u oblik energije koji se može skladištiti, skladištenje takve energije i naknadna pretvorba takve energije u električnu energiju ili njezina uporaba kao nositelja energije. Pojmovi *agregiranje*, *upravljanje potrošnjom* i *skladištenje energije* istovjetni su s pojmovima iz članka 3. stavka 1. točaka 4., 93. i 109. Zakona o tržištu električne energije („Narodne novine“, br. 111/21. i 83/23.).
		– operatori mjesta za punjenje koji su odgovorni za upravljanje i rad mjesta za punjenje kojim se krajnjim korisnicima pruža usluga opskrbe, među ostalim u ime i za račun pružatelja usluga mobilnosti
	(b) centralizirano grijanje i hlađenje	– operator sustava centraliziranog grijanja ili centraliziranog hlađenja Pojam *centralizirano grijanje ili centralizirano hlađenje* u smislu ovoga Zakona znači distribucija toplinske energije u obliku pare, vruće vode ili pothlađenih tekućina iz centralnih ili decentraliziranih proizvodnih postrojenja putem centralnih i zatvorenih toplinskih sustava u više zgrada ili na više lokacija radi uporabe za zagrijavanje ili hlađenje prostora ili procesa. Pojam *centralizirano grijanje ili centralizirano hlađenje* istovjetan je s pojmom iz članka 4. stavka 1. točke 4. Zakona o obnovljivim izvorima energije i visokoučinkovitoj kogeneraciji („Narodne novine“, br. 138/21. i 83/23.) kojim je u hrvatsko zakonodavstvo preuzeta Direktiva 2018/2001 Europskog parlamenta i
		Vijeća od 11. prosinca 2018. o promicanju uporabe energije iz obnovljivih izvora (preinaka) (Tekst značajan za EGP) (SL L 328, 21. 12. 2018.).
	(c) nafta	– operatori naftovoda
		– operatori proizvodnje nafte, rafinerija i tvornica nafte te njezina skladištenja i prijenosa
		– središnja tijela za zalihe Pojam *središnje tijelo za zalihe* u smislu ovoga Zakona znači Agencija za ugljikovodike, kao središnje tijelo u Republici Hrvatskoj za obvezne zalihe nafte i naftnih derivata, koja je jedinstveno tijelo ovlašteno formirati, održavati i prodavati obvezne zalihe. Pojam *središnje tijelo za zalihe* istovjetan je s pojmom iz članka 3. stavka 2. točke 5. Zakona o tržištu nafte i naftnih derivata („Narodne novine“, br. 19/14., 73/17. i 96/19.) kojim je u hrvatsko zakonodavstvo preuzeta Direktiva 2009/119/EZ Europskog parlamenta i Vijeća od 14. rujna 2009. kojom se države članice obvezuju održavati minimalne zalihe sirove nafte i/ili naftnih derivata (SL L 265/9 od 9. 10. 2009.).
	(d) plin	– opskrbljivači plinom, uključujući opskrbljivače u obvezi javne usluge Pojam *opskrbljivač plinom* u smislu ovoga Zakona znači energetski subjekt koji obavlja energetsku djelatnost opskrbe plinom. Pojam *opskrbljivač plinom u obvezi javne usluge* u smislu ovoga Zakona znači opskrbljivač plinom koji obavlja energetsku djelatnost opskrbe u obvezi javne usluge. Pojam *opskrba plinom* u smislu ovoga Zakona znači prodaja ili preprodaja plina kupcu, uključujući prodaju ili preprodaju UPP-a i SPP-a. Pojam *opskrba plinom u obvezi javne usluge* u smislu ovoga Zakona znači opskrba plinom koja se u općem gospodarskom interesu obavlja po reguliranim uvjetima radi osiguravanja sigurnosti, redovitosti, kvalitete i cijene opskrbe kućanstava. Pojmovi *opskrbljivač plinom, opskrbljivač plinom u obvezi javne usluge*, *opskrba plinom* i *opskrba plinom u obvezi javne usluge* istovjetni su s pojmovima iz članka 3. stavka 2. točaka 36., 37., 38. i 39. Zakona o tržištu plina („Narodne novine“, br. 18/18. i 23/20.) kojim je u hrvatsko zakonodavstvo preuzeta Direktiva 2009/73/EZ Europskog parlamenta i Vijeća od 13.

