EnCaViBS

WP 2: The NIS Directive and its transposition into national law.

Member State:

Slovenia

Information Security Act

Important notice:

This text is an unofficial translation conducted at the SnT/ University of Luxembourg in the framework of the research project EnCaViBS.

The original legal acts which Member States notified to the European Commission as national execution measures were retrieved from official national databases. In order to focus on the core of the research project, only selected transpositions have been translated.

The translations only serve the purpose of being an information resource; there is no guarantee whatsoever that the translations correctly correspond to the original versions of the laws. Therefore, evidently, the texts have no legal value. The original, as well as the translated version of the legal acts, are available at www.encavibs.uni.lu, where additional information on the research project may be found.

This research project is funded by the Luxembourg National Research Fund (FNR), C18/IS/12639666/EnCaViBS/Cole,

https://www.fnr.lu/projects/the-eu-nis-directive-enhancing-cybersecurity-across-vital-business-sectors-encavibs/.

Fonds National de la Recherche Luxembourg

Member State: Slovenia

Information Security Act (ZInfV)

Official State Gazette of the Republic of Slovenia No.30/18

I. General Provisions

1. Article (content of the Act)

This Act regulates the field of information security and necessary measures to achieve a high level of security of networks and information systems within the Republic of Slovenia, which are essential for the smooth operation of the state under all security conditions in order to provide essential services for maintaining key social and economic activities within the Republic of Slovenia. Furthermore, this Act provides minimum security requirements and incident reporting requirements for those liable under this Act. It also regulates the competences, tasks, organization and operation of the competent national information security authority (hereinafter: the competent national authority), single contact points for information security (hereinafter: single contact point(s)), National Electronic Network and Information Security Incident Teams (hereinafter: National CSIRT) as well as teams for dealing with incidents in the field of electronic networks and information security of state administrative bodies (hereinafter: CSIRT of state administration bodies) in the field of information security.

2. Article (purpose and scope of the Act)

(1) The purpose of this Act is to regulate the field of information security, thus ensuring a high level of security for networks and information systems in the Republic of Slovenia, which are essential for the smooth operation of the state under all security conditions and serve to provide essential services for maintaining key social and economic activities.

(2) This Act transposes into the legal order of the Republic of Slovenia Directive (EU) 2016/1148/EU of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of networks and information systems across the Union (OJ L 194 of 19/07/2016, p. 1), (hereinafter: Directive 2016/1148/EU).

(3) This Act shall not apply to legal or natural persons insofar as they provide public communications networks or publicly available electronic communications services (operators) subject to special obligations regarding the security and integrity of networks and services under the Act governing electronic communications, and to trust services providers subject to the requirements of Article 19 of Regulation (EU) No. 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (OJ L No. 257 of 28/08/2014, p. 73).

3. Article (data processing)

(1) The processing of personal data on the basis of this Act is carried out in accordance with the regulations governing the protection of personal data.

(2) Data and information processed on the basis of this Act and defined as either a secret or as a business secret shall be treated in accordance with the regulations governing classified information and business secrets.

4. Article (definition of terms)

For the purposes of this Act, the terms used in this Act shall have the following meanings:

1. An essential service is a service provided in the areas referred to in the second paragraph of Article 5 of this Act and, as such, is essential for the preservation of key social and economic activities.

2. CSIRT is a group that responds to information security incidents, accepts reports regarding security breaches, conducts analyses, and assists notifiers in managing incidents.

3. Digital infrastructure includes IXPs, top-level domain name registries, and domain name system service providers.

4. Digital services are the following information society services: online marketplaces, search engines and cloud computing services.

5. An incident is any event that has an actual negative impact on the security of networks and information systems.

6. The information environment is a collection of social networks and cyberspace, including data and other types of information.

7. Information security consists of the protection, safeguarding and defence of the information environment against unauthorized access, use, disclosure, interference, modification or destruction, in order to ensure confidentiality, authenticity, integrity and availability.

8. An essential service provider is a public or private entity pertaining to one of the areas listed in Article 5 of this Act and meets the criteria set out in Article 7 of this Act, as well as additional sectoral criteria set forth by regulatory bodies.

9. A cyber threat is a malicious threat or attempt to damage or disrupt a computer network system, its services and its data.

10. Cyber defence is a set of measures and activities of the state that deter, prevent, or repel cyber attacks in the information environment.

11. Cyber security is the ability to protect, safeguard and defend cyberspace against cyber threats, incidents and cyber attacks.

12. A cyber attack is a cyberspace attack with the intent to maliciously destroy, expose, control or alter, disable, collect and obstruct any part of cyberspace, including data and secret information which is essential for the smooth functioning of the state.

13. Cyberspace is a global information environment consisting of communications networks and information systems. Cyberspace enables the creation, processing and exchange of electronically transmitted information.

14. Highly sensitive areas of the national security system include specialised networks and information systems dedicated to national defence, protection against natural and other disasters, the police force, intelligence and security activities, as well as foreign affairs.

15. All information systems within the entity are key and essential components, without which it would not be possible to provide services continuously.

16. Control systems are information systems which enable the implementation of correct procedures and perform the appropriate sequence of operations for key information systems within the entity.

17. A qualified auditor is an auditor in the field of information security who has obtained a special certificate from one of the independent audit organizations.

18. The CSIRT group network is an association in which CSIRTs from the Member States and CERT-EU participate.

19. The National Crisis Management Centre is the centre specified in the regulation governing the organization and operation of the National Crisis Management Centre.

20. Supervisory information systems are information systems which are responsible for monitoring the implementation of the supervisory function within the entity's information systems.

21. Incident management refers to all necessary procedures which enable the detection, analysis, containment and response to incidents.

22. Network and information system include:

- Electronic communication networks, including transmission systems and, where appropriate, switching or routing equipment and other resources, including non-active network elements, enabling the transmission of signals by wires, radio waves, optical or other electromagnetic means, including satellite networks, fixed (wired and packet switched, including the Internet) and mobile terrestrial networks; electric cable systems, if used for signal transmission, radio and television broadcasting networks, and cable television networks, regardless of the type of information transmitted;
- any device or group of interconnected or related devices, which performs automatic processing of digital data on a program basis, or
- digital data which has been stored, processed, retrieved or transmitted by the elements referred to in the first and previous indents of this point for purposes of their operation, use, protection and maintenance.

