THE CROATIAN PARLIAMENT

254

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

DECISION

PROMULGATING THE CYBERSECURITY ACT

I hereby promulgate the Cybersecurity Act, passed by the Croatian Parliament on its session on 26 January 2024.

Class: 011-02/24-02/03
No: 71-10-01/1-24-2
Zagreb, 1 February 2024

The President of
the Republic of Croatia
Zoran Milanović, m. p.

CYBERSECURITY ACT

PART ONE

BASIC PROVISIONS

Aim and subject-matter of the Act

Article 1

(1) This Act regulates the procedures and measures for achieving a high common level of cybersecurity, the criteria for the classification of essential and important entities, cybersecurity requirements for essential and important entities, specific requirements for the management of domain name registration data and the control of their implementation, the voluntary cyber protection mechanisms, competent authorities in the area of cybersecurity and their tasks and powers, expert supervision over the implementation of cybersecurity requirements, infringement provisions, monitoring of the implementation of this Act and other matters relevant to the area of cybersecurity.

(2) This Act establishes a strategic planning and decision-making framework in the area of cybersecurity, as well as national frameworks for managing large-scale cybersecurity incidents and crises.

(3) Achieving and maintaining a high common level of cybersecurity, especially through the development and continuous improvement of cybersecurity policies and their implementation, development of national capabilities in the area of cybersecurity, strengthening of the cooperation and coordination of all relevant bodies, strengthening of public and private sector cooperation, promotion of the development, integration and use of relevant advanced and innovative technologies, promotion and development of education and trainings in the area of cybersecurity and development activities aimed at raising awareness on cybersecurity, are of national importance to the Republic of Croatia.

(4) This Act aims to establish a cybersecurity management system that will ensure the effective implementation of procedures and measures for achieving a high level of cybersecurity in sectors of particular importance for the smooth performance of critical societal 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 is an integral part of this Act:

− Annex I Sectors of High Criticality (hereinafter: Annex I to this Act)

− Annex II Other Critical Sectors (hereinafter: Annex II to this Act)

− Annex III Cybersecurity Jurisdiction List (hereinafter: Annex III to this Act) and

− Annex IV Mandatory Content of the National Strategic Planning Act in the Area of Cybersecurity (hereinafter: Annex IV to this Act).

Harmonisation of regulations with legal acts of the European Union

Article 3

This Act transposes into the legislation of the Republic of Croatia Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2024 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (OJ L 333/80, 27.12.2022).

Definitions

Article 4

(1) For the purposes of this Act, the following definitions shall apply:

1. *active cyber protection* is protection that introduces an advanced approach that implies preventing incidents rather than reactively addressing them, i.e. prevention, detection, monitoring, analysis and mitigation of network and information system security breaches in an active manner, combined with the use of capacities deployed within and outside of the victim network and information system

2. *CSIRT* stands for Computer Security Incident Response Team, i.e. the competent authority for the prevention and protection against cybersecurity incidents, also known under the abbreviation CERT (Computer Emergency Response Team)

3. *CSIRT network* is a network of national CSIRTs established for the purpose of developing confidence and trust and promoting swift and effective operational cooperation among Member States of the European Union (hereinafter: Member States), composed of, apart

from representatives of national CSIRTs, representatives of the competent authority of the European Union for prevention and protection against cybersecurity incidents (CERT-EU)

4. *digital service* is any Information Society service, that is to say, any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services, whereby in the sense of this term:

(a)"at a distance" means that the service is provided without the parties being simultaneously present

(b) "by electronic means" means that the service is sent initially and received at its destination by means of electronic equipment for the processing, including digital compression and storage of data, and entirely transmitted, conveyed and received by wire, by radio, by optical means or by other electromagnetic means

(c)"at the individual request of a recipient of services" means that the service is provided through the transmission of data on individual request

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

(a)"internet access service", i.e. publicly available electronic communications service that provides access to the internet, and thereby connectivity to virtually all end points of the internet, irrespective of the network technology and terminal equipment used

(b) "interpersonal communications service", i.e. a service normally provided for remuneration that enables direct interpersonal and interactive exchange of information via electronic communications networks between a finite number of persons, whereby the persons initiating or participating in the communication determine its recipient(s). This service does not include services which enable interpersonal and interactive communication merely as a minor ancillary feature that is intrinsically linked to another service; and

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

6. *EU-CyCLONe network* is a European cyber crises liaison organisation network established with the aim of operating at the operational level as an intermediary between the technical level (CSIRT network) and the political level, in order to create an efficient process of operational assessment and management during large-scale cybersecurity incidents and crises, and to support decision-making 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, point (14), of Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (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 compromising the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by, or accessible via, network and information systems

12. *online search engine* is an online search engine as defined in Article 2, point (5), of Directive (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 using software, including a website, part of a website or an application, operated by or on behalf of a trader which allows consumers to conclude distance contracts with other traders or consumers

14. *research organisation* is an entity which has as its primary goal to conduct applied research or experimental development with a view to exploiting the results of that research for commercial purposes, but which does not include educational institutions

15. *avoided incident* is any event that could have compromised the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by, or accessible via, network and information systems, but that was successfully prevented from materialising or that did not materialise

16. *public electronic communications network* is an electronic communications network used wholly or mainly for the provision of publicly available electronic communications services which support the transfer of information between network termination points

17. *public entities* are legal persons established by the Republic of Croatia or local or regional self-government units, legal persons that perform public service, legal persons that, under a special regulation, are financed mainly or fully from the state budget or from the budget of local and regional self-government units i.e. from public funds, and companies in which the Republic of Croatia and local and regional self-government units have separate or joint majority ownerships, not including the Croatian National Bank

18. *single point of contact* is a national point of contact responsible for national coordination and cooperation with other Member States in matters of network and information system security

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

20. *large-scale cybersecurity incident* is an incident at the level of the European Union which causes disruptions that exceed a Member State's capacity to respond to it or which has a significant impact on at least two Member States, as well as an incident at the national level which causes disruptions that exceed the capacity of a sector CSIRT body to respond to it or which has a significant impact on at least two sectors, and in those cases cyber crisis management procedures are started in accordance with the existing national general crisis management framework and the European Union cyber crisis management framework

21. *cybersecurity* is cybersecurity 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, point (20), 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 (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, point (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 fast delivery of digital content and services to internet users on behalf of content and service providers

25. *network and information system* consist of:

(a)"electronic communications network" i.e. transmission systems, whether or not based on a permanent infrastructure or centralised administration capacity, and, where applicable, switching or routing equipment and other resources, including network elements which are not active, which permit the conveyance of signals by wire, radio, optical or other electromagnetic means, including satellite networks, fixed (circuit- and packet-switched,

including internet) and mobile networks, electricity cable systems, to the extent that they are used for the purpose of transmitting signals, networks used for radio and television broadcasting, and cable television networks, irrespective of the type of information conveyed

(b) any device or group of interconnected or related devices, one or more of which, pursuant to a programme, carry out automatic processing of digital data; or

(c) digital data stored, processed, retrieved or transmitted by elements covered under subitems (a) and (b) of this item, for the purposes of their operation, use, protection and maintenance

26. *national strategic planning act in the area of cybersecurity* is a comprehensive framework that defines specific objectives and priorities in the area of cybersecurity and management in order to achieve them

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

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

29. *competent CSIRT* is the CSIRT at the central government authority for cybersecurity or the CSIRT at the Croatian Academic and Research Network (hereinafter: CARNET), depending on the division of jurisdiction under this Act

30. *standard* is the standard as defined in Article 2, point (1), of 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, 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* are any information as defined in Article 4, paragraph 1, point (1), of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119/1, 4 May 2016) (hereinafter: Regulation (EU) 2016/679), and especially information required for the identification of registrants and points of contact administering the domain names, as well as IP addresses (internet protocol address used on any device connected to the internet), uniform resources locators (URLs), domain names, email addresses, time stamps and other information that, in certain cases, may reveal personal data within the framework of activities carried out under this Act

32. *significant cyber threat* is a cyber threat which, based on its technical characteristics, can be assumed to have the potential to have a severe impact on the network and information systems of an entity or the users of the entity's services by causing considerable material or non-material damage, i.e. service interruptions to users

33. *social networking services platform* is a platform that enables end-users to connect, share, discover and communicate with each other across multiple devices, in particular via chats, posts, videos and recommendations

34. *incident handling* are any actions and procedures aiming to prevent, detect, analyse, and contain or to respond to and recover from an incident

35. *representative* is a natural or legal person established in the European Union explicitly designated to act on behalf of a domain name system provider (hereinafter: DNS service provider), a country code top-level domain (ccTLD) name registry, 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 a provider of an online marketplace, of an online search engine or of a social networking services platform that is not established in the European Union, which may be addressed by a competent authority or a CSIRT in the place of the entity itself with regard to the obligations of that entity under this Act

36. *private entities* are natural or legal persons created and recognised as such under the national law of their place of establishment, which may, acting under their own name, exercise rights and be subject to obligations

37. *managed security service provider* is a managed service provider that carries out or provides assistance for activities relating to cybersecurity risk management

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, via assistance or active administration carried out either on customers' premises or remotely

39. *DNS service provider* is an entity that provides:

(a)publicly available recursive domain name resolution services for internet end-users and/or

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

40. *trust service provider* is a trust service provider as defined in Article 3, point (19), of Regulation (EU) No 910/2014

41. *vulnerability* is a weakness, susceptibility or flaw of ICT products or ICT services that can be exploited by a cyber threat

42. *country code top-level domain name registry* is an entity which has been delegated a specific online TLD and is responsible for administering the TLD including the registration of domain names under the TLD and the technical operation of the TLD, including the operation of its name servers, the maintenance of its databases and the distribution of TLD zone files across name servers, irrespective of whether any of those operations are carried out by the entity itself or are outsourced, but excluding situations where TLD names are used by a registry only for its own use. In the Republic of Croatia this is CARNET

43. *registrar* is an entity providing domain name registration services, i.e. a legal or natural person who performs an independent activity authorised for the registration and administration of .hr domains on behalf of the ccTLD name registry

44. *regulatory authority for network activities* is the Croatian Regulatory Authority for Network Industries

45. *risk* is the potential for loss or disruption caused by an incident and is expressed as a combination of the magnitude of such loss or disruption and the likelihood of occurrence of the incident

46. *security of network and information systems* is the ability of network and information systems to resist, at a given level of confidence, any event that may compromise the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by, or accessible via, those network and information systems

47. *systemic risk* is the risk of disruption in the service or in carrying out an activity, which could have serious negative impacts on one or more sectors or could have a cross-border impact

48. *Cooperation Group* is a group established for the purpose of supporting and facilitating strategic cooperation and the exchange of information among Member States, and developing trust and safety in the area of cybersecurity at the level of the European Union

49. *central government authority for information security* is the Office of the National Security Council

50. *central government authority for cybersecurity* is the Security and Intelligence Agency

51. *central government authority for performing tasks in technical areas of information security* is the Information Systems Security Bureau

52. *internet exchange point* is a network facility which enables the interconnection of more than two independent networks (autonomous systems), primarily for the purpose of facilitating the exchange of internet traffic, which provides interconnection only for autonomous systems and which neither requires the internet traffic passing between any pair of participating autonomous systems to pass through any third autonomous system nor alters or otherwise interferes with such traffic

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

54. *public sector entities* are state administration authorities, other state authorities, legal persons with public authority, local and regional self-government units, as well as private and public entities for which classification is carried out under this Act due to their role in the management, development and maintenance of state information infrastructure

55. *domain name system* or *DNS* is a hierarchical distributed naming system which enables the identification of internet services and resources, allowing end-user devices to use internet routing and connectivity services to reach those services and resources

56. *education system* includes early childhood education and care, primary education, secondary education and higher education, system monitoring, evaluation and development and programme implementation

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

58. *state administration authority responsible for the development of the digital society* is the Central State Office for the Development of Digital Society

59. *state administration authority responsible for science and education* is the Ministry of Science and Education

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

61. *ICT third-party service provider* is an ICT service provider as defined in Article 3, point (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 Regulations (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. *management body of an essential and important entity* is a body or bodies appointed in accordance with the law regulating the establishment and operation of the entity, and which have the authority to manage and conduct the affairs of the entity

63. *data centre service* is a service that encompasses structures, or groups of structures, dedicated to the centralised accommodation, interconnection and operation of IT and network equipment providing data storage, processing and transport services together with all the facilities and infrastructures for power distribution and environmental control

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

65. *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 where such resources are distributed across several locations

66. *employee of the entity* is a natural person employed to perform certain tasks for the entity, including a natural person who, according to the regulation on companies, as a member of the management board or executive director or natural person who is authorised to

manage the affairs of the entity in another capacity according to a special law, individually and independently or jointly and collectively, or natural person who, as an employee in the employment relationship, performs certain tasks for the entity.

(2) The terms used in this Act, which are gender-specific, refer equally to the male and female gender.

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

Article 5

(1) If, in the implementation of this Act, classified data or other data are created or used, for which rules of procedure have been determined by special regulations in order to safeguard their secrecy or confidentiality, special regulations on their protection shall apply to such data.

(2) This Act shall not apply to information systems that have a security accreditation for handling classified data.

Application of rules on personal data protection

Article 6

(1) The application of the provisions of this Act leaves unaffected the obligations of the providers of public electronic communications networks or providers of publicly available electronic communications services to process personal data in accordance with special regulations on personal data protection and protection of privacy.

(2) The application of the provisions of this Act leaves unaffected the obligations of essential and important entities to, in case of a personal data breach, act in accordance with the provisions of Articles 33 and 34 of Regulation (EU) 2016/679.

Relationship with the law governing the area of electronic communications

Article 7

(1) The application of the provisions of this Act leaves unaffected the obligation to implement basic requirements for electronic communications infrastructure and other related equipment prescribed by the law governing the area of electronic communications.

(2) The application of the provisions of this Act leaves unaffected the rules on managing the ccTLD and the rights and obligations of registrants prescribed by the law governing the area of electronic communications.

Application of special laws in matters of cybersecurity

Article 8

(1) If, for essential and important entities from individual sectors from Annex I and Annex II to this Act, special laws prescribe requirements, which in their content and purpose correspond to the cybersecurity requirements referred to in this Act, or pose more rigorous requirements, the corresponding provisions of that special law shall apply to these entities in matters that are regulated in relation to these requirements and their implementation, including provisions on supervision over the implementation of the requirements.

(2) The requirements referred to in paragraph 1 of this Article shall correspond to the cybersecurity requirements from this Act in their content and purpose if:

– they are at least equivalent in effect to cybersecurity risk-management measures laid down in this Act

– an immediate access, where appropriate automatic and direct, to the incident notifications has been determined for the competent CSIRT by a special law, and if the obligations to notify significant incidents from the special law are at least equivalent in effect to the obligations to notify significant incidents laid down in this Act.

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

PART TWO

CLASSIFICATION OF ENTITIES

CHAPTER I

CRITERIA FOR THE IMPLEMENTATION OF THE CLASSIFICATION OF ENTITIES

General criteria for the implementation of the classification of essential entities

Article 9

The following are classified into the category of essential entities:

– private and public entities from Annex I to this Act that exceed the ceilings for medium-sized small business entities established under the law regulating the bases for the application of economic policy stimulus measures aimed at developing and restructuring small business and adapting it to the market

– qualified trust service providers, ccTLD name registry and DNS service providers, regardless of their size

– providers of public electronic communications networks or of publicly available electronic communications services who represent a medium-sized small business entity under the law regulating the bases for the application of economic policy stimulus measures aimed at developing and restructuring small business and adapting it to the market or that exceed the ceilings for medium-sized small business entities

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

– entities determined as critical entities under the law regulating the area of critical infrastructure, regardless of their size.

General criteria for the implementation of the classification of important entities

Article 10

The following are classified into the category of important entities:

– private and public entities from Annex II to this Act that represent medium-sized small business entities under the law regulating the bases for the application of economic policy stimulus measures aimed at developing and restructuring small business and adapting it to the market or that exceed the ceilings for medium-sized small business entities

– private and public entities from Annex I to this Act that are not determined as essential entities under Article 9, subparagraph 1 of this Act, and that represent a medium-sized small business entity under the law regulating the bases for the application of economic policy stimulus measures aimed at developing and restructuring small business and adapting it to the market

– trust service providers who are not classified as essential entities under Article 9, subparagraph 2 of this Act, regardless of their size, and

– providers of public electronic communications networks or of publicly available electronic communications services who are not classified as essential entities under Article 9, subparagraph 3 of this Act, regardless of their size.

Special criteria for the implementation of the classification of essential and important entities

Article 11

Notwithstanding Article 9, subparagraph 1 and Article 10, subparagraphs 1 and 2 of this Act, private and public entities from Annex I and Annex II to this Act may be classified into the essential or important entities category, regardless of their size, if:

– the entity is the sole provider of a service that is essential for the maintenance of critical societal or economic activities

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

– a disruption of the service provided by the entity or a disruption in the performance of activities of the entity could induce a significant systemic risk in sectors from Annex I and Annex II to this Act, in particular in sectors where such a disruption could have a cross-border impact or

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

Classification of public sector entities

Article 12

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

– state administration authorities, and

– other state authorities and legal persons with public authority, depending on the results of the conducted assessment of their importance for the smooth performance of critical societal or economic activities.

