LAW

ON INFORMATION SECURITY (ZINFV-1)

I. GENERAL PROVISIONS

Article 1

(content of the law)

(1) This Act regulates the field of information and cyber security and establishes the national information security system in the Republic of Slovenia. In doing so, it regulates the powers, tasks, organisation and operation of the competent national authority for information security (hereinafter referred to as: the competent national authority), the authority for managing major incidents and crises, the single point of contact for cybersecurity (hereinafter referred to as: the single point of contact) and computer security incident response teams (hereinafter referred to as: CSIRT teams), regulates the adoption of the Cybersecurity Strategy of the Republic of Slovenia, cyber defence and the cooperation of competent state authorities and CSIRT teams.

(2) In order to preserve key social and economic activities in the Republic of Slovenia, this Act also lays down measures for managing information and cyber security risks, as well as the reporting obligation of persons liable under this Act and the voluntary notification of incidents. It also regulates the rules and obligations regarding the exchange of information on cyber security and supervision, including for cyber security certification.

Article 2

(purpose of the law)

(1) The purpose of the Act is to systematically regulate the field of information and cybersecurity and to ensure a high level of cybersecurity, including strengthening trust in information and communication technology (hereinafter referred to as: ICT) products, ICT services and ICT procedures, and strengthening their security in the Republic of Slovenia in areas that are essential for the smooth functioning of the state and maintaining the provision of key social and economic activities.

(2) This Act transposes Directive 2022/2555 /EU into the legal order of the Republic of Slovenia. **of the European Parliament and of the Council of 14 December 2022 concerning measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972 and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (OJ L 333 of 27. 12. 2022, p. 80), last amended by Corrigendum (OJ L 90348 of 12. 6. 2024, p. 139), (hereinafter: Directive 2022/2555/EU).**

(3) This Act regulates the implementation of Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on the European Union Agency for Cybersecurity (ENISA) and on information and communication technology certification in the area of cybersecurity, and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (OJ L 151, 7.6.2019, p. 15), last amended by Regulation (EU) 2025/37 European Parliament

and of the Council of 19 December 2024 amending Regulation (EU) 2019/881 on managed security services (OJ L No. 2025/37 of 15. 1. 2025), (hereinafter referred to as: Regulation 2019 /881/EU).

(4) This Act regulates the implementation of 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, 8.6.2021, p. 1), (hereinafter referred to as: Regulation 2021/887/EU).

(5) This Act regulates the implementation of Regulation (EU) 2025/38 of the European Parliament and of the Council of 19 December 2024 laying down measures to strengthen solidarity and capabilities in the Union to detect, prepare for and respond to cyber threats and incidents and amending Regulation (EU) 2021/694 (Cyber Solidarity Act) (OJ L No. 2025/38 of 15. 1. 2025), (hereinafter: Regulation 2025/38/EU).

Article 3

(exclusion of application of the law)

(1) For essential and significant entities in the banking and infrastructure sectors financial market referred to in Annex 1 to this Act, Chapters IV and IX of this Act shall not apply.

(2) This Act shall not apply to entities that the Republic of Slovenia exempts from the scope 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, 27.12.2022, p. 1), as last amended by Commission Delegated Regulation (EU) 2024/1774 of 13 March 2024 supplementing Regulation (EU) 2022/2554 of the European Parliament and of the Council with regard to regulatory technical standards specifying tools, methods, procedures and policies for ICT risk management and a simplified framework for ICT risk management (OJ L 2024/1774 of 25.6.2024), (hereinafter referred to as: Regulation 2022/2554/EU) in accordance with the fourth paragraph of Article 2 of the said regulation.

(3) This Act shall not apply to those information and communication systems in which classified information is protected, for which the national security authority referred to in the Act regulating classified information has carried out a security assessment and issued a security authorisation for the operation of the system in accordance with the said Act. Regulations in the field of protection of classified information and rules for the protection of classified information of international associations or organisations of which the Republic of Slovenia is a member, or international agreements in the field of classified information concluded by the Republic of Slovenia, shall apply to these systems.

(4) Notwithstanding the previous paragraph, the national security authority referred to in the act regulating classified information shall report incidents in information and communication systems referred to in the previous paragraph to the competent national authority pursuant to this act.

(5) For an autonomous information and telecommunications system referred to in the law governing defence that is not covered by the third paragraph of this Article, the measures for risk management and incident notification referred to in Chapter IV of this Act shall apply mutatis mutandis.

Article 4

(data and information processing)

(1) The processing of personal data pursuant to this Act shall be carried out in accordance with the regulations governing the protection of personal data, and providers of public electronic communications networks or publicly available electronic communications services shall also carry out the processing of personal data in accordance with the regulations governing privacy in the field of electronic communica

(2) Data and information processed on the basis of this Act and defined as confidential, business secret or protected data shall be handled in accordance with the sectoral regulations governing their handling and protection.

(3) The exchange of protected data of the competent national authority for the purposes of implementing this Act must be limited to the extent that is appropriate and proportionate to the purpose of such exchange, while maintaining the confidentiality of the information and data concerned and protecting the security and business interests of the entities concerned. The Government shall determine the more detailed organisational and logical-technical procedures and measures for determining and protecting protected data of the competent national authority and for managing databases controlled by the competent national authority and containing protected data of the competent national authori

(4) When sending or exchanging data and information on the basis of this Act, (informal) non-disclosure agreements, such as the traffic light protocol, are also taken into account.

(5) The obligation to exchange data and information outside the Republic of Slovenia pursuant to this Act does not apply to public administration entities that carry out activities in the field of national security, where the disclosure of such data and information would endanger the vital interests of the Republic of Slovenia.

Article 5

(meaning of terms)

The terms used in this Act mean:

1. the central state information and communication system is a central state information and communication network or system managed by the ministry responsible for the management of information and communication systems, and is intended to connect local networks of state administration bodies and other entities for the purposes of implementing their legal obligations and accessing common information solutions and information and communication infrastructure on the basis of centralized management and control;

2. CSIRT is a team that responds to computer security incidents, receives reports of security breaches, conducts analyses and assists the notifiers in managing incidents;

3. digital service means any information society service or any service which is normally provided for remuneration, at a distance, electronically and at the individual request of the recipient of the service;

4. Logs are structured or unstructured records of events in network and information systems that enable the analysis and reconstruction of incidents or near-incidents;

5. electronic communications service is a service normally provided for remuneration over electronic communications networks, excluding services providing content or exercising editorial control over content transmitted over electronic communications networks and electronic communications services, and includes the following services:

– Internet access service: which is a publicly available electronic communications service that enables access to the Internet and thus connectivity to virtually all Internet endpoints, regardless of the network technology and terminal equipment used,

– interpersonal communication service and

– services which consist wholly or mainly of the transmission of signals, such as services transmissions used for the provision of machine-to-machine services and for broadcasting;

6. The European Cyber Crisis Coordination Network (hereinafter referred to as the EU-CyCLONe network) is a community that supports the coordinated management of large-scale cyber incidents and crises at the operational level and ensures the regular exchange of relevant information between the Member States of the European Union and the institutions, bodies, offices and agencies of the European Union, and is composed of representatives of the Member States' cyber crisis management authorities and, in some cases, also representatives of the European Commission, which participates as an observer;

7. European cybersecurity certificate is a document certifying that the ICT product, ICT service or ICT process in question has been assessed for compliance with specific security requirements set out in a European cybersecurity certification scheme;

8. financial incentive is the implementation of financing in the form of grants, covering the costs of supplying goods or services, or co-financing the costs of supplying goods or services to increase the level of cybersecurity;

9. Incident is an event that has compromised the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or services provided by or accessible through network and information systems;

10. information security means the protection and safeguarding of network and information systems and associated data against unauthorized access, use, disclosure, disruption, alteration or destruction, namely to ensure the confidentiality, authenticity, integrity and availability of the aforementioned systems and data;

11. security inspection is a procedure in which an inspector (hereinafter referred to as: inspector) identifies and assesses potential vulnerabilities in network and information systems at the obliged entity during the inspection procedure, tests the effectiveness of security measures or mechanisms and exposure to cyber threats, and also checks the adequacy of effective detection and handling of cyber incidents;

12. public electronic communications network is an electronic communications network that is used wholly or mainly for the provision of publicly available electronic communications services that support the transmission of information between network termination points;

13. cyber threat is any potential circumstance, event or action that could damage, disrupt or otherwise adversely affect networks and information systems, users of such systems and other persons;

14. Cyber hygiene is the good practice of maintaining security and protecting information in the digital environment. This includes measures and procedures designed to protect computer systems, networks and data from security threats;

15. a large-scale cyber incident is an incident that causes a disruption that exceeds the ability of the Republic of Slovenia to respond to it, or an incident that significantly affects at least two Member States of the European Union;

16. **Cyber defense is the set of measures, activities and capabilities of state authorities, local government authorities, companies, institutions and other organizations, and citizens that are necessary to protect and safeguard cyberspace against cyber threats and incidents;**

17. **Cyberspace is the global information environment formed by information systems and networks, data, digital devices and their users;**

18. **Cybersecurity means the activities necessary to protect network and information systems, the users of such systems and other persons affected by cyber threats;**

19. **The key parts of the national security system are the systems of defence, internal security, protection against natural and other disasters and subsystems of the national security system, which also includes foreign policy, economic, information and other activities that directly affect national security;**

20. **key information systems are all network and information systems with associated data of the liable party, without which the latter cannot continuously provide the services referred to in Annex 1 or 2 to this Act, the disruption of which could have a significant negative impact on key social or economic activities;**

21. **A crisis is a serious threat to fundamental values and social norms, characterised by time pressure and uncertain circumstances that require rapid decision-making and the implementation of measures that deviate from normal and prescribed institutional pathways and require the use of crisis management mechanisms;**

22. **control information systems are information systems that enable the control, regulation, automation or optimization of the operation of key industrial, technological or infrastructure processes of an entity;**

23. **a qualified trust service is a trust service that meets the relevant requirements set out in the law, which regulates electronic identification and trust services;**

24. **Cross-sectoral communities of obliged entities are communities of obliged entities that go beyond the functioning of sectoral communities of obliged entities and involve cooperation between them with the aim of pooling knowledge and experience in order to solve challenges that go beyond the framework of individual sectors;**

25. **The CSIRTs Network is a community that contributes to building trust and promotes rapid and effective operational cooperation between the Member States of the European Union, in which CSIRTs from the Member States of the European Union, the Computer Emergency Response Team for the European Union institutions, bodies and agencies (CERT-EU) and the European Commission as an observer participate;**

26. **supervisory information systems are information systems in which the management and control of the operation of the entity's networks and information systems are carried out, including the detection of security events, anomalies and threats and the response to them;**

27. **internal auditor (hereinafter referred to as: internal auditor) is a certified internal auditor (hereinafter referred to as: certified internal auditor) who has obtained a professional title from the Slovenian Institute of Auditors and is entered in its register of active certified internal auditors or a person who has obtained the title of state internal auditor or certified state internal auditor;**

28. Incident management is all actions and procedures intended to prevent, detect, analyzing and containing incidents or responding to and recovering from them;

29. Threatening the vital interests of the Republic of Slovenia means threatening its constitutional order, independence, territorial integrity, defense capability and public security;

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

31. network and information system:

– is an electronic communications network as defined in the law governing electronic communications communications,

– is any device or group of interconnected or related devices, one or more performs automatic processing of digital data based on the program, or

– covers digital data that the elements referred to in the first and second indents of this point store, process, retrieve or transmit for the purposes of their operation, use, protection and maintenance;

32. conformity assessment body for the purposes of this Act is a conformity assessment body referred to in the Act regulating technical requirements for products and conformity assessment, which meets the additional requirements set out in the Annex to Regulation 2019/881/EU;

33. A social networking service platform is a platform that enables end users to connect, share content, get to know each other and communicate with each other across multiple devices, in particular through chats, posts, videos and messages;

34. a significant cyber threat is a cyber threat that, given its technical characteristics, can be assumed to have a serious negative impact on the network and information systems of an entity or on the users of its services, causing significant material or non-material damage;

35. qualified trust service provider is a trust service provider that provides one or more trust services and is granted qualified status by a supervisory authority;

36. Domain Name System service provider (hereinafter referred to as: DNS service provider) is an entity that performs:

– publicly available recursive domain name resolution services for end-users Internet users or

– authoritative domain name resolution services for use by third parties, except for root name servers.

37. trust service provider is a natural or legal person that provides one or more trust services, as a qualified or non-qualified trust service provider;

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, through assistance or active management, carried out either on-site or remotely;

39. Managed security service provider is a managed service provider that performs or provides assistance for activities related to cybersecurity risk management;

40. ICT process is a set of activities carried out to design, develop, deliver or maintain an ICT product or service;

41. connected entity is an entity that connects to the central state information and communication system;

42. ICT product is an element or group of elements of a network or information system;

43. the representative referred to in Chapter V of this Act is a natural or legal person established in a Member State of the European Union, where that person is expressly appointed to act on behalf of a DNS service provider, a top-level domain (hereinafter referred to as: TLD) registry, an entity providing domain name registration services, 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, online search engine or social networking service platform not established in a Member State of the European Union, with whom the competent authority or the CSIRT may contact instead of the entity concerned in relation to the obligations of the entity concerned under this Act;

44. Vulnerability is a deficiency, susceptibility or fault in an ICT product or service that a cyber threat can exploit;

45. A research organisation is, regardless of the law governing scientific research activity, an entity that devotes the main part of its activities to the conduct of applied research or experimental development with the aim of using the results of such research for commercial purposes, but does not include academic and other educational institutions;

46. top-level domain name registry (hereinafter referred to as: TLD registry) is an entity to which a specific top-level domain has been assigned and which is responsible for its management, including the registration of domain names under the top-level domain and the technical management of the top-level domain, including the management of its name servers, the maintenance of its databases and the distribution of the top-level domain zone files across name servers, regardless of whether any of these activities is performed by the entity itself or by external providers, excluding cases in which the TLD registry uses the top-level domain names solely for its own needs;

47. An audit trail is an immutable trace or set of data about an event that occurred in an information system or device, with a precise timestamp;

48. information systems auditor is a certified information systems auditor with appropriate auditing knowledge who has obtained a professional title from the Slovenian Institute of Auditors and is entered in its register of active certified information systems auditors;

49. Sectoral communities of obliged entities are groups of obliged entities operating in the same sector and focusing on a specific sector with the aim of exchanging information, cooperating and solving common challenges;

50. The traffic light protocol is a set of rules and agreements on restrictions regarding the further dissemination of received or shared information, as used in CSIRT information exchange;

51. Domain Name System (hereinafter referred to as: DNS) is a hierarchically distributed naming system that enables the identification of Internet services and resources and enables end-user devices to access these services and resources using Internet routing and connectivity services;

52. A near-miss is an event that could have compromised the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or services provided by or accessible through network and information systems, but which was successfully prevented from occurring or did not occur;

53. The administrator of an information and communication system is the person responsible for managing, maintenance and protection of the information system in the organization;

54. The Cooperation Group is a group that supports and facilitates strategic cooperation and information exchange between the Member States of the European Union and strengthens trust between them, and is composed of representatives of the Member States of the European Union, the European Commission and the European Union Agency for Cybersecurity (hereinafter referred to as the ENISA Agency), and the European External Action Service as observers;

55. A web search engine is a digital service that allows users to enter queries to perform a search across all websites or all websites in a specific language, based on a query on any topic in the form of a keyword, voice request, phrase or other input, and provides results in any format with information about the requested content;

56. online marketplace means a service that uses software, including a website, part of a website or an application, operated by a trader or someone on his behalf, and that enables consumers to conclude distance contracts with other traders or consumers;

57. A standard is a technical specification adopted by a recognised standardisation body for repeated or continuous use, with which compliance is not mandatory, and which falls into one of the following categories:

– international standard means a standard adopted by an international body for standardization,

– European standard means a standard adopted by a European organisation for standardization,

– harmonised standard means a European standard adopted on the basis of a request from the European the Commission for the application of European Union harmonisation legislation,

– national standard means a standard adopted by a national standardisation body;

58. network junction is a network facility that enables the interconnection of more than two independent networks (autonomous systems), primarily for the purpose of exchanging Internet traffic, and that provides interconnection only to autonomous systems, does not require the exchange of Internet traffic between any participating autonomous systems to pass through a third autonomous system, and does not modify or otherwise interfere with such traffic;

59. ICT service is a service that consists wholly or mainly of the transmission, storage, retrieval or processing of information via networks and information systems;

60. Data center service is a service that includes structures or groups of structures intended for the centralized placement, interconnection and operation of information technology and network equipment, for storage, processing and

data transmission, together with all facilities and infrastructures to ensure uninterrupted electricity supply and ensure the required environmental conditions in the data center;

61. cloud service is a digital service that enables on-demand management and broad remote access to a flexible and scalable set of shareable computing resources, even when those resources are distributed across multiple locations;

62. A trust service is an electronic service that is generally provided for a fee and includes:

– creation, verification and validation of electronic signatures, electronic seals or electronic time stamps, electronic registered delivery services and certificates related to these services, or

– creating, verifying and validating certificates for website authentication or

– storage of electronic signatures, seals or certificates related to these services;

63. An entity providing domain name registration services is a registrar or an agent acting on behalf of a registrar, such as a privacy registration service provider or an agent or reseller;

64. entity is a person governed by public or private law;

65. public administration entities are public administration entities at the state and local level that are established by a public law act, except for judicial authorities, the State Prosecutor's Office, the Constitutional Court of the Republic of Slovenia, the National Assembly of the Republic of Slovenia, the National Council of the Republic of Slovenia and the Bank of Slovenia;

66. Public administration entities at the state level are ministries, bodies within their composition, government services and administrative units, and those public infrastructure institutions established in accordance with the law regulating scientific research and innovation activities. They also include other public administration entities from Annex 3, which as an Annex is an integral part of this Act

67. Public administration entities at the local level are municipalities;

68. technical specification means a technical specification for information and communication technology;

69. third country is a country that is not a member of the European Union or a country that is not a signatory to the Agreement establishing the European Economic Area (OJ L 1 of 3 January 1994, p. 3);

70. Risk is the possibility of loss or disruption due to an incident and is expressed as a combination of the magnitude of the loss or disruption and the probability that the incident will occur;

71. A secure location is a location that is resistant to environmental influences, climate change and other risks that could threaten the safe handling of incidents and the protection of information and system resources;

72. Security of network and information systems is the ability of network and information systems to prevent, at a given level of confidence, any event that may compromise the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or services provided by or accessible through these network and information systems;

73. the security operations centre of a state administration body is an internal organisational unit of an individual state administration body that responds to incidents in the field of information security and meets the conditions set out in this Act;

74. Protected information of the competent national authority is information on the vulnerabilities or status of the information systems and networks of the obliged entities and their identity, which is not confidential or a trade secret, and its disclosure to unauthorized persons could cause disruptions to the functioning and performance of the tasks of the competent national authority or could harm taxpayers.

II. OBLIGATORS

Article 6

(obligors)

(1) Obligors under this Act are entities that fall within the types of entities listed in Annex 1 or Annex 2, which as Annexes form an integral part of this Act (hereinafter referred to as Annex 1 or 2 of this Act), if they have:

– at least 50 employees and

– annual turnover or annual balance sheet total of at least 10 million euros.

