EnCaViBS

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

Member State:

Poland

Act of 5 July 2018 on the national cyber security system

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: Poland

Act of 5 July 2018 on the national cyber security system[1),2)]

Chapter 1

General provisions

Article 1.

1. The Act defines

1) organisation of the national system of cyber security as well as tasks and obligations of entities that are part of that system;

2) the way of exercising supervision and control within the scope of application of the provisions of the Act;

3) the scope of the Cyber Security Strategy of the Republic of Poland.

2. The Act shall not apply to:

1) telecommunications enterprises referred to in the Act of 16 July 2004 - Telecommunications Law (Journal of U. of 2017, item 1907 and 2201 and of 2018, item 106, 138, 650 and 1118), with regard to security and incident reporting requirements;

2) trust service providers who are 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 EU L 257 of 28/08/2014, p. 73).

3) entities performing medical activities, created by the Head of the Internal Security Agency or the Head of the Intelligence Agency.

Article 2.

The definitions used herein shall have the following meaning:

1) CSIRT GOV - Computer Security Incident Response Team operating on a national level, led by the Head of the Internal Security Agency;

2) CSIRT MON - Computer Security Incident Response Team operating on a national level, led by the Minister of National Defence;

3) CSIRT NASK - Computer Security Incident Response Team operating on a national level, managed by the Research and Academic Computer Network - National Research Institute;

4) cybersecurity - the resilience of information systems to actions that compromise the confidentiality, integrity, availability and authenticity of the data processed or the related services offered by those systems;

---

1) This Act, within the scope of its regulation, implements Directive 2016/1148 of the European Parliament and of the Council of 6 July 2016 on measures for a high common level of security of networks and information systems within the Union (OJ EU L 194 of 19/07/2016, p. 1).

2) This Act amends the following acts: the Act of 7 September 1991 on the Educational System, the Act of 4 September 1997 on the Departments of Government Administration, the Act of 24 May 2002 on the Internal Security Agency and the Intelligence Agency, the Act of 29 January 2004 - The Act on the Public Procurement Law, the Act of 16 July 2004. - Telecommunication Law and the Act of 26 April 2007 on crisis management.

5) incident - an event that has or may have an adverse impact on cyber security;

6) critical incident - an incident resulting in significant damage to security or public order, international interests, economic interests, operation of public institutions, civil rights and freedoms or human life and health, classified by the competent CSIRT MON, CSIRT NASK or CSIRT GOV;

7) major incident - an incident that causes or is likely to cause a serious degradation of quality or interruption of the continuity of the provision of a key service;

8) significant incident - an incident that has a significant impact on the provision of a digital service as provided in Article 4 of Commission Implementing Regulation (EU) 2018/151 of 30 January 2018 laying down rules for the application of Directive (EU) 2016/1148 of the European Parliament and of the Council as regards further specification of the elements to be considered by digital service providers in managing existing risks to the security of networks and information systems and the parameters for determining whether an incident has a significant impact (OJ EU L 26 of 31/01/2018, p. 48), hereinafter 'Implementing Regulation 2018/151';

9) incident in a public entity - an incident which causes or may cause a decline in quality or interruption of the performance of a public task carried out by a public entity, referred to in Article 4(7-15);

10) incident handling - activities which enable to detect, record, analyse, classify, prioritise, take corrective actions and limit the effects of an incident;

11) vulnerability - a property of an information system that can be exploited by a cyber security threat;

12) risk - the combination of the probability of an adverse event occurring and its consequences;

13) risk assessment - the overall process of risk identification, analysis and evaluation;

14) information system - an ICT system referred to in Article 3(3) of the Act of 17 February 2005 on the computerisation of the activities of entities performing public tasks (Journal of Laws of 2017, item 570 and of 2018, items 1000 and 1544), together with the data processed therein electronically;

15) digital service - a service provided by electronic means within the meaning of the Act of 18 July 2002 on provision of services by electronic means (Journal of Laws of 2017, item 1219 and of 2018, item 650), listed in Annex 2 to the Act;

16) key service - a service that is critical to maintaining a critical social or economic activity, listed in the list of key services;

17) cyber security threat - a potential cause of an incident;

18) incident management - the handling of an incident, finding links between incidents, removing the causes of incidents and developing lessons learned from handling an incident;

19) risk management - coordinated cyber security management activities in relation to assessed risks.

Article 3.

The National Cyber Security System is to ensure cyber security at national level, including the uninterrupted provision of critical and digital services, by achieving an adequate level of security of the information systems used to provide these services and ensuring incident handling.

Article 4.

The National Cyber Security System includes

1) key service operators;

2) digital service providers;

3) CSIRT MON;

4) CSIRT NASK;

5) CSIRT GOV;

6) sector cyber security teams;

7) units of the public finance sector referred to in Article 9(1-6) (8-9) (11-12) of the Act of 27 August 2009 on public finance (Journal of Laws of 2017, item 2077 and of 2018, item 62, 1000 and 1366);

8) research institutes;

9) Narodowy Bank Polski (National Bank of Poland);

10) Bank Gospodarstwa Krajowego [National Economy Bank);

11) Office of Technical Inspection;

12) Polish Air Navigation Services Agency;

13) Polish Accreditation Centre;

14) National Fund for Environmental Protection and Water Management and provincial funds for environmental protection and water management;

15) commercial law companies performing public utility tasks as provided in Article 1(2) of the Act of 20 December 1996 on municipal management (Journal of Laws of 2017, item 827 and of 2018, item 1496);

16) entities providing cyber security services;

17) authorities competent for cyber security matters;

18) The Single Point of Contact for Cyber Security, hereinafter the ‘Single Point of Contact’;

19) Government Commissioner for Cyber Security, hereinafter ‘Commissioner’;

20) the Government Plenipotentiary for Cyber Security, hereinafter ‘Plenipotentiary’;

Chapter 2

Identification and registration of key service providers

Article 5.

1. A key service operator is an entity referred to in Annex 1 to the Act, having an organisational unit in the Republic of Poland, for which the authority competent for cyber security has issued a decision on recognition as a key service operator. Sectors, subsectors and types of entities are specified in Annex 1 to the Act.

2. The authority competent for cyber security shall issue a decision on recognition of an entity as a key service operator if:

1) the entity provides a key service; the provision of this service;

2) depends on information systems;

3) the incident would have a significant disruptive effect on the provision of the key service by that operator.

3. The materiality of the disruptive effect of the incident on the provision of the key service referred to in section 2(3) shall be determined on the basis of the thresholds of materiality of the disruptive effect.

4. Where an entity provides a key service in other Member States of the European Union, the competent authority for cyber security shall, in the course of administrative proceedings, through the Single Point of Contact, carry out consultations with those States to determine whether that entity has been recognised as a key service operator in those States.

5. The period for holding consultations referred to in section 4 shall not be included in the time limits referred to in Article 35 of the Act of 14 June 1960 - Code of Administrative Proceedings (Journal of Laws of 2017, item 1257 and of 2018, item 149, 650 and 1544);

6. For an entity that ceased to meet the conditions referred to in sections 1 and 2, the authority competent for cyber security shall issue a decision stating the expiry of the decision on recognition as a key service operator.

7. The decisions referred to in sections 2 and 6 are immediately enforceable.

Article 6.

The Council of Ministers shall determine the following in its regulations:

1) the list of key services referred to in Article 5(2)(1), guided by the assignment of the key service to a given sector, subsector and type of entity listed in Annex 1 to the Act and by the importance of the service for the maintenance of critical social or economic activity;

2) the thresholds of materiality of the disruptive effect of the incident on the provision of the key services listed in the list of key services, taking into account:

   a) the number of users dependent on the key service provided by the entity:

   b) the dependence of other sectors referred to in Annex 1 of the Act on the service provided by the entity:

   c) the impact that the incident, in terms of its scale and duration, could have on economic and social activity or public safety:

   d) the market share of the key service provider:

   e) the geographical scope of the area which could be affected by the incident,

   f) the ability of the provider to maintain a sufficient level of performance of the key service, given the availability of alternative means of delivery,

   g) other sector- or subsector-specific factors, if any,

   - based on the need to protect against threats to human life or health, significant damage to property and degradation of the quality of the key service provided.

Article 7.

1. The minister competent for informatisation shall maintain a list of key service operators.

2. The list of key service operators includes:

1) name (business name) of the key service operator;

2) sector, sub-sector and type of entity

3) seat and address;

4) Tax identification number (NIP), if assigned;

5) the number in the relevant register, if any;

6) name of the key service, according to the list of key services;

7) key service start date;

8) information stating in which Member States of the European Union the entity has been recognised as a key service operator;

9) key service termination date;

10) the date of removal from the list of key service operators.

3. Entry into and removal from the list of key service operators shall take place upon an application of the competent authority for cyber-security submitted immediately after the issuance of a decision on recognition as a key service operator or a decision stating the expiry of a decision on recognition as a key service operator. The application shall contain data referred to in section 2(1-9).

4. A change of data in the list of key service providers shall be made upon request of the authority competent for cyber security, submitted no later than within 6 months from the change of such data.

5. The applications referred to in sections 3 and 4 shall be drawn up in an electronic form and affixed with a qualified electronic signature or a signature confirmed by a trusted ePUAP [Electronic Platform of Public Administration Services] profile.

6. Entering into the list of key service providers and removing from the list as well as changing the data in the list of key service providers is a material and technical activity.

7. The minister competent for informatisation shall make available to the CSIRT MON, CSIRT NASK, CSIRT GOV and the sectoral cyber security team within the scope of the sector or subsector for which it has been established, as well as to the key service operator within the scope related to it.

8. The data from the list of key service operators to the extent necessary for the performance of their statutory tasks, shall be made available by the minister in charge of informatisation, upon request, to the following entities:

1) authorities competent in matters of cyber security;

2) the Police

3) Military Police

4) Border Guard;

5) the Central Anti-Corruption Bureau;

6) the Internal Security Agency and the Intelligence Agency;

7) the Military Counterintelligence Service and the Military Intelligence Service;

8) courts;

9) prosecutor's office;

10) bodies of the National Treasury Administration;

11) the Director of the Government Centre for Security;

12) National Protection Service.

Chapter 3

Obligations of key service providers

Article 8.

The operator of the key service shall implement a security management system for the information system used for the provision of the key service that ensures:

1) conducting a systematic estimation and management of the risk of an incident;

2) implementation of technical and organisational measures appropriate and proportionate to the assessed risk, taking into account the state of the art, including:

   a) maintenance and safe operation of the information system,

   b) physical and environmental security, including access control,

   c) security and continuity of supply of services upon which the provision of the critical service depends,

   d) implementation, documentation and maintenance of action plans enabling the continuous and uninterrupted provision of the key service and ensuring confidentiality, integrity, availability and authenticity of the information,

   e) the information system used for the provision of the key service is subject to continuous monitoring;

3) collection of information on cyber security threats and vulnerabilities of the information system used to provide the critical service;

4) incident management;

5) application of measures to prevent and mitigate the impact of incidents on the security of the information system used to provide the key service, including:

   a) application of mechanisms ensuring confidentiality, integrity, availability and authenticity of data processed in the information system;

   b) care for updating the software;

   c) protection against unauthorised modification of the information system;

   d) taking immediate action upon becoming aware of vulnerabilities or threats to cyber security;

6) the application of means of communication allowing proper and secure communication within the national cyber security system.

Article 9.

1. Key service operator:

1) designate a contact person for the national cyber-security system;

2) provide the key service user with access to knowledge to understand cyber threats and apply effective ways of protecting against those threats to the extent related to the key service provided, in particular by publishing information on this subject on its website;

3) provide the authority competent for cyber security with the data referred to in Article 7(2)(8) and (9) no later than 3 months after the change of such data.

2. The operator of a key service shall provide the competent authority for cyber security, the competent CSIRT MON, CSIRT NASK, CSIRT GOV and sectoral cyber security team with the data of the person referred to in section 1(1), including name, surname, telephone number and e-mail address, within 14 days from the date of appointment, as well as information on change of such data - within 14 days from the date of change.

Article 10.

1. The operator of a key service shall develop, apply and update cyber security documentation for the information system used to provide the key service.

2. The key service operator shall be required to establish oversight of the information system cyber security documentation used to provide the key service, ensuring:

1) accessibility of documents only to persons authorised according to their tasks;

2) protection of documents against misuse or loss of integrity;

3) marking the successive versions of documents to identify changes made to them.

3. The operator of a key service shall store documentation related to the cyber security of the information system used to provide a key service for at least 2 years from the date of its withdrawal from use or termination of the key service, taking into account the provisions of the Act of 14 July 1983 on National Archive Resources and Archives (Journal of Laws of 2018 items 217, 357, 398 and 650).

4. The operator of a key service who is at the same time an independent owner, owner or dependent possessor of facilities, installations, equipment or services constituting critical infrastructure, listed in the list referred to in Article 5b(7)(1) of the Act of 26 April 2007 on crisis management (Journal of Laws of 2018, item 1401), which has an approved critical infrastructure protection plan that includes documentation on the cyber security of the information system used to provide the key service, is not required to develop the documentation referred to in section 1.

5. The Council of Ministers shall determine, in an ordinance, the types of documentation referred to in section 1, taking into account the Polish Standards and the need to ensure cyber security during the provision of key services and the continuity of such services.

Article 11.

1. Key service operator:

1) ensures incident handling;

2) provides access to information on registered incidents to the competent CSIRT MON, CSIRT NASK or CSIRT GOV to the extent necessary to perform its tasks;

3) classifies an incident as major on the basis of thresholds for considering an incident as major;

4) reports the major incident immediately, not later than within 24 hours from the moment of detection to the appropriate CSIRT MON, CSIRT NASK or CSIRT GOV;

5) cooperates during the handling of a major incident and a critical incident with the appropriate CSIRT MON, CSIRT NASK or CSIRT GOV by providing necessary data, including personal data

6) removes vulnerabilities referred to in Article 32.2 and informs the authority competent for cyber security about their removal;

2. The notification referred to in section 1(4) shall be transmitted in electronic form, and if it is not possible to transmit it in electronic form - using other available means of communication.

3. In the event of the establishment of a sectoral cyber-security team, the operator of a key service shall, irrespective of the tasks referred to in section 1:

1) simultaneously provides the team with the notification referred to in section 1(4) in electronic form;

2) cooperates with this team during the handling of a major incident and a critical incident by providing necessary data, including personal data;

3) provides this team with access to information on registered incidents to the extent necessary to perform its tasks;

4. The Council of Ministers shall define, by way of a regulation, the thresholds for recognising an incident as major according to the type of incident in individual sectors and subsectors specified in Annex 1 to the Act, taking into account:

1) the number of users affected by the disruption of the provision of the key service,

2) time of impact of the incident on the provided key service,

3) the geographical scope of the area which could be affected by the incident,

4) other sector- or subsector-specific factors, if any,

- based on the need to protect against threats to human life or health, significant damage to property and degradation of the quality of the key service provided.