		srpnja 2009. o zajedničkim pravilima za unutarnje tržište prirodnog plina i stavljanju izvan snage Direktive 2003/55/EZ (Tekst značajan za EGP) (SL L 211, 14. 8. 2009.)
		– operatori distribucijskog sustava Pojam *operator distribucijskog sustava* u smislu ovoga Zakona znači energetski subjekt koji obavlja energetsku djelatnost distribucije plina i odgovoran je za rad, održavanje i razvoj distribucijskog sustava na svom distribucijskom području i, gdje je izvodivo, njegovo povezivanje s drugim sustavima te za osiguranje dugoročne sposobnosti sustava da zadovoljava razumne potrebe za distribucijom plina. Pojam *distribucija plina* u smislu ovoga Zakona znači razvod plina distribucijskim sustavom visoke, srednje i niske tlačne razine radi isporuke plina krajnjim kupcima, uključujući pomoćne usluge, a isključujući opskrbu plinom. Pojam *distribucijski sustav* u smislu ovoga Zakona znači sustav plinovoda i ostalih pripadajućih objekata i opreme koji su u vlasništvu operatora distribucijskog sustava i/ili kojima upravlja operator distribucijskog sustava, a koji se koristi za distribuciju plina, nadzor i upravljanje, mjerenje i prijenos podataka. Pojmovi *operator distribucijskog sustava, distribucija plina* i *distribucijski sustav* istovjetni su s pojmovima iz članka 3. stavka 2. točaka 5., 6. i 30. Zakona o tržištu plina („Narodne novine“, br. 18/18. i 23/20.).
		– operatori transportnog sustava Pojam *operator transportnog sustava* u smislu ovoga Zakona znači energetski subjekt koji obavlja energetsku djelatnost transporta plina i odgovoran je za rad, održavanje i razvoj transportnog sustava na određenom području i, gdje je izvodivo, njegovo povezivanje s drugim sustavima te za osiguranje dugoročne sposobnosti sustava da zadovoljava razumne potrebe za transportom plina. Pojam *transport plina* u smislu ovoga Zakona znači prijenos plina kroz transportni sustav, isključujući opskrbu plinom i trgovinu plinom, a uključujući tranzit plina i pomoćne usluge. Pojam *transportni sustav* u smislu ovoga Zakona znači objekt koji je u vlasništvu i/ili kojim upravlja operator transportnog sustava, a koji čine sustav visokotlačnih
		plinovoda, kompresorske stanice, mjerne stanice, mjerno-redukcijske stanice, plinski čvorovi i ostali tehnološki objekti i oprema koji se koriste za transport plina, nadzor i upravljanje, mjerenje i prijenos podataka, isključujući mrežu proizvodnih plinovoda i visokotlačne distribucijske plinovode, uključujući plin za tehnološke kapacitete kojima se isključivo koristi operator transportnog sustava i operativnu akumulaciju. Pojmovi *operator transportnog sustava*, *transport plina* i *transportni sustav* istovjetni su s pojmovima iz članka 3. stavka 2. točaka 34., 58. i 59. Zakona o tržištu plina („Narodne novine“, br. 18/18. i 23/20.).
		– operatori sustava skladišta plina Pojam *operator sustava skladišta plina* u smislu ovoga Zakona znači energetski subjekt koji obavlja energetsku djelatnost skladištenja plina i odgovoran je za rad, održavanje i razvoj sustava skladišta plina. Pojam *skladištenje plina* u smislu ovoga Zakona znači utiskivanje plina u sustav skladišta plina, skladištenje plina u radnom volumenu sustava skladišta plina i povlačenje plina iz sustava skladišta plina, uključujući pomoćne usluge. Pojmovi *operator sustava skladišta plina* i *skladištenje plina* istovjetni su s pojmovima iz članka 3. stavka 2. točaka 54. i 56. Zakona o tržištu plina („Narodne novine“, br. 18/18. i 23/20.).
		– operatori terminala za UPP Pojam *operator terminala za UPP* u smislu ovoga Zakona znači energetski subjekt koji obavlja energetsku djelatnost upravljanja terminalom za UPP i odgovoran je za rad, održavanje i razvoj terminala za UPP. Pojam *terminal za UPP* u smislu ovoga Zakona znači terminal koji se koristi za ukapljivanje prirodnog plina ili prihvat, iskrcaj i ponovno uplinjavanje UPP-a, uključujući pomoćne usluge i privremeno skladištenje potrebno za postupak ponovnog uplinjavanja i daljnju otpremu u transportni sustav, ali isključujući dijelove terminala za UPP koji se koriste za skladištenje. Pojmovi *operator terminala za UPP* i *terminal za UPP* istovjetni su s pojmovima iz članka 3. stavka 2. točaka 33. i 57. Zakona o tržištu plina („Narodne novine“, br. 18/18. i 23/20.).
		– poduzeća za prirodni plin