(2) Notwithstanding Article 9, subparagraph 1 and Article 10, subparagraph 2 of this Act, private and public entities that manage, develop and maintain state information infrastructure in accordance with the law regulating state information infrastructure are classified into the category of essential entities, regardless of their size.

(3) Local and regional self-government units are classified, regardless of their size, in the important entities category, depending on the results of the conducted assessment of their importance for the smooth performance of critical societal or economic activities.

Classification of entities from the education system

Article 13

Notwithstanding Article 10, subparagraph 1 of this Act, private and public entities from the education system are classified, regardless of their size, in the category of important entities, depending on the results of the conducted assessment of their special importance for the performance of education and care at the national or regional level.

Establishing jurisdiction based on territoriality

Article 14

(1) Entities from Annex I and Annex II to this Act are subject to the jurisdiction and authority set out in this Act if they provide services or perform activities within the European Union, and they are established in the territory of the Republic of Croatia.

(2) Notwithstanding paragraph 1 of this Article, providers of public electronic communications networks or publicly available electronic communications services are subject to the jurisdiction and authority set out in this Act if they provide their services in the territory of the Republic of Croatia, regardless of the country of establishment.

(3) Notwithstanding paragraph 1 of this Article, DNS service providers, the ccTLD name registry and registrars, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, managed security service providers, providers of online marketplaces, providers of online search engines or providers of social networking services platforms are subject to the jurisdiction and authority set out in this Act if they have their main establishment in the territory of the Republic of Croatia or their representative has their establishment in the territory of the Republic of Croatia.

(4) The entity has its main establishment within the meaning of paragraph 3 of this Article if it carries out the following in the territory of the Republic of Croatia:

– predominantly takes decisions related to cybersecurity risk management or

– carries out cybersecurity risk-management measures when the Member State in which the decisions from subparagraph 1 of this paragraph are made cannot be determined or if such decisions are not taken in the European Union or

– has an establishment with the highest number of employees in the European Union when the Member State where the activities from subparagraph 2 of this paragraph are carried out, cannot be determined.

Application of entity size criteria

Article 15

(1) When determining if an entity represents a medium-sized small business entity or if the entity exceeds the ceilings for medium-sized small business entities under the law regulating the bases for the application of economic policy stimulus measures aimed at developing and restructuring small business and adapting it to the market, the following is taken into account:

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

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

regardless of whether the entity also provides other services or also performs other activities that are not included in Annex I and Annex II to this Act.

(2) When classifying entities, the guidelines of the European Commission on the implementation of the size criteria applicable to microenterprises and small enterprises are taken into account.

Application of the Act in case of double classification of an entity

Article 16

If the entity is classified in both the category of essential and important entities, the provisions of this Act related to essential entities shall apply to that entity.

CHAPTER II

LISTS OF ESSENTIAL AND IMPORTANT ENTITIES

Maintaining lists

Article 17

(1) Competent authorities for implementing cybersecurity requirements and competent authorities for implementing special laws shall carry out the classification of entities in accordance with this Act and shall establish and maintain the lists of essential and important entities.

(2) Competent authorities for implementing cybersecurity requirements and competent authorities for implementing special laws shall check the lists of essential and important entities regularly, at least once every two years, and update them if necessary.

Submission of data to the European Commission and the Cooperation Group

Article 18

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

– to the European Commission and the Cooperation Group, data on the number of essential 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 referred to in Annex I and Annex II to this Act

– to the European Commission, data on the number of essential and important entities classified on the basis of Article 11 of this Act, the sector and subsector to which they belong, the type of service provided and the provisions laid down in Article 11 of this Act on the basis of which the classification was conducted, and additionally, it may also submit data on the names of these entities to the European Commission at its request.

(2) Competent authorities for implementing cybersecurity requirements and competent authorities for implementing special laws shall submit data required for the submission of data in accordance with paragraph 1 of this Article to the single point of contact.

Notifications on the conducted entity classification

Article 19

(1) Competent authorities for implementing cybersecurity requirements shall notify all entities from the list referred to in Article 17, paragraph 1 of this Act that are under their jurisdiction on the conducted classification of entities and the obligations they are subject to under this Act and the implementing regulation on the cybersecurity requirements referred to in this Act.

(2) Competent authorities for implementing cybersecurity requirements shall notify the entities with regard to which, after the update of the list of essential and important entities, there has been a change in the classification of entities on the change in the category and the fact that the obligations that they are subject to under this Act and the implementing regulation on the cybersecurity requirements under this Act are also changing as of the date of

receipt of this notification, with the indication of significant changes that must be taken into account depending on the category change being notified.

(3) Competent authorities for implementing cybersecurity requirements shall notify entities that are no longer considered essential nor important entities after the update of the list of essential and important entities on this fact and the fact that as of the date of receipt of this notification they are no longer subject to the obligations of implementing the cybersecurity requirements referred to in this Act.

(4) Competent authorities for implementing cybersecurity requirements shall notify the entities on the conducted classification of entities, as well as on the changes referred to in paragraphs 2 and 3 of this Article, within 30 days from the date of the conducted classification of entities or the update of the list of essential and important entities.

Obligations of entities referred to in Annex I and Annex II to the Act in terms of data collection

Article 20

(1) For the purpose of entity classification in accordance with this Act and maintaining the list of essential and important entities, the entities referred to in Annex I and Annex II to this Act shall submit to the competent authorities for implementing cybersecurity requirements and competent authorities for implementing special laws, upon their request, the following data:

– the name of the entity

– the address and up-to-date contact details, including email addresses, IP ranges and telephone numbers

– the relevant sector, subsector and entity type referred to in Annex I and Annex II to this Act

– a list of the Member States where they provide services falling within the scope of this Act

– other data on providing their services or carrying out their activities relevant to the implementation of the classification of the entity or to the determination of jurisdiction over the entity.

(2) Deadlines for the submission of data pursuant to paragraph 1 of this Article are determined depending on the scope and complexity of the data to which the request refers, provided that the deadline cannot be shorter than 15 days nor longer than 45 days from the date of receipt of the request for the submission of data.

(3) Entities referred to in paragraph 1 of this Article shall notify without delay the competent authority for implementing the cybersecurity requirements or the competent authority for implementing special laws on all changes in the data submitted to that authority in accordance with paragraph 1 of this Article within two weeks from the date of the change.

Collecting data from other sources for the implementation of entity classification

Article 21

(1) State administration authorities, other state authorities, local and regional self-government units, legal persons with public authority and public entities that collect data within the scope of their activities or keep registries, records and collections of data on entities referred to in Annex I and Annex II to this Act shall, without compensation, provide the following to the competent authorities for implementing cybersecurity requirements:

– regularly submit lists of entities referred to in Annex I and Annex II to this Act or enable access to the appropriate data in registers, records and data collections by electronic means

– upon request of the competent authority for implementing cybersecurity requirements, submit the following for the entities referred to in the list in subparagraph 1 of this paragraph:

(a) data on their size and/or

(b) other data on entities, including data on provision of their services or performance of their activities, if those data are necessary for the implementation of the classification of entities in accordance with this Act or

(c) refer them to the state administration authority, other state authority, local and regional self-government unit, legal person with public authority or public entity in possession of such data.

(2) If the data based on this Article are submitted upon request of the competent authorities for implementing cybersecurity requirements, the deadlines for the submission of data are determined depending on the scope and complexity of the data to which the request refers, provided that the deadline cannot be shorter than 15 days nor longer than 45 days from the date of receipt of the request for the submission of data.

CHAPTER III

SPECIAL REGISTRY OF ENTITIES

Maintaining a special registry of entities

Article 22

(1) The central government authority for cybersecurity shall create and maintain a special registry of the following entities:

– DNS service providers
– ccTLD name registry
– registrars
– cloud computing service providers
– data centre service providers
– content delivery network providers
– managed service providers
– managed security service providers
– providers of online marketplaces
– providers of online search engines and
– providers of social networking services platforms.

(2) The registry referred to in paragraph 1 of this Article shall be maintained independently of the obligation to maintain a list of essential and important entities.

Collecting data

Article 23

(1) The entities referred to in Article 22 of this Act shall submit the following data to the central government authority for cybersecurity:

– the name of the entity
– a list of services referred to in Article 22 of this Act that they provide
– the address of the entity's main establishment and its other establishments or the address of its representative
– up-to-date contact details, including e-mail addresses and telephone numbers of the entity and its representative

– a list of the Member States where they provide services referred to in Article 22 of this Act

– the entity's IP ranges.

(2) The deadline for the submission of data based on paragraph 1 of this Article is 15 days from the date of receipt of the request for the submission of data.

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

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

The implementing regulation on the classification of entities, maintaining lists of essential and important entities and a special registry of entities

Article 24

The benchmarks for the classification of entities in the category of essential or important entities based on special criteria referred to in Article 11 of this Act, criteria for the implementation of assessments referred to in Article 12, paragraph 1, subparagraph 2 and paragraph 3 and Article 13 of this Act, maintaining a list of essential and important entities, collecting data for the purpose of implementing the classification of entities in accordance with this Act and maintaining a special registry of entities referred to in Article 22 of this Act are prescribed by the Government of the Republic of Croatia (hereinafter: the Government) by a regulation, at the proposal of the central government authority for cybersecurity.

PART THREE

CYBERSECURITY REQUIREMENTS

Scope of cybersecurity requirements

Article 25

(1) Cybersecurity requirements include procedures and measures that essential and important entities shall apply in order to achieve a high level of cybersecurity in providing their services or performing their activities, and they consist of the following:

– cybersecurity risk-management measures, and

– the obligation to notify significant incidents and significant cyber threats.

(2) Cybersecurity requirements refer to all network and information systems that essential or important entities use in their operations or in providing their services and all services that essential and important entities provide or activities they perform, regardless of whether the entity also provides other services or also performs other activities that are not included in Annex I and Annex II to this Act.

CHAPTER I

CYBERSECURITY RISK-MANAGEMENT MEASURES AND COMPLIANCE CHECKS FOR ESSENTIAL AND IMPORTANT ENTITIES

Application of measures

Article 26

(1) Essential and important entities shall implement appropriate and proportionate measures of cybersecurity risk management.

(2) Cybersecurity risk-management measures shall be based on an all-hazards approach that aims to protect network and information systems and the physical environment of those systems from incidents.

(3) Cybersecurity risk-management measures include:

– technical, operational and organisational measures to manage the risks posed to the security of network and information systems which essential and important entities use for their operations or for the provision of their services, and

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

(4) Essential and important entities shall implement cybersecurity risk-management measures regardless of whether they manage and/or maintain their network and information systems themselves or outsource the management and maintenance thereof.

(5) Essential and important entities shall implement cybersecurity risk-management measures within one year from the date of submission of the notification referred to in Article 19, paragraph 1 of this Act.

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

(7) The deadline referred to in paragraph 6 of this Article is determined depending on the scope and complexity of obligations on which the entity is being notified, provided that the deadline cannot be shorter than 60 days nor 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 proportionate to the risk determined

Article 27

(1) Essential and important entities shall ensure a level of security of network and information systems proportionate to the determined risk by applying cybersecurity risk-management measures.

(2) When assessing the proportionality of the applied cybersecurity risk-management measures, the following is taken into account:

– degree of the entity's exposure to risks

– entity's size

– likelihood of occurrence of incidents and their severity, including their potential societal and economic impact.

Manner of implementing cybersecurity risk-management measures

Article 28

(1) Cybersecurity risk-management measures are implemented in such a way that, without imposing or discriminating in favour of the use of a particular type of technology, they take into account the state-of-the-art used within the best security practices in the area of

cybersecurity, as well as European and international standards and technical specifications relevant for the security of network and information systems, also taking into account the cost of implementation.

(2) Essential and important entities shall use certain ICT products, ICT services and ICT processes and managed security services certified under European cybersecurity certification schemes or national cybersecurity certification schemes when implementing cybersecurity risk-management measures, if such an obligation is prescribed by:

– relevant regulations of the European Union

– special regulations regulating the area of provision of specific services or performance of specific activities

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

Responsibility for the implementation of measures

Article 29

(1) In accordance with this Act, the members of management bodies of essential and important entities or the heads of state administrative authorities, other state authorities, executive bodies of local and regional self-government units (hereinafter: persons responsible for the management of measures) are responsible for the implementation of cybersecurity risk-management measures.

(2) Persons responsible for the management of measures shall approve cybersecurity risk-management measures that the entity shall apply in order to comply with obligations defined under this Act and the implementing regulation on cybersecurity requirements and control their implementation.

(3) For the purpose of acquiring know-how and skills in matters of cybersecurity risk management and their impact on the services provided by the entity or the activities it performs, the persons responsible for the management of measures shall do the following:

– attend appropriate trainings

– enable employees of the entity to attend appropriate trainings.

(4) The provisions of this Article also apply to other natural persons that participate in making decisions on cybersecurity risk-management measures and/or their implementation on the basis of a power to carry out the supervision over the operating of the entity or acting as a legal representative of the entity under power of attorney or other power to represent it or power of attorney or other power to make decisions on behalf of the entity.

Cybersecurity risk-management measures

Article 30

(1) Cybersecurity risk-management measures include the following:

– policies on risk analysis and information system security

– incident handling, including their monitoring, documenting and reporting

– business continuity, such as backup management and disaster recovery, downtime and incidents referred to in Article 37 of this Act, and cyber crisis management

– supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers

– security in network and information systems acquisition, development and maintenance, including vulnerability remediation and disclosure

– policies and procedures to assess the effectiveness of cybersecurity risk-management measures

– basic cyber hygiene practices and cybersecurity training

– policies and procedures regarding the use of cryptography and, where appropriate, encryption

– human resources security, access control policies and management of software and hardware assets, including regular updates to the list of these assets

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

(2) When assessing the proportionality of the applied measures referred to in paragraph 1, subparagraph 4 of this Article, essential and important entities shall take into account the vulnerabilities specific to each direct supplier and service provider and the overall quality of products and cybersecurity practices of their suppliers and service providers, as well as the results of the coordinated security risk assessments of critical ICT service, ICT system or ICT product supply chains, carried out by the Cooperation Group in cooperation 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 cybersecurity risk-management measures

Article 31

(1) Essential and important entities shall check the compliance of the established cybersecurity risk-management measures with the cybersecurity risk-management measures set out under this Act and the regulation referred to in Article 24 of this Act.

(2) Compliance checks referred to in paragraph 1 of this Article are carried out within the audit of cybersecurity of essential and important entities and in the process of self-assessment of cybersecurity of important entities.

Cybersecurity auditors

Article 32

(1) Auditing of the cybersecurity of essential and important entities is carried out by cybersecurity auditors.

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

– a national security certificate for cybersecurity auditing or

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

(3) Notwithstanding paragraph 2 of this Article, the cybersecurity auditor for state administration authorities and other state authorities is the central government authority for performing tasks in technical areas of information security.

(4) Cybersecurity auditors shall draw up a report on the conducted cybersecurity audit.

National security certificate for cybersecurity auditing

Article 33

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

(2) The rules from paragraph 1 of this Article are laid down by the central government authority for performing tasks in technical areas of information security, and these include the following:

– organisational and expert requirements that must be met by managed security service providers for implementing a cybersecurity audit

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

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

(3) The rules from paragraph 1 of this Article shall apply if no appropriate European cybersecurity certification scheme, which includes cybersecurity audits, has been adopted.

(4) The central government authority for performing tasks in technical areas of information security shall maintain a publicly available registry of managed security service providers referred to in Article 32, paragraph 2, subparagraph 1 of this Act.

Implementation of a cybersecurity audit

Article 34

(1) Essential entities shall carry out a cybersecurity audit at least once every two years.

(2) Essential entities shall carry out 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 implementing cybersecurity requirements under Article 79, paragraph 1, subparagraph 7 or Article 81, paragraph 1, subparagraph 2 of this Act.

(3) A cybersecurity audit referred to in paragraph 1 of this Article shall be carried out as a separate procedure or within the business audit or another compliance check of the entity carried out on the basis of special regulations that regulate the area of provision of specific services or the performance of specific activities.

(4) Important entities shall carry out a cybersecurity audit when requested by the competent authority for implementing cybersecurity requirements under Article 79, paragraph 1, subparagraph 7 of this Act.

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

(6) Notwithstanding paragraph 5 of this Article, when the cybersecurity audit was conducted upon request of the competent authority for implementing cybersecurity requirements under Article 79, paragraph 1, subparagraph 7 or Article 81, paragraph 1, subparagraph 2 of this Act, the entity for which the cybersecurity audit was conducted shall submit the report referred to in Article 32, paragraph 4 of this Act to the competent authority for implementing cybersecurity requirements immediately upon its receipt.

(7) The costs of the implementation of the cybersecurity audit shall be borne by the essential and important entities, unless otherwise prescribed by this Act.

Implementation of a cybersecurity self-assessment

Article 35

(1) Important entities shall carry out a cybersecurity self-assessment at least once every two years.

