A C T

of 5 July 2018

on the national cybersecurity system[1), 2)]

Chapter 1

General provisions

Article1. 1. The Act governs the following:

1) organisation of the national cybersecurity system and tasks and responsibilities of entities forming part of the system;
2) manner of exercising supervision and control of application of the provisions of the Act;
3) scope of the Polish National Cybersecurity Strategy.

2. The Act shall not apply to:

1) telecommunications companies referred to in the Act of 16 July 2004 - Telecommunications Law (Journal of Laws of the Republic of Poland of 2017, items 1907 and 2201, and of 2018 items 106, 138, 650 and 1118), regarding security requirements and incident reporting;
2) trust services providers that 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, established by the Head of Agencja Bezpieczeństwa Wewnętrznego (Internal Security Agency) or the Head of Agencja Wywiadu (Foreign Intelligence Agency).

---

1) This Act, within the scope of its regulation, implements Directive of the European Parliament and of the Council (EU) 2016/1148 of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (OJ EU L 194 of 19.07.2016, p. 1).

2) The following acts are amended by this Act: the Act of 7 September 1991 on the education system, the Act of 4 September 1997 on government administration sectors, the Act of 24 May 2002 on the Internal Security Agency and the Foreign Intelligence Agency, the Act of 29 January 2004 – Public procurement law, the Act of 16 July 2004 – Telecommunications law, and the Act of 26 April 2007 on crisis management.

Article 2. The terms used in the Act shall mean as follows:

1) CSIRT GOV - Computer Security Incident Response Team operating at the national level, led by the Head of the Internal Security Agency;
2) CSIRT MON - Computer Security Incident Response Team operating at the national level, led by the Minister of National Defence;
3) CSIRT NASK - Computer Security Incident Response Team operating at the national level, led by Naukowa i Akademicka Sieć Komputerowa – Państwowy Instytut Badawczy (Research and Academic Computer Network – National Research Institute);
4) cybersecurity – the resistance of information systems to activities that compromise the confidentiality, integrity, availability and authenticity of data being processed or related services offered by these systems;
5) incident – any event having an actual adverse effect or may have an adverse effect on cybersecurity;
6) critical incident – an incident that results in a major detriment to the public security or public order, international interests, economic interests, operation of public institutions, civil rights and freedoms, or human life and health, classified by competent CSIRT MON, CSIRT NASK or CSIRT GOV;
7) serious incident – an incident that causes or may cause a serious reduction in the quality or interruption in continuity of supplying of an essential service; ;
8) significant incident – an incident that has a significant impact on the provision of a digital service within the meaning of Article 4 of the Commission Implementing Regulation (EU) 2018/151 of 30 January 2018 laying down rules for application of Directive (EU) 2016/1148 of the European Parliament and of the Council as regards further specification of the elements to be taken into account by digital service providers for managing the risks posed to the security of network and information systems and of the parameters for determining whether an incident has a substantial impact (OJ EU L 26 of 31.01.2018, p. 48), hereinafter referred to as the "Regulation 2018/151";
9) incident in a public entity – an incident that causes or may cause a deterioration of quality or interruption of the performance of a public task carried out by a public entity referred to in Article 4, items 7-15;

10) incident handling – activities that allow detecting, registering, analysing, classifying, prioritizing, taking corrective actions and reducing effects of an incident;
11) vulnerability – the quality or stateof an information system that can be exploited by a cybersecurity threat;
12) risk – a combination of probability of occurrence of an undesirable event and its consequences;
13) risk estimation – a comprehensive process of risk identification, analysis and assessment;
14) information system - an ICT system, referred to in Article 3, subparagraph 3 of the Act of 17 February 2005 on the computerisation of activities of entities performing public tasks (Journal of Laws of 2017, item 570, and of 2018, item 1000), together with electronic data processed within it ;
15) digital service – a service provided electronically as defined in the provisions of the Act of 18 July 2002 on providing services by electronic means (Journal of Laws of 2017, item 1219, and of 2018, item 650), as listed in the Annex No. 2 to that Act;
16) key service – a service of key importance for maintaining a critical social or economic activity listed in the key services list;
17) cybersecurity threat – a potential cause of occurrence of an incident;
18) incident management – incident handling, searching for links between incidents, removing the causes of their occurrence and drawing conclusions from incident handling;
19) risk management – coordinated actions in the field of cybersecurity management regarding to estimated risk.

Article 3. The purpose of the national cybersecurity system is to ensure cybersecurity at the national level, including uninterrupted providing of essential services and digital services, by achieving an appropriate level of security of information systems used to provide these services, and by providing incident handling.

Article 4. The national cybersecurity system includes:
1) operators of essential services ;
2) digital services providers;
3) CSIRT MON;
4) CSIRT NASK;

5) CSIRT GOV;
6) sectoral cybersecurity teams;
7) public finance sector entities referred to in Article 9, subparagraphs 1-6, 8.9, 11 and 12 of the Act of 27 August 2009 on public finance (Journal of Laws of the Republic of Poland of 2017, item 2077, and of 2018, items 62 and 1000);
8) research institutes;
9) Narodowy Bank Polski (National Bank of Poland);
10) Bank Gospodarstwa Krajowego (National Development Bank);
11) Urząd Dozoru Technicznego (Office of Technical Inspection);
12) Polska Agencja Żeglugi Powietrznej (Polish Air Navigation Services Agency);
13) Polskie Centrum Akredytacji (Polish Centre for Accreditation);
14) Narodowy Fundusz Ochrony Środowiska i Gospodarki Wodnej (National Fund for Environmental Protection and Water Management) and regional funds for environmental protection and water management;
15) commercial law companies performing public utility tasks as defined in Article 1 item 2 of the Act of 20 December 1996 on municipal services management (Journal of Laws of 2017, item 827);
16) entities providing services in the cybersecurity area;
17) competent authorities for cybersecurity matters;
18) Single Point of Contact for cybersecurity, hereinafter referred to as the "Single Point of Contact";
19) Government Plenipotentiary for Cybersecurity, hereinafter referred to as "the Plenipotentiary";
20) Kolegium do Spraw Cyberbezpieczeństwa (Cybersecurity Committee for Cybersecurity), hereinafter referred to as "the Cybersecurity Committee".

Chapter 2

Identification and registration of operators of essential services

Article 5. 1. An operator of essential service shall be an entity specified in Annex 1 to the Act, having an organizational unit in the territory of the Republic of Poland, for which the competent authority for cybersecurity matters issued a decision to recognize it as an operator of essential service. Sectors, subsectors and types of entities are specified in Annex 1 to the Act.

2. The competent authority for cybersecurity matters shall issue a decision on recognizing an entity as an operator of essential service if:

1) the entity provides an essential service;
2) providing of that service depends on information systems;
3) the incident would have a significant disruptive effect on the provision of essential service by that operator.

3. The significance of the disruptive effects on the provision of service in providing of an essential service, referred to in paragraph 2 subparagraph 3, shall be determined based on the significance of a disruptive effect thresholds.

4. Where the entity provides an essential service in other European Union Member States, the competent authority for cybersecurity matters shall consult these states during the administrative procedure, via the Single Point of Contact, in order to find out whether the entity has been recognized as an operator of essential service in these states.

5. The period for conducting consultations referred to in paragraph 4 shall not count for the time limits referred to in Article 35 of the Act of 14 June 1960 – the Code of Administrative Procedure (Journal of Laws of the Republic of Poland of 2017, item 1257, and of 2018, items 149 and 650).

6. Where the entity no longer meets the conditions referred to in paragraphs 1 and 2, the competent authority for cybersecurity matters shall issue a decision declaring the expiry of the decision on recognition as an operator of essential service.

7. The decisions referred to in paragraphs 2 and 6 are subject to immediate execution.

Article 6. The Council of Ministers shall determine, by way of regulation:

1) the list of essential services referred to in Article 5 paragraph 2 subparagraph 1, guided by the assignment of an essential service to a given sector, subsector and type of entity listed in Annex 1 to the Act and the importance of service for maintaining of critical societal and economic activities.;
2) significance of a disruptive effect thresholds of the incident on the provision of essential services listed in the list of essential services, including:
   a) the number of users relying on the essential service provided by the entity concerned,
   b) the dependency of other sectors, referred to in Annex 1 to the Act, on the service provided by that entity,

c) the impact the incident could have, in terms of degree and duration, on the economic and societal activities or public safety,,

d) the market share of that entity which provides an essential service,

e) the geographic spread with regard to the area that could be affected by an incident,

f) the capability of the entity for maintaining a sufficient level of the provision of essential service, taking into account the availability of alternative means for the provision of that service,

g) other factors specific for the sector or subsector concerned, if any

– guided by the need to provide protection against threats to human life or health, significant property losses and decrease in the quality of the essential service being provided.

Article 7. 1. The minister competent for digitalisation shall set up a list of operators of essential services.

2. The list of operators of essential services includes the following details:

1) the name (business name) of the operator of essential service;
2) the sector, sub-sector and type of the entity;
3) the registered office and address;
4) the tax identification number (NIP), if given;
5) the number in the relevant register, if given;
6) the name of the essential service, consistent with the list of essential services;
7) the date of commencement of providing the essential service;
8) the information specifying in which European Union Member States the entity was recognized as an operator of essential service;
9) the date of completion of provision of the essential service;
10) date of deletion from the list of operators of essential service.

3. Entering into the list of operators of essential services and deleting from that list shall be made at the request of the competent authority for cybersecurity matters upon the decision on declaring the entity as an operator of essential service or the decision on the expiry of the decision on declaring the entity as an operator of essential service. The request shall contain the details referred to in paragraph 2 subparagraph 1-9.

4. The data on the list of operators of essential services shall be modified at the request of the authority competent for cybersecurity matters, submitted not later than within 6 months from the amendment of this details.

5. The requests referred to in paragraphs 3 and 4 shall be executed in an electronic form and shall be provided with a qualified electronic signature or a signature confirmed with a trusted ePUAP profile.

6. Entering into the list of operators of essential services and deleting from that list, and modifying data on the list of operators of essential services is a substantive-technical operation.

7. The minister competent for digital affairs shall make the data from the list of operators of essential services available to CSIRT MON, CSIRT NASK and CSIRT GOV and the sectoral cybersecurity team to the extent covered by the sector or subsector for which it was established, as well as to the operators of essential services to the extent concerning the operator.

8. The minister competent for digitalisation makes available data from the list of operators of essential services, on request, to the following entities to the extent necessary for the implementation of their statutory tasks:

1) competent authorities for cybersecurity;
2) Policja (Police);
3) Żandarmeria Wojskowa (Military Police);
4) Straż Graniczna (Border Guard);
5) Centralne Biuro Antykorupcyjne (Central Anti-Corruption Bureau);
6) Agencja Bezpieczeństwa Wewnętrznego (Internal Security Agency) and Agencja Wywiadu (Foreign Intelligence Agency);
7) Służba Kontrwywiadu Wojskowego (Military Counterintelligence Service) and Służba Wywiadu Wojskowego (Military Intelligence Service);
8) courts of justice;
9) public prosecutor's offices;
10) of Krajowa Administracja Skarbowa (National Internal Revenue Administration);
11) the Director of Rządowe Centrum Bezpieczeństwa (Government Centre for Security);
12) Służba Ochrony Państwa (State Protection Service).

Chapter 3

Responsibilities of operators of essential services

Article 8. The operator of essential service shall implement the security management system in the information system used to provide the essential service which ensures:

1) conducting systematic estimation of the risk of incident occurrence and managing that risk;
2) implementation of appropriate technical and organisational measures relevant to the estimated risk, taking into account the latest state of the art, including:
   a) maintenance and secure operation of the information system,
   b) physical and environmental security, including access control,
   c) security and continuity of supplies of the services that determines provision of the essential service,
   d) implementing, documenting and maintaining action plans enabling continuous and uninterrupted provision of the essential service and ensuring confidentiality, integrity, accessibility and authenticity of information,
   e) covering the information system used to provide the essential service with a continuous monitoring system;
3) collecting information on cybersecurity threats and incident vulnerabilities of the information system used to provide the essential service;
4) incident management;
5) taking appropriate measures to prevent and minimise the impact of incidents affecting the information system used for the provision of essential service, including:
   a) applying mechanisms to ensure the confidentiality, integrity, accessibility and authenticity of data processed in the information system,
   b) care about updating the software,
   c) protection against unauthorized modification in the information system,
   d) immediate response once vulnerabilities or threats to cybersecurity are found;
6) using means of communication enabling proper and safe communication within the national cybersecurity system.

Article 9. 1. The operator of essential service shall:

1) appoint a person responsible for contacts with the entities of the national cybersecurity system;
2) provide essential service users with access to knowledge that allows them to understand cybersecurity threats and use effective means to protect themselves against those threats to the extent related to the essential service being provided, in particular by publishing information on its website;

3) provide the authority competent for cybersecurity matters with the data referred to in Article 7, paragraph 2, items 8 and 9, not later than within 3 months from the modification of those data.

2. The operator of essential service shall provide the authority competent for cybersecurity matters, the competent CSIRT MON, CSIRT NASK, CSIRT GOV and the sectoral cybersecurity team with data of the person referred to in paragraph 1 subparagraph 1, including forename and surname, telephone number and e-mail address, within 14 days from the date of his or her appointment, and information about the change of those data –within 14 days from the date of their modification.

Article 10. 1. The operator of essential service shall develop, apply and update the documentation on cybersecurity of the information system used to provide the essential service.

2. The operator of essential service is obliged to establish supervision over the documentation on cybersecurity of the information system used to provide the essential service, ensuring:

1) availability of documents only to those authorized in accordance with their responsibilities;
2) protection of documents from improper use or loss of integrity;
3) marking subsequent versions of documents enable to determine of revisions made to those documents.

3. The operator of essential service shall keep the documentation on cybersecurity of the information system used to provide the essential service, for at least 2 years from the date of its withdrawal from operation or of termination of providing the essential service, with the provisions of the Act on the national archival resource and state archives of 14 July 1983 (Journal of Laws the Republic of Poland of of 2018, items 217, 357, 398 and 650).

4. The operator of essential service who is also an owner independent or dependent holder of facilities, installations, devices or services included in the critical infrastructure specified in the list referred to in Article 5b paragraph 7 item 1 of the Act of 26 April 2007 on crisis management (Journal of Laws the Republic of Poland of of 2017, items 209 and 1566, and of 2018, item 1118), having an approved plan for the protection of critical infrastructure, including documentation on cybersecurity of the information system used to provide the essential service, has no obligation to prepare the documentation referred to in paragraph 1.

5. The Council of Ministers shall determine, in an ordinance , the types of documentation referred to in paragraph 1, taking into account the Polish Standards and the necessity to ensure cybersecurity during the provision of essential services, and the continuity of those services.

Article 11. 1. The operator of essential service shall:

1) provide incident handling;
2) provide access to information on reported incidents for the competent CSIRT MON, CSIRT NASK or CSIRT GOV to the extent necessary to fulfil their tasks;
3) classify the incident as a serious in accordance with the thresholds for considering incidents as serious;
4) notify a serious incident without undue delay , however not later than within 24 hours from its detection, to the competent CSIRT MON, CSIRT NASK or CSIRT GOV;
5) acting together with the competent CSIRT MON, CSIRT NASK or CSIRT GOV during the handling of a serious incident and critical incident, providing the necessary data, including personal data;
6) remove the vulnerabilities referred to in Article 32 paragraph 2, and shall notify the competent authority for cybersecurity matters of their removal.