		Pojam *poduzeće za prirodni plin* u smislu ovoga Zakona, a u skladu sa zakonom kojim se uređuje tržište plina, znači fizička ili pravna osoba koja obavlja najmanje jednu od sljedećih funkcija: proizvodnju, transport, distribuciju, opskrbu, nabavu ili skladištenje prirodnog plina, uključujući UPP, a odgovorna je za komercijalne i tehničke zadatke i/ili zadatke održavanja koji su povezani s tim funkcijama, isključujući krajnje kupce.
		– operatori postrojenja za rafiniranje i obradu prirodnog plina
	(e) vodik	– operatori proizvodnje, skladištenja i prijenosa vodika
2. Promet	(a) zračni promet	– zračni prijevoznici kako su definirani u članku 3. točki 4. Uredbe (EZ) br. 300/2008 Europskog parlamenta i Vijeća od 11. ožujka 2008. o zajedničkim pravilima u području zaštite civilnog zračnog prometa i stavljanju izvan snage Uredbe (EZ) br. 2320/2002 (Tekst značajan za EGP) koji se upotrebljavaju u komercijalne svrhe
		– upravna tijela zračne luke, zračne luke, uključujući osnovne zračne luke navedene u odjeljku 2. Priloga II. Uredbe (EU) br. 1315/2013 Europskog parlamenta i Vijeća od 11. prosinca 2013. o smjernicama Unije za razvoj transeuropske prometne mreže i stavljanju izvan snage Odluke br. 661/2010/EU (Tekst značajan za EGP) te tijela koja upravljaju pomoćnim objektima u zračnim lukama Pojam *upravno tijelo zračne luke* u smislu ovoga Zakona znači tijelo koje, osim drugih aktivnosti ili ne, ima prema nacionalnim propisima ili ugovorima kao cilj rukovođenje i upravljanje infrastrukturom zračne luke te koordinaciju i nadzor djelatnosti različitih operatora u dotičnoj zračnoj luci. Pojam *zračna luka* u smislu ovoga Zakona znači svaka površina koja je posebno prilagođena za slijetanje, uzlijetanje i manevriranje zrakoplova, uključujući i pripadajuće objekte, sredstva i uređaje namijenjene za odvijanje zračnog prometa i pružanje usluga te objekte, sredstva i uređaje za pomoć u pružanju usluga komercijalnog zračnog prijevoza. Pojmovi *upravno tijelo zračne luke* i *zračna luka* istovjetni su s pojmovima iz članka 3. stavka 1. podstavaka 1. i 2. Pravilnika o naknadama zračnih luka („Narodne novine“, br. 65/15.) kojim je u hrvatsko zakonodavstvo preuzeta Direktiva 2009/12/EZ Europskog parlamenta i Vijeća od 11. ožujka 2009. o naknadama zračnih luka.
		– operatori kontrole upravljanja prometom koji pružaju usluge kontrole zračnog prometa (ATC) kako su definirani u članku 2. točki 1. Uredbe (EZ) br. 549/2004 Europskog parlamenta i Vijeća od 10. ožujka 2004. o definiranju pravnog okvira za stvaranje jedinstvenog europskog neba (Okvirna uredba) i Izjava država članica o vojnim pitanjima u svezi s jedinstvenim europskim nebom
	(b) željeznički promet	– upravitelji infrastrukture Pojam *upravitelj infrastrukture* u smislu ovoga Zakona znači pravna osoba ili u vertikalno integriranom trgovačkom društvu organizacijska jedinica odgovorna za upravljanje, održavanje i obnovu željezničke infrastrukture, kao i za sudjelovanje u razvoju željezničke infrastrukture na način koji je određen u okviru opće politike razvoja i financiranja željezničke infrastrukture Republike Hrvatske. Pojam *upravitelj infrastrukture* istovjetan je s pojmom iz članka 5. stavka 1. točke 36. Zakona o željeznici („Narodne novine“, br. 32/19., 20/21. i 114/22.) kojim je u hrvatsko zakonodavstvo preuzeta Direktiva 2012/34/EU Europskog parlamenta i Vijeća od 21. studenoga 2012. o uspostavi jedinstvenog Europskog željezničkog prostora (preinačena) (SL L 343, 14. 12. 2012.), kako je posljednji put izmijenjena Direktivom (EU) 2016/2370 Europskog parlamenta i Vijeća od 14. prosinca 2016. o izmjeni Direktive 2012/34/EU u pogledu otvaranja tržišta za usluge domaćeg željezničkog prijevoza putnika i upravljanja željezničkom infrastrukturom (Tekst značajan za EGP) (SL L 352, 23. 12. 2016.).
		– željeznički prijevoznici, među ostalim i operatori uslužnih objekata Pojam *željeznički prijevoznik* u smislu ovoga Zakona znači svaka pravna osoba koja ima dozvolu za obavljanje usluga željezničkog prijevoza i čija je glavna djelatnost pružanje usluga željezničkog prijevoza putnika i/ili tereta, uz uvjet da ta pravna osoba osigura vuču vlakova; to uključuje i pravnu osobu koja pruža samo uslugu vuče vlakova. Pojam *operator uslužnih objekata* u smislu ovoga Zakona znači pravna osoba odgovorna za upravljanje jednim ili s više uslužnih objekata (upravitelj uslužnog objekta) ili za pružanje željezničkim prijevoznicima jedne ili više usluga iz Priloga 2. točaka 2. do 4. Zakona o željeznici („Narodne novine“, br. 32/19., 20/21. i 114/22.) (pružatelj usluga).