Article 12.

1. The notification referred to in Article 11(1)(4) shall include:

1) data of the notifying entity, including the entrepreneur's company name, number in the relevant register, seat and address;

2) name and surname, telephone number and e-mail address of the person making the notification;

3) name and surname, telephone number and e-mail address of a person authorised to give explanations regarding the reported information;

4) a description of the impact of the major incident on the provision of the critical service, including:

   a) the notifier's key services affected by the major incident;

   b) number of users of the critical service impacted by the major incident;

   c) the time of occurrence and detection of the major incident and its duration;

   d) the geographical scope of the area affected by the major incident;

   e) impact of the major incident on the provision of the key service by other key service operators and digital service providers;

   f) the cause and course of the major incident and the consequences of its impact on the information systems or the key services provided;

5) information enabling the competent CSIRT MON, CSIRT NASK or CSIRT GOV to determine whether the incident concerns two or more Member States of the European Union;

6) for an incident that may have affected the provision of a key service, description of the causes of the incident, how the incident unfolded and the likely impact on the information systems;

7) information on preventive actions taken;

8) information about corrective actions taken;

9) other relevant information.

2. The operator of the key service shall provide information known to it at the time of the notification which it completes in the course of handling the major incident.

3. The operator of a key service shall provide, to the extent necessary, in the notification referred to in Article 11(1)(4), information constituting legally protected secrets, including business secrets, where this is necessary for the performance of the tasks of the competent CSIRT MON, CSIRT NASK or CSIRT GOV and the sector cyber security team.

4. The competent CSIRT MON, CSIRT NASK or CSIRT GOV and the sectoral cyber security team may request the operator of the key service to supplement the notification with information, including information constituting legally protected secrets, to the extent necessary to perform the tasks referred to in the Act.

5. In the notification, the operator of the key service shall flag information which constitutes legally

protected secrets, including business secrets.

Article 13.

1. The operator of the key service may transmit information to the competent CSIRT MON, CSIRT NASK or CSIRT GOV:

1) about other incidents;

2) on cyber security threats;

3) on risk assessment;

4) on vulnerabilities;

5) on the technologies used.

2. The notification referred to in section 1(4) shall be transmitted in electronic form, and if it is not possible to transmit it in electronic form - using other available means of communication.

3. In the case of the establishment of a sectoral cyber-security team, the key service operator may simultaneously provide the information referred to in section 1 to that team in electronic form.

4. In the notification, the operator of the key service shall flag information which constitutes legally protected secrets, including business secrets.

Article 14.

1. The operator of a key service shall, in order to perform the tasks referred to in Article 8, Article 9, Article 10(1-3), Article 11(1-3), Article 12 and Article 13, establish internal structures responsible for cyber-security or enter into an agreement with a cyber-security service provider.

2. The internal structures established by the key service operator responsible for cyber security and the providers of cyber security services shall:

1) meet the organisational and technical conditions to provide cyber security to the supported key service operator;

2) have premises for the provision of incident response services that are protected against physical and environmental threats;

3) apply safeguards to ensure confidentiality, integrity, availability and authenticity of the information handled, taking into account personal security, operations and systems architecture.

3. The operator of the key service shall inform the authority competent for cyber security and the competent CSIRT MON, CSIRT NASK, CSIRT GOV and the sectoral cyber security team about the entity with which the agreement for the provision of cyber security services has been concluded, the contact details of this entity, the scope of the provided service and the termination of the agreement within 14 days from the date of conclusion or termination of the agreement.

4. The minister competent for information technology shall determine, by means of an ordinance, the organisational and technical conditions for entities providing cyber security services and internal structures responsible for cyber security, taking into account the Polish Standards and the need to ensure security for internal structures responsible for cyber security and entities providing cyber security services to key service operators, as well as the need to ensure the security of information processed in these structures or entities.

Article 15.

1. The operator of the key service shall ensure that a security audit of the information system used for the provision of the key service, hereinafter referred to as ‘audit’, is carried out at least every 2 years.

2. The audit may be conducted by:

1) a compliance assessment body accredited in accordance with the provisions of the Act of 13 April 2016 on compliance assessment and market surveillance systems (Journal of Laws of 2017, item 1398 and of 2018, item 650 and 1338), to the extent applicable to undertaking information systems security assessments;

2) at least two auditors with:

   a) certificates specified in regulations issued as provided in section 8 or

   b) at least three years of practice in information systems security auditing, or

   c) at least two years of practice in information systems security auditing and holding a post-graduate diploma in information systems security auditing issued by an organisational unit which, on the date of issuing the diploma, was authorised, in accordance with separate regulations, to award a doctoral degree in economics, technical or legal sciences

3) sectoral cyber security team, established within the sector or subsector listed in Annex 1 to the Act, if auditors meet the conditions referred to in item 2.

3. The practice in information systems security audits referred to in section 2(2)(b-c), is the documented performance of 3 audits in information systems security or business continuity in the last 3 years before the date of start of the audit, or the performance of information systems security or business continuity audits with a working time of not less than 1/2 time, related to:

1) conducting an internal audit under the supervision of an internal auditor

2) conducting out an external audit under the supervision of a lead auditor;

3) conducting an internal audit in the field of information security referred to in the regulations issued on the basis of Article 18 of the Act of 17 February 2005 on Informatisation of the Activities of Entities Performing Public Task;

4) performance of inspection activities referred to in the Act of 15 July 2011 on inspection in the government administration (Journal of Laws item 1092);

5) performance of inspection activities referred to in the Act of 23 July 1994 on the Supreme Audit Office (Journal of Laws of 2017, item 524 and of 2018, item 1000);

4. The auditor shall keep secret the information obtained in connection with the audit, observing the provisions on the protection of classified information and other legally protected information.

5. Based on the documents and evidence collected, the auditor shall draw up a written audit report and forward it to the key service operator together with the audit documentation.

6. A key service operator, for which in a given year an internal audit covering information security referred to in the regulations issued on the basis of Article 18 of the Act of 17 February 2005 on Informatisation of the Activities of Entities Executing Public Tasks has been performed by persons fulfilling the conditions defined in section 2(2), shall not be obliged to perform an audit for 2 years.

7. The operator of a key service shall provide a copy of the audit report upon a reasonable request issued by

1) the authority competent for cyber security matters;

2) the operator of a key service who is at the same time an independent owner, owner or dependent possessor of facilities, installations, equipment or services constituting critical infrastructure, listed in the list referred to in Article 5b(7)(1) of the Act of 26 April 2007 on crisis management;

3) the Internal Security Agency and the Intelligence Agency;

8. The minister competent for information technology shall define by issuing an ordinance, a list of certificates entitling to conduct an audit, taking into consideration the scope of expertise required from persons holding particular certificates.

Article 16.

The operator of a key service shall fulfil the obligations set forth in

1) Article 8(1) and (4), Article 9, Article 11(1)-(3), Article 12 and Article 14(1) - within 3 months from the date of delivery of a decision on designation as a key service operator;

2) Article 8(2), (3), (5) and (6) and Article 10(1) to (3) - within 6 months of the delivery of a decision to recognise a key service operator;

3) Article 15(1) - within one year of the delivery of a decision to recognise a key service operator.

Chapter 4

Obligations of digital service providers

Article 17.

1. A digital service provider shall be a legal person or an organisational unit without legal personality having its registered office or management on the territory of the Republic of Poland or a representative having an organisational unit on the territory of the Republic of Poland, providing a digital service, except for micro-entrepreneurs and small entrepreneurs referred to in Article 7(1)(1) and (2) of the Act of 6 March 2018 - Entrepreneurs' Law (Journal of Laws item 646 and 1479). Types of digital services are specified in Annex 2 to the Act.

2. The digital service provider shall take appropriate and proportionate technical and organisational measures, as defined in Implementing Regulation 2018/151, to manage the risks to which the information systems used to provide the digital service are exposed. Those measures shall ensure cyber security appropriate to the risks involved and shall consider the following:

1) information systems and facilities security;

2) incident handling;

3) business continuity management of the provider to deliver the digital service;

4) monitoring, auditing and testing;

5) state of the art, including compliance with international standards as referred to in Implementing Regulation 2018/151.

3. The digital service provider shall take measures to prevent and minimise the impact of incidents on the digital service in order to ensure the continuity of the digital service.

4. A digital service provider that does not have a business unit in one of the Member States of the European Union but offers digital services in the Republic of Poland shall appoint a representative with a business unit in the Republic of Poland, unless it has appointed a representative with a business unit in another Member State of the European Union.

5. A representative may be a natural person, a legal person or an organisational unit without legal personality, established in the Republic of Poland or in another European Union Member State, appointed to act on behalf of a digital service provider that does not have an organisational unit in the European Union, to whom the authority competent for cyber security, the CSIRT MON, the CSIRT NASK or the CSIRT GOV may address in relation to the obligations of the digital service provider under

the Act.

Article 18.

1. The digital service provider shall

1) perform activities enabling detection, recording, analysis and classification of incidents;

2) provide access to information to the competent CSIRT MON, CSIRT NASK or CSIRT GOV on incidents classified as critical by the competent CSIRT MON, CSIRT NASK or CSIRT GOV, to the extent necessary;

3) classify an incident as significant;

4) report the significant incident immediately, not later than within 24 hours from the moment of detection to the competent CSIRT MON, CSIRT NASK or CSIRT GOV;

5) ensure handling of a major incident and a critical incident with the appropriate CSIRT MON, CSIRT NASK or CSIRT GOV by providing necessary data, including personal data;

6) remove vulnerabilities referred to in Article 32(2);

7) communicate to the operator of the key service that provides the key service through that digital service provider, information regarding an incident affecting the continuity of the provision of the key service of that operator.

2. The digital service provider shall, in order to classify an incident as significant, take into account the following:

1) the number of users affected by the incident, in particular users dependent on the service for the provision of their own services;

2) the duration of the incident;

3) the geographical scope of the area affected by the incident;

4) the extent of disruption of the service;

5) the extent of impact of the incident on economic and social activity.

3. When classifying an incident as significant, the digital service provider shall assess the materiality of the impact of the incident on the provision of the digital service based on the parameters referred to in section 2 and the thresholds set out in Implementing Regulation 2018/151.

4. The digital service provider shall not be required to make the notification referred to in section 1(4) when it does not have information to assess the materiality reports the major incident impact on the provision of digital service.

5. The notification referred to in section 1(4) shall be transmitted in electronic form, and if it is not possible to transmit it in electronic form - using other available means of communication.

Article 19.

1. The notification referred to in Article 18(1)(4) shall include:

1) data of the notifying entity, including the entrepreneur's company name, number in the relevant register, seat and address;

2) name and surname, telephone number and e-mail address of the person making the notification;

3) name and surname, telephone number and e-mail address of a person authorised to give explanations regarding the reported information;

4) a description of the impact of the major incident on the provision of the critical service, including:

   a) the number of users affected by the material incident,

   b) the time of occurrence and detection of the material incident and its duration,

   c) the geographical scope of the area affected by the major incident;

   d) the extent of disruption of the service;

   e) the extent of impact of the incident on economic and social activity.

5) information enabling the competent CSIRT MON, CSIRT NASK or CSIRT GOV to determine whether the incident concerns two or more Member States of the European Union;

6) information about the cause and origin of the major incident;

7) information on preventive actions taken;

8) information about corrective actions taken;

9) other relevant information.

2. The operator of the key service shall provide information known to it at the time of the request which it completes in the course of handling the major incident.

3. The operator of a key service shall provide, to the extent necessary, in the notification referred to in Article 18(1)(4), information constituting legally protected secrets, including business secrets, where this is necessary for the performance of the tasks of the competent CSIRT MON, CSIRT NASK or CSIRT GOV.

4. The competent CSIRT MON, CSIRT NASK or CSIRT GOV and the sectoral cyber security team may request the operator of the key service to supplement the notification with information, including information constituting legally protected secrets, to the extent necessary to perform the tasks referred to in the Act.

5. In the notification, the operator of the key service shall flag information which constitutes legally protected secrets, including business secrets.

Article 20.

The operator of the key service may transmit information to the competent CSIRT MON, CSIRT NASK or CSIRT GOV: The said information shall be transmitted in electronic form, and if it is not possible to transmit it in electronic form - using other available means of communication.

Chapter 5

Obligations of public entities

Article 21.

1. The public entity, referred to in Article 4(7-15), performing a public task dependent on the information system shall appoint a person responsible for maintaining contact with the entities of the national cyber security system.

2. A public administration body may designate one person responsible for maintaining contact with the entities of the national cyber security system with regard to public tasks dependent on the information systems and performed by units subordinate to it or supervised by it.

3. A local government unit may designate one person responsible for maintaining contact with the entities of the national cyber security system with regard to public tasks dependent on information systems and performed by its organisational units.

Article 22.

1. The public entity, referred to in Article 4(7-15), performing a public task dependent on an information system shall:

1) ensure incident management in the public entity;

2) report the significant incident immediately, not later than within 24 hours from the moment of detection to the competent CSIRT MON, CSIRT NASK or CSIRT GOV;

3) ensure handling of a major incident and a critical incident with the appropriate CSIRT MON, CSIRT NASK or CSIRT GOV by providing necessary data, including personal data;

4) provide the key service user with access to knowledge to understand cyber threats and apply effective protection measures against those threats to the extent related to the key service provided, in particular by publishing information on this subject on its website;

5) provide the competent CSIRT MON, CSIRT NASK, CSIRT GOV and sectoral cyber security team with the data of the person referred to in Article 21, including name, surname, telephone number and e-mail address, within 14 days from the date of appointment, as well as information on change of such data - within 14 days from the date of change.

2. The notification referred to in section 1(2) shall be transmitted in electronic form, and if it is not possible to transmit it in electronic form - using other available means of communication.

Article 23.

1. The notification referred to in Article 22(1)(2) shall include:

1) data of the notifying entity, including the entity name, number in the relevant register, seat and address;

2) name and surname, telephone number and e-mail address of the person making the notification;

3) name and surname, telephone number and e-mail address of a person authorised to give explanations regarding the reported information;

4) description of the impact of the incident in the public entity on the public task performed, including:

   a) indication of the public task affected by the incident,

   b) number of persons affected by the incident

   c) the time of occurrence and detection of the incident and its duration,

   d) the geographical scope of the area that is affected by the incident,

   e) the cause of the incident and the consequences of its impact on the information systems or the public entity;

5) information about the cause and origin of the incident;

6) information on preventive actions taken;

7) information about corrective actions taken;

8) other relevant information.