2. The notification referred to in paragraph 1 item 4, shall be submitted electronically,– or by using other available means of communication, when it is impossible to provide it in an electronic form.

3The operator of essential service , apart of the tasks set out in paragraph 1, if a sector-specific cybersecurity team is established, shall:

1) simultaneously provide to that team, in electronic form, the notification referred to in paragraph 1 subparagraph 4;
2) act together with that team, at the sector or sub-sector level, during the handling of a serious or critical incident, by providing the necessary data, including personal data;
3) provide that team with access to information on reported incidents to the extent necessary to carry out its tasks.

4. The Council of Ministers shall determine, in an ordinance , the thresholds for considering incidents as serious in accordance with the type of incident in particular 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 essential service,,
2) the duration of the incident which affected the provided essential service,
3) the geographical area affected by the incident,
4) other factors specific to the sector or subsector, if any

– guided by the need to provide protection against threats to human life or health, significant property losses and decrease in the quality of the essential service being provided.

Article 12.1. The notification mentioned in Article 11 paragraph 1 item 4must provide following:

1) details of the notifying entity, including the business name, number in the relevant register, registered office and address;
2) forename and surname, telephone number and e-mail address of the person reported the notification;
3) forename and surname, telephone number and e-mail address of the person entitled to provide explanations regarding the information reported;
4) description of the impact of a serious incident on the provision of the essential service, including:
   a) the notifier's essential services affected by the serious incident,
   b) number of users of the essential service affected by the serious incident,
   c) moment of occurrence and detection of the serious incident and its duration
   d) the geographical area affected by the incident,
   e) impact of the serious incident on the provision of the essential service by other operators of essential service and digital service providers,
   f) cause of the occurrence of the serious incident and the manner of its course, and the effects of its impact on information systems or essential services provided;
5) information enabling the competent CSIRT MON, CSIRT NASK or CSIRT GOV to determine whether the incident affects two or more European Union Member States;
6) in case of an incident which occurrence could have affected the provision of an essential service, a description of the cause of the incident, the manner of its occurrence and its likely impact on the information systems;
7) information on preventive actions taken;

8) information on the remedial actions taken;

9) other relevant information.

2. The operator of essential service shall provide information which is expected to be known at the moment of notification, which it shall complement when handling the serious incident.

3. The operator of essential service shall, to the extent necessary, provide with the notification referred to in Article 11 paragraph 1 subparagraph 4, information constituting legally protected secrets, including business secrets, if this is necessary to perform tasks by the competent CSIRT MON, CSIRT NASK or CSIRT GOV and the sectoral cybersecurity team.

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

5. The operator of essential service shall mark in the notification the information constituting legally protected secrets, including business secrets.

Article 13.1. The operator of essential service may provide the competent CSIRT MON, CSIRT NASK or CSIRT GOV with information on:

1) other incidents;

2) cybersecurity threats;

3) risk estimation;

4) vulnerabilities;

5) technologies used.

2.. The information referred to in paragraph 1 shall be submitted electronically or by using other available means of communication, when it is impossible to provide it in an electronic form.

3. If a sectoral cybersecurity team is established, the operator of essential service may provide electronically the information referred to in paragraph 1 to that team.

4. The operator of essential service shall mark the information constituting legally protected secrets, including business secrets.

Article 14. 1. The operator of essential service, in order to perform the tasks referred to in Article 8, Article 9, Article 10 paragraphs 1-3, Article 11 paragraphs 1-3, Article 12

and Article 13, shall establish internal structures responsible for cybersecurity or shall conclude a contract with an entity providing services in the field of cybersecurity.

2. Internal structures responsible for cybersecurity, set up by the operator of essential service , and entities providing services in the field of cybersecurity are obliged to:

1) meet organisational and technical conditions that allow ensuring cybersecurity to the operator of essential service being supported;
2) have rooms to provide services of response to incidents, protected against physical and environmental threats;
3) use safeguards to ensure the confidentiality, integrity, accessibility and authenticity of the information being processed, including personal, operational and system architecture security.

3. The operator of essential service shall notify the competent authority for cybersecurity matters and the competent CSIRT MON, CSIRT NASK, CSIRT GOV and the sectoral cybersecurity team about the entity that was contracted for the provision of cybersecurity services , contact details of this entity, the scope of the service provided and of termination of the contract, within 14 days from the date of concluding or terminating the contract.

4. The minister competent for digitalisation shall specify, in an ordinance , organisational and technical conditions for entities providing cybersecurity services and internal structures responsible for cybersecurity, considering the Polish Standards and the need to ensure security for internal structures responsible for cybersecurity and entities providing services in the field of cybersecurity for operators of essential service, as well as the need to ensure the security of information processed within these structures or entities.

Article 15. 1. The operator of essential service shall ensure a security audit of the information system used to provide the essential service, hereinafter referred to as "the audit", being carried out at least every two years.

2. The audit may be conducted by:

1) a conformity assessment body accredited in accordance with the provisions of the Act of 13 April 2016 on conformity assessment and market surveillance systems (Journal of Laws of the Republic of Poland of 2017, item 1398, and of 2018, item 650), to the extent as relevant for security assessments of information systems being undertaken;
2) at least two auditors who have:

a) certificates specified in the regulations issued under paragraph 8, or

b) at least a three-year experience in the field of auditing the security of information systems, or

c) at least a two-year experience in the field of auditing the security of information systems, and hold a diploma of post-graduate studies in the field of information systems security audits, issued by an organisational unit that was entitled, as of the day of graduation, to grant doctoral degrees in economics, technology or laws;

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

3. A documented performance, in the last 3 years before the date of audit commencement, of 3 audits in the field of information system security or business continuity, or a performance of information system security audits or business continuity in the working time of not less than 1/2 full-time, associated with the below mentioned activities, shall be deemed the experience in information systems security audit referred to in paragraph 2 item 2 points b and c:

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

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

3) conducting an internal audit in the area of information security, as referred to in the regulations issued pursuant to Article 18 of the Act of 17 February 2005 on the computerisation of activities of entities performing public tasks;

4) performing inspection activities, referred to in the Act of 15 July 2011 on controlling in government administration (Journal of Laws the Republic of Poland, item 1092).

5) performing inspection activities referred to in the Act of 23 December 1994 on the Supreme Audit Office (Journal of Laws of the Republic of Poland of 2017, item 524, and of 2018, item 1000).

4. The auditor is obliged to keep confidential the information obtained in connection with the auditing carried out, subject to the provisions on the protection of classified information and other legally protected information.

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

6. The operator of essential service with whom an internal information security audit referred to in the regulations issued pursuant to Article 18 of the Act of 17 February

2005 on the computerisation of activities of entities performing public tasks was carried out in a given year, by persons who meet the conditions set out in paragraph 2 subparagraph 2, with regard to the information system used to provide the essential service, has no obligation to conduct an audit for 2 years.

7. The operator of essential service shall provide a copy of the audit report on a reasoned request of:

1) the competent authority for cybersecurity matters;
2) Director of Rządowe Centrum Bezpieczeństwa (Government Centre for Security) –in the case if the operator of essential service is also the owner, independent or dependent holder of facilities, installations, devices or services included in the critical infrastructure specified in the list referred to in Article 5b paragraph 7 subparagraph 1 of the Act of 26 April 2007 on crisis management;
3) Head of Agencja Bezpieczeństwa Wewnętrznego (Internal Security Agency).

8. The minister competent for digitalisation shall specify, in a regulation, a list of certificates entitling to carry out the audit, considering the scope of specialist knowledge required from persons holding individual certificates.

Article 16. The operator of essential service shall perform the responsibilities specified in:

1) Article 8, items 1 and 4, Article 9, Article 11, paragraphs 1 to 3, Article 12 and Article 14, paragraph 1 – within 3 months from the date of delivery of the decision on declaring the entity as an operator of essential service;
2) Article 8, items 2, 3, 5 and 6, and Article 10, paragraphs 1 to 3 – within 6 months from the date of delivery of the decision on declaring the entity as an operator of essential service;
3) Article 15, paragraph 1 – within one year from the date of delivery of the decision on declaring the entity as an operator of essential service.

Chapter 4

Responsibilities of digital service providers

Article 17. 1. A digital service provider is a legal person or an organisational unit without legal personality, having a registered office or management board on the territory of the Republic of Poland or a representative having an organisational unit on the territory of the Republic of Poland, and who provides digital services, except for micro enterprises and small enterprises referred to in Article 7 paragraph 1 items 1 and 2 of the Act of 6

March 2018 – Law on entrepreneurs (Journal of Laws, item 646). The types of digital services are set out in Annex 2 to the Act.

2. The digital service provider shall take appropriate and proportionate technical and organisational measures, as set out in the Regulation 2018/151, to manage the risks to which the information systems used to provide the digital service are exposed. These measures shall provide cybersecurity appropriate to the risk and cover:

1) security of information systems and facilities;
2) procedure for incident handling;
3) managing the continuity of the provider's operations to provide the digital service;
4) monitoring, auditing and testing;
5) the latest state of the art, including compliance with the international standards referred to in the 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 that service.

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

5. A representative may be a natural person, legal person or organisational unit without legal personality, established in the Republic of Poland or in another EU Member State, authorised to act on behalf of a digital service provider who does not have an organisational unit in the European Union, which may be contacted by the competent authority for cybersecurity matters, CSIRT MON, CSIRT NASK or CSIRT GOV due to the issues related to the obligations of the digital service provider under the Act.

Article 18. 1. The digital service provider shall:

1) perform activities aimed at detecting, recording, analysing and classifying incidents;
2) provide, as necessary, access to information for the competent CSIRT MON, CSIRT NASK or CSIRT GOV about incidents classified as critical by the competent CSIRT MON, CSIRT NASK or CSIRT GOV;
3) classify the incident as significant;
4) report a significant incident without undue delay , however not later than within 24 hours from its detection, to the competent CSIRT MON, CSIRT NASK or CSIRT GOV;

5) provides handling of a significant incident and critical incident in collaboration with the competent CSIRT MON, CSIRT NASK or CSIRT GOV, providing the necessary data, including personal data;
6) remove the vulnerabilities referred to in Article 32, paragraph 2;
7) provide the operator of essential service who provides an essential service through that digital service provider, information on the incident affecting the continuity of the provision of that essential service operator's service.

2. In order to determine whether the impact of an incident is substantial the digital service provider shall take into account, in particular, the following parameters:
1) the number of users affected by the incident and, in particular, the users relying on the digital service for the provision of their own services;
2) the duration of the incident;
3) the geographic spread with regard to the area that could be affected by an incident;;
4) the extent of the disruption to the functioning of the service ;
5) the extent of impact of the incident on economic and societal activities.

3. The digital service provider, when classifying the incident as significant, shall assess the significance of the impact of the incident on the provision of the digital service, based on the parameters referred to in paragraph 2, and the thresholds set out in the Regulation 2018/151.

4. If the digital service provider does not hold information allowing to assess the significance of the impact of the incident on the provision of the digital service, it has no obligation to make the notification referred to in paragraph 1, point 4.

5. The notification referred to in paragraph 1 item 4, shall be submitted electronically or by using other available means of communication, when it is impossible to provide it in an electronic form.

Article 19. 1. The notification mentioned in Article 18 paragraph 1 item 4 must provide the following information: 1) details of the notifying entity, including the business name, number in the relevant register, registered office and address;
2) forename and surname, telephone number and e-mail address of the person reporting the notification;
3) forename and surname, telephone number and e-mail address of the person entitled to provide explanations regarding the information reported;
4) an assessment of the impact of the significant incident on the provision of the digital service, including:

a) number of users affected by the significant incident,
b) the time the incident occurred and detected , and the duration of the significant incident,
c) the geographic spread with regard to the area that could be affected by the significant incident,
d) the extent of the disruption to the functioning of the digital service,
e) the extent of impact of the significant incident on economic and societal activities;

5) information enabling the competent CSIRT MON, CSIRT NASK or CSIRT GOV to determine whether the significant incident affects two or more European Union Member States;
6) information about the cause and nature of the significant incident;
7) information on preventive actions taken;
8) information on the remedial actions taken;
9) other relevant information.

2. The digital service provider shall provide information, available for the provider at the time of notification, , which shall be complemented when handling the significant incident.

3. The digital service provider shall, as necessary, provide in the notification referred to in Article 18 paragraph 1 subparagraph 4, information constituting legally protected secrets, including business secrets, if this is necessary to perform tasks by the competent CSIRT MON, CSIRT NASK or CSIRT GOV.

4. The competent CSIRT MON, CSIRT NASK or CSIRT GOV may request the digital service provider to supplement the notification with information, including information constituting legally protected secrets, as necessary to perform the tasks referred to in the Act.

5. Digital service providers shall mark in the notification the information constituting legally protected secrets, including business secrets.

Article 20. The digital service provider may provide information referred to in Article 13, paragraph 1 to the competent CSIRT MON, CSIRT NASK or CSIRT GOV. The information shall be submitted electronically or by using other available means of communication, when it is impossible to provide it in an electronic form.

Chapter 5

Responsibilities of public entities

Article 21. 1. The public entity referred to in Article 4, items 7 to 15, which perform a public task relying on the information system, is obliged to appoint a person responsible for contacting the entities of the national cybersecurity system.

2. A public administration authority may designate one person responsible for contacting entities of the national cybersecurity system in terms of public tasks relying on information systems, fulfilled by its subordinate units or units supervised by it.

3. A unit of local government may designate one person responsible for contacting entities of the national cybersecurity system in terms of public tasks relying on information systems, fulfilled by its organisational units.

Article 22. 1. The public entity referred to in Article 4, items 7 to 15, which performs a public task relying on the information system shall:

1) ensure incident management within the public entity;
2) report an incident at the public entity and the critical incident without undue delay , however not later than within 24 hours from its detection, to the competent CSIRT MON, CSIRT NASK or CSIRT GOV;
3) provide handling of an incident at the public entity in collaboration with the competent CSIRT MON, CSIRT NASK or CSIRT GOV, providing the necessary data, including personal data;
4) provide an access to the knowledge which allow to understand cybersecurity threats and the use of effective ways to protect from those threats the persons for whom the public task is carried out, in particular by publishing relevant information on its website;
5) provide the competent CSIRT MON, CSIRT NASK, or CSIRT GOV with data of the person referred to in Article21, including forename and surname, telephone number and e-mail address, within 14 days from the date of his or her appointment, and information about the modification of those details – within 14 days from the date of their change.

2. The notification referred to in paragraph 1 item 2, shall be submitted electronically or by using other available means of communication, when it is impossible to provide it in an electronic form.