		Pojmovi *željeznički prijevoznik* i *operator uslužnih objekata* istovjetni su s pojmovima iz članka 5. stavka 1. točaka 22. i 46. Zakona o željeznici („Narodne novine“, br. 32/19., 20/21. i 114/22.).
	(c) vodeni promet	– kompanije za prijevoz putnika unutarnjim plovnim putovima, morem i duž obale kako su definirane za pomorski promet u Prilogu I. Uredbe (EZ) br. 725/2004 Europskog parlamenta i Vijeća od 31. ožujka 2004. o jačanju sigurnosne zaštite brodova i luka (Tekst značajan za EGP), ne uključujući pojedinačna plovila kojima upravljaju te kompanije
		– upravljačka tijela luka, uključujući njihove luke kako su definirane u članku 2. točki 11. Uredbe (EZ) br. 725/2004, te subjekti koji upravljaju postrojenjima i opremom u lukama Pojam *luka* u smislu ovoga Zakona znači morska luka, tj. morski i s morem neposredno povezan kopneni prostor u utvrđenim granicama lučkog područja s izgrađenim i neizgrađenim obalama; lukobranima, uređajima, postrojenjima i drugim objektima i sustavima namijenjenim za pristajanje, sidrenje i zaštitu brodova, jahti i brodica, ukrcaj i iskrcaj putnika i tereta, uskladištenje i drugo rukovanje teretom, proizvodnju, oplemenjivanje i doradu tereta te ostale gospodarske djelatnosti koje su s tim djelatnostima u međusobnoj ekonomskoj, prometnoj ili tehnološkoj vezi. Pojam *luka* istovjetan je s pojmom iz članka 3. stavka 1. točke 1. Zakona o sigurnosnoj zaštiti pomorskih brodova i luka („Narodne novine“, br. 108/17. i 30/21.) kojim je u hrvatsko zakonodavstvo preuzeta Direktiva 2005/65/EZ Europskog parlamenta i Vijeća od 26. listopada 2005. o jačanju sigurnosne zaštite luka (Tekst značajan za EGP) (SL L 320, 25. 11. 2005.).
		– služba za nadzor i upravljanje pomorskim prometom (VTS) kako je definirana u članku 75.a stavku 1. i članku 75.b stavku 1. Pomorskog zakonika („Narodne novine“, br. 181/04., 76/07., 146/08., 61/11., 56/13., 26/15. i 17/19.) kojim je u hrvatsko zakonodavstvo preuzeta Direktiva 2002/59/EZ Europskog parlamenta i Vijeća od 27. lipnja 2002. o uspostavi sustava nadzora plovidbe i informacijskog sustava Zajednice i stavljanju izvan snage Direktive Vijeća 93/75/EEZ
	(d) cestovni promet	– tijela nadležna za ceste kako su definirana u članku 2. točki 12. Delegirane uredbe Komisije (EU) 2015/962 od 18. prosinca 2014. o dopuni Direktive 2010/40/EU Europskog parlamenta i Vijeća u pogledu pružanja usluga prometnih informacija u cijeloj Europskoj uniji u realnom vremenu (Tekst značajan za EGP),
		odgovorna za kontrolu upravljanja prometom, osim javnih subjekata kojima upravljanje prometom ili rad inteligentnih prometnih sustava nisu ključan dio njihove opće djelatnosti Prema članku 2. točki 12. Delegirane uredbe Komisije (EU) 2015/962, pojam *tijelo nadležno za ceste* znači svako javno tijelo koje je nadležno za planiranje, nadzor ili upravljanje cestama u okviru svoje mjesne nadležnosti.
		– operatori inteligentnih prometnih sustava Pojam *inteligentni prometni sustavi (ITS)* u smislu ovoga Zakona znači informacijsko-komunikacijska nadgradnja klasičnog sustava cestovnog prometa kojim se postiže znatno poboljšanje učinaka cjelokupnog prometnog sustava. ITS uključuje ceste, vozila i korisnike cesta, a primjenjuje se u upravljanju prometom, upravljanju mobilnosti, upravljanju prometnim incidentima te za veze s ostalim vrstama prijevoza. Pojam *inteligentni prometni sustavi (ITS)* istovjetan je s pojmom iz članka 72. stavka 1. Zakona o cestama („Narodne novine“, br. 84/11., 22/13., 54/13., 148/13., 92/14., 110/19., 144/21, 114/22., 04/23. i 133/23.) kojim je u hrvatsko zakonodavstvo preuzeta Direktiva 2010/40/EZ Europskog parlamenta i Vijeća od 7. srpnja 2010. o okviru za uvođenje inteligentnih transportnih sustava u cestovnom prometu i za veze s ostalim vrstama prijevoza (Tekst značajan za EGP) (SL L 207 od 6. kolovoza 2010.).
3. Bankarstvo		– kreditne institucije kako su definirane u članku 4. točki 1. Uredbe (EU) br. 575/2013 Europskog parlamenta i Vijeća od 26. lipnja 2013. o bonitetnim zahtjevima za kreditne institucije i investicijska društva i o izmjeni Uredbe (EU) br. 648/2012 (Tekst značajan za EGP)
4. Infrastruktura financijskog tržišta		– operatori mjesta trgovanja Pojam *mjesta trgovanja* u smislu ovoga Zakona znači uređeno tržište, MTP ili OTP. Pojam *multilateralna trgovinska platforma ili MTP* u smislu ovoga Zakona znači multilateralni sustav kojim upravlja investicijsko društvo ili tržišni operater koji u sustavu i prema unaprijed poznatim i nediskrecijskim pravilima spaja ili omogućuje spajanje ponuda za kupnju i ponuda za prodaju financijskih instrumenata trećih tako da nastaje ugovor u skladu s odredbama dijela drugoga glave III. poglavlja VII. Zakona o tržištu