2. The operator of the key service shall provide information known to it at the time of the notification, which it completes in the course of handling the incident in a public entity.

3. The public entity referred to in Article 4(7-15) shall, to the extent necessary, provide in the notification referred to in Article 22(1)(2) information constituting legally protected secrets, including business secrets, where this is necessary for the performance of the tasks of the competent CSIRT MON, CSIRT NASK or CSIRT GOV.

4. The competent CSIRT MON, CSIRT NASK or CSIRT GOV and the sectoral cyber security team may request the operator of the key service to supplement the notification with information, including information constituting legally protected secrets, to the extent necessary to perform the tasks referred to in the Act.

5. In the notification, the operator of the key service shall flag information which constitutes legally protected secrets, including business secrets.

Article 24.

The public entity referred to in Article 4(7-15), executing a public task may, depending on the information system, transfer to the competent CSIRT MON, CSIRT NASK or CSIRT GOV information referred to in Article 13(1). The said information shall be transmitted in electronic form, and if it is not possible to transmit it in electronic form - using other available means of communication.

Article 25.

A public entity referred to in Article 4(7-15), for which a decision on recognition as a key service operator has been issued, shall be subject to the provisions of Chapter 3 with regard to the provision of the key service for the provision of which it has been recognised as a key service operator.

Chapter 6

Tasks of CSIRT MON, CSIRT NASK i CSIRT GOV

Article 26.

1. CSIRT MON, CSIRT NASK and CSIRT GOV shall cooperate with each other, with authorities competent in matters of cyber security, the minister competent in matters of informatisation and the Plenipotentiary, ensuring a coherent and complete risk management system at the national level, performing tasks to counter cyber security threats of cross-sectoral and cross-border nature, as well as ensuring coordination of handling reported incidents.

2. CSIRT MON, CSIRT NASK and CSIRT GOV, in justified cases, upon the request of operators of key services, providers of digital services, public entities referred to in Article 4(7-15), sectoral cyber security teams or owners, owners or dependent owners of facilities, installations, devices or services constituting critical infrastructure, listed in the list referred to in Article 5b(7)(1) of the Act of 26 April 2007 on crisis management, may provide support in handling incidents.

3. Under section 5-7, the tasks incumbent on CSIRT MON, CSIRT NASK i CSIRT GOV include:

1) monitoring of cyber threats and incidents at national level;
2) risk assessment of disclosed cyber threats and incidents, including conducting dynamic risk analysis;
3) communicating information on incidents and risks to the national cyber-security stakeholders;
4) notifications on identified cyber threats;
5) responding to reported incidents;
6) classifying incidents, including major incidents and significant incidents, as critical incidents and

coordinating the handling of critical incidents;

7) reclassifying major incidents and significant incidents;

8) submitting to the competent CSIRT MON, CSIRT NASK or CSIRT GOV technical information regarding the incident, the co-ordination of which requires co-operation of CSIRT;

9) conducting, in justified cases, examination of an IT device or software in order to identify vulnerabilities, the use of which may threaten, in particular, the integrity, confidentiality, accountability, authenticity or availability of the processed data, which may affect public security or a significant interest of state security, and submitting proposals on recommendations to the entities of the national cyber security system on the use of IT devices or software, in particular as regards the impact on public security or a significant interest of state security, hereinafter referred to as 'recommendations on the use of IT devices or software';

10) cooperating with sector cyber security teams in coordinating the handling of major incidents, including those involving two or more Member States of the European Union, and critical incidents and in sharing information to counter cyber security threats;

11) forwarding to and receiving from other states, including European Union Member States, information on major and significant incidents concerning two or more Member States, as well as forwarding to the Single Point of Contact notification of a major and significant incident concerning two or more European Union Member States;

12) submission, by 30 May each year, to the Single Point of Contact of a list of serious incidents reported in the previous calendar year by operators of key services, affecting continuity of provision of key services by them in the Republic of Poland and continuity of provision of key services by them in the Member States of the European Union, as well as a list of significant incidents reported in the previous calendar year by digital service providers, including those concerning two or more Member States of the European Union;

13) joint development and submission to the minister competent for informatisation of the part of the Report on threats to national security, referred to in Article 5a(1) of the Act of 26 April 2007 on crisis management, concerning cyber security;

14) provision of analytical and research and development facility, which, in particular:

   a) conducts advanced malware and vulnerability analyses,

   b) monitors cyber-security threat indicators,

   c) develops tools and methods to detect and combat cyber threats,

   d) carries out analyses and develops standards, recommendations, and good practices in the area of cyber security.

   e) supports the National Cyber Security System actors in capacity building in the area of cyber security,

   f) conducts awareness-building activities in the area of cyber security,

   g) cooperates on educational solutions in the area of cyber security. consisting of:

15) providing notifications and information referred to in Article 11(1)(4), Article 13(1), Article 18(1)(4), Article 20, Article 22(1)(2), Article 24 and Article 30(1), as well as provision and operation of means of communication allowing for those notifications;

16) participation in the CSIRT Network consisting of representatives of CSIRTs of the Member States of the European Union, a CSIRT for the institutions of the European Union, the European Commission and the European Union Agency for Network and Information Security (ENISA).

4. The CSIRT MON, CSIRT NASK and CSIRT GOV shall jointly develop the main elements of the

procedures to be followed in the event of an incident, the coordination of the handling of which requires the cooperation of CSIRTs, and shall determine in cooperation with the sectoral cyber security teams the manner of cooperation with these teams, including the manner of coordination of the handling of the incident.

5. CSIRT MON shall coordinate the handling of the incidents reported by

1) entities subordinate to the Minister of National Defence or supervised by him, including entities whose data communication systems or networks are covered by the uniform list of objects, installations, devices and services comprising critical infrastructure referred to in Article 5b(7)(1)of the act of 26 April 2007 on crisis management;

2) entrepreneurs of special economic and defence importance with reference to which the organising and supervising body for the execution of tasks for national defence as provided in Article 5(3) of the act of 23 August 2001 on the organisation of tasks for national defence performed by entrepreneurs (Journal of Laws No. 1320 and of 2002 No. 1571) where the competent role is that of the Minister of National Defence.

6. CSIRT NASK shall

1) coordinate the handling of the incidents reported by:

   a) units of the public finance sector referred to in Article 9(2-6) (11-12) of the Act of 27 August 2009 on public finance;

   b) units subordinate to government administration bodies or supervised by them, except for the units referred to in section 7(2);

   c) research institutes;

   d) Office of Technical Inspection;

   e) Polish Air Navigation Services Agency;

   f) Polish Accreditation Centre;

   g) National Fund for Environmental Protection and Water Management and provincial funds for environmental protection and water management;

   h) commercial law companies performing public utility tasks as provided in Article 1(2) of the Act of 20 December 1996 on municipal management;

   i) providers of digital services, with the exception of those listed in section 5(7);

   j) operators of digital services, with the exception of those listed in sections 5 and 7;

   k) other entities than those listed in points (a-j) and sections 5 and 7;

   l) natural persons;

2) setting up and providing tools for voluntary cooperation and exchange of information on cyber threats and incidents;

3) provision of a telephone hotline or a website service for reporting and investigating the distribution, dissemination or transmission of child pornography by means of information and communication technology, as referred to in Directive 2011/92/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse, sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA (OJ EU L 335 of 17/12/2011, p. 1).

7. CSIRT MON shall coordinate the handling of the incidents reported by:

1) units of the public finance sector referred to in Article 9(1)(8-9) of the Act of 2009 August 5 on public finance, except those referred to in sections 5 and 6;

2) units subordinate to the Prime Minister or under his supervision;

3) Narodowy Bank Polski (National Bank of Poland);

4) Bank Gospodarstwa Krajowego [National Economy Bank);

5) entities other than those listed in items 1-4 and section 5, whose ICT systems or networks are covered by the uniform list of facilities, installations, equipment and services constituting critical infrastructure referred to in Article 5b(7)(1) of the Act of 26 April 2007 on crisis management;

6) entities referred to in section 6, if the incident regards IT systems or networks covered by the uniform list of critical infrastructure facilities, installations, devices and services, referred to in Article 5b(7)(1)of the act of 1 April 26 on crisis management;

8. CSIRT MON, CSIRT NASK or CSIRT GOV, which received the incident report, and is not competent to coordinate its handling, shall immediately forward this report to the competent CSIRT together with the received information.

9. Operations of CSIRT NASK are financed by subjective grant from the part of state budget at the disposal of which a competent minister for IT matters is responsible.

10. CSIRT MON, CSIRT NASK and CSIRT GOV may, under an agreement, entrust to each other the performance of tasks with respect to some types of entities referred to in sections 5-7. The CSIRT that entrusted the performance of tasks shall inform entities for which the CSIRT was changed of the conclusion of the agreement.

11. The announcement on the conclusion of the agreement referred to in section 10 shall be published in the official journal of the Minister of National Defence, the Minister of Digitalisation or the Internal Security Agency, respectively. The announcement shall include information on

1) the address of the website on which the content of the Memorandum of Understanding together with its Annexes, constituting its integral part, shall be posted;

2) the date from which the agreement will enter into force.

Article 27.

1. The CSIRT GOV shall be competent with regard to incidents related to terrorist events referred to in Article 2.7 of the Act of 10 June 2016 on anti-terrorist activities (Journal of Laws of 2018 items 452, 650 and 730).

2. The CSIRT GOV shall be competent with regard to incidents related to terrorist events referred to in Article 5(1) (2a) of the Act of 9 June 2006 on anti-terrorist activities (Journal of Laws of 2017 items 1978 and 2405 and 2018 items 650 and 1544).

3. In case it is stated that an incident, which is coordinated by the relevant CSIRT MON, CSIRT NASK or CSIRT GOV, is related to events referred to in section 1 or 2, the coordination of incident handling shall be assumed by the relevant CSIRT MON or CSIRT GOV.

Article 28.

1. The competent CSIRT MON, CSIRT NASK or CSIRT GOV shall, based on a notification of a major incident made by the operator of a key service, inform the other Member States of the European Union affected by this incident through the Single Point of Contact.

2. The competent CSIRT MON, CSIRT NASK or CSIRT GOV shall, if circumstances allow, provide the key service operator reporting a serious incident with information on actions taken after the reporting of this incident, which could help to handle it.

3. The relevant CSIRT MON, CSIRT NASK or CSIRT GOV may request the Single Contact Point to forward the notification of a serious incident, referred to in section 1, to the Single Contact Points in other Member States of the European Union affected by this incident.

Article 29.

CSIRT MON, CSIRT NASK or CSIRT GOV shall inform the other Member States of the European Union through the points of single contact in cases where two or more Member States of the European Union are affected by a major incident.

Article 30.

1. Entities other than key service operators and digital service providers, including individuals, may report an incident to the NASK CSIRT. The report should include:

1) name of the entity or information system, in which the incident occurred;

2) description of the incident;

3) other relevant information.

2. Incident reports from key service operators and digital service providers shall be given priority over the reports referred to in section 1.

3. The submissions referred to in section 1 may be processed, if this does not constitute disproportionate or excessive burden for the CSIRT NASK.

4. The entity, referred to in section 1, shall mark in the report information constituting legally protected secrets, including business secrets.

Article 31.

1. The CSIRT MON, CSIRT NASK and CSIRT GOV shall define the manner of making notifications and submitting information in electronic form, referred to in Article 11(1)(4), Article 13(1), Article 18(1)(4), Article 20, Article 22(1)(2), Article 24 and Article 30(1), as well as define the manner of submitting reports and information by other means of communication - in the event of impossibility of making notifications or submitting them in electronic form.

2. The report containing the information referred to in section 1 is published by the CSIRT MON, CSIRT NASK and CSIRT GOV on the subject page of the Public Information Bulletin of the Minister of National Defence, the Research and Academic Computer Network - National Research Institute or the Internal Security Agency, respectively.

Article 32.

1. CSIRT MON, CSIRT NASK and CSIRT GOV may perform necessary technical activities related to threat analysis, coordination of handling of major incident, significant incident and critical incident.

2. In the course of coordination of handling of a major incident, a significant incident or a critical incident, CSIRT MON, CSIRT NASK or CSIRT GOV may request the authority competent for cyber security to call upon the operator of a key service or the provider of a digital service to remove vulnerabilities that led or could lead to a major incident, a significant incident or a critical incident within a specified period.

3. CSIRT MON, CSIRT NASK or CSIRT GOV may request directly the key service operator to provide technical information related to a serious or critical incident, which will be necessary to analyse or coordinate handling of such incident.

4. CSIRT MON, CSIRT NASK, CSIRT GOV or sector cyber security teams on the basis of information referred to in Article 13, section 1, subsections 3 and 5, obtained from the key service operator, digital service provider or public entity referred to in Article 4, subsections 7-15, may provide them with information on vulnerabilities and the manner of removing vulnerabilities in used technologies.

Article 33.

1. CSIRT MON, CSIRT NASK or CSIRT GOV may test an IT device or software in order to identify a vulnerability, the exploitation of which may threaten, in particular, the integrity, confidentiality, accountability, authenticity or availability of the processed data, which may affect public security or an essential interest of state security.

2. The CSIRT MON, CSIRT NASK or CSIRT GOV, when undertaking the examination of an IT device or software, shall inform the other CSIRTs of the fact of undertaking the examination and the IT device or software to which the examination relates.

3. CSIRT MON, CSIRT NASK or CSIRT GOV in case of identification of vulnerability referred to in section 1, submits a request for recommendation referred to in section 4.

4. After obtaining an opinion of the College, the Plenipotentiary issues, amends or revokes recommendations regarding the use of IT equipment or software, in particular in the scope of impact on public security or essential interest of state security.

5. An entity of the national cyber security system may raise objections to the Plenipotentiary with respect to recommendations concerning the use of IT devices or software, due to their negative impact on the provided service or performed public task, no later than within 7 days of receiving the recommendation.

6. The Plenipotentiary shall respond to the reservations received under the procedure of section 5 without delay, but no later than within 14 days of the receipt thereof and uphold the recommendations concerning the use of IT devices or software or issue amended recommendations.

7. The entity of the national cyber security system shall inform the Plenipotentiary, upon the Plenipotentiary's request, of the manner and scope of taking into account the recommendations concerning the use of IT devices or software.

8. Failure to consider recommendations concerning the use of IT devices or software constitutes grounds for the Plenipotentiary to apply to the body supervising the entity referred to in section 7, with information on their disregard.

Article 34.

1. CSIRT MON, CSIRT NASK, CSIRT GOV and sectoral cyber security teams and cyber security service providers cooperate with law enforcement and justice authorities and special services in the implementation of their statutory tasks.