(2) Important entities may also outsource the implementation of the cybersecurity self-assessment.

(3) If the results of the conducted cybersecurity self-assessment show that the established cybersecurity risk-management measures are in accordance with the cybersecurity risk-management measures prescribed under this Act and the regulation referred to in Article 24 of this Act, the important entities shall draw up a statement on 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 under this Act and the regulation referred to in Article 24 of this Act, the important entities shall establish a plan for follow-up action, including a plan for a timely repeated cybersecurity self-assessment and remediation of the 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 implementing cybersecurity requirements without delay, and no later than eight days from the date of their drafting.

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

Implementing regulation for the cybersecurity self-assessment

Article 36

Rules, technical requirements, standards and procedures applied in the implementation of the cybersecurity self-assessment, including the contents of the statement on compliance, shall be regulated by the regulation referred to in Article 24 of this Act.

CHAPTER II

NOTIFICATION OBLIGATION REGARDING CYBER THREATS AND INCIDENTS

Notifying significant incidents

Article 37

(1) Essential and important entities shall notify the competent CSIRT on any incident that has a significant impact on the availability, integrity, confidentiality and authenticity of data significant for the operation of the entity and/or the continuity of services they provide or the activities they perform (hereinafter: significant incident).

(2) An incident shall be considered to be significant if:

– it has caused or is capable of causing severe operational disruption of the services provided by the entity or the activities it performs or financial loss for the entity

– it has affected or is capable of affecting other natural or legal persons by causing considerable material or non-material damage.

(3) Essential and important entities shall submit the notifications referred to in paragraph 1 of this Article to law enforcement authorities in cases in which there are grounds to suspect that significant incidents were caused as a result of a criminal offence, based on the provisions of the act governing criminal proceedings.

(4) Essential and important entities shall start to submit the notifications referred to in paragraph 1 of this Article within 30 days from the date of the submission of the notification referred to in Article 19, paragraph 1 of this Act.

Notifying service recipients

Article 38

(1) Essential and important entities shall notify the recipients of their services on significant incidents that are likely to affect the provision of those services.

(2) In the event of a significant cyber threat, essential and important entities shall notify the recipients of their services potentially affected by such a threat on any protective measures or judicial remedies they can use for the purpose of preventing or compensating the caused damage and, where appropriate, notify the recipients of the services of the significant cyber threat itself.

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

Notifying on a voluntary basis

Article 39

Essential and important entities may voluntarily notify the competent CSIRT of any incident, cyber threat and near miss.

Notifying significant incidents with cross-border and cross-sectoral impact

Article 40

(1) Upon request of the competent CSIRT or at its own discretion, the single point of contact shall notify the single points of contact of the affected Member State and ENISA on the significant incident with cross-border impact, especially if the incident concerns two or more Member States.

(2) Upon request of the competent CSIRT or at its own discretion, the single point of contact shall notify the state administration authorities competent for the affected sectors on the significant incident with cross-sectoral impact.

Notifying the public on the significant incident

Article 41

Where public awareness is necessary to prevent a significant incident or deal with an ongoing significant incident, or where disclosure of the significant incident is otherwise in the public interest, 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 implementing cybersecurity requirements or the competent authority for implementing special laws, depending on the division of jurisdiction referred to in Annex III to this Act, and the affected entity, notify the public on the significant incident or request the essential and important entity to do so.

Notifying the single point of contact and ENISA

Article 42

(1) The competent CSIRTs shall notify the single point of contact on significant incidents, other incidents, significant cyber threats and near misses on which they were notified by essential and important entities based on 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, significant cyber threats and near misses that essential and important entities notified the competent CSIRT based on Articles 37 and 39 of this Act.

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

Article 43

(1) Notifying based on Articles 37 and 39 of this Act and the exchange of data on cyber threats and incidents between competent authorities referred to in Annex III to this Act shall be carried out via a national platform for the collection, analysis and exchange of data on cyber threats and incidents, as a single entry point for reporting on cyber threats and incidents.

(2) CARNET is competent for the development and management of the national platform referred to in paragraph 1 of this Article.

Implementing regulation on notification of cyber threats and incidents

Article 44

The criteria for determining significant incidents, including criterion thresholds, if they are necessary due to the specificity of a particular sector, the types and content of the notifications referred to in Articles 37 to 40 of this Act, the deadlines for their delivery, the handling of such notifications, including the actions of the competent CSIRT in connection with the received notifications referred to in Articles 37 and 39 of this Act, the right of access and other matters relevant for the use of the national platform for the collection, analysis and exchange of data on cyber threats and incidents, including the possibility of using other ways of delivering notifications referred to in Articles 37 and 39 of this Act, are laid down in the regulation referred to in Article 24 of this Act.

CHAPTER III

SPECIFIC REQUIREMENTS FOR THE MANAGEMENT OF DOMAIN NAME REGISTRATION DATA

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

Article 45

For the purpose of ensuring a reliable, resilient and secure domain name system, the ccTLD name registry and registrars shall implement specific requirements for the management of domain name registration data.

Content of information in databases of domain name registration data and determining the identity of the registrant

Article 46

(1) The ccTLD name registry and registrars shall ensure that the database of domain name registration data contains the necessary information to identify and contact the registrants and registrars who administer the domain names, namely:

– the domain name

– the date of registration

– the registrant's name, contact email address and telephone number

– the contact email address and telephone number of the registrar administering the domain name.

(2) The ccTLD name registry and registrars shall determine the identity of the registrant and check their identity on the basis of identification documents, i.e. documents, data or information received from a credible, reliable and independent source, including, if the registrant has one, a qualified certificate for an electronic signature or electronic seal or any other safe, remote or electronic identification procedure that is regulated, recognised, approved or accepted by the relevant national authorities.

(3) Failure of the applicant for domain registration and the registrant to act in accordance with the obligations prescribed under this Act represents a basis for denial of domain registration or deletion of the domain.

Obligations of the ccTLD name registry and the registrars

Article 47

(1) If the domain registration request does not contain all data referred to in Article 46, paragraph 1, subparagraphs 1 to 3 of this Act, the ccTLD name registry and registrars shall deny such a request, and the applicant shall be notified on the denial of domain registration or the temporary deactivation of the domain and the inability to use it until the request is duly submitted, namely within eight days from the date of receipt of the notification.

(2) The ccTLD name registry and registrars shall periodically, and at least once a year, check the existence of registrants for all of its registrants, as well as the compliance of the actions of the registrant with the obligations from the regulation regulating the organisation and management of the ccTLD.

(3) In the event of unavailability of the registrant as part of the multiple checks referred to in paragraph 2 of this Article regarding different registered contact details of the registrant or an established abuse of rights or other improper conduct of the registrant, the ccTLD name registry and registrars shall delete such a domain.

(4) The ccTLD name registry and registrars shall establish and make publicly available database management policies referred to in Article 46 of this Act that must also include data verification procedures from the domain registration requests.

(5) After the domain name registration, the ccTLD name registry and registrars shall immediately make publicly available the domain name registration data that are not personal data.

Data storage and registrant data access

Article 48

(1) The ccTLD name registry and registrars shall keep the data, information and documentation collected on the basis of 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 shall include:

– identification documents and other documents on the basis of which the identity of the registrant was determined

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

(3) The ccTLD name registry and registrars shall submit or otherwise appropriately enable access to registrant data to law enforcement authorities and the competent CSIRT, the authority responsible for the protection of personal data and other legal persons with public authority, as well as to state authorities within the exercise of public authority, upon their reasoned request, without delay, and no later than 72 hours from the receipt of the request.

(4) After the expiry of the deadline for storing data referred to in paragraph 1 of this Article, the ccTLD name registry and registrars shall delete the personal data on the registrant and destroy the documentation referred to in paragraph 2 of this Article in accordance with regulations on the protection of personal data.

(5) The ccTLD name registry and registrars shall indicate their obligation of acting in accordance with paragraphs 1 and 3 of this Article in their management policies referred to in Article 47, paragraph 4 of this Act.

(6) The technical and organisational measures for the protection of personal data of registrants are regulated by special regulations governing the organisation and management of the ccTLD.

Implementation of compliance control regarding specific requirements for the management of name registration data

Article 49

Control of compliance of the actions of the ccTLD name registry with the specific requirements for the management of domain name registration data referred to in Articles 45 to 48 of this Act is carried out by the state administration authority responsible for science and education.

PART FOUR

VOLUNTARY CYBER PROTECTION MECHANISMS

Implementation of self-assessments regarding cybersecurity and voluntary notification of incidents and cyber threats

Article 50

(1) Any entity not classified as an essential and important entity pursuant to this Act may:

– implement self-assessments regarding cybersecurity for any network and information system they use for their operations or for the provision of their services

– notify the competent CSIRT on a voluntary basis regarding any significant incident, other incidents, cyber threats or near misses, provided that they periodically implement self-assessments regarding cybersecurity referred to in subparagraph 1 of this paragraph.

(2) The possibility of implementing self-assessments regarding cybersecurity and of voluntary notification referred to in paragraph 1 of this Article shall be regulated by the regulation referred to in Article 24 of this Act.

National system for the detection of cyber threats and the protection of cyberspace

Article 51

(1) So as to increase the overall capabilities and resilience in the area of cybersecurity, the central government authority for cybersecurity shall continuously develop the national system for the detection of cyber threats and the protection of cyberspace (hereinafter: the national system).

(2) This national system may be voluntarily accessed by essential entities, important entities and other entities which have not been classified as essential or important pursuant to this Act, depending on the assessment of an entity's criticality conducted by the central government authority for cybersecurity.

(3) Accessing the national system may be conducted as a binding cyber protection measure for public sector entities if such a requirement has been set out in the regulation referred to in Article 24 of this Act.

(4) Accessing the national system shall be conducted based on an agreement concluded between the central government authority for cybersecurity and the entity accessing the system.

(5) Accessing the national system shall not have an impact on the obligations of any essential or important entities referred to in Article 25 of this Act, but rather functions as an additional cybersecurity measure.

Criteria for assessing an entity's criticality

Article 52

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

– the importance and significance of services provided by the entity or activities carried out by the entity in relation to other providers of identical or equivalent services or activities in the Republic of Croatia

– the importance of network and information systems used by the entity for providing services or carrying out activities, and their exposure to risks, dangers and threats in the cyberspace, and

– the condition of network and information systems used by the entity for providing services or carrying out activities, in relation to the design, management and maintenance of the entity's network and information systems, as well as the applicable relevant European and international standards and security practices.

(2) The entity criticality assessment referred to in Article 51, paragraph 2 of this Act shall be carried out pursuant to:

– a request by the entity for accessing the national system, or

– a proposal for accessing the national system submitted by a state administration authority or a regulatory body competent for the entity's sector.

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

(4) The process of submitting requests and proposals for accessing the national system, collecting data necessary to carry out a criticality assessment of an entity in order to grant access to the system, and access of entities to the national system shall be regulated by the regulation referred to in Article 24 of this Act.

Voluntary cybersecurity information-sharing

Article 53

(1) Essential entities, important entities and other entities not classified as essential or important pursuant to this Act may share information regarding cybersecurity on a voluntary basis in order to increase the level of cybersecurity or incident handling.

(2) Information sharing referred to in paragraph 1 of this Article may include information regarding cyber threats, including information regarding the source of the threat, near misses, vulnerabilities, tactics, techniques and procedures, vulnerability indicators, tactics, techniques and procedures used by cyber attackers, indicators of compromise, cybersecurity alerts and recommendations regarding configuration of cybersecurity tools to detect cyberattacks.

(3) Information sharing referred to in paragraph 2 of this Article shall take place between the entities referred to in paragraph 1 of this Article and, if appropriate, their suppliers and service providers, using information-sharing arrangements established for this purpose.

(4) The arrangements referred to in paragraph 3 of this Article shall be established based on an agreement on voluntary cybersecurity information sharing.

(5) The agreement referred to in paragraph 4 of this Article shall set out the requirements for accessing the arrangement established by the agreement, the contents of information being shared, the possibility of using dedicated platforms and other tools for automated information sharing, as well as any other operational elements essential for effective and secure information sharing.

(6) Essential and important entities shall notify the competent authority for implementing cybersecurity requirements of their participation in voluntary cybersecurity information-sharing arrangements referred to in paragraph 3 of this Article, and public sector entities classified as essential entities shall also, prior to participating, request an opinion from the central government authority for cybersecurity on such participation and the extent of information which may be shared with other participating stakeholders.

Coordinated vulnerability disclosure

Article 54

(1) Any natural and legal person may anonymously report a vulnerability.

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

(3) The CSIRT vulnerability disclosure coordinator shall act as a trusted intermediary, facilitating, where necessary, the interaction between the natural or legal person reporting a vulnerability and the manufacturer or provider of the potentially vulnerable ICT products or ICT services, upon the request of either party.

(4) The tasks of the CSIRT vulnerability disclosure coordinator include identifying and contacting the entities concerned, assisting the natural or legal persons reporting a vulnerability, and negotiating disclosure timelines for coordinated disclosure and managing vulnerabilities that affect multiple entities.

(5) The CSIRT vulnerability disclosure coordinator shall ensure that follow-up action is carried out with regard to the reported vulnerability and shall ensure the anonymity of the natural or legal person reporting the vulnerability.

(6) The CSIRT vulnerability disclosure coordinator shall, when sharing information about the reported vulnerability, ensure the anonymity of the person reporting the vulnerability by applying the technique for the removal of direct identifiers, the generalisation techniques, the data randomisation techniques, as well as any other known techniques.

(7) Where there is a need to store data regarding the person reporting the vulnerability so as to carry out activities referred to in paragraph 4 of this Article, the CSIRT vulnerability disclosure coordinator shall keep records of such stored data.

(8) The CSIRT vulnerability disclosure coordinator shall keep the data and records referred to in paragraph 7 of this Article for no more than three years from the reporting of the vulnerability, and upon the expiry of this period they shall erase the data regarding the

person reporting the vulnerability and destroy any records referred to in paragraph 7 of this Article in accordance with personal data protection regulations.

(9) The CSIRT vulnerability disclosure coordinator shall deliver any information regarding newly disclosed vulnerabilities to the competent CSIRTs referred to in this Act, together with instructions regarding further reporting of the vulnerabilities of entities within their jurisdiction.

(10) The competent CSIRTs shall draw up guidelines for users of vulnerable ICT products or ICT services regarding ways to mitigate risks resulting from disclosed vulnerabilities and deliver reports on best practices to entities within their jurisdiction pursuant to this Act.

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

(12) The tasks of the CSIRT vulnerability disclosure coordinator shall be carried out by the CSIRT at the central government authority for cybersecurity.

PART FIVE

STRATEGIC PLANNING AND MANAGING CYBERSECURITY

The national strategic planning act in the area of cybersecurity

Article 55

(1) At the proposal of the central government authority for cybersecurity, the Government shall adopt a medium-term strategic planning act in the area of cybersecurity.

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

– specific objectives and priorities in the area of cybersecurity development, including at least the public policies set out in Annex IV to this Act, and

– a framework for monitoring and evaluating the implementation of the objectives and priorities referred to in subparagraph 1 of this paragraph.

(3) With a view to elaborate measures for implementing the specific objectives and priorities set out in the strategic planning act referred to in paragraph 1 of this Article, an action plan shall be drawn up for its implementation.

(4) Reporting, monitoring and evaluation activities related to the strategic planning act referred to in paragraph 1 of this Article shall be carried out in accordance with the regulation governing strategic planning and managing of the development of the Republic of Croatia.

(5) The central government 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 from the date of its adoption, i.e. within three months from the date of the adoption of its modifications and/or amendments.

Managing large-scale cybersecurity incidents and crises

Article 56

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

(2) At the proposal of the authority responsible for cyber crisis management, the Government shall adopt the national cyber crisis management programme.

(3) The national programme referred to in paragraph 2 of this Article shall set out the capacities, resources and processes for cyber crisis management and more closely identify:

– the objectives of cyber crisis management, including objectives related to developing national preparedness measures, as well as compliance with the framework for cyber crisis management of the European Union

– coherence with the general national crisis management framework

– measures and activities for strengthening national preparedness

– the plan for implementing national preparedness measures, including the plan for training activities and the implementation of exercises which form part of the plan referred to in Article 58 of this Act

– tasks and responsibilities of authorities involved in cyber crisis management

– the role of the public and private sector and the infrastructure essential for cyber crisis management, and

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

(4) Also forming part of the national programme referred to in paragraph 2 of this Article are the standard operating procedures which more closely identify:

– cyber crisis management procedures, including their integration into the general national crisis management framework, and

– all issues essential for information sharing.

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

Assessing the state of cybersecurity

Article 57

(1) With the aim of exchanging the acquired know-how and experience, strengthening trust, capacities and capabilities in the area of cybersecurity, and improving the policies in the area of cybersecurity, self-assessment procedures related to the state of cybersecurity shall be organised and implemented.

(2) The self-assessments related to the state of cybersecurity shall also be organised and implemented on a national level (hereinafter: national self-assessments), independent of the self-assessments implemented by Member States within the frameworks of peer reviews implemented in accordance with the methodology set out by the Cooperation Group, the European Commission and ENISA.