		kapitala („Narodne novine“, br. 65/18., 17/20., 83/21. i 151/22.). Pojam *organizirana trgovinska platforma* ili OTP u smislu ovoga Zakona znači multilateralni sustav, koji nije uređeno tržište ili MTP, koji omogućuje da se u tom sustavu susretnu ponude za kupnju i ponude za prodaju obveznica, strukturiranih financijskih proizvoda, emisijskih jedinica ili izvedenica više zainteresiranih trećih strana tako da nastaje ugovor u skladu s odredbama dijela drugoga glave III. poglavlja VII. Zakona o tržištu kapitala („Narodne novine“, br. 65/18., 17/20., 83/21. i 151/22.). Pojmovi *mjesta trgovanja, multilateralna trgovinska platforma ili MTP* i *organizirana trgovinska platforma* ili OTP istovjetni su s pojmovima iz članka 3. stavka 1. točaka 61., 65. i 77. Zakona o tržištu kapitala („Narodne novine“, br. 65/18., 17/20., 83/21. i 151/22.) kojim je u hrvatsko zakonodavstvo preuzeta Direktiva 2014/65/EU Europskog parlamenta i Vijeća od 15. svibnja 2014. o tržištu financijskih instrumenata i izmjeni Direktive 2002/92/EZ i Direktive 2011/61/EU (preinačena) (Tekst značajan za EGP) (SL L 173, 12. 6. 2014.).
		– središnje druge ugovorne strane (CCP-i) kako su definirane u članku 2. točki 1. Uredbe (EU) br. 648/2012 Europskog parlamenta i Vijeća od 4. srpnja 2012. o OTC izvedenicama, središnjoj drugoj ugovornoj strani i trgovinskom repozitoriju (SL L 201, 27. 7. 2012.)
5. Zdravstvo		– pružatelji zdravstvene zaštite Pojam *pružatelj zdravstvene zaštite* u smislu ovoga Zakona znači svaka fizička ili pravna osoba ili bilo koji subjekt koji obavlja zdravstvenu djelatnost u Republici Hrvatskoj u skladu sa zakonom kojim se uređuje zdravstvena zaštita. Pojam *pružatelj zdravstvene zaštite* ne odnosi se na ustrojstvene jedinice Ministarstva obrane i Oružanih snaga Republike Hrvatske i ministarstva nadležnog za pravosuđe koje obavljaju zdravstvenu djelatnost prema posebnim propisima.
		– referentni laboratoriji Europske unije iz članka 15. Uredbe (EU) 2022/2371 Europskog parlamenta i Vijeća od 23. studenoga 2022. o ozbiljnim prekograničnim prijetnjama zdravlju i o stavljanju izvan snage Odluke br. 1082/2013/EU (Tekst značajan za EGP)
		– subjekti koji obavljaju djelatnosti istraživanja i razvoja lijekova
		Pojam *lijek* u smislu ovoga Zakona znači: – svaka tvar ili kombinacija tvari prikazana sa svojstvima liječenja ili sprječavanja bolesti kod ljudi ili – svaka tvar ili kombinacija tvari koja se može upotrijebiti ili primijeniti na ljudima u svrhu obnavljanja, ispravljanja ili prilagodbe fizioloških funkcija farmakološkim, imunološkim ili metaboličkim djelovanjem ili za postavljanje medicinske dijagnoze. Pojam *lijek* istovjetan je s pojmom iz članka 3. stavka 1. točke 1. Zakona o lijekovima („Narodne novine“, br. 76/13., 90/14. i 100/18.) kojim je u hrvatsko zakonodavstvo preuzeta Direktiva 2001/83/EZ Europskog parlamenta i Vijeća od 6. studenoga 2001., o Zakoniku Zajednice koji se odnosi na lijekove za primjenu kod ljudi (SL L 311, 28. 11. 2001.).
		– subjekti koji proizvode osnovne farmaceutske proizvode i farmaceutske pripravke iz područja C odjeljka 21. Nacionalne klasifikacije djelatnosti 2007. – NKD 2007. („Narodne novine“, br. 58/07. i 72/07.)
		– subjekti koji proizvode medicinske proizvode koji se smatraju ključnima tijekom izvanrednog stanja u području javnog zdravlja („popis ključnih medicinskih proizvoda u slučaju izvanrednog stanja u području javnog zdravlja“) u smislu članka 22. Uredbe (EU) 2022/123 Europskog parlamenta i Vijeća od 25. siječnja 2022. o pojačanoj ulozi Europske agencije za lijekove u pripravnosti za krizne situacije i upravljanju njima u području lijekova i medicinskih proizvoda (Tekst značajan za EGP)
6. Voda za ljudsku potrošnju		– dobavljači i distributeri vode namijenjene za ljudsku potrošnju, isključujući distributere kojima distribucija vode za ljudsku potrošnju nije ključan dio njihove općenite djelatnosti distribucije druge robe i proizvoda Pojam *voda namijenjena za ljudsku potrošnju* u smislu ovoga Zakona znači: – sva voda, bilo u njezinu izvornom stanju ili nakon obrade, koja je namijenjena za piće, kuhanje, pripremu hrane ili druge potrebe kućanstva i u javnim i u privatnim prostorima, neovisno o njezinu podrijetlu te o tome isporučuje li se iz vodoopskrbne mreže, isporučuje li se iz cisterne ili se stavlja u boce ili ambalažu, uključujući izvorsku i stolnu vodu – sva voda koja se u poslovanju s hranom upotrebljava za proizvodnju, obradu, očuvanje ili stavljanje na tržište proizvoda ili tvari namijenjenih za ljudsku potrošnju.
		Pojam *voda namijenjena za ljudsku potrošnju* istovjetan je s pojmom iz članka 3. stavka 1. točke 1. Zakona o vodi za ljudsku potrošnju („Narodne novine“, br. 30/23.) kojim je u hrvatsko zakonodavstvo preuzeta Direktiva (EU) 2020/2184 Europskog parlamenta i Vijeća od 16. prosinca 2020. o kvaliteti vode namijenjene za ljudsku potrošnju (preinaka) (Tekst značajan za EGP) (SL L 435, 23. 12. 2020.).
7. Otpadne vode		– poduzeća koja prikupljaju, odlažu ili pročišćavaju komunalne otpadne vode, sanitarne otpadne vode ili industrijske otpadne vode, isključujući poduzeća kojima prikupljanje, odlaganje ili pročišćavanje komunalnih otpadnih voda, otpadnih voda iz kućanstva ili industrijskih otpadnih voda nije ključan dio njihove općenite djelatnosti Pojam *komunalne otpadne vode* u smislu ovoga Zakona znači otpadne vode sustava javne odvodnje koje čine sanitarne otpadne vode ili otpadne vode koje su mješavina sanitarnih otpadnih voda s industrijskim otpadnim vodama i/ili oborinskim vodama određene aglomeracije. Pojam *sanitarne otpadne vode* u smislu ovoga Zakona znači otpadne vode koje se nakon korištenja ispuštaju iz stambenih objekata i uslužnih objekata te koje uglavnom potječu iz ljudskog metabolizma i aktivnosti kućanstava. Pojam *industrijske otpadne vode* u smislu ovoga Zakona znači sve otpadne vode, osim sanitarnih otpadnih voda i oborinskih voda, koje se ispuštaju iz prostora korištenih za obavljanje trgovine ili industrijske djelatnosti. Pojmovi *komunalne otpadne vode*, *sanitarne otpadne vode* i *industrijske otpadne vode* istovjetni su s pojmovima iz članka 4. stavka 1. točaka 25., 34. i 81. Zakona o vodama („Narodne novine“, br. 66/19., 84/21. i 47/23.) kojim je u hrvatsko zakonodavstvo preuzeta Direktiva Vijeća 91/271/EEZ od 21. svibnja 1991. o pročišćavanju komunalnih otpadnih voda (SL L 135, 30. 5. 1991.), dopunjena Direktivom Komisije 98/15/EZ od 27. veljače 1998. s obzirom na određene zahtjeve utvrđene u Dodatku I. (Tekst značajan za EGP) (SL L 67, 7. 3. 1998.).
8. Digitalna infrastruktura		– pružatelji središta za razmjenu internetskog prometa
		– pružatelji usluga DNS-a, osim operatora korijenskih poslužitelja naziva
		– registar naziva vršne nacionalne internetske domene
		– pružatelji usluga računalstva u oblaku
		– pružatelji usluga podatkovnog centra
		– pružatelji mreže za isporuku sadržaja
		– pružatelji usluga povjerenja
		– pružatelji javnih elektroničkih komunikacijskih mreža
		– pružatelji javno dostupnih elektroničkih komunikacijskih usluga
9. Upravljanje uslugama IKT-a (B2B)		– pružatelji upravljanih usluga
		– pružatelji upravljanih sigurnosnih usluga
		– informacijski posrednici kako su definirani propisom kojim se uređuje razmjena elektroničkog računa između poduzetnika
10. Javni sektor		– tijela državne uprave
		– druga državna tijela i pravne osobe s javnim ovlastima
		– privatni i javni subjekti koji upravljaju, razvijaju ili održavaju državnu informacijsku infrastrukturu sukladno zakonu kojim se uređuje državna informacijska infrastruktura
		– jedinice lokalne i područne (regionalne) samouprave
11. Svemir		– operatori zemaljske infrastrukture koji su u vlasništvu, kojima upravljaju i koje vode države članice ili privatne strane te koji podupiru pružanje usluga u svemiru, isključujući pružatelje javnih elektroničkih komunikacijskih mreža