2. CSIRT MON, CSIRT NASK and CSIRT GOV, coordinating the handling of an incident that led to a personal data protection breach, shall cooperate with the authority competent for personal data protection.

Article 35.

1. CSIRT MON, CSIRT NASK and CSIRT GOV shall communicate to each other information about a critical incident and inform the Government Security Centre.

2. The information referred to in section 1 shall include:

1) preliminary analysis of potential consequences of the incident, considering in particular:

a) number of users affected by the incident, in particular if it disrupts the provision of a key service;

b) the time of occurrence and detection of the incident and its duration;

c) the geographical scope of the area that is affected by the incident,

2) recommendation on the convening of the Government Crisis Management Team referred to in Article 8(1) of the Act of 26 April 2007 on crisis management.

3. The information referred to in section 1 may contain a request to convene a Team for Critical Incidents, hereinafter referred to as the 'Team'.

4. In case of obtaining information about threats to cyber security, CSIRT MON, CSIRT NASK and CSIRT GOV may inform each other and inform the Government Centre for Security about these threats. Provisions of sections 2 and 3 shall apply mutatis mutandis.

5. CSIRT MON, CSIRT NASK and CSIRT GOV may publish, to the extent necessary, information on vulnerabilities, critical incidents and threats to cyber security on the subject page of the Public Information Bulletin of the Minister of Defence, the Research and Academic Computer Network - National Research Institute or the Internal Security Agency, respectively, provided that the provision of the information will contribute to increasing cyber security of the information systems used by citizens and entrepreneurs or ensuring secure use of those systems. The information published shall not violate provisions on the protection of classified information and other legally protected secrets or provisions on the protection of personal data.

Article 36.

1. The team is an auxiliary body in matters of handling critical incidents notified to CSIRT MON, CSIRT NASK or CSIRT GOV and coordinating activities undertaken by CSIRT MON, CSIRT NASK, CSIRT GOV and Government Centre for Security.

2. The Team consists of representatives of CSIRT MON, CSIRT NASK, Head of the Internal Security Agency performing tasks within CSIRT GOV and the Government Centre for Security.

3. The Head of the Government Centre for Security chairs the works of the Team.

4. Team operations are supported by the Government Centre for Security.

5. To participate in the works of the Team, in an advisory capacity, the members of the Team may invite representatives of the authorities competent in matters of cyber security or their subordinate units or supervised by them, law enforcement authorities, judiciary or special services.

6. In the case referred to in Article 35(3), or at the request of a member of the Team or on his own initiative after having obtained the information referred to in Article 35(1), the Director of the Government Centre for Security shall immediately notify the members of the Team of the date and place of the Team's meeting Team meetings may be conducted by means of electronic communication.

7. During the meeting, the Team:

1) unanimously designates the CSIRT coordinating the handling of the incident covered by the information referred to in Article 35(1);

2) defines roles of other CSIRTs and the Government Centre for Security in handling the incident referred to in Article 35(1);

3) defines the way of exchanging technical information regarding a critical incident handled jointly by the CSIRT MON, the CSIRT NASK or the Head of the Internal Security Agency who performs tasks within the CSIRT GOV;

4) decides on a request of the Director of the Government Centre for Security to the Prime Minister to convene a Government Crisis Management Team

5) in the event of a critical incident that may result in a threat of a terrorist incident involving ICT systems of public administration bodies or ICT systems that are part of critical infrastructure, as referred to in Article 15(2) of the Anti-Terrorist Activities Act of 10 June 2016, prepares, with regard to such incident, information and conclusions for the minister in charge of internal affairs and the Head of the Internal Security Agency

Chapter 7

Rules of providing access to information and processing personal data

Article 37.

1. The provision of information on cyber security vulnerabilities, incidents and threats and the risk of incidents shall not be subject to the Act of 6 September 2001 on access to public information (Journal of Laws of 2018 item 1330).

2. The relevant CSIRT MON, CSIRT NASK or CSIRT GOV may, after consultation with the notifying Key Service Operator, publish information on serious incidents on the subject page of the Public Information Bulletin of the Minister of National Defence, the Research and Academic Computer Network - National Research Institute or the Internal Security Agency, respectively, when it is necessary to prevent the occurrence of an incident or to ensure incident handling.

3. The competent CSIRT MON, CSIRT NASK or CSIRT GOV may, after consultation with the digital service provider reporting a major incident, publish information on major incidents on the subject page of the Public Information Bulletin of the Minister of National Defence or the Research and Academic Computer Network - National Research Institute or the Internal Security Agency, respectively, or apply to the authority competent for cyber security of the digital service provider to oblige the digital service provider to make this information public when it is necessary to prevent the occurrence of an incident or to ensure the handling of an incident, or when for other reasons the disclosure of the incident is in the public interest.

4. The publication of the information referred to in section 2 and 3 shall not violate the provisions on the protection of classified information and other legally protected secrets or the provisions on the protection of personal data.

Article 38.

Information processed under the Act shall not be made available if its disclosure would undermine the protection of the public interest as regards security or public order, as well as adversely affect the conduct of preparatory proceedings in respect of criminal offences, their detection and prosecution.

Article 39.

1. To perform the tasks referred to in Article 26(3)(1-11) (14-15) and sections 5-8 and in Article 44(1-3), CSIRT MON, CSIRT NASK, CSIRT GOV and sectoral cyber security teams process the data collected in relation to cyber security incidents and threats, including personal data, including the data defined in Article 9(1) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ EU L 119 of 04/05/2016, p. 1), hereinafter ‘Regulation 2016/679’, to the extent and for the purpose necessary to perform those tasks.

2. CSIRT MON, CSIRT NASK and sectoral cyber security teams, when processing personal data as defined in Article 9(1) of Regulation 2016/679, shall conduct risk analysis, apply malware protection measures and access control mechanisms, and develop procedures for secure exchange of information.

3. CSIRT MON, CSIRT NASK, CSIRT GOV and sectoral cyber security teams process personal data acquired in connection with cyber security incidents and threats:

1) concerning users of information systems and users of telecommunications terminal equipment;

2) concerning telecommunication terminal equipment as provided in Article 2.43 of the Act of 16 July 2004 - Telecommunications Law;

3) collected by key service providers and digital service providers in connection with the provision of services;

4) collected by public entities in connection with the performance of public tasks; concerning entities reporting an incident in accordance with Article 30 (1).

4. To perform the tasks set out in the Act, the Minister competent for IT, the Director of the Government Security Centre, the Plenipotentiary and the authorities in charge of cyber security shall process personal data collected in connection with cyber security incidents and threats:

1) collected by key service providers and digital service providers in connection with the provision of services;

2) collected by public bodies in connection with the performance of public tasks;

3) concerning those who report an incident in accordance with Article 30(1).

5. The data referred to in sections 3 and 4 shall be deleted or anonymised by the CSIRT of MON, the CSIRT of NASK and the sector cyber security team immediately after ascertaining that they are not necessary for the performance of the tasks referred to in Article 26(3)(1-11)(14-15) and sections 5-8 and Article 44(1-3).

6. The data referred to in sections 3 and 4, which are necessary for the performance of the tasks referred to in Article 26(3)(1-11)(14-15) and sections 5-8 and Article 44(1-3), shall be deleted or anonymised by the CSIRT of MON, the CSIRT of NASK and the sector cyber security team within 5 years of the completion of the handling of the incident to which they relate.

7. To execute tasks set forth in the Act, CSIRT MON, CSIRT NASK, CSIRT GOV and sector cyber security teams may provide each other with data referred to in section 3, to the extent necessary to execute these tasks and cooperate with the authority competent for personal data protection.

8. The processing of the data referred to in section 3 by the CSIRT MON, CSIRT NASK and sectoral cyber-security teams does not require the fulfilment of the obligations under Article 15, Article 16, Article 18(1)(a) and (d) and Article 19, second sentence, of Regulation 2016/679 if this would prevent the fulfilment of the tasks of the CSIRT NASK, CSIRT MON and sectoral cyber-security teams referred to in Art. 26(3)(1)-(11), (14) and (15) and (5)-(8) and Article 44(1)-(3), and is possible when CSIRT MON, CSIRT NASK and sectoral cyber security teams conduct risk analysis, apply protection measures against malware, apply access control mechanisms and develop procedures for secure exchange of information.

9. CSIRT MON, CSIRT NASK and the sectoral cyber security teams shall publish on their websites:

1) the contact details of the controller and, where applicable, the contact details of the Data Protection Officer;

2) the purposes of the processing and the legal basis for the processing;

3) categories of personal data processed;

4) information on the recipients of the personal data;

5) information on the period for which the personal data will be stored;

6) information on the limitations of the data subjects' obligations and rights;

7) information about the right to lodge a complaint with the authority competent for the protection of personal data;

8) the source of the personal data.

Article 40.

1. CSIRT MON, CSIRT NASK, CSIRT GOV, sectoral cyber security teams and the minister in charge of informatisation shall process information constituting legally protected secrets, including those constituting company secrets, when it is necessary for the performance of tasks referred to in the Act.

2. The CSIRT MON, CSIRT NASK, CSIRT GOV and sectoral cyber-security teams provide the information referred to in section 1 to law enforcement authorities in connection with an incident that constitutes an offence.

3. CSIRT MON, CSIRT NASK, CSIRT GOV and sector cyber security teams are obliged to keep secret the information, including information constituting legally protected secrets, obtained in relation to the implementation of tasks referred to in the Act.

Chapter 8

Authorities competent for cyber security matters

Article 41.

The authorities competent in matters of cyber security are:

1) for the energy sector - the minister competent for energy;

2) for the transport sector excluding the water transport subsector - the minister competent for transport;

3) for the water transport subsector - the minister competent for maritime economy and the minister competent for inland waterway transport

4) for the banking sector and financial market infrastructure - the Polish Financial Supervision Authority;

5) for the health care sector excluding the entities referred to in Article 26(5) - the minister competent for health matters;

6) for the health sector including the entities referred to in Article 26(5) - the Minister of National Defence;

7) for the drinking water supply and distribution sector - the minister competent for water management;

8) for the sector of digital infrastructure excluding the entities referred to in Article 26(5) - the minister competent for informatisation;

9) for the digital infrastructure sector including the entities referred to in Article 26(5) - the Minister of National Defence;

10) for the sector of digital infrastructure excluding the entities referred to in Article 26(5) - the minister competent for informatisation;

11) for digital service providers including the entities referred to in Article 26(5) - the Minister of National Defence;

Article 42.

1. The authority competent for cyber security shall:

1) conduct an ongoing analysis of entities in a given sector or subsector for recognition as a key service operator or failure to meet the conditions qualifying an entity as a key service operator;

2) issue a decision to recognise an entity as a key service operator or a decision stating the expiry of a decision to recognise an entity as a key service operator;

3) immediately after issuing a decision to recognise an entity as a key service operator or a decision stating the expiry of a decision to recognise an entity as a key service operator, submits applications to the minister competent for IT for entering the entity into the list of key service operators or deleting it from the list;

4) submit applications for changing data in the register of key service operators, not later than within 6 months after the change of the data;

5) prepare in cooperation with CSIRT NASK, CSIRT GOV, CSIRT MON and sectoral cyber security teams, recommendations for actions to strengthen cyber security, including sectoral guidelines on incident reporting

6) monitor the application of the Act by key service operators and digital service providers;

7) at the request of the CSIRT NASK, the CSIRT GOV or the CSIRT MON, summon key service operators or digital service providers to remediate, within a specified period of time, vulnerabilities that led or may have led to a serious, significant or critical incident;

8) maintain supervision of the key service operators and digital service providers;

9) may cooperate with the competent authorities of the Member States of the European Union via the Points of Single Contact;

10) process information, including personal data, related to the provided key services and digital services as well as key service operators or digital service providers to the extent necessary to perform the tasks under the Act;

11) participate in cyber security exercises organised in the Republic of Poland or in the European Union.

2. Where a legal person or a non-corporate organisational unit providing digital services does not have its registered office or management in the Republic of Poland or has not appointed a representative in the territory of the Republic of Poland, but its information systems are located in the Republic of Poland or does not meet the requirements set out in Implementing Regulation 2018/151, the authority competent for cyber security for digital service providers may provide information and request the actions referred to in Article 53(2), to the competent authority in another Member State of the European Union on the territory of which it has its registered office or management or its representative has been appointed.

3. The authority competent for cyber security may entrust, on its behalf, the execution of certain tasks referred to in section 1 to entities subordinate to or supervised by that authority.

4. The delegation shall be made based on an agreement of the authority competent for cyber security with the entities referred to in section 3.

5. The agreement referred to in section 4 shall set forth the rules for exercising control by the authority competent for cyber security over the proper performance of the entrusted tasks.

6. The notification on the conclusion of the agreement shall be published in the official journal of the authority competent for cyber security. The announcement shall include information on

1) the address of the website on which the content of the Memorandum of Understanding together with its Annexes, constituting its integral part, shall be posted;

2) the date from which the agreement will enter into force.

7. The competent cyber security authorities and the Single Point of Contact shall cooperate with law enforcement authorities and the competent authority for the protection of personal data where appropriate.

8. Recommendations for actions to strengthen cyber security, including sectoral guidelines for incident reporting referred to in section 1(5), shall be prepared taking into account in particular the Polish Standards transposing European standards, common technical specifications, understood as technical specifications in the field of ICT products defined in accordance with Article 13 and Article 14 of the Regulation (EU) No. 1025/2012 of the European Parliament and of the Council of 25 October 2012 on European Standardization, amending Council Directives 89/686/EEC and 93/15/EEC and Directives 94/9/EC, 94/25/EC, 95/16/EC, 97/23/EC, 98/34/EC, 2004/22/EC, 2007/23/EC, 2009/23/EC and 2009/105/EC of the European Parliament and of the Council, and repealing Council Decision 87/95/EEC and Decision No. 1673/2006/EC of the European Parliament and of the Council (OJ EU L 316 of 14/11/2012, p. 12) and the guidelines of the European Commission and the European Network and Information Security Agency (ENISA) in this regard.

Article 43.

1. The competent authority for cyber security may, without initiating proceedings for the recognition of an entity as a key service operator, request information from the entity referred to in Annex 1 to the Act, which will enable a preliminary assessment of whether the entity meets the conditions for recognition as a key service operator.

2. The authority competent for cyber security may, without initiating an audit, request information from the operator of a key service that will enable it to determine the need for an audit, and may, without initiating an investigation, request information from the operator of a key service that will enable a preliminary assessment of whether the entity no longer meets the conditions for recognition as a key service operator.

3. The authority competent for cyber security, when requesting the entity referred to in Annex 1 to the Act, or the operator of a key service, shall indicate a time limit for providing information. The time limit set may not be shorter than 14 days from the date of receipt of the request by the operator or operator of the key service.