Article 23. 1. The notification referred to in Article 22 paragraph 1 item 2 must provide the following information:

1) details of the notifying entity, including the name of the entity, number in the relevant register, registered office and address;
2) forename and surname, telephone number and e-mail address of the person reporting the notification;
3) forename and surname, telephone number and e-mail address of the person entitled to provide explanations regarding the information reported;
4) an assessment of the impact of the incident at the public entity on the public task being carried out, including:
   a) the public task affected by the incident,
   b) the number of those affected by the incident,
   c) the time the incident occurred and detected and the duration of the incident,
   d) the geographic spread with regard to the area that could be affected by an incident ,
   e) cause of the occurrence of the incident and the manner of its course, and the effects of its impact on information systems of the public entity;
5) information about the cause and nature of the incident;
6) information on preventive actions taken;
7) information on the remedial actions taken;
8) other relevant information.

2. The public entity referred to in Article 4, items 7 to 15, shall provide information, available for the entity at the time of notification, which shall be complemented by the entity while handling the incident in the public entity.

3. The public entity referred to in Article 4, items 7 to 15, shall, as necessary, provide in the notification referred to in Article 22 paragraph 1 item 2, information constituting legally protected secrets, including business secrets, if this is necessary to perform tasks by the competent CSIRT MON, CSIRT NASK or CSIRT GOV.

4. The competent CSIRT MON, CSIRT NASK or CSIRT GOV may request the public entity referred to in Article 4, items 7 to 15, to supplement the notification with information, including information constituting legally protected secrets, as necessary to perform the tasks referred to in the Act.

5. In the notification, the public entity referred to in Article 4, items 7 to 15, shall mark the information constituting legally protected secrets, including business secrets.

Article 24. The public entity referred to in Article 4, items 7 to 15, which performs public tasks relying on the information system, may provide the competent CSIRT MON, CSIRT NASK or CSIRT GOV with information referred to in Article13, paragraph 1. The information shall be submitted electronically or by using other available means of communication, when it is impossible to provide it in an electronic form. **Article 25.** To the public entity referred to in Article 4, items 7 to 15, with regard to whom a decision on declaring as an operator of essential service was issued, the provisions of Chapter 3 shall apply to the extent covering the provision of the essential service, for which it was declared as an operator of essential service. .

Chapter 6

Tasks of CSIRT MON, CSIRT NASK and CSIRT GOV

Article 26. 1. CSIRT MON, CSIRT NASK and CSIRT GOV shall act together with the competent authorities for cybersecurity matters, the minister competent for digitalisation and the Plenipotentiary, by ensuring a coherent and comprehensive risk management system at the national level, carrying out tasks to counteract cybersecurity threats of a cross-sectoral and cross-border nature, and by ensuring the coordination of handling reported incidents.

2. In reasonable cases , CSIRT MON, CSIRT NASK and CSIRT GOV, at the request of operators of essential services, digital service providers, public entities referred to in Article 4, items 7 to 15, sectoral cyber-security teams, or owners, independent holders or dependent holders of facilities, installations, devices or services included in the critical infrastructure listed in Article 5b, paragraph 7, subparagraph 1 of the Act of 26 April 2007 on crisis management, may provide support in handling the incidents.

3. The tasks of CSIRT MON, CSIRT NASK and CSIRT GOV, in accordance with the scope of jurisdiction referred to in paragraphs 5 to 7, shall include:

1) monitoring cybersecurity threats and incidents at the national level;
2) estimating the risk related to cybersecurity threats and incidents identified, including conducting a dynamic risk analysis;
3) sharing information on incidents and risks to entities of the national cybersecurity system;
4) disseminating of information on identified cybersecurity threats;
5) responding to reported incidents;

6) classifying the incidents as critical, including serious incidents and significant incidents, and coordinating of handling critical incidents;
7) modifying the classification of serious incidents and significant incidents;
8) submitting to the competent CSIRT MON, CSIRT NASK or CSIRT GOV technical information on incidents requiring CSIRT's cooperation for the coordination of their handling;
9) carrying out, in justified cases, testing of IT equipment or software to identify vulnerabilities, the use of which may pose a threat, especially to integrity, confidentiality, accountability, authenticity or availability of processed data, which may affect public security or a key security interest of the state, and submitting requests for recommendations for entities of the national cybersecurity system regarding the use of IT equipment or software, in particular in terms of impact on public security or a key security interest of the state, hereinafter referred to as the "recommendations regarding the use of IT equipment or software";
10) cooperation with sectoral cybersecurity teams in the field of coordinating the handling of serious incidents, including those affected two or more European Union Member States, and critical incidents, as well as information sharing with the aim to counter cybersecurity threats;
11) sending to and receiving from other countries, including the European Union Member States, information on serious incidents and significant incidents affected two or more Member States, and notifying the Single Point of Contact of serious and significant incidents affected two or more Member States of the European Union;
12) submitting to the Single Point of Contact, by 30 May each year, by the operators of essential services a list of serious incidents affecting the continuity of their provision of essential services in the Republic of Poland and the continuity of essential services provided by them in the European Union Member States reported in the previous calendar year , and submitting, by digital service providers, a list of significant incidents reported in the previous calendar year, including those affected two or more Member States of the European Union;
13) jointly developing of the cybersecurity-related part of the Report on threats to national security, referred to in Article 5a, paragraph 1 of the Act of 27 April 2007 on crisis management and submitting it to the minister competent e for digitalisation;
14) providing analytical and R&D facilities, including in particular:

a) conducting advanced malware and vulnerability analysis,
b) monitoring cybersecurity threat indicators,
c) developing tools and methods to detect and counter cybersecurity threats,
d) conducting analyses and developing standards, recommendations and good practices in the field of cybersecurity,
e) supporting entities of the national cybersecurity system in building potential and capabilities in the area of cybersecurity,
f) conducting awareness-raising activities in the area of cybersecurity,
g) cooperating in the field of educational solutions in cybersecurity;

15) ensuring the possibility of submitting notifications and providing information referred to in Article 11 paragraph 1 subparagraph 4, Article 13 paragraph 1, Article 18 paragraph 1 subparagraph 4, Article 20, Article 22 paragraph 1 subparagraph 2, Article 24 and Article 30 subparagraph 1, and providing and handling means of communication allowing for such notifications;
16) participating in the CSIRT Network composed of representatives of CSIRTs of the European Union Member States, the competent CSIRT for the European Union institutions, the European Commission, and the European Union Agency for Network and Information Security (ENISA).

4. CSIRT MON, CSIRT NASK and CSIRT GOV shall jointly develop the principles of incident handling procedures, whose coordination requires CSIRT's cooperation, and shall determine, in cooperation with sectoral cybersecurity teams, the manner of interacting between those teams, including the manner of incident handling coordination.

5. The tasks of the CSIRT MON include the coordination of handling the incidents reported by:

1) entities subordinate to or supervised by the Minister of National Defence, including entities whose ICT systems or ICT networks are covered by a single list of facilities, installations, devices and services included in the critical infrastructure referred to in Article 5b, paragraph 7, subparagraph 1 of the Act of 26 April 2007 on crisis management;
2) companies of significant importance in terms of economy and defence, for whom the authority organising and supervising their performance of tasks for the defence of the state within the meaning of Article 5, subparagraph 3 of the Act of 23 August 2001 on organising tasks for the defence of the state implemented by entrepreneurs

(Journal of Laws of the Republic of Poland, items 1320 and of 2002, item 1571) is the Minister of National Defence.

6. The tasks of CSIRT NASK include:

1) coordination of handling the incidents reported by:
   a) public finance sector entities referred to in Article 9, subparagraphs 2 to 6, 11 and 12 of the Act of 27 August 2009 on public finance,
   b) entities subordinate to or supervised by central government administration authorities , with the exception of entities referred to in paragraph 7, item 2,
   c) research institutes,
   d) Urząd Dozoru Technicznego (Office of Technical Supervision),
   e) Polska Agencja Żeglugi Powietrznej (Polish Air Navigation Services Agency),
   f) Polskie Centrum Akredytacji (Polish Centre for Accreditation),
   g) Narodowy Fundusz Ochrony Środowiska i Gospodarki Wodnej (National Fund for Environmental Protection and Water Management) and regional funds for environmental protection and water management,
   h) commercial law companies performing public utility tasks as defined in Article 1 item 2 of the Act of 20 December 1996 on municipal services management,
   i) digital service providers, except for those mentioned in paragraph 7 item 5,
   j) operators of essential services , except for those mentioned in paragraphs 5 and 7,
   k) entities other than those mentioned in items a to j and paragraphs 5 and 7,
   l) natural persons;
2) creating and sharing tools for voluntary cooperation and information exchange on cybersecurity threats and incidents;
3) providing the support of telephone or web helpline operating in the field of reporting and analysis of cases of distribution, dissemination or transmission of child pornography via ICT referred to in Directive 2011/92/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and 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. The tasks of CSIRT GOV include the coordination of handling the incidents reported by:

1) public finance sector entities referred to in Article 9, items 1, 8 and 9 of the Act of 27 August 2009 on public finance, except those referred to in paragraphs 5 and 6;

2) entities subordinate to or supervised by the President of the Council of Ministers;

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

4) Bank Gospodarstwa Krajowego (National Development Bank);

5) other entities than listed in items 1 to 4 and paragraph 5, whose ICT systems or ICT networks are covered by a single list of facilities, installations, devices and services included in the critical infrastructure referred to in Article 5b, paragraph 7, subparagraph 1 of the Act of 26 April 2007 on crisis management;

6) entities referred to in paragraph 6, if the incident affects ICT systems or ICT networks covered by a single list of facilities, installations, devices and services included in the critical infrastructure referred to in Article 5b, paragraph 7, item 1 of the Act of 26 April 2007 on crisis management;

8. The CSIRT MON, CSIRT NASK or CSIRT GOV, which received an incident report, but is not competent to coordinate its handling, must without undue delay forward that notification to the competent CSIRT together with the information received.

9. The operational of CSIRT NASK shall be funded in the form of a specified-user subsidy from the part of the state budget assigned to the minister competent for digitalisation.

10. CSIRT MON, CSIRT NASK and CSIRT GOV may, by mutual agreement, entrust each other with the performance of tasks with regard to the certain types of entities referred to in paragraphs 5 to 7. The CSIRT that entrusted to another CSIRT, in a mutual agreement, the performance of tasks, shall inform the entities in respect of which the CSIRT has changed.

11. An announcement on the conclusion of the agreement referred to in paragraph 10 shall be published in the official journal of the Minister of National Defence, the Minister of Digital Affairs or the Internal Security Agency respectively. The announcement shall indicate information about:

1) the website address where the contents of the agreement is to be posted together with the attachments constituting the whole of the agreement;

2) the date from which the agreement starts to be effective.

Article 27. 1. CSIRT GOV shall be competent for incidents related to terrorist events, referred to in Article 2 subparagraph 7 of the Act of 10 June 2016 on counter-terrorism activities (Journal of Laws the Republic of Poland of of 2018, items 452, 650 and 730).

2. CSIRT MON shall be competent for incidents related to terrorist events, referred to in Article 5 paragraph 1 item 2a of the Act of 9 June 2006 on the Military Counterintelligence Service and the Military Intelligence Service (Journal of Laws of the Republic of Poland of 2017, items 1978 and of 2018, item 650).

3. If it is found that the incident, the handling of which is coordinated by the competent CSIRT MON, CSIRT NASK or CSIRT GOV, is related to the events referred to in paragraphs 1 or 2, the coordination of handling the incident shall be taken over by the competent CSIRT MON or CSIRT GOV.

Article 28. 1. The competent CSIRT MON, CSIRT NASK or CSIRT GOV, based on the report of a serious incident reported by the operator of essential service, shall notify, via the Single Point of Contact, other European Union Member States affected by the incident.

2. If circumstances so permit, the competent CSIRT MON, CSIRT NASK or CSIRT GOV shall forward to the operator of essential service which reported a serious incident the information about the action taken after reporting the incident, that could be helpful in handling it.

3. The competent CSIRT MON, CSIRT NASK or CSIRT GOV may request the Single Point of Contact for forwarding the serious incident notification referred to in paragraph 1, to single points of contact in other European Union Member States affected by the incident.

Article 29. CSIRT MON, CSIRT NASK or CSIRT GOV shall notify other Member States of the European Union via the Single Point of Contact if the significant incident affects two or more European Union Member States.

Article 30. 1. Other entities than operators of essential services and digital service providers, including natural persons, may report an incident to CSIRT NASK. The notification should include:

1) the name of the entity or information system in which the incident has occurred;
2) description of the incident;
3) other relevant information.

2. Notifications of incidents from operators of essential services and digital service providers shall be prioritized over those referred to in paragraph 1.

3. The notifications referred to in paragraph 1 may be considered if it does not constitute a disproportionate or excessive burden for CSIRT NASK.

4. The entity referred to in paragraph shall mark in the notification the information constituting legally protected secrets, including business secrets.

Article 31. 1. CSIRT MON, CSIRT NASK and CSIRT GOV shall define the method of making notifications and providing information in electronic form, as referred to in Article 11 paragraph 1 subparagraph 4, Article 13 paragraph 1, Article 18 paragraph 1 subparagraph 4, Article 20, Article 22 paragraph 1 subparagraph 2, Article 24 and Article 30 paragraph 1, and shall also define the method of making notifications and providing information using other means of communication when it is impossible to submit or forward it in electronic form.

2. The announcement containing the information referred to in paragraph 1 shall be published by CSIRT MON, CSIRT NASK and CSIRT GOV on the Public Information Bulletin websites of the Minister of National Defence, Research and Academic Computer Network – State Research Institute, or 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 a serious, significant or critical incident.

2. During the coordination of handling a serious, significant or critical incident, CSIRT MON, CSIRT NASK or CSIRT GOV may request the competent authority for cybersecurity matters to request the operator of essential service or digital service provider to remove within the prescribed period the vulnerabilities that led or could lead to a serious, significant or a critical incident.

3. CSIRT MON, CSIRT NASK or CSIRT GOV may request directly the operator of essential service to disclose technical information related to a serious or critical incident that will be necessary to analyse or coordinate such an incident.

4. CSIRT MON, CSIRT NASK, CSIRT GOV or sectoral cybersecurity teams, based on the information referred to in Article 13, paragraph 1, items 3 and 5, obtained from the operator of essential service, digital service provider or public entity referred to in Article 4, items 7to 15, may provide them with information on vulnerabilities and the method of removing the vulnerabilities in the technologies being used.

Article 33. 1. CSIRT MON, CSIRT NASK or CSIRT GOV may test IT equipment or software to identify vulnerabilities, the use of which may put at risk, in particular, the integrity, confidentiality, accountability, authenticity or availability of data processed, which may affect public security or a key security interest of the State.

2. When undertaking to test IT equipment or software, CSIRT MON, CSIRT NASK or CSIRT GOV shall inform other CSIRTs about the fact of commencing the test and about the IT equipment or software being tested.

3. Where a vulnerability referred to in paragraph 1 is found, CSIRT MON, CSIRT NASK or CSIRT GOV shall submit a request on recommendations referred to in paragraph 4.

4. The Plenipotentiary, having consulted the Cybersecurity Committee, shall issue, amend or cancel recommendations regarding the use of IT equipment or software, in particular as regards impact on public security or a key security interest of the State.