ANNEX II.

OTHER CRITICAL SECTORS

Sektor	Podsektor	Vrsta subjekta
1. Poštanske i kurirske usluge		– davatelji poštanskih usluga Pojam *davatelj poštanskih usluga* u smislu ovoga Zakona znači pravna ili fizička osoba koja obavlja poštanske usluge, uključujući *davatelja univerzalne usluge* kao davatelja poštanskih usluga koji obavlja univerzalnu uslugu u Republici Hrvatskoj. Pojam *poštanska usluga* u smislu ovoga Zakona znači usluga koja uključuje svako postupanje s poštanskim pošiljkama od strane davatelja poštanskih usluga, a osobito prijam, usmjeravanje, prijenos i uručenje poštanskih pošiljaka u unutarnjem ili međunarodnom poštanskom prometu. *Poštanska usluga* ne uključuje prijenos pošiljke primatelju koji pošiljatelj obavlja sam (samodostava), prijevoz kao samostalnu uslugu te prijam, prijenos i uručenje poštanskih pošiljaka izravno od pošiljatelja do primatelja po individualnom zahtjevu, bez usmjeravanja, na način da isti radnik davatelja usluga obavlja sve navedene radnje (kurirska usluga). Pojam *univerzalna usluga* u smislu ovoga Zakona znači skup poštanskih usluga određene kakvoće koje su dostupne po pristupačnoj cijeni svim korisnicima poštanskih usluga na cijelom području Republike Hrvatske, neovisno o njihovoj zemljopisnoj lokaciji. Pojmovi *davatelj poštanskih usluga*, *davatelj univerzalne usluge*, *poštanska usluga* i *univerzalna usluga* istovjetni su s pojmovima iz članka 2. stavka 1. točkama 4., 5., 21. i 32. Zakona o poštanskim uslugama („Narodne novine“, br. 144/12., 153/13., 78/15. i 110/19.) kojim je u hrvatsko zakonodavstvo preuzeta Direktiva (EU) 97/67/EZ Europskog parlamenta i Vijeća od 15. prosinca 1997. o zajedničkim pravilima za razvoj unutarnjeg tržišta poštanskih usluga u Zajednici i poboljšanje kvalitete usluga (SL L 15, 21. 1. 1998.).
		– pružatelji kurirskih usluga
2. Gospodarenje otpadom		– subjekti koji se bave gospodarenjem otpadom, isključujući subjekte kojima gospodarenje otpadom nije glavna gospodarska djelatnost Pojam *gospodarenje otpadom* u smislu ovoga Zakona znači djelatnosti prikupljanja, prijevoza, oporabe
		uključujući razvrstavanje i zbrinjavanje otpada, uključujući nadzor nad obavljanjem tih djelatnosti, nadzor i mjere koje se provode na lokacijama na kojima se zbrinjavao otpad te radnje koje poduzimaju trgovac otpadom i posrednik u gospodarenju otpadom. Pojam *otpad* u smislu ovoga Zakona znači svaka tvar ili predmet koji posjednik odbacuje, namjerava ili mora odbaciti. Pojam *djelatnost prikupljanja otpada* u smislu ovoga Zakona znači djelatnost koja uključuje postupak prikupljanja otpada i postupak prikupljanja otpada u reciklažno dvorište. Pojam *djelatnost prijevoza otpada* u smislu ovoga Zakona znači prijevoz otpada za vlastite potrebe ili za potrebe drugih na teritoriju Republike Hrvatske. Pojam *djelatnost oporabe otpada* u smislu ovoga Zakona znači djelatnost koja uključuje obavljanje postupka oporabe iz Popisa postupaka oporabe otpada. Pojam *tehnološki procesi gospodarenja otpadom* u smislu ovoga Zakona znači određene funkcionalno-tehnološke cjeline gospodarenja otpadom kojima se opisuje materijalni tok otpada, a uključuju prikupljanje, prihvat, skladištenje, prethodno razvrstavanje i razvrstavanje, miješanje otpada, pakiranje, popravak, čišćenje, provjera budućeg proizvoda i drugi procesi u sklopu postupka oporabe i zbrinjavanja otpada. Pojam *djelatnost zbrinjavanja otpada* u smislu ovoga Zakona znači djelatnost koja uključuje obavljanje postupka zbrinjavanja otpada iz Popisa postupaka zbrinjavanja otpada. Pojam *trgovac otpadom* u smislu ovoga Zakona znači pravna ili fizička osoba – obrtnik koja u svoje ime i za svoj račun kupuje i prodaje otpad, uključujući trgovca otpadom koji ne preuzima otpad u neposredni posjed. Pojam *posrednik* u smislu ovoga Zakona znači pravna ili fizička osoba – obrtnik koja obavlja djelatnost posredovanja u gospodarenju otpadom, uključujući i posrednika koji ne preuzima otpad u neposredni posjed.
		Pojmovi *gospodarenje otpadom*, *otpad, djelatnost prikupljanja otpada, djelatnost prijevoza otpada, djelatnost oporabe otpada, tehnološki procesi gospodarenja otpadom, djelatnost zbrinjavanja otpada, trgovac otpadom i posrednik* istovjetni su s pojmovima iz članka 4. stavka 1. točaka 15., 48., 11., 10., 8., 82., 13., 84. i 60. Zakona o gospodarenju otpadom („Narodne novine“, br. 84/21. i 142/23.) kojim je u hrvatsko zakonodavstvo preuzeta Direktiva 2008/98/EZ Europskog parlamenta i Vijeća od 19. studenoga 2008. o otpadu i stavljanju izvan snage određenih direktiva (SL L 312, 22. 11. 2008.), kako je posljednji put izmijenjena Direktivom (EU) 2018/851 Europskog parlamenta i Vijeća od 30. svibnja 2018. o izmjeni Direktive 2008/98/EZ o otpadu (SL L 150, 14. 6. 2018.)
3. Izrada, proizvodnja i distribucija kemikalija		– subjekti koji se bave izradom tvari te distribucijom tvari ili mješavina kako su definirani u članku 3. točkama 9. i 14. Uredbe (EZ) br. 1907/2006 Europskog parlamenta i Vijeća EZ o registraciji, evaluaciji, autorizaciji i ograničavanju kemikalije (REACH) i osnivanju Europske agencije za kemikalije te o izmjeni Direktive 1999/45/EZ i stavljanju izvan snage Uredbe Vijeća (EEZ) br. 793/93 i Uredbe Komisije (EZ) br. 1488/94, kao i Direktive Vijeća 76/769/EEZ i direktiva Komisije 91/155/EEZ, 93/67/EEZ, 93/105/EZ i 2000/21/EZ (Tekst značajan za EGP)
		– subjekti koji se bave proizvodnjom proizvoda kako su definirani u članku 3. točki 3. Uredbe (EZ) br. 1907/2006, iz tvari ili mješavina
4. Proizvodnja, prerada i distribucija hrane		– poduzeća za poslovanje s hranom kako su definirana u članku 3. točki 2. Uredbe (EZ) br. 178/2002 Europskog parlamenta i Vijeća od 28. siječnja 2002. o utvrđivanju općih načela i uvjeta zakona o hrani, osnivanju Europske agencije za sigurnost hrane te utvrđivanju postupaka u područjima sigurnosti hrane, koja se bave veleprodajom te industrijskom proizvodnjom i preradom
5. Proizvodnja	(a) proizvodnja medicinskih proizvoda i in vitro dijagnostičkih medicinskih proizvoda	– subjekti koji proizvode medicinske proizvode kako su definirani u članku 2. točki 1. Uredbe (EU) 2017/745 Europskog parlamenta i Vijeća od 5. travnja 2017. o medicinskim proizvodima, o izmjeni Direktive 2001/83/EZ, Uredbe (EZ) br. 178/2002 i Uredbe (EZ) br. 1223/2009 te o stavljanju izvan snage direktiva Vijeća 90/385/EEZ i 93/42/EEZ (Tekst značajan za EGP) i subjekti koji proizvode in vitro dijagnostičke medicinske proizvode kako su definirani u članku 2. točki 2. Uredbe (EU) 2017/746 Europskog parlamenta i Vijeća od 5. travnja 2017. o in vitro dijagnostičkim
		medicinskim proizvodima te o stavljanju izvan snage Direktive 98/79/EZ i Odluke Komisije 2010/227/EU (Tekst značajan za EGP), osim subjekata koji proizvode medicinske proizvode navedene u Prilogu I. točki 5. petoj alineji ovoga Zakona. Prilog I. točka 5. peta alineja ovoga Zakona upućuje na *„subjekte koji proizvode medicinske proizvode koji se smatraju ključnima tijekom izvanrednog stanja u području javnog zdravlja“* odnosno na *„popis ključnih medicinskih proizvoda u slučaju izvanrednog stanja u području javnog zdravlja“* u smislu članka 22. Uredbe (EU) 2022/123.
	(b) proizvodnja računala te elektroničkih i optičkih proizvoda	– subjekti koji obavljaju bilo koju od gospodarskih djelatnosti iz područja C odjeljka 26. Nacionalne klasifikacije djelatnosti 2007. – NKD 2007. („Narodne novine, br. 58/07. i 72/07.).
	(c) proizvodnja električne opreme	– subjekti koji obavljaju bilo koju od gospodarskih djelatnosti iz područja C odjeljka 27. Nacionalne klasifikacije djelatnosti 2007. – NKD 2007. („Narodne novine, br. 58/07. i 72/07.).
	(d) proizvodnja strojeva i uređaja, d. n.	– subjekti koji obavljaju bilo koju od gospodarskih djelatnosti iz područja C odjeljka 28. Nacionalne klasifikacije djelatnosti 2007. – NKD 2007. („Narodne novine, br. 58/07. i 72/07.).
	(e) proizvodnja motornih vozila, prikolica i poluprikolica	– subjekti koji obavljaju bilo koju od gospodarskih djelatnosti iz područja C odjeljka 29. Nacionalne klasifikacije djelatnosti 2007. – NKD 2007. („Narodne novine, br. 58/07. i 72/07.).
	(f) proizvodnja ostalih prijevoznih sredstava	– subjekti koji obavljaju bilo koju od gospodarskih djelatnosti iz područja C odjeljka 30. Nacionalne klasifikacije djelatnosti 2007. – NKD 2007. („Narodne novine, br. 58/07. i 72/07.).
6. Pružatelji digitalnih usluga		– pružatelji internetskih tržišta
		– pružatelji internetskih tražilica
		– pružatelji platformi za usluge društvenih mreža
7. Istraživanje		– istraživačke organizacije
8. Sustav obrazovanja		– privatni i javni subjekti iz sustava obrazovanja