4. The entity referred to in Annex 1 to the Act or the operator of a key service to which the authority competent for cyber security has addressed the request may provide information on the matter to which the request relates or inform about the refusal to provide information.

5. The request for information and the failure to provide information shall not affect the possibility of initiating administrative proceedings or control.

6. The information provided by an entity or a key service operator, referred to in sections 1 and 2, may constitute evidence in the initiated administrative proceedings or control. Failure to provide the information shall not affect the procedural situation of the party or the controlled person or the administrative proceedings or control initiated.

Article 44.

1. The authority competent for cyber security may establish, pursuant to separate provisions, a sectoral cyber security team for a given sector or sub-sector listed in Annex 1 to the Act, responsible in particular for:

1) receiving notifications of major incidents and support in handling these incidents;

2) supporting the key service operators in carrying out the obligations laid down in Article 8, Article 9, Article 10(1)-(3), Article 11(1)-(3), Article 12 and Article 13;

3) analysing serious incidents, searching for links between incidents, and developing conclusions from incident handling;

4) cooperation with the competent CSIRT MON, CSIRT NASK and CSIRT GOV in the coordination of serious incident handling.

2. The Sector Cyber Security Team may transmit to and receive from other countries, including European Union Member States, information on serious incidents, including those involving two or more European Union Member States.

3. The sectoral cyber-security team may receive reports of a major incident from another Member State of the European Union involving two or more Member States of the European Union. The Sector Cyber Security Team shall forward these reports to the appropriate CSIRT MON, CSIRT NASK or CSIRT GOV and the Single Point of Contact.

4. In the event of the establishment of a sectoral cyber security team, the competent authority for cyber security shall inform the operators of key services in the sector concerned and the CSIRT MON, CSIRT NASK and CSIRT GOV of the establishment of the team and the scope of the tasks to be performed.

Chapter 9

Tasks of a minister competent for informatisation

Article 45.

1. The Minister competent for informatisation shall be responsible for:

1) monitoring the implementation of the Cyber Security Strategy of the Republic of Poland, hereinafter referred to as the ‘Strategy’, and implementing action plans for its implementation;

2) recommending areas of cooperation with the private sector in order to increase the cyber security of the Republic of Poland;

3) preparing annual reports on:

   a) major incidents reported by key service providers affecting the continuity of key services they provide in the Republic of Poland and the continuity of key services provided in the Member States of the European Union:

   b) major incidents reported by digital service providers, including incidents concerning two or more European Union Member States;

4) conducting information activities on good practices, educational programmes, campaigns and training to increase knowledge and build awareness of cyber security, including safe use of the Internet by different categories of users;

5) collecting information on serious incidents involving or reported by another European Union Member State;

6) sharing information and good practices related to the reporting of serious incidents by key service operators and significant incidents by digital service providers, obtained from the Cooperation

Group, including:

a) procedures to be followed for incident management,

b) procedures to be followed for risk management,

c) classification of information, risks and incidents.

2. Cooperation Group means the group referred to in Commission Implementing Decision EU 2017/179 of 1 February 2017 laying down the procedures necessary for the operation of the Cooperation Group in accordance with Article 11(5) of Directive (EU) 2016/1148 of the European Parliament and of the Council on measures for a high common level of security of networks and information systems within the Union (OJ EU L 28 of 02/02/2017, p. 73).

Article 46.

1. The minister competent for informatisation shall ensure the development or maintenance of an ICT system supporting:

1) cooperation of entities that are part of the national cyber security system;

2) generating and forwarding recommendations on activities increasing the level of cyber security;

3) incident reporting and handling;

4) risk assessment at the national level;

5) alerting on cyber security threats;

2. CSIRT MON, CSIRT NASK, CSIRT GOV, sectoral cyber security teams and the President of the Office of Electronic Communications may use the ICT system on the basis of an agreement concluded with the minister in charge of informatisation.

3. The agreement defines the scope and conditions of using the ICT system.

Article 47.

1. The minister competent for informatisation may perform the tasks referred to in Article 45(1) and Article 46(1) in accordance with the rules laid down in separate provisions, by means of the units subordinate to or supervised by the minister in charge of information technology.

2. The tasks entrusted to the units referred to in section 1 shall be financed in the form of a purposeful grant from the part of the State budget administered by the minister competent for informatisation.

Article 48.

The minister competent for informatisation shall run the Single Point of Contact, whose tasks shall include:

1) receiving reports of a major or significant incident regarding two or more European Union Member States from Single Points of Contact in other European Union Member States, as well as forwarding these reports to CSIRT MON, CSIRT NASK, CSIRT GOV or sector cyber security team;

2) transmission, at the request of the competent CSIRT MON, CSIRT NASK or CSIRT GOV, of a report of a serious or significant incident concerning two or more Member States of the European Union to single contact points in other Member States of the European Union;

3) ensuring representation of the Republic of Poland in the Cooperation Group

4) ensuring cooperation with the European Commission in cyber security;

5) coordinate the cooperation between the competent authorities in cyber security and the public authorities in the Republic of Poland with the relevant authorities in the European Union Member States;

6) ensuring exchange of information needed by the Cooperation Group and CSIRT Network.

Article 49.

1. A Single Point of Contact provides the Cooperation Group with:

1) information referred to in Article 45(1)(3);

2) good national practices referred to in Article 45(1)(3) regarding reporting incidents;

3) proposals for the Cooperation Group operational programme;

4) good national practices regarding cyber security awareness raising, training, research and development;

5) good practices with regard to identifying key service operators, including those in two or more dependencies on risks and incidents occurring in the European Union Member States.

2. The data provided to the Cooperation Group shall not include information that concerns national security and public order.

3. The Single Point of Contact shall provide the authorities competent for cyber security, the CSIRT MON, the CSIRT NASK, the CSIRT GOV, the sectoral cyber security teams and other public authorities with information from the Cooperation Group on:

1) assessments of the European Union Member States' national cyber security strategies and the effectiveness of CSIRTs, as well as good cyber security practices;

2) activities undertaken with regard to cyber exercises, European education and training programmes, including the activities of the European Union Agency for Network and Information Security (ENISA);

3) strategic guidance on the activities of the CSIRT Network;

4) good practices in the exchange of information related to the reporting in the European Union of serious incidents by key service operators and significant incidents by digital service providers;

5) good practices in European Union Member States regarding awareness raising, training, research and development in the field of cyber security;

6) good practices in the identification of key service operators by European Union Member States, including those with cross-border dependencies, risks and incidents.

Article 50.

A Single Point of Contact provides the European Commission the following:

1) immediate information on:

   a) the designated competent authorities for cyber security, the Points of Single Contact, their tasks and subsequent developments,

   b) the provisions on fines concerning the national cyber security system;

2) every 2 years, information making it possible to assess the implementation of Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 on measures for a high common level of security of network and information systems within the Union (OJ EU L 194, 19/07/2016, p. 1), including in particular:

a) measures to identify key service operators;

b) the list of key service;

c) number of identified key service operators in each sector referred to in Annex 1 to the Act, and an indication of their significance in relation to that sector;

d) the thresholds of significance of the disruptive effect on the key service provided which are taken into account when qualifying entities as key service operators;

3) information about the tasks of CSIRT MON, CSIRT NASK and CSIRT GOV, including the main elements of procedures to be followed in the event of an incident.

Chapter 10

Obligations of the Minister of National Defence

Article 51.

The Minister of National Defence shall be responsible for:

1) cooperation of the Polish Armed Forces with the competent authorities of the North Atlantic Treaty Organisation, the European Union and international organisations in the area of national defence in cyber security

2) ensuring the ability of the Polish Armed Forces in the national, allied and coalition configuration to conduct military operations in the event of a cyber security threat necessitating defensive measures;

3) developing the skills of the Armed Forces of the Republic of Poland in ensuring cyber security through organisation of specialised training tasks;

4) acquisition and development of tools for building cyber security capability in the Polish Armed Forces;

5) managing activities related to handling incidents during martial law;

6) assessing the impact of incidents on the state defence system;

7) assessing cyber security threats during martial law and submitting proposals on defence measures to the relevant authorities;

8) coordinating, in cooperation with the minister competent for internal affairs and the minister competent for informatisation, the implementation of the tasks of governmental administration bodies and local government units during martial law concerning defence actions in the event of a cyber security threat.

Article 52.

The Minister of National Defence runs the National Contact Point for cooperation with the North Atlantic Treaty Organisation, whose tasks include:

1) ensuring cooperation in the area of national defence with the competent bodies of the North Atlantic Treaty Organisation in the field of cyber security;

2) coordinating activities in the area of strengthening defence capabilities in the event of a cyber security threat;

3) ensuring cooperation between national and allied armed forces in ensuring cyber security;

4) developing information sharing systems on cyber security threats in the area of national defence;

5) contributing to the North Atlantic Treaty Organisation's objectives in the area of cyber security and cryptology.

Chapter 11

Supervision and control of key service operators, digital service providers and cyber security service providers in the area of cyber security

Article 53.

1. The supervision on application of the provisions of the Act shall be exercised by:

1) the minister competent for informatisation concerning compliance by entities providing cyber security services with the requirements referred to in Article 14(2);

2) the authorities competent for matters of cyber security concerning:

   a) the fulfilment by key service providers of their obligations under the Act to counter cyber security threats and to report major incidents,

   b) compliance by digital service providers with the security requirements for the digital services they provide as set out in Implementing Regulation 2018/151 and the performance of the obligations under the Act on the reporting of major incidents.

2. As part of the supervision referred to in section 1:

3) the authority competent for cyber security or the minister competent for informatisation shall carry out audits within the scope referred to in section 1;

4) the authority competent for cyber security shall impose fines on key service operators and digital service providers.

3. With respect to a digital service provider, the actions referred to in section 2 shall be taken upon obtaining evidence that the digital service provider fails to comply with the requirements set out in Executive Order 2018/151 or fails to comply with the obligations under the Act regarding the reporting of material incidents.

Article 54.

1. The provisions of Chapter 5 of the Act of 6 March 2018 shall apply to audits whose scope is defined in Article 53(1)(1). - Entrepreneurs' Law.

2. For the audit, the scope of which is defined in Article 53(1) (2), carried out with regard to

1) entrepreneurial entities, the provisions of Chapter 5 of the Act of 6 March 2018 - Entrepreneurs' Law, shall apply;

2) non-entrepreneurial entities, the provisions of the Act of 15 July 2011 on governmental administration audits, which define the method and rules of audits, shall apply;

Article 55.

A person conducting audit with respect to entrepreneurial entities has the right to:

1) freely enter and move around the premises of the audited entity without the obligation to obtain a pass;

2) access to documents related to the operations of the audited entity, collection against a receipt and securing of documents related to the scope of control, with observance of the provisions on the legally protected secrecy;

3) make copies, copies or extracts of documents as well as statements or calculations necessary for the audit, and if necessary, requesting them to be made;

4) process personal data to the extent necessary for the realization of the audit objective;

5) request to provide oral or written explanations in matters related to the scope of audit;

6) carry out audit of devices, carriers and information systems.

Article 56.

1. The audited intrapreneurial entities shall provide the auditor with the conditions necessary to carry out the audit in an efficient manner, in particular by ensuring immediate presentation of the documents requested, providing verbal and written explanations on the issues covered by the audit in a timely manner, providing access to the necessary technical facilities as well as making copies or printouts of the documents and information collected on the media, in equipment or in their own information systems.

2. The audited entity confirms the conformity of the copies or printouts referred to in section 1 with the originals. In the event of a refusal to provide confirmation of conformity with the originals, they shall be confirmed by the person conducting the inspection activities, with a note to this effect in the audit protocol.

Article 57.

The auditor with respect to entrepreneurial entities establishes the facts based on the evidence collected in the course of audit, in particular documents, objects, inspection as well as oral or written explanations and statements.

Article 58.

1. The auditor with respect to entrepreneurial entities presents the course of the audit in the audit report.

2. The audit report shall include:

1) the indication of the name and address of the audited entity;

2) the name and surname of the representative of the audited entity and the name of the body representing that entity;

3) name and surname, position and authorisation number of the auditor;

4) the date of beginning and end of the audit;

5) description of the subject and scope of control;

6) description of the facts established in the course of audit as well as other information of significant importance for the conducted audit, including the scope, reasons and results of identified irregularities;

7) attachment details.

3. The audit report is signed by the person conducting the audit and the representative of the audited entity.

4. Prior to signing the report, the audited entity may, within 7 days of the date of its presentation for signature, file written reservations to the report.

5. In the event of raising objections, the auditor shall analyse the objections and, if necessary, undertake additional audits, and in the event of determining that the objections are justified, amend or supplement

the relevant part of the report as an annex thereto.

6. If the reservations are not accepted in whole or in part, the auditor shall inform the audited entity in writing.

7. The auditor makes a note on the refusal to sign the audit, including the date of such refusal.

8. A hard copy of the report is drawn up in two copies, one of which is left for the audited entity, and in the case of an electronic report, it is delivered to the audited entity electronically.

Article 59.

1. If, based on the information gathered in the audit report, the authority competent for cyber security or the minister competent for informatisation considers that there may have been a violation of the provisions of the Act by the audited entity, it shall provide post-audit recommendations for the removal of irregularities.

2. The post-audit recommendations do not provide for the right to appeal.

3. The audited entity shall, within the prescribed time limit, inform the authority competent for cyber security or the minister competent for informatisation on the manner in which the recommendations have been implemented.

Chapter 12

Plenipotentiary and College

Article 60.

The coordination of activities and implementation of the government's policy on ensuring cyber security in the Republic of Poland is entrusted to the Plenipotentiary.

Article 61.

1. Plenipotentiary is appointed and dismissed by the Prime Minister.

2. The Plenipotentiary is responsible to the Council of Ministers.

3. The Plenipotentiary is either a Secretary of State or an Undersecretary of State.

4. The Plenipotentiary's substantive, organisational, legal, technical, office and clerical support is provided by the ministry or other government administration office where the Plenipotentiary has been appointed.

Article 62.

1. In coordinating activities and implementing the government's policy on ensuring cyber security, the Plenipotentiary's tasks include:

1) analysis and assessment of the functioning of the national cyber security system on the basis of aggregated data and indicators developed with the participation of public administration bodies, bodies competent for cyber security, CSIRT MON, CSIRT NASK and CSIRT GOV;

2) supervision of the risk management process of the national cybersecurity system using aggregated data and indicators developed with participation of authorities responsible for cybersecurity, CSIRT MON, CSIRT NASK and CSIRT GOV;

3) providing opinions on government documents, including draft legal acts, which have an impact on

the implementation of tasks in the area of cyber security;

4) disseminating new solutions and initiating activities in the area of ensuring cyber security at the national level;

5) initiating national cyber security exercises;

6) issuing recommendations on the use of IT equipment or software at the request of the CSIRT.