(2) The entities referred to in the previous paragraph are liable under this Act, regardless of the number of employees or annual turnover or annual balance sheet total, if:

1. they provide the service as:

- **providers of public electronic communications networks or publicly available electronic communication services,**
- **trust service providers,**
- **TLD name registries and DNS service providers;**

2. the entity is the sole provider of a service or activity in the Republic of Slovenia, the performance of which places it among the types of entities from Annex 1 or 2;

3. a disruption in the provision of the entity's service could have a significant impact on public order, public security or public health;

4. a disruption in the provision of the entity's service could create systemic risk, in particular for sectors listed in Annex 1 or 2 where such disruption could have a cross-border impact;

5. the entity has a special importance at the national or local level for an individual sector from Annex 1 or 2 or for the provision of an individual service, which classifies it among the types of entities from Annex 1 or 2 or due to interdependence with other sectors from Annex 1 or 2 in the Republic of Slovenia;

6. it is a public administration entity at the state level.

(3) Notwithstanding the first and second paragraphs of this Article, the following are also liable under this Act:

1. entities designated as critical under the law governing critical infrastructure;

2. entities providing domain name registration services, regardless of their size;

3. entities that are defined as services of national importance in national protection and rescue plans, if the failure of their network and information systems would jeopardize the implementation of protection and rescue tasks from the aforementioned plans, and

4. urban municipalities as public administration entities at the local level.

(4) Notwithstanding the previous paragraphs, other natural and legal persons falling within the scope of Regulation 2019/881/EU are also obliged to implement Article 27 of this Act, which refers to cybersecurity certification, **namely in the part of the aforementioned regulation that regulates the cybersecurity certification framework.**

(5) Notwithstanding the previous paragraphs, the Bank of Slovenia is not a party liable under this Act.

Article 7

(essential and important entities)

(1) The liable entities referred to in the previous article, with the exception of the entities referred to in point 2 of the third paragraph and the fourth paragraph, are divided into essential and significant entities.

(2) The essential entities are:

1. types of entities listed in Annex 1 that have at least 250 employees or an annual turnover of at least 50 million euros or an annual balance sheet total of at least 43 million euros,

2. qualified trust service providers and TLD name registries and DNS service providers, regardless of their size,

3. providers of public electronic communications networks or publicly available electronic communications services that have at least 50 employees and an annual turnover or annual balance sheet total of at least EUR 10 million,

4. public administration entities at the state level,

5. all other types of entities from Annex 1 to this Act, which are determined by the government by decision on the basis of points 2 to 5 of the second paragraph of the previous article and at the proposal of the competent national authority,

6. entities designated as critical under the law governing critical infrastructure;

7. entities from sector 9. ICT service management from Annex 1 and not entities from points 1 to 6 of this paragraph, which are determined by the government on the proposal of the competent national authority.

(3) Significant entities are:

– the types of entities referred to in Annex 2 to this Act, including those determined by the government by decision on the basis of points 2 to 5 of the second paragraph of the previous article and at the proposal of the competent national authority,

– entities referred to in point 3 of the third paragraph of the previous article, which are determined by the government by decision at the proposal of the competent national authority. The competent national authority prepares a proposal based on the initiative of the Administration of the Republic of Slovenia for Protection and Rescue, which contains a list of the names of the entities concerned, and

– other entities or bodies referred to in the previous article that are not essential entities pursuant to the previous paragraph.

(4) For the implementation of point 7 of the second paragraph of this Article, the Bank of Slovenia, the Securities Market Agency and the Insurance Supervision Agency shall send to the competent national authority a list of names of entities providing ICT service management services referred to in Annex 1 to this Act in the area of sector 3. Banking or 4. Financial market infrastructures referred to in Annex 1.

(5) No appeal is permitted against the decisions referred to in point 5 of the second paragraph and in the first and second indents of the third paragraph of this Article, but an administrative dispute is permitted.

Article 8

(self-registration and list of taxpayers)

(1) The competent national authority shall establish a mechanism for self-registration of taxable persons referred to in Article 6 of this Act, except for taxable persons referred to in the fourth paragraph of Article 6 of this Act and for entities referred to in the first paragraph of Article 3 of this Act.

(2) Taxpayers for whom the self-registration mechanism referred to in the previous paragraph has been established must register through this mechanism within thirty days of the date on which the circumstances arose on the basis of which they meet the criteria referred to in Articles 6 and 7 of this Act. Notwithstanding this, the thirty-day period for self-registration for those taxpayers who have been served with the decision referred to in point 5 of the second paragraph or in the first or second indent of the third paragraph of the previous Article shall run from the date on which the decision was served. Taxpayers shall provide at least the following information upon self-registration:

1. about the name and address, contact details, personal identification number and email address of the taxpayer for serving,

2. on the relevant sector and subsector from Annex 1 or 2 of this Act in which the taxable person provides the types of services from these Annexes, or the category of taxable persons not included in the said Annexes but who are taxable persons pursuant to the third paragraph of Article 6 of this Act,

3. an indication of whether the entity has at least 50 employees and an annual turnover or balance sheet total of at least EUR 10,000,000.00,

4. an indication of whether the entity has at least 250 employees or an annual turnover of at least EUR 50,000,000.00 or annual balance sheet total of at least 43,000,000.00 euros,

5. the contact person for information security and their deputy and their contact details, including email addresses and telephone numbers,

6. about allocated blocks of public IP addresses,

7. on the list of European Union Member States where services falling within the scope of this Act are provided, and

8. on the registered numbers of autonomous systems and all domain names used by the liable party in its business operations.

(3) Regardless of the set of information referred to in the previous paragraph, the entities referred to in the first paragraph of Article 32 of this Act shall provide the set of information referred to therein upon self-registration referred to in the previous paragraph.

(4) On the basis of the information of the obliged entities referred to in the second or third paragraph of this Article and taking into account the second and third paragraphs of the previous Article, the competent national authority shall establish a list of essential and significant entities and entities providing domain name registration services. This list, which contains the information of the obliged entities referred to in the second or third paragraph of this Article, shall be protected information of the competent national authority and shall be reviewed by the competent national authority regularly or at least every two years and updated as necessary. The competent national authority shall also provide access to the list, in the part relating to the obliged entities within its jurisdiction, to the competent CSIRTs.

(5) The taxpayers referred to in the second paragraph of this Article shall, using the self-registration mechanism, report any changes to the data submitted pursuant to the second or third paragraph of this Article no later than ten working days from the date of the change. The relevant changes shall be transferred to the list referred to in the previous paragraph without delay.

(6) Notwithstanding the previous paragraph, an entity referred to in the second paragraph of this Article that considers that it is no longer a taxable person shall notify the competent national authority of this and the reasons for such a determination, which shall verify its statements and, upon confirmation of the reasons in the self-registration mechanism and in the list referred to in the fourth paragraph of this Article, shall note with the entity concerned that this entity is no longer a taxable person, and shall inform the entity concerned thereof. In the event that the taxable person to whom the decision referred to in point 5 of the second paragraph or in the first or second indent of the third paragraph of the previous Article has been issued considers that it no longer meets the conditions for its issuance, it shall notify the competent national authority thereof, which, upon confirmation of the cessation of these conditions, shall propose to the government that its decision in question be revoked. If the government revokes the decision in question, the competent national authority, after being served with the revocation decision, shall note with the entity concerned that this entity is no longer a taxable person, and shall inform the entity concerned thereof.

(7) Notwithstanding the second paragraph of this Article, the Bank of Slovenia, the Securities Market Agency and the Insurance Supervision Agency shall send to the competent national authority a list of names of financial entities referred to in Regulation 2022/2554/EU, who are entities referred to in the first paragraph of Article 3 of this Act, within thirty days of their identification. They shall inform the competent national authority of any changes to the list within the same period.

(8) The competent national authority shall immediately include the information referred to in the previous paragraph in the list referred to in the fourth paragraph of this Article.

(9) For the purposes of implementing this Article, the competent national authority shall obtain, free of charge, the data of the persons liable under the second paragraph of this Article from the Business Register of Slovenia database managed by the Agency of the Republic of Slovenia for Public Legal Records and Services.

III. ORGANIZATION OF THE NATIONAL INFORMATION SECURITY SYSTEM

Article 9

(cybersecurity strategy)

(1) The Government shall adopt a cybersecurity strategy (hereinafter referred to as: the strategy), which shall be a framework for implementing measures to establish an effective national system for ensuring information or cybersecurity security. The strategy shall include:

1. objectives and priorities of the strategy;

2. a governance framework for achieving the objectives and implementing the priorities referred to in the previous point, including the policies referred to in the second paragraph of this article;

3. a governance framework that defines the roles and responsibilities of relevant cybersecurity stakeholders at the national level, supports cooperation and coordination at the national level between the competent national authority, the single point of contact and the CSIRTs referred to in this Act, and supports coordination and cooperation between these authorities and competent authorities on the basis of sectoral legal acts of the European Union or sectoral legislation transposing these acts into the Slovenian legal order;

4. a mechanism for identifying appropriate resources and assessing risks;

5. definition of measures to ensure preparedness for incident response and recovery them, including cooperation between the public and private sectors;

6. a list of authorities, organisations and stakeholders involved in the implementation of the strategy;

7. a policy framework for enhanced coordination between the competent national authority referred to in this Act and the competent national authority referred to in the Act regulating critical infrastructure, for the purposes of exchanging information on risks, cyber threats and incidents and on non-cyber risks, threats and incidents and carrying out supervisory tasks;

8. a policy framework for enhanced coordination between the competent national authority referred to in this Act and the authority which, by decision of the Government, is the central authority for monitoring and coordinating the response to hybrid threats in the Republic of Slovenia (hereinafter referred to as: the central authority for responding to hybrid threats), for the purposes of exchanging information on risks, cyber threats and incidents, and on non-cyber risks, threats and incidents that would indicate hybrid activity;

9. a plan, including necessary measures, to increase general awareness of citizens about cybersecurity.

(2) The strategy includes the following policies:

1. on addressing cybersecurity in the supply chain of ICT products and services used by entities to provide their services;

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

3. on vulnerability management, including promoting and facilitating coordinated disclosure vulnerabilities pursuant to the first paragraph of Article 17 of this Act;

4. related to maintaining the general availability, integrity and confidentiality of the public core of the open Internet, including the cybersecurity of submarine communication cables;

5. on promoting the development and integration of appropriate advanced technologies for the implementation of state-of-the-art risk management measures in the field of cybersecurity;

6. on promoting and developing cybersecurity education and training, cybersecurity skills, awareness-raising, cybersecurity research and development initiatives, and guidelines on good practices and cyber hygiene controls for citizens, stakeholders and entities;

7. on supporting academic and research institutions in developing and improving cybersecurity tools and secure network infrastructure and promoting their deployment;

8. on the inclusion of appropriate procedures and appropriate tools to support the voluntary exchange of cybersecurity information between entities in accordance with European Union law;

9. on strengthening the cyber resilience and basic cyber hygiene of small and medium-sized enterprises, in particular those excluded from the scope of this Act, by providing easily accessible guidance and assistance for their specific needs;

10. on promoting active cyber protection.

(3) The competent national authority shall notify the European Commission thereof within three months of the adoption of the strategy referred to in this Article. In doing so, it may exclude information referred to in points 5, 7 and 8 of the first paragraph that is important for national security.

(4) The competent national authority shall assess the strategy on an ongoing and regular basis, at least every five years, on the basis of key performance indicators resulting from the achievement of the objectives and priorities of the strategy.

Article 10

(competent national authority)

(1) The competent national authority is the Office of the Government of the Republic of Slovenia for Information security.

(2) The competent national authority shall carry out the following tasks:

1. coordinates the operation of the national information security system;

2. develops capabilities for implementing cyber defence;

3. provides professional support to all obliged entities in the performance of their tasks in the field of information security;

4. provides analyses, methodological support and preventive action in the field of information security security and provides opinions within its area of competence;

5. cooperates with authorities and organizations operating in the field of information security, in particular with CSIRT teams, security operations centers, regulators or supervisors of sectors from Annexes 1 and 2 of this Act, the Information Commissioner, law enforcement authorities and security solution providers;

6. makes those liable aware of the importance of reporting an incident with all signs of a criminal offence that is prosecuted ex officio to law enforcement authorities, in accordance with the Criminal Code;

7. coordinates training, exercises and education in the field of information security and ensures the strengthening of public awareness of information security, and may also organize and conduct training in the field of information and cybersecurity;

8. encourages and supports research and development in the field of information security;

9. is responsible for the preparation and implementation of the strategy;

10. develop and maintain a national plan for responding to cyber incidents, large-scale cyber incidents and crises, taking into account the strategy, plans of CSIRT teams, other competent authorities and security documentation of obliged entities;

11. reviews the adequacy of the determination of liable persons referred to in point 5 of the second paragraph and the first and second indents of the third paragraph of Article 7 of this Act at least every two years and may propose to the government to update the list of liable persons;

12. prepares anonymized information on reported incidents twice a year for statistical and public information purposes, and then publishes it publicly on the central website of the state administration;

13. professional and advisory tasks and tasks of a coordinator in the field of public relations, which include communication with external and internal publics and crisis communication in the event of an incident;

14. in cooperation with the government service responsible for public communication, produces and maintains national incident communication plan;

15. is a single point of contact that plays a coordinating role in the field of cybersecurity and defence to ensure cross-border cooperation with other countries and international organisations;

16. represents and advocates the interests of the Republic of Slovenia in working groups in the field of cybersecurity and defence within the framework of the Council of the European Union, the European Commission, the ENISA agency, NATO and other international organisations;

17. appoints and seconds its representatives to working groups, committees and networks in the field of cybersecurity and defence within the framework of the Council of the European Union, the European Commission, the ENISA agency, NATO and other international organisations;

18. is a member of the Cooperation Group, to which it appoints its representatives, and ensures the conditions for their efficient and successful operation;

19. Appoint representatives to the EU-CyCLONe network;

20. participates in activating the provision and acceptance of assistance for crisis management in accordance with international treaties and agreements;

21. appoints a representative to the Management Board of ENISA and participates in its work;

22. fulfils other obligations arising from directly applicable acts of the European Union in the field of cybersecurity;

23. fulfils the obligations to inform the European Commission, ENISA, NATO and the Cooperation Group, as well as the obligations to inform other international organisations;

24. leads the interdepartmental coordination working group for international cooperation in the field of cybersecurity and defense;

25. performs other tasks of international cooperation;

26. performs inspection tasks under this Act through the Information Security Inspectorate security, which is its internal organizational unit;

27. prepares proposals for regulations in the field of information and cybersecurity;

28. performs the tasks of the national cybersecurity certification body;

29. is the National Coordination Center for Cybersecurity;

30. as a recipient or allocator of funds, participates in funding programmes at the national and European Union levels and other international connections in the field of information and cybersecurity;

31. grants financial incentives for the implementation of selected projects in the field of information and communication technology cybersecurity;

32. finances staff scholarships for work in the competent national authority, in accordance with the law governing scholarships;

33. decides on participation in peer reviews;

34. determine a uniform information security policy, except for information and communication systems intended for the areas of defence, protection against natural and other disasters, police, internal information system for internal affairs, intelligence and security activities, foreign affairs, prevention and detection of money laundering and terrorist financing, and the performance of payment transactions for budget users, and

35. is the National Cyber Hub in accordance with the first, second and third paragraphs of Article 4 of Regulation 2025/38/EU, which participates in the cross-border cyber hub pursuant to the fourth paragraph of the said Article of this Regulation and in the European Cybersecurity Alert System referred to in Article 3 of the said Regulation, and

36. performs other tasks specified by this Act or other regulations.

Article 11

(national coordination center for cyber security)

(1) The competent national authority is the National Cybersecurity Coordination Centre (hereinafter referred to as: NCC-SI) and in this capacity is responsible for carrying out the tasks referred to in 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, 8.6.2021, p. 1).

(2) In accordance with the EU regulation referred to in the previous paragraph, NCC-SI carries out tasks to strengthen cybersecurity, including promoting research, technological development and industrial capacity in this area, and cooperates with the European Cybersecurity Centre and other national cybersecurity coordination centres of the Member States of the European Union.

Article 12

(cyber crisis management authority)

(1) The competent authority for the management of large-scale cyber incidents and crises (hereinafter referred to as: the cyber crisis management authority) in the Republic of Slovenia is the competent national authority which, in this capacity, is responsible for participating in the EU-CyCLONe networ

(2) The Cyber Crisis Management Authority shall develop a national response plan for cyber incidents, large-scale cyber incidents and crises (hereinafter referred to as: national response plan).

(3) The Government shall adopt a national response plan, which shall define the objectives and arrangements for managing cyber incidents, large-scale cyber incidents and crises. This plan shall specify in particular:

1. objectives of national preparedness measures and activities,

2. tasks and responsibilities of authorities for managing cyber incidents, cyber large-scale incidents and crises,

3. procedures for managing cyber incidents and large-scale cyber incidents dimensions,

4. procedures for managing cyber crises in a way that complies with regulations in the field crisis management and leadership,

5. preparedness measures, including exercises and training,

6. relevant public and private stakeholders and infrastructure involved,

7. procedures for cooperation between the cyber crisis management authority and the authorities referred to in the regulation in the field of crisis management and crisis management with the aim of effective cooperation of the Republic of Slovenia and its support in the coordinated management of large-scale cyber incidents and crises at the level of the European Union and

8. cooperation procedures between the cyber crisis management authority and the central authority for responding to hybrid threats with a view to effective coordination in responding to hybrid threats.

(4) Upon detection of cyber incidents that it deems may cause a crisis, the Cyber Crisis Management Authority shall immediately notify the National Security Council (hereinafter referred to as: SNAV) and the central authority for responding to hybrid threats. In cooperation with the affected parties under this Act, the competent sectoral regulators and the relevant bodies of the critical infrastructure sectors referred to in the Act regulating critical infrastructure, and the central authority for responding to hybrid threats, it shall analyse the situation and inform SNAV of the findings and, if necessary, propose measures. SNAV shall prepare an assessment of the situation on the basis of the regulation governing the field of crisis management and crisis management. Based on the assessment, it shall advise the government on further measures.

(5) The Government may, at the proposal of SNAV, adopt a decision to involve other state capacities in crisis management, declare a crisis and, if necessary, adopt a decision to implement crisis management and leadership in a complex crisis in accordance with the law governing the Government of the Republic of Slovenia.

(6) The competent national authority shall notify the European Commission of the designation of the cyber crisis management authority and of any changes thereto. It shall submit to the European Commission and the EU-CyCLONe network relevant information on the adoption of the national response plan in relation to the requirements referred to in the third paragraph of this Article. The data and information referred to in the fifth paragraph of Article 4 of this Act shall be excluded from the transmission.

(7) If the public needs to be informed in connection with the implementation of this Article, the competent national authority, together with the government service responsible for communicating with the public, shall prepare a statement for public release, which may only be published by the media in an unaltered form.

Article 13

(computer security incident response teams)

(1) The CSIRT groups and their responsibilities for handling incidents of individual groups of obliged entities shall be determined by the government. Among the CSIRT groups thus determined, the government shall also determine the CSIRT group that is the coordinator for coordinated vulnerability disclosure in the Republic of Slovenia pursuant to Article 17 of this Act.