ANNEX III.

LIST OF COMPETENCES IN THE FIELD OF CYBER SECURITY

No.	Sector	Subsector	Subject type	Competent authority for the implementation of cybersecurity requirements	Competent body for the implementation of special laws	Responsible CSIRT
1.	Energy	All	All	Central State Cybersecurity Authority	–	National Cyber Security Center
2.	Traffic	Air traffic	All	–	Croatian Cyber Civil Aviation Agency	National Center security
3.	Traffic	Railway Aqueous Road	All	Central State Cybersecurity Authority	–	National Cyber Security Center
4.	Banking	–	All	–	Croatian National Bank	National CERT
5.	Financial market infrastructure	–	All	–	Croatian Financial Services Supervisory Agency	National CERT
6.	Healthcare	–	All	Central State Cybersecurity Authority	–	National Cyber Security Center
7.	Water for human consumption	–	All	Central State Cybersecurity Authority	–	National Cyber Security Center
8.	Wastewater	–	All	Central State Cybersecurity Authority	–	National Cyber Security Center
9.	Digital infrastructure	–	Trust service providers	State administration body responsible for the development of the digital society	–	National Cyber Security Center
10.	Digital infrastructure	–	Providers of public electronic communications networks Providers of publicly available electronic communications services	Croatian Regulatory Agency for Network Activities	–	National Cyber Security Center
11.	Digital infrastructure	–	Internet traffic exchange providers DNS service providers, other than root name server operators Cloud computing service providers Data center service providers Content Delivery Network Providers	Central State Cybersecurity Authority	–	National Cyber Security Center
12.	Digital infrastructure	–	Registry of country code top-level domain names	State administration body responsible for science and education	–	National CERT