2. The tasks of the Plenipotentiary performed in consultation with the relevant ministers also include:

1) co-operating with other countries, organisations and international institutions on matters related to cyber security;

2) taking action to support scientific research and technology development in the area of cyber security;

3) taking action to raise public awareness of cyber security threats and safe use of the Internet.

Article 63.

1. The Plenipotentiary shall prepare and submit to the Council of Ministers, by 31 March of each year, a report for the previous calendar year containing information on the activities carried out in the field of ensuring cyber security at the national level.

2. The Plenipotentiary may submit to the Council of Ministers conclusions and recommendations on actions that should be taken by the entities of the national cyber security system to ensure cyber security at the national level and counter threats in this regard.

Article 64.

The Council of Ministers shall establish a College as an opinion-giving and advisory body on matters of cyber security and activities of CSIRT MON, CSIRT NASK, CSIRT GOV, sectoral cyber security teams and bodies competent in matters of cyber security.

Article 65.

1. The tasks of the College include expressing opinions on:

1) directions and plans for counteracting cyber threats;

2) performance by the CSIRT MON, CSIRT NASK, Head of the Internal Security Agency performing tasks within the CSIRT GOV, sector cyber security teams and bodies competent in matters of cyber security of the tasks entrusted to them in accordance with the directions and plans for counteracting cyber security threats;

3) cooperation of the bodies conducting or supervising CSIRT MON, CSIRT GOV and CSIRT NASK;

4) cooperation of the entities of CSIRT MON, CSIRT NASK, Head of the Internal Security Agency and the minister - member of the Council of Ministers responsible for coordinating activities of special services, sector cyber security teams and authorities responsible for cyber security;

5) organisation of the exchange of information relevant to cyber security and the international position of the Republic of Poland between government administration bodies;

6) requests of CSIRT MON, CSIRT NASK or CSIRT GOV for recommendations on the use of IT equipment or software.

2. The tasks of the College include the development of recommendations for the Council of Ministers on activities in the field of ensuring cyber security at the national level, referred to in Article 67.

Article 66.

1. The College is composed of:

1) President of the College - Prime Minister;

2) Plenipotentiary;

3) Secretary of the College;

4) members of the College;

   a) minister competent for internal affairs;

   b) minister competent for informatisation;

   c) Minister of National Defence;

   d) minister competent for foreign affairs;

   e) the Head of the Chancellery of the Prime Minister;

   f) the Head of the National Security Bureau, if appointed by the President of the Republic of Poland;

   g) a minister - member of the Council of Ministers responsible for coordinating the activities of special services or a person authorised by them in the rank of Secretary of State or Undersecretary of State, and if the minister - member of the Council of Ministers responsible for coordinating the activities of special services has not been appointed - the Head of the Internal Security Agency.

2. The Prime Minister may authorise the Plenipotentiary to act as the Chairman of the College.

3. The members of the College referred to in section 1(4)(a-e) may be deputised by authorised representatives in the rank of Secretary of State or Undersecretary of State.

4. The meetings of the College are also attended by:

1) the Director of the Government Centre for Security;

2) the Head of the Internal Security Agency or his deputy;

3) the Head of the Military Counterintelligence Service or his deputy

4) he Director of the Research and Academic Computer Network - National Research Institute.

5. The College Chairperson:

1) convenes meetings of the College;

2) may invite the chairpersons of the relevant parliamentary committees, representatives of state bodies, representatives of bodies competent in matters of cyber security and other persons whose participation is necessary due to the subject matter of the meeting to participate in the meetings of the College.

6. The Secretary of the College shall be appointed by the Prime Minister from among the persons fulfilling the requirements laid down in the provisions on the protection of classified information with regard to access to information classified as ‘secret’. The Secretary of the College is dismissed by the Prime Minister.

7. The Secretary of the College organises the work of the College and, in this respect, may request the CSIRT MON, CSIRT GOV, CSIRT NASK, sectoral cyber security teams, bodies competent in cyber security matters and government administration bodies to present information necessary in matters considered by the College.

8. The service of the College is provided by the Ministry or other government administration office that

serves the Plenipotentiary.

9. The Council of Ministers shall define, by way of a regulation, a detailed scope of activities and work procedures of the College, taking into consideration the nature of the tasks of the College and the need to ensure its efficient work.

Article 67.

1. The Prime Minister, in order to coordinate the activities of the government administration in the field of cyber security, may, on the recommendation of the College, issue binding guidelines on ensuring cyber security at the national level and the functioning of the national cyber security system, as well as request information and opinions in this respect from:

1) the minister competent for internal affairs - with regard to activities of the Police, Border Guard and State Protection Service;
2) the Minister of National Defence - with respect to the activities of the CSIRT MON;
3) Head of Internal Security Agency - with respect to CSIRT GOV;
4) Director of the Government Centre for Security - with respect to the tasks performed in accordance with the Act;
5) Director of the Research and Academic Computer Network - National Research Institute - with respect to the operations of the CSIRT NASK;
6) Minister competent for informatization - with respect to the tasks performed in compliance with the Act.

2. The Prime Minister issues binding guidelines for CSIRT MON, CSIRT GOV and CSIRT NASK with respect to critical incident handling, including designation of a CSIRT responsible for handling a critical incident.

Chapter 13

Strategy

Article 68.

The Council of Ministers adopts he Strategy by a Resolution.

Article 69.

1. The Strategy sets out the strategic objectives and the relevant policy and regulatory measures to achieve and maintain a high level of cyber security. The Strategy covers the sectors referred to in Annex 1 to the Act, digital services and public entities referred to in Article 4(7-15).

2. The Strategy shall, in particular, take into account:

1) objectives and priorities in cyber security;
2) entities involved in the implementation and delivery of the Strategy;
3) the means to achieve the objectives of the Strategy;
4) the definition of preparedness, response and recovery measures, including principles of cooperation between the public and private sectors;
5) an approach to risk assessment;
6) Activities relating to cyber security education, information and training programmes;

7) activities relating to cyber security research and development plans.

3. The strategy shall be set for a five-year period with the possibility of amendments during the period of its validity.

Article 70.

1. The draft Strategy shall be developed by the minister competent for informatisation in cooperation with the Plenipotentiary, other ministers and relevant heads of central offices.

2. A representative of the President of the Republic of Poland may participate in the works on the draft.

Article 71.

The minister competent for informatisation in cooperation with the Plenipotentiary, other ministers and relevant heads of central offices reviews the Strategy every 2 years.

Article 72.

The minister in charge of informatisation shall forward the Strategy to the European Commission within 3 months of its adoption by the Council of Ministers.

Chapter 14

Rules on monetary penalties

Article 73.

1. A financial penalty shall be imposed on the operator of a key service who:

1) fails to conduct a systematic risk assessment or fails to manage the risk of an incident referred to in Article 8(1);

2) does not implement technical and organisational measures taking into account the requirements referred to in Article 8(2)(a-e);

3) fails to carry out the measures referred to in Article 8(5)(5(a-d);

4) has failed to designate the person referred to in Article 9(1)(1);

5) fails to comply with the obligation referred to in Article 10(1);

6) fails to comply with the obligation referred to in Article 11(1)(1);

7) fails to fulfil the obligation referred to in Article 11(1)(4);

8) fails to comply with the obligation referred to in Article 11(1)(5);

9) fails to remove vulnerabilities referred to in Article 32(2);

10) fails to comply with the obligation referred to in Article 14(1);

11) fails to carry out an audit;

12) prevents or obstructs the performance of the audit referred to in Article 53(2)(1);

13) failed to implement the post-audit recommendations referred to in Article 59(1) within the prescribed time limit.

2. Monetary penalty is imposed om the supplier of a digital service who:

1) fails to comply with the obligation referred to in Article 18(1)(4);

2) fails to comply with the obligation referred to in Article 18(1)(5);

3) fails to remove vulnerabilities referred to in Article 32(2);

3. The amount of the monetary penalty referred to in:

1) section 1(1) is up to PLN 150,000;

2) section 1(2) is up to PLN 100,000;

3) section 1(3) is up to PLN 50,000;

4) section 1(4) is up to PLN 15,000;

5) section 1(5) is up to PLN 50,000;

6) section 1(6) is up to PLN 15,000 for each identified case of failure to handle an incident;

7) section 1(7) is up to PLN 20,000 for each identified case of failure to handle a major incident;

8) section 1(8-9) is up to PLN 20,000;

9) section 1(10) is up to PLN 100,000;

10) section 1(11 and 13) is up to PLN 200,000;

11) section 1(12) is up to PLN 50,000;

12) section 2(1) is up to PLN 20,000 for each identified case of failure to handle a significant incident;

13) section 2(2 and 3) is up to PLN 20,000;

4. The penalty referred to in:

1) section 1(4) cannot be less than PLN 1,000;

2) section 1(1-3)(6-9) and (12) cannot be less than PLN 5,000;

3) section 1(5)(10-11) and (13) cannot be less than PLN 15,000;

5. If, as a result of an inspection, the authority competent for cyber security determines that a key service operator or a digital service provider persistently violates the provisions of the Act, causing:

1) a direct and major cyber security threat to defence, state security, public safety and order or human life and health, or

2) a threat that can cause serious damage to property or serious hindrance to the provision of key services

- shall be fined a penalty of up to PLN 1,000,000 imposed by the authority competent for cyber security.

Article 74.

1. The financial penalty referred to in Article 73 shall be imposed by decision of the authority competent for cyber security.

2. Proceeds from the fines referred to in Article 73 shall constitute revenue for the State budget.

Article 75.

The authority competent for cyber security may impose a fine on the head of the operator of a key service in case of failure to exercise due diligence to fulfil the obligations referred to in Article 8(1), Article 9(1)(1), and Article 15(1) but such fine may not exceed 200% of his monthly remuneration.

Article 76.

The penalty referred to in Article 73 may also be imposed if the entity has ceased the infringement of the law or has repaired the damage caused, if the authority competent for cyber security considers that this is justified by the duration, scope or consequences of the infringement.

Chapter 15

Amendments, transitional, adaptation and final provisions

Article 77.

In the Act of 7 September 1991 on the educational system (Journal of Laws of 2018 items 1457 and 730), in Article 90u

1) section 1(6) shall now read as follows:

   '6) developing the competences, interests and talents of children and young people and other social groups, including supporting the bodies that run schools or institutions in the implementation of projects in this area, in particular in the field of safe use of information and communication technologies';

2) section 4(6) shall now read as follows:

   '6) detailed conditions, forms and procedures for the implementation of projects in the field of developing competencies, interests and talents of children and young people and other social groups, as well as the conditions and procedures for assisting the bodies that run schools or institutions in the implementation of projects in this area, in particular in the field of safe use of information and communication technologies, taking into account the need to develop skills that facilitate adaptation to changes occurring in social and economic life, the possibility of providing financial support to the bodies that run schools or institutions and the requirement of efficiency and effectiveness of spending budgetary funds';

Article 78.

The Act of 4 September 1997 on divisions of government administration (Journal of Laws of 2018 items 762, 810, 1090, 1467 and 1544), shall be amended as follows:

1) section 12a(1)(10) shall now read as follows:

   '10) civil cyber security';

2) in Article 19(1), the following item (1a) shall be appended after item (1):

   '1a) military cyber security';

Article 79.

In the Act of 24 May 2002 on the Internal Security Agency and the Intelligence Agency (Journal of Laws of 2017, item 1920, [3)]) as amended, the following Article 32aa shall be appended after Article 32a:

'Article 32aa. 1. For the purpose of preventing, counteracting and combating incidents of a terrorist nature concerning information and communication systems of public administration bodies or networks covered by the uniform list of objects, installations, devices and services constituting critical infrastructure, as well as information and communication systems of owners, self-owners

[3)] The amendments to the consolidated text of the said Act have been announced in the Journal of Laws of 2017, item 2405 and of 2018, item 138, 650, 723, 730 and 1544.

and dependent owners of objects, installations or devices of critical infrastructure, referred to in Article 5b(7)(1) of the Act on Crisis Management of 26 April 2007, or data processed in these systems, as well as prevention and detection of terrorist offences in this area and prosecution of their perpetrators, the Internal Security Agency (ABW) implements in these entities the Internet Threat Early Warning System, hereinafter referred to as the "Warning System", which it also operates and coordinates its functioning.

2. The implementation of the warning system elements in the entities referred to in section 1 shall take place in accordance with an annual implementation plan developed by the Head of the ABW by 30 September of the preceding year. In justified cases, upon the request of an entity, the implementation of the warning system elements may be carried out without the plan.

3. The ABW shall immediately notify the entity referred to in section 1 of its inclusion in the annual plan of the alert system implementation.

4. 4. The entity referred to in section 1 is obliged to join the alert system and provide the ABW with necessary information making the implementation of the alert system in that entity possible.

5. In the entities referred to in section 1, subordinated to the Minister of National Defence or supervised by him, the alert system may be implemented with the consent of the Minister of National Defence.

6. The costs of the implementation and maintenance of the warning system in the entities referred to in section 1 are covered by the Internal Security Agency.

7. The ABW, under an agreement, agrees with the entity referred to in section 1 on the technical aspects of participation in the warning system and the model of the system configuration.

8. In the event of the conclusion of the agreement referred to in section 7 being impossible due to reasons attributable to the entity referred to in section 1, the ABW shall inform the entity supervising it or the minister competent for informatisation.

9. The Prime Minister shall define, by an ordinance, the conditions and procedure for conducting, coordinating and implementing the alert system, in particular shall define the activities necessary for its activation and maintenance and the model of the agreement referred to in section 7, guided by the need to ensure the security of information and communication systems important for the continuity of the functioning of the state’.

Article 80.

In the Act of 29 January 2004 - Public Procurement Law (Journal of Laws of 2017, item 1579 and 2018), in Article 89(1) item 7d) is replaced by the following:

‘7d) its adoption would violate public security or a significant interest of the state security, including the security of entities covered by the uniform list of facilities, installations, equipment and services included in the critical infrastructure referred to in Article 5b(7)(1) of the Act of 26 April 2007 on crisis management (Journal of Laws of 2018, item 1401), and this security or interest cannot be guaranteed otherwise’.

Article 81.