(2) CSIRTs must meet the requirements set out in Article 14 of this Act and are responsible for handling incidents in accordance with the procedure set out in this Act.

(3) CSIRTs shall exchange information with essential and relevant entities and other relevant stakeholders using an appropriate, secure and resilient communication and information infrastructure established by the competent national authority, and shall cooperate with the competent national authority in the implementation and use of tools for secure information exchange.

(4) CSIRTs shall cooperate with each other and, in accordance with Article 34 of this Act, exchange relevant information with sectoral or cross-sectoral communities of taxpayers.

(5) CSIRTs shall participate in peer reviews in accordance with Article 19 of this Act.

(6) CSIRTs participate in the CSIRT network, but may also participate in other networks. for international cooperation.

(7) CSIRTs may cooperate with CSIRTs from third countries. In doing so, they may exchange information with these third country teams using appropriate protocols, including the semaphore protocol, to ensure an efficient, effective and secure way of exchanging information. CSIRTs may exchange appropriate information with CSIRTs from third countries, including personal data, in accordance with the provisions of Chapter 10 of the Personal Data Protection Act (Official Gazette of the Republic of Slovenia, No. 163/22).

(8) CSIRTs may cooperate with CSIRTs from third countries or equivalent third country authorities, in particular to provide assistance in the field of cybersecurity.

(9) The competent national authority shall immediately inform the European Commission of the identity of the CSIRTs referred to in the first paragraph of this Article and the responsibilities referred to in the second and third paragraphs of this Article and of any changes in the identities and responsibilities of the essential and relevant entities. It shall also inform the European Commission of the identity of the CSIRT designated as the coordinator referred to in the first paragraph of Article 17 of this Act.

Article 14

(requirements and technical capabilities of CSIRTs)

The CSIRTs referred to in the first paragraph of the previous article must meet the following requirements: requirements:

1. Ensure a high level of availability of their own communication channels by preventing single points of failure and having multiple ways for others to contact them and for them to contact others at any time. They clearly define the communication channels and inform users and partners about them;

2. premises and supporting information systems are in secure locations;

3. have an appropriate system for managing and routing claims, in particular to facilitate their efficient and effective submission;

4. ensure the confidentiality and reliability of their activities;

5. have sufficient staff to ensure continuous availability of services, with ensure that this staff is appropriately trained, and

6. have backup systems and a backup workspace to ensure the continuity of their services.

Article 15

(tasks of CSIRTs)

(1) The CSIRTs referred to in the first paragraph of Article 13 of this Act shall perform the following tasks in the areas for which they are responsible:

1. monitoring and analyzing cyber threats, vulnerabilities and incidents at the national level, and, at the request of essential and important entities, providing them with assistance in relation to the real-time monitoring of their network and information systems;

2. Providing early warning, alerts, notifications and dissemination of information on cyber threats, vulnerabilities and incidents to relevant essential and significant entities, the competent national authority and other competent authorities, central hybrid response bodies and other relevant stakeholders, where possible, promptly;

3. Responding to incidents and providing assistance to relevant essential and important subjects;

4. collecting and analyzing forensic data and performing dynamic risk analyses; and incidents and situational awareness in the field of cybersecurity;

5. at the request of a significant or important entity, conducting a proactive review of the network and information systems of the entity concerned to identify vulnerabilities that could have a significant adverse impact;

6. participating in the CSIRT network and providing mutual assistance, in accordance with their capabilities and competences, to other members of the CSIRT network upon their request;

7. contributing to the use of tools for secure information exchange pursuant to the third paragraph of Article 13 of this Act and

8. providing mutual assistance and cooperation with other authorities that are based on regulations responsible for handling incidents.

(2) CSIRTs may conduct proactive and unobtrusive reviews of publicly accessible network and information systems of essential and important entities for which they are responsible, with the aim of detecting vulnerabilities in network and information systems that are not configured in a secure manner and to inform the relevant entities with the aim of eliminating security threats. Such reviews shall not adversely affect the operation of the services of these entities.

(3) When carrying out the tasks referred to in the first paragraph of this Article, CSIRTs may prioritize tasks based on a risk-based approach.

(4) CSIRTs shall submit to the competent national authority a weekly and quarterly report on the performance of their tasks, including information on all reported incidents they have handled.

(5) CSIRTs shall immediately notify the competent national authority of their own incident that may affect or has an impact on the operation and availability of their services provided to obliged entities and voluntary notifiers.

(6) In accordance with the guidelines of the competent national authority, the CSIRT team shall, in the event of a high or critical threat assessment, issue a security notice or instruction in accordance with paragraphs 5 and 6 of Article 37 of this Act.

(7) The CSIRT referred to in the first paragraph of Article 13, which is responsible for handling incidents of public administration entities at the state and local level, is authorised to have direct, necessary and proportionate access to the operation of the information infrastructure of the central state information and communication system for the purpose of effectively carrying out information and cyber security and cyber defence tasks. The operator of the central state information and communication system must enable it to do so.

(8) For the purpose of responding to cyber threats in a timely manner and preventing the harmful consequences of a potential serious or critical incident, and for implementing cyber defence, the CSIRT referred to in the previous paragraph is authorised to order the operator of the central national information and communication system to take appropriate, urgent and proportionate measures, which the operator must implement immediately or within a set deadline in its information and communication system.

(9) The CSIRTs referred to in the first paragraph of Article 13 of this Act shall also implement awareness-raising programmes in accordance with the cybersecurity strategy.

Article 16

(CSIRTs collaborating with private sector stakeholders)

(1) The CSIRTs referred to in the first paragraph of Article 13 of this Act shall cooperate with private sector entities to achieve the objectives of this Act. They may also conclude cooperation agreements for this purpose.

(2) To facilitate the cooperation referred to in the previous paragraph, CSIRTs shall encourage the adoption and use of common or established practices, classification systems and taxonomies in relation to:
with:

– incident management procedures,

– crisis management and

– coordinated vulnerability disclosure based on the first paragraph of Article 17 of this Act.

(3) A CSIRT team that detects a vulnerability in the information and communication system of an entity referred to in the first paragraph of this Article shall immediately notify the entity thereof.

Article 17

(harmonised vulnerability disclosure and European vulnerability database)

(1) The CSIRT referred to in the first paragraph of Article 13 of this Act, which is designated as the coordinator for coordinated vulnerability disclosure in the Republic of Slovenia (hereinafter referred to as: the coordinator), acts as a trusted intermediary and, where necessary, facilitates cooperation between a natural or legal person reporting vulnerabilities and the manufacturer or provider of ICT products or services that are said to contain the vulnerability, at the initiative of either party.

(2) The tasks of the coordinator include:

– identification of the relevant entities and establishing contact with them,

– supporting natural or legal persons who report vulnerabilities, and

– negotiating disclosure timelines and managing vulnerabilities that affect multiple entities.

(3) Natural or legal persons referred to in the first paragraph of this Article may report vulnerabilities to the coordinator anonymously. The coordinator shall ensure careful follow-up of the reported vulnerabilities and the anonymity of the natural or legal person who reported the vulnerability.
Where the reported vulnerability could have a significant impact on entities in other Member States of the European Union, the coordinator shall, where necessary, cooperate with other CSIRTs designated as coordinators within the CSIRTs network.

(4) The coordinator shall also cooperate with ENISA regarding reported vulnerabilities.

(5) The coordinator shall send the competent national authority a weekly report on the implementation of its tasks referred to in this Article, including information on all detected vulnerabilities referred to in the first paragraph of this Article.

Article 18

(cooperation at national level)

(1) In order to ensure the effective performance of the tasks and obligations of the competent national authority, the single point of contact and the CSIRT referred to in this Act, the competent national authority shall establish appropriate cooperation at national level in such a way that these entities:

1. cooperate with each other in fulfilling their obligations;

2. cooperate with the Civil Aviation Agency of the Republic of Slovenia, the Nuclear Safety Administration of the Republic of Slovenia, the Information Society Inspectorate, the Bank of Slovenia, the Agency for Communications Networks and Services of the Republic of Slovenia and the competent national authority from the act regulating critical infrastructure, as well as competent authorities or sectoral regulators from other sectoral acts in the areas to which the obliged entities from Article 6 of this Act belong;

3. cooperate with law enforcement authorities and the Information Commissioner, unless this is detrimental to the exercise of supervisory or decision-making powers by these authorities;

4. regularly cooperate with the competent national authority referred to in the law governing critical infrastructure and exchange information on the identification of critical entities, on risks, cyber threats and incidents, and on non-cyber risks, threats and emergencies in the area of critical infrastructure affecting essential entities defined as critical entities under the law governing critical infrastructure, and on measures taken in response to such risks, threats, incidents and emergencies;

5. cooperate regularly with the central authority for responding to hybrid threats and exchange information on risks, cyber threats and incidents, as well as on non-cyber risks, threats and incidents that would indicate hybrid activity, and on the measures taken in response to such risks, threats and incidents; and

6. regularly exchange information, including on relevant incidents and cyber threats, with the Information Society Inspectorate, the Information Commissioner, the Bank of Slovenia, the Civil Aviation Agency of the Republic of Slovenia, the Agency for Communications Networks and Services of the Republic of Slovenia, the national security authority for the protection of classified information on the basis of the law governing classified information, and other sectoral regulators.

(2) The mutual exchange of information on incidents, cyber threats and imminent incidents referred to in Articles 29 and 35 of this Act between the competent national authority, the single point of contact, the CSIRTs referred to in this Act and the competent authorities referred to in points 4, 5 and 6 of the previous paragraph shall be carried out using the digital platform of the competent national authority referred to in the tenth paragraph of Article 30 of this Act.

Article 19

(peer review)

(1) The competent national authority may, with the aim of learning from common experiences, strengthening mutual trust, achieving a high common level of cybersecurity and strengthening cybersecurity capabilities and policies, engage in peer reviews conducted by designated cybersecurity experts from other Member States of the European Union.

(2) The peer review referred to in the previous paragraph includes at least one of the following: the following:

Level 1 implementation of cybersecurity risk management requirements and obligations reporting from Articles 21, 22, 29 and 30 of this Act,

2. the level of capacity, including available financial, technical and human resources, and the effectiveness of the performance of the tasks of the competent national authority,

3. operational capabilities of CSIRTs,

4. level of implementation of mutual assistance referred to in Article 51 of this Act,

5. level of implementation of agreements on the exchange of information on cybersecurity referred to in Article 34 of this law and

6. specific cross-border or cross-sectoral aspects identified by the competent national authority.

(3) The methodology of the Cooperation Group shall be used for the implementation of the peer reviews referred to in the first paragraph of this Article, and the competent national authority shall publish this methodology on the central website of the state administration.

(4) Before the start of the peer review referred to in the first paragraph of this Article, the competent national authority shall communicate the scope of the review, including the aspects referred to in the second paragraph of this Article, to the participating single points of contact of other Member States of the European Union through the single point of contact.

(5) Before the start of the peer review, the competent national authority may carry out a self-assessment of the aspects to be reviewed, taking into account the methodology for self-assessment by the Member States of the European Union, as established by the Cooperation Group with the assistance of the European Commission and ENISA. The results of the self-assessment shall then be sent to the designated cybersecurity experts.

(6) Peer reviews shall include physical or virtual on-site visits and remote exchanges. In the cases referred to in the first paragraph of this Article, the competent national authority shall, without prejudice to Article 4 of this Act and in order to protect essential state functions such as national security, and taking into account the principle of good cooperation, provide the designated cybersecurity experts with the information necessary for their assessment.

(7) All information obtained in the course of a peer review shall be used exclusively for that purpose. The cybersecurity experts participating in the peer review shall not disclose to third parties any sensitive or confidential information obtained during the peer review. The cybersecurity experts shall also take into account the codes of conduct drawn up by the Cooperation Group and published by the competent national authority on the central website of the national administration as a basis for their working methods.

(8) The competent national authority shall, with a view to participating in peer reviews in other Member States of the European Union, nominate cybersecurity experts on the basis of the criteria set out in the methodology referred to in the third paragraph of this Article. In relation to the nominated cybersecurity experts, it shall disclose to the Member States of the European Union, the Cooperation Group, the European Commission and ENISA any risks of conflict of interest relating to the cybersecurity experts in the manner referred to in the fourth paragraph of this Article before the start of the peer review process.

(9) In the cases referred to in the first paragraph of this Article, the competent national authority may object to the appointment of individual cybersecurity experts from another Member State of the European Union and notify it thereof in the manner referred to in the previous paragraph. In doing so, the competent national authority shall communicate the reasons for objecting to the appointment of individual experts, unless the reasons are related to national security.

(10) Cybersecurity experts participating in peer reviews shall prepare reports on the findings and conclusions of the peer reviews.
The reports contain recommendations for improving the aspects included in the peer review.
Reports shall be submitted to the Cooperation Group and, where appropriate, to the CSIRTs network.

(11) The competent national authority may submit comments on the draft report relating to the cases referred to in the first paragraph of this Article. In the cases referred to in the first paragraph of this Article, the competent national authority may decide to publish the report in full or a redacted version on the central website of the state administration.

IV. RISK MANAGEMENT MEASURES AND INCIDENT REPORTING

Article 20

(management)

(1) The heads of public administration entities and responsible persons of legal entities, i.e. natural persons who manage, are responsible for the implementation of the measures referred to in Articles 21 and 22 of this A

supervise or manage the operations of a legal entity or are competent and obliged by law, the act of establishment or authorization to ensure the lawful operation (hereinafter referred to as: responsible persons) of essential or significant entities.

(2) The responsible persons referred to in the previous paragraph shall approve the risk management measures referred to in Article 22 of this Act, which the entity implements in order to fulfil the obligations set out in this Act, and shall supervise their implementation.

(3) The responsible persons referred to in the first paragraph of this Article shall receive education or training at least every four years in the field of information and cybersecurity risk management and their impact on the activities or services performed by the entity.

(4) Responsible persons shall ensure that employees receive regular training to acquire sufficient knowledge and skills to enable them to identify information and cybersecurity risks and their impact on the services provided by the entity. The competent national authority shall publish on the central website of the state administration the recommended content of regular employee training.

(5) Responsible persons shall ensure that all administrators of the obliged entity's information and communication systems undergo regular annual training to acquire and maintain a level of knowledge and skills and are qualified to identify and assess risks and to assess information and cybersecurity risk management practices and their impact on the services provided by the entity.

(6) The competent national authority shall be responsible for organising the training of responsible persons referred to in the first paragraph of this Article. The programme and method of implementing the training of responsible persons in the field of information and cyber security shall be determined by the government at the proposal of the competent national authority.

(7) The competent national authority shall keep a list of the responsible persons referred to in the first paragraph of this Article who have completed the training referred to in the previous paragraph. The list shall include the person's first and last name, the national identity number and the date of completion of the training.

Article 21

(safety documentation)

(1) In order to ensure a high level of information and cyber security and the resilience of their network and information systems, essential and significant entities shall establish and maintain a documented information security management system and a business continuity management system, which shall be based on an all-hazards approach and shall include at least:

1. policy or sectoral policies on the security of network and information systems,

2. a precise and up-to-date inventory of information and other resources and data necessary for the smooth operation of network and information systems used for their operation or provision of services, and their operators;

3. risk management analysis, including determination of acceptable risk levels and description of the methodology used;

4. a business continuity policy and plan, including an assessment of the impact on business, a statement of procedures for ensuring business continuity, the definition of a minimum level of operation, the management of backup copies and the definition of roles and responsibilities;

5. a plan for the recovery and re-establishment of the operation of network and information systems that they require for their operation or the provision of services, including a description of responsibilities and procedures for restoring the operation of these systems after an event that causes an interruption of their operation;

6. an incident response plan with a notification protocol for the competent CSIRT team, including a description of the incident detection and response system and a description of the roles and responsibilities for responding to incidents;

7. a plan of security measures to ensure the integrity, authenticity, confidentiality and availability of network and information systems or to manage risks to information and cyber security, whereby this plan takes into account the risks and sectoral specificities of the essential or important entity and

8. a policy with procedures for assessing the effectiveness of security measures to manage information and cybersecurity risks, including the determination of performance indicators and the analysis of the collected data.

(2) Essential and significant entities shall determine the scope of the information management and security system and business continuity, taking into account the results of the business impact analysis, whereby this system must include at least those information, communication and other resources, data and processes that are necessary for their operation or provision of services.

(3) If an essential or important entity has already prepared security documentation on the basis of other regulations to ensure the security of its networks and information systems, it shall supplement it as necessary for the purposes of implementing this Act.

(4) A significant entity that is an associated entity under this Act, and the ministry responsible for the management of information and communication systems, on the basis of the first paragraph in conjunction with the second paragraph of Article 74.a of the State Administration Act (Official Gazette of the Republic of Slovenia, No. 113/05 – official consolidated text, 89/07 – decision of the Supreme Court, 126/07 – ZUP-E, 48/09, 8/10 – ZUP-G, 8/12 – ZVRS-F, 21/12, 47/13, 12/14, 90/14, 51/16, 36/21, 82/21, 189/21, 153/22 and 18/23; hereinafter referred to as: ZDU-1), shall carry out the tasks referred to in the first paragraph of Article 74.a of the ZDU-1, shall carry out an inventory of information assets referred to in point 1 of the first paragraph of this Article and include therein: at least those information assets that support its main or important services and processes to ensure connectivity to the central state information and communication network or system. The essential entity shall carry out the inventory in cooperation with the ministry responsible for the management of information and communication systems, which shall, upon request, send the relevant data at its disposal, within thirty days of receipt of an individual request.

(5) Notwithstanding the provisions of this Article, essential and significant entities to which the implementing acts of the European Commission referred to in the first subparagraph of the fifth paragraph of Article 21 of Directive 2022/2555/EU apply or from the second subparagraph of the fifth paragraph of Article 21 of Directive 2022 /2555/EU, apply the provisions of the implementing act regarding the safety documentation of the entities concerned.

Article 22

(risk management measures)

(1) Essential and important entities must adopt technical, operational and organisational measures to ensure the integrity, authenticity, confidentiality and availability of network and information systems or to manage risks to the security of network and information systems.

information systems that they use for their operations or provision of services and to prevent or reduce the impact of incidents on the recipients of their services and other services (hereinafter referred to as: security measures).

(2) Security measures must be based on an all-hazards approach aimed at protecting network and information systems and their physical environment from incidents and must include at least:

1. support of the entity's management in ensuring information and cyber security and the inclusion of the area of information and cyber security in the annual business plan or annual work program,

2. ensuring the integrity of personnel in relation to information and cybersecurity before employment, during employment and upon termination or change of employment in accordance with Article 23 of this Act,

3. basic cyber hygiene practices and training in the field of information and cybersecurity,

4. human resource security, user identity verification, ensuring the level of information accessibility and managing access authorizations,

5. implementing and managing data backups,

6. providing and maintaining logs of the operation of network and information systems in accordance with Article 24 of this Act,

7. management of network and information systems used for their operations or provision of services, by determining appropriate responsibility for their protection,

8. policies and procedures regarding the use of cryptography and, where applicable, encryption,

9. traffic and communications management,

10. supply chain security by setting appropriate minimum requirements related to information and cybersecurity for key suppliers or service providers, the requirements relating to the relationship between an individual entity and its direct suppliers or service providers, in accordance with the fourth paragraph of this Article,

11. physical and technical security of premises and access to premises where key parts of network and information systems are located, which they use for their operations or the provision of services,

12. security mechanisms in individual application software for the performance of activities, including security in the acquisition, development and maintenance of network and information systems and the handling and disclosure of vulnerabilities,

13. management and prevention of exploitation of technical vulnerabilities,

14. protection against malicious software code and a method for detecting attempted intrusions and preventing incidents,

15. use of multi-factor authentication or continuous authentication solutions when necessary for risk management,

16. the use of secure voice, video and text communications and secure emergency communication systems within the entity, where appropriate given the entity's activity, and

17. policies and procedures regarding the use of cloud services they use for their operations or provision of services.