13.	ICT service management (B2B)	–	All	Central State Cybersecurity Authority	–	National Cyber Security Center
14. Public sector		–	All	Central State Authority for Information Security	–	National Cyber Security Center
15. Space		–	All	Central State Cybersecurity Authority	–	National Cyber Security Center
16.	Postal and courier services	–	All	Central State Cybersecurity Authority	–	National Cyber Security Center
17.	Waste management	–	All	Central State Cybersecurity Authority	–	National Cyber Security Center
18.	Development, production and distribution of chemicals	–	All	Central State Cybersecurity Authority	–	National Cyber Security Center
19.	Production, processing and distribution food waste	–	All	Central State Cybersecurity Authority	–	National Cyber Security Center
20. Production		Production of medical products and in vitro diagnostics - medical medicine - products Production of computers and electronic and optical products - water Electricity production equipment Production of machinery and equipment - me, dn Production of motor vehicles, trailers and semi-trailer Manufacture of other transport equipment	All	Central State Cybersecurity Authority	–	National Cyber Security Center
21.	Digital providers - floor services	–	All	Central State Cybersecurity Authority	–	National Cyber Security Center
22. Research		–	All	State administration body responsible for science and education	–	National CERT
23.	Education system - vanya	–	All	State administration body responsible for science and education	–	National CERT

ANNEX IV.

MANDATORY CONTENT OF THE NATIONAL STRATEGIC ACT
CYBERNETIC PLANNING
SECURITY

AND.

The National Strategic Planning Act from Article 55 of this Act establishes:

- goals and priorities for strengthening cyber security, which especially include sectors and sub-sectors from Annex I and Annex II. of this Act, as well as competent authorities from Annex III. of this Act

– a governance framework for achieving the objectives and priorities referred to in subparagraph 1 of this paragraph, for developing and implementing the policies referred to in point II of this Annex, for developing and strengthening cooperation and coordination at national level between the competent authorities for the implementation of cybersecurity requirements, the single point of contact and the competent CSIRTs, as well as cooperation and coordination between these authorities and the competent authorities for the implementation of specific laws, with explanations of the roles and responsibilities of all authorities relevant for the implementation of cybersecurity policies at national level

– policy frameworks for better coordination between the competent authorities under this Act and the competent authorities under the law regulating the area of critical infrastructures, for the purpose of exchanging information on risks, cyber threats and incidents and on risks, threats and incidents outside cyberspace and performing supervisory tasks

– a mechanism for identifying relevant assets and assessing cyber risks

– measures to ensure preparedness and ability to respond to and recover from cyber incidents, including cooperation between the public and private sectors

– a plan to increase the general level of awareness of cybersecurity among citizens and the necessary measures

– plan for the development of national capabilities in the field of cybersecurity and necessary measures

- a list of competent authorities, other public entities and all other subjects involved in the implementation of the national act of strategic planning in the field of cyber security.

II.

The national strategic planning act referred to in Article 55 of this Law shall elaborate the following policies:

- to resolve cyber security issues in the supply chain for ICT products and ICT services that are used by entities to which this Act applies to provide their services or perform their activities

- to include and define cyber security requirements for ICT products and ICT services in the field of public procurement, including, in relation to cyber security certification, encryption and the use of open source cyber security products

– for the management of cyber vulnerabilities, including the promotion and facilitation of coordinated detection of cyber vulnerabilities in accordance with Article 54 of this Act

– relating to maintaining the general availability, integrity and confidentiality of the public core of the open Internet and, if necessary, the cybersecurity of submarine communication cables

– to promote the development, integration and use of relevant advanced and innovative technologies to implement state-of-the-art cybersecurity risk management measures

– to promote and develop cybersecurity education and training, cybersecurity skills, information and research and development initiatives in the field of cybersecurity, as well as guidelines on good practice and cyber hygiene controls aimed at citizens, as well as public and private entities

- to support academic and research institutions in research, development, improvement and encouragement of the introduction of tools for cyber security and secure information and communication infrastructure, systems and applications

– which include relevant procedures and appropriate information exchange tools to encourage and ensure the voluntary exchange of cybersecurity information in accordance with regulations governing the rules for accessing and handling certain types of information

– to strengthen the cyber resilience and basic level of cyber hygiene of small and medium-sized enterprises, especially those not covered by this Act, by providing easily accessible guidance and assistance for their specific needs, and

– to promote active cyber protection as part of a broader approach to national cybersecurity.

255

Pursuant to Article 89 of the Constitution of the Republic of Croatia, I hereby adopt

DECISION

ON THE PROCLAMATION OF THE LAW ON AMENDMENTS TO THE LAW ON SEA FISHERIES

I hereby promulgate the Act on Amendments to the Marine Fisheries Act, which was adopted by the Croatian Parliament at its session on January 26, 2024.

Class: 011-02/24-02/04

Reg. No.: 71-10-01/1-24-2

Zagreb, February 1, 2024.

President
Republic of Croatia
Zoran Milanoviÿ, senior

LAW

ON AMENDMENTS TO THE LAW ON SEA FISHERIES

Article 1.

Article 2 of the Marine Fisheries Act (Official Gazette, No. 62/17, 14/19 and 30/23) is amended to read:

"This Law regulates the implementation of the following acts:

1. Regulation (EU) No 1380/2013 of the European Parliament and of the Council of 11 December 2013 on the Common Fisheries Policy, amending Council Regulations (EC) No 1954/2003 and (EC) No 1224/2009 and repealing Regulations (EC) No 2371/2002 and (EC) No 639/2004 and Council Decision 2004/585/EC (OJ L 354, 28. 12. 2013), as last amended by Regulation (EU) 2015/812 of the European Parliament and of the Council of 20 May 2015 amending Council Regulation (EC) No 850/98,