5. The entities of the national cybersecurity system may provide objections to the recommendations regarding the use of IT equipment due to their negative impact on the service provided or the public task carried out to file with the Plenipotentiary, not later than within 7 days from the day of receiving the recommendation.

6. The Plenipotentiary shall consider the objections received under paragraph 5 without undue delay, but not later than within 14 days from the date of their receipt and shall either maintain the recommendations regarding the use of IT equipment or software, or issue revised recommendations.

7. The entities of the national cybersecurity system shall notify the Plenipotentiary, at a request of the Plenipotentiary, about the manner and scope of taking into account recommendations regarding the use of IT equipment or software.

8. Failure to take into account recommendations regarding the use of IT equipment or software forms the basis for the Plenipotentiary to request the authority supervising the entity referred to in paragraph 7 with information that the recommendations have not been applied. .

Article 34. 1. CSIRT MON, CSIRT NASK, CSIRT GOV and sectoral cybersecurity teams, as well as entities providing services in the field of cybersecurity, shall cooperate with law enforcement agencies and judicial institutions and with Intelligence agencies in the implementation of their statutory tasks.

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

Article 35. 1. CSIRT MON, CSIRT NASK and CSIRT GOV shall inform each other about critical incidents and inform the Government Centre for Security about it.

2. The information referred to in paragraph 1 shall contain:

1) a preliminary analysis of possible effects of the incident, including in particular:
   a) the number of users affected by the incident, especially if it disturbs the provision of the essential service,
   b) the time the incident occurred and detected and the duration of the incident,
   c) the geographic spread with regard to the area that could be affected by an incident,
2) recommendation regarding the convening of the Government Crisis Management Team, referred to in Article 8 paragraph 1 of the Act of 26 April 2007 on crisis management.

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

4. Where information about cybersecurity threats is obtained, CSIRT MON, CSIRT NASK and CSIRT GOV may inform each other and inform the Government Centre for Security about those threats. Provisions of paragraphs 2 and 3 shall apply accordingly.

5. CSIRT MON, CSIRT NASK and CSIRT GOV may publish on the Public Information Bulletin websites of the Minister of National Defence, Research and Academic Computer Network - State Research Institute or the Internal Security Agency respectively, to the extent necessary, notices on vulnerabilities, critical incidents and cybersecurity threats, provided that posting the information will increase the cybersecurity of information systems used by the public and businesses or ensure safe use of these systems. The information so published may not violate the 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 for the matters of handling critical incidents reported to CSIRT MON, CSIRT NASK or CSIRT GOV, and coordinating activities undertaken by CSIRT MON, CSIRT NASK, CSIRT GOV and the Government Centre for Security..

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

3. The Director of the Government Centre for Security shall preside over the work of the Team.

4. The work of the Team shall be supported by the Government Centre for Security.

5. Team members may invite representatives of the competent authorities for cyber-security matters or their subordinate or supervised entities, law enforcement agencies, justice or Intelligence agencies to participate in the work of the Team in an advisory capacity.

6. Having received the information referred to in Article 35 paragraph 1, the Director of the Government Centre for Security , in the case referred to in Article 35 paragraph 3, or at the request of a Team member, or on Director's own initiative, shall without undue delay notify Team members of the date and place of the Team's meeting. Participation in the Team meeting may take place via electronic means of communication.

7. At the meeting, the Team shall:

1) unanimously designates one CSIRT to coordinate the handling of the incident covered by the information referred to in Article 35 paragraph 1;
2) defines the roles of the other CSIRTs and the Government Centre for Security in the handling of the incident covered by the information referred to in Article 35 paragraph 1;
3) defines the method of sharing technical information on the critical incident handled jointly by CSIRT MON, CSIRT NASK or the Head of the Internal Security Agency performing tasks under the CSIRT GOV;
4) takes a decision whether the Director of the Government Centre for Security is to apply to the President of the Council of Ministers for the convening of the Government Crisis Management Team;
5) in the case of a critical incident that may cause a terrorist threat concerning ICT systems of public administration bodies or ICT systems forming part of the critical infrastructure referred to in Article 15 paragraph 2 of the Act of 10 June 2016 on counter-terrorism activities, shall prepare for the minister competent for internal affairs and the Head of the Internal Security Agency information and conclusions concerning such an incident.

Chapter 7

Rules for sharing information and processing personal data

Article 37. 1. The Act of 6 September 2001 on access to public information (Journal of Laws of the Republic of Poland of 2016, item 1764 and of 2017, item 933) shall not

be used to provide information on vulnerabilities, incidents and threats to cybersecurity and the risk of incidents.

2. Where it is necessary to prevent the serious incident from occurring or to provide serious incident handling, the competent CSIRT MON, CSIRT NASK or CSIRT GOV , having consulted the notifying the operator of essential service , may publish information on serious incidents on the Public Information Bulletin website of the Minister of National Defence, Research and Academic Computer Network-National Research Institute or Internal Security Agency respectively.

3. Competent CSIRT MON, CSIRT NASK or CSIRT GOV, having consulted the notifying digital service provider, may publish information on significant incidents on the Public Information Bulletin website of the Minister of National Defence, Research and Academic Computer Network-National Research Institute or Internal Security Agency respectively, or request the competent authority for cybersecurity for the digital service provider to cause the digital service provider to publish this information, where it is necessary to prevent the incident from occurring or to provide incident handling, or where disclosing the incident is in the public interest for other reasons,

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

Article 38. Information processed pursuant to the Act shall not be disclosed if the disclosure would violate protection of the public interest with respect to security or public order, and would adversely affect the conduct of pre-trial proceedings in respect of crimes, their detection and prosecution.

Article 39. 1. In order to perform the tasks referred to in Article 26 paragraph 3 items 1 to 11, 14 and 15 and paragraphs 5 to 8 and Article 44 paragraphs 1 to 3, CSIRT MON, CSIRT NASK, CSIRT GOV and sectoral cybersecurity teams shall process data acquired in connection with cybersecurity incidents and threats, including personal data, which covers also the data specified 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) (O J EU L 119 of 04.05.2016, p. 1), hereinafter referred to as "Regulation 2016/679", to the extent and for the purposes as necessary to carry out these tasks.

2. CSIRT MON, CSIRT NASK and sectoral cybersecurity teams, when processing personal data specified in Article 9(1) of Regulation 2016/679, shall conduct a risk analysis, apply anti-malware protection measures and access control mechanisms, and shall develop procedures for the secure sharing of information.

3. CSIRT MON, CSIRT NASK, CSIRT GOV and sector cybersecurity teams shall process the following personal data acquired in connection with cybersecurity incidents and threats:

1) regarding users of information systems and users of telecommunication end-points devices;
2) regarding end-point devices within the meaning of Article 2 item 43 of the Act of 16 July 2004 – Telecommunications law;
3) collected by operators of essential services and digital service providers in connection with the provision of services;
4) collected by public entities in connection with the implementation of public tasks, regarding entities reporting incidents in accordance with Article 30 paragraph 1.

4. To perform the tasks specified in the Act, the Minister competent for digitalization , the Director of the Government Centre for Security , the Plenipotentiary and the competent authorities for cybersecurity matters shall process the following personal data obtained in connection with cybersecurity incidents and threats:

1) collected by operators of essential services and digital service providers in connection with the provision of services;
2) collected by public entities in connection with the implementation of public tasks;
3) regarding entities reporting the incident pursuant to Article 30 paragraph 1.

5. The data referred to in paragraphs 3 and 4 shall be removed or anonymised by CSIRT MON, CSIRT NASK and the sectoral cybersecurity team without undue delay upon finding that they are not necessary to perform the tasks referred to in Article 26 paragraph 3 items 1 to 11, 14 and 15, and paragraphs 5 to 8, and Article 44 paragraphs 1 to 3.

6. The data referred to in paragraphs 3 and 4, which are necessary to perform the tasks referred to in Article 26 paragraph 3 subparagraphs 1 to 11, 14 and 15, and paragraphs 5 to 8, and Article 44 paragraphs 1 to 3, shall be removed or anonymised by CSIRT MON, CSIRT NASK and the sectoral cybersecurity team within 5 years from the end of handling the incident they concern.

7. In order to perform the tasks specified in the Act, CSIRT MON, CSIRT NASK, CSIRT GOV and sectoral cybersecurity teams may share with each other the data referred to in paragraph 3 to the extent necessary to perform these tasks, and cooperate with the authority competent for the protection of personal data.

8. The processing of data referred to in paragraph 3 by CSIRT MON, CSIRT NASK and sectoral cybersecurity teams does not require fulfilment of the obligations resulting from Article 15, Article 16, Article 18(1)(a) and (d), and Article 19, second sentence, of Regulation 2016/679, if it would prevent the implementation by CSIRT NASK, CSIRT MON and sectoral cybersecurity teams of the tasks referred to in Article 26(3) items 1-11, 14 and 15 and Article 25 (5) to (8), and Article 44(1) to (3), and it is possible when CSIRT MON, CSIRT NASK and sector cybersecurity teams conduct risk analysis, apply anti-malware protection measures, apply access control mechanisms and develop procedures for secure information sharing.

9. CSIRT MON, CSIRT NASK and sectoral cybersecurity teams shall publish the following information on their websites:

1) contact details of the personal data controller and, where applicable, contact details of the personal data protection officer;
2) purposes of processing and the legal basis for processing;
3) categories of personal data processed;
4) information about recipients of personal data;
5) information on the personal data retention period;
6) information on restrictions on the obligations and rights of data subjects;
7) information on the right to file a complaint to the authority competent for the protection of personal data;
8) source of personal data.

Article 40. 1. CSIRT MON, CSIRT NASK, CSIRT GOV, sectoral cybersecurity teams and the minister competent for digitalisation shall process information constituting legally protected secrets, including that constituting company secrets, when it is necessary for the implementation of tasks referred to in the Act.

2. CSIRT MON, CSIRT NASK, CSIRT GOV and sectoral cybersecurity teams shall provide the information referred to in paragraph 1 to law enforcement agencies in connection with an incident that meets the criteria of an offence.

3. CSIRT MON, CSIRT NASK, CSIRT GOV and sectoral cybersecurity teams are obliged to keep confidentiality of information obtained in connection with the

implementation of tasks referred to in the Act. including information constituting legally protected secrets.

Chapter 8

The competent authorities for cybersecurity matters

Article 41. The competent authorities for cybersecurity matters include:

1) for the energy sector – the minister competent for energy matters;
2) for the transportation sector, excluding the water transport sub-sector – the minister competent for transportation matters;
3) for the water transport sub-sector – the minister competent for maritime economy and the minister competent for inland waterway transport;
4) for the banking sector and financial market infrastructure – KNF - Polish Financial Supervision Authority;
5) for the health sector, excluding the entities referred to in Article 26 paragraph 5 – the minister competent for health matters;
6) for the health sector covering the entities referred to in Article 26 paragraph 5 – Minister of National Defence;
7) for the drinking water supply and distribution sector – the minister competent for water management;
8) for the digital infrastructure sector, excluding the entities referred to in Article 26 paragraph 5 – the minister competent for digitalisation;
9) for the digital infrastructure sector covering entities referred to in Article 26 paragraph 5 – Minister of National Defence;
10) for digital service providers, excluding the entities referred to in Article 26 paragraph 5 –the minister competent for digitalisation;
11) for digital service providers covering the entities referred to in Article 26 paragraph 5 – Minister of National Defence.

Article 42. 1. The competent authorities for cybersecurity matters shall:

1) conduct ongoing analysis of entities in a given sector or sub-sector in terms of considering them either as an operator of essential service or as non-compliant with the conditions qualifying the entity as key service provider;
2) issue decisions on declaring the entity as an operator of essential service , or decisions confirming the expiry of the decision on declaring the entity as an operator of essential service;

3) without undue delay upon the decision on declaring the entity as an operator of essential service or the decision confirming the expiry of the decision on declaring the entity as an operator of essential service , shall submit applications to the minister competent for digitalisation to write an entity in or delay an entity from the list of operators of essential services;
4) submit applications for the change of data in the list of operators of essential services, not later than within 6 months from the change of these data;
5) prepare, in cooperation with CSIRT NASK, CSIRT GOV, CSIRT MON and sector-specific cybersecurity teams, recommendations on actions aimed at strengthening cybersecurity, including sectoral guidelines on incident reporting;6) monitor the application of the provisions of the Act by operators of essential services and digital service providers;
7) require key service providers or digital service providers, at the request of CSIRT NASK, CSIRT GOV or CSIRT MON, to remove within the prescribed period the vulnerabilities that led or could led to a serious, significant or critical incident;
8) conduct inspections of the operators of essential services and digital service providers;
9) may cooperate with the competent authorities of the European Union Member States via the Single Point of Contact;
10) process information, including personal data, about the essential and digital services being provided and operators of essential services or digital service providers to the extent necessary to perform the tasks under the Act;
11) participate in cybersecurity exercises held in the Republic of Poland or in the European Union.

2. Where a legal person or an organisational unit without legal personality, providing digital services, does not have its registered office or management in the territory of 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 territory of the Republic of Poland; or where it does not meet the requirements specified in the Regulation 2018/151, the competent authority for cybersecurity matters for digital service providers may provide information and require taking the action referred to in Article 53 paragraph 2 to a competent authority in another Member State of the European Union, in the territory of which the entity has its registered office or management or its representative has been appointed.

3. The competent authority for cybersecurity matters may entrust the implementation, on its behalf, of certain tasks referred to in paragraph 1, to entities subordinated to or supervised by the authority.

4. The tasks shall be entrusted under an agreement between the competent authority for cybersecurity matters and the entities referred to in paragraph 3.

5. The agreement referred to in paragraph 4 shall comprise rules allowing the competent authority for cybersecurity matters to control the proper performance of the tasks entrusted.

6. An announcement about the agreement shall be published in the official journal of the competent authority for cybersecurity matters. The communication shall indicate information about:

1) the website address where the contents of the agreement is to be posted together with the attachments constituting the whole of the agreement;
2) the date from which the agreement starts to be effective.

7. The competent authorities for cybersecurity matters and the Single Point of Contact shall cooperate, in justified cases, with law enforcement agencies and the authority competent for the protection of personal data.

8. Recommendations regarding actions aimed at strengthening cybersecurity, including sectoral guidelines for reporting incidents referred to in paragraph 1, item 5, shall be prepared taking into account, in particular, the Polish Standards transferring European standards, common technical specifications, understood as technical specifications of ICT products determined in accordance with Articles 13 and 14 of Regulation (EU) No 1025/2012 of the European Parliament and of the Council of 25 October 2012 on European standardisation, amending Council Directives 89/686/EEC and 93/15/EEC and Directives 94/9/EC, 94/25/EC, 95/16/EC, 97/23/EC, 98/34/EC, 2004/22/EC, 2007/23/EC, 2009/23/EC and 2009/105/EC of the European Parliament and of the Council and repealing Council Decision 87/95/EEC and Decision No 1673/2006/EC of the European Parliament and of the Council (OJ 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 cybersecurity matters may, without starting proceedings on declaring an entity as an operator of essential service , request the entity referred to in Annex 1 to the Act to provide information that will allow an initial

assessment of whether the entity meets the conditions to be considered as an operator of essential service.