(3) The security measures referred to in the previous paragraph must, taking into account the most modern and relevant European and international standards and the costs of implementation, ensure a level of security of network and information systems that corresponds to existing or identified risks.
When assessing the proportionality of security measures, essential and significant entities shall duly take into account:

– the level of risk exposure,

– size of the entity,

– the probability of incidents occurring and

– the severity of potential incidents, including their social and economic impact.

(4) When assessing and implementing appropriate security measures for the security of the supply chain, essential and significant entities shall take into account the vulnerabilities specific to each direct supplier and service provider and the overall quality of their suppliers' and service providers' cybersecurity products and practices, including their secure development processes. They shall determine which security measures are appropriate and suitable to ensure the security of the supply chain and may verify their implementation by suppliers and service providers. In doing so, they shall take into account the results of any harmonised risk assessments for critical supply chains prepared by the Cooperation Group in cooperation with the European Commission and ENISA in accordance with the first paragraph of Article 22 of Directive 2022/2555 /EU.

(5) Significant or important entities shall, at least once a year or at regular intervals specified in the policy and procedures for assessing the effectiveness of cybersecurity risk management measures, and in the event of identified vulnerabilities, verify compliance with the security measures referred to in the second paragraph of this Article. In the event of identified deficiencies or inadequate implementation of security measures, they shall immediately take all necessary, appropriate and proportionate corrective measures.

(6) DNS service providers, TLD name registries, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, managed security service providers, providers of online marketplaces, online search engines and social networking service platforms and trust service providers shall take into account the implementing acts of the European Commission referred to in the first subparagraph of the fifth paragraph of Article 21 of Directive 2022/2555/EU when adopting the security measures referred to in the second paragraph of this Article.

(7) When adopting the security measures referred to in the second paragraph of this Article, essential and significant entities not referred to in the previous paragraph shall take into account the implementing acts of the European Commission laying down technical, methodological and sectoral requirements for the security measures referred to in the second subparagraph of the fifth paragraph of Article 21 of Directive 2022/2555/EU.

(8) Essential and significant entities may not use information and communication solutions in which actively exploited vulnerabilities have been detected without an additional risk assessment being carried out and appropriate additional security measures being implemented that reduce the level of risk to an acceptable level.

(9) If essential or important entities draw input data and information from key parts of the national security system for the performance of their activities, they shall establish all necessary security requirements with the consent of the competent ministry or government service responsible for the individual key part of the national security system.

(10) The operator of the central state information and communication system must set minimum security requirements for information and cyber security for the connected entities. In order to respond to cyber threats in a timely manner and prevent the harmful consequences of a possible serious or critical incident and to implement cyber defence, the operator of the central state information and communication system is authorised to implement appropriate, urgent and proportionate measures to protect the central state information and communication system. The measures shall also include the temporary disconnection of an individual connected entity from the central state information and communication system until the identified risks have been eliminated.

(11) The essential entity referred to in the fourth paragraph of the previous article shall adopt the measures referred to in points 1 to 4 of the second paragraph of this article. The remaining measures referred to in the second paragraph of this article shall be adopted only for any information and communication systems that it manages. In doing so, it shall also take into account the minimum security requirements for connected entities of the operator of the central national information and communication system referred to in the previous para

(12) Essential entities that are designated as critical entities under the law governing critical infrastructure and belong to the types of entities from sector 8. Digital infrastructure from Annex 1 to this Act, in order to ensure the security measures referred to in point 11 of the second paragraph of this Article, shall, at the proposal of the critical infrastructure sector operator for digital infrastructure, be designated as entities subject to mandatory security arrangements and must protect critical infrastructure in accordance with the aforementioned regulations.

(13) The security measures referred to in the second paragraph of this Article must be:

1. effective in that they increase information security in relation to existing and anticipated threats;

2. adapted so that the efforts of essential and important entities are focused on measures that have the greatest impact on their information security, and duplication is avoided;

3. coherent in such a way that basic and common security vulnerabilities of essential and important entities are addressed as a priority, despite sectoral specificities, which can be supplemented by security measures for individual areas,

4. proportionate to the risks by avoiding excessive burden on any single material or a significant entity;

5. concrete so that essential and important entities implement these security measures and that these measures contribute to strengthening their information security and

6. verifiable in such a way that evidence of their existence can be provided upon request by the competent authority.
performance.

Article 23

(background check)

(1) A significant or important entity may, taking into account a risk assessment, conduct background checks on employees and candidates for employment in positions relevant to the provision of the entity's services who have or will have direct or remote access to its critical information systems. It may also conduct background checks on employees of contractors in accordance with the risk assessment. Background checks shall be carried out for the past five years.

(2) The background check of the person referred to in the previous paragraph shall be carried out after his/her prior consent is made in such a way that:

– confirms the identity of the person whose background is being checked, and

– check the criminal records of the Republic of Slovenia, the Member States of the European Union and third countries for records of final criminal convictions for criminal offences that are prosecuted ex officio and that, in the opinion of the essential or important entity, are questionable from the perspective of performing tasks in the relevant workplace or for the implementation of contractual obligations, namely in the areas of terrorism and violations against life and limb, human rights and freedoms, human health, employment relationships and social security, property, the economy, legal transactions, official duties, public powers and public funds, public order and peace, general safety of people and property, safety of public transport, the environment, space and natural resources, the sovereignty of the Republic of Slovenia, its defence power and international law, and in other areas, unless otherwise provided for by the law regulating background checks for individual sectors referred to in Annexes 1 and 2 to this Act.

(3) If the person referred to in the previous paragraph does not consent to a background check, he or she shall not be permitted to work in the positions and premises referred to in the first paragraph of this Article or the contract shall not be concluded.

(4) For the purpose of background checks referred to in the second paragraph of this Article, essential and significant entities may collect the following data:

– the person's first and last name,

– Social Security Number or date of birth,

– the number of the official identification document confirming the person's identity and

– information about the absence of a criminal record or a final conviction for the criminal offense referred to in the second indent the second paragraph of this article.

The personal data referred to in this paragraph shall be stored for five years from the end of the calendar year in which they were collected, after which they shall be irreversibly deleted or destroyed.

(5) Authorities, organisations and other entities that, pursuant to the law, maintain databases referred to in the previous paragraph, must send the requested personal and other data free of charge to essential and important entities on the basis of a written or equivalent written request, stating the appropriate legal basis for the submission of data and the appropriate number or other designation of the request.

Article 24

(diary entries)

(1) Essential and significant entities shall establish procedures and appropriate tools for monitoring and recording events in their networks and information systems, or ensure the collection and retention of log records, in order to detect or detect events that could be considered incidents or near-incidents, and to respond appropriately to mitigate their negative impact. Log records must be collected and retained to a extent and in a manner that allows for the reconstruction and analysis of incidents or near-incidents.

(2) The logbook entries referred to in the previous paragraph shall include at least:

1. outgoing and incoming network traffic,

2. creating, modifying or deleting users of network and information systems of the entities concerned and the extension of permits,

3. access to systems, applications and databases,

4. events related to authentication,

5. all privileged access to systems and applications and activities performed by administrators invoices,

6. access or changes to critical configuration and security files,

7. event logs and logs from security tools such as antivirus programs, firewalls, intrusion detection or firewalls,

8. the use of system resources and their capacity,

9. access to and use of network equipment and devices, and

10. activating, stopping and interrupting system services and logging.

(3) The log records referred to in the previous paragraph must be stored in a manner that ensures their authenticity, integrity, availability and confidentiality. Essential and important entities shall ensure that all systems have synchronized time sources so that log records can be correlated between systems for the purpose of assessing events.

(4) Essential and significant entities shall ensure that the log records referred to in the first paragraph of this Article are retained for at least six months, but may also be retained for a longer period when the risk management analysis and assessment of the acceptable level of risks indicate that the risks would be appropriately managed by retaining the log records for a longer period.

(5) The preservation of log records of essential entities, which are designated as critical entities pursuant to the law governing critical infrastructure, shall be ensured within the territory of the Republic of Slovenia, and a second copy may be ensured within the territory of an EU Member State.

(6) Notwithstanding the previous paragraph, entities in the digital infrastructure, banking and financial market infrastructure sectors may ensure that logs are kept entirely within the territory of an EU Member State, subject to personal data protection regulations and proportionate security controls identified and implemented on the basis of a risk assessment, and also outside the territory of the EU Member States.

(7) Notwithstanding the fifth paragraph of this Article, the logbook records of key parts of the national security system are kept only on the territory of the Republic of Slovenia.

(8) Notwithstanding the previous paragraph, the ministry responsible for foreign affairs may also ensure the storage of diary records at diplomatic missions and consulates of the Republic of Slovenia abroad.

(9) Notwithstanding the second paragraph of this Article, essential and significant entities that are DNS service providers, TLD name registries, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, managed security service providers, providers of online marketplaces, online search engines and social networking service platforms and trust service providers shall, with regard to the scope of log records, comply with the provisions on monitoring and maintaining logs set out in the European Commission implementing act referred to in the first subparagraph of the fifth paragraph of Article 21 of Directive 2022/2555 /EU.

Article 25

(assessment and self-assessment of compliance)

(1) Significant entities must conduct a compliance assessment at least once every two years or in the event of a significant incident. The compliance assessment is carried out as an audit of compliance with regulations in the field of information security or as part of an internal audit carried out on the basis of other regulations and including the field of information security referred to in this Act and the implementing regulations or implementing acts of the European Commission issued on the basis of this Act. In addition to information systems auditors, the compliance assessment may also be carried out as part of an internal audit by internal auditors in cooperation with an information technology expert, who is an individual or organization with demonstrated in-depth expertise in the field of information and communication technologies, whose work the auditor uses as professional assistance in obtaining sufficient and appropriate audit evidence. The information systems auditor or internal auditor prepares a report on the compliance assessment carried out.

(2) If the report on the compliance assessment referred to in the previous paragraph contains findings of non-compliance and recommendations of the information systems auditor for their elimination, the significant entity shall prepare a plan for the elimination of the identified non-compliances, determine the method of their elimination and the deadlines for implementation.

(3) Significant entities shall conduct a self-assessment of compliance at least once every two years or in the event of a significant incident. The self-assessment of compliance shall be conducted by documenting the significant entity's compliance with its security documentation and the implementation of measures to manage cybersecurity risks. The self-assessment of compliance may also be conducted as part of an internal audit.

(4) If the results of the self-assessment of conformity show that the relevant entity meets the requirements prescribed by this Act, it shall draw up a declaration of conformity, which shall contain the necessary elements of the self-assessment of conformity that enable the repeatability of the assessment carried out.

(5) If the results of the self-assessment of compliance show that the significant entity does not meet the prescribed requirements, it shall draw up a statement of non-compliance, stating the non-compliances identified and the method of their elimination, with deadlines for implementation.

Article 26

(obligation to submit data and information)

(1) Essential and significant entities must submit to the competent national authority, upon written request, the data and information that it needs to exercise its powers under this Act, within the deadline specified in its written request.

(2) The data and information requested must be proportionate to the purpose for which they will be used. The competent national authority must state in the request the purpose for which the data and information requested will be used.

(3) If the competent national authority requests data and information that is classified as confidential or a business secret or other form of protected data by the entities referred to in the first paragraph of this Article, only secure communication channels shall be used to submit such data and information to the competent national authority.

Article 27

(certification)

(1) Cybersecurity certification means the confirmation that ICT products, services and processes have been assessed in accordance with the applicable European cybersecurity certification schemes set out in the implementing acts of the European Commission adopted pursuant to Article 49 of Regulation 2019/881/EU. (hereinafter referred to as: European cybersecurity certification schemes), and that they meet the security requirements specified in these schemes.

(2) The competent national authority is the competent national cybersecurity certification authority referred to in the first paragraph of Article 58 of Regulation 2019/881/EU.

(3) Self-assessment of conformity, which is the sole responsibility of the manufacturer or provider of ICT products, services or processes, and the issuance of the EU declaration of conformity shall be carried out in accordance with Article 53 of Regulation 2019/881/EU.

(4) Tasks of the national accreditation body under Regulation 2019/881/EU In the Republic of Slovenia, it is carried out by the public institution Slovenian Accreditation, which also accredits conformity assessment bodies that meet the conditions set out in the aforementioned regulation.

(5) The conformity assessment body in the Republic of Slovenia shall be designated in accordance with the procedure and in the manner set out in Chapter IV of the Act on Technical Requirements for Products and on Conformity Assessment (Official Gazette of the Republic of Slovenia, Nos. 17/11 and 29/23), whereby this body shall meet the requirements of the aforementioned Act and the additional requirements set out in the Annex to Regulation 2019/881/EU.

(6) The conformity assessment body referred to in the previous paragraph may, pursuant to Regulation 2019/881/EU issues a European cybersecurity certificate relating to a basic or substantial level of assurance, based on the criteria included in the European cybersecurity certification scheme.

(7) Notwithstanding the previous paragraph, where the European cybersecurity certification scheme provides that European cybersecurity certificates may be issued exclusively by public authorities, the competent authority for the issue of such certificates in the Republic of Slovenia shall be the conformity assessment body referred to in the fifth paragraph of this Article, if that body is a subject of public law. If there is no such authority, the competent authority for the issue of such certificates shall be the national cybersecurity certification body.

(8) Where a European cybersecurity certification scheme requires a high level of assurance, a European cybersecurity certificate may be issued in the Republic of Slovenia by a national cybersecurity certification body based on that scheme.

(9) Notwithstanding the seventh and eighth paragraphs of this Article, a European cybersecurity certificate may be issued by a conformity assessment body if the national cybersecurity certification body has previously approved this for each individual European cybersecurity certificate individually or on the basis of a general delegation of the task of issuing such European cybersecurity certificates to the conformity assessment body.

(10) The national cybersecurity certification body may, with the prior consent of the government, delegate the authority to issue European cybersecurity certificates for a high level of assurance from its jurisdiction to the competent national cybersecurity certification body of another Member State of the European Union. In such a case, the national certification body shall decide on the recognition of the European cybersecurity certificate for a high level of assurance thus issued.

(11) The national cybersecurity certification body shall decide on applications for recognition of a European cybersecurity certificate held by natural or legal persons who have applied for such recognition in the Republic of Slovenia. In addition, it may, by decision, revoke a European cybersecurity certificate issued by a competent authority referred to in the sixth, seventh or tenth paragraph of this Article where such a certificate does not comply with Regulation 2019/881/EU. or with European cybersecurity certification schemes adopted pursuant to Article 49 of Regulation 2019/881/EU.

(12) Natural and legal persons who are parties or secondary participants in the procedure referred to in the sixth, seventh or eighth paragraph of this Article may lodge a complaint with the authority competent for issuing the European cybersecurity certificate against the European cybersecurity certificate or against the silence of the authority. Where the complaint concerns a European cybersecurity certificate issued by a conformity assessment body in accordance with the seventh paragraph of this Article, such a complaint shall be lodged with the national cybersecurity certification body.

(13) The body with which the complaint was lodged shall examine the content of the complaint and inform the complainant of the progress of the procedure or of the referral of the complaint to the national cybersecurity certification body, which shall decide on the complaint. An administrative dispute is permitted against the decision of the complaint body.

(14) Where, pursuant to the seventh or eighth paragraph of this Article, a decision on the issuance of a European cybersecurity certificate is made by a national cybersecurity certification body, an administrative dispute shall be permitted against the European cybersecurity certificate or against the silence of the body.

(15) The judicial protection referred to in paragraphs 13 and 14 of this Article also includes the incorrect issuance, failure to issue or recognition of a European cybersecurity certificate held by natural or legal persons who are parties or secondary participants in the proceedings, and the silence of the authority.

(16) In order to manage risks to the security of networks and information systems, essential and significant entities shall, when implementing the measures referred to in Article 22 of this Act, give priority to using qualified trust services and those ICT products, services or procedures that have been developed by essential or significant entities or purchased from other entities and are certified under European cybersecurity certification schemes adopted pursuant to Article 49 of Regulation 2019/881/EU.

Article 28

(standardization)

(1) Essential and important entities to ensure the consistent implementation of the measures referred to in Articles 21 and 22 of this Act to the greatest extent possible and in accordance with the best available practices

and also ENISA recommendations and guidelines apply European and international standards and technical specifications addressing the security of network and information systems.

(2) The competent national authority shall publish relevant information on the central website of the state administration on European and international standards and technical specifications that address the security of network and information systems referred to in the previous paragraph, and shall raise awareness among those liable regarding their use.

(3) In order to upgrade the level of cybersecurity of essential and significant entities, regulatory authorities or supervisors responsible for the sectors referred to in Annexes 1 and 2 to this Act shall publish technically specific industry standards and technical specifications, which shall be considered as recommendations, on the central website of the state administration.

Article 29

(obligation to report and inform)

(1) Essential and significant entities shall immediately notify the competent CSIRT team in accordance with the first and second paragraphs of Article 30 of this Act and the national response plan referred to in the second paragraph of Article 12 of this Act of all incidents that have a significant impact on the provision of their services. An incident shall be considered significant (hereinafter referred to as: significant incident) if:

– has caused or is likely to cause serious operational disruption of services or financial loss to the entity concerned, or

– has affected or could affect other natural or legal persons by causing significant material or non-material damage.

(2) When assessing the significance of an incident, essential and significant entities shall take into account the impact on network and information systems, in particular their importance in providing the entity's services, the severity and technical characteristics of the cyber threat and its impact on users, the vulnerabilities exploited and the entity's experience with similar incidents. When making the notification referred to in the previous paragraph, they shall take into account the implementing acts of the European Commission referred to in the first subparagraph of the eleventh paragraph of Article 23 of Directive 2022/2555/EU, which specify in more detail the type of information, the form and procedure for notification, as well as voluntar

(3) DNS service providers, TLD name registries, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, managed security service providers and providers of online marketplaces, online search engines and social networking service platforms shall, when notifying under the previous paragraph, take into account the implementing acts of the European Commission referred to in the second subparagraph of the eleventh paragraph of Article 23 of Directive 2022/2555/EU, which specify in more detail individual cases where an incident is considered significant.

(4) The essential and significant entities referred to in the first paragraph of this Article, which are not entities referred to in the previous paragraph, shall comply with the implementing acts of the European Commission referred to in the second subparagraph of the eleventh paragraph of Article 23 of Directive 2022/2555/EU. If the European Commission does not adopt such implementing acts, the methodology for determining the significance of an incident as defined in the national response plan shall be taken into accou

(5) Essential and significant entities shall communicate to the competent CSIRT all information necessary to determine the cross-border impact of a significant incident. In the event of a significant cross-border or cross-sectoral significant incident, the relevant information shall be communicated in a timely manner to the single point of contact in accordance with Article 30 of this Act.