(3) The aspects assessed as part of the national self-assessments shall be the level of implementation of the cybersecurity requirements set out in this Act, the level of cyber capabilities, including the available financial, technical and human resources, the effectiveness of exercise of the tasks and the level of implementing the cooperation of competent authorities for implementing cybersecurity requirements, the competent CSIRTs, the competent authorities for implementing special laws and the competent authorities from the act governing the area of critical infrastructure, the level of implementing cybersecurity information-sharing arrangements referred to in Article 53 of this Act, and the specific issues of cross-sector nature.

(4) The national self-assessments are duly subject to the methodology for conducting self-assessments of Member States which shall be adopted by the Cooperation Group, the European Commission and ENISA.

(5) The plans and programmes for implementing self-assessments by Member States within the framework of peer reviews referred to in paragraph 2 of this Article and national self-assessments shall be adopted by the Government at the proposal of the central government authority for cybersecurity.

(6) Before the start of the peer reviews referred to in paragraph 2 of this Article, the central government authority for cybersecurity shall consider the existence of the risk of any conflict of interest concerning the cybersecurity experts designated for their implementation, and notify the remaining Member States, the Cooperation Group, the European Commission and ENISA of any identified risks.

(7) Where there are duly substantiated grounds for objecting to the designation of a particular cybersecurity expert for implementing the peer reviews referred to in paragraph 2 of this Article, the central government authority for cybersecurity shall notify the designating Member State thereof.

Cybersecurity exercises

Article 58

(1) In order to achieve the maximum level of preparedness, especially in the event of a cyber crisis, so as to examine the available capacities and capabilities in the area of cybersecurity, test the established communication mechanisms, and exchange the acquired know-how, experience and best practices, as well as to increase trust, cybersecurity exercises shall be carried out.

(2) These cybersecurity exercises shall be organised and carried out pursuant to the Cybersecurity Exercise Implementation Plan adopted by the Government at the proposal of the central government authority for cybersecurity, for a period of two years.

(3) The Cybersecurity Exercise Implementation Plan shall include:

(a)international cybersecurity exercises – exercises carried out in the Republic of Croatia with the participation of experts from other Member States or other countries and international organisations, as well as exercises carried out abroad with the participation of representatives of competent authorities from the Republic of Croatia

(b) national cybersecurity exercises – exercises planned, organised and carried out by the competent authorities referred to in this Act, including the competent CSIRTs.

(4) The Cybersecurity Exercise Implementation Plan shall set out the quantity of planned exercises, the persons competent for carrying out the exercises, the title and objective of exercises, the time and location of the exercises, the approximate number of participants in the exercises, the entity responsible for the financial obligations related to the implementation of exercises, and the contents, deadlines and manner of reporting on the exercises carried out.

(5) The proposals for the plans for carrying out cybersecurity exercises shall be drawn up by the central government authority for cybersecurity in cooperation with other competent authorities for implementing cybersecurity requirements, competent CSIRTs, and competent authorities for implementing special laws.

PART SIX

COMPETENT AUTHORITIES IN THE AREA OF CYBERSECURITY

CHAPTER I

COMPETENT AUTHORITIES FOR IMPLEMENTING CYBERSECURITY REQUIREMENTS

Tasks of the competent authorities for implementing cybersecurity requirements

Article 59

(1) The competent authorities for implementing cybersecurity requirements shall carry out the following activities:

– classify entities in accordance with this Act, identify and maintain lists of essential and important entities

– carry out expert supervision of essential and important entities as regards the implementation of cybersecurity requirements in accordance with this Act and the regulation referred to in Article 24 of this Act

– when classifying entities, handling significant incidents and carrying out expert supervision, closely cooperate and coordinate their activities with state administration authorities competent for the relevant sector in which the entities within their jurisdiction are active

– closely cooperate and exchange relevant information with personal data protection authorities when handling incidents resulting in personal data breaches, as well as with law enforcement authorities when these incidents are the result of criminal activities

– cooperate with one another and exchange relevant information and experience related to the implementation of this Act

– cooperate and exchange relevant information with the national coordination centre nominated 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 competent CSIRTs, and

– carry out other activities set out in this Act as activities carried out by the competent authorities for implementing cybersecurity requirements.

(2) The competent authorities for implementing cybersecurity requirements shall carry out the activities referred to in paragraph 1 of this Article in accordance with the division of jurisdiction from Annex III to this Act.

(3) Where a certain entity is under the jurisdiction of two or more authorities from Annex III to this Act, so as to avoid duplication and overlap in carrying out activities, the central government authority for cybersecurity shall, in cooperation with all authorities responsible for the said entity, draw up a protocol regarding the actions of the competent authorities, primarily having in mind the entity's principal activities.

(4) The central government authority for cybersecurity shall initiate the process of drawing up the protocol referred to in paragraph 3 of this Article *ex officio*, at the proposal of one of the competent authorities from Annex III to this Act, or at the entity's proposal.

Application of cybersecurity requirements to competent authorities for implementing cybersecurity requirements

Article 60

(1) The competent authorities for implementing cybersecurity requirements which have not been classified as essential or important entities pursuant to this Act shall:

– implement the cybersecurity requirements stipulated in Article 25 of this Act in accordance with the provisions of the regulation referred to in Article 24 of this Act pertaining to essential entities, and

– conduct, at least once every two years, a self-assessment of cybersecurity for the network and information systems they use in their business, and notify the central government authority for cybersecurity of the conducted self-assessments of cybersecurity.

(2) Within the meaning of paragraph 1, subparagraph 1 of this Article, the tasks of CSIRT shall be carried out by the central government authority for cybersecurity.

Tasks of the central government authority for cybersecurity

Article 61

(1) Alongside the tasks stipulated in Article 59 of this Act, the central government authority for cybersecurity shall also carry out the following tasks:

– coordinate the drawing up and adoption of the strategic planning act in the area of cybersecurity

– direct and monitor the implementation of the strategic planning act in the area of cybersecurity

– improve the cybersecurity risk-management measures by planning the development of a regulatory framework for cybersecurity

– monitor the implementation of this Act and provide recommendations, opinions, guidelines and instructions related to the implementation of cybersecurity requirements

– encourage the establishment of voluntary cybersecurity information-sharing arrangements as set out in Article 53 of this Act, and provide recommendations, guidelines and instructions for facilitating their establishment

– as the body responsible for managing cyber crises, coordinate activities related to cyber crisis management on the national level

– participate in the activities of EU-CyCLONe and coordinate activities related to cyber crisis management at the European Union level on behalf of the Republic of Croatia

– operate as a single point of contact

– operate as a CSIRT authority in accordance with the division of jurisdiction from Annex III to this Act

– carry out activities related to identifying cyber threats and protecting the national cyberspace

– draft reports regarding the state of cybersecurity

– cooperate with other competent authorities referred to in this Act

– pursue international cooperation in the area of cybersecurity within the framework of its competences set out in this Act

– carry out other activities set out in this Act as activities to be carried out by the central government authority for cybersecurity.

(2) The central government authority for cybersecurity shall be the Security and Intelligence Agency.

Tasks of a single point of contact

Article 62

A single point of contact shall:

– notify 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 of their tasks and any subsequent changes to the submitted information

– notify the European Commission without delay of the provisions of this Act regulating the imposing of administrative fines, as well as any subsequent changes to the submitted information

– participate in the activities of the Cooperation Group

– ensure cross-border cooperation of competent authorities for implementing cybersecurity requirements, competent authorities for implementing special laws and the competent CSIRTs with the relevant authorities in other Member States and, as necessary, with the European Commission and ENISA

– ensure cross-sectoral cooperation of competent authorities for implementing cybersecurity requirements, competent authorities for implementing special laws and the competent CSIRTs with other relevant authorities on the national level

– draw up guidelines regarding the contents of notifications, as well as the manners of and deadlines for notifying the single point of contact of any notified significant incidents, other incidents, cyber threats and near misses, and

– carry out other activities set out in this Act as activities to be carried out by the single point of contact.

National Cybersecurity Centre

Article 63

The National Cybersecurity Centre shall be established at the Security and Intelligence Agency for the purpose of carrying out tasks referred to in Articles 59, 61 and 62 of this Act.

CHAPTER II

COOPERATION OF COMPETENT AUTHORITIES ON THE NATIONAL LEVEL

Cooperation with competent authorities for implementing special laws

Article 64

(1) The central government authority for cybersecurity and other competent authorities for implementing cybersecurity requirements and competent authorities for implementing special laws shall cooperate with each other and share relevant information and experiences.

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

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

(4) The central government authority for cybersecurity shall notify the Oversight Forum established in accordance with Article 32, paragraph 1 of Regulation (EU) 2022/2554 regarding the oversight activities conducted based on this Act for all essential and important entities which have been designated as critical ICT third-party service providers pursuant to Article 31 of Regulation (EU) 2022/2554.

Cooperation with competent authorities from the act regulating the area of critical infrastructure

Article 65

(1) The competent authorities for implementing cybersecurity requirements and the competent authorities from the act regulating the area of critical infrastructure shall cooperate and exchange relevant information, notably those regarding:

– identifying entities as critical entities pursuant to the act regulating the area of critical infrastructure

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

– cybersecurity requirements and physical protective measures implemented by these entities, and

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

(2) The competent authorities from the act regulating the area of critical infrastructure may request the competent authorities for implementing cybersecurity requirements and the competent authorities for implementing special laws to exercise their supervisory powers over entities identified as critical entities.

(3) The exchange of information regarding critical entities shall take place within the framework established by an agreement between the central government authority for cybersecurity and the competent coordinating authority of the state administration from the act regulating the area of critical infrastructure.

(4) The agreement referred to in paragraph 3 of this Article shall regulate all essential issues related to the exchange of information and coordination of competent authorities, including the manner of exchanging information from paragraph 1 of this Article, as well as the information on conducted supervision of critical entities.

CHAPTER III

CSIRT JURISDICTION

CSIRT tasks

Article 66

(1) The CSIRTs shall have the following tasks:

– monitor and analyse cyber threats, vulnerabilities and incidents and, upon their request, provide assistance to essential and important entities regarding real-time or near real-time monitoring of their network and information systems

– provide early warnings and announcements, disseminate information to essential and important entities, as well as to other competent authorities from this Act or other relevant stakeholders on cyber threats, vulnerabilities and incidents, if possible, in near real-time

– process received incident notifications and, if circumstances allow, after receiving an incident notification, deliver to essential and important entities relevant information regarding follow-up actions, especially information which could contribute to a more effective handling of an incident

– respond to incidents and provide assistance to essential and important entities, upon their request or with their consent

– provide, at the request of essential or important entities, a proactive scanning of the network and information systems of the entity concerned to detect vulnerabilities with a potential significant impact

– collect and analyse computer forensic data and provide dynamic risk and incident analysis in sectors within their jurisdiction, and draw up a situational awareness overview regarding cybersecurity within that sector

– adopt guidelines for standardising and improving the state of implementation of the notification obligations from Articles 37 and 38 of this Act, as well as of implementation of the voluntary notification from Article 39 of this Act

– identify, in cooperation with the competent authority for implementing cybersecurity requirements, the cross-border and cross-sectoral impacts of significant incidents

– cooperate with other CSIRTs on the national and international level

– participate in the CSIRTs network

– provide mutual assistance in accordance with their capacities and competencies to other members of the CSIRTs network upon their request

– cooperate and, where appropriate, share relevant information with sectoral or cross-sectoral communities of essential and important entities established based on an agreement on voluntary cybersecurity information sharing from Article 53 of this Act

– cooperate with relevant private-sector stakeholders and, so as to establish this cooperation, promote the adoption and use of common or standardised practices, classification schemes and taxonomies in relation to incident handling, managing cyber crises and coordinated vulnerability disclosure in accordance with Article 54 of this Act

– contribute to the deployment and use of secure information-sharing tools

– participate in the implementation of peer reviews in accordance with the methodology set out by the Cooperation Group, the European Commission and ENISA

– participate in the implementation of self-assessments related to the state of cybersecurity carried out on the national level, and

– carry out other tasks set out in this Act as activities to be carried out by the competent CSIRT.

(2) When carrying out the tasks from paragraph 1 of this Article, CSIRTs shall prioritise tasks which were deemed to be of prime concern according to the risk assessment, and when processing the received notifications, pursuant to this Act, they shall prioritise processing notifications regarding significant incidents.

(3) Where the cooperation from paragraph 1, subparagraph 9 of this Article involves the participation of the CSIRT in international cooperation networks and/or its participation in third-country CSIRTs, the CSIRT shall apply the relevant information-sharing protocols.

Proactive non-intrusive scanning of publicly available network and information systems

Article 67

(1) So as to detect vulnerable or insecurely configured network and information systems, the CSIRT may carry out a proactive non-intrusive scanning of publicly available network and information systems of essential and important entities in its jurisdiction.

(2) The scanning referred to in paragraph 1 of this Article shall not have any negative impact on the functioning of the services provided and activities carried out by the essential and important entity.

(3) The competent CSIRT shall notify the essential and important entity of any vulnerabilities or insecurely configured network and information systems detected during the scanning referred to in paragraph 1 of this Article.

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

Article 68

(1) Essential and important entities shall cooperate with the competent CSIRT and share with it the necessary information during an incident handling procedure.

(2) During the course of its activities, the CSIRT may not be held liable for any damage caused by the incident to the network and information systems of essential and important entities.

Securing conditions for carrying out the tasks of a competent CSIRT

Article 69

The competent CSIRT shall:

– ensure a high level of availability of their communication services by avoiding single points of failure, and have means for being contacted and for contacting others, with clearly specified and known communication channels for their constituency and cooperative partners

– ensure confidentiality and trustworthiness of their operations

– ensure that their premises and the supporting information systems are located at secure sites

– ensure that they are equipped with an appropriate system for managing requests for incident handling

– ensure an adequate number of trained staff, as well as the appropriate redundant systems and relevant working spaces, so as to ensure continuity of carrying out CSIRT tasks and the development of technical capabilities necessary to carry out CSIRT tasks

– have at its disposal a secure and resilient communication and information infrastructure through which to exchange information with essential and important entities and other relevant stakeholders from this Act, and

– ensure other resources which are necessary to efficiently carry out the tasks of a CSIRT.

Determining the CSIRT jurisdiction

Article 70

(1) The central government authority for cybersecurity, through the National Cybersecurity Centre and CARNET, and the National CERT, shall carry out the CSIRT tasks on the national level, in accordance with the division of jurisdiction from Annex III to this Act.

(2) Within the meaning of Article 50, paragraph 1, subparagraph 2 of this Act, the central government authority for cybersecurity shall carry out the CSIRT tasks for state authorities, legal persons with public authority, as well as local and regional self-government units, while CARNET shall carry out the CSIRT tasks for public and private entities, including the general population.

Public interest tasks

Article 71

The tasks which are, pursuant to this Act, entrusted to the central government authority for cybersecurity, the competent authorities for implementing cybersecurity requirements and the competent CSIRTs, including tasks related to cooperation, providing

assistance and information sharing, at the national and international level, shall be required for ensuring an effective implementation of procedures and measures for achieving a high level of cybersecurity in sectors of particular importance for the smooth performance of critical societal and economic activities, and the proper functioning of the internal market, and these tasks are deemed to be of public interest.

PART SEVEN

PERSONAL DATA PROTECTION AND PROCESSING, AND ACCESS TO INFORMATION

Personal data protection and processing

Article 72

The processing of personal data by the competent authorities for implementing cybersecurity requirements and the competent CSIRTs during the course of their tasks set out in this Act shall be subject to Regulation (EU) 2016/679.

Restrictions regarding using of and right of access to information

Article 73

(1) Lists of essential and important entities, as well as any other records created during the implementation of this Act shall be used and exchanged solely for the purpose of fulfilling the requirements set out in this Act, all the while respecting the need to restrict access to these records, under the conditions stipulated in the act governing protection of natural persons with regard to the processing and exchange of personal data for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties.

(2) The lists and other records referred to in paragraph 1 of this Article shall represent information subject to the possibility of restricting access to holders of the right of access and reuse of information, depending on the results of the proportionality and public interest test conducted in accordance with the provisions of the act governing right of access to information.

Reporting obligation regarding infringements including personal data breaches

Article 74

(1) Should the competent authority for implementing cybersecurity requirements, in the course of carrying out expert supervision of the implementation of cybersecurity requirements or any other activities referred to in this Act, become aware of an infringement of any of the requirements from Article 25 of this Act, including personal data breaches, committed by an essential or important entity, it shall notify, without undue delay, the authority competent for personal data protection regarding this infringement and the facts of the case.

(2) If the authority competent for personal data protection which is being notified of the infringement referred to in paragraph 1 of this Article was established in a different Member State, the competent authority for implementing cybersecurity requirements shall also notify the Croatian Personal Data Protection Agency of this infringement.

PART EIGHT

EXPERT SUPERVISION OF THE IMPLEMENTATION OF CYBERSECURITY REQUIREMENTS

CHAPTER I

IMPLEMENTATION OF EXPERT SUPERVISION

Implementation of expert supervision of essential entities

Article 75

(1) The expert supervision of the implementation of cybersecurity requirements (hereinafter: expert supervision) of an essential entity shall be conducted at least once every three to five years.