The Act of 16 July 2004 - Telecommunications Law (Journal of Laws of 2017 items 1907 and 2201 and of 2018 items 106, 138, 650 and 1118), shall be amended as follows:

1) In Article 174a:

a) section 1 shall have sections 1a and 1b appended, which shall read as follows:

‘1a. The President of UKE (Urząd Komunikacji Elektronicznej [Office of Electronic Communications]) shall provide the information referred to in section 1, if it relates to incidents which are incidents as defined in the Act of 5 July 2018 on the National Cyber Security System (Journal of Laws, item 1560), to the CSIRT competent for the notifying telecommunications entity, in accordance with Article 26 (5-7) of that Act, with the exclusion of information constituting an enterprise secret, reserved under Article 9.

1b. The notification referred to in section 1a shall be transmitted in electronic form, and if it is not possible to transmit it in electronic form - using other available means of communication’.

b) section 2 shall have sections 2a appended, which shall read as follows:

‘2a. The minister competent for informatisation shall determine, in a regulation, the criteria for considering a breach of security or integrity of the telecommunications network or services as a breach with a significant impact on the functioning of the network or services, taking into account, in particular, the percentage of users affected by the breach of security or integrity of the telecommunications network or services, the duration of the breach of security or integrity of the telecommunications network or services resulting in unavailability or reduced availability of the telecommunications network or services, and the recommendations and guidelines of the European Network and Information Security Agency (ENISA)’.

2) In Article 176a

a) section 1(3) shall now read as follows:

‘3. direct threats to the security or integrity of the undertaking's telecommunications infrastructure or services’.

b) Section 2(4) shall now read as follows:

‘4. technical and organisational measures to ensure the security and integrity of the telecommunications infrastructure and services provided, including protection against the occurrence of incidents within the meaning of the Act of 5 July 2018 on the National Cyber Security System’.

3) in Article 209(1), item 27^1 shall be appended which shall read as follows:

‘27^1) fails to fulfil the obligation referred to in Article 175a(1)’.

Article 82.

In the Act of 26 April 2007 on crisis management (Journal of Laws of 2018, item 1401) shall be amended as follows:

1) Article 5a(2) shall now read as follows:

‘2. Coordination of the preparation of the Report shall be ensured by the Director of the Government Centre for Security, while in the part concerning threats of a terrorist nature which may lead to a crisis situation - by the Head of the Internal Security Agency, and in the part concerning threats of a cyber security nature which may lead to a crisis situation - by the Government Plenipotentiary for Cyber Security’.

2) In Article 6(5a), section 5b shall be appended which shall read as follows:

‘5b. The owners, proprietary and dependent holders referred to in section 5, being also operators of key services as provided in the Act of 5 July 2018 on the National Cyber Security System Journal of Laws, item 1560), shall include in critical infrastructure protection plans documentation on the cybersecurity of information systems used for the provision of key services in accordance with the scope of information defined in the regulations issued pursuant to Article

10(5) of the Act of 5 July 2018 on the national cybersecurity system'.

3) in Article 8(3), in item 14, the full stop shall be replaced by a semicolon and the following item 15 shall be added, reading as follows:

'15) The Government Plenipotentiary competent for cyber security'.

4) section 11 shall have sections 1a and 1b appended, which shall read as follows:

'1a. The Centre shall provide support for the Critical Incidents Team referred to in Article 36(1) of the Act of 5 July 2018 on the National Cyber Security System'.

Article 83.

Cyber security threats, which may lead to a crisis situation, will be included for the first time in the Report on National Security Threats, which will be drawn up with the participation of the Plenipotentiary, after the entry into force of the Act.

Article 84.

The Prime Minister shall appoint the Plenipotentiary within 3 months of the Act entering into force of the Act.

Article 85.

The minister competent for informatisation shall provide the European Commission with information on:

1) the designated competent authorities for cyber security, the Point of Single Contact, and their tasks;

2) information about the tasks of CSIRT MON, CSIRT NASK and CSIRT GOV, including the main elements of procedures to be followed in the event of an incident.

Article 86.

The authorities competent for cybersecurity shall, by 9 November 2018, issue decisions on recognition as a key service operator and submit to the minister competent for informatisation applications for inclusion of key service operators in the list referred to in Article 7.

Article 87.

The minister competent for informatisation shall, by 9 August 2018, provide the Cooperation Group with a summary report on:

1) major incidents reported by operators of key services, affecting continuity of their provision of key services in the Republic of Poland and continuity of provision of key services in the Member States of the European Union;

2) significant incidents reported by digital service providers, including incidents concerning two or more European Union Member States;

Article 88.

By 9 November 2018, the minister competent for informatisation shall provide the European Commission with information on:

1) domestic measures to identify key service operators;

2) the list of key services;

3) number of identified key service operators in each sector referred to in Annex 1 to the Act, and an indication of their significance in relation to that sector;

4) the thresholds of significance of the disruptive effect on the key service provided, which are taken into account when qualifying entities as key service operators;

Article 89.

By 1 January 2021, the minister competent for informatisation shall launch the ICT system referred to in Article 46(1).

Article 90.

The Strategy shall be adopted by 31 October 2019.

Article 91.

1. The annual implementation plan referred to in Article 32aa(2) of the Act amended by Article 79 shall be developed by the Head of the Internal Security Agency for the first time for the year 2019.

2. An entity which, by the date of entry into force of the Act, has joined the ARAKIS-GOV programme implemented by the Internal Security Agency, shall be deemed to have joined the alert system, within the meaning of Article 32aa(4) of the Act amended in Article 79.

3. The entity referred to in section 2, which by the date of entry into force of the Act has not fully implemented the elements of the warning system, within the meaning of Art. 32aa(4) of the Act amended in Article 79, shall be obliged to complete them within one year from the date of entry into force of the Act.

4. Agreements concluded before the date of entry into force of the Act on participation in the ARAKIS-GOV programme shall be considered as agreements referred to in Article 32aa(7) of the Act amended in Article 79

Article 92.

1. The hitherto implementing regulations issued on the basis of Article 90u(4)(6) of the Act amended by Article 77 shall remain in force until the date of entry into force of the implementing regulations issued on the basis of Article 90u(4)(6) of the Act amended by Article 77 as amended by this Act, but no longer than until 1 December 2019, and may be amended.

2. The hitherto implementing regulations issued pursuant to Article 176a(5) of the Act amended in Article 81 shall remain in force until the date of entry into force of new implementing regulations issued pursuant to Article 176a(5) of the Act amended in Article 81, but no longer than for 24 months from the date of entry into force of this Act.

3. The hitherto implementing provisions issued on the basis of Article 5a (6) of the Act amended in Article 82 shall remain in force until the date of entry into force of new implementing provisions issued on the basis of Article 5a (6) of the Act amended in Article 82, but not longer than for 12 months from the date of entry into force of this Act.

Article 93.

1. The maximum limit of expenditure from the State budget for the budgetary part 21 - Maritime Economy, as a financial consequence of the entry into force of this Act, shall be:

1) in 2018 - 0 PLN;

2) in 2019 - 388 thousand PLN;

3) in 2020 - 404 thousand PLN;

4) in 2021 - 404 thousand PLN;

5) in 2022 - 404 thousand PLN;

6) in 2023 - 404 thousand PLN;

7) in 2024 - 404 thousand PLN;

8) in 2025 - 404 thousand PLN;

9) in 2026 - 404 thousand PLN;

10) in 2027 - 404 thousand PLN;

2. The maximum limit of expenditure from the State budget for the budgetary part 22 - Water Management, as a financial consequence of the entry into force of this Act, shall be:

1) in 2018 - 0 PLN;

2) in 2019 - 388 thousand PLN;

3) in 2020 - 404 thousand PLN;

4) in 2021 - 404 thousand PLN;

5) in 2022 - 404 thousand PLN;

6) in 2023 - 404 thousand PLN;

7) in 2024 - 404 thousand PLN;

8) in 2025 - 404 thousand PLN;

9) in 2026 - 404 thousand PLN;

10) in 2027 - 404 thousand PLN;

3. The maximum limit of expenditure from the State budget for the budgetary part 27 - Informatisation, as a financial consequence of the entry into force of this Act, shall be:

1) in 2018 - 6,450 thousand PLN;

2) in 2019 - 13,349 thousand PLN;

3) in 2020 - 17,334 thousand PLN;

4) in 2021 - 17,314 thousand PLN;

5) in 2022 - 18,904 thousand PLN;

6) in 2023 - 18,904 thousand PLN;

7) in 2024 - 18,904 thousand PLN;

8) in 2025 - 18,904 thousand PLN;

9) in 2026 - 18,904 thousand PLN;

10) in 2027 - 18,904 thousand PLN;

4. The maximum limit of expenditure from the State budget for the budgetary part 39 - Transport, as a financial consequence of the entry into force of this Act, shall be:

1) in 2018 - 0 PLN;

2) in 2019 - 388 thousand PLN;

3) in 2020 - 404 thousand PLN;

4) in 2021 - 404 thousand PLN;

5) in 2022 - 404 thousand PLN;

6) in 2023 - 404 thousand PLN;

7) in 2024 - 404 thousand PLN;

8) in 2025 - 404 thousand PLN;

9) in 2026 - 404 thousand PLN;

10) in 2027 - 404 thousand PLN;

5. The maximum limit of expenditure from the State budget for the budgetary part 46 - Health, as a financial consequence of the entry into force of this Act, shall be:

1) in 2018 - 0 PLN;

2) in 2019 - 388 thousand PLN;

3) in 2020 - 404 thousand PLN;

4) in 2021 - 404 thousand PLN;

5) in 2022 - 404 thousand PLN;

6) in 2023 - 404 thousand PLN;

7) in 2024 - 404 thousand PLN;

8) in 2025 - 404 thousand PLN;

9) in 2026 - 404 thousand PLN;

10) in 2027 - 404 thousand PLN;

6. The maximum limit of expenditure from the State budget for the budgetary part 47 - Energy, as a financial consequence of the entry into force of this Act, shall be:

1) in 2018 - 0 PLN;

2) in 2019 - 758 thousand PLN;

3) in 2020 - 789 thousand PLN;

4) in 2021 - 789 thousand PLN;

5) in 2022 - 789 thousand PLN;

6) in 2023 - 789 thousand PLN;

7) in 2024 - 789 thousand PLN;

8) in 2025 - 789 thousand PLN;

9) in 2026 - 789 thousand PLN;

10) in 2027 - 789 thousand PLN;

7. The maximum limit of expenditure from the State budget for the budgetary part 57 - Internal Security

Agency, as a financial consequence of the entry into force of this Act, shall be:

1) in 2018 - 0 PLN;

2) in 2019 - 255 thousand PLN;

3) in 2020 - 3,605 thousand PLN;

4) in 2021 - 5,605 thousand PLN;

5) in 2022 - 5,605 thousand PLN;

6) in 2023 - 9,705 thousand PLN;

7) in 2024 - 705 thousand PLN;

8) in 2025 - 705 thousand PLN;

9) in 2026 - 705 thousand PLN;

10) in 2027 - 8,705 thousand PLN;

8. The maximum limit of expenditure from the State budget for the budgetary part 70 - Financial Supervision Authority, as a financial consequence of the entry into force of this Act, shall be:

1) in 2018 - 0 PLN;

2) in 2019 - 758 thousand PLN;

3) in 2020 - 789 thousand PLN;

4) in 2021 - 789 thousand PLN;

5) in 2022 - 789 thousand PLN;

6) in 2023 - 789 thousand PLN;

7) in 2024 - 789 thousand PLN;

8) in 2025 - 789 thousand PLN;

9) in 2026 - 789 thousand PLN;

10) in 2027 - 789 thousand PLN;

9. The maximum limit of expenditure from the State budget for the budgetary part 76 - Office of Electronic Communications, as a financial consequence of the entry into force of this Act, shall be:

1) in 2018 - 0 PLN;

2) in 2019 - 203 thousand PLN;

3) in 2020 - 212 thousand PLN;

4) in 2021 - 212 thousand PLN;

5) in 2022 - 212 thousand PLN;

6) in 2023 - 212 thousand PLN;

7) in 2024 - 212 thousand PLN;

8) in 2025 - 212 thousand PLN;

9) in 2026 - 212 thousand PLN;

10) in 2027 - 212 thousand PLN;

10. The maximum limit of expenditure from the State budget for the budgetary part 42 - Internal Affairs, as a financial consequence of the entry into force of this Act, shall be:

1) in 2018 - 242 thousand PLN;

2) in 2019 - 360 thousand PLN;

3) in 2020 - 0 PLN;

4) in 2021 - 0 PLN;

5) in 2022 - 0 PLN;

6) in 2023 - 0 PLN;

7) in 2024 - 0 PLN;

8) in 2025 - 0 PLN;

9) in 2026 - 0 PLN;

10) in 2027 - 0 PLN;

11. In the event of a risk of exceeding or having exceeded the maximum expenditure limits adopted for a given budgetary year, referred to in paragraphs 1-6 and 8, corrective mechanisms shall be applied consisting of:

1) reduction of expenditures related to the implementation of the tasks of the body competent for cyber security in the field of identification of key service operators and ongoing analysis of entities in a given sector in terms of their recognition as a key service operator or non-fulfilment of conditions qualifying an entity as a key service operator;

2) reducing the number of inspections of key service operators and digital service providers;

3) resignation from organising or participating in cyber security exercises organised in the Republic of Poland or in the European Union;

4) reduced funding for the activities of the sectoral cyber security team set up by the competent authority for cyber security.

12. In the event of a threat of exceeding or going beyond the maximum expenditure limit adopted for a given budget year, referred to in section 7, a corrective mechanism shall be applied consisting in limiting the number of entities implementing the system of early warning of threats occurring on the Internet, indicated in the annual implementation plan, developed by the Head of the Internal Security Agency.

13. In the event of a threat of the maximum limit of expenditures, referred to in section 9, adopted for a given budgetary year being exceeded or exceeded, a corrective mechanism shall be applied consisting in the limitation of expenditures related to the implementation of statutory tasks concerning the handling of incidents.

14. In the event of a threat of exceeding or having exceeded the maximum limit of expenditures adopted for a given budgetary year, referred to in section 10, a correction mechanism shall be applied consisting in the reduction of expenditures related to the provision of equipment necessary to operate the Team.

15. In the event that the amount of expenditures in particular months is in line with the financial plan, the provisions of sections 11-14 shall not apply.

16. The minister competent for maritime economy monitors the use of the expenditure limit referred to in section 1 and at least four times a year, as at the end of each quarter, evaluates the use of the expenditure limit for a given year. The minister competent for maritime economy shall implement corrective mechanisms referred to in section 11.

17. The minister competent for water management shall monitor the use of the expenditure limit referred to in section 2 and at least four times a year shall, as at the end of each quarter, assess the use of the expenditure limit for a given year. The minister competent for water management shall implement corrective mechanisms referred to in section 11.