2. The competent authority for cybersecurity matters may, without starting of an inspection , request the operator of essential service to provide information that will allow the determination of the need to conduct the inspection , and also may, without starting proceedings, request the operator of essential service to provide information that will allow initial assessment, whether the entity ceased to meet the conditions to be considered as an operator of essential service..

3. The competent authority for cybersecurity matters, when requesting the entity referred to in Annex 1 to the Act or an operator of essential service, shall indicate the deadline for providing information. The deadline may not be shorter than 14 days from the date of receipt of the request by the entity or the operator of essential service..

4. The entity referred to in Annex 1 to the Act, or the operator of essential service requested by the competent authority for cybersecurity matters, may provide information in the case covered by the request or inform about the refusal to provide information.

5. The request for information and the lack of information does not affect the possibility of initiating administrative proceedings or inspections..

6. The information provided by the entity or operator of essential service, referred to in paragraphs 1 and 2, may constitute evidence in the course of administrative proceedings or inspections. The lack of information does not affect the party's or inspected entity's legal situation or the administrative proceedings or inspections.

Article 44. 1. The competent authority for cybersecurity matters may establish, in accordance with separate provisions, a sectoral cybersecurity team for a given sector or sub-sector listed in Annex No. 1 to the Act, in particular responsible for:

1) receiving notifications of serious incidents and supporting in handling these incidents;
2) supporting operators of essential services in performing the duties set out in Article 8, Article 9, Article 10 paragraphs 1 to 3, Article 11 paragraphs 1 to 3, Article 12 and Article 13;
3) analysing serious incidents, searching for links between incidents, and writing conclusions for incident handling;
4) cooperation with the competent CSIRT MON, CSIRT NASK and CSIRT GOV in the field of coordinating the handling of serious incidents.

2. The sectoral cybersecurity team may send to other countries, including European Union Member States, and receive from these countries information on serious incidents, including those concerning two or more European Union Member States.

3. The sectoral cybersecurity team may receive notifications of serious incidents from another EU Member State regarding two or more European Union Member States. The sectoral cybersecurity team shall forward these notifications to the competent CSIRT MON, CSIRT NASK or CSIRT GOV and the Single Point of Contact.

4. Where a sectoral cybersecurity team is established, the competent authority for cybersecurity matters shall inform operators of essential services in a given sector, as well as CSIRT MON, CSIRT NASK and CSIRT GOV, about the establishment of this team and the scope of its tasks.

Chapter 9

Tasks of the minister competent for digitalisation

Article 45. 1. The minister competent for digitalisation shall be responsible for:

1) monitoring the implementation of the Polish National Cybersecurity Strategy, hereinafter referred to as the "Strategy", and performance of action plans for its implementation;
2) recommending areas of cooperation with the private sector in order to increase the cybersecurity of the Republic of Poland;
3) developing annual reports on:
   a) serious incidents reported by operators of essential services affecting the continuity of essential services provided by them in the Republic of Poland and the continuity of essential services provided in European Union Member States,
   b) significant incidents reported by digital service providers, including incidents involving two or more European Union Member States;
4) conducting awareness activities regarding good practices, educational programmes, campaigns and trainings for the expanding of knowledge and raising the awareness in the field of cybersecurity, including the safe use of the Internet by various categories of users;
5) collecting information about serious incidents that concern or have been passed by another European Union Member State;

6) sharing information and good practices related to reporting serious incidents by operators of essential services and significant incidents by digital service providers, obtained from the Cooperation Group, including:
   a) incident management procedures,
   b) risk management procedures,
   c) classification of information, risk and incidents.

2. The Cooperation Group shall mean the group referred to in the Commission Implementing Decision 2017/179 of 1 February 2017 laying down procedural arrangements necessary for the functioning of the Cooperation Group pursuant to Article 11(5) of the Directive (EU) 2016/1148 of the European Parliament and of the Council concerning measures for a high common level of security of network and information systems across the Union (OJ EU L 28 of 02.02.2017, p. 73).

Article 46. 1. The minister competent for digitalisation shall ensure the development or maintenance of an ICT system supporting:

1) cooperation of entities being part of the national cybersecurity system;
2) generating and passing recommendations on activities to raise the level of cybersecurity;
3) incident reporting and handling;
4) risk assessment at the national level;
5) warning about cybersecurity threats.

2. CSIRT MON, CSIRT NASK, CSIRT GOV, sector cybersecurity teams and the President of the Office of Electronic Communications may use the ICT system under an agreement with the minister competent for digitalisation.

3. The agreement shall set out the scope and terms of use of the ICT system.

Article 47. 1. The minister competent for digitalisation may perform the tasks referred to in Article 45 paragraph 1 and Article 46 paragraph 1, on the terms set out in separate regulations, by means of relevant subordinated entities or those supervised by the minister competent for digitalisation.

2. Tasks entrusted to the entities referred to in paragraph 1 shall be financed in the form of a special-purpose subsidy from the part of the state budget assigned to the minister competent for digitalisation..

Article 48. The minister competent for digitalisation shall run the Single Point of Contact, whose tasks include:

1) receiving notifications of serious incidents or incidents relevant for two or more European Union Member States from single points of contact in other European Union Member States, and forwarding such notifications to CSIRT MON, CSIRT NASK, CSIRT GOV or sectoral cybersecurity teams;
2) forwarding, upon the request of the competent CSIRT MON, CSIRT NASK or CSIRT GOV, notifications of serious incidents or incidents relevant for two or more European Union Member States to ingle points of contact in other European Union Member States;
3) ensuring representation of the Republic of Poland in the Cooperation Group;
4) ensuring cooperation with the European Commission in the field of cybersecurity;
5) coordination of cooperation between the competent authorities for cybersecurity matters and public authorities in the Republic of Poland with relevant competent authorities in the European Union Member States;
6) ensuring information sharing for the needs of the Cooperation Group and the CSIRT Network.

Article 49. 1. The Single Point of Contact shall forward the following to the Cooperation Group:

1) the information referred to in Article 45 paragraph 1 subparagraph 3;
2) good practices referred to in Article 45 paragraph 1 subparagraph 4, related to incident reporting;
3) proposals for the agenda of the Cooperation Group;
4) national good practices regarding awareness raising, training, research and development in the field of cybersecurity;
5) good practices regarding identification of operators of essential services, including links concerning risks and incidents in two or more European Union Member States.

2. The data forwarded to the Cooperation Group shall not include information concerning national security and public order.

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

1) assessment of national strategies of European Union Member States in the field of cybersecurity and the effectiveness of CSIRT, and good practices in the field of cybersecurity;

2) actions taken with regard to cyber-security exercises , European educational and training programmes, including the activities of the European Union Agency for Network and Information Security (ENISA);
3) strategic guidelines regarding the activities of the CSIRT Network;
4) good practices in the European Union concerning information sharing related to the reporting of serious incidents by operators of essential services and significant incidents by digital service providers;
5) good practices in the European Union member states regarding awareness raising, training, scope of research and development in the field of cybersecurity;
6) good practices in identifying operators of essential services by European Union Member States, including cross-border links regarding risk and incidents.

Article 50. The Single Point of Contact shall forward to the European Commission:
1) without undue delay, the information on:
   a) designated competent authorities for cyber-security, the Single Point of Contact, their tasks and subsequent changes in this respect,
   b) regulations regarding fines related to the national cybersecurity system;
2) every two years, information allowing the assessment of the implementation of Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (OJ EU 194 of 19.07.2016, p. 1), covering in particular:
   a) measures to identify operators of essential services,
   b) list of essential services,
   c) number of operators of essential services identified in each sector of those listed in Annex No. 1 to the Act, and their significance in relation to that sector,
   d) materiality thresholds of the distorting effect for the operator of essential service which are taken into account when qualifying entities as an operator of essential service;
3) information on the tasks of CSIRT MON, CSIRT NASK and CSIRT GOV, including the main elements of procedure in case of an incident.

Chapter 10

Tasks of the Minister of National Defence

Article 51. The Minister of National Defence shall be responsible for:

1) cooperation of the Armed Forces of the Republic of Poland with the relevant institutions of the North Atlantic Treaty Organization, the European Union and international organizations in the area of national defence as regards cybersecurity;
2) providing the Armed Forces of the Republic of Poland within the national, allied and coalition system with capabilities to carry out military operations in case of cybersecurity threats causing the necessity of defence operations;
3) developing the capabilities of the Armed Forces of the Republic of Poland in the field of ensuring cybersecurity by organising specialised training projects;
4) acquiring and developing tools for building the capability to provide cybersecurity within the Armed Forces of the Republic of Poland;
5) managing activities related to incident handling during martial law;
6) assessment of the impact of incidents on the national defence system;
7) assessment of cybersecurity threats during martial law and submitting proposals for defence activities to competent authorities;
8) coordination, in cooperation with the minister competent for internal affairs and the minister competent for digitalisation , of the performance of tasks of central government administration institutions and local government units during martial law, regarding defence activities in case of cybersecurity threats.

Article 52. The Minister of National Defence shall operate the National Contact Point for cooperation with the North Atlantic Treaty Organization, whose tasks include:

1) ensuring cooperation in the area of national defence with the relevant North Atlantic Treaty Organization institutions in the field of cybersecurity;
2) coordination of activities in the field of strengthening defence capabilities in case of cybersecurity threats;
3) ensuring cooperation between national and allied armed forces in terms of providing cybersecurity;
4) developing the systems for sharing information on cybersecurity threats in the area of national defence;
5) participation in achieving the objectives of the North Atlantic Treaty Organization in the area of cybersecurity and cryptology.

Chapter 11

Supervision and control over operators of essential service, digital service providers and entities providing cybersecurity services

Article 53. 1. The supervision over application of the provisions of the Act shall be exercised by:

1) the minister competent for digitalisation, in the field of compliance of entities providing services in the field of cybersecurity with the requirements referred to in Article 14 paragraph 2;
2) the competent authorities for cybersecurity matters, in the field of:
   a) the performance by operators of essential service of the responsibilities set out in the Act related to counteracting cybersecurity threats and reporting serious incidents,
   b) if digital service providers compliance with the security requirements of the digital services they provide, as set out in the Regulation 2018/151, and the obligations under the Act for reporting significant incidents.

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

1) the competent authority for cybersecurity matters or the minister competent for digitalisation shall carry out inspections in the field referred to in paragraph 1;
2) the competent authority for cybersecurity matters may serve a penalty notice on operators of essential services and digital service providers.

3. As regards digital service providers, the actions referred to in paragraph 2 shall be taken upon obtaining evidence that the digital service provider fails to meet the requirements specified in the Regulation 2018/151 or fails to perform obligations under the Act regarding the reporting of significant incidents.

Article 54. 1. For the inspection , the scope of which is specified in Article 53 paragraph 1 subparagraph 1, the provisions of Chapter 5 of the Act of 6 March 2018 – Law on entrepreneurs shall apply.

2. For the inspection , the scope of which is specified in Article 53 paragraph 1 item 2, conducted at the entities which:

1) are entrepreneurs the provisions of Chapter 5 of the Act of 6 March 2018 – Law on entrepreneurs shall apply;

2) are not entrepreneurs, the provisions of the Act of 15 July 2011 on controlling in government administration laying down the rules and procedure for conducting inspections shall apply.

Article 55. A person conducting inspection activities with respect to entities which are entrepreneurs shall be entitled to:

1) enter and move freely at the premises of the inspected entity without the obligation to obtain a pass;
2) access to documents related to the activity of the inspected entity, collect those documents with a receipt and secure documents related to the scope of the inspection, in accordance with the provisions on legally protected confidentiality;
3) make and, if necessary, require to make copies, extracts or excerpts from documents and statements or calculations necessary for the inspection;
4) process personal data to the extent necessary to achieve the objective of the inspection;
5) demand providing oral or written explanations on the issues regarding the scope of the inspection;
6) inspecting devices, storage media and information systems.

Article 56. 1. Controlled entities that are entrepreneurs provide the inspector with the conditions necessary for carry out a smooth inspection, in particular by ensuring, without undue delay, delivery of any requested documents, timely providing oral and written explanations on issues covered by the inspection, providing any technical equipment as necessary, and preparing on one's own copies or printouts of documents and information stored in data storage media, devices or information systems.

2. The inspected entity shall certify as true copies the copies or printouts referred to in paragraph 1. In case of refusal to certify as true copy, these copies shall be certified as true copy by the inspector, which shall be mentioned in the inspection report.

Article 57. The person inspecting entities that are entrepreneurs, shall drew up the facts-based report on evidence gathered during the inspection, including in particular documents, items, visual inspection and oral or written explanations and statements.

Article 58. 1. The person inspecting entities that are entrepreneurs shall present the course of the inspection in the inspection report.

2. The inspection report shall include following::

1) name or forename and surname, and address of the inspected entity;

2) forename and surname of the person representing the inspected entity and the name of the body representing that entity;
3) forename and surname, position and the authorisation number of the inspector;
4) dates of commencement and completion of the inspection activities;
5) specification of the subject and scope of the inspection;
6) description of the facts established during the inspection and other information relevant to the inspection, including the scope, causes and results of the irregularities found;
7) specification of attachments.

3. The inspection report shall be signed by the inspector and the representative of the inspected entity.

4. Prior to signing the report, the inspected entity may, within 7 days from presenting it to the entity for signature, submit a written objection to this report.

5. Where objections are raised, the inspector shall analyse them and, if necessary, undertake additional inspection activities, and in case of the objections are justified , the inspector shall modify or supplement the relevant part of the report in the form of an amendment to the report.

6. If the objections are not accepted in whole or in part, the inspector shall notify the inspected entity in writing.

7. The inspector shall make a record in the report on the refusal to sign the report, along with the date when the mention was drawn up.

8. When drawn up in a paper version, the report shall be made in two counterparts, one of which shall be given to the inspected entity, while in electronic form it shall be served to the inspected entity.

Article 59. 1. If, based on information collected in the inspection report, the competent authority for cybersecurity matters or the minister competent for digitalisation considers that the provisions of the Act may have been violated by the inspected entity, it shall issue post-inspection recommendations to remove the irregularities.

2. There are no appeal measures against post-inspection recommendations.

3. The inspected entity shall notify within the prescribed period the competent authority for cybersecurity matters or the minister competent for digitalisation about the manner of implementing the recommendations.

Chapter 12

The Plenipotentiary and the Cybersecurity Committee

Article 60. The coordination of activities and implementation of the government policy in the field of providing cybersecurity in the Republic of Poland shall be responsibility of the Plenipotentiary.

Article 61. 1. The Plenipotentiary shall be appointed and dismissed by the President of the Council of Ministers.

2. The Plenipotentiary shall be subordinate to the Council of Ministers.

3. The Plenipotentiary shall be a Secretary of State or Undersecretary of State.

4. The substantive, organisational, legal, technical, and office support for the Plenipotentiary shall be provided by the ministry or other government administration office in which the Plenipotentiary was appointed.