(2) The expert supervision of an essential entity shall also be conducted prior to the expiry of the deadlines referred to in paragraph 1 of this Article should the competent authority for implementing cybersecurity requirements come into possession of information warning it that the entity is not implementing cybersecurity risk-management measures in accordance with their obligations, or that it is not fulfilling requirements related to notifications regarding cyber threats and incidents in the stipulated manner or within the stipulated or set deadlines, or that it is not fulfilling the requests of the competent authorities referred to in this Act.

(3) The implementation plan for expert supervision from paragraph 1 of this Article shall be set out in the annual work plan of the competent authority for implementing cybersecurity requirements.

(4) In order to set out the implementation plans for expert supervision from paragraph 1 of this Article, as well as to set priorities for conducting the supervisions, the competent authority for implementing cybersecurity requirements may classify essential entities based on their risk category.

Implementation of expert supervision of important entities

Article 76

(1) The expert supervision of an important entity shall be conducted when the competent authority for implementing cybersecurity requirements comes into possession of information warning it that the entity is not implementing cybersecurity risk-management measures in accordance with their obligations, or that it is not fulfilling requirements related to notifications regarding cyber threats and incidents in the stipulated manner and within the stipulated or set deadlines, or that it is not fulfilling the requests of the competent authorities referred to in this Act.

(2) In order to set out the implementation plans for expert supervision from paragraph 1 of this Article, as well as to set priorities for conducting the supervisions, the competent authority for implementing cybersecurity requirements may classify important entities based on their risk category.

Manner of conducting expert supervision and notification of conducting supervision

Article 77

(1) The competent authorities for implementing cybersecurity requirements shall conduct expert supervision:

– by an immediate inspection carried out at the supervised entity regarding the data, documents, conditions and ways of implementing cybersecurity risk-management measures, fulfilling requirements related to notifications regarding cyber threats and incidents, as well as fulfilling requests of the competent authorities referred to in this Act, or

– by consulting reports regarding the conducted cybersecurity audits, as well as other additionally requested and submitted data and documents of the supervised entity, if necessary.

(2) The competent authority for implementing cybersecurity requirements shall notify the supervised entity 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, where expert supervision is to be conducted pursuant to Article 75, paragraph 2 and Article 76, paragraph 1 of this Act, the expert supervision from paragraph 1, subparagraph 1 of this Act may be conducted without prior notice:

– should there be any reasons that point to the need to take immediate action by the entity regarding a significant incident, or

– so as to prevent or mitigate risks resulting from a significant cyber threat.

(4) The competent authority for implementing cybersecurity requirements shall, in the course of conducting expert supervision from paragraph 1, subparagraph 1 of this Article, take account of the impact that the supervision has on the activities and operations of the supervised entity and ensure that the supervision does not lead to disruption of the activities and operations of the supervised entity, unless there is no other way to conduct the expert supervision.

Obligations of essential and important entities related to expert supervision

Article 78

Essential and important entities shall enable the implementation of expert supervision and ensure all the conditions required for an undisturbed expert supervision, particularly the following:

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

– enabling inspection and use of all necessary data and documents, including making copies

– enabling interviews with responsible and accountable persons of the supervised entity.

CHAPTER II

AUTHORISATIONS OF COMPETENT AUTHORITIES FOR IMPLEMENTING CYBERSECURITY REQUIREMENTS WHEN CONDUCTING EXPERT SUPERVISION

General supervisory measures for essential and important entities

Article 79

(1) When conducting expert supervision, the competent authority for implementing cybersecurity requirements shall be authorised to:

– carry out immediate inspection of data and documents, as well as network and information systems

– carry out immediate checks of conditions and ways of implementing cybersecurity risk-management measures, including random checks

– carry out immediate inspection of documents related to fulfilling the obligations of notifying on cyber threats and incidents, as well as other actions taken at the request of the competent authorities referred to in this Act

– request data and documents necessary for assessing the proportionality of cybersecurity risk-management measures applied by the entity

– request reports regarding the cybersecurity audits conducted by a cybersecurity auditor referred to in Article 32 of this Act, as well as any other relevant evidence regarding the implementation of cybersecurity policies from Article 30 of this Act

– request any other data, documents and information necessary for conducting the supervision

– request that a targeted cybersecurity audit be conducted.

(2) When implementing the supervisory measures from paragraph 1, subparagraphs 4 to 6 of this Article, the competent authority for implementing cybersecurity requirements shall stipulate their purpose and specify the data, documents and other information requested from the entity.

(3) When the supervisory measure from paragraph 1, subparagraph 7 of this Article is being applied, the competent authority for implementing cybersecurity requirements shall carry out an additional cybersecurity scan based on objective, non-discriminatory, fair and transparent risk assessment criteria, where necessary with the cooperation of the entity concerned, so as to provide recommendations for improving the situation or reducing 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 based on the available data regarding the assessment of risks to which the 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 the targeted cybersecurity audit may be borne by the competent authority for implementing cybersecurity requirements if the audit is conducted as part of immediate measures taken so as to avoid or prevent significant incidents or mitigate the consequences of significant incidents or other risks to which the supervised entity is exposed and which have or may have a cross-border or cross-sectoral impact.

Specific supervisory measures for essential entities

Article 81

(1) Apart from the supervisory measures from Article 79 of this Act, when conducting expert supervision of an essential entity, the competent authority for implementing cybersecurity requirements shall be authorised to request the implementation of:

– regular cybersecurity audits, when it is in possession of information showing that the concerned entity has not conducted a cybersecurity audit within the deadlines referred to in Article 34, paragraph 1 of this Act, and

– extraordinary cybersecurity audits, in the event of a significant incident, or where it determines that the previously conducted cybersecurity audit identified irregularities, shortcomings or failures in implementing cybersecurity risk-management measures which have

not been resolved in the meantime, or when it is in possession of information showing that the entity is not implementing cybersecurity risk-management measures in accordance with this Act and the regulation from Article 24 of this Act.

(2) Costs related to cybersecurity audits conducted in accordance with paragraph 1 of this Article shall be subject to the provisions of Article 34, paragraph 7 of this Act.

(3) Where a specific supervisory measure from paragraph 1, subparagraph 2 of this Article is being applied in the event of a significant incident, the competent authority for implementing cybersecurity requirements shall carry out an additional cybersecurity scan from Article 79, paragraph 3 of this Act.

CHAPTER III

CORRECTIVE MEASURES, TEMPORARY SUSPENSIONS, AND PROHIBITION OF EXERCISING FUNCTIONS

Corrective measures for essential and important entities

Article 82

(1) Depending on the results of the conducted expert supervision, the competent authority for implementing cybersecurity requirements may impose the following corrective measures to essential and important entities:

– issue warnings about infringements of this Act and the regulation referred to in Article 24 of this Act

– issue binding instructions or orders requiring them to remedy the identified deficiencies or the infringements of this Act or the regulation from Article 24 of this Act, including measures that the entity needs to take so as to prevent significant incidents or remedy their consequences

– order them to cease conduct that infringes this Act and the regulation from Article 24 of this Act and to desist from repeating that conduct

– order them to ensure that their cybersecurity risk-management measures comply with the stipulated obligations or to fulfil the reporting obligations regarding cyber threats and incidents in the stipulated manner and within the stipulated or set deadline, i.e. to fulfil the requests of the competent authorities referred to in this Act in the specified manner and/or within the set deadline

– order them to implement the recommendations provided as a result of the conducted cybersecurity audit or as part of the security scans within a reasonable deadline, and

– order the entities concerned to make public the aspects of the infringements of this Act and the regulation from Article 24 of this Act in the specified manner.

(2) The instructions and orders referred to in paragraph 1 of this Article shall contain the deadline for implementing corrective measures and the deadline for reporting on the implementation of the imposed corrective measures.

(3) If a certain essential or important entity fails to comply with the imposed corrective measures from paragraph 1, subparagraphs 1 to 5 of this Article, the competent authority for implementing cybersecurity requirements shall grant this entity an appropriate extension of the deadline for implementing the corrective measures.

(4) By way of derogation from paragraph 3 of this Article, in exceptional cases, the supervised entity shall not be granted this appropriate extension of the deadline for implementing the corrective measures if this would prevent the implementation of immediate measures imposed so as to prevent significant incidents or respond to such incidents.

Specific corrective measure for essential entities

Article 83

(1) Apart from the corrective measures from Article 82 of this Act, the competent authority for implementing cybersecurity requirements may designate an officer for monitoring the compliance of the essential entity with the cybersecurity requirements for a specific period of time.

(2) The decision regarding the designation referred to in paragraph 1 of this Article shall stipulate the period for which the officer for monitoring the compliance of the essential entity with the cybersecurity requirements is designated and their tasks.

Temporary suspensions and prohibition of exercising functions

Article 84

(1) If an essential entity fails to comply with the imposed corrective measures from Article 82 of this Act, the competent authority for implementing cybersecurity requirements may:

– request the competent authority to temporarily suspend the authorisation issued to the entity for providing services or carrying out activities from Annex I or Annex II to this Act

– request the competent authority to temporarily prohibit any natural person from Article 29 of this Act from exercising managerial functions in the essential entity concerned.

(2) The measures from paragraph 1 of this Article shall be applied only until the essential entity concerned complies with the imposed corrective measures from Article 82 of this Act.

(3) The measures from paragraph 1 of this Article shall not apply to state administration authorities, other state authorities, local and regional self-government units or public entities who, in the capacity of a public law body, represent a contracting authority in accordance with the regulation governing public procurement.

Circumstances taken into account when adopting decisions on imposing corrective measures, recommending temporary suspensions and prohibition of exercising functions

Article 85

(1) When adopting decisions on imposing corrective measures from Articles 82 and 83 of this Act and submitting requests in accordance with Article 84 of this Act, the competent authority for implementing cybersecurity requirements shall take into account:

– the seriousness of the infringement and the importance of the provisions breached by the supervised entity

– the duration of the infringement

– any relevant previous infringement by the entity concerned

– any damage caused, including any financial or economic loss, effects on other services or activities and the number of users affected

– any intent or negligence on the part of the supervised entity

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

– any adherence to relevant codes of conduct or rules and requirements for certifications related to providing services or carrying out activities, and

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

(2) The following shall constitute serious infringements referred to in paragraph 1, subparagraph 1 of this Article:

– repeated violations

– a failure to notify or remedy significant incidents

– a failure to remedy irregularities and deficiencies following instructions or orders issued by the competent authority for implementing cybersecurity requirements

– the obstruction or hindering of the cybersecurity audit procedure requested by the competent authority for implementing cybersecurity requirements or of the monitoring activities ordered pursuant to Article 83 of this Act, and

– providing false or grossly inaccurate information in relation to the implementation of cybersecurity requirements or other obligations of the supervised entity laid down in this Act or in the regulation from Article 24 of this Act.

Imposing administrative fines

Article 86

(1) Alongside the corrective measures laid out in this Act and the submitting of requests in accordance with Article 84 of this Act, the competent authority for implementing cybersecurity requirements may also report the liable essential and important entities to the authorised prosecutor or issue an infringement notice in accordance with the infringement provisions of this Act.

(2) By way of derogation from paragraph 1 of this Article, no reports can be made to the authorised prosecutor nor can an infringement notice be issued in accordance with the infringement provisions of this Act during expert supervision if the supervised entity has been imposed an administrative fine pursuant to Regulation (EU) 2016/679 by the authority competent for personal data protection for personal data breaches arising from the same activities of the entity.

CHAPTER IV

REPORT ON THE CONDUCTED EXPERT SUPERVISION

Contents of the report

Article 87

(1) Following the expert supervision, the competent authority for implementing cybersecurity requirements shall draw up a report on the conducted supervision (hereinafter: report).

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

(3) The report shall contain the indication of the subject of the expert supervision, the identified facts, and the instructions regarding the right to submit comments to the report.

(4) If the conducted expert supervision identified infringements of stipulated obligations or a failure to comply with cybersecurity requirements, the report shall contain descriptions of the identified infringements and non-compliances, the imposed supervisory measures and the notification obligation regarding the implemented corrective measures.

Comments to the report

Article 88

(1) The responsible person may submit comments to the report, in writing and within the deadline set by the competent authority for implementing cybersecurity requirements for submitting comments.

(2) When setting out deadlines for submitting comments, account shall be taken of the size of the entity, scope of the performed expert supervision and facts identified therein, the applied supervisory measures, and the 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 comments to the report if this would prevent the implementation of immediate measures imposed so as to prevent significant incidents or respond to such incidents.

Processing comments to the report

Article 89

(1) Should the competent authority for implementing cybersecurity requirements determine that the comments to the report are completely or partially justified, it shall draw up a supplementary report to address the comments.

(2) Should the competent authority for implementing cybersecurity requirements determine that the comments to the report are completely unjustified, it shall deliver a written notification thereof to the supervised entity.

(3) The supplementary report from paragraph 1 or the notification from paragraph 2 of this Article shall be delivered to the responsible person no later than 30 days after receiving the comments.

(4) No comments shall be allowed regarding the supplementary report and the notification from paragraph 3 of this Article.

Judicial remedy

Article 90

After the delivery of the supplementary report or notification from Article 89 of this Act, the responsible person of the supervised entity may bring a claim before the competent administrative court in order to request an assessment of the lawfulness of the actions taken by the competent authority for implementing cybersecurity requirements as regards the subject of the expert supervision and the report on the performed expert supervision.

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

Article 91

(1) If the expert supervision of a state administration authority, another state authority or a local and regional self-government unit identified deficiencies or infringements of this Act and the regulation from Article 24 of this Act, and the supervised authority fails to implement the imposed corrective measure within the set deadline, the central government authority for information security shall deliver to the central government authority for cybersecurity a report on the results of the expert supervision of that authority.

(2) The central government authority for cybersecurity shall issue binding instructions on the implementation of measures, which the head of the supervised authority shall ensure, including a deadline for implementing such measures, and it shall notify the Government thereof.

Logbooks of performed expert supervisions

Article 92

(1) The competent authorities for implementing cybersecurity requirements shall keep logbooks of the performed expert supervisions.

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

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

Article 93

The tasks included in expert supervision of the implementation of provisions of this Act and the regulation from Article 24 of this Act related to expert supervision of providers of public electronic communications networks and providers of publicly available electronic communications services shall be carried out by electronic communications inspectors in accordance with this Act and the act governing the area of electronic communications.

CHAPTER V

MUTUAL ASSISTANCE IN PERFORMING EXPERT SUPERVISION WITH COMPETENT AUTHORITIES FROM OTHER MEMBER STATES

Performing supervision which includes cross-border elements

Article 94

Where an essential or important entity provides services in more than one Member State, or provides services in one or more Member States and its network and information systems are located in one or more other Member States, the competent authority for implementing cybersecurity requirements may perform expert supervision with the mutual assistance of and in cooperation with the competent authorities of the Member States concerned.

Frameworks for providing mutual assistance

Article 95

(1) The mutual assistance from Article 94 of this Act shall entail:

– notification, via the single point of contact, regarding the supervisory measures taken and corrective measures imposed, as well as advisory activities

– submission of a request to take supervisory measures or impose corrective measures, and

– after receiving a substantiated request, provision of assistance proportionate to own resources so that the supervisory measures or imposed corrective measures can be implemented in an effective, efficient and consistent manner.

(2) The mutual assistance referred to in paragraph 1, subparagraph 3 of this Article may cover acting upon requests for delivery of relevant information and taking supervisory measures or imposing corrective measures, including requests for performing expert supervisions or targeted cybersecurity audits.

(3) The competent authority for implementing cybersecurity requirements who has received a request for mutual assistance in performing expert supervision shall not be allowed to refuse such a request, unless it determines that:

– it does not have the competence to provide the requested assistance

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

– the request concerns information or entails activities which, if disclosed or carried out, would be contrary to the interests of national security, public security or defence.

(4) Before refusing the request referred to in paragraph 3 of this Article, the competent authority for implementing cybersecurity requirements shall consult the competent authorities of the Member State who has submitted the request.

(5) In the event described in paragraph 4 of this Article, at the request of the involved Member State, the competent authority for implementing cybersecurity requirements shall also consult the European Commission and ENISA.

(6) The provisions of this Article shall also apply in the event of receiving a request for mutual assistance in performing expert supervision of entities from Article 14, paragraph 3 of this Act, which provide services or have network and information systems in the territory of the Republic of Croatia.

Joint implementation of supervisory measures

Article 96

The competent authority for implementing cybersecurity requirements may perform joint implementation of the supervisory measures from this Act together with competent authorities from other Member States.

CHAPTER VI

COMPLIANCE CHECKS AS REGARDS SPECIFIC REQUIREMENTS FOR MANAGING DOMAIN NAME REGISTRATION DATA

Manner of performing checks, notifications regarding the performance of checks, and obligations of entities being checked

Article 97

(1) The compliance checks referred to in Article 49 of this Act (hereinafter: compliance checks) shall be performed in all entities subject to these checks at least once annually.