23. A digital service provider is any natural or legal person who provides a digital service.

24. A domain name system service provider is an entity which provides domain name system services on the Internet.

25. A representative is any natural or legal person established in the European Union (hereinafter referred to as: EU) expressly designated to act on behalf of a digital service provider which is not established in the Union, and whom the competent national authority or national CSIRT may contact instead of the digital service provider as regards the obligations of that digital service provider under this law.

26. The registry of top-level domain names is an entity which manages and performs the registration of Internet domain names within a specific top-level domain.

27. An audit trail is an irreversible trace or data set which has occurred over time within an information system or device, with an accurately recorded time record in the form of a log which enables an accurate overview of all records related to all events as well as all stored information from the creation of the data or information onwards to the present.

28. A domain name system is a hierarchically distributed system for assigning names in a network which forwards queries for domain names.

29. The Cooperation Group is a group composed of EU Member States representatives, the European Commission and the European Union Network and Information Security Agency (ENISA).

30. A specification is a document which prescribes the minimal technical requirements which a product, process, service, or system must meet.

31. An online marketplace is a digital service providing consumers (any natural person acting for purposes outside their trade, business, craft or profession) or traders (any natural or legal person, privately or publicly owned, who, alone or through a person acting on his or her behalf or at his or her request, acts for purposes relating to their commercial, business, craft or professional activity) with the possibility of entering into online sales or online service agreements with traders on the online marketplace website or a trader’s website using the computer services of the online marketplace.

32. A web search engine is a digital service that provides users a means to search all topics or sites in a particular language based upon a query about any topic in the form of a keyword, phrase, or other entry, and offers links to pages with information about the required content.

33. A standard is a technical specification adopted by a recognized standardization body for repeated or continuous use.

34. A network junction is a network capacity which provides for the interconnection of more than two independent autonomous systems, mainly due to the exchange of Internet traffic. It solely provides interconnectivity services between autonomous systems, enabling the free exchange of Internet traffic between any participating autonomous systems, eliminating the need to pass through a third autonomous system, and does not alter or otherwise interfere with such traffic.

35. An information society service is any service normally provided for a fee, remotely (the service is performed without the customers being present at the same time), electronically (the service is sent at the starting point and received at the destination with electronic data processing and storage equipment, which is fully transmitted, sent and received by wire, radio, optical or other electromagnetic means) and at the individual request of the recipient of the service (the service is performed by transmitting data at an individual request).

36. A cloud computing service is a digital service that provides access to a flexible and scalable set of shared computing resources.

37. The Cyber Security Strategy is a national strategy for the security of networks and information systems and represents a framework with strategic goals and priorities in the field of security of networks and information systems in the Republic of Slovenia.

38. Risk is any reasonably identifiable circumstance or event that may have a negative impact on the security of networks and information systems.

39. The security of networks and information systems is the ability of networks and information systems to prevent, at a certain level of trust, all events that jeopardize the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or related services provided by or accessible through those networks and information systems.

40. The Security Operations Centre is an internal organizational unit of individual state administration bodies that responds to incidents in the field of information security.

II. Persons liable

5. Article (persons liable)

(1) Persons liable under this Act are:

- essential service providers,
- digital service providers and
- state administrative bodies which manage information systems and other parts of the network or provide information services necessary for the smooth operation of the state or for the purpose of ensuring national security (hereinafter: state administrative bodies).

(2) Providers of essential services are entities which operate in the following areas:

1. energy,

2. digital infrastructure,

3. drinking water supply and distribution,

4. health,

5. traffic,

6. banking,

7. financial market infrastructure,

8. food supply, and

9. environmental protection.

6. Article (identification of essential service providers)

(1) For the purpose of classification of essential service providers, the Government of the Republic of Slovenia (hereinafter: the Government) shall determine the list of essential services pursuant to the regulation which governs the standard classification of activities.

(2) An individual essential service provider shall be appointed by the Government based on the criteria referred to in Article 7 of this Act.

(3) Notwithstanding the preceding paragraph, the Government shall also designate as essential service providers those critical infrastructure managers pursuant to the regulations governing critical infrastructure and defence planning bodies which have been formed and designated in accordance with national regulations governing the field of defence, whose provision of services depend on networks and information systems.

(4) If the provider provides essential services in the Republic of Slovenia and any other EU Member State, the competent national authority shall consult the competent national authority of the other EU Member State, wherein the provider provides such service, prior to designating the essential service providers referred to in the second paragraph or in the previous paragraph of this Article in accordance with Directive 2016/1148/EU.

7. Article (criteria - methodology)

(1) When determining an essential service providers referred to in the second paragraph of Article 5 of this Act, the following criteria shall be taken into account:

- the entity provides a service which is essential for the maintenance of key social or economic activities.
- the provision of this service depends on networks and information systems, and
- the incident would have a significant negative impact on the provision of this service.

(2) In determining the significance of the negative impact referred to in the third indent of the preceding paragraph, at least three of the following factors shall be taken into account:

1. the number of users that depend on the entity's service,

2. the dependence of other areas referred to in the second paragraph of Article 5 of this Act on the service of the entity,

3. the degree and duration of the impact that incidents could have on economic and social activities or public safety,

4. market share of the entity,

5. geographical distribution in terms of the area that could be affected by the incident,

6. the importance of the entity in maintaining a sufficient level of service, taking into account the availability of alternative means of provision of the service.

(3) At least two of the following factors shall be considered when deciding whether an incident would have a significant negative impact:

- the number of users affected by the disruption in the provision of the essential service,
- duration of the incident,
- the geographical distribution in terms of the area that could be affected by the incident.

(4) The methodology for identifying essential service providers is specified in more detail by the Government.

8. Article (designation of digital service providers)

(1) Digital service providers referred to in the second indent of the first paragraph of Article 5 of this Act shall be liable to meet their obligations under this Act.

(2) Notwithstanding the previous paragraph, digital service providers with less than 50 employees and an annual turnover or an annual balance sheet total below ten million euros shall not be liable.

9. Article (designation of state administration bodies)

(1) The Government shall designate the state administrative bodies referred to in the third indent of the first paragraph of Article 5 of this Act and the CSIRT of state administrative bodies.

(2) Notwithstanding the previous paragraph, the CSIRT of state administrative bodies shall not be designated if the state administrative bodies have own capacities provided for within their internal organizational structure, with at least at the level of the security operations centre meeting this requirement.

10. Article (designation of the contact person of the liable persons)

(1) The essential service provider shall, within 15 days of the decision referred to in the second paragraph of Article 6 of this Act, appoint a contact person for information security and his deputy and forward their contact details to the competent national authority.

(2) The state administration body may designate a contact person for information security and his deputy and provide their contact details to the competent national authority.

(3) The digital service provider, which has its main registered office in the Republic of Slovenia in accordance with the first paragraph of Article 15 of this Act, may designate and authorize a contact person for information security and his deputy and forward this contact information to the competent national authority.

(4) If the digital service provider is not established in the EU, but designates the representative's headquarters for the EU in the Republic of Slovenia in accordance with the second paragraph of Article 15 of this Act, this representative shall be considered the contact person. The contact details of the representative may be forwarded by digital service providers to the competent national authority.

(5) The liable persons referred to in the first paragraph of this Article shall notify the competent national authority of the change of contact details within 15 working days of the change.

III. Information security of essential service providers

11. Article (security requirements)

(1) In accordance with the methodology referred to in the third paragraph of Article 12 of this Act, essential service providers shall determine the key parts of the network, control and monitoring information systems by which they ensure the provision of essential services.

(2) The essential service providers shall carry out an analysis, assessment and evaluation of the risks and, on that basis, prepare and implement the necessary measures to manage the risks related to the security of the networks and information systems used in the essential services.

(3) Essential service providers shall, in order to ensure the continuity of the services, take all appropriate measures to prevent and reduce the impact of incidents affecting the security of those networks and information systems that are used to provide essential services.

(4) If the essential service providers draw input data and information from key parts of the national security system for the performance of their activity, they shall establish all necessary security requirements with the consent of the competent Ministry for each key part of the national security system.

12. Article (security documentation and security measures)

(1) Essential service providers shall establish and maintain a documented information security management system and an ongoing business continuity management system for ensuring that information security and a high level of security of networks and information systems is maintained, which must include at least:

1. risk management analysis with an assessment of the acceptable level of risk,

2. business continuity policy with its management plan,

3. a comprehensive list of his key, control and monitoring information systems and parts of the network and associated data which are essential for the operation of the essential services,

4. a plan for renewal and restoration of the operation of the information systems referred to in the previous indent,

5. an incident response plan with a national CSIRT notification protocol;

6. a plan of security measures to ensure the integrity, confidentiality and availability of network and information systems, which take account of sectoral specificities.

(2) Based on the security documentation referred to in the previous paragraph, the essential service providers shall prepare and implement the necessary security measures, which shall be divided into organizational, logical-technical and technical measures.

(3) The Minister responsible for the information society (hereinafter: the Minister) shall determine in detail the content and structure of the security documentation referred to in the first paragraph of this Article and the minimum scope and content of security measures referred to in the previous paragraph. He shall also prescribe the methodology for the preparation of risk management analysis and for the designation of key, control and monitoring information systems and parts of the network and the associated data referred to in points 2 and 3 of the first paragraph of this Article.

(4) If the essential service provider has already prepared security documentation on the basis of other regulations for ensuring the security of his networks and information systems, he shall supplement it in accordance with this Act.

(5) For the purpose of incident management, in accordance with the risk management analysis with an assessment of the acceptable level of risk and taking into account the state of the art, the essential service providers shall also ensure the maintenance of logs of key, control or monitoring information systems or network parts for a period of six months. The log record keeping is ensured on the territory of the Republic of Slovenia, except for the areas of digital infrastructure, banking and financial market infrastructure, where it can be provided on the territory of the EU.

13. Article (notification of incidents)

(1) Essential service providers shall notify the national CSIRT without undue delay of incidents with a significant impact on the continued provision of the essential services which they provide.

The notification shall contain information on the basis of which the potential cross-border impact of the incident can be determined. In determining the significance of the impact of an incident, essential service providers shall take into account in particular:

- the number of users affected by the disruption in the provision of the essential service,
- the duration of the incident, and
- the geographical distribution in terms of the area that could be affected by the incident.

(2) When reporting an incident, the notifier must ensure the adequate safety of the log entries or audit trails, if any exist.

(3) The national CSIRT shall immediately notify the competent national authority of the incident, which maintains a list of incidents referred to in the third paragraph of Article 25 of this Act. The competent national authority shall immediately inform the police (MUP) and the National Crisis Management Centre of an incident which, if prolonged, could have a greater inter-sectoral impact or could cause a deterioration in the stability of the national security of the Republic of Slovenia over an extended period of time.

(4) If the incident has a significant impact on the continuity of the provision of essential services in another EU Member State, the competent national authority or national CSIRT shall inform the single point of contact in the affected EU Member State(s). In doing so, it shall protect the security and business interests of the essential service provider and the confidentiality of the information provided by the latter in its notification.

(5) The information and data referred to in the previous paragraph, which are confidential, shall be provided, if necessary, for the application of Directive 2016/1148/EU or for the implementation of this Act. The transmission shall be limited to the extent appropriate and necessary for the purpose referred to in the preceding paragraph and shall preserve the confidentiality of the information and data provided.

(6) In performing the notification obligation, the national CSIRT must ensure that information on the vulnerability of the essential service remains confidential and uncompromised until security can be restored.

(7) If the national CSIRT deems necessary, it shall following the notification of the incident, provide the essential service provider with relevant information on further measures, based on its notification, which could contribute to the effective management of the incident.

(8) The competent national authority may, after consulting the essential service provider who notified the incident, inform the public of individual incidents, where public awareness is rquired to deal with it or to prevent the escalation of the incident or new incidents.

(9) In informing the public referred to in the previous paragraph, the competent national authority shall take into account the balance between the public interest in being informed of the risks, on the one hand, and the potential damage to the reputation and business of essential service providers.

IV. Information security of digital service providers

14. Article (security requirements and incident notification)

(1) Digital service providers shall identify and adopt appropriate and proportionate technical and organizational measures to manage the security risks of the networks and information systems which they use to provide these services in the EU. Taking into account the state of the art, these measures shall

ensure a level of security of networks and information systems appropriate to the existing risk. Thereby, they shall take into account the following elements:

- security of systems and capabilities;
- incident management;
- business continuity management;
- monitoring, auditing and testing; and
- compliance with international standards.

(2) Digital service providers shall take appropriate measures to prevent and reduce the impact of incidents that threaten the security of their networks and information systems on the services they provide in the EU in order to ensure the continuity of those services.

(3) Digital service providers shall notify the national CSIRT without undue delay of any incident which has a significant impact on the provision of the services they offer in the EU. The notification shall include information on the basis of which the national CSIRT can determine the significance of the potential cross-border impact. The obligation to notify an incident applies only when the digital service provider has access to the information necessary to determine the impact of the incident in the light of the parameters referred to in the fifth paragraph of this Article.

(4) The national CSIRT shall notify the competent national authority of the incident, which shall keep a list of incidents referred to in the third paragraph of Article 25 of this Act. The competent national authority shall immediately inform the police and the National Crisis Management Centre of an incident which, if prolonged, could have a greater inter-sectoral impact or could cause a deterioration in the stability of the national security of the Republic of Slovenia over a longer period of time.

(5) In determining the level of impact of the incident, the following parameters in particular shall be taken into account:

- the number of users affected by the incident, in particular users who depend on the service to provide their own services;
- the duration of the incident;
- the geographical distribution in terms of the area that could be affected by the incident;
- the extent to which the operation of the service is disrupted, and
- the extent of the impact on economic and social activities.

(6) Where an essential service provider is dependent on a third party digital service provider for the provision of a service essential to the maintenance of key social and economic activities, that essential service provider shall notify any significant impact on the continued provision of essential services, which is a result of an incident affecting the digital services provider.

(7) The competent national authority shall inform the other affected EU Member States if the incident concerns two or more EU Member States or, in other cases, if it deems that notifying other EU Member States would contribute to the improvement of the level of security of networks and information systems.

(8) The transmission of information and data, which are confidential, referred to in the preceding paragraph shall be limited to the extent appropriate and proportionate to the purpose of this exchange.

(9) In performing the notification obligation, the national CSIRT must ensure that the information on the vulnerability of the essential service remains confidential until security is restored.

(10) The competent national authority may, after consulting the digital service provider concerned, inform the public of individual incidents, or require the digital service provider to do so where public awareness is necessary to prevent an incident or to address an ongoing incident or where disclosure of the incident is otherwise in public interest.

(11) In informing the public referred to in the previous paragraph, the competent national authority shall take into account the balance between the public interest in being informed of the risks, on the one

hand, and the potential damage to the reputation and business of essential service providers on the other hand.

15. Article (jurisdiction and territoriality)

(1) The digital service provider with its registered office in the Republic of Slovenia falls within the jurisdiction of the competent national authority and the national CSIRT, which it notifies of incidents. For the purposes of this Act, the aforementioned digital service provider shall be deemed to have the seat of its headquarters in the Republic of Slovenia if it has its head office in the Republic of Slovenia.

(2) If a digital service provider does not have its headquarters in the EU but provides such services in the EU and designates the seat of its EU representative in the Republic of Slovenia, where it also provides digital services, it falls within the jurisdiction of the competent national authority and the national CSIRT. The representative shall represent the digital service provider in connection with the obligations under this Act.

(3) If a digital service provider's head office or representative is located in one EU Member State and networks and information systems in another or more than one other EU Member States, the competent national authority shall cooperate with the Republic of Slovenia in the event that the operation of this digital service provider is in any way related to the Republic of Slovenia, and shall cooperate with the competent authority of the EU Member State where the digital service provider or its representative is located in the EU, or with the relevant competent authorities of those other EU Member States. Such cooperation may include the exchange of information between competent authorities and requests for the adoption of appropriate control measures from the chapter on inspections of this Act.

(4) The information and data referred to in the previous paragraph, which are confidential, shall be provided, if necessary, for the application of Directive 2016/1148/EU or for the implementation of this Act. The transmission shall be limited to the extent appropriate and necessary for the purpose referred to in the preceding paragraph and shall preserve the confidentiality of the information and data provided.

V. Information security of state administration bodies

16. Article (security requirements)

(1) State administration bodies must perform analysis, assessment and evaluation of risks and on this basis prepare and implement measures necessary for security risk management regarding information systems and parts of the network they manage (hereinafter: networks and information systems of state administration bodies), or for information services which they provide and are necessary for the smooth functioning of the state or for ensuring national security (hereinafter: services of state administration bodies).

(2) State administration bodies shall adopt the necessary measures to prevent and reduce the impact of incidents affecting the security of networks and information systems of state administration bodies in order to ensure a continuous provision of services by state administration bodies.

(3) If the essential service providers draw the input data and information for the performance of their activity from the key parts of the national security system, they shall establish all the necessary security requirements with the consent of the competent Ministry for each key part of the national security system.

17. Article (security documentation and security measures)

(1) State administration bodies shall establish and maintain a documented information security management system and a business continuity management system for ensuring information security and a high level of security of networks and information systems, which must include at least:

1. a risk management analysis with an assessment of the acceptable level of risk;

2. a business continuity policy with its management plan;

3. a list of its key, control and monitoring information systems and parts of the network and associated data which are essential for the operation of services of state administration bodies;

4. a plan for renewal and restoration of the operation of the information systems referred to in the previous indent;

5. an incident response plan with a national CSIRT notification protocol, and

6. a plan of security measures to ensure the integrity, confidentiality and availability of network and information systems of state administration bodies.

(2) Based on the security documentation referred to in the previous paragraph, the state administration bodies shall prepare and implement the necessary security measures, which shall be divided into organizational, logical-technical and technical measures.

(3) The Minister shall determine in more detail the content and structure of the security documentation referred to in the first paragraph of this Article and the minimum scope and content of the security measures referred to in the previous paragraph. He shall also prescribe the methodology for the preparation of risk management analysis and for the designation of key, control and monitoring information systems and parts of the network and the associated data referred to in points 2 and 3 of the first paragraph of this Article.

(4) If the state administration body has already prepared security documentation on the basis of other regulations for ensuring the security of its networks and information systems, it shall supplement it in accordance with this Act.

(5) For the purpose of incident management, in accordance with the risk management analysis with an assessment of the acceptable level of risk and taking into account the state of the art, the state administration bodies shall also ensure the maintenance of logs of key, control or monitoring information systems or network parts for a period of six months. The storage of these log entries must be ensured on the territory of the Republic of Slovenia.

18. Article (notification of incidents)

(1) State administration bodies shall, without undue delay notify the CSIRT bodies of state administration of incidents with a significant impact on the continuous provision of services of state administration bodies, and those state administration bodies which have their own capabilities, at least at the level of the Security Operations Centre, the competent national authority. In determining the significance of the impact of an incident, they shall take into account in particular:

- the number of users affected by the disruption in the provision of the state administration bodies;
- the duration of the incident, and
- the geographical distribution in terms of the area which could be affected by the incident.

(2) When reporting an incident, the notifier must ensure an adequate safety of the log entries or audit trails, if there are any.

(3) The CSIRT of state administration bodies shall notify the national CSIRT and the competent national authority which keeps the list of incidents referred to in the third paragraph of Article 25 of this Act. The competent national authority shall immediately notify the police and the National Crisis Management Centre of an incident which, if prolonged, could lead to a deterioration in the stability of the national security of the Republic of Slovenia.

(4) In performing the notification obligation, the national CSIRT of the state administration bodies must ensure that the information on the vulnerability of the essential service remains confidential until security is restored.

(5) The competent national authority may, after consulting the state administration body who notified of the incident, inform the public of individual incidents, where public awareness is needed to prevent the incident or to deal with it.

(6) When informing the public referred to in the previous paragraph, the competent national authority shall take into account the balance between the public interest in being informed of the risks, on the one hand, and the possible negative impact of such disclosure on criminal investigation, law and order, national security and national defence on the other hand.

VI. Standardization and voluntary notification

19. Article (standardization)

In order to harmonize the approaches of essential service providers, digital service providers and state administration bodies in the implementation of obligations under Articles 3, 4 and 5 of this Act, the competent national authority shall, in order to promote the use of European or internationally accepted standards and specifications, important for the security of networks and information systems, publish this information on its website.

20. Article (voluntary notification)

(1) Entities which have not been identified as liable under this Act may voluntarily report incidents that have a significant impact on the continued provision of the services they provide. In this case, public sector entities which are not state administration bodies referred to in Article 9 of this Act shall act in accordance with the procedure referred to in Article 18 of this Act, and private sector entities in accordance with the procedure referred to in Article 13 of this Act.

(2) National CSIRTs and CSIRTs of state administration bodies shall prioritize mandatory notifications over voluntary notifications. In determining the order of processing of voluntary notifications, they shall take into account the impact of voluntarily notified incidents on the continuous provision of essential services, services of state administration bodies and the cross-border impact of the incident.

(3) Voluntarily reported incidents that have no or negligible impact on the provision of essential services, services of public authorities and have negligible cross-border impact shall only be processed where such processing does not impose a disproportionate or unjustified burden on the national CSIRT or the CSIRT of the state administration bodies.

VII. Incident evaluation, increased threat state, and cyber defence

21. Article (incident evaluation and action)

(1) Notified incidents are evaluated by the competent national CSIRT or the CSIRT of state administration bodies, and in case the state administration bodies have their own facilities at least at the level of the safety operations centre, they are evaluated by the competent national authority. The said authorities may consult each other in the evaluation. Given the severity of the incident:

- a minor incident is a one-off incident which, with regard to the parameters of determining the significance of the impact of the incident referred to in the first paragraph of Article 13 or the fifth paragraph of Article or the first paragraph of Article 18 of this Act, has a small negative impact on the confidentiality, integrity and availability of the network, information system or information services of the liable party and

- does not cause him greater damage. Also, such an incident must not have a negative cross-sectoral impact or a negative impact on the operation of defence, internal security and protection and rescue information systems;
- a serious incident is a single incident or a sequence of a large number of different incidents in a short period which, depending on the parameters of determining the significance of the impact of the incident from the first paragraph of Article 13 or the fifth paragraph of Article 14 or the first paragraph of Article 18 of this Act, has a significant negative impact and the availability of the liable party's network, information system or information services. Such an incident has a significant impact on the smooth operation of the liable party and causes him greater damage. Also, such an incident can have a negative cross-sectoral impact or a negative impact on the operation of defence, internal security and protection and rescue information systems,
- however, this impact does not meet the criteria set out in the following indent;
- a critical incident is the incident which, depending on the parameters of determining the significance of the impact of the incident referred to in the first paragraph of Article 13 or the fifth paragraph of Article 14 or the first paragraph of Article 18 of this Act, has a very large negative impact on the confidentiality, integrity and availability of the liable party's network, information system or information services. At the same time, such an incident also makes it difficult for the state to function, especially information systems for defence, internal security and the protection and rescue system, or partially disables the operation of at least three areas of essential services or one in its entirety.

(2) The competent national authority on the basis of the data and information on the severity of the incident referred to in the previous paragraph, provided by the national CSIRT or the CSIRT of the state administration bodies, assess whether this is also a cyber attack at the same time.

(3) The competent national authority must immediately notify the Government and the National Security Council of the critical incident and the cyber attack (hereinafter: NSC) of the critical incident and cyber attack, but may also, depending on the relevant circumstances, notify them of a more serious incident whereby it is likely to escalate into a critical incident.

(4) In the event of a serious or critical incident or in the event of a cyber attack, the competent national authority may, by written decision or, in urgent cases, orally, impose such appropriate and proportionate measures as are necessary to stop the already ongoing incident or to remedy its consequences. The written copy of the oral decision shall be served on the liable party as soon as possible, but no later than within 48 hours after the oral decision.

(5) The measures issued pursuant to the preceding paragraph shall be determined to the extent and for such time as is strictly necessary to achieve the purpose referred to in the preceding paragraph. An appeal against the decision referred to in the preceding paragraph shall not suspend its execution.

(6) The competent national authority shall inform the Government and the NSC of the measures referred to in the fourth paragraph of this Article.

22. Article (situations of increased risk and prescribed actions)

(1) A state of increased risk for the security of networks or information systems (hereinafter: state of increased risk) is a state of high probability for a serious or critical incident from the first paragraph or cyber attack from the second paragraph of the previous Article within 72 hours of detection of such probability.

(2) The competent national authority shall, on the basis of the data and information at its disposal and in cooperation with the other competent authorities, assess whether this is the situation of increased risk referred to in the previous paragraph.

(3) The competent national authority shall inform the government and NSC of the state of increased risk due to the likelihood of a critical incident or cyber attack referred to in the first paragraph of this

Article, but may also, depending on the assessment of the relevant circumstances, inform them of the likelihood of a serious incident referred to in the first paragraph of this Article.

(4) The competent national authority may, in a state of increased risk referred to in the first or third indent of the first paragraph of Article 5 of this Act, determine to the liable party by written decision, or in urgent cases also orally, such appropriate and proportionate measures as necessary to prevent or reduce the likelihood of an incident referred to in the first paragraph of this Article, as well as to reduce the expected harmful consequences in the event of the realization of such an incident. The written copy of the oral decision shall be served on the liable party as soon as possible, but no later than within 48 hours after the oral decision.

(5) The measures issued pursuant to the preceding paragraph shall be determined to the extent and for such time as is strictly necessary to achieve the purpose referred to in the preceding paragraph. An appeal against the decision shall not suspend its execution.

(6) The competent national authority shall inform the Government and the NSC of the measures referred to in the fourth paragraph of this Article.

23. Article(public information)

If the adopted measures referred to in Article 21 or in previous paragraph of this Act also require addressing the public, the competent national authority shall, in collaboration with the government service responsible for communication with the public, prepare a press release, which the media may publish only in unchanged form.

24. Article (cyber defence)

(1) Cyber defence is coordinated and implemented by the competent national authority, the national CSIRT and the CSIRT of state administration bodies as well as the ministry responsible for defence, the police, the Slovenian Intelligence and Security Agency (hereinafter: the SISA) and other national authorities in accordance with their competences in ensuring national security.

(2) The competent authorities referred to in the preceding paragraph shall ensure adequate cyber-defence capabilities in their cyberspace. In doing so, the Ministry responsible for public administration, the Ministry responsible for defence, the Ministry responsible for foreign affairs, and the police and the SISA constantly monitor the situation and responses to events in cyberspace.

(3) For the purpose of cyber defence, the bodies referred to in the first and previous paragraphs shall implement coordinated organizational, logical-technical, technical and administrative measures and activities at various levels to ensure comprehensive information security in accordance with their competencies.

(4) The purpose referred to in the preceding paragraph shall also be realized by involving the bodies referred to in the first and second paragraphs of this Article in international security relations and their active participation in these relations and through other forms of multilateral and bilateral cooperation.

VIII. Lists

25. Article (management and content of lists)

(1) For the purpose of cooperating with liable parties, the competent national authority shall manage a list of contact details containing:

- registration and tax identification number as well as classification of the liable party’s activities;
- name, address, telephone number and e-mail address of the liable party;

- name and surname, telephone number and e-mail address of the contact person of the liable party and its deputy referred to in Article 10 of this Act.

(2) The national CSIRTs and the CSIRTs of state administrative bodies shall also have access to the list referred to in the preceding paragraph in the part relating to liable parties within their competence.

(3) For the purpose of preventing and responding to incidents and cyber attacks, the competent national authority shall manage a common list of incidents and cyber attacks, containing:

- an incident or cyber attack report with the identification data of the liable party and the information system or network where the incident or attack occurred, as well as information on the incident or attack;
- information on the source of the incident or attack;
- the procedure for informing the other competent authorities and the procedure for informing other potentially affected entities;
- the procedure of resolving the incident or attack and the end result and the measures taken to prevent recurrence or to reduce the risk of an incident or attack.

(4) The national CSIRT and the CSIRT of state administration bodies shall manage a list of incidents and cyber attacks with the data referred to in the previous paragraph for the incidents they are dealing with so as to prevent and respond to incidents and cyber attacks.

(5) The competent national authority shall also manage a list of essential services and a list of information systems, parts of the network and information services of state administration bodies necessary for the smooth functioning of the state or for ensuring national security so as to properly identify providers of essential services and state administration bodies.

(6) The competent national authority and the national CSIRT and the CSIRT of state administration bodies shall twice a year, on the basis of the data referred to in the third and fourth paragraphs of this Article, prepare anonymised information for statistical and public information purposes, which they shall also publish on their websites.

IX. Organization of the national information security system

26. Article (information security strategy)

The Government shall adopt an information security strategy (hereinafter: the strategy), which shall provide a framework for the implementation of measures for establishing an effective national information security system. To this end, it shall define strategic objectives as well as policy measures and regulatory measures, which must cover at least the areas referred to in the second paragraph of Article 5, digital services referred to in Article 8 and services of state administration bodies referred to in Article 9 of this Act. In doing so, it shall address in particular:

1. the objectives and priorities of the strategy;

2. a management framework to achieve the objectives and priorities of the strategy, including the roles and responsibilities of state authorities and other relevant stakeholders;

3. identification of measures related to information security preparedness, response and restoration, including cooperation between public and private sectors;

4. defining education, awareness and training programs related to the strategy;

5. defining research and development plans in relation to the strategy;

6. a risk assessment plan to identify risks;

7. a list of the various actors involved in the implementation of the strategy.

27. Article (competent national authority)

(1) The competent national authority is the body within the ministry responsible for the information society.

(2) In addition to other tasks specified by this Act, the competent national authority shall perform the following tasks:

1. coordinate the operation of the information security system;

2. develop capabilities to implement cyber defence;

3. provide professional support in the performance of their tasks to all liable parties in the field of information security;

4. provide analysis, methodological support and preventive action in the field of information security and give opinions in the field of its presence;

5. cooperate with bodies and organizations operating in the field of information security, especially with the national CSIRT and the CSIRT of state administration bodies, with security and operational centres, with regulators or supervisors of areas referred to in the second paragraph of Article 5, with the Agency for Communication Networks and Services of the Republic of Slovenia, with the Information Commissioner and law enforcement authorities, as well as with security solution providers;

6. raise awareness among liable parties of the importance of reporting an incident with all the signs of a criminal offense, prosecuted ex officio, to law enforcement authorities, in accordance with the Criminal Code;

7. coordinate training, practice and education in the field of information security and take care of raising public awareness of information security;

8. encourage and support research and development in the field of information security;

9. perform testing of information and communication technologies in the field of information security;

10. take care of the preparation and implementation of the strategy;

11. draws up a national incident response plan, in light of the strategy, the plans of the national CSIRT and the CSIRT of state administration bodies, other competent authorities and the safety documentation of liable parties;

12. reviews the adequacy of the designation of essential service providers and public administration bodies at least every two years and may propose to the Government to update the designations;

13. for the purposes of reviewing Directive 2016/1148/EC, informs the European Commission at least every two years of the measures to designate the services of essential service providers, their number and importance, the list of essential services and the thresholds for identifying the appropriate level of provision of essential services given the number of users or the importance of the essential service provider concerned;

14. act as the single point of contact for cross-border cooperation with the relevant authorities of other EU Member States and with the network of the CSIRT groups and the cooperation group to which it contributes its representative;

15. meets other information obligations of the European Commission and the cooperation group, information obligations and notification obligations of other international organizations;

16. performs other tasks of international cooperation as needed.

28. Article (national CSIRT)

(1) The national CSIRT is a response centre for dealing with incidents in the field of safety electronic network and information SI-CERT at the public institution Academic and Research Network of Slovenia.

(2) In addition to other tasks specified by this Act, the national CSIRT shall perform the following tasks:

1. provide methodological support, assistance and cooperation to liable parties for which it is responsible in the event of an incident;

2. receive information on risks and vulnerabilities in the field of information security, forward it to the administrators of the affected systems and publish warnings;

3. participate in the network of CSIRT groups, but may also participate in other international cooperation networks;

4. cooperate with CSIRT groups and security operations centres in the Republic of Slovenia and CSIRT groups in other EU Member States;

5. raise user awareness in the field of information security;

6. publish warnings on risks and vulnerabilities in the field of information security;

7. cooperate with the competent national authority and provide information on the exercise of its powers under this Act upon request.

(3) The national CSIRT meets the requirements regarding a high level of availability of its services, security of its business premises and business continuity in accordance with Directive 2016/1148/EU.

29. Article (CSIRT of state administration bodies)

(1) The tasks of the CSIRT of state administration bodies are performed by the ministry responsible for the management of information and communication systems of the state administration.

(2) In addition to other tasks specified by this Act, the CSIRT of state administration bodies shall perform the following tasks:

- receive, process and evaluate incident notifications received from liable parties for which it is responsible, and record, store and protect this information;
- provide methodological support, assistance and cooperation to liable parties for which it is responsible in the event of an incident;
- cooperate with the national CSIRT and the competent national authority and provide information on the exercise of its powers under this Act upon request;
- publish warnings on risks and vulnerabilities in the field of information security of the state administration bodies;

30. Article (cooperation at national level)

(1) The national CSIRT and the CSIRT of state administration bodies shall submit a quarterly report to the competent national authority on the implementation of their tasks.

(2) For the needs of the national information security system, the competent national authority, the national CSIRT and the CSIRT of state administration bodies may cooperate with entities in public administration, the economy, research and development organizations, scientific institutions, interest groups and individuals.

X. Supervision

31. Article (jurisdiction, procedure and legal remedies)

(1) Supervision over the implementation of the provisions of this Act, regulations adopted on its basis and over the implementation of administrative decisions issued on the basis of the fourth paragraph of Article 21 and fourth paragraph of Article 22 of this Act shall be performed by information security inspectors of the competent national authority (hereinafter: inspector)

(2) In addition to the measures he has under the law governing inspection supervision, the inspector may also order measures determined by this Act.

(3) The inspector shall inform the Information Commissioner about the consideration of matters referred to in the first paragraph of this Article, the consequence of which is a violation of personal data protection. For the purpose of timely action in towards ensuring the elimination of breaches of personal data protection, the inspector shall also inform the Information Commissioner in cases of suspected breaches of personal data protection.

(4) An action in an administrative dispute against a final decision issued in supervision procedures under this Act shall be filed at the seat of the Administrative Court of the Republic of Slovenia. The procedure is necessary and preferred.

32. Article (supervision of essential service providers)

(1) The inspector shall supervise whether the providers of essential services meet their obligations from the first and fifth paragraphs of Article 10, from Article 11, from the first, second and fifth paragraphs of Article 12, from the first and second paragraphs of Article 13, from the sixth paragraph of Article 14 of this Act and from decisions issued in compliance with the fourth paragraph of Article 21 and the fourth paragraph of Article 22 of this Act, and measures for the security of networks and information systems issued in compliance with them.

(2) The inspector may require essential service providers to provide the information necessary to assess the security of their networks and information systems, including documented security rules, and evidence of the effective implementation of security rules. Whenever an inspector requests such information or evidence, he shall state the purpose of that request and specify what additional information is required. In conformity with that information, he may impose measures on essential service providers to remedy the deficiencies identified.

(3) An assessment of the security of networks and information systems prepared by the essential service provider jointly with the competent national authority or a safety assessment prepared by a qualified auditor for the essential service provider shall be deemed evidence of the effective implementation of the security rules referred to in the previous paragraph.

33. Article (supervision of digital service providers)

(1) The inspector shall supervise whether the digital service providers for which he is competent in compliance with the first or second paragraph of Article 15 of this Act meet their obligations from the first, second and third paragraphs of Article 14 of this Act and from the decision issued in conformity with the fourth paragraph of Article 21 of this Act.

(2) If evidence is provided to the inspector that the digital service provider is not meeting any of the obligations referred to in the preceding paragraph, he shall issue a decision ordering remedial action.

(3) The evidence referred to in the previous paragraph may also be submitted by the competent authorities of other EU Member States where the service is provided, and which may also propose the adoption of supervision measures referred to in the previous paragraph.

(4) The inspector may require essential service providers to provide the information necessary to assess the security of their networks and information systems, including documented security rules.

(5) In the supervision procedures referred to in the first paragraph of this Article, the inspector shall, if necessary, cooperate with the competent supervision authorities in other EU Member States if the digital service provider has its networks and information systems in one or more other EU Member States. Such cooperation shall include the exchange of information between the supervisory authorities concerned.

(6) The information and data referred to in the previous paragraph, which are confidential, shall be exchanged, if necessary, for the application of Directive 2016/1148/EU or for the implementation of this Act. The exchange shall be limited to the extent appropriate and necessary for the purpose referred to in the preceding paragraph and shall preserve the confidentiality of the information and data provided.

34. Article (supervision of state administration bodies)

(1) The inspector supervises whether the state administration bodies meet their obligations from the first and second paragraphs of Article 16, from the first, second and fifth paragraphs of Article 17, from the first and second paragraphs of Article 18 of this Act and from decisions issued in compliance with the fourth paragraph of Article 21 and the fourth paragraph of Article 22 of this Act, as well as measures for the security of networks and information systems determined on the basis thereof.

(2) The inspector may require state administration bodies to provide the information necessary to assess the security of their networks and information systems, including documented security rules, and evidence of the effective implementation of security rules. Whenever an inspector requests such information or evidence, he shall state the purpose of that request and specify what additional information is required.

(3) An assessment of the security of networks and information systems prepared by the essential service provider jointly with the competent national authority or a safety assessment prepared by a qualified auditor for the state administration body shall be deemed evidence of the effective implementation of the security rules referred to in the previous paragraph.

(4) Based on the safety assessment referred to in the previous paragraph, the inspector may impose measures for remedial action.

35. Article (special measure)

Notwithstanding the provisions of the Act governing inspections, the inspector may, as a last resort and with due consideration given to the importance of the areas referred to in the second paragraph of Article 5 of this Act or their system and activities, prohibit the use of this system or its part until the deficiency is remedied and if this measure does not compromise the security of supply in an individual area or the provision of their services.

XI. Penal provisions

36. Article (expedited fine proceedings for minor offences)

For offenses under this Act, a fine may also be imposed in an expedited procedure in an amount higher than the minimum prescribed fine determined by this Act.

37. Article (essential service provider offenses)

(1) A fine of EUR 500 to 10,000 shall be imposed upon any legal person, and a fine of EUR 10,000 to 50,000 shall be imposed on a legal person which, under the Act governing companies, is considered to be a medium-sized or large company if, during the course of dealings, it:

1. fails to meet the obligations referred to in the first or fifth paragraph of Article 10 of this Act;

2. fails to meet the obligations referred to in Article 11 of this Act;

3. fails to meet the obligations referred to in the first, second or fifth paragraph of Article 12 of this Act;

4. fails to meet the obligations referred to in the first or second paragraph of Article 13 of this Act;

5. fails to meet the obligations referred to in the sixth paragraph of Article 14 of this Act;

6. fails to meet the obligations from the decision issued in compliance with the fourth paragraph of Article 21 of this Act;

7. it fails to meet the obligations from the decision issued in compliance with the fourth paragraph of Article 22 of this Act;

(2) A fine of EUR 500 to 10,000 shall be imposed upon a sole proprietor or an individual who performs an activity independently if he commits an offense referred to in the preceding paragraph.

(3) A fine of EUR 200 to 2,000 shall be imposed upon the responsible person of a legal person or the responsible person of a sole proprietor, the responsible person of a self-employed person and the responsible person in a state body, self-governing local community or in any other party governed by public law who is a provider of essential services under this Act if he commits an offense referred to in the first paragraph of this Article.

38. Article (offenses by digital service provider)

(1) A fine of EUR 500 to 10,000 shall be imposed upon any legal person, and a fine of EUR 10,000 to 50,000 shall be imposed on a legal person which, under the Act governing companies, is considered to be a medium-sized or large company if it:

- fails to meet the obligations referred to in the first, second or third paragraph of Article 14 of this Act;
- fails to meet the obligations from the decision issued in compliance with the fourth paragraph of Article 21 of this Act;

(2) A fine of EUR 500 to 10,000 shall be imposed upon a sole proprietor if he commits an offense referred to in the preceding paragraph.

(3) A fine of EUR 200 to 2,000 shall be imposed upon the responsible person of a legal person or the responsible person of a sole proprietor who is a provider of digital services under this Act if he commits an offense referred to in the first paragraph of this Article.

39. Article (minor offences of state administrative bodies)

A fine of EUR 200 to 2,000 shall be imposed on a responsible person in a state administration body if the latter:

- fails to meet the obligations referred to in Article 16 of this Act;
- fails to meet the obligations referred to in the first, second or fifth paragraph of Article 17 of this Act;

- fails to meet the obligations referred to in the first or second paragraph of Article 18 of this Act;
- fails to meet the obligations from the decision issued in compliance with the fourth paragraph of Article 21 of this Act;
- fails to meet the obligations from the decision issued in compliance with the fourth paragraph of Article 22 of this Act;

XII. Transitional provisions

40. Article (commissioning of the competent national authority)

(1) The competent national authority shall become operational by 1 January 2020 at the latest.

(2) Until the competent national authority becomes operational, its tasks shall be performed by the Office of the Government of the Republic of Slovenia for the Protection of Classified Information (hereinafter: OGCI) in accordance with this Act, except for administrative decision-making and supervision tasks performed by the ministry responsible for information society.

(3) With the date of commencement of operations, the competent national authority shall take over from OGCI the tasks, archives and documentation related to information security, as well as civil servants, budget spending rights, equipment and other databases or records from the taken over field of work.

(4) The Government shall harmonize the Decision on the Establishment, Tasks and Organization of the Office of the Government of the Republic of Slovenia for the Protection of Classified Information (Official Gazette of the Republic of Slovenia, Nos. 6/02 and 17/17) with this Act within three months of its entry into force.

41. Article (operation of other competent authorities)

(1) The national CSIRT shall take effect under this Act on 1 January 2019.

(2) The CSIRT of state administration bodies shall be established at the ministry responsible for the management of information and communication systems of the state administration on 1 January 2019.

(3) Until the establishment of the CSIRT of state administration bodies, its tasks related to the handling of incidents shall be performed by the national CSIRT.

Article 42 (issuance of secondary regulations and strategies)

(1) The Government shall harmonize the Regulation on Bodies within Ministries (Official Gazette of the Republic of Slovenia, Nos. 35/15, 62/15, 84/16, 41/17 and 53/17) with this Act within three months of its entry into force.

(2) The secondary regulations referred to in the first paragraph of Article 6, the fourth paragraph of Article 7, the third paragraph of Article 12 and the third paragraph of Article 17 of this Act shall be adopted within six months of the entry into force of this Act.

(3) The Government shall adopt the strategy referred to in Article 26 of this Act within one year of the entry into force of this Act.

43. Article (transitional period)

(1) The Government shall designate individual providers of essential services referred to in the second and third paragraphs of Article 6 of this Act within six months of the entry into force of the regulations referred to in the first paragraph of Article 6 and the fourth paragraph of Article 7 of this Act.

(2) The provider of essential services must meet the security requirements and requirements for notification of incidents referred to in Articles 11, 12 and 13 of this Act in accordance with this Act within six months of its designation referred to in the preceding paragraph.

(3) The provider of essential services must meet the security requirements and requirements for notification of incidents referred to in Article 14 of this Act in accordance with this Act within nine months from the entry into force of this Act

(4) The Government shall designate state administration bodies in accordance with Article 9 of this Act within nine months of the entry into force of this Act.

(5) State administration bodies must meet the security requirements and requirements for the notification of incidents referred to in Articles 16, 17 and 18 of this Act in accordance with this Act within twelve months of their designation referred to in the preceding paragraph.

XIII. Final provision

44. Article (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.