Article 62. 1. As a part of activities of coordinating and implementing the government policy to provide cybersecurity, the tasks of the Plenipotentiary include:

1) analysis and assessment of the functioning of the national cybersecurity system based on aggregated data and indicators developed with public administration institutions , the competent authorities for cybersecurity matters, CSIRT MON, CSIRT NASK and CSIRT GOV;
2) supervision over the risk management process of the national cybersecurity system using aggregated data and indicators developed with the competent authorities for cybersecurity matters, CSIRT MON, CSIRT NASK and CSIRT GOV;
3) issuing opinions on government documents, including draft legal acts, affecting the implementation of tasks in the field of cybersecurity;
4) disseminating of new solutions and initiating activities in the field of providing cybersecurity at the national level;
5) initiating national cybersecurity exercises;
6) issuing recommendations regarding the use of IT devices or software at the request of CSIRT.

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

1) cooperation with other states, organizations and international institutions in issues related to cybersecurity;

2) undertaking activities aimed at supporting research and development of technologies in the field of cybersecurity;
3) undertaking activities aimed at increasing public awareness of cybersecurity threats and safe Internet use.

Article 63. 1. The Plenipotentiary shall draw up and submit to the Council of Ministers, by 31 March each year, a report for the previous calendar year, containing information on its activities in the area of providing cybersecurity at the national level.

2. The Plenipotentiary may submit to the Council of Ministers conclusions and recommendations regarding actions that should be undertaken by the entities of the national cybersecurity system in order to provide cybersecurity at the national level and to counteract threats in this respect.

Article 64. The Cybersecurity Committee operates at the Council of Ministers, in the capacity of a consultative and advisory body in matters of cybersecurity and relevant activities of CSIRT MON, CSIRT NASK, CSIRT GOV, sectoral cybersecurity teams and the competent authorities for cybersecurity.

Article 65. 1. The tasks of the Cybersecurity Committee shall include expressing opinions on:

1) trends and plans for counteracting cybersecurity threats;
2) performing entrusted tasks by CSIRT MON, CSIRT NASK, the Head of the Internal Security Agency in terms of its responsibilities under CSIRT GOV, sectoral cybersecurity teams and the competent authorities for cybersecurity matters in accordance with the trends and plans for counteracting cybersecurity threats;3) cooperation of authorities that conduct or supervise CSIRT MON, CSIRT GOV and CSIRT NASK;
4) cooperation between entities of CSIRT MON, CSIRT NASK, the Head of the Internal Security Agency and the minister – a member of the Council of Ministers competent for coordinating the activities of special services, sectoral cybersecurity teams and the competent authorities for cybersecurity matters;
5) organisation of sharing information that is essential for cybersecurity and international position of the Republic of Poland between institutions of government administration;
6) conclusions of CSIRT MON, CSIRT NASK or CSIRT GOV regarding recommendations on the use of IT devices or software.

2. The tasks of the Cybersecurity Committee include the development of recommendations for the Council of Ministers on activities in the field of providing cybersecurity at the national level, referred to in Article 67.

Article 66. 1. The Cybersecurity Committee shall be composed of:

1) Chairman of the Cybersecurity Committee – President of the Council of Ministers;
2) the Plenipotentiary;
3) Secretary of the Cybersecurity Committee;
4) members of the Cybersecurity Committee:
   a) minister competent for internal affairs,
   b) minister competent for digitalisation,
   c) Minister of National Defence,
   d) minister competent for foreign affairs,
   e) Head of the Chancellery of the Prime Minister,
   f) Head of the National Security Bureau, if appointed by the President of the Republic of Poland,
   g) minister – member of the Council of Ministers competent for coordinating the activities of special services, or a person authorized by him having the rank of secretary of state or undersecretary of state, and if the minister – member of the Council of Ministers competent for coordinating the activities of special services has not been designated, then the Head of the Internal Security Agency.

2. The President of the Council of Ministers may authorise the Plenipotentiary to act as the Chairman of the Cybersecurity Committee.

3. The members of the Cybersecurity Committee referred to in paragraph 1 item 4 points a to e may be substituted by authorised representatives with the rank of secretary of state or undersecretary of state.

4. The meetings of the Cybersecurity Committee shall also be attended by:

1) Director of the Government Centre for Security;
2) Head of the Internal Security Agency or his deputy;
3) Head of the Military Counterintelligence Service or his deputy;
4) Director of the Research and Academic Computer Network – State Research Institute.

5. The Chairman of the Cybersecurity Committee:

1) shall convene meetings of the Cybersecurity Committee;

2) may invite chairmen of relevant parliamentary committees, representatives of state authorities, representatives of the competent authorities for cybersecurity matters and other persons whose participation is necessary due to the subject of the meeting, to attend the meetings of the Cybersecurity Committee.

6. The Secretary of the Cybersecurity Committee shall be appointed by the President of the Council of Ministers from among those who meet the requirements set out in the regulations on the protection of classified information in the field of access to classified information with the clause "secret". The Secretary of the Cybersecurity Committee shall be dismissed by the President of the Council of Ministers.

7. The Secretary of the Cybersecurity Committee organises the work of the Cybersecurity Committee and, in this respect, may request CSIRT MON, CSIRT GOV, CSIRT NASK, sectoral cybersecurity teams, the competent authorities for cybersecurity matters and institutions of government administration, for providing necessary information in matters dealt with by the Cybersecurity Committee.

8. The Cybersecurity Committee actions s shall be handled by the ministry or other government administration office that supports the Plenipotentiary.

9. The Council of Ministers shall determine, in an ordinance, the detailed scope of activities and the procedure of operation of the Cybersecurity Committee, having in mind the nature of the Cybersecurity Committee's tasks and the need to ensure its efficient work.

Article 67. 1. The President of the Council of Ministers, in order to coordinate government administration activities in the field of cybersecurity, may, upon a recommendation of the Cybersecurity Committee, issue binding guidelines on providing cybersecurity at the national level and the functioning of the national cybersecurity system, and also may request information and opinions in this respect from :

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

6) the minister competent for digitalization – with regard to tasks carried out in accordance with the Act.

2. The President of the Council of Ministers shall issue binding guidelines for the CSIRT MON, CSIRT GOV and CSIRT NASK on handling critical incidents, including the appointment of the CSIRT responsible for critical incident handling.

Chapter 13

Strategy

Article 68. The Council of Ministers shall adopt the Strategy by way of a resolution.

Article 69. 1. The strategy shall define strategic goals and appropriate political and regulatory measures aimed at achieving and maintaining a high level of cybersecurity. The strategy shall cover the sectors referred to in Annex 1 to the Act, the digital services and public entities referred to in Article 4, subparagraphs 7 to 15.

2. The strategy shall include in particular:

1) objectives and priorities in cybersecurity;
2) entities involved in the implementation and performance of the Strategy;
3) measures used to achieve the objectives of the Strategy;
4) specification of means for readiness, response and restoration of normal status, including principles of cooperation between the public and private sectors;
5) risk assessment approach;
6) activities related to education, information and training programmes on cybersecurity;
7) activities related to plans on cybersecurity research and development.

3. The strategy shall be adopted for a five-year period with the possibility of introducing changes during the period of its validity.

Article 70. 1. The draft of the Strategy shall be drawn up by the minister competent for digitalization 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 work on the draft of the Strategy.

Article 71. The minister competent for digitalization, in cooperation with the Plenipotentiary, other ministers and relevant heads of central offices shall review the Strategy every two years.

Article 72. The minister competent for digitalization shall notify the Strategy to the European Commission within 3 months from the date of its adoption by the Council of Ministers.

Chapter 14

Provisions on fines

Article 73. 1. An operator of essential service shall be fined if the following::

1) fails to systematically assess the risk or fails to manage of occurrence of the incident risk referred to in article 8 subparagraph 1;
2) has failed to implement technical and organisational measures taking into account the requirements referred to in Article 8 subparagraph 2 points a) to e).
3) fails to apply the measures referred to in Article 8 subparagraph 5 points a) to d).
4) has failed to appoint the person referred to in Article 9 paragraph 1 subparagraph 1;
5) fails to perform the obligations referred to in Article 10 paragraph 1;
6) fails to perform the obligation referred to in Article 11 paragraph 1 subparagraph 1;
7) fails to perform the obligation referred to in Article 11 paragraph 1 subparagraph 4;
8) fails to perform the obligation referred to in Article 11 paragraph 1 subparagraph 5;
9) fails to remove the vulnerabilities referred to in Article 32, paragraph 2;
10) fails to perform the obligation referred to in Article 14 paragraph 1;
11) fails to conduct an audit;
12) prevents or hinders conducting of the inspection referred to in Article 53 paragraph 2 point 1;
13) failed to implement the post-inspection recommendations referred to in art. 59 par.1.

2. A digital service provider shall be fined if the following:

1) fails to perform the obligation referred to in Article 18 paragraph 1 subparagraph 4;
2) fails to perform the obligation referred to in Article 18 paragraph 1 subparagraph 5;
3) fails to remove the vulnerabilities referred to in Article 32, paragraph 2.

3. The amount of the financial penalty notice referred to in:

1) paragraph 1 item 1, shall be up to PLN 150,000;
2) paragraph 1 item 2, shall be up to PLN 100,000;
3) paragraph 1 item 3, shall be up to PLN 50,000;
4) paragraph 1 item 4, shall be up to PLN 15,000;
5) paragraph 1 item 5, shall be up to PLN 50,000;

6) paragraph 1 item 6, shall be up to PLN 15,000 for each case of failure to handle an incident;
6) paragraph 1 item 7, shall be up to PLN 20,000 for each case of failure to report a serious incident;
8) paragraph 1 items 8 and 9, shall be up to PLN 20,000;
9) paragraph 1 item 10, shall be PLN 100,000;
10) paragraph 1 items 11 and 13, shall be up to PLN 200,000;
11) paragraph 1 item 12, shall be up to PLN 50,000;
12) paragraph 1 item 7, shall be up to PLN 20,000 for each case of failure to report a serious incident;
13) paragraph 2 items 2 and 3, shall be up to PLN 20,000.

4. The fine referred to in:
1) paragraph 1 item 4, may not be lower than PLN 1,000;
2) paragraph 1 items 1 to 3, 6 to 9 and 12, may not be lower than PLN 5,000;
3) paragraph 1 items 5, 10, 11 and 13, may not be lower than PLN 15,000;

5. If, as a result of an inspection, the competent authority for cybersecurity matters finds that the operator of essential service or digital service provider persistently violates the provisions of the Act, posing:
1) a direct and serious threat to cybersecurity of defence, state security, public security and public order or for human life and health,
2) a threat of causing serious damage to property or serious disruption in providing essential services,

then the competent authority for cybersecurity matters shall impose a penalty notice of up to PLN 1,000,000.

Article 74. 1. The fine referred to in Article 73 shall be imposed, by way of a decision by the competent authority for cybersecurity matters.

2. The sum that is to be imposed under a penalty notice as referred to in Article 73 shall constitute the income of the state budget.

Article 75. The competent authority for cybersecurity matters may impose a fine on the manager of an operator of essential service in the case the manager fails to exercise due diligence to fulfil the obligations referred to in Article 8 item 1, Article 9 paragraph 1 subparagraph 1, and Article 15 paragraph 1, except that the fine may not exceed 200% of the manager’s monthly remuneration.

Article 76. The fine referred to in Article 73 may also be imposed, if the entity has ceased to the law or remedied the damage caused, if the authority competent for cybersecurity matters considers that such a decision is reasonable due to the duration, scope or effects of the violation.

Chapter 15

Changes in regulations, interim provisions, adapting provisions and final provisions

Article 77. In the Act of 7 September 1991 on the system of education (Journal of Laws of the Republic of Poland of 2017, items 2198, 2203 and 2361) in Article 90u:

1) in paragraph 1 point 6 shall read as follows:
   "6) developing competences, interests and talents of children and youth and other social groups, including supporting authorities which 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) in paragraph 4 point 6 shall read as follows:
   "6) detailed conditions, forms and procedure of implementation of projects in the scope of developing competences, interests and talents of children and youth and other social groups, as well as conditions and procedure of supporting authorities which run schools, or institutions in the implementation of projects in this area, in particular in the field of safe the use of information -and communication technologies, taking into account the need to develop skills to facilitate adaptation to changes in social and economic life, the possibility of providing financial support to authorities which run schools, or institutions, and the requirement of effectiveness and efficiency in budget spending;".

Article 78. The Act of 4 September 1997 on sectors of government administration (Journal of Laws of the Republic of Poland of 2018, items 762, 810 and 1090) shall be amended as follows:

1) in Article 12a, in paragraph 1 point 10 it shall read as follows:
   "10) cyberspace security in the civil dimension;";
2) in Article 19, in paragraph 1 after item 1, the following item 1a shall be added:
   "1a) cyberspace security in the military dimension,".

Art. 79. In the Act of 24 May 2002 on the Internal Security Agency and the Foreign Intelligence Agency (Journal of Laws of the Republic of Poland of 2017, items 1920 and

2405, and of 2018, items 138 and 650 and 730), the following Article 32aa is added after Article 32a, reading as follows:

"Article 32aa. 1. In order to prevent and counteract terrorist events concerning information and communication systems of public administration institutions or IT networks subject to a uniform list of facilities, installations, devices and services included in the critical infrastructure, as well as IT systems of the owners, which all are essential from the point of view of continuity of operation of the state, and also ITC systems of owners, independent and dependent holders of facilities, installations or critical infrastructure devices referred to in Article 5b paragraph 7 item 1 of the Act of 26 April 2007 on crisis management, or data processed in these systems, and prevention and detection of terrorist offences in this area and prosecution of their offenders, the Internal Security Agency shall implement in these entities an early warning system for threats occurring in the Internet, hereinafter referred to as "the warning system", operate it and coordinate its functioning.

2. The elements of the warning system shall be implemented in the entities referred to in paragraph 1 in accordance with the annual implementation plan developed by the Head of the Internal Security Agency by 30 September of the preceding year. In the justified cases, at the request of the entity, the implementation of elements of the warning system may be carried out without the plan.

3. The Internal Security Agency shall without undue delay notify the entity referred to in paragraph 1 on its inclusion in the annual warning system implementation plan.

4. The entity referred to in paragraph 1 is obliged to join the warning system and provide the Internal Security Agency with necessary information enabling implementation of the warning system in this entity.

5. In entities referred to in paragraph 1 that are subordinate to or supervised by the Minister of National Defence, the implementation of the warning system may take place with the consent of the Minister of National Defence.

6. The costs of implementing and maintaining the warning system in the entities referred to in paragraph 1 shall be covered by the Internal Security Agency.

7. The Internal Security Agency, by way of an agreement, shall agree with the entity referred to in paragraph 1, technical aspects of participation in the warning system and the system configuration model.

8. If it is not possible to conclude the agreement referred to in paragraph 7 for reasons attributable to the entity referred to in paragraph 1, the Internal Security Agency shall inform the supervising entity or the minister competent for digitalization.

9. The President of the Council of Ministers shall determine, in an ordinance, the conditions and procedure for running, coordinating and implementing the warning system, in particular shall specify the activities necessary for its activation and maintenance and the model of the agreement referred to in paragraph 7, guided by the need to ensure the security of ICT systems essential from the point of view of the continuity of the functioning of the state."