(2) The compliance checks shall be performed by the state administration authority competent for science and education by:

– consulting the ccTLD name registry and the registrars in order to carry out immediate inspection of the data, documents, conditions and ways of implementing specific requirements for managing domain name registration data from Articles 45 to 48 of this Act, or

– consulting requested and delivered data and documents of the entity being checked.

(3) The state administration authority competent for science and education shall notify the concerned entity of the performance of checks from paragraph 2, subparagraph 1 of this Article no later than five days before the start of the checks.

(4) By way of derogation from paragraph 2 of this Article, a compliance check can be performed without previous notification provided that there are justified reasons for taking immediate action.

(5) The ccTLD name registry and registrars shall enable the performance of the compliance checks and ensure all conditions for their unhindered performance, including in particular:

– enabling unhindered access and use of the premises, equipment, systems, and other infrastructure or technical means of the ccTLD name registry and registrars

– enabling inspection and use of all necessary data and documents, including making copies

– enabling interviews with responsible and accountable persons of the ccTLD name registry and registrars.

Imposing corrective measures

Article 98

(1) Depending on the results of the performed compliance check, the state administration authority competent for science and education may issue the following to the ccTLD name registry and registrars:

– warnings about infringements of this Act

– binding instructions or orders requiring them to remedy the identified deficiencies or the infringements of this Act, including measures that the entity needs to take so as to remedy these deficiencies or infringements.

(2) The instructions and orders referred to in paragraph 1 of this Article shall contain the deadline for implementing the imposed measures and the deadline for reporting on their implementation.

Temporary suspensions of issued authorisations for providing domain name registration services

Article 99

(1) Where the registrars fail to act according to the warnings, instructions or orders from Article 98 of this Act, the state administration authority competent for science and education shall request from CARNET to temporarily suspend the authorisation issued to the entity for providing domain name registration services.

(2) The measure from paragraph 1 of this Article shall be applied only until the entity concerned complies with the warnings, instructions or orders from Article 98 of this Act.

Reports on performed checks and judicial remedy

Article 100

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

PART NINE

INFRINGEMENT PROVISIONS

Administrative fines for essential entities

Article 101

(1) An administrative fine in the amount of EUR 10,000.00 to EUR 10,000,000.00 or 0.5% to no more than 2% of the total worldwide annual turnover in the preceding financial year of the entity concerned, whichever is higher, shall be imposed in the event of an infringement on the liable essential entity:

– who fails to implement, only partially implements or fails to implement within the set deadline the prescribed cybersecurity risk-management measures (Article 26 of this Act)

– who fails to use certified ICT products, ICT services and ICT processes while implementing cybersecurity risk-management measures, where such a requirement has been set out for the entity (Article 28 of this Act)

– whose persons responsible for managing the measures fail to approve the cybersecurity risk-management measures and/or do not control their implementation or do not ensure the implementation of the appropriate training sessions aimed at acquiring the know-how and skills in matters of cybersecurity risk management and their impact on the services provided by the entity or the activities it performs (Article 29 of this Act)

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

– who fails to notify, or fails to notify within the set deadline, any significant incidents or significant cyber threats to the service recipients, as well as any measures or judicial remedies which may be available to these recipients in order to respond to the threat (Article 38 of this Act)

– who fails to perform a cybersecurity audit at least once every two years (Article 34 of this Act)

– who fails to deliver within the set deadline the report on the performed cybersecurity audit to the competent authority for implementing cybersecurity requirements (Article 34 of this Act)

– who hinders, disrupts or disturbs the performance of the cybersecurity audit or fails to bear the costs of performing the cybersecurity audit (Article 34 of this Act)

– who fails to cooperate with the competent CSIRT and share with it the necessary information during the incident handling procedure (Article 68 of this Act)

– who fails to cooperate with the competent authority during supervision activities, or fails to deliver to such an authority the requested data or documents (Articles 77 and 79 of this Act)

– who fails to ensure unhindered access of competent authorities for expert supervision to the premises, equipment, systems and documents necessary to perform the supervision (Article 78 of this Act)

– who fails to act or acts only partially, or fails to act within the set deadline, in accordance with the corrective measures imposed during the expert supervision (Articles 82 and 83 of this Act).

(2) For infringements referred to in paragraph 1 of this Article, any natural person who is, in accordance with Article 29 of this Act, responsible for managing the measures of the liable essential entity, shall also be fined EUR 1,000.00 to EUR 6,000.00.

(3) When deciding on imposing fines in accordance with paragraphs 1 and 2 of this Article and their amounts, account shall be taken of the circumstances described in Article 85 of this Act.

Administrative fines for important entities

Article 102

(1) An administrative fine in the amount of EUR 5,000.00 to EUR 7,000,000.00 or 0.2% to no more than 1.4% of the total worldwide annual turnover in the preceding financial year of the entity concerned, whichever is higher, shall be imposed in the event of an infringement on the liable important entity:

– who fails to implement, only partially implements or fails to implement within the set deadline the prescribed cybersecurity risk-management measures (Article 26 of this Act)

– who fails to use certified ICT products, ICT services and ICT processes while implementing cybersecurity risk-management measures, where such a requirement has been set out for the entity (Article 28 of this Act)

– whose persons responsible for managing the measures fail to approve the cybersecurity risk-management measures and/or do not control their implementation or do not ensure the implementation of the appropriate training sessions aimed at acquiring the know-how and skills in matters of cybersecurity risk management and their impact on the services provided by the entity or the activities it performs (Article 29 of this Act)

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

– who fails to notify, or fails to notify within the set deadline, any significant incidents or significant cyber threats to the service recipients, as well as any measures or judicial remedies which may be available to these recipients in order to respond to the threat (Article 38 of this Act)

– who fails to perform a self-assessment of cybersecurity at least once every two years (Article 35 of this Act)

– who fails to deliver within the set deadline the statement on compliance or the plan for follow-up action to the competent authority for implementing cybersecurity requirements (Article 35 of this Act)

– who hinders, disrupts or disturbs the performance of the targeted cybersecurity audit or fails to bear the costs of performing the cybersecurity audit (Article 34 of this Act)

– who fails to cooperate with the competent CSIRT and share with it the necessary information during the incident handling procedure (Article 68 of this Act)

– who fails to cooperate with the competent authority during supervision activities, or fails to deliver to such an authority the requested data or documents (Articles 77 and 79 of this Act)

– who fails to ensure unhindered access of competent authorities for expert supervision to the premises, equipment, systems and documents necessary to perform supervision (Article 78 of this Act)

– who fails to act or acts only partially, or fails to act within the set deadline, in accordance with the corrective measures imposed during the expert supervision (Articles 82 of this Act).

(2) For infringements referred to in paragraph 1 of this Article, any natural person who is, in accordance with Article 29 of this Act, responsible for managing the measures of the liable important entity, shall also be fined EUR 500.00 to EUR 3,000.00.

(3) When deciding on imposing fines in accordance with paragraphs 1 and 2 of this Article and their amounts, account shall be taken of the circumstances described in Article 85 of this Act.

Administrative fines for non-compliance with the obligation to deliver information

Article 103

(1) The administrative fine in the amount of EUR 2,000.00 to EUR 20,000.00 shall be imposed in the event of an infringement on the liable entities:

– from Annex I and Annex II to this Act, if they fail to deliver, or fail to deliver within the set deadline, the information required for performing the classification of entities or maintaining the list of essential and important entities, or if they fail to notify any changes to this information in a timely manner (Article 20 of this Act)

– from Article 22 of this Act, if they fail to deliver, or fail to deliver within the set deadline, the information required for maintaining the special registry of entities, or if they fail to notify any changes to this information in a timely manner (Article 23 of this Act).

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

Authorised prosecutor

Article 104

(1) In case of a suspected infringement, the competent authority for implementing cybersecurity requirements shall report this to the authorised prosecutor.

(2) Within the meaning of this Act, the authorised prosecutor shall be the state attorney who brings charges.

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

(4) By way of derogation from paragraph 2 of this Article, the authorised prosecutor for infringements caused by trust service providers shall be the state administration authority responsible for the development of digital society.

PART TEN

TRANSITIONAL AND FINAL PROVISIONS

Responsibilities of operators of essential services and digital service providers in the transitional period

Article 105

Operators of essential services and digital service providers who had been, until entry into force of this Act, implementing measures for achieving a high level of cybersecurity in accordance with the provisions of the Act on Cybersecurity of Operators of Essential Services and Digital Service Providers (Official Gazette 64/18) and the Regulation on cybersecurity of operators of essential services and digital service providers (Official Gazette 68/18), shall continue implementing measures based on these regulations until the delivery of the notification regarding the performed classification of entities referred to in Article 19, paragraphs 1 and 3 of this Act.

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

Article 106

(1) Providers of public electronic communications networks and providers of publicly available electronic communications services who had been, until entry into force of this Act, implementing the security requirements aimed at safeguarding the security of electronic communications networks and electronic communications services in accordance with Article 41 of the Electronic Communications Act (Official Gazette 76/22), shall continue implementing the requirements pursuant to Article 41 of that Act until the delivery of the notification regarding the performed classification of entities referred to in Article 19, paragraph 1 of this Act.

(2) Trust service providers who had been, until entry into force of this Act, implementing security requirements aimed at safeguarding the security of trust services in accordance with 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 of the Act on the Implementation of 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 62/17), shall continue implementing the requirements pursuant to those regulations until the delivery of the notification regarding the performed classification of entities referred to in Article 19, paragraph 1 of this Act.

Transitional provision regarding the concluded agreements on accessing the national system

Article 107

Agreements on accessing the national system concluded pursuant to the Decision on measures and activities for increasing national capacities for a timely detection and protection against state-sponsored cyberattacks, Advanced Persistent Threat (APT) campaigns and other cyber threats, CLASS: 022-03/21-04/91, REG. NO: 50301-29/09-21-2, of 1 April 2021, shall remain valid until their expiry.

Deadline for compliance with requirements pertaining to managing domain name registration data and implementing checks for existing registrants

Article 108

The ccTLD name registry and registrars shall comply with the requirements of this Act pertaining to managing domain name registration data and perform checks referred to in Article 47, paragraph 2 of this Act for the existing registrants within one year from entry into force of this Act.

Commenced procedures

Article 109

(1) Procedures commenced in accordance with the provisions of the Act on Cybersecurity of Operators of Essential Services and Digital Service Providers (Official Gazette 64/18) shall be concluded in accordance with the provisions of that Act and the regulations adopted based on that Act.

(2) Procedures commenced in accordance with the provisions of Article 41 of the Electronic Communications Act (Official Gazette 76/22) shall be concluded in accordance with the provisions of that Act and the regulations adopted based on that Act.

Deadline for performing the first classification of entities

Article 110

(1) The competent authorities for implementing cybersecurity requirements from Article 4, paragraph 1, item 28 of this Act and the competent authorities for implementing special laws from Article 4, paragraph 1, item 27 of this Act shall perform the first classification of entities and deliver notifications regarding the performed classification of entities within one year from the date of entry into force of this Act.

(2) The entity classification procedure and delivery of notifications regarding the performed classification of entities shall be carried out within the deadline from paragraph 1

of this Article for all operators of essential services included in the list from Article 12 of the Act on Cybersecurity of Operators of Essential Services and Digital Service Providers (Official Gazette 64/18).

(3) The procedure of the first classification of information intermediaries in the exchange of electronic invoices between undertakings and the delivery of notifications regarding the performed classification pursuant to this Act shall be carried out within three months from the date of entry into force of the act governing the exchange of electronic invoices between undertakings.

Deadline for establishing a special registry of entities

Article 111

The central government authority for cybersecurity shall establish a special registry of entities from Article 22 of this Act within one year from the date of entry into force of this Act.

Beginning of the term for performing security audits and expert supervisions

Article 112

The deadlines for performing cybersecurity audits from Article 34, paragraph 1 of this Act and expert supervisions of implementing cybersecurity requirements from Article 75, paragraph 1 of this Act shall begin on the first working day following the expiry of the deadline from Article 26, paragraph 5 of this Act.

Adoption of implementing regulations

Article 113

(1) The Government shall adopt the regulation referred to in Article 24 of this Act within nine months from the date of entry into force of this Act.

(2) The Government shall 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 shall adopt the national cyber crisis management programme referred to in Article 56 of this Act within three months from the date of entry into force of this Act.

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

(5) The Information Systems Security Bureau 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 from paragraph 1 of this Article.

Adoption of regulations on internal organisation and internal order

Article 114

(1) The Government shall, at the proposal of the Director of the Office of the National Security Council and with the prior approval of the President of the Republic of Croatia, adjust the Regulation on internal organisation of the Office of the National Security Council to the provisions of this Act within 30 days from the date of entry into force of this Act.

(2) The Director of the Office of the National Security Council shall adjust the Ordinance on the internal order of the Office of the National Security Council to the Regulation

referred to in paragraph 1 of this Article, with the prior approval of the National Security Council, within 30 days from the date of entry into force of the Regulation.

(3) The Government shall, at the proposal of the Director of the Security and Intelligence Agency, and with the prior approval of the President of the Republic of Croatia, adjust the Regulation on internal organisation of the Security and Intelligence Agency to 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 adjust the Ordinance on the internal order of the Security and Intelligence Agency to the Regulation referred to in paragraph 3 of this Article, with the prior approval of the Director 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, at the proposal of the Information Systems Security Bureau, and with the prior approval of the Council for the Coordination of Security and Intelligence Services, adjust the Regulation on internal organisation of the Information Systems Security Bureau to 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 Bureau shall adjust the Ordinance on the internal order of the Information Systems Security Bureau to the Regulation referred to in paragraph 5 of this Article, with the prior approval of the Government, within 30 days from the date of entry into force of the Regulation.

Termination of validity

Article 115

(1) As of the date of entry into force of this Act, the following shall cease to have effect:

– the Act on Cybersecurity of Operators of Essential Services and Digital Service Providers (Official Gazette 64/18)

– Article 17, paragraph 2, subparagraph 4 and Article 21 of the Information Security Act (Official Gazette 79/07)

– Article 41 of the Electronic Communications Act (Official Gazette 76/22)

– the Regulation on cybersecurity of operators of essential services and digital service providers (Official Gazette 68/18) and

– the Decision on the establishment of the National Cyber Security Council and the Operational and Technical Cyber Security Coordination Group (Official Gazette 61/16, 28/18, 110/18, 79/19 and 136/20).

(2) the Decision on measures and activities for increasing national capacities for a timely detection and protection against state-sponsored cyber attacks, Advanced Persistent Threat (APT) campaigns and other cyber threats, CLASS: 022-03/21-04/91, REG. NO: 50301-29/09-21-2, of 1 April 2021, shall remain in effect until the entry into force of the regulation referred to in Article 113, paragraph 1 of this Act.

Entry into force of the Act

Article 116

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

Class: 022-02/23-01/94
Zagreb, 26 January 2024

THE CROATIAN PARLIAMENT

The President of
the Croatian Parliament
Gordan Jandroković, m.p.

ANNEX I

SECTORS OF HIGH CRITICALITY

Sector	Subsector	Type of entity
1. Energy	(a) Electricity	– electricity entities which carry out the function of electricity supply, including public service electricity supply Within the meaning of this Act, the term "electricity entity" shall mean a legal or natural person other than the final customer, who carries out at least one electricity activity and who is responsible for the commercial, technical or maintenance tasks related to those activities. Within the meaning of this Act, the term "electricity supply" shall mean the purchase and sale of electricity on the wholesale market, the sale of electricity to final customers and energy storage facilities, the purchase of electricity from active customers, energy storage facilities and producers, and aggregation. Within the meaning of this Act, the term "public service electricity supply" shall mean the supply of electricity to those final customers who have the right to that supply method and freely choose it or use it automatically. The terms "electricity entity", "electricity supply" and "public service electricity supply" are equivalent to the terms referred to in Article 3, paragraph 1, items 17, 77 and 78 of the Electricity Market Act (Official Gazette 111/21 and 83/23) transposing Directive (EU) 2019/944 of the European Parliament and of the Council of 5 June 2019 on common rules for the internal market for electricity and amending Directive 2012/27/EU (OJ L 158, 14.6.2019) into Croatian law.
		– distribution system operators Within the meaning of this Act, the term "distribution system operator" shall mean a natural or legal person responsible for the operation and management, maintenance, development and construction of the distribution network in a given area, as well as common facilities under the transmission network and, where applicable, interconnection with other distribution systems, and for ensuring the long-term ability of the distribution network to meet reasonable requirements for the distribution of electricity.