(6) Essential and significant entities shall immediately inform users of their services of significant incidents referred to in the first paragraph of this Article that are likely to negatively affect the provision of these services.

(7) Essential and relevant entities shall promptly communicate to users of their services that may be affected by a significant cyber threat any measures or means that those users may take in response to that threat. They shall also inform the users concerned of the significant cyber threat in question.

(8) Notwithstanding the sixth and seventh paragraphs of this Article, essential and significant entities shall not inform users of their services in cases where such notification would be contrary to the second or third paragraphs of Article 4 of this Act, and in cases where they are instructed to do so by the competent CSIRT or the competent national authority because disclosure of the data could harm the investigation of the incident or national security.

(9) Essential and important entities operating in systems that are key parts of the national security system shall implement the obligations under this Article, taking into account the processing of information and data that are the subject of national security in accordance with sectoral regulations.

(10) Incidents in information and communication systems specified in regulations governing classified information shall be considered significant incidents under this Act and shall be notified to the competent national authority by the national security authority referred to in the act governing classified information in the manner referred to in the first paragraph of Article 30 of this Act.

Article 30

(procedure for reporting significant incidents)

(1) Essential and important entities for reporting significant incidents from the first paragraphs of the previous article, the competent CSIRT team shall submit:

1. immediately, and no later than 24 hours after the detection of a significant incident, an early warning, indicating, where appropriate, whether the significant incident was allegedly caused by an unlawful or malicious act and whether it could have a cross-border impact;

2. immediately, and no later than 72 hours after the detection of a significant incident, an incident notification, updating the information referred to in the previous point as necessary and providing an initial assessment of the significant incident, including its severity and impact, and, where available, threat indicators;

3. At the request of the CSIRT, an interim report on relevant status updates;

4. a final report, no later than one month after the submission of the incident notification referred to in 2. points of this paragraph, which includes:

– a detailed description of the incident, including its severity and impact,

– the type of threat or root cause that likely caused the incident,

– mitigation measures implemented and such measures being implemented, and

– if applicable, the cross-border impact of the incident.

5. In the event of a significant incident that is still ongoing at the time of submission of the final report referred to in the previous point, the notifying entity shall submit a progress report and a final report no later than one month after the resolution of the incident.

(2) Notwithstanding point 2 of the previous paragraph, the trust service provider must, in relation to significant incidents affecting the provision of its services, immediately, and no later than 24 hours after the detection of a significant incident, notify the relevant CSIRT team.

(3) The competent CSIRT shall respond to the reporting entity without delay and, if possible, within 24 hours of receiving the early notification referred to in point 1 of the first paragraph of this Article, including initial feedback on the significant incident and, at the request of the reporting entity, with guidance or operational advice on the implementation of any mitigating measures. In addition, it shall inform the competent national authority of the notification without undue delay and inform it of the activities carried out. It shall provide additional technical support at the request of the entity concerned. Where there are reasons to suspect that the incident has elements of a criminal offence, it shall also provide guidance on reporting significant incidents to law enforcement authorities.

(4) In the event of a major cross-border or cross-sectoral major incident, the competent CSIRT shall immediately provide the competent national authority with the notified information on the incident referred to in the first paragraph of this Article. Where the competent national authority or the CSIRT deems it necessary, in particular where the major incident concerns two or more Member States of the European Union, the single point of contact shall, upon request, immediately notify the single points of contact of the other affected Member States and ENISA of the major incident. This notification shall include the type of information received in accordance with the first paragraph of this Article. In doing so, the single point of contact shall protect the security and commercial interests of the obliged entity and the confidentiality of the information provided in its notification.

(5) The single point of contact shall submit a summary report to ENISA every three months, including anonymised and aggregated data on incidents, significant cyber threats and near-misses notified in accordance with the first paragraph of this Article and Article 35 of this Act.

(6) Where public awareness is necessary to prevent a significant incident or to deal with an ongoing significant incident, or where disclosure of a significant incident is otherwise in the public interest, the competent national authority shall, after consulting the obliged entity concerned, inform the public of the significant incident or request the obliged entity to do so. A proposal for such notification may also be submitted to the competent national authority by the competent CSIRT.

(7) When the competent national authority is informed through the single point of contact about a significant cross-border or cross-sectoral incident that also has an impact in the Republic of Slovenia, it may, after consulting the entity that notified the incident, inform the public about the significant incident or request the obliged entity to do so, even when the incident was notified in another Member State of the European Union.

(8) The competent national authority shall provide the competent national authority referred to in the law governing critical infrastructure and the relevant critical infrastructure sector operator referred to in that law with information on significant incidents, incidents, cyber threats and near-incidents notified by essential entities identified as critical entities under the regulations governing critical infrastructure in accordance with the first paragraph of Article 29 of this Act or upon voluntary notification referred to in Article 35 of this Act.

(9) The competent CSIRT shall immediately notify the competent national authority of a significant incident. The competent national authority shall notify the National Crisis Management Centre, established in accordance with the Act regulating the Government of the Republic of Slovenia, and the central body for responding to hybrid threats of an incident that could have a major cross-sectoral impact or, if it continues for a longer period, could deteriorate the stability of the national security of the Republic of Slovenia, and may also notify other competent authorities with which it cooperates at the national level, in accordance with Article 18 of this Act.

(10) Notifications of significant incidents and mutual cooperation referred to in this Article shall also be carried out via a dedicated digital platform established by the competent national authority and through which information is also exchanged between the participating authorities pursuant to the second paragraph of Article 18 of this Act. The participating authorities shall have access to information on notifications from entities related to their area of work.

(11) In the incident reporting procedure referred to in the tenth paragraph of the previous article, the first paragraph of this article shall apply mutatis mutandis.

(12) For the purpose of carrying out the tasks referred to in this Act, the competent national authority shall also maintain:

– a common list of significant incidents containing data from the final incident reports from of this article, and

– a list of network and information systems, network parts and digital or electronic communication services of obligated parties, necessary for the smooth functioning of the state or for ensuring national security, which is protected information of the competent national authority.

(13) For the purpose of handling reported incidents, implementing mitigating measures, ensuring network and information security and preventing illegal or malicious acts that threaten the availability, authenticity, integrity and confidentiality of information systems, parts of the network or data of essential and important entities, the competent CSIRT and the competent national authority may collect and process the following data:

– the person's first and last name,

– Social Security Number or date of birth,

– the person's email address,

– the person's phone number,

– IP address (static or dynamic),

– MAC address or similar device identifier,

– username and password,

– alias names, pseudonymous identities or other nicknames that people use online

– file metadata (which may contain, for example, information about the file's author, file paths, time zones, language settings, and other data) and

– other data that may assist in handling reported incidents (e.g. user agent strings, installed fonts and plugins, cookie identifiers, crypto wallet addresses, etc.).

Personal data obtained in this way is stored for a maximum of three years after the end of the calendar year in which it was obtained, and after this period it is deleted or destroyed.

(14) For the performance of the tasks referred to in the previous paragraph, the lists referred to in the twelfth paragraph of this article should be linked to the list from the fourth paragraph of Article 8 of this Act.

V. JURISDICTION AND REGISTRATION

Article 31

(jurisdiction and territoriality)

(1) Obliged entities referred to in Article 6 of this Act, established by the Republic of Slovenia or having their registered office in the Republic of Slovenia, fall under the jurisdiction of the competent national authority and competent CSIRTs in accordance with this Act, except for:

– providers of public electronic communications networks or providers of publicly available electronic communications services that fall under the jurisdiction of the competent authorities of the Member State of the European Union in which they provide their services, and

– DNS service providers, TLD name registries, entities providing domain name registration services, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, managed security service providers and providers of online marketplaces, online search engines and social networking service platforms, which fall under the jurisdiction of the competent authorities of the Member State of the European Union in which they have their main establishment in the European Union, in accordance with the second paragraph of this Article.

(2) For the purposes of this Act, the entities referred to in the second indent of the previous paragraph shall be deemed to have their principal place of business in a Member State of the European Union where the majority of decisions relating to measures to manage cybersecurity risks are taken. If that Member State of the European Union cannot be determined or if those decisions are not taken in the European Union, the principal place of business shall be deemed to be in a Member State of the European Union where the operations relating to cybersecurity are carried out. If that Member State of the European Union cannot be determined, the principal place of business shall be deemed to be in a Member State of the European Union where the entity concerned has its principal place of business with the largest number of employees in the European Union.

(3) If an entity referred to in the second indent of the first paragraph of this Article, which is not established in the European Union but provides such services there, establishes the seat of its representative for the European Union in the Republic of Slovenia, where it also provides such services, it shall fall within the competence of the competent national authority and the competent CSIRT. The representative shall represent the entity in relation to the obligations under this Act.

(4) The fact that an entity appoints a representative referred to in the second indent of the first paragraph of this Article does not exclude the possibility of initiating legal proceedings that may be initiated against the entity in the Republic of Slovenia.

(5) If the competent national authority receives a request for mutual assistance pursuant to Article 51 of this Act in relation to an entity referred to in the second indent of the first paragraph of this Article, the information security inspector may, within the limits of the request, take appropriate supervisory and enforcement measures in relation to the entity concerned that provides services or has a network and information system on the territory of the Republic of Slovenia.

Article 32

(collection of information for the ENISA service provider register)

(1) Entities falling under the jurisdiction of the competent national authority in accordance with the first paragraph of the previous article and which are providers of DNS services, TLD name registries, domain name registration or cloud computing services, data centre services, content delivery networks, managed services, managed security services and online marketplaces, online search engines and social networking service platforms shall provide the competent national authority with the following information in order to facilitate the cooperation of the obliged providers of these services with the competent authorities in managing an imminent incident, incident or significant incident:

1. name of the entity,

2. the relevant sector, subsector and type of entity from Annex 1 or 2 to this Act,

3. the address of its head office and its other legal offices in the European Union or, if it does not have a registered office in the European Union, of its representative appointed in accordance with the third paragraph of the previous article,

4. updated contact details, including email addresses and telephone numbers, of the entity and, where applicable, of its representative appointed in accordance with the third paragraph of the previous article,

5. the Member States of the European Union in which the entity provides services, and

6. blocks of autonomous system numbers and public IP addresses assigned to the subject.

(2) The entities referred to in the previous paragraph shall notify the competent national authority of any change to the information they have submitted in accordance with the previous paragraph. They shall submit the notification of the change immediately or at the latest within three months of the date of the change in the information.

(3) The entities referred to in the first paragraph of this Article shall submit the information referred to in the first and second paragraphs of this Article to the competent national authority through the mechanism for self-registration of taxpayers referred to in the first paragraph of Article 8 of this Act.

(4) Upon receipt of the information referred to in the first and second paragraphs of this Article, with the exception of the information referred to in point 6 of the first paragraph of this Article, the competent national authority acting as the single point of contact shall immediately submit this information to ENISA.

Article 33

(domain name registration database)

(1) TLD name registries and entities providing domain name registration services shall, with due diligence, collect and maintain accurate and complete domain name registration data in the database to ensure the security, stability and resilience of the DNS.

(2) The database referred to in the previous paragraph must contain information on domain name registrations, which includes information for identifying and contacting domain name holders and contact points that manage domain names within the top-level domain names. Such information includes:

– domain name,

– date of registration,

– the name of the domain name holder, their contact email address and telephone number, and

– contact email address and telephone number of the contact point managing the domain name, if it differs from the domain name holder's address.

The entities referred to in the first paragraph of this Article must, after deletion from the database, store the information referred to in this paragraph separately for ten years after the end of the calendar year in which it was deleted from the database, and after this period, the separately stored information shall also be deleted or destroyed.

(3) TLD name registries and entities providing domain name registration services shall establish policies and procedures, including verification procedures, to ensure that the databases referred to in the first paragraph of this Article contain accurate and complete information, taking into account that they must verify at least one contact information referred to in the third and fourth indents of the previous paragraph and establish verification periods. These policies and procedures must be publicly available.

(4) The entities referred to in the first paragraph of this Article shall, after registering a domain name, immediately make the registration data, which are not personal data, publicly available. They shall publish such data on their website or publish a link to the website where such data is available.

(5) The entities referred to in the first paragraph of this Article shall provide access to the registration data of individual domain names without delay, and no later than 72 hours after receipt of a lawful and substantiated request from a person with a legitimate reason for access. The policies and procedures relating to the disclosure of such data shall be publicly available.

(6) Compliance with the obligations referred to in paragraphs 1 to 5 of this Article shall not result in duplication of data collection on domain name registration. To this end, TLD registries and entities providing domain name registration services shall cooperate with each other by exchanging relevant information.

VI. EXCHANGE OF INFORMATION

Article 34

(Agreements on the exchange of information on cybersecurity)

(1) Obliged persons under this Act and other entities may voluntarily exchange relevant information on cybersecurity, including information relating to cyber threats, imminent incidents, vulnerabilities, techniques and procedures, indicators of threat, hostile tactics, threat and actor-specific information, cybersecurity alerts and recommendations regarding the configuration of cybersecurity tools to detect malicious cyber activities, where such exchange of information:

– helps prevent, detect, respond to, or recover from incidents or mitigating their impact or

– increases the level of cybersecurity, in particular by raising awareness of cyber threats, limiting or hindering the ability of such threats to spread, supporting a range of defence capabilities, addressing and disclosing vulnerabilities, techniques for detecting, mitigating and preventing threats, risk reduction strategies or response and recovery phases, or by promoting cooperation between public and private entities in researching cyber threats.

(2) The exchange of information referred to in the previous paragraph shall take place within sectoral or cross-sectoral communities of obliged entities, and may also take place with their suppliers or service providers. Such exchange shall be carried out on the basis of agreements on the exchange of information on cybersecurity, taking into account the potentially sensitive nature of the information exchanged. The data subject to exchange shall be appropriately marked with a traffic light protocol. When concluding agreements on the exchange of information, good practices and guidelines of the ENISA agency shall be taken into

(3) The agreements on the exchange of information on cybersecurity referred to in the previous paragraph shall contain the content and conditions for such agreements and may also include operational elements, including the use of dedicated digital platforms and automation tools. The competent national authority shall encourage the conclusion of such agreements by raising awareness among the obliged entities and by providing methodological support in concluding the agreements.

(4) Essential and significant entities shall notify the competent national authority and their competent CSIRT of their participation in the arrangements for the exchange of cybersecurity information referred to in the second paragraph of this Article, upon conclusion of such arrangements or of withdrawal from the arrangement when the withdrawal takes effect. The administrator of such arrangement shall send the notification to the competent national authority and the competent CSIRT within 15 days of the occurrence of the event.

(5) At the request of the parties subject to this Act, the competent national authority or CSIRT groups may participate in the individual agreement referred to in the previous paragraph and, in doing so, determine the conditions regarding the information they make available.

Article 35

(voluntary notification)

(1) In addition to the mandatory notification referred to in Article 30 of this Act, obligated parties may voluntarily notify the competent CSIRT of incidents, cyber threats and imminent incidents and submit relevant information to them.

(2) Entities that are not subject to obligations under this Act may, regardless of whether they fall within the scope of this Act, voluntarily notify the CSIRT referred to in the first paragraph of Article 13 of this Act of significant incidents, cyber threats and imminent incidents and submit relevant information to it.

(3) Voluntary reporting referred to in the first and second paragraphs of this Article shall be handled by CSIRTs in accordance with the procedure referred to in Article 30 of this Act. Voluntary reporting shall not impose any additional obligations on the reporting entity.

(4) The competent CSIRTs shall, where appropriate, forward information on notifications received in accordance with this Article to the competent national authority acting as a single point of contact, ensuring the confidentiality and appropriate protection of the information sent by the notifying entity.

(5) Competent CSIRTs may prioritize mandatory notifications over voluntary notifications. When determining the order of processing voluntary notifications, they shall take into account the impact of voluntarily reported incidents on the continuity of services of the obliged entities and the potential cross-border impact.

(6) Voluntary notifications that have no or negligible impact on the provision of services by obliged entities and have negligible cross-border impact shall only be processed where such processing does not impose a disproportionate or unjustified burden on CSIRTs.

(7) Voluntary notification of relevant information referred to in this Article may also be carried out via the dedicated digital platform referred to in the tenth paragraph of Article 30 of this Act, through which information is also exchanged between participating authorities pursuant to the second paragraph of Article 18 of this Act. Participating authorities shall have access to information on notifications from entities related to their area of work.

VII. INCIDENT EVALUATION, RISK ASSESSMENT AND ACTION

Article 36

(incident assessment and action)

(1) When resolving reported incidents, the competent CSIRT team shall evaluate them, which, in addition to the provisions of this Article, shall also take into account the national response plan referred to in the second paragraph of Article 12 of this Act. If the state administration body has ensured capacities at least at the level of the security operations centre, the competent CSIRT team shall carry out the evaluation after prior consultation with the security operations centre of the state administration body. If the competent national authority determines that the assessment of the competent CSIRT team does not reflect the real situation or new facts have been established, it may re-evaluate the incident. Security events and incidents shall be evaluated in the following levels with the following designation:

1. **C6 event # detected cyber activities that do not have a negative impact on the networks and information systems or information services of the obliged entities. Detected or possible impact on individual natural persons or individual companies in the country that are not obliged entities;**

2. **C5 near-miss # means an event that could have compromised the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or services provided by or accessible through network and information systems, but that event was prevented from occurring or did not occur;**

3. **C4 minor incident # a one-off incident that, according to the parameters for determining the significance of the impact of the incident, has not caused and cannot cause significant operational disruption to the entity concerned in the provision of services or financial loss, and has not affected and cannot affect other natural or legal persons by causing significant property or non-property damage.**
   Such an incident must not have a negative cross-sectoral impact or a negative impact on the operation of defense, internal security, and protection and rescue information systems;

4. **C3 major incident # a single significant incident or a sequence of several different incidents within a short period of time which, based on the parameters for determining the significance of the impact of the incident, has caused or could cause significant operational disruptions to the entity concerned in the provision of services or financial loss, has affected or could affect other natural or legal persons by causing significant material or non-material damage, or has**

negative cross-sectoral impact or negative impact on the operation of information systems for defence, internal security and the protection and rescue system;

5. C2 major incident # a single significant incident or a sequence of several different incidents in a short period of time, where there is a possibility of developing into a critical incident, and

6. C1 critical incident # a significant incident that, in addition to the impacts referred to in point 4 of this paragraph, also causes difficulties in the functioning of the state, in particular the performance of defence, internal security and protection and rescue tasks, or partially disables the functioning of at least three highly critical sectors from Annex 1 or one in its entirety.

(2) The competent national authority shall, on the basis of the data and level of the incident referred to in the previous paragraph, which are continuously reported to it by the CSIRTs, assess whether it is also a large-scale cyber incident or crisis.

(3) The competent national authority must immediately notify the government, SNAV and the central body for responding to hybrid threats of a critical incident, but may also notify them of a more serious incident, depending on the assessment of the relevant circumstances, when there is a possibility that it will escalate into a critical incident.

(4) The competent national authority shall inform the central body for responding to hybrid threats of major C3 and C2 cyber incidents.