Art. 80. In the Act of 29 January 2004 – Public Procurement Law (Journal of Laws of the Republic of Poland of 2017, items 1579 and 2018), Article 89 in paragraph 1 item 7d shall read as follows:

"7d) its adoption would violate public security or a material interest of the state security, including the security of entities covered by the uniform list of facilities, installations, equipment and services constituting the critical infrastructure referred to in Article 5b paragraph 7 item 1 of the Act of 26 April 2007 on crisis management (Journal of Laws of the Republic of Poland of 2017, items 209 and 1566, and of 2018, item 1118), and this security or interest could not be guaranteed otherwise:"

Article 81. The Act of 16 July 2004 – The telecommunications law (Journal of Laws of the Republic of Poland of 2017, items 1907 and 2201, and of 2018, items 106, 138, 650 and 1118) shall be amended as follows:

1) in Article 175a:

a) paragraphs 1a and 1b shall be inserted following paragraph 1:

"1a. The President of UKE shall submit the information referred to in paragraph 1, if it concern events that are incidents within the meaning of the Act of 5 July 2018 on the national cyber-security system (Journal of Laws of the Republic of Poland of, item …), the CSIRT competent for the notifying telecommunications company , pursuant to Article 26 paragraphs 5 to 7 of this Act, with the exception of information constituting a trade secret, reserved under Article 9.

1b. The transfer referred to in paragraph 1a shall be performed electronically or by using other available means of communication, when it is impossible to transfer it in an electronic form".

b) after paragraph 2, the following paragraph 2a shall be added:

"2a. The minister competent for computerisation shall specify, by regulation, the criteria for considering a breach of the security or integrity of a telecommunications networks or services as having a significant impact on the operation of the networks or services, taking into account in particular the percentage of users affected by the breach of security or integrity of the networks or services, duration of the breach of security or integrity of the telecommunications networks or services resulting in unavailability or restriction of the availability of the telecommunications networks or services, and the recommendations and guidelines of the European Union Agency for Network and Information Security (ENISA)."

2) in Article 176a:

a) in paragraph 1 item 3 shall read as follows:

"3) direct threats to the security or integrity of the telecommunications infrastructure of the company or the services provided by it",

b) in paragraph 2 item 4 shall read as follows:

"4) technical and organisational measures to ensure the security and integrity of the telecommunications infrastructure and services provided, including protection against occurrence of incidents within the meaning of the Act of 5 July 2018 on the national cybersecurity system;";

3) in Article 209, in paragraph 1 after item 27, the following item 27^1 shall be added:

"27^1) fails to perform the obligation referred to in Article 175a paragraph 1,".

Article 82. The Act of 26 April 2007 on crisis management (Journal of Laws of the Republic of Poland of 2017, items 209 and 1566, and of 2018, item 1118) shall be amended as follows:

1) in Article 5a, paragraph 2 shall read as follows:

"2. The coordination of the report preparation shall be ensured by the Director of the Government Centre for Security, while in the part concerning terrorist threats that could lead to a crisis situation it shall be ensured by the Head of the Internal Security Agency, whole in part on the cybersecurity threats that could lead to a crisis situation – the Government Plenipotentiary for Cybersecurity.";

2) in Article 6, after paragraph 5a, the following paragraph 5b shall be added:

"5b. Owners, independent and dependent holders referred to in paragraph 5, which at the same time are operators of essential services within the meaning of the Act of 5 July 2018 on the national cybersecurity system (Journal of Laws of the Republic of Poland of, item …) shall include in the critical infrastructure protection plans the documentation on the cybersecurity of information systems used to provide essential services in accordance with the scope of information specified in the regulations issued pursuant to Article 10 paragraph 5 of the Act of 5 July 2018 on the national cybersecurity system.";

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

"15) Government Plenipotentiary for Cybersecurity.";

4) in Article 11, after paragraph 1, the following paragraph 1a shall be added:

"1a. The Centre shall provide support for the Team for Critical Incidents referred to in Article 36 paragraph 1 of the Act of 5 July 2018 on the national cybersecurity system.".

Article 83. Cybersecurity threats that may lead to a crisis situation shall be included for the first time in the Report on threats to national security, which will be prepared with the participation of the Plenipotentiary, after the entry into force of the Act.

Article 84. The President of the Council of Ministers shall appoint the Plenipotentiary within 3 months from the date of entry into force of the Act.

Article 85. The minister competent for digitalization shall notify the European Commission of:

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

2) the scope of tasks of CSIRT MON, CSIRT NASK and CSIRT GOV, including the main elements of the incident handling procedures.

Article 86. The competent Authorities for cybersecurity matters shall, by 9 November 2018, issue decisions on declaring the operators of essential services and provide the minister competent for digitalization with applications to enter operator of essential service in the list referred to in Article 7.

Article 87. The minister competent for digitalization, by 9 August 2018, submit to the Cooperation Group a summary report on:

1) serious incidents reported by operators of essential services affecting the continuity of their provision of essential service in the Republic of Poland and continuity of essential service provision in EU Member States;
2) significant incidents reported by digital service providers, including those affected two or more Member States of the European Union.

Article 88. The minister competent for digitalization shall, by 9 November 2018, submit to the European Commission information on:
1) national measures enabling identification of operators of essential services;
2) list of essential services;
3) number of operators of essential services identified in each sector of those listed in Annex No. 1 to the Act, and their significance in relation to that sector;
4) thresholds of the disruptive effect for the operators of essential services which are taken into account when qualifying entities as operators of essential services.

Article 89. The minister competent for digitalisation shall launch by 1 January 2021 the ICT system referred to in Article 46 paragraph 1.

Article 90. The strategy shall be adopted by 31 October 2019.

Article 91. 1. The annual implementation plan referred to in Article 32aa paragraph 2 of the act amended under Article 79, shall be developed for the first time by the Head of the Internal Security Agency for 2019.

2. An entity that before the date of entry of this Act into force joined the ARAKIS-GOV programme implemented by the Internal Security Agency shall be considered as an entity that joined the warning system as defined in Article 32aa paragraph 4 of the Act amended under Article 79.

3. The entity referred to in paragraph 2, which by the date of entry of this Act into force did not fully implement the elements of the warning system, as defined in Article 32aa paragraph 4 of the Act amended under Article 79 is obliged to complete them within one year from the date of entry into force of the Act.

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

Article 92. 1. The previous secondary legislation issued under Article 90u paragraph 4 item 6 of the Act amended under Article 77 shall remain valid until the date of entry into force of the secondary legislation issued under Article 90u paragraph 4 item 6 of the

Act amended under Article 77 in the wording given by this Act, but not longer than until 1 December 2019, and may be subject to amendment.

2. The previous secondary legislation issued under Article 176a paragraph 5 of the Act amended under Article 81 shall remain valid until the date of entry into force of a new secondary legislation issued under Article 176a paragraph 5 of the Act amended under Article 81, but not longer than for 24 months from the date of entry of this Act into force.

3. The previous secondary legislation issued under Article 5a paragraph 6 of the Act amended under Article 82 shall remain valid until the date of entry into force of a new secondary legislation issued under Article 5a paragraph 6 of the Act amended under Article 82, but not longer than for 12 months from the date of entry of this Act into force.

Article 93 .1. The maximum limit of expenses from the state budget for the budgetary part 21 –Maritime Economy, which is the financial result of the entry of this Act into force, shall be:

1) in 2018 – PLN 0;
2) in 2019 – PLN 388 thousand;
3) in 2020 – PLN 404 thousand;
4) in 2021 – PLN 404 thousand;
5) in 2022 – PLN 404 thousand;
6) in 2023 – PLN 404 thousand;
7) in 2024 – PLN 404 thousand;
8) in 2025 – PLN 404 thousand;
9) in 2026 – PLN 404 thousand;
10) in 2027 – PLN 404 thousand.

2. The maximum limit of expenses from the state budget for the budgetary part 22 – Water management, which is the financial result of the entry of this Act into force, shall be:

1) in 2018 – PLN 0;
2) in 2019 – PLN 388 thousand;
3) in 2020 – PLN 404 thousand;
4) in 2021 – PLN 404 thousand;
5) in 2022 – PLN 404 thousand;
6) in 2023 – PLN 404 thousand;
7) in 2024 – PLN 404 thousand;

8) in 2025 – PLN 404 thousand;

9) in 2026 – PLN 404 thousand;

10) in 2027 – PLN 404 thousand.

3. The maximum limit of expenses from the state budget for the budgetary part 27 – Digitalization, which is the financial result of the entry of this Act into force, shall be:

1) in 2018 – PLN 6,450 thousand;

2) in 2019 – PLN 13,349 thousand;

3) in 2020 – PLN 17,334 thousand;

4) in 2021 – PLN 17,314 thousand;

5) in 2022 – PLN 18,904 thousand;

6) in 2023 – PLN 18,904 thousand;

7) in 2024 – PLN 18,904 thousand;

8) in 2025 – PLN 18,904 thousand;

9) in 2026 – PLN 18,904 thousand;

10) in 2027 – PLN 18,904 thousand.

4. The maximum limit of expenses from the state budget for the budgetary part 39 – Transport, which is the financial result of the entry of this Act into force, shall be:

1) in 2018 – PLN 0;

2) in 2019 – PLN 388 thousand;

3) in 2020 – PLN 404 thousand;

4) in 2021 – PLN 404 thousand;

5) in 2022 – PLN 404 thousand;

6) in 2023 – PLN 404 thousand;

7) in 2024 – PLN 404 thousand;

8) in 2025 – PLN 404 thousand;

9) in 2026 – PLN 404 thousand;

10) in 2027 – PLN 404 thousand.

5. The maximum limit of expenses from the state budget for the budgetary part 46 – Health, which is the financial result of the entry of this Act into force, shall be:

1) in 2018 – PLN 0;

2) in 2019 – PLN 388 thousand;

3) in 2020 – PLN 404 thousand;

4) in 2021 – PLN 404 thousand;

5) in 2022 – PLN 404 thousand;

6) in 2023 – PLN 404 thousand;
7) in 2024 – PLN 404 thousand;
8) in 2025 – PLN 404 thousand;
9) in 2026 – PLN 404 thousand;
10) in 2027 – PLN 404 thousand.

6. The maximum limit of expenses from the state budget for the budgetary part 47 – Energy, which is the financial result of the entry of this Act into force, shall be:

1) in 2018 – PLN 0;
2) in 2019 – PLN 758 thousand;
3) in 2020 – PLN 789 thousand;
4) in 2021 – PLN 789 thousand;
5) in 2022 – PLN 789 thousand;
6) in 2023 – PLN 789 thousand;
7) in 2024 – PLN 789 thousand;
8) in 2025 – PLN 789 thousand;
9) in 2026 – PLN 789 thousand;
10) in 2027 – PLN 789 thousand.

7. The maximum limit of expenses from the state budget for the budgetary part 57 – Internal Security Agency, which is the financial result of the entry of this Act into force, shall be:

1) in 2018 – PLN 0;
2) in 2019 – PLN 255 thousand;
3) in 2020 – PLN 3,605 thousand;
4) in 2021 – PLN 5,605 thousand;
5) in 2022 – PLN 5,605 thousand;
6) in 2023 – PLN 9,705 thousand;
7) in 2024 – PLN 705 thousand;
8) in 2025 – PLN 705 thousand;
9) in 2026 – PLN 705 thousand;
10) in 2027 – PLN 8,705 thousand.

8. The maximum limit of expenses from the state budget for the budgetary part 70 – Polish Financial Supervision Authority, which is the financial result of the entry of this Act into force, shall be:

1) in 2018 – PLN 0;

2) in 2019 – PLN 758 thousand;
3) in 2020 – PLN 789 thousand;
4) in 2021 – PLN 789 thousand;
5) in 2022 – PLN 789 thousand;
6) in 2023 – PLN 789 thousand;
7) in 2024 – PLN 789 thousand;
8) in 2025 – PLN 789 thousand;
9) in 2026 – PLN 789 thousand;
10) in 2027 – PLN 789 thousand.

9. The maximum limit of expenses from the state budget for the budgetary part 76 – Office of Electronic Communication, which is the financial result of the entry of this Act into force, shall be:

1) in 2018 – PLN 0;
2) in 2019 – PLN 203 thousand;
3) in 2020 – PLN 212 thousand;
4) in 2021 – PLN 212 thousand;
5) in 2022 – PLN 212 thousand;
6) in 2023 – PLN 212 thousand;
7) in 2024 – PLN 212 thousand;
8) in 2025 – PLN 212 thousand;
9) in 2026 – PLN 212 thousand;
10) in 2027 – PLN 212 thousand.

10. The maximum limit of expenses from the state budget for the budgetary part 42 – Internal Affairs, which is the financial result of the entry of this Act into force, shall be:

1) in 2018 – PLN 242 thousand;
2) in 2019 – PLN 360 thousand;
3) in 2020 – PLN 0;
4) in 2021 – PLN 0;
5) in 2022 – PLN 0;
6) in 2023 – PLN 0;
7) in 2024 – PLN 0;
8) in 2025 – PLN 0;
9) in 2026 – PLN 0;
10) in 2027 – PLN 0.

11. Where there is a risk of exceeding the maximum expenditure limits referred to in paragraphs 1 to 6 and 8, or where the limits are exceeded, corrective mechanisms shall be applied, involving:

1) reduction of spending related to the implementation of the tasks of the competent authority for cybersecurity matters in the field of identification of operators of essential services and conducting ongoing analysis of entities in a given sector in terms of declaring them as an operator of essential service or disqualify them as an operator of essential service;;
2) reduction of the number of inspections at operators of essential services and digital service providers;
3) withdrawal from organising or participating in cybersecurity exercises organized in the Republic of Poland or in the European Union;
4) limiting the financing of activities of the sectoral cybersecurity team established by a given the competent authority for cybersecurity matters.

12. Where there is a risk of exceeding the maximum expenditure limit referred to in paragraph 7, adopted for a given budget year, or where the limit is exceeded, a corrective mechanism shall be applied, consisting in limiting the number of entities implementing the early warning system about threats occurring in the Internet, specified in the annual implementation plan developed by the Head of the Internal Security Agency.

13. Where there is a risk of exceeding the maximum expenditure limit referred to in paragraph 9, adopted for a given budget year, or where the limit is exceeded, a corrective mechanism shall be applied, consisting in reduction of spending on the fulfilment of statutory tasks related to incident handling.

14. Where there is a risk of exceeding the maximum expenditure limit referred to in paragraph 10, adopted for a given budget year, or where the limit is exceeded, a corrective mechanism shall be applied, consisting in limiting the spending related to providing the equipment necessary for the support for the Team.

15. If the amount of expenditure in individual months is consistent with the financial plan, the provisions of paragraphs 11 to14 shall not be applied.

16. The minister competent for maritime economy shall monitor the use of the expenditure limit referred to in paragraph 1, and at least four times a year, at the end of each quarter, shall assess the use of the spending limit for a given year. Implementation of correction mechanisms referred to in paragraph 11 shall be performed by the minister competent for maritime economy.