		The term "distribution system operator" is equivalent to the term referred to in Article 3, paragraph 1, item 71 of the Electricity Market Act (Official Gazette 111/21 and 83/23).
		– transmission system operators Within the meaning of this Act, the term "transmission system operator" shall mean a natural or legal person responsible for the operation and management, maintenance, development and construction of the transmission network in a given area, cross-border transmission lines to other transmission networks, as well as common facilities under the distribution network, and for ensuring the long-term ability of the transmission network to meet reasonable requirements for the transmission of electricity. The term "transmission system operator" is equivalent to the term referred to in Article 3, paragraph 1, item 72 of the Electricity Market Act (Official Gazette 111/21 and 83/23).
		– electricity producers Within the meaning of this Act, the term "electricity producer" shall mean a natural or legal person that produces electricity. The term "electricity producer" is equivalent to the term referred to in Article 3, paragraph 1, item 90 of the Electricity Market Act (Official Gazette 111/21 and 83/23).
		– nominated electricity market operators as defined in Article 2, point (8) of Regulation (EU) 2019/943 of the European Parliament and of the Council of 5 June 2019 on the internal market for electricity (OJ L 158, 14.6.2019)
		– market participants as defined in Article 2, point (25) of Regulation (EU) 2019/943 providing aggregation, demand response or energy storage services Within the meaning of this Act, the term "aggregation" shall mean an activity carried out by a natural or legal person who is able to combine power and/or electricity imported from the grid of multiple customers or energy storage operators, or power and/or electricity fed into the grid of multiple producers or active customers or energy storage operators for the purpose of participating in any electricity market.

		Within the meaning of this Act, the term "consumption management" shall mean a change in the load of the final customers in relation to their usual or current electricity consumption patterns in response to market signals, including a time-dependent change in the price of electricity or monetary incentives, or in response to the acceptance of an offer by the final customer to sell a reduction or increase in demand at a price set on organised markets, as defined in Article 2, point (4) of Commission Implementing Regulation (EU) No 1348/2014 of 17 December 2014 on data reporting and implementing Article 8(2) and Article 8(6) of Regulation (EU) No 1227/2011 of the European Parliament and of the Council on wholesale energy market integrity and transparency (Text with EEA relevance) (OJ L 363, 18.12.2014), either individually or via aggregation. Within the meaning of this Act, the term "energy storage" shall mean, in the context of the electricity system, the postponement of the final use of electricity until the moment later than the moment in which it was produced, or the conversion of electricity into a form of energy that may be stored, the storage of such energy and the subsequent conversion of such energy into electricity or its use as an energy carrier. The terms "aggregation", "demand response" and "energy storage" are equivalent to the terms referred to in Article 3, paragraph 1, items 4, 93 and 109 of the Electricity Market Act (Official Gazette 111/21 and 83/23).
		– operators of a recharging point that are responsible for the management and operation of a recharging point, which provides a recharging service to end users, including in the name and on behalf of a mobility service provider
	(b) District heating and cooling systems	– operator of district heating or district cooling systems Within the meaning of this Act, the term "district heating or district cooling" shall mean the distribution of thermal energy in the form of steam, hot water or chilled liquids, from a centralised or decentralised production plant through central or closed thermal systems located in multiple buildings or sites, for the use of space or process heating or cooling. The term "district heating or district cooling" is equivalent to the term referred to in Article 4, paragraph 1, item 4 of the Act on Renewable Energy

		Sources and High-Efficiency Cogeneration (Official Gazette 138/21 and 83/23) transposing Directive (EU) 2018/2001 of the European Parliament and of the Council of 11 December 2018 on the promotion of the use of energy from renewable sources (recast) (Text with EEA relevance) (OJ L 328, 21.12.2018) into Croatian law.
	(c) Oil	– operators of oil transmission pipelines
		– operators of oil production, refining and treatment facilities, storage and transmission
		– central stockholding entities Within the meaning of this Act, the term "central stockholding entity" shall mean the Croatian Hydrocarbon Agency, as the central entity in the Republic of Croatia for compulsory stocks of oil and petroleum products, which is a single body authorised to form, maintain and sell compulsory stocks. The term "central stockholding entity" is equivalent to the term referred to in Article 3, paragraph 2, item 5) of the Oil and Petroleum Products Market Act (Official Gazette 19/14, 73/17 and 96/19) transposing Directive 2009/119/EC of the European Parliament and of the Council of 14 September 2009 imposing an obligation on Member States to maintain minimum stocks of crude oil and/or petroleum products (OJ L 265/9, 9.10.2009) into Croatian law.
	(d) Gas	– gas suppliers, including public service suppliers Within the meaning of this Act, the term "gas supplier" shall mean an energy entity that performs the energy activity of gas supply. Within the meaning of this Act, the term "public service gas supplier" shall mean a gas supplier who performs the energy activity of public supply. Within the meaning of this Act, the term "gas supply" shall mean the sale or resale of gas to a customer, including the sale or resale of LNG and CNG. Within the meaning of this Act, the term "public service gas supply" shall mean gas supply carried out in the general economic interest under regulated conditions in order to ensure the safety, regularity, quality and price of household supply. The terms "gas supplier", "public gas supplier", "gas supply" and "public gas supply" are equivalent to the terms referred to in Article 3, paragraph 2, items 36, 37,

		38 and 39 of the Gas Market Act (Official Gazette 18/18 and 23/20) transposing Directive 2009/73/EC of the European Parliament and of the Council of 13 July 2009 concerning common rules for the internal market in natural gas and repealing Directive 2003/55/EC (Text with EEA relevance) (OJ L 211, 14.8.2009) into Croatian law.
		– distribution system operators Within the meaning of this Act, the term "distribution system operator" shall mean an energy entity that performs the energy activity of gas distribution and is responsible for the operation, ensuring the maintenance and development of the distribution system in its distribution area and, where applicable, its interconnections with other systems, and for ensuring the long-term ability of the system to meet reasonable gas distribution needs. Within the meaning of this Act, the term "gas distribution" shall mean the distribution of gas through a high, medium and low-pressure distribution system for the purpose of delivering gas to final customers, including ancillary services, and excluding gas supply. Within the meaning of this Act, the term "distribution system" shall mean a system of gas pipelines and other associated facilities and equipment owned and/or operated by the distribution system operator, which is used for gas distribution, supervision and management, measurement and data transmission. The terms "distribution system operator", "gas distribution" and "distribution system" are equivalent to the terms referred to in Article 3, paragraph 2, items 5, 6 and 30 of the Gas Market Act (Official Gazette 18/18 and 23/20).
		– transmission system operators Within the meaning of this Act, the term "transmission system operator" shall mean an energy entity that performs the energy activity of gas transport and is responsible for the operation, ensuring the maintenance and development of the transmission system in a particular area and, where applicable, its interconnections with other systems and for ensuring the long-term ability of the system to meet reasonable gas transport needs. Within the meaning of this Act, the term "gas transport" shall mean the transmission of gas via the transmission

		system, excluding gas supply and gas trade, and including gas transit and ancillary services. Within the meaning of this Act, the term "transmission system" shall mean a facility owned and/or operated by the transmission system operator, which consists of a system of high-pressure gas pipelines, compressor stations, metering stations, metering and reduction stations, gas nodes and other technological facilities and equipment used for gas transport, monitoring and management, measurement and data transmission, excluding the network of production gas pipelines and high-pressure distribution gas pipelines, including gas for technological capacities exclusively used by the transmission system operator and operational accumulation. The terms "transmission system operator", "gas transmission" and "transmission system" are equivalent to the terms referred to in Article 3, paragraph 2, items 34, 58 and 59 of the Gas Market Act (Official Gazette 18/18 and 23/20).
		– storage system operators Within the meaning of this Act, the term "storage system operator" shall mean an energy entity that performs the energy activity of gas storage and is responsible for the operation, maintenance and development of the gas storage system. Within the meaning of this Act, the term "gas storage" shall mean the injection of gas into the gas storage system, its storage within the operating volume of the gas storage system and its withdrawal from the gas storage system, including ancillary services. The terms "storage system operator" and "gas storage" are equivalent to the terms referred to in Article 3, paragraph 2, items 54 and 56 of the Gas Market Act (Official Gazette 18/18 and 23/20).
		– LNG system operators Within the meaning of this Act, the term "LNG system operator" shall mean an energy entity that performs the energy activity of managing an LNG facility and is responsible for the operation, maintenance and development thereof. Within the meaning of this Act, the term "LNG facility" shall mean a terminal used for the liquefaction of natural gas or the importation, offloading, and re-

		gasification of LNG, and includes ancillary services and temporary storage necessary for the re-gasification process and subsequent delivery to the transmission system, but does not include any part of LNG terminals used for storage. The terms "LNG system operator" and "LNG facility" are equivalent to the terms referred to in Article 3, paragraph 2, items 33 and 57 of the Gas Market Act (Official Gazette 18/18 and 23/20).
		– natural gas undertakings Within the meaning of this Act and in accordance with the legislation governing the gas market, the term "natural gas undertaking" shall mean a natural or legal person carrying out at least one of the following functions: production, transmission, distribution, supply, purchase or storage of natural gas, including LNG, which is responsible for the commercial, technical and/or maintenance tasks related to those functions, but shall not include final customers.
		– operators of natural gas refining and treatment facilities
	(e) Hydrogen	– operators of hydrogen production, storage and transmission
2. Transport	(a) Air	– air carriers as defined in Article 3, point (4), of Regulation (EC) No 300/2008 of the European Parliament and of the Council of 11 March 2008 on common rules in the field of civil aviation security and repealing Regulation (EC) No 2320/2002 (Text with EEA relevance), used for commercial purposes
		– airport managing bodies, airports, including the core airports listed in Section 2 of Annex II to Regulation (EU) No 1315/2013 of the European Parliament and of the Council of 11 December 2013 on Union guidelines for the development of the trans-European transport network and repealing Decision No 661/2010/EU (Text with EEA relevance), and entities operating ancillary installations contained within airports Within the meaning of this Act, the term "airport managing body" shall mean a body which, in conjunction with other activities or not as the case may be, has as its objective under national regulations or contracts the administration and management of the airport infrastructure and the coordination and control of the activities of the different operators present in the airport concerned. Within the meaning of this Act, the term "airport" shall mean any land area specifically adapted for the landing, taking-off and manoeuvring of aircraft,

		including the ancillary installations, resources and devices for the requirements of aircraft traffic and services, including the installations, resources and devices needed to assist commercial air services. The terms "airport managing body" and "airport" are equivalent to the terms referred to in Article 3, paragraph 1, subparagraphs 1 and 2 of the Ordinance on airport charges (Official Gazette 65/15) transposing Directive 2009/12/EC of the European Parliament and of the Council of 11 March 2009 on airport charges into Croatian law.
		– traffic management control operators providing air traffic control (ATC) services as defined in Article 2, point (1), of Regulation (EC) No 549/2004 of the European Parliament and of the Council of 10 March 2004 laying down the framework for the creation of the single European sky (the framework Regulation) and the Statement by the Member States on military issues related to the single European sky
	(b) Rail	– infrastructure managers Within the meaning of this Act, the term "infrastructure manager" shall mean a legal person or an organisational unit within a vertically integrated undertaking responsible for the operation, maintenance and renewal of railway infrastructure, as well as for participating in its development as determined by the framework of the general policy on development and financing of rail infrastructure of the Republic of Croatia. The term "infrastructure manager" is equivalent to the term referred to in Article 5, paragraph 1, item 36 of the Railway Act (Official Gazette 32/19, 20/21 and 114/22) transposing Directive 2012/34/EU of the European Parliament and of the Council of 21 November 2012 establishing a single European railway area (recast) (OJ L 343, 14.12.2012), as last amended by Directive (EU) 2016/2370 of the European Parliament and of the Council of 14 December 2016 amending Directive 2012/34/EU as regards the opening of the market for domestic passenger transport services by rail and the governance of the railway infrastructure (Text with EEA relevance) (OJ L 352, 23.12.2016), into Croatian law.
		– railway undertakings, including operators of service facilities Within the meaning of this Act, the term "railway undertaking" shall mean any legal person licensed to provide rail transport services and whose principal

		business is the provision of rail transport services for passengers and/or freight, provided that the said legal person ensures train traction; this also includes a legal person providing traction only. Within the meaning of this Act, the term "operator of service facilities" shall mean a legal person responsible for the management of one or more service facilities (service facility manager) or for supplying one or more services to railway undertakings referred to in items 2 to 4 of Annex 2 of the Railway Act (Official Gazette os 32/19, 20/21 and 114/22) (service provider). The terms "railway undertaking" and "operator of service facilities" are equivalent to the terms referred to in Article 5, paragraph 1, items 22 and 46 of the Railway Act (Official Gazette 32/19, 20/21 and 114/22).
	(c) Water	– inland, sea and coastal passenger water transport companies as defined for maritime transport in Annex I to Regulation (EC) No 725/2004 of the European Parliament and of the Council of 31 March 2004 on enhancing ship and port facility security (Text with EEA relevance), not including the individual vessels operated by those companies
		– managing bodies of ports, including their port facilities as defined in Article 2, point (11), of Regulation (EC) No 725/2004, and entities operating works and equipment contained within ports Within the meaning of this Act, the term "port" shall mean a maritime port, i.e. a maritime area and a land area directly connected to the sea within the defined boundaries of the port area with developed and undeveloped shore, breakwaters, devices, installations and other facilities and systems intended for docking, anchoring and sheltering of ships, yachts and boats, embarking and discharging passengers and goods, for storage and other handling of goods, production, refinement and final processing of goods, and other economic activities related to the aforementioned activities on an economic, transport or technological basis. The term "port" is equivalent to the term referred to in Article 3, paragraph 1, item1 of the Act on the Security of Maritime Ships and Ports (Official Gazette 108/17 and 30/21) transposing Directive 2005/65/EC of the European Parliament and of the Council of 26 October 2005 on enhancing port security (Text with EEA relevance) (OJ L 320, 25.11.2005) into Croatian law.

		– vessel traffic service (VTS) as defined in Article 75a, paragraph 1 and Article 75b, paragraph 1 of the Maritime Code (Official Gazette 181/04, 76/07, 146/08, 61/11, 56/13, 26/15 and 17/19) transposing Directive 2002/59/EC of the European Parliament and of the Council of 27 June 2002 establishing a Community vessel traffic monitoring and information system and repealing Council Directive 93/75/EEC, into Croatian law
	(d) Road	– road authorities as defined in Article 2, point (12), of Commission Delegated Regulation (EU) 2015/962 of 18 December 2014 supplementing Directive 2010/40/EU of the European Parliament and of the Council with regard to the provision of EU-wide real-time traffic information services (Text with EEA relevance), responsible for traffic management control, excluding public entities for which traffic management or the operation of intelligent transport systems is a non-essential part of their general activity According to Article 2, point (12), of Commission Delegated Regulation (EU) 2015/962, the term "road authority" shall mean any public authority responsible for the planning, control or management of roads falling within its territorial competence.
		– operators of intelligent transport systems Within the meaning of this Act, the term "intelligent transport systems (ITS) " shall mean an information and communication upgrade of the classic road transport system that significantly improves the performance of the transport system as a whole. ITS includes roads, vehicles and road users, and is applied in traffic management, mobility management, traffic incident management, as well as for interfaces with other modes of transport. The term "intelligent transport systems (ITS)" is equivalent to the term referred to in Article 72, paragraph 1 of the Roads Act (Official Gazette 84/11, 22/13, 54/13, 148/13, 92/14, 110/19, 144/21, 114/22, 04/23 and 133/23) transposing Directive 2010/40/EC of the European Parliament and of the Council of 7 July 2010 on the framework for the deployment of Intelligent Transport Systems in the field of road transport and for interfaces with other modes of transport (Text with EEA relevance) (OJ L 207 of 6 August 2010), into Croatian law.
3. Banking		– credit institutions as defined in Article 4, point (1), of Regulation (EU) No 575/2013 of the European Parliament and of the Council of 26 June 2013 on

		prudential requirements for credit institutions and investment firms and amending Regulation (EU) No 648/2012 (Text with EEA relevance)
4. Financial market infrastructure		– operators of trading venues Within the meaning of this Act, the term "trading venue" shall mean a regulated market, an MTF or an OTF. Within the meaning of this Act, the term "multilateral trading facility" or MTF shall mean a multilateral system operated by an investment firm or a market operator, which brings together multiple third-party buying and selling interests in financial instruments – in the system and in accordance with non-discretionary rules – in a way that results in a contract, in accordance with the provisions of Part 2, Title III, Chapter VII of the Capital Market Act (Official Gazette 65/18, 17/20, 83/21 and 151/22). Within the meaning of this Act, the term "organised trading facility" or OTF shall mean a multilateral system, which is not a regulated market or an MTF, and in which multiple third-party buying and selling interests in bonds, structured finance products, emission allowances or derivatives are able to interact in the system in a way that results in a contract, in accordance with the provisions of Part 2, Title III, Chapter VII of the Capital Market Act (Official Gazette 65/18, 17/20, 83/21 and 151/22). The terms "trading venue", "multilateral trading facility (MTF) " and "organised trading facility (OTF) " are equivalent to the terms referred to in Article 3, paragraph 1, items 61, 65 and 77 of the Capital Market Act (Official Gazette 65/18, 17/20, 83/21 and 151/22) transposing Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU (recast) (Text with EEA relevance) (OJ L 173, 12.6.2014) into Croatian law.
		– central counterparties (CCPs) as defined in Article 2, point (1), of Regulation (EU) No 648/2012 of the European Parliament and of the Council of 4 July 2012 on OTC derivatives, central counterparties and trade repositories (OJ L 201, 27.7.2012)
5. Health		– healthcare providers Within the meaning of this Act, the term "healthcare provider" shall mean any natural or legal person or any

		entity performing healthcare activities in the Republic of Croatia in accordance with the legislation governing healthcare. The term "healthcare provider" shall not refer to organisational units of the Ministry of Defence and the Armed Forces of the Republic of Croatia and the ministry responsible for judicial matters that perform healthcare activities according to special regulations.
		– European Union reference laboratories referred to in Article 15 of Regulation (EU) 2022/2371 of the European Parliament and of the Council of 23 November 2022 on serious cross-border threats to health and repealing Decision No 1082/2013/EU (Text with EEA relevance)
		– entities carrying out research and development activities of medicinal products Within the meaning of this Act, the term "medicinal product" shall mean: – any substance or combination of substances presented for treating or preventing disease in human beings or – any substance or combination of substances which may be used in or administered to human beings either with a view to restoring, correcting or modifying physiological functions by exerting a pharmacological, immunological or metabolic action, or to making a medical diagnosis. The term "medicinal product" is equivalent to the term referred to in Article 3, paragraph 1, item 1 of the Medicinal Products Act (Official Gazette 76/13, 90/14 and 100/18) transposing Directive 2001/83/EC of the European Parliament and of the Council of 6 November 2001 on the Community code relating to medicinal products for human use (OJ L 311, 28.11.2001) into Croatian law.
		– entities manufacturing basic pharmaceutical products and pharmaceutical preparations referred to in section C of division 21 of the 2007 National Classification of Activities – NKD 2007. (Official Gazette 58/07 and 72/07)
		– entities manufacturing medical devices considered to be critical during a public health emergency ("public health emergency critical devices list") within the meaning of Article 22 of Regulation (EU) 2022/123 of the European Parliament and of the Council of 25 January 2022 on a reinforced role for the European Medicines Agency in crisis preparedness and management for medicinal products and medical devices (Text with EEA relevance)