(5) In the event of a serious incident C3 or C2 or a critical incident C1, the competent national authority may, by written decision, impose on the obliged entity such appropriate and proportionate measures as are necessary to stop the ongoing incident or to remedy its consequences. In urgent cases where the issuance of a written decision could adversely affect the effectiveness of such measures due to the passage of time, the competent national authority may also impose the relevant measures on the obliged entity by oral decision. In such a case, a written copy of the oral decision shall be served on the obliged entity no later than 48 hours after the oral decision.

(6) If the competent CSIRT team determines that it does not have all the facts absolutely necessary to define the incident and to prevent further harmful consequences of such an incident, it shall request information and explanations from the obligated party by means of a written request, or in urgent cases by means of an oral request, where a written request could negatively affect the efficiency of resolving the incident in question due to the passage of time. In doing so, the competent CSIRT team shall also set a deadline for the submission of such information and explanations.

(7) If the obliged entity fails to submit the requested information and explanations to the competent CSIRT within the deadline set in the previous paragraph, the competent national authority may, at the proposal of the competent CSIRT, request the submission of information and explanations by written decision and set a deadline for their submission. In urgent cases where the issuance of a written decision could negatively affect the efficiency of resolving the incident in question due to the passage of time, the competent national authorities may also decide on this by oral decision. In such a case, a written copy of the oral decision shall be served on the obliged entity no later than 48 hours after the oral decision.

(8) The measures issued on the basis of the fifth, sixth and seventh paragraphs of this Article shall be determined to such an extent and for such a period as is strictly necessary to achieve the purpose referred to in the fifth paragraph of this Article. The data and information requested on the basis of the previous paragraph shall be requested to such an extent and for such a period as is strictly necessary to achieve the purpose referred to in the previous paragraph. No appeal is permitted against the decisions referred to in the fourth and seventh paragraphs of this article, but an administrative dispute is permitted.

(9) In order to prevent the emergence of a crisis or to manage it or to manage the situation more quickly and limit further harmful consequences of a serious C2 incident or a critical C1 incident, the competent national authority may issue a written order requiring the obliged entities to:

order the implementation of urgent measures. In doing so, it shall determine in particular the type and scope of the work to be carried out at the obliged party and the deadline for their implementation. In urgent cases where the issuance of a written order could, due to the passage of time, have a negative impact on preventing the emergence of a crisis or its management, the competent national authority may also decide to do so by means of an oral order. In such a case, a written copy of the oral order shall be served on the obliged party no later than 48 hours after the oral

(10) The competent national authority shall inform the government and SNAV and the central body for responding to hybrid threats of the measures referred to in the fifth and eighth paragraphs of this article.

Article 37

(threat assessment)

(1) The competent national authority shall prepare, on the basis of data and information relating to the security of networks and information systems, an assessment of the threat to cybersecurity in the Republic of Slovenia (hereinafter referred to as: threat assessment). In order to prepare the threat assessment, it shall also obtain other data that could influence this threat assessment from authorities that are key parts of the national security system, upon request, to the extent strictly necessary for the preparation of the threat assessment. The competent national authority shall check the threat assessment and, if necessary, update it monthly or, in the event of a sudden change in the security situation, even earlier. In doing so, it shall evaluate t

– low risk,

– medium risk,

– high risk,

– critical threat.

(2) Regardless of the threat assessment referred to in the previous paragraph, the obliged entities shall implement at least the measures referred to in Articles 21 and 22 of this Act.

(3) If the threat assessment is assessed as medium, the competent national authority shall inform the obliged entities thereof and may recommend that they implement additional measures for the security of network or information systems. The competent national authority may also inform the general public thereof on its website and in the media and may at the same time recommend appropriate measures.

(4) Where the threat assessment is assessed as critical, the competent national authority shall immediately inform the government, SNAV and the central body for responding to hybrid threats, and may also inform them, depending on the assessment of the relevant circumstances and information, when the threat is assessed as high. The competent national authority shall inform the obliged entities of the threat assessment as high or critical, and may also inform the general public on its website and in the media, and may at the same time recommend appropriate measures. The competent national authority shall inform the previously informed stakeholders referred to in this paragraph of the withdrawal or change of the threat assessment as crit

(5) In cases of high-risk assessment, obliged entities must immediately begin implementing at least the following additional security measures and implement them until such threat is removed:

– monitoring security notifications from the competent CSIRT or the competent national authority, relating to the declared high threat,

– checking the proper maintenance of logbooks on the operation of its key, control and control information systems and network parts,

– immediate implementation of security instructions from the CSIRT or the competent national authority, which relate to a declared high threat, and

– reporting on the security status of its networks and information systems and on the implementation of measures the manner as follows from the safety instructions in the previous indent.

(6) In cases of critical threat assessment, in addition to the measures referred to in the previous paragraph, the obliged entities must immediately begin implementing the following additional security measures and implement them until such threat is lifted:

1. continuous monitoring of security notifications from the competent CSIRT or the competent national authority relating to the declared critical threat,

2. verifying the proper functioning of the recording and maintenance of log records referred to in Article 24 of this Act and reporting on this and any activities carried out in accordance with point 6 of this paragraph,

3. monitoring all traffic on its network to identify anomalies and report on this and any activities carried out in accordance with point 6 of this paragraph,

4. immediate implementation of any security instructions from the CSIRT or the competent national authority relating to the declared critical threat,

5. immediate notification of incidents regardless of the deadlines set out in Article 30 of this Act,

6. at least weekly reporting to the competent CSIRT group on the security status of its networks and information systems, including detections of security events and related activities, and on the implementation of the security instructions referred to in point 1 of this paragraph, and

7. more frequent reporting to the competent CSIRT group on the contents from the previous point, if this results from the safety instructions referred to in point 1 of this paragraph.

(7) Notwithstanding the fifth and sixth paragraphs of this Article, the competent national authority may, by written decision, impose on the liable party such appropriate and proportionate measures as are strictly necessary to mitigate the risk. In urgent cases where the issuance of a written decision could, due to the passage of time, adversely affect the effectiveness of the measures to mitigate the risk, the competent national authority may also impose the relevant measures on the liable party by oral decision. In such a case, a written copy of the oral decision shall be served on the liable party no later than 48 hours after the oral decision.

(8) Measures issued pursuant to the preceding paragraph shall be determined to such an extent and for such a period as is strictly necessary to achieve the purpose referred to in the preceding paragraph. No appeal shall be permitted against the decision referred to in the preceding paragraph, but an administrative dispute shall be permitted.

(9) In order to reduce the assessment of a high or critical threat and consequently to prevent the emergence of a crisis or to manage it, the competent national authority may issue a written order ordering the implementation of urgent measures at the obliged entities, security operations centres of state administration bodies or CSIRT groups. The order shall specify in particular the type and scope of the work to be carried out at the aforementioned entities and the deadline for their implementation. If the issuance of a written order could, due to the passage of time, negatively affect the effectiveness of the measures to reduce the relevant threat assessment, the competent national authority may also decide on this by means of an oral order. In such a case, a written copy of the oral order shall be served on the obliged entity no later than 48 hours after the oral order.

(10) The competent national authority shall inform the Commission of the measures referred to in paragraphs 7 and 9 of this Article 11 informs the government and SNAV and the central authority for responding to hybrid threats.

VIII. CYBER DEFENSE

Article 38

(cyber defense)

To prevent cyber threats and incidents in cyberspace and to mitigate their impacts, cyber defense is implemented, which includes all layers of cyberspace, namely social, logical-technical and physical. In doing so:

– the social layer encompasses users of interconnected communications, who may be natural or legal persons and their virtual identities,

– the logical-technical layer includes digital data from the third indent of point 31 of Article 5 of this law and

– the physical layer covers networks and devices from the first and second indents of point 31 of Article 5 of this law.

Article 39

(cyber defense at the level of state authorities)

(1) Cyber defence measures and activities at the level of state authorities shall be coordinated and implemented by the competent national authority, CSIRTs and the ministry responsible for defence, the ministry responsible for information and communication systems management, the ministry responsible for foreign affairs, the ministry responsible for the interior, the Police, the Slovenian Intelligence and Security Agency and other state authorities in accordance with their competences in ensuring national security. They shall implement coordinated organisational, logical-technical, technical and administrative measures and activities at different levels to ensure comprehensive cyber security in accordance with their competences. Coordination of cyber defence at the level of state authorities shall be carried out by the competent national authority, which shall establish a coordination group for this purpose.

(2) The authorities referred to in the previous paragraph shall ensure appropriate cyber defence capabilities in the areas for which they are competent. To this end, they may establish their own security operations centres of state administration bodies, which shall meet at least the minimum requirements:

– constantly ensuring the availability of its communication channels,

– premises and supporting information systems are in secure locations,

– ensure the confidentiality and reliability of their activities,

– have sufficient staff to ensure continuous availability of services, with ensure that this staff is appropriately trained, and

– have backup systems and a backup workspace to ensure the continuity of their services.

(3) The competent national authority, the ministry responsible for the management of information and communication systems, the ministry responsible for defence, the ministry responsible for foreign affairs, the Police and the Slovenian Intelligence and Security Agency shall constantly monitor the situation and responses to events in cyberspace in their area of operation.

(4) The competent national authority for the implementation of point 2 of the second paragraph of Article 10 of this Act shall establish a cyber defence situation centre for the early detection of cyber threats, which is intended for the detection and monitoring of cyber threats and the implementation of procedures for limiting the consequences of cyber threats. The bodies responsible for defence planning, which are determined on the basis of the law governing defence, may be included in the cyber defence situation centre, which, in the event of their inclusion, shall enable the competent national authority to have direct, necessary and proportionate insight into the operation of their network and information system. The cyber defence situation centre shall operate as an internal organisational unit of the competent national authority.

(5) The competent national authority may also offer the capacity of the cyber defence situation centre to essential and important entities that are not the bearers of defence planning referred to in the previous paragraph. In doing so, the entities involved in the early detection of cyber threats shall provide the competent national authority with direct, necessary and proportionate insight into the operation of their network and information system.

(6) The competent authorities referred to in the first paragraph of this Article shall notify the establishment of a security operations centre of a state administration body to the competent national authority within 30 days of its establishment and shall at the same time submit a declaration of compliance with the requirements referred to in the second paragraph of this Article.

(7) The implementation of cyber defence referred to in the first paragraph of this Article shall be complemented by the inclusion of the bodies and CSIRT groups referred to in this Article in international networks and their active participation in these networks, as well as by other forms of multilateral and bilateral cooperation.

(8) Security operations centres of state administration bodies shall submit to the competent national authority a weekly and annual report on the performance of their tasks. The report shall include information on significant incidents notified to the competent CSIRT and on other incidents detected.

Article 40

(cooperation in the field of cyber defence)

(1) For cyber defence, the competent national authority may cooperate with public administration entities, the economy, research and development organisations, scientific institutions, interest groups and individuals.

(2) The competent national authority may cooperate in implementing cyber defence also invites individuals:

– who are citizens of the Republic of Slovenia,

– who have not been placed under guardianship by a final decision,

– who are at least 18 years old,

– who have not been finally convicted of an intentional criminal offence prosecuted ex officio and have not been sentenced to an unconditional prison sentence of more than six months

or have not been finally convicted of criminal offences under Articles 221 and 237 of the Criminal Code (Official Gazette of the Republic of Slovenia, No. 50/12 – official consolidated text, 6/16 – amended, 54/15, 38/16, 27/17, 23/20, 91/20, 95/21, 186/21, 105/22 – ZZNŠPP and 16/23; hereinafter referred to as the KZ-1),

– against whom no final indictment has been filed for an intentional criminal offence that is prosecuted ex officio, or criminal proceedings have not been initiated on suspicion of committing a criminal offence under Articles 221 and 237 of the Criminal Code-1,

– have the consent of their employer, if they are in an employment relationship,

– have the appropriate knowledge and competences to perform tasks in the field of information and cybersecurity and

– agree to psychological testing and security screening pursuant to Article 99 of the Police Tasks and Powers Act (Official Gazette of the Republic of Slovenia, No. 15/13, 23/15 – amended, 10/17, 46/19 – amended) US, 47/19 and 153/21 – sec. US).

(3) The competent national authority shall publish the invitation to participate referred to in the previous paragraph on the central website of the state administration.

(4) The competent national authority shall select candidates for participation in cyber defence referred to in the second paragraph of this Article and shall initiate the psychological testing and security screening procedures referred to in the last indent of the second paragraph of this Article for them. After successfully completing the security screening, they shall be included in the list of individuals participating in cyber defence. This list shall contain:

– name, surname and date of birth,

– tax number,

– name, address, telephone number and email address,

– education achieved,

– possible employment and

– knowledge and competences.

(5) The competent national authority shall offer the individual from the list referred to in the previous paragraph the conclusion of a contractual relationship, which shall regulate the type or form of the contractual relationship, mutual rights and obligations and remuneration. If the individual is in an employment relationship, the provisions on supplementary work from the law governing employment relationships shall be taken into account for the regulation of his rights and obligations. After concluding the contractual relationship, the competent national authority shall organise preparations, additional training and exercises for the individual to operate in the field of cyber defence.

(6) The competent national authority shall, depending on the needs and the state of threat to cybersecurity, form one or more operational groups for cyber defence, which shall include individuals with whom it has concluded a contract referred to in the previous paragraph and representatives of state authorities, local self-government bodies, companies, institutions and other organisations referred to in the first paragraph of this Article, which have undergone security checks, as specified in the eighth indent of the second paragraph of this Article. When forming operational groups, any potential conflicts of interest of individuals towards obliged entities shall also be taken into account.

(7) The director of the competent national authority shall appoint the head and deputy head of each operational group referred to in the previous paragraph. Where the head or deputy head is

appoints a person from a state authority who is not an employee of the competent national authority, the consent of his/her superior shall be ensured. The administrative and technical conditions for the operation of the operational teams referred to in the previous paragraph shall be ensured by the competent national authority.

(8) The participation of civil servants in the operational group referred to in the sixth and seventh paragraphs of this Article is in the interest of the employer in accordance with the provisions on performing additional work in the interest of the employer referred to in the law governing civil servants.

Article 41

(additional assistance in the field of cyber defense)

(1) The competent national authority may provide additional assistance to obliged entities in the field of cyber defence in the event of cyber threats and incidents about which the competent national authority notifies the government and SNAV in accordance with this Act, and in the event of large-scale cyber incidents or crises.

(2) The obliged entity or the competent CSIRT may request additional assistance from the competent national authority referred to in the previous paragraph, stating the circumstances for which assistance is requested. The provision of additional assistance shall be approved in each individual case by the director of the competent national authority, taking into account the aspects of the urgency of managing the situation or events referred to in the previous paragraph, the availability of operational teams and other capabilities for implementing cyber defence, and the current assessment of cyber security in the country.
The method and rules for providing additional assistance and the possibility of involving operational teams from the previous article shall be coordinated between the competent national authority, the competent CSIRT and the obligated party, taking into account the rules set out in the national response plan.

(3) If the assistance referred to in the previous paragraph is not granted, the competent national authority shall inform the applicant referred to in the previous paragraph, who may apply for assistance again in the event of changed circumstances.

Article 42

(assistance with cyber defence in the European Union)

(1) The Republic of Slovenia may request assistance in implementing cyber defence from other Member States of the European Union or relevant institutions, bodies, offices and agencies of the European Union. It may also provide assistance to the aforementioned entities in implementing cyber defence.

(2) If the competent national authority for the management of the situation or events referred to in the first paragraph of the previous article assesses that the persons liable under this Act or the competent CSIRT group need assistance from another state or Member States of the European Union in the cyber defence of the Republic of Slovenia, it shall immediately inform SNAV, which shall formulate a position on the proposal for a request and send it to the government for decision. The mutual agreement on assistance shall also determine the coverage of any costs of both parties, with any costs of the Republic of Slovenia being covered by the recipient of the assistance.

(3) The competent national authority shall notify SNAV of the receipt of a request from competent institutions or bodies of another country or Member State of the European Union for assistance in cyber defence, which shall formulate a position on the proposed response to such a request and submit it to the government for decision. The response to the request shall take into account the availability of cyber defence capabilities and

current assessment of cybersecurity in the country. The mutual assistance agreement also determines the coverage of costs for both parties, with the costs of the Republic of Slovenia being covered by the authority from which the seconded person comes.

Article 43

(assistance in cyber defense at the international level)

(1) The Republic of Slovenia may also request assistance in implementing cyber defence from third countries or international organisations with which it has concluded international agreements. In addition, it may provide assistance to the aforementioned entities in implementing cyber defence.

(2) The previous article shall apply mutatis mutandis to the provision and receipt of assistance.

(3) The Republic of Slovenia may participate in joint cyber defence units established by international organisations of which it is a member. The decision on such participation shall be taken by the Government on the proposal of SNAV.

Article 44

(working during less favorable working hours)

(1) Employees of bodies implementing cyber defence must also work during less favourable working hours when this is necessary for the performance of tasks specified in this Act, if security conditions so require, or if this is the only way to perform certain tasks that cannot be postponed or must be completed within a certain deadline. Work during less favourable working hours shall be ordered by the head of the body.

(2) Working during less favourable working hours is:

1. working with unevenly distributed working hours,

2. shift work,

3. work on Saturdays, Sundays, holidays and other days off,

4. working overtime,

5. afternoon and night work and

6. part-time work.

(3) Work during less favourable working hours is carried out by redistributing working hours within the framework of a certain regular monthly or annual work obligation, except in the case of work beyond full-time working hours.

(4) The workplaces where work is carried out in accordance with the previous paragraph shall be determined in the act on organization and systematization.

(5) Notwithstanding the second to fourth paragraphs of this Article, for work during less favourable working hours:

– the Ministry of Defence and the Slovenian Armed Forces apply the provisions regulating work in less favourable working conditions and less favourable working hours in the law governing defence and in the law governing service in the Slovenian Armed Forces,

– the Police apply the provisions regulating work in less favourable working conditions and less favourable working hours in the law regulating the organisation and work of the Police,

– the Slovenian Intelligence and Security Agency applies the provisions regulating work in less favourable working conditions and less favourable working hours in the law governing the operation Slovenian Intelligence and Security Agency, and

– the Administration of the Republic of Slovenia for Protection and Rescue applies the provisions regulating work in less favourable working conditions and less favourable working hours in the law regulating protection against natural and other disasters.

IX. SUPERVISION

Article 45

(general provisions)

(1) The information security inspectors of the competent national authority (hereinafter referred to as: inspector) shall be responsible for supervising the implementation of the provisions of this Act, the regulations adopted on its basis, and the execution of administrative decisions issued on the basis of the fifth or seventh paragraph of Article 36, the seventh paragraph of Article 37 of this Act, and the execution of orders issued on the basis of the ninth paragraph of Article 36 and the ninth paragraph of Article 37 of this Act, except in the field of defence, where this supervision is carried out by the Defence Inspectorate of the Republic of Slovenia, and in the field of intelligence and security activities, where this supervision is carried out by the Inspectorate of the Republic of Slovenia for Internal Affairs.

(2) The inspector is also responsible for supervising the implementation of the provisions of Regulation 2019/881/EU. and the implementation of European certification schemes and the enforcement of administrative decisions issued by the national cybersecurity certification body on the basis of the seventh or eighth paragraph of Article 27 of this Act.