17. The minister competent for water management shall monitor the use of the expenditure limit referred to in paragraph 2, and at least four times a year, at the end of each quarter, shall assess the use of the spending limit for a given year. Implementation of correction mechanisms referred to in paragraph 11 shall be performed by the minister competent for water management.

18. The minister competent for digitalization shall monitor the use of the expenditure limit referred to in paragraph 3, and at least four times a year, at the end of each quarter, shall assess the use of the spending limit for a given year. Implementation of correction mechanisms referred to in paragraph 11 shall be performed by the minister competent for computerisation.

19. The minister competent for transport shall monitor the use of the expenditure limit referred to in paragraph 4, and at least four times a year, at the end of each quarter, shall assess the use of the spending limit for a given year. Implementation of correction mechanisms referred to in paragraph 11 shall be performed by the minister competent for transport.

20. The minister competent for health shall monitor the use of the expenditure limit referred to in paragraph 5, and at least four times a year, at the end of each quarter, shall assess the use of the spending limit for a given year. Implementation of correction mechanisms referred to in paragraph 11 shall be performed by the minister competent for health.

21. The minister competent for energy shall monitor the use of the expenditure limit referred to in paragraph 6, and at least four times a year, at the end of each quarter, shall assess the use of the spending limit for a given year. Implementation of correction mechanisms referred to in paragraph 11 shall be performed by the minister competent for energy.

22. The Head of the Internal Security Agency shall monitor the use of the expenditure limit referred to in paragraph 7, and at least four times a year, at the end of each quarter, shall assess the use of the spending limit for a given year. Implementation of the correction mechanism referred to in paragraph 12 shall be performed by the Head of the Internal Security Agency.

23. The Polish Financial Supervision Authority shall monitor the use of the expenditure limit referred to in paragraph 8, and at least four times a year, at the end of each quarter, shall assess the use of the spending limit for a given year. Implementation

of the correction mechanisms referred to in paragraph 11 shall be performed by the Polish Financial Supervision Authority.

24. The President of the Office of Electronic Communications shall monitor the use of the expenditure limit referred to in paragraph 9, and at least four times a year, at the end of each quarter, shall assess the use of the spending limit for a given year. Implementation of the correction mechanism referred to in paragraph 13 shall be performed by The President of the Office of Electronic Communications.

25. The minister competent for internal affairs shall monitor the use of the expenditure limit referred to in paragraph 10, and shall assess its use. Implementation of the correction mechanism referred to in paragraph 14 shall be performed by the minister competent for internal affairs.

Article 94. The Act shall enter into force after 14 days from the day of announcement.

MARSHAL OF THE SEJM

Marek Kuchciński

Annex 1 to the Act
of 5 July 2018 (item ...)

SECTORS AND SUB-SECTORS AND TYPES OF ENTITIES

Sector	Sub-sector (if any)	Type of entity
Energy	Mining	Entities running a business in the field of natural gas extraction under the mining licence referred to in Article 22 paragraph 1 of the Act of 9 June 2011 – Geological and mining law (Journal of Laws of the Republic of Poland of 2017, item 2126, and of 2018, items 650 and 723).
		Entities running a business in the field ofcrude oil extraction under the mining licence referred to in Article 22 paragraph 1 of the Act of 9 June 2011 – Geological and mining law.
		Entities running a business in the field of brown coal under the mining licence referred to in Article 22 paragraph 1 of the Act of 9 June 2011 – Geological and mining law.
		Entities running a business in the field of hard coal mining under the mining licence referred to in Article 22 paragraph 1 of the Act of 9 June 2011 – Geological and mining law.
		Entities running a business in the field of extraction of other minerals under the mining licence referred to in Article 22 paragraph 1 of the Act of 9 June 2011 – Geological and mining law.
	Electricity	Energy company referred to in Article 3 item 12 of the Act of 10 April 1997 – Energy law (Journal of Laws of the Republic of Poland of 2018, items 755, 650, 685, 771 and 1000), having a license to conduct the business of electric power generation.
		Energy company referred to in Article 3 item 24 of the Act of 10 April 1997 – Energy law, having a license to conduct the business of electric power transmission.
		Energy company referred to in Article 3 item 25 of the Act of 10 April 1997 – Energy law, having a license to conduct the business of electric power distribution.
		Energy company referred to in Article 3 item 12 of the Act of 10 April 1997 – Energy law, having a license to conduct the business of electricity trading.
		Energy company referred to in Article 3 item 12 of the Act of 10 April 1997 – Energy law, running the business of electric power processing or storage.

		Entities running a business of the provision system quality-assurance services and management of energy infrastructure.
	Heat supply	Energy company referred to in Article 3 item 12 of the Act of 10 April 1997 – Energy law, having a license to conduct the business of heatgeneration.
		Energy company referred to in Article 3 item 12 of the Act of 10 April 1997 – Energy law, having a license to conduct the business of heattrading.
		Energy company referred to in Article 3 item 12 of the Act of 10 April 1997 – Energy law, having a license to conduct the business of heat transmission.
		Energy company referred to in Article 3 item 12 of the Act of 10 April 1997 – Energy law, having a license to conduct the business of heat distribution.
	Crude oil	Energy company referred to in Article 3 item 12 of the Act of 10 April 1997 – Energy law, having a license for production of liquid fuel , referred to in Article 32 paragraph 1 of the Act of 10 April 1997 – Energy law.
		Entities conducting business of crude oil pipeline transportation .
		Energy company referred to in Article 3 item 12 of the Act of 10 April 1997 – Energy law, having a license for pipeline transportation of liquid fuel through a pipeline networka, referred to in Article 32 paragraph 1 of the Act of 10 April 1997 – Energy law.
		Entity running a business in the field of crude oil storage, including in the field of non-tank underground storage of crude oil, referred to in Article 22 paragraph 1 of the Act of 9 June 2011 – Geological and mining law.
		Entities conducting business of crude oil transhipment.
		Energy company referred to in Article 3 item 12 of the Act of 10 April 1997 – Energy law, running a business in the field of storage of liquid fuels, referred to in Article 32 paragraph 1 of the Act of 10 April 1997 – Energy law, and an entity running a business in the field of non-tank underground storage of liquid fuels, referred to in Article 22 paragraph 1 of the Act of 9 June 2011 – Geological and mining law.
		Energy company referred to in Article 3 item 12 of the Act of 10 April 1997 – Energy law, running the business of transhipment of liquid fuels, referred to in Article 32 paragraph 1 of the Act of 10 April 1997 – Energy law.
		Energy company referred to in Article 3 item 12 of the Act of 10 April1997 – Energy law, running the business of trade in liquid fuels or foreign trade in liquid fuels, referred to in Article 32 paragraph 1 of the Act of 10 April 1997 – Energy law.

		Entities running a business in the field of synthetic fuels production.
	Gas	Energy company referred to in Article 3 item 12 of the Act of 10 April 1997 – Energy law, running the business of gaseous fuels production, referred to in Article 3 paragraph 45 of the Act of 10 April 1997 – Energy law.
		Energy company referred to in Article 3 item 12 of the Act of 10 April 1997 – Energy law, having a license to conduct the business of gaseous fuels transmission.
		Energy company referred to in Article 3 item 12 of the Act of 10 April 1997 – Energy law, having a license to conduct business of foreign trade of natural gas or for conducting business in the field of trade in gaseous fuels.
		Energy company referred to in Article 3 item 24 of the Act of 10 April 1997 – Energy law, which is a gas transmission system operator designated by the President of the Energy Regulatory Office.
		Energy company referred to in Article 3 item 25 of the Act of 10 April 1997 – Energy law, which is a gas distribution system operator designated by the President of the Energy Regulatory Office.
		Energy company referred to in Article 3 item 26 of the Act of 10 April 1997 – Energy law, which is a gaseous fuel storage system operator designated by the President of the Energy Regulatory Office.
		Energy company referred to in Article 3 item 27 of the Act of 10 April 1997 – Energy law, which is a natural gas liquefaction system operator designated by the President of the Energy Regulatory Office.
	Supplies and services for the energy sector	Entities running a business in the field of supply of systems, machinery, equipment, materials, raw materials and providing services to the energy sector.
	Supervised and subordinate units	Organisational entities subordinate to or supervised by the minister competent for energy matters.
		Organisational entities subordinate to or supervised by the minister competent for the management of mineral deposits.
Transport	Air Transport	Air carrier referred to in Article 3(4) of the Regulation (EC) No 300/2008 of the European Parliament and of the Council of 11 March 2008 on common rules in the field of civil aviation security and repealing Regulation (EC) (OJ EU L 97 of 09.04.2008, p. 72).
		Airport operator referred to in Article 2 item 7 of the Act of 3 July 2002 – Aviation law (Journal of Laws of the Republic of Poland of 2018, item 1183).

		An entity referred to in Article 177 paragraph 2 of the Act of 3 July 2002 – Aviation law, which provides for air carriers and other aircraft users one or more categories of services, as referred to in Article 176 of this Act, and the entity referred to in Article 186b paragraph 1 item 2 of the Act of 3 July 2002 – Aviation law, performing tasks related to security check for air carriers.
		Air navigation service provider referred to in Article 127 paragraph 1 of the Act of 3 July 2002 – Aviation law.
	Railway transport	Railway infrastructure manager within the meaning of Article 4 item 7 of the Act of 28 March 2003 on rail transport (Journal of Laws of the Republic of Poland of 2017, items 2117 and 2361, and of 2018, items 650 and 927), excluding managers of only inactive infrastructure referred to in Article 4 item 1b of that act, private infrastructure referred to in Article 4 item 1c, and narrow-gauge railway infrastructure referred to in Article 4 item 1d of that act.
		Railway carrier referred to in Article 4 item 9 of the Act of 28 March 2003 on rail transport, the business of which is subject to licensing. and operator of a service infrastructure facility referred to in Article 4 item 52 of the Act of 28 March 2003 on railway transport, if the an entity performing the operator's function is also a railway carrier.
	Water transport	Shipowner in 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), with the exception of individual vessels on which these shipowners operate.
		Shipowner referred to in Article 5 paragraph 1 item 2 of the Act of 21 December 2000 on inland navigation (Journal of Laws of the Republic of Poland of 2017, item 2128 and of 2018, item 1137).
		Port managing entity referred to in Article 2 item 6 of the Act of 20 December 1996 on ports and marinas (Journal of Laws of the Republic of Poland of 2017, item 1933).
		Entity managing a port facility referred to 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 in the port area a business supporting maritime transport.

		VTS (Vessel Traffic Service) – an auxiliary service of the director of a maritime office established to monitor vessel traffic and provide information, which is a component of the SafeSeaNet National System, referred to in Article 91 of the Act of 18 August 2011 on maritime safety (Journal of Laws of the Republic of Poland of 2018, items 181 and 1137).
	Road transport	The bodies referred to in Article 19 paragraphs 2, 5 and 5a of the Act of 21 March 1985 on public roads (Journal of Laws of 2017, items 2222 and 2018, items 12, 138, 159 and 317).
		Entities referred to in Article 43a paragraph 1 of the Act of 21 March 1985 on public roads.
Banking and financial market infrastructures		Credit institution referred to in Article 4 paragraph 1 item 17 of the Act of 29 August 1997 – Banking law (Journal of Laws of the Republic of Poland of 2017, item 1876, as amended[3)]).
		National bank referred to in Article 4 paragraph 1 item 1 of the Act of 29 August 1997 – Banking law.
		Branch of a foreign bank referred to in Article 4 paragraph 1 item 20 of the Act of 29 August 1997 – Banking law.
		Branch of the credit institution referred to in Article 4 paragraph 1 item 18 of the Act of 29 August 1997 – Banking law.
		Cooperative savings and credit unions within the meaning of the Act of 5 November 2009 on cooperative savings and credit unions (Journal of Laws of the Republic of Poland of 2017, item 2065, as amended[4)]).
		Entity operating a regulated market as referred to in Article 14 paragraph 1 of the Act of 29 July 2005 on trading in financial instruments (Journal of Laws of the Republic of Poland of 2017, items 1768, 2486 and 2491, and of 2018, items 106, 138, 650, 685, 723 and 771).
		The entity referred to in Article 3 item 49 of the Act of 29 July 2005 on trading in financial instruments.
		The entity referred to in Article 48 item 7 of the Act of 29 July 2005 on trading in financial instruments.
Health sector		Medical entity referred to in Article 4 paragraph 1 of the Act of 15 April 2011 on medical activities (Journal of Laws of the Republic of Poland of 2018, items 160, 138, 650 and 1128).

3) Amendments to the consolidated text of the act were promulgated in Journal of Laws of 2017, items 2361 and 2491, and of 2018, items 62, 106, 138, 650, 723, 864, 1000 and 1075.

4) Amendments to the consolidated text of the act were promulgated in Journal of Laws of 2017, items 2486 and 2491, and of 2018, items 106, 138, 650, 723, 771, 864, 1000 and 1075.

		Entity subordinate to the minister competent for health matters, operating in the field of health information systems.
		National Health Fund.
		Medical entity in whose business operates a hospital pharmaceutical department, within the meaning of the Act of 6 September 2001 – Pharmaceutical law (Journal of Laws of the Republic of Poland of 2017, items 2211, and of 2018, items 650, 697 and 1039).
		Medical entity in whose business operates a hospital pharmacy, within the meaning of the Act of 6 September 2001 – Pharmaceutical law.
		An entity conducting a business consisting in running a pharmaceutical warehouse within the meaning of the Act of 6 September 2001 – Pharmaceutical law.
		An entity conducting a business in a Member State of the European Union or in a Member State of the European Free Trade Association (EFTA) – a party to the Agreement on the European Economic Area, who obtained the marketing authorisation for a medicinal product.
		Importer of a medicinal product/active substance within the meaning of the Act of 6 September 2001 – Pharmaceutical law.
		Manufacturer of a medicinal product/active substance within the meaning of the Act of 6 September 2001 – Pharmaceutical law.
		Parallel importer within the meaning of the Act of 6 September 2001 – Pharmaceutical law.
		Distributor of an active substance within the meaning of the Act of 6 September 2001 – Pharmaceutical law.
		An entity operating in the form of a generally accessible pharmacy within the meaning of the Act of 6 September 2001 – Pharmaceutical law.
Drinking water supply and distribution		Water and sewage service company referred to in Article 2 item 4 of the Act of 7 June 2001 on collective water supply and collective sewage disposal (Journal of Laws of the Republic of Poland of 2018, item 1152).
Digital infrastructure		DNS provider.
		Entity that operates an internet exchange point (IXP), which is a network facility that allows interconnection between more than two independent autonomous systems, mainly for facilitating the exchange of Internet traffic.
		Entity that manages the registration of Internet domain names as part of the top-level domain (TLD).

Annex 2 to the Act
of 5 July 2018
(item …)

DIGITAL SERVICES

Name of service	Definition of service
Online marketplace	A service allows consumers or entrepreneurs to conclude electronically contracts with entrepreneurs on the website of an online marketplace or on the website of an entrepreneur which uses services provided by the online marketplace.
Cloud computing service	A service that allow access to a scalable and elastic pool of shareable computing resources for many users.
Online search engine	A service allows users to search all websites or websites in a given language on the basis of a query by using a keyword, phrase or other element, which results in links that relate to information related to the query.