6.Water intended for human consumption		– suppliers and distributors of water intended for human consumption, excluding distributors for which distribution of water for human consumption is a non-essential part of their general activity of distributing other commodities and goods Within the meaning of this Act, the term "water intended for human consumption" shall mean: – all water, either in its original state or after treatment, intended for drinking, cooking, food preparation or other domestic purposes in both public and private premises, regardless of its origin and whether it is supplied from a distribution network, supplied from a tanker or put into bottles or containers, including spring and table waters – all water used in any food business for the manufacture, processing, preservation or marketing of products or substances intended for human consumption. The term "water intended for human consumption" is equivalent to the term referred to in Article 3, paragraph 1, item 1 of the Act on Water for Human Consumption (Official Gazette 30/23) transposing Directive (EU) 2020/2184 of the European Parliament and of the Council of 16 December 2020 on the quality of water intended for human consumption (recast) (Text with EEA relevance) (OJ L 435, 23.12.2020) into Croatian law.
7. Waste water		– undertakings collecting, disposing of or treating urban waste water, sanitary waste water or industrial waste water, excluding undertakings for which collecting, disposing of or treating urban waste water, domestic waste water or industrial waste water is a non-essential part of their general activity Within the meaning of this Act, the term "urban waste water" shall mean waste water from the public sewage system consisting of sanitary waste water or waste water that is a mixture of sanitary waste water and industrial waste water and/or run-off rain water of a specific agglomeration. Within the meaning of this Act, the term "sanitary waste water" shall mean waste water discharged from residential settlements and services which originates predominantly from the human metabolism and from household activities. Within the meaning of this Act, the term "industrial waste water" shall mean any waste water, other than

		sanitary waste water and run-off rain, discharged from premises used for trade or industrial activities. The terms "urban waste water", "sanitary waste water" and "industrial waste water" are equivalent to the terms referred to in Article 4, paragraph 1, items 25, 34 and 81 of the Water Act (Official Gazette 66/19, 84/21 and 47/23) transposing Council Directive 91/271/EEC of 21 May 1991 concerning urban waste water treatment (OJ L 135, 30.5.1991), as amended by Commission Directive 98/15/EC of 27 February 1998 with respect to certain requirements established in Annex I (Text with EEA relevance) (OJ L 67, 7.3.1998), into Croatian law.
8. Digital infrastructure		– Internet Exchange Point providers
		– DNS service providers, excluding operators of root name servers
		– ccTLD name registry
		– cloud computing service providers
		– data centre service providers
		– content delivery network providers
		– trust service providers
		– providers of public electronic communications networks
		– providers of publicly available electronic communications services
9. ICT service management (B2B)		– managed service providers
		– managed security service providers
		– information intermediaries as defined by the regulation governing the exchange of electronic invoices between undertakings
10. Public sector		– state administration authorities
		– other state authorities and legal persons with public authority
		– private and public entities that manage, develop or maintain the state information infrastructure in accordance with the law governing the state information infrastructure
		– local and regional self-government units
11. Space		– operators of ground-based infrastructure, owned, managed and operated by Member States or by private parties, that support the provision of space-based services, excluding providers of public electronic communications networks

ANNEX II

OTHER CRITICAL SECTORS

Sector	Subsector	Type of entity
1. Postal and courier services		– postal service providers Within the meaning of this Act, the term "postal service provider" shall mean a legal or natural person performing postal services, including a "universal service provider" as a postal service provider performing a universal service in the Republic of Croatia. Within the meaning of this Act, the term "postal service" shall mean a service that includes any handling of postal items by a postal service provider, and in particular the receipt, routing, transfer and delivery of postal items in domestic or international postal traffic. "Postal service" shall not include the transport of an item to a sender which the sender performs on their own (self-delivery), transportation as a standalone service, nor the receipt, transport and delivery of postal items directly from the sender to the recipient upon individual request, without routing, in such a way that a single employee of the service provider performs all the aforementioned activities (courier service). Within the meaning of this Act, the term "universal service" shall mean a set of postal services of specified quality available at an affordable cost to all postal service users in the territory of the Republic of Croatia, regardless of their geographical location. The terms "postal service provider", "universal service provider", "postal service" and "universal service" are equivalent to the terms referred to in Article 2, paragraph 1, items 4, 5, 21 and 32 of the Postal Services Act (Official Gazette 144/12, 153/13, 78/15 and 110/19) transposing Directive (EU) 97/67/EC of the European Parliament and of the Council of 15 December 1997 on common rules for the development of the internal market of Community postal services and the improvement of quality of service (OJ L 15, 21.1.1998) into Croatian law.
		– providers of courier services
2. Waste management		– entities carrying out waste management, excluding entities for whom waste management is not their principal economic activity Within the meaning of this Act, the term "waste management" shall mean the activities of collection,

		transport, recovery including sorting and disposal of waste, including supervision over the performance of these activities, supervision and measures carried out at disposal sites, and actions taken by the waste dealer and waste management broker. Within the meaning of this Act, the term "waste" shall mean any substance or object which the holder discards or intends or is required to discard. Within the meaning of this Act, the term "waste collection activity" shall mean an activity that includes the waste collection procedure and the waste collection procedure involving a recycling yard. Within the meaning of this Act, the term "waste transport activity" shall mean the transport of waste for own use or for the use of others in the territory of the Republic of Croatia. Within the meaning of this Act, the term "waste recovery activity" shall mean an activity involving the performance of a recovery operation from the List of Waste Recovery Operations. Within the meaning of this Act, the term "technological processes of waste management" shall mean specific functional and technological units of waste management that describe the material flow of waste and include collection, reception, storage, preliminary sorting and sorting, waste mixing, packaging, repair, cleaning, checking of future products and other processes within the waste recovery and disposal process. Within the meaning of this Act, the term "waste disposal activity" shall mean an activity involving the performance of a waste disposal procedure from the List of Waste Disposal Operations. Within the meaning of this Act, the term "waste dealer" shall mean a legal or natural person – a craftsman who buys and sells waste on their own behalf and for their own account, including a waste dealer who does not take immediate possession of the waste. Within the meaning of this Act, the term "broker" shall mean a legal or natural person – a craftsman who performs the activity of mediation in waste

		management, including a broker who does not take immediate possession of the waste. The terms "waste management", "waste", "waste collection activity", "waste transport activity", "waste recovery activity", "technological processes of waste management", "waste management activity", "waste dealer" and "broker" are equivalent to the terms referred to in Article 4, paragraph 1, items 15, 48, 11, 10, 8, 82, 13, 84 and 60 of the Waste Management Act (Official Gazette 84/21 and 142/23) transposing Directive 2008/98/EC of the European Parliament and of the Council of 19 November 2008 on waste and repealing certain Directives (OJ L 312, 22.11.2008) as last amended by Directive (EU) 2018/851 of the European Parliament and of the Council of 30 May 2018 amending Directive 2008/98/EC on waste (OJ L 150, 14.6.2018) into Croatian law.
3. Manufacture, production and distribution of chemicals		– entities carrying out the manufacture of substances and the distribution of substances or mixtures, as defined in in Article 3, points (9) and (14) of Regulation (EC) No 1907/2006 of the European Parliament and of the Council concerning the Registration, Evaluation, Authorisation and Restriction of Chemicals (REACH), establishing a European Chemicals Agency, amending Directive 1999/45/EC and repealing Council Regulation (EEC) No 793/93 and Commission Regulation (EC) No 1488/94 as well as Council Directive 76/769/EEC and Commission Directives 91/155/EEC, 93/67/EEC, 93/105/EC and 2000/21/EC (Text with EEA relevance)
		– entities carrying out the production of articles, as defined in Article 3, point (3), of Regulation (EC) No 1907/2006, from substances or mixtures
4. Production, processing and distribution of food		– food businesses as defined in Article 3, point (2), of Regulation (EC) No 178/2002 of the European Parliament and of the Council of 28 January 2002 laying down the general principles and requirements of food law, establishing the European Food Safety Authority and laying down procedures in matters of food safety, which are engaged in wholesale distribution and industrial production and processing
5. Manufacturing	(a) Manufacture of medical devices and in vitro diagnostic medical devices	– entities manufacturing medical devices as defined in Article 2 , point (1), of Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC (Text with

		EEA relevance) and entities manufacturing in vitro diagnostic medical devices as defined in Article 2, point (2), of Regulation (EU) 2017/746 of the European Parliament and of the Council of 5 April 2017 on in vitro diagnostic medical devices and repealing Directive 98/79/EC and Commission Decision 2010/227/EU (Text with EEA relevance), with the exception of entities manufacturing medical devices referred to in Annex I, item 5, fifth indent of this Act. The fifth indent of Annex I, item 5, refers to "entities manufacturing medical devices considered to be critical during a public health emergency" or to the "public health emergency critical devices list" within the meaning of Article 22 of Regulation (EU) 2022/123.
	(b) Manufacture of computer, electronic and optical products	– entities carrying out any of the economic activities referred to in section C of division 26 of the 2007 National Classification of Activities – NKD 2007. (Official Gazette 58/07 and 72/07).
	(c) Manufacture of electrical equipment	– entities carrying out any of the economic activities referred to in section C of division 27 of the 2007 National Classification of Activities – NKD 2007. (Official Gazette 58/07 and 72/07).
	(d) Manufacture of machinery and equipment n.e.c.	– entities carrying out any of the economic activities referred to in section C of division 28 of the 2007 National Classification of Activities – NKD 2007. (Official Gazette 58/07 and 72/07).
	(e) Manufacture of motor vehicles, trailers and semi-trailers	– entities carrying out any of the economic activities referred to in section C, division 29 of the 2007 National Classification of Activities – NKD 2007. (Official Gazette 58/07 and 72/07).
	(f) Manufacture of other transport equipment	– entities carrying out any of the economic activities referred to in section C of division 30 of the 2007 National Classification of Activities – NKD 2007. (Official Gazette 58/07 and 72/07).
6. Digital providers		– providers of online marketplaces
		– providers of online search engines
		– providers of social networking services platforms
7. Research		– research organisations
8. Education system		– private and public entities in the education system

ANNEX III

Cybersecurity Jurisdiction List

No.	Sector	Subsector	Type of entity	Competent authority for implementing cybersecurity requirements	Competent authority for implementing special laws	Competent CSIRT
1.	Energy	All	All	Central government authority for cybersecurity	-	National Cybersecurity Centre
2.	Transport	Air	All	-	Croatian Civil Aviation Agency	National Cybersecurity Centre
3.	Transport	Rail Water Road	All	Central government authority for cybersecurity	-	National Cybersecurity Centre
4.	Banking	-	All	-	Croatian National Bank	National CERT
5.	Financial market infrastructure	-	All	-	Croatian Financial Services Supervisory Agency	National CERT
6.	Health	-	All	Central government authority for cybersecurity	-	National Cybersecurity Centre
7.	Water intended for human consumption	-	All	Central government authority for cybersecurity	-	National Cybersecurity Centre
8.	Waste water	-	All	Central government authority for cybersecurity	-	National Cybersecurity Centre
9.	Digital infrastructure	-	Trust service providers	State administration authority responsible for the development of digital society	-	National Cybersecurity Centre
10.	Digital infrastructure	-	Providers of public electronic communications networks	Croatian Regulatory Authority for Network Industries	-	National Cybersecurity Centre

			Providers of publicly available electronic communications services			
11.	Digital infrastructure	-	Internet Exchange Point providers DNS service providers, excluding operators of root name servers Cloud computing service providers Data centre service providers Content delivery network providers	Central government authority for cybersecurity	-	National Cybersecurity Centre
12.	Digital infrastructure	-	ccTLD name registry	State administration authority responsible for science and education	-	National CERT
13.	ICT service management (B2B)	-	All	Central government authority for cybersecurity	-	National Cybersecurity Centre
14.	Public sector	-	All	Central government authority for information security	-	National Cybersecurity Centre
15.	Space	-	All	Central government authority for cybersecurity	-	National Cybersecurity Centre

16.	Postal and courier services	-	All	Central government authority for cybersecurity	-	National Cybersecurity Centre
17.	Waste management	-	All	Central government authority for cybersecurity	-	National Cybersecurity Centre
18.	Manufacture, production and distribution of chemicals	-	All	Central government authority for cybersecurity	-	National Cybersecurity Centre
19.	Production, processing and distribution of food	-	All	Central government authority for cybersecurity	-	National Cybersecurity Centre
20.	Manufacturing	Manufacture of medical devices and in vitro diagnostic medical devices	All	Central government authority for cybersecurity	-	National Cybersecurity Centre
		Manufacture of computer, electronic and optical products				
		Manufacture of electrical equipment				
		Manufacture of machinery and equipment n.e.c.				
		Manufacture of motor vehicles, trailers and semi-trailers				
		Manufacture of other transport equipment				
21.	Digital providers	-	All	Central government authority for cybersecurity	-	National Cybersecurity Centre
22.	Research	-	All	State administration	-	National CERT

				authority responsible for science and education		
23.	Education system	-	All	State administration authority responsible for science and education	-	National CERT

ANNEX IV

Mandatory Content of the National Strategic Planning Act in the Area of Cybersecurity

I

The national strategic planning act referred to in Article 55 of this Act shall set out:

– objectives and priorities of strengthening cybersecurity covering in particular the sectors and subsectors referred to in Annex I and Annex II to this Act, as well as the competent authorities referred to in Annex III to this Act

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

– policy frameworks for enhanced coordination between the competent authorities referred to in this Act and the competent authorities referred to in the legislation governing critical infrastructures, for the purpose of information sharing on risks, cyber threats, and incidents as well as on non-cyber risks, threats and incidents and the exercise of supervisory tasks

– a mechanism to identify relevant assets and an assessment of the cyber risks

– measures ensuring preparedness for, responsiveness to and recovery from cybersecurity incidents, including cooperation between the public and private sectors

– a plan, including necessary measures, to enhance the general level of cybersecurity awareness among citizens

– a plan, including necessary measures, to develop national cybersecurity capabilities

– a list of competent authorities, other public entities and all other entities involved in the implementation of the national strategic planning act in the area of cybersecurity.

II

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

– addressing cybersecurity issues in the supply chain for ICT products and ICT services used by entities to which this Act applies for the purpose of providing their services or performing their activities

– on the inclusion and specification of cybersecurity-related requirements for ICT products and ICT services in public procurement, including in relation to cybersecurity certification, encryption and the use of open-source cybersecurity products

– managing cyber vulnerabilities, encompassing the promotion and facilitation of coordinated cyber vulnerability disclosure under Article 54 of this Act

– related to sustaining the general availability, integrity and confidentiality of the public core of the open internet, including, where relevant, the cybersecurity of undersea communications cables

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

– promoting and developing education and training on cybersecurity, cybersecurity skills, awareness raising and research and development initiatives in the area of cybersecurity, as well as guidance on good cyber hygiene practices and controls, aimed at citizens, as well as public and private entities

– supporting academic and research institutions to research, develop, enhance and promote the deployment of cybersecurity tools and secure information and communication infrastructures, systems and applications

– including relevant procedures and appropriate information-sharing tools to support and ensure voluntary cybersecurity information sharing in accordance with the regulations governing the rules of access to and treatment of a particular type of information

– strengthening the cyber resilience and the cyber hygiene baseline of small and medium-sized enterprises, in particular those to which this Act does not apply, by providing easily accessible guidance and assistance for their specific needs and

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