(3) The Inspector shall also supervise the implementation of the implementing acts of the European Commission adopted pursuant to Directive 2022/2555/EU, which have direct effect in the legal order of the Republic of Slovenia.

(4) In the supervision procedure under this Act, the provisions of the Act governing inspection control, unless otherwise provided for by this Act.

(5) When performing inspection tasks at a person liable under this Act, the In addition to the rights under the law governing inspection supervision, the inspector also has the following powers:

1. carry out on-site inspection and remote monitoring, which may be carried out together with qualified experts;

2. conduct a security inspection based on objective, non-discriminatory, fair and transparent risk assessment criteria;

3. perform direct inspection of data, documentation, and network and information systems systems;

4. verify the conditions and method of implementing measures to manage cybersecurity risks;

5. inspect areas, facilities and premises of the obliged entities where key, control and supervisory functions are information systems and data;

6. review documentation on the implementation of prescribed obligations to notify about cybercrime incidents and other obligations based on the requests of the competent authorities under this Act;

7. review reports on the implementation of an audit of information systems and the implementation of security checks of the network and information systems, and

8. review other documentation necessary for the performance of the inspection.

(6) Obliged persons must, when carrying out an inspection, submit the requested information and data to the inspector without delay and enable access to systems, areas, facilities and premises.

(7) No appeal shall be allowed against a decision issued in supervision proceedings under this Act. appeal, but an administrative dispute is permitted.

(8) In the inspection procedure, the inspector may, on the basis of a reasoned proposal by the liable party for an extension of the deadlines for the elimination of irregularities and deficiencies, submitted before the expiry of the deadline for the implementation of the ordered measures, extend the deadlines for the elimination of irregularities and deficiencies or the implementation of the ordered measures, taking into account the activities already carried out by the liable party to eliminate irregularities and deficiencies, the objective circumstances for the delay and the consequences for the public interest.

(9) In addition to the measures specified in the law governing inspection supervision, the inspector may also order measures specified in this law or measures specified in Regulation 2019/881 /EU.

Article 46

(supervision of significant entities)

(1) When carrying out his supervisory tasks, the inspector may carry out random inspections at essential entities.

(2) If, while performing inspection tasks, an inspector finds that a significant entity has violated this Act, another regulation or another act, the implementation of which he supervises, he shall, in addition to the rights and obligations under the Act regulating inspection, also have the right and obligation to:

1. order the implementation of a regular and targeted audit of compliance with regulations in the field of information and cybersecurity, carried out by an information systems auditor;

2. order the performance of an extraordinary compliance audit by an information systems auditor when this is justified due to a significant incident or because a significant entity has clearly violated this Act;

3. order the obliged entity to inform natural or legal persons in relation to whom it provides services or carries out an activity and who could be affected by a significant cyber threat of the nature of the threat and of the protective or remedial measures that those natural or legal persons can take in response to that threat;

4. order the obliged entity to implement the recommendations made on the basis of the compliance audit carried out within a reasonable time;

5. appoint an authorized person with precisely defined tasks for a specified period to monitor whether the significant entity complies with Articles 21, 22, 29 and 30 of this Act, and

6. order the obligated party to publish violations of this Act in a specified manner.

(3) If the inspector determines that the measures ordered to eliminate irregularities or deficiencies were not effective, he shall set a deadline for the essential entity concerned by such measures within which it must take the necessary measures to eliminate the irregularities or deficiencies or comply with the inspector's requirements. If the essential entity fails to take the measures within the specified deadline, the inspector may by decision:

1. temporarily prohibit the performance of part of the services or activities or temporarily prohibit the performance of all the services or activities performed by the material entity, and

2. requires a temporary ban on the performance of management functions for all persons who perform management tasks at the level of chief executive officer or legal representative for a significant entity.

(4) A temporary revocation or prohibition imposed pursuant to the preceding paragraph shall apply only until the relevant essential entity has taken the necessary measures to remedy the deficiencies or has complied with the inspector's requirements for which such measure was applied.

(5) The measures referred to in the third paragraph of this Article shall not apply to public administration entities at the state level.

(6) When adopting measures referred to in the second and third paragraphs of this Article, the inspector shall take into account the circumstances of each individual case, taking due account of:

1. the seriousness of the violation and the importance of the provisions violated, whereby serious violations in each case case are considered:

– repeated violations,

– failure to report or resolve significant incidents,

– failure to remedy deficiencies in accordance with the inspector's binding instructions,

– obstructing audits or monitoring activities ordered by an inspector after a violation has been identified,

– providing false information regarding cyber risk management measures security or reporting obligations under Articles 21, 22, 29 or 30 of this Act;

2. duration of the infringement;

3. any relevant previous violations by the relevant material entity;

4. any material or non-material damage caused, including financial or economic losses, effects on other services and the number of users affected;

5. intent or negligence of the perpetrator of the violation;

6. measures taken by the significant entity to prevent or reduce the financial or non-pecuniary damage;

7. adherence to approved codes of conduct or approved certification mechanisms; and

8. level of cooperation between responsible natural or legal persons and the inspector.

(7) The measures imposed by the inspector on essential entities in relation to the obligations under this Act must be effective, proportionate and dissuasive, taking into account the circumstances of the individual case.

(8) The regular and targeted compliance audits referred to in point 1 of the second paragraph of this Article shall be based on risk assessments carried out by the competent national authorities or the relevant entity subject to the audit, or on other available risk information. The report on the targeted security audit carried out shall be made available to the inspector.

(9) The costs of a regular, extraordinary or targeted compliance audit carried out by an information systems auditor shall be borne by the significant entity, except in duly justified cases where the competent authority decides otherwise.

(10) When exercising his powers, the inspector shall state the purpose of the request and specify the information requested. When ordering an extraordinary compliance audit referred to in point 2 of the second paragraph of this Article, the inspector shall determine the scope of the audit.

(11) When carrying out supervision over a significant entity that is designated as critical under the law governing critical infrastructure, the inspector shall notify the competent inspection body for the area of critical infrastructure. The inspector for the area of critical infrastructure may also submit a reasoned initiative to the Information Security Inspectorate to carry out supervision in relation to an entity that is designated as critical under the law governing critical infrastructure.

(12) The inspector shall cooperate with the supervisory authorities designated by the law governing the implementation of Regulation 2022/2554/EU. on digital operational resilience for the financial sector. In doing so, the inspector shall ensure that the supervision of a significant entity designated as a key third party ICT service provider pursuant to Article 31 of Regulation 2022/2554/EU, inform the Supervisory Forum established pursuant to the first paragraph of Article 32 of Regulation 2022/2554/EU thereof.

(13) When an inspector carries out administrative enforcement of enforceable decisions issued in the procedure for the supervision of essential entities and in doing so applies coercive measures by imposing fines, the first fine, regardless of the law governing the general administrative procedure, may not exceed EUR 10,000. Any subsequent fine for coercion may be imposed again up to this amount.

(14) The previous paragraph does not apply to legal entities under public law.

(15) The head of a body of a public administration entity or the responsible person of a legal entity that is a material entity, i.e. a natural person or persons who manage, supervise or administer the operations of the legal entity or who are competent and obliged to ensure lawful operations under the law, the act of establishment or authorisation, is the person responsible for ensuring compliance with the operations of the material entity under this Act (hereinafter: the responsible person of the material entity) and is liable for violations of their duties in accordance with this Act.

Article 47

(supervision of significant entities)

(1) An inspection of a significant entity shall be carried out if the inspector receives evidence, indications or information that the significant entity is not implementing measures to manage cybersecurity risks in accordance with the prescribed obligations under this Act, or that it is not fulfilling its obligations regarding notification of cyber incidents in the prescribed manner and within the prescribed deadlines, or that it is not acting in accordance with the requirements of the competent national authority under this Act.

(2) If, in the course of performing inspection tasks, an inspector finds that a significant entity has violated this Act or another regulation or other act, the implementation of which he supervises, he shall, in addition to the rights and obligations under the Act regulating inspection, also have the right and obligation to:

1. order the implementation of a targeted audit of compliance with regulations in the field of information and cybersecurity performed by an information systems auditor,

2. order that the obliged entity informs natural or legal persons for whom it provides services or carries out activities and who could be affected by a significant cyber threat of the nature of the threat and of the protective or remedial measures that these natural or legal persons can take in response to that threat,

3. order that the liable party implement the recommendations made on the basis of the targeted targeted compliance audits, and

4. order that the person liable publish violations of this Act in a specified manner.

(3) When ordering the measures referred to in the previous paragraph, the inspector shall respect the procedural rights of the relevant entity in the supervision procedure and take into account the circumstances of each individual case, taking into account:

1. the seriousness of the violation and the importance of the provisions violated, whereby serious violations are, among other things, in any case, the following are considered:

– repeated violations,

– failure to report or resolve significant incidents,

– failure to remedy deficiencies in accordance with the inspector's binding instructions,

– obstructing audits or monitoring activities ordered by an inspector after a violation has been identified,

– providing false information regarding cyber risk management measures security or reporting obligations under Articles 21, 22, 29 and 30 of this Act;

2. the duration of the infringement;

3. any relevant previous violations by the relevant significant entity;

4. any material or non-material damage caused, including financial or economic losses, effects on other services and the number of users affected;

5. possible intent or negligence of the perpetrator of the violation;

6. any measures taken by the significant entity to prevent or mitigate material or non-material damage;

7. possible adherence to approved codes of conduct or approved certification mechanisms and

8. level of cooperation between responsible natural or legal persons and the inspector.

(4) Targeted compliance audits referred to in point 1 of the second paragraph of this Article shall be based on risk assessments carried out by the competent national authorities or the relevant entity subject to the audit, or on other available risk information. The report on the targeted compliance audit carried out shall be made available to the inspector.

(5) The costs of a targeted compliance audit carried out by an information systems auditor shall be borne by the significant entity, except in duly justified cases where the competent authority decides otherwise.

(6) The head of a body of a public administration entity or the responsible person of a legal entity that is a significant entity, i.e. a natural person or persons who manage, supervise or administer the operations of a legal entity or who are competent and obliged to ensure lawful operations under the law, the act of establishment or authorisation, is the person responsible for ensuring compliance with the operations of the significant entity under this Act (hereinafter: the responsible person of the significant entity) and is liable for violations of their duties in accordance with this Act.

(7) When an inspector carries out administrative enforcement of enforceable decisions issued in the course of supervision of significant entities and in doing so applies coercive measures by imposing fines, the first fine, regardless of the law governing general administrative procedure, may not exceed EUR 7,000. Any subsequent fine for coercion may be imposed again up to this amount.

(8) The previous paragraph does not apply to legal entities under public law.

(9) The inspector shall cooperate with the supervisory authorities designated by the law governing the implementation of Regulation 2022/2554/EU. on digital operational resilience for the financial sector. In doing so, the inspector shall ensure that the supervision of a significant entity designated as a key third party ICT service provider pursuant to Article 31 of Regulation 2022/2554/EU, inform the Supervisory Forum established pursuant to the first paragraph of Article 32 of Regulation 2022/2554/EU thereof.

Article 48

(supervision of entities under Regulation 2019/881/EU)

(1) Inspection of entities under Regulation 2019/881/EU shall be carried out if the inspector receives evidence, indications or information that a conformity assessment body, a holder of European cybersecurity certificates or an issuer of EU declarations of conformity does not comply with the requirements of Regulation 2019/881/EU or European certification schemes.

(2) When exercising his powers, the inspector shall state the purpose of the request and specify the information requested. When ordering a targeted compliance audit, the inspector shall determine the scope of the audit.

(3) When performing inspection tasks at a taxable person referred to in Regulation 2019/881 /EU In addition to the rights under the law governing inspection supervision, the inspector also has the right to conduct on-site inspections and remote supervision, which he or she may carry out together with qualified experts.

(4) If, while performing inspection tasks, the inspector finds that the person liable under Regulation 2019/881/EU has violated this Act or another regulation or other act, the implementation of which he supervises, has, in addition to the rights and obligations under the Act regulating inspection supervision, the right and obligation to:

1. order the implementation of a targeted audit of compliance with Regulation 2019/881/EU, which is carried out by information systems auditor, and

2. order the implementation of appropriate measures to ensure compliance with the requirements of Regulation 2019/881 /EU or European certification schemes.

(5) The inspector may propose to the national cybersecurity certification body to revoke a European cybersecurity certificate where such certificate does not comply with Regulation 2019/881/EU. or with a European certification scheme.

(6) The report on the conducted targeted compliance audit referred to in point 1 of the fourth paragraph of this Article shall be submitted to the inspector.

(7) The costs of a targeted compliance audit carried out by an information systems auditor shall be borne by the entity referred to in the first paragraph of this Article.

Article 49

(appointment of an information systems auditor)

(1) A significant or important entity shall select an information systems auditor to conduct a compliance audit requested by an inspector under this Act. It shall notify the inspector of its selection and the commencement of the compliance audit procedure with regulations in the field of information security within 30 days of the inspector's request.

(2) Notwithstanding the previous paragraph, a significant or important entity that has among its employees a person who has the status of an active certified information systems auditor may also select that employee for the relevant audit, provided that it can ensure the impartiality and independence of the auditor.

(3) If a significant or important entity does not select an information systems auditor in accordance with the first or second paragraph of this Article, the information systems auditor shall be appointed by the inspector by decision.

Article 50

(violations constituting a breach of personal data protection)

(1) The Inspector shall inform the Information Commissioner about the handling of matters referred to in the first paragraph of Article 45 of this Act, which result in a violation of the protection of personal data. The Information Commissioner shall also be notified in cases of suspected violations of personal data protection. The inspector shall also inform the Agency for Communications Networks and Services of the Republic of Slovenia about the handling of such matters relating to operators under the law regulating electronic communications.

(2) When the Information Commissioner imposes a fine on the basis of the law governing the protection of personal data due to a violation of the protection of personal data referred to in the previous paragraph, the inspector shall not impose a fine for the same conduct, but may impose measures pursuant to this law.

(3) Where the supervisory authority competent in accordance with Regulation (EU) 2016/679 has **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, 4.5.2016, p. 1), established in another Member State of the European Union as an inspector, the inspector shall notify the Information Commissioner of a possible breach of personal data protection referred to in the first paragraph of this Article.**

Article 51

(mutual assistance and cross-border surveillance)

(1) Where a significant or important entity falls within the jurisdiction of the competent national authority in accordance with Article 31 of this Act, but provides services:

– in more than one Member State of the European Union or

– in one or more Member States of the European Union and its network and information systems are in another Member State of the European Union or in more than one Member State of the European Union,

The inspector may carry out inspections of these entities in cooperation with the competent supervisory authorities of the other Member States of the European Union concerned. The inspector and the competent supervisory authorities of the other Member States of the European Union shall assist each other in carrying out such inspections.

(2) For the implementation of mutual assistance referred to in the previous paragraph, the inspector shall, through a single contact points:

– informs the competent supervisory authorities in other Member States of the European Union of its adopted supervisory measures and measures imposed to eliminate irregularities,

– may request the competent supervisory authority in another Member State of the European Union to carry out supervisory measures or the imposition of measures to eliminate irregularities and

– request proportionate mutual assistance from the competent supervisory authority in another Member State of the European Union or provide it with such assistance upon a reasoned request.

(3) The request for mutual assistance referred to in the last indent of the previous paragraph may include requests for the submission of relevant information and for the implementation of supervisory measures, including requests for the implementation of on-site inspections, remote monitoring or targeted security assessments.

(4) An inspector who has been sent a request for mutual assistance from a competent supervisory authority from another Member State of the European Union may not refuse such a request when carrying out the inspection referred to in the first paragraph of this Article, unless he establishes that:

– is not competent to provide the requested mutual assistance,

– the requested mutual assistance is not consistent with the inspector's powers under this Act and

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

(5) Before rejecting the request referred to in the previous paragraph, the inspector shall consult with other competent supervisory authorities of the Member States of the European Union which are also competent to handle the supervision in the specific case. If another Member State of the European Union which is also competent to handle the supervision procedure in question so requests, the inspector shall also consult with the European Commission and ENISA before rejecting the request for mutual assistance.

(6) In the cases referred to in the first paragraph of this Article, joint inspections may be carried out on the basis of and within the framework of a joint agreement between the inspector and the authorities of other Member States of the European Union competent for such inspections.

X. PENAL PROVISIONS

Article 52

(violations of essential entities)

(1) A fine of 0.5 percent to 2 percent of the total annual turnover of the legal person achieved in the previous business year, but not less than EUR 10,000 and not more than EUR 10,000,000, whichever is the higher, shall be imposed on a legal person if:

– fails to fulfill the obligations referred to in the first, second, third, fourth or fifth paragraphs of Article 21 of this law,

– fails to fulfill the obligations referred to in the first, second, third, fourth, fifth, sixth, seventh, eighth, ninth, eleventh or thirteenth paragraphs of Article 22 of this Act,

– fails to fulfill the obligations referred to in the first, second, third, fourth, fifth, sixth, seventh or ninth paragraphs of Article 24 of this Act,

– fails to fulfill the obligations under the first, second, third, fourth, fifth, sixth and seventh paragraph 29 of Article 29 of this Act or

– fails to fulfill the obligations referred to in the first or second paragraph of Article 30 of this Act.

(2) A fine of between EUR 5,000 and EUR 25,000 shall be imposed on a sole proprietor or an individual who independently carries out an activity if he commits an offence referred to in the previous paragraph.

(3) A fine of between EUR 1,000 and EUR 10,000 shall be imposed on the responsible person of a legal entity or the responsible person of a sole proprietor, the responsible person of an individual who independently carries out an activity, and the responsible person in a state body or self-governing local community, if they commit an offence referred to in the first paragraph of this Article.

(4) A legal entity shall be punished with a fine of EUR 3,000 to EUR 15,000 if:

1. fails to fulfill the obligations referred to in the second or fifth paragraph of Article 8 of this Act,

2. fails to fulfill the obligations referred to in the second, third, fourth or fifth paragraphs of Article 20 of this law,

3. fails to fulfill the obligations referred to in the first or second paragraph of Article 25 of this Act,

4. fails to fulfill the obligations referred to in the first paragraph of Article 26 of this Act,

5. fails to fulfill the obligations referred to in the sixteenth paragraph of Article 27 of this Act,

6. fails to fulfill the obligations referred to in the first paragraph of Article 28 of this Act,

7. fails to fulfill the obligations referred to in the first, second or third paragraphs of Article 32 of this Act,

8. fails to fulfill the obligations referred to in the first, second, third, fourth or fifth paragraphs of Article 33 of this law,

9. fails to fulfill the obligations referred to in the fifth or sixth paragraph of Article 37 of this Act,

10. fails to comply with the obligations arising from a decision issued on the basis of paragraphs 7 or 9 of Article 37. of this Act, or

11. fails to fulfill the obligations referred to in the first paragraph of Article 49 of this Act.

(5) A fine of between EUR 1,000 and EUR 10,000 shall be imposed on a sole proprietor or an individual who independently carries out an activity if he fails to fulfill the obligations referred to in the previous paragraph of this Article.

(6) A fine of between EUR 500 and EUR 3,000 shall be imposed on the responsible person of a legal person or the responsible person of a sole proprietor, the responsible person of an individual who independently carries out an activity, and the responsible person in a state body or self-governing local community if they fail to comply with the obligations referred to in the fourth paragraph of this Article.

Article 53

(violations of important entities)

(1) A fine of 0.3 percent to 1.4 percent of the total annual turnover of the legal person achieved in the previous business year, but not less than EUR 7,000 and not more than EUR 7,000,000, whichever is the higher, shall be imposed on a legal person if:

– fails to fulfill the obligations referred to in the first, second, third or fifth paragraphs of Article 21 of this Act,

– fails to fulfill the obligations from the first, second, third, fourth, fifth, sixth, seventh, the eighth, ninth or thirteenth paragraph of Article 22 of this Act,

– fails to fulfill the obligations under the first, second, third, fourth, sixth, seventh or ninth paragraph 24 of Article 24 of this Act,

– fails to fulfill the obligations under the first, second, third, fourth, fifth, sixth or seventh paragraph 29 of Article 29 of this Act or

– fails to fulfill the obligations referred to in the first or second paragraph of Article 30 of this Act.

(2) A fine of between EUR 3,000 and EUR 20,000 shall be imposed on a sole proprietor or an individual who independently carries out an activity and is a significant entity under this Act if he commits an offence referred to in the previous paragraph.

(3) A fine of between EUR 1,000 and EUR 7,000 shall be imposed on the responsible person of a legal person or the responsible person of a sole proprietor, the responsible person of an individual who independently carries out an activity, and the responsible person in a state body, self-governing local community that is a significant entity under this Act, if they commit an offence referred to in the first paragraph of this Article.

(4) A legal entity shall be punished with a fine of EUR 1,000 to EUR 10,000 if:

1. fails to fulfill the obligations referred to in the second or fifth paragraph of Article 8 of this Act,

2. fails to fulfill the obligations referred to in the second, third, fourth or fifth paragraphs of Article 20 of this law,

3. fails to fulfill the obligations referred to in the third, fourth or fifth paragraphs of Article 25 of this Act,

4. fails to fulfill the obligations referred to in the first paragraph of Article 26 of this Act,

5. fails to fulfill the obligations referred to in the sixteenth paragraph of Article 27 of this Act,

6. fails to fulfill the obligations referred to in the first paragraph of Article 28 of this Act,

7. fails to fulfill the obligations referred to in the first, second or third paragraphs of Article 32 of this Act,

8. fails to fulfill the obligations referred to in the fifth or sixth paragraph of Article 37 of this Act,

9. fails to comply with the obligations arising from the decision issued on the basis of the seventh or ninth paragraph of Article 37 of this Act,

10. fails to fulfill the obligations referred to in the first paragraph of Article 49 of this Act.

(5) A fine of between EUR 500 and EUR 7,000 shall be imposed on a sole proprietor or an individual who independently carries out an activity if he fails to comply with the obligations referred to in the previous paragraph of this Article.

(6) A fine of between EUR 200 and EUR 2,000 shall be imposed on the responsible person of a legal person or the responsible person of a sole proprietor, the responsible person of an individual who independently carries out an activity, and the responsible person in a state body or in a self-governing local community if they fail to comply with the obligations referred to in the fourth paragraph of this Article.

Article 54

(violations of the operator of the central state information and communication system)

The person responsible for the violation shall be punished with a fine of between 200 euros and 2,000 euros. the operator of the central state information and communication system, if:

– does not provide the competent CSIRT group referred to in the first paragraph of Article 13 of this Act with insight into the operation of the information infrastructure of the central national information and communication system (seventh paragraph of Article 15),

– fails to implement the measures ordered by the competent CSIRT group referred to in the first paragraph of Article 13 of this Act (eighth paragraph of Article 15) in its information and communication system.

Article 55

(offences for breach of Regulation 2019/881/EU)

(1) A fine of between EUR 5,000 and EUR 50,000 shall be imposed on a manufacturer or provider of ICT products, services or processes who is a legal person if, contrary to Article 53 of Regulation 2019/881/EU: after a self-assessment of conformity, it issues an EU declaration of conformity corresponding to the basic level of assurance, even though the ICT product, service or process does not meet the requirements of the certification scheme.

(2) A fine of between EUR 1,000 and EUR 10,000 shall be imposed on a sole proprietor or an individual who independently carries out an activity who is a manufacturer or provider of ICT products, services or processes referred to in Article 53 of Regulation 2019/881/EU, if he commits an offense referred to in the previous paragraph.

(3) A fine of between EUR 500 and EUR 5,000 shall be imposed on the responsible person of a legal person or a responsible person of a sole proprietor, the responsible person of an individual who independently carries out an activity, and the responsible person in a state body, self-governing local community who is a manufacturer or provider of ICT products, ICT services or ICT procedures referred to in Article 53 of Regulation 2019/881/EU, if he commits an offense referred to in the first paragraph of this article.

(4) A fine of between EUR 3,000 and EUR 20,000 shall be imposed on a manufacturer or provider, who is a legal person, of certified ICT products, services and processes or ICT products, services and processes for which an EU declaration of conformity referred to in Article 55 of Regulation 2019/881/EU has been issued, if:

– does not provide additional information on cybersecurity referred to in the first paragraph of Article 55 of the Regulation 2019/881/EU whether this information is incomplete or misleading or

– before the expiry of the relevant European cybersecurity certificate or EU declaration of conformity in breach of the second paragraph of Article 55 of Regulation 2019/881/EU disables access to additional cybersecurity information or does not update the information.

(5) A fine of between EUR 500 and EUR 7,000 shall be imposed on a sole proprietor or an individual who independently carries out an activity who is a manufacturer or provider of certified ICT products, services and processes or ICT products, services and processes for which an EU declaration of conformity referred to in Article 55 of Regulation 2019/881/EU has been issued, if he commits an offense referred to in the previous paragraph.

(6) A fine of between EUR 500 and EUR 2,000 shall be imposed on the responsible person of a legal entity or a responsible person of a sole proprietor, the responsible person of an individual who independently carries out an activity, and the responsible person in a state body or local self-governing community who is a manufacturer or provider of certified ICT products, services and processes or ICT products, services and processes for which an EU declaration of conformity referred to in Article 55 of Regulation 2019/881/EU has been issued, if he commits an offence referred to in the fourth paragraph of this Article.

Article 56

(imposition of sanctions for misdemeanors)

(1) In addition to the general rules for imposing sanctions under the law governing minor offences, when deciding on the amount of the fine imposed, if essential and significant entities violate Articles 21, 22, 24, 29 or 30 of this Act, the annual turnover or annual balance sheet total of the essential or significant entity in the previous business year shall also be taken into account.

(2) When deciding on the imposition and amount of the fine referred to in this Article, the circumstances of the individual case and the elements referred to in the sixth paragraph of Article 46 or the third paragraph of Article 47 of this Act shall be taken into account.

Article 57

(imposing a fine in a speedy misdemeanor procedure)

A fine may be imposed for misdemeanors under this Act in expedited misdemeanor proceedings. even in an amount higher than the minimum prescribed fine determined by this Act.

Article 58

(application of provisions on misdemeanours)

The amount and ranges of fines specified in Articles 52 and 53 of this Act shall apply and be apply regardless of the provisions of the law governing misdemeanors.

XI. TRANSITIONAL PROVISIONS

Article 59

(CSIRTs)

Until the CSIRT teams referred to in the first paragraph of Article 13 of this Act are designated, their tasks shall be performed by:

– SIGOV-CERT, which operates as an internal organizational unit at the competent national authority and is responsible for handling incidents of public administration entities at the state and local levels and trust service providers provided by state administration entities, and

– SI-CERT, which operates as an internal organizational unit at the public infrastructure institution Academic and Research Network of Slovenia and is responsible for handling incidents reported by other obliged entities referred to in the first paragraph of Article 6 of this Act, which are not covered by the previous indent, and acts as the coordinator referred to in the first paragraph of Article 17 of this Act. It is also responsible for handling incidents reported voluntarily by entities that are not obliged entities under this Act in accordance with the second paragraph of Article 35 of this Act.

Article 60

(establishment of self-registration and lists and notification)

(1) The competent national authority shall establish a mechanism for self-registration of taxpayers referred to in Article 6 of this Act pursuant to the first paragraph of Article 8 of this Act within four months of the entry into force of this Act.

(2) Obliged persons who, upon the entry into force of this Act, meet the criteria set out in Articles 6 and 7 of this Act, shall complete their first registration under the self-registration mechanism within six months of the entry into force of this Act. Until the self-registration mechanism is established, the information shall be sent in digital form to the electronic address of the competent national authority.

(3) The authorities referred to in the seventh paragraph of Article 8 of this Act shall send the list of names referred to in this Article to the competent national authority for the first time within six months of the entry into force of this Act.

(4) The competent national authority shall establish the first list referred to in the fourth paragraph of Article 8 of this Act within one month after the expiry of the deadline referred to in the previous paragraph.

(5) The Government shall adopt the training programme for responsible persons referred to in the sixth paragraph of Article 20 of this Act within six months of the entry into force of this Act.

(6) The competent national authority shall establish a dedicated digital platform referred to in the tenth paragraph of Article 30 of this Act within one year of the entry into force of this Act. Until its establishment, the relevant entities shall send notifications referred to in Articles 29 and 35 of this Act to the electronic address of the competent CSIRT referred to in this Act. Until the establishment of this platform, the exchange of information referred to in the second paragraph of Article 18 of this Act shall also take place in digital form via the electronic addresses of the competent national authority and the participating authorities.

(7) The entities referred to in the first paragraph of Article 32 of this Act shall
provisions shall be notified to the competent national authority for the first time within six months of the entry into force of this Act.

(8) TLD name registries and entities providing domain name registration services shall establish the policies and procedures referred to in paragraphs 3 and 5 of Article 33 of this Act within six months of the entry into force of this Act.

(9) The authorities referred to in the first paragraph of Article 39 of this Act shall inform the competent national authority about the security operations centres of state administration bodies that meet the requirements referred to in the second paragraph of Article 39 of this Act, within thirty days of the entry into force of this Act.

(10) The authorities referred to in the first paragraph of Article 39 of this Act shall inform the competent national authority of the security operations centres of state administration bodies that do not meet the requirements referred to in the second paragraph of Article 39 of this Act within thirty days of the entry into force of this Act and shall ensure compliance with these requirements within one year of the entry into force of the Act.

Article 61

(status of providers of essential services and state administration bodies)

Entities that were designated as providers of essential services before 16 January 2023 on the basis of the second or third paragraph of Article 6 of the Information Security Act (Official Gazette of the Republic of Slovenia, Nos. 30/18, 95/21, 130/22 – ZEKom-2, 18/23 – ZDU-1O and 49/23; hereinafter: ZInfV) and state administration bodies that manage information systems and parts of networks or provide information services necessary for the smooth functioning of the state or for ensuring national security (hereinafter: state administration bodies), and were designated as obligated state administration bodies on the basis of the first paragraph of Article 9 of ZInfV before the entry into force of this Act, shall continue to be obligated as essential entities under this Act.

Article 62

(adoption of risk management measures)

(1) Essential and significant entities shall adopt measures to manage the risks to information and cybersecurity referred to in Articles 21 and 22 of this Act within eighteen months of the entry into force of this Act.

(2) Notwithstanding the previous paragraph, essential entities designated as providers of essential services pursuant to Article 6 of the ZInfV and state administration bodies designated pursuant to Article 9 of the ZInfV shall adopt measures to manage the risks to information and cyber security referred to in Articles 21 and 22 of this Act within one year of the entry into force of this Act. Until the expiry of this period, the security requirements, security documentation, security measures and the associated provisions on supervision and criminal provisions from the ZInfV and the regulations referred to in the second or third indent of the second paragraph of Article 69 of this Act shall apply to them.

(3) Notwithstanding the first paragraph of this Article, essential and significant entities that are operators under the Electronic Communications Act (Official Gazette of the Republic of Slovenia, Nos. 130/22 and 18/23 – ZDU-1O) shall adopt measures to manage the risks to information and cyber security referred to in Articles 21 and 22 of this Act within one year of the entry into force of this Act. Until the expiry of this period, the security measures referred to in Chapter VII of the Electronic Communications Act (Official Gazette of the Republic of Slovenia, Nos. 130/22 and 18/23 – ZDU-1O) and the general act referred to in the second indent of the third paragraph of Article 69 of this Act shall apply to them.

Article 63

(harmonization of the domain name registration database)

TLD name registries and entities providing domain name registration services shall align their domain name registration databases with the second and fourth paragraphs of Article 33 of this Act for registrations that were carried out before the entry into force of this Act, within eighteen months of the entry into force of this Act.

Article 64

(issuance of implementing regulations and strategies)

(1) The Government shall issue regulations referred to in the third paragraph of Article 4 and the sixth paragraph of Article 20. of this Act within six months of the entry into force of this Act.

(2) The Government shall align the Ordinance on the Establishment, Tasks and Organisation of the Government Office of the Republic of Slovenia for Information Security (Official Gazette of the Republic of Slovenia, Nos. 114/21 and 69/23) with this Act within three months of its entry into force.

(3) The Government shall adopt the strategy referred to in Article 9 of this Act within one year of its entry into force. law.

(4) The Government shall adopt the national response plan referred to in the third paragraph of Article 12 of this Act within three months of the entry into force of this Act.

Article 65

(amendments to the Electronic Communications Act)

In the Electronic Communications Act (Official Gazette of the Republic of Slovenia, No. 130/22 and 18/23 – ZDU-1O):

1. in Article 115, the text of the article is replaced by the following text:

»(1) In accordance with the law governing information security, operators must establish and maintain documented SUVI and SUNP and, in doing so, adopt appropriate, effective and proportionate technical, operational and organisational measures to ensure the integrity, authenticity, confidentiality and availability of network and information systems or to manage the risks to the security of network and information systems that they use for their operations or provision of services, as well as measures to prevent or reduce the impact of incidents on recipients of their services and other services.

(2) The operator must designate SUVI and SUNP as a trade secret.

(3) Insofar as the SUNP referred to in the first paragraph relates to the provision of emergency communications, it shall be reviewed at least once a year. Its adoption and any amendments or updates shall require prior approval by the competent authorities responsible for the operation of emergency communications reception centres.

(4) If it follows from the documents or technical recommendations of the ENISA Agency and the guidelines of the European Commission that sector-specific measures for operators are also necessary in order to ensure a higher level of cybersecurity, taking into account security risks, the Agency shall issue a general act prescribing specific technical guidelines and technical and organisational measures. In adopting the general act, the Agency shall cooperate with the authority responsible for information security.';

2. in Article 116, paragraph four, in the first sentence, the words "from the third paragraph of the previous Article" shall be replaced by the text "in accordance with the previous Article";

3. Articles 118, 119, 120, 121 and 122 are deleted;

4. in Article 123, in the first paragraph, after the first sentence, the following text is added: "A security audit under this Act does not include cases referred to in the first paragraph of Article 115 of this Act, which are carried out in accordance with the law governing information security. The Agency may, when requesting an audit and reviewing the audit results it requests, request assistance from the competent national authority referred to in the law governing information security.";

5. in Article 124, paragraph four, the text "the provision of paragraph five of Article 115 of this Act shall apply" shall be replaced by the text "it must be reviewed at least once a year. Its adoption and amendments or updates shall require prior approval by the competent authorities responsible for the operation of emergency communication reception centres.";

6. in Article 128, the text "provisions 120 and 121" is replaced by the text "paragraph one of Article 115", and a new sentence is added at the end, which reads: "The Agency shall also supervise the implementation of the decision referred to in paragraph one of Article 117 of this Act";

7. in Article 287, paragraph 1, the first sentence shall be deleted of the text "or the authority responsible for information security pursuant to Article 128 of this Act", and the text of the third sentence shall be replaced by the text "The Agency shall also exercise supervision over the implementation of the government decision referred to in the first paragraph of Article 117 of this Act.";

8. the third paragraph of Article 289 is deleted;

9. in Article 298, paragraph one:

– adds a new point 1, which reads:

"1. fails to implement the government decision referred to in the first paragraph of Article 117 of this Act,";

– the previous points 1 to 10 become points 2 to 11;

10. in Article 299, paragraph one:

– points 22, 23 and 24 are amended to read as follows:

"22. does not designate SUVI or SUNP as a business secret in accordance with the second paragraph of Article 115 of this law,

23. fails to adopt, review or update the SUNP in the part relating to emergency communications, with the prior approval of the competent authorities responsible for the operation of emergency communication reception centres, in accordance with the third paragraph of Article 115 of this Act,

24. does not comply with the general act of the agency referred to in the fourth paragraph of Article 115 of this Act,";

– Points 26, 27, 28 and 29 are deleted;

– the previous points 30 to 119 become points 26 to 115.

Article 66

(amendment to the Access to Public Information Act)

In the Access to Public Information Act (Official Gazette of the Republic of Slovenia, No. 51/06 – official consolidated text, 117/06 – ZDavP-2, 23/14, 50/14, 19/15 – Supreme Court decision, 102/15, 7/18 and 141/22), in Article 6, in the first paragraph, at the end of point 11, the full stop is replaced by a semicolon and a new point 12 is added, which reads:

"12. information that is defined as protected information by the competent national authority in accordance with the law governing information security.".

Article 67

(amendment to the Personal Data Protection Act)

In the Personal Data Protection Act (Official Gazette of the Republic of Slovenia, No. 163/22), in Article 23, paragraph 1, the text "on security requirements" is replaced by the text "on risk management measures", and the text "providers of essential services" is replaced by the text "essential entities".

Article 68

(completion of procedures initiated before the entry into force of this Act)

Administrative and inspection procedures that have not yet been finally concluded by the entry into force of this Act shall be concluded in accordance with the previous regulations.

XII. FINAL PROVISIONS

Article 69

(termination of validity and extension of use)

(1) On the date of entry into force of this Act, the Information Security Act shall cease to be in force. (Official Gazette of the Republic of Slovenia, Nos. 30/18, 95/21, 130/22 – ZEKom-2, 18/23 – ZDU-1O and 49/23).

(2) On the date of entry into force of this Act, the following shall cease to be in force:

– Decree on the determination of essential services and a more detailed methodology for determining providers of essential services (Official Gazette of the Republic of Slovenia, No. 39/19),

– Regulation on security documentation and security measures of providers of essential services (Official Gazette of the Republic of Slovenia, No. 8/23),

– Regulation on security documentation and security measures of state administration bodies (Official Gazette RS, No. 98/23),

– Regulation on security documentation and minimum security measures of related entities (Official Gazette of the Republic of Slovenia, No. 118/23).

(3) On the date of entry into force of this Act, the following shall cease to be in force:

– General Act on Notification and Evaluation of Security Incidents and on Notification of Restrictions or Interruptions (Official Gazette of the Republic of Slovenia, No. 74/23), which continues to apply in the part relating to the notification of restrictions or interruptions, and

– General Act on the Security of Networks, Services and Information (Official Gazette, No. 106/23).

Article 70

(entry into force)

This Act shall enter into force on the fifteenth day after its publication in the Official Gazette of the Republic of Slovenia.

No. 011-02/25-7/21

Ljubljana, 23 May 2025

EPA 2057-IX

National Assembly

Republic of Slovenia
Urška Klakoÿar Zupanÿiÿ, MSc.
President

Annex 1: Highly critical sectors

Annex 2: Other critical sectors

Annex 3: Other public administration entities at the state level