18. The minister competent for informatisation shall monitor the use of the expenditure limit referred to in section 3 and at least four times a year shall, as at the end of each quarter, assess the use of the expenditure limit for a given year. The minister competent for informatisation shall implement corrective mechanisms referred to in section 11.

19. The minister competent for transport shall monitor the use of the expenditure limit referred to in section 4 and at least four times a year shall, as at the end of each quarter, assess the use of the expenditure limit for a given year. The minister competent for transport shall implement corrective mechanisms referred to in section 11.

20. The minister competent for health care shall monitor the use of the expenditure limit referred to in section 5 and at least four times a year shall, as at the end of each quarter, assess the use of the expenditure limit for a given year. The minister competent for health care shall implement corrective mechanisms referred to in section 11.

21. The minister competent for energy shall monitor the use of the expenditure limit referred to in section 6 and at least four times a year shall, as at the end of each quarter, assess the use of the expenditure limit for a given year. The minister competent for energy shall implement corrective mechanisms referred to in section 11.

22. The Head of the Internal Security Agency shall monitor the use of the expenditure limit referred to in section 7 and at least four times a year shall, as at the end of each quarter, assess the use of the expenditure limit for a given year. The Head of the Internal Security Agency shall implement corrective mechanisms referred to in section 12.

23. Financial Supervision Authority shall monitor the use of the expenditure limit referred to in section 8 and at least four times a year shall, as at the end of each quarter, assess the use of the expenditure limit for a given year. Financial Supervision Authority shall implement corrective mechanisms referred to in section 11.

24. The President of the Electronic Communications Office shall monitor the use of the expenditure limit referred to in section 9 and at least four times a year shall, as at the end of each quarter, assess the use of the expenditure limit for a given year. The President of the Electronic Communications Office shall implement corrective mechanisms referred to in section 13.

25. The minister competent for internal affairs shall monitor the use of the expenditure limit referred to in section 10 and assess its use. The minister competent for internal affairs shall implement corrective mechanisms referred to in section 14.

Article 94.

The Act shall enter into force within 14 days from announcement.

President of the Republic of Poland *A. Duda*

Annexes to the Act of 5 July 2018

Annex 1

SECTORS AND SUBSECTORS AND ENTITY TYPES

Sector	Subsector (if any)	Entity type
Energy	Mining of minerals	Entities running a business of mining natural gas under the concession referred to in Article 22(1) of the Act of 9 June 2011 - Geological and Mining Law (Journal of Laws of 2017, item 2126 and of 2018, item 650 and 723).
		Entities running a business of mining crude oil under the concession referred to in Article 22(1) of the Act of 9 June 2011 - Geological and Mining Law.
		Entities running a business of mining lignite under the concession referred to in Article 22(1) of the Act of 9 June 2011 - Geological and Mining Law.
		Entities running a business of mining hard coal under the concession referred to in Article 22(1) of the Act of 9 June 2011 - Geological and Mining Law.
		Entities running a business of mining other minerals under the concession referred to in Article 22(1) of the Act of 9 June 2011 - Geological and Mining Law.
	Electrical power	The energy company referred to in Article 3(12) of the Act of 10 April 1997 - Energy Law (Journal of Laws of 2018, item 755, 650, 685, 771, 1000, as amended), holding a licence to run a business producing electricity.
		The energy company referred to in Article 3(24) of the Act of 10 April 1997 - Energy Law, holding a licence to run a business involving the transmission of electricity.
		The energy company referred to in Article 3(25) of the Act of 10 April 1997 - Energy Law, holding a licence to run a business involving the distribution of electricity.
		The energy company referred to in Article 3(12) of the Act of 10 April 1997 - Energy Law, holding a licence to run a business involving the trading of electricity.
		The energy company referred to in Article 3(12) of the Act of 10 April 1997 - Energy Law, holding a licence to run a business involving the processing or storing electricity.
		Entities providing system services, quality services and energy infrastructure management.
	Heat	The energy company referred to in Article 3(12) of the Act of 10 April 1997 - Energy Law, holding a licence to run a business involving heat generation.
		The energy company referred to in Article 3(12) of the Act of 10 April 1997 - Energy Law, holding a licence to run a business involving heat trading.

		The energy company referred to in Article 3(12) of the Act of 10 April 1997 - Energy Law, holding a licence to run a business involving heat transmission.
		The energy company referred to in Article 3(12) of the Act of 10 April 1997 - Energy Law, holding a licence to run a business involving heat distribution.
	Crude oil	The energy company referred to in Article 3(12) of the Act of 10 April 1997 - Energy Law, holding a licence to run a business involving liquid fuel production referred to in Article 32(1) of the Act of 10 April 1997 - Energy Law.
		Entities active in the transmission of crude oil.
		The energy company referred to in Article 3(12) of the Act of 10 April 1997 - Energy Law, holding a licence to run a business involving transmission of liquid fuels through the pipeline network referred to in Article 32(1) of the Act of 10 April 1997 - Energy Law.
		Entities running a business of crude oil storage, including tankless underground crude oil storage referred to in Article 22(1) of the Act of 9 June 2011 - Geological and Mining Law.
		Entities active in the transshipment of crude oil.
		The energy company referred to in Article 3(12) of the Act of 10 April 1997 - The Energy Law, running a business involving storage of liquid fuels referred to in Article 32(1) of the Act of 10 April 1997 - Energy Law and the entity running a business involving tankless underground crude oil storage referred to in Article 22(1) of the Act of 9 June 2011 - Geological and Mining Law.
		The energy company referred to in Article 3(12) of the Act of 10 April 1997 - Energy Law, holding a licence to run a business involving transshipment of liquid fuels, referred to in Article 32(1) of the Act of 10 April 1997 - Energy Law.
		The energy company referred to in Article 3(12) of the Act of 10 April 1997 - Energy Law, holding a licence to run a business involving trading of liquid fuels or trading of liquid fuels abroad, referred to in Article 32(1) of the Act of 10 April 1997 - Energy Law.
		Entities running a business involving the production of synthetic fuels.
	Gas	The energy company referred to in Article 3(12) of the Act of 10 April 1997 - Energy Law, holding a licence to run a business involving production of gas fuels, referred to in Article 3(45) of the Act of 10 April 1997 - Energy Law.
		The energy company referred to in Article 3(12) of the Act of 10 April 1997 - Energy Law, holding a licence to run a business involving gas fuel transmission.
		The energy company referred to in Article 3(12) of the Act of 10 April 1997 - Energy Law, holding a licence to run a business involving trading in natural gas with foreign countries or to run a business of trading in gaseous fuels.
		The energy company referred to in Article 3(24) of the Act of 10 April 1997 - Energy law, being an operator of a gas transmission system operator designated by the President of the Energy Regulatory Office.

		The energy company referred to in Article 3(25) of the Act of 10 April 1997 - Energy law, being an operator of a gas transmission system operator designated by the President of the Energy Regulatory Office.
		The energy company referred to in Article 3(26) of the Act of 10 April 1997 - Energy law, being an operator of a gas storage system operator designated by the President of the Energy Regulatory Office.
		The energy company referred to in Article 3(27) of the Act of 10 April 1997 - Energy law, being an operator of a gas liquefaction system operator designated by the President of the Energy Regulatory Office.
	Supplies and services for the energy sector	Entities running a business of the supply of systems, machinery, equipment, materials, raw materials and services to the energy sector.
	Supervised and subordinate units	Organisational units subordinate to the minister competent for energy or supervised by this minister.
		Organisational units subordinated to or supervised by a minister competent for mineral resources management.
Transport	Air transport	An air carrier referred to in Article 3(4) of Regulation (EC) No 300/2008 of the European Parliament and of the Council of 11 March 2008 on common rules in civil aviation security and repealing Regulation (EC) No 2320/2002 (OJ EU L 97 of 09/04/2008, p. 72).
		The airport authority referred to in Article 2(7) of the Act of 3 July 2002. - Aviation Law (Journal of Laws of 2018 item 1183).
		The entity referred to in Article 177(2) of the Act of 3 July 2002 - Aviation Law, performing for air carriers and other users of aircraft one or more categories of services referred to in Article 176 of this Act, and the entity referred to in Article 186b(1)(2) of the Act of 3 July 2002 - Aviation Law, performing for air carriers' safety control-related tasks.
		Air navigation service provider referred to in Article 127(1) of the Act of 3 July 2002 - Aviation Law.
	Rail transport	Railway infrastructure manager as provided in Article 4(7) of the Transport Act of 28 March 2003 (Journal of Laws of 2017, items 2117 and 2361 and of 201 items 650, 927 and 1338, as amended), excluding managers of inactive infrastructure referred to in Article 4(1b) of that Act, private infrastructure referred to in Article 4(1c), and narrow-gauge railway infrastructure referred to in Article 4(1d) of that Act.
		Rail carrier referred to in Article 4(9) of the Railway Transport Act of 28 March 2003, whose activity is subject to licensing and operator of service facility referred to in Article 4(52) of the Railway Transport Act of 28 March 2003, if the entity performing the operator's function is simultaneously a rail carrier.
	Waterway transport	A shipowner in the maritime transport of passengers and goods as defined for maritime transport in Annex I to Regulation (EC) No 725/2004 of the European Parliament and of the Council of 31 March 2004 on enhancing ship and port facility security (OJ EU L 129 of 29/04/2004, p. 6), excluding individual ships on which these shipowners operate.

		Shipowner referred to in Article 5 (1) (2) of the Act of 21 December 2000 on inland navigation (Journal of Laws of 2017, item 2128 and of 2018, item 1137).
		Marine port authority, referred to in Article 2 point 6 of the Act of 20 December 1996, on seaports and harbours (Journal of Laws of 2017 item 1933).
		Port Authority defined in Article 2(11) of Regulation (EC) 725/2004 of the European Parliament and of the Council of 31 March 2004 on enhancing ship and port facility security.
		Entities running a business supporting maritime transport in the port area.
		VTS (Vessel Traffic Services) - an auxiliary apparatus of the Director of the Maritime Office established for the purpose of monitoring vessel traffic and transmitting information, being a component of the National SafeSeaNet System, referred to in Article 91 of the Act of 18 August 2011 on Maritime Safety (Journal of Laws of 2018 items 181 and 1137).
	Road transport	The authorities referred to in Article 19(2), (5) and (5a) of the Act of 21 March 1985 on public roads Journal of Laws of 2017, item 2222 and of 2018, items 12, 138, 159, 317 and 1356).
		Entities referred to in Article 43a (1) of the Act of 21 March 1985 on public roads
Banking and financial markets infrastructure		Credit institution referred to in Article(1)(17) of the Act of 29 August 1997 - Banking Law (Journal of Laws of 2017, item 1876, as amended [4)]).
		Domestic bank referred to in Article(4)(1)(1) of the Act of 29 August 1997 - Banking Law.
		Foreign bank branch referred to in Article(4)(1)(20) of the Act of 29 August 1997 - Banking Law.
		A branch of a credit institution referred to in Article 4(1)(18) of the Act of 29 August 1997 - Banking Law.
		Cooperative savings and credit unions as provided in the Act of 5 November 2009 on cooperative savings and credit unions (Journal of Laws of 2017, item 2065, as amended [5)]).
		Entity operating a regulated market referred to in Article 14(1) of the Act of 29 July 2005 on trading in financial instruments. Laws of 2017, item 1768, as amended [6)]).
		Entity operating a regulated market referred to in Article 3(49) of the Act of 29 July 2005 on trading in financial instruments.
		Entity operating a regulated market referred to in Article 48(7) of the Act of 29 July 2005 on trading in financial instruments
		The therapeutic entity referred to in Article 4(1) of the Act of 15 April

4) The amendments to the consolidated text of the said Act have been announced in the Journal of Laws of 2017 items 2361 and 2491 and 2018 items 62, 106, 138, 650, 685, 723, 864, 1000, 1075 and 1499.

5) The amendments to the consolidated text of the said Act have been announced in the Journal of Laws of 2017 items 2486 and 2491 and 2018 items 62, 106, 138, 650, 723, 771, 864, 1000, 1075, 1499 and 1544.

6) The amendments to the consolidated text of the said Act have been announced in the Journal of Laws of 2017 items 2486 and 2491 and 2018 items 106, 138, 650, 685, 723 and 771.

Healthcare		2011 on therapeutic activity (Journal of Laws of 2018 items 160, 138, 650, 1128, 1375 and 1532).
		Unit subordinate to a minister competent for health matters, responsible for health care information systems.
		National Health Fund (NFZ).
		Healthcare facility, where a hospital pharmacy department operates, as provided in the Act of 6 September 2001 - Pharmaceutical Law (Journal of Laws of 2017, item 2211, as amended [7)]).
		Healthcare facility, where a hospital pharmacy operates, as provided in the Act of 6 September 2001 - Pharmaceutical Law.
		Entity running a business involving running a pharmaceutical wholesale warehouse as provided in the Act of 6 September 2001. - Pharmaceutical Law.
		Entrepreneur or entity conducting business activity in a European Union Member State or member state of the European Free Trade Association (EFTA) - party to the Agreement on the European Economic Area which obtained authorisation for marketing of a medicinal product.
		Importer of an active substance as provided in the Act of 6 September 2001 - Pharmaceutical Law.
		Manufacturer of an active substance as provided in the Act of 6 September 2001 - Pharmaceutical Law.
		Parallel importer as provided inf the Act of 6 September 2001. - Pharmaceutical Law.
		Distributor of an active substance as provided in the Act of 6 September 2001 - Pharmaceutical Law.
		Entity running a business involving running a generally accessible pharmacy as provided in the Act of 6 September 2001. - Pharmaceutical Law.
Supply and distribution of drinking water		A water supply and sewerage company referred to in Article 2(4) of the Act of 7 June 2001 on collective water supply and collective wastewater disposal (Journal of Laws of 2018 item 1152).
Digital infrastructure		Entity providing DNS services.
		Entity operating an Internet traffic exchange point (IXP), which is a network facility that provides an interconnection between more than two independent autonomous systems, primarily for the purpose of facilitating the exchange of Internet traffic operation.
		Entity managing the registration of Internet domain names under the Top Level Domain (TLD).

[7)] The amendments to the consolidated text of the said Act have been announced in the Journal of Laws of 2018 items 650, 697, 1039, 1375, 1515 and 1544.

Annex 2

DIGITAL SERVICES

Service name	Service definition
Online sales platform	A service which enables consumers or traders to conclude contracts electronically with traders on the website of a sales platform or on the website of a trader who uses the services provided by the online sales platform.
Cloud computing service	A service that provides access to a scalable and flexible set of computing resources for shared use by multiple users.
Internet search engine	A service that allows users to search all websites or web pages in a particular language using a query by entering a keyword, phrase or other element, resulting in links that refer to information